ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

СПЕЦИАЛЬНОСТЬ 09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

2024 год

СОДЕРЖАНИЕ

1 ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

1.1.Область применения

Фонд оценочных средств предназначен для контроля и оценки результатов освоения профессионального модуля «Настройка сетевой инфраструктуры» по специальности 09.02.06 Сетевое и системное администрирование в части освоения основного вида профессиональной деятельности (ВПД) «Настройка сетевой инфраструктуры», и соответствующих профессиональных компетенций (ПК) и общих компетенций (ОК):

ПК 1.1 Документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации

ПК 1.2. Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем.

ПК 1.3. Устранять неисправности в работе инфокоммуникационных систем

ПК 1.4. Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности.

ПК 1.5. Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем.

ПК 1.6 Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта.

ПК 1.7 Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем.

ОК 1 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 2. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности;

ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;

ОК 4. Эффективно взаимодействовать и работать в коллективе и команде

ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста

ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения

ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.

При реализации программы ПМ 01 «Настройка сетевой инфраструктуры», МДК.01.01 «Компьютерные сети» УП И ПП у обучающихся должны быть сформированы:

практический опыт:

ПО 1 проектирование архитектуры локальной сети в соответствии с поставленной задачей;

ПО 2 установке и настройке сетевых протоколов и сетевого оборудования в соответствии с конкретной задачей;

ПО 3 выборе технологии, инструментальных средств при организации

процесса исследования объектов сетевой инфраструктуры;

ПО 4 обеспечении безопасного хранения и передачи информации в локальной сети;

ПО 5 использовании специального программного обеспечения для моделирования, проектирования и тестирования компьютерных сетей

умения:

- У 1. проектировать локальную сеть, выбирать сетевые топологии
- У 2. использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети

знания:

- З 1. общие принципы построения сетей, сетевых топологий, многослойной модели OSI, требований к компьютерным сетям
- З 2. архитектуру протоколов, стандартизации сетей, этапов проектирования сетевой инфраструктуры
- З 3. базовые протоколы и технологии локальных сетей; принципы построения высокоскоростных локальных сетей
- З 4. стандарты кабелей, основные виды коммуникационных устройств, терминов, понятий, стандартов и типовых элементов структурированной кабельной системы

1.2. Формы контроля и оценивания элементов профессионального модуля

Элементы модуля, профессиональный модуль	Формы контроля и оценивания	
	Промежуточная аттестация	**Текущий контроль**
МДК 01.01 Компьютерные сети	Экзамен	Устный и письменный опрос; Тестирование; Оценка результатов выполнения практических работ; Контроль выполнения домашних и самостоятельных работ; Разбор ситуационных заданий.
МДК 01.02 Организация, принципы построения и функционирования компьютерных сетей	Экзамен	
УП Настройка сетевой инфраструктуры	Дифференцированный зачет	Оценка выполнения проверочных заданий по учебной практике; Наблюдение и оценка выполнения работ при прохождении учебной практики
ПП Настройка сетевой инфраструктуры	Дифференцированный зачет	Наблюдение и оценка выполнения работ при прохождении производственной практики
ПМ.01 Настройка сетевой инфраструктуры	Экзамен квалификационный	

1.3. Перечень оценочных средств и их характеристика

Формы контроля	**Виды контроля**	**Краткая характеристика**	**Формы контрольно-оценочного средства в фонде**
Текущий контроль успеваемости	Устный опрос	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемым МДК, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.	Вопросы для обсуждения

	Защита практических работ	Учебные занятия, которые направлены на экспериментальное подтверждение теоретических положений и формирование учебных и профессиональных практических умений и составляют важную часть теоретической и профессиональной практической подготовки.	Перечень практических работ
	Ситуационные задания	Проблемное задание, в котором обучающемуся предлагают осмыслить реальную профессионально-ориентированную ситуацию, необходимую для решения данной проблемы. Сущность данного метода состоит в том, что учебный материал подается обучающемуся в виде реальных профессиональных проблем конкретного предприятия или характерных для определенного вида профессиональной деятельности. Работая над решением кейса, обучающийся приобретает профессиональные знания, умения, навыки в результате активной творческой работы. Он самостоятельно формулирует цели, находит и собирает различную информацию, анализирует ее, выдвигает гипотезы, ищет варианты решения проблемы, формулирует выводы, обосновывает оптимальное решение ситуации.	Варианты заданий, ситуационных заданий составляются на основе типовых заданий.
	Домашняя и самостоятельная работа	Самостоятельная работа, домашняя работа - планируемая учебная, учебно-исследовательская, научно-исследовательская работа обучающихся, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.	Задания для самостоятельной работы выдается преподавателем дифференцированно согласно рабочей программе
	Тестирование	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Банк тестовых заданий, составляется на основе типовых заданий
Промежуточная аттестация	Дифференцированный зачет Экзамен квалификационный	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Задания, вопросы по учебному материалу, направленному на освоение компетенций и вида деятельности согласно требованиям федерального государственного образовательного стандарта.	Банк заданий, составляется на основе типовых заданий

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ МОДУЛЯ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

В результате контроля и оценки по профессиональному модулю осуществляется комплексная проверка следующих профессиональных и общих компетенций:

Показатели оценки результата освоения профессиональных компетенций

В результате оценки осуществляется проверка следующих объектов:

Предмет оценивания (*ПК,ОК,У,З,ПО)*	**Объекты оценивания**	**Показатели**
У.1. проектировать локальную сеть, выбирать сетевые топологии ПК 1.1-ПК 1.7 ОК 01-ОК 07	МДК 01.01. Компьютерные сети Раздел 01. Компьютерные сети. Тема 1.1. Введение в сетевые технологии	Документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем.
У.2. использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети ПК 1.1-ПК 1.7 ОК 01-ОК 07	Тема 1.2. Принципы маршрутизации и коммутации	Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем. Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем. Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта Устранять неисправности в работе инфокоммуникационных систем

3.3. базовые протоколы и технологии локальных сетей; принципы построения высокоскоростных локальных сетей ПК 1.1-ПК 1.7 ОК 01-ОК 07	МДК.01.02. Организация, принципы построения и функционирования компьютерных сетей Раздел 2. Организация, принципы построения и функционирования компьютерных сетей Тема 2.1. Маршрутизация и коммутация. Масштабирование сетей	Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности. Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем. Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем. Устранять неисправности в работе инфокоммуникационных систем
3.4. стандарты кабелей, основные виды коммуникационных устройств, терминов, понятий, стандартов и типовых элементов структурированной кабельной системы ПК 1.1-ПК 1.7 ОК 01-ОК 07	Тема 2.2. Соединение сетей.	Документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем. Документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации
ПО.4. использовании специального программного обеспечения для моделирования, проектирования и тестирования компьютерных сетей ПО.1. ПО.2. ПО.3. ПК 1.1-ПК 1.7 ОК 01-ОК 07	Учебная практика	проектирование архитектуры локальной сети в соответствии с поставленной задачей; установке и настройке сетевых протоколов и сетевого оборудования в соответствии с конкретной задачей; выборе технологии, инструментальных средств при организации процесса исследования объектов сетевой инфраструктуры; обеспечении безопасного хранения и передачи информации в локальной сети; использовании специального программного обеспечения для моделирования, проектирования и тестирования компьютерных сетей

ПО.4. использовании специального программного обеспечения для моделирования, проектирования и тестирования компьютерных сетей ПО.1. ПО.2. ПО.3. ПК 1.1-ПК 1.7 ОК 01-ОК 07	Производственная практика	проектирование архитектуры локальной сети в соответствии с поставленной задачей; осуществление регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем. установке и настройке сетевых протоколов и сетевого оборудования в соответствии с конкретной задачей; выборе технологии, инструментальных средств при организации процесса исследования объектов сетевой инфраструктуры; обеспечении безопасного хранения и передачи информации в локальной сети; использовании специального программного обеспечения для моделирования, проектирования и тестирования компьютерных сетей

3. ОЦЕНКА ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Основной целью оценки профессионального модуля является оценка умений и знаний, ПК и ОК.

Оценка профессионального модуля осуществляется с использованием следующих форм и методов контроля:

- практические занятия;
- тестирование;
- экзамен.

3.1 ТЕКУЩИЙ И РУБЕЖНЫЙ КОНТРОЛЬ

Материалы для проведения текущей и рубежной аттестации

Материально-техническое обеспечение фонда оценочных мероприятий

Контрольно-оценочные мероприятия проводятся в учебном кабинете Информатики.

- Оборудование учебного кабинета:
- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- учебная доска.

Технические средства обучения:

- компьютер с программным обеспечением
- мультимедийный проектор
- мультимедийное оборудование;

– принтер лазерный;

– сканер;

– аудиосистема;

– локальная сеть;

– подключение к глобальной сети Интернет.

Комплект оценочных средств

Комплект материалов для оценки сформированности общих и профессиональных компетенций по МДК.01.01 «Компьютерные сети», МДК.01.02 «Организация, принципы построения и функционирования компьютерных сетей», УП.01.01 "Настройка сетевой инфраструктуры", ПП.01.01 "Настройка сетевой инфраструктуры", ПМ.01 «Настройка сетевой инфраструктуры»

Задания рубежного контроля

Тестирование

МДК 01.01. Компьютерные сети

1) Предоставляющий свои ресурсы пользователям сети компьютер – это:

- Пользовательский
- Клиент
+ Сервер

2) Центральная машина сети называется:

- Центральным процессором
+ Сервером
- Маршрутизатором

3) Обобщенная геометрическая характеристика компьютерной сети – это:

+ Топология сети
- Сервер сети
- Удаленность компьютеров сети

4) Глобальной компьютерной сетью мирового уровня является:

+ WWW
- E-mail
- Интранет

5) Основными видами компьютерных сетей являются сети:

+ локальные, глобальные, региональные

- клиентские, корпоративные, международные

- социальные, развлекательные, бизнес-ориентированные

6) Протокол компьютерной сети - совокупность:

- Электронный журнал для протоколирования действий пользователей сети

- Технических характеристик трафика сети

+ Правил, регламентирующих прием-передачу, активацию данных в сети

7) Основным назначением компьютерной сети является:

+ Совместное удаленное использование ресурсов сети сетевыми пользователям

- Физическое соединение всех компьютеров сети

- Совместное решение распределенной задачи пользователями сети

8) Узловым в компьютерной сети служит сервер:

- Располагаемый в здании главного офиса сетевой компании

+ Связывающие остальные компьютеры сети

- На котором располагается база сетевых данных

9) К основным компонентам компьютерных сетей можно отнести все перечисленное:

+ Сервер, клиентскую машину, операционную систему, линии

- Офисный пакет, точку доступа к сети, телефонный кабель, хостинг-компанию

- Пользователей сети, сайты, веб-магазины, хостинг-компанию

10) Первые компьютерные сети:

+ ARPANET, ETHERNET

- TCP, IP

- WWW, INTRANET

11) Передачу всех данных в компьютерных сетях реализуют с помощью:

- Сервера данных

- E-mail

+ Сетевых протоколов

12) Обмен информацией между компьютерными сетями осуществляют всегда посредством:

+ Независимых небольших наборов данных (пакетов)

- Побайтной независимой передачи

- Очередности по длительности расстояния между узлами

13) Каналами связи в компьютерных сетях являются все перечисленное в списке:

- Спутниковая связь, солнечные лучи, магнитные поля, телефон

+ Спутниковая связь, оптоволоконные кабели, телефонные сети, радиорелейная связь

- Спутниковая связь, инфракрасные лучи, ультрафиолет, контактно-релейная связь

14) Компьютерная сеть – совокупность:

- Компьютеров, пользователей, компаний и их ресурсов

+ Компьютеров, протоколов, сетевых ресурсов

- Компьютеров, серверов, узлов

15) В компьютерной сети рабочая станция – компьютер:

+ Стационарный

- Работающий в данный момент

- На станции приема спутниковых данных

16) Указать назначение компьютерных сетей:

- Обеспечивать одновременный доступ всех пользователей сети к сетевым ресурсам

- Замещать выходящие из строя компьютеры другими компьютерами сети

+ Использовать ресурсы соединяемых компьютеров сети, усиливая возможности каждого

17) Составляющие компьютерной сети:

+ Серверы, протоколы, клиентские машины, каналы связи

- Клиентские компьютеры, смартфоны, планшеты, Wi-Fi

- E-mail, TCP, IP, LAN

18) Локальная компьютерная сеть – сеть, состоящая из компьютеров, связываемых в рамках:

- WWW

+ одного учреждения (его территориального объединения)

- одной города, района

19) Сетевое приложение – приложение:

- Распределенное

- Устанавливаемое для работы пользователем сети на свой компьютер

+ каждая часть которого выполнима на каждом сетевом компьютере

20) Наиболее полно, правильно перечислены характеристики компьютерной сети в списке:

- Совокупность однотипных (по архитектуре) соединяемых компьютеров

+ Компьютеры, соединенные общими программными, сетевыми ресурсами, протоколами

- Компьютеры каждый из которых должен соединяться и взаимодействовать с другим

21) Сеть, разрабатываемая в рамках одного учреждения, предприятия – сеть:

+ Локальная

- Глобальная

- Интранет

22) Маршрутизатор – устройство, соединяющее различные:

+ Компьютерные сети

- По архитектуре компьютеры

- маршруты передачи адресов для e-mail

23) Локальную компьютерную сеть обозначают:

+ LAN

- MAN

- WAN

24) Глобальную компьютерную сеть обозначают:

- LAN

- MAN

+ WAN

25) Соединение нескольких сетей дает:

+ Межсетевое объединение

- Серверную связь

- Рабочую группу

26) Основной (неделимой) единицей сетевого информационного обмена является:

+ Пакет

- Бит

- Канал

27) Часть пакета, где указаны адрес отправителя, порядок сборки блоков (конвертов) данных на компьютере получателя называется:

+ Заголовком

- Конструктор

- Маршрутизатор

28) Передача-прием данных в компьютерной сети может происходить

- Лишь последовательно

- Лишь параллельно

+ Как последовательно, так и параллельно

29) Компьютерная сеть должна обязательно иметь:

+ Протокол

- Более сотни компьютеров

- Спутниковый выход в WWW

30) Скорость передачи данных в компьютерных сетях измеряют обычно в:

- Байт/мин

- Килобайт/узел

+ Бит/сек

31) Сеть, где нет специально выделяемого сервера называется:

+ Одноранговой (пиринговой)

- Не привязанной к серверу

- Одноуровневой

32) Выделенным называется сервер:

+ Функционирующий лишь как сервер

- На котором размещается сетевая информация

- Отвечающий за безопасность ресурсов, клиентов

33) Сервер, управляющий клиентским доступом к файлам называется:

+ Файл-сервером

- Почтовым

- Прокси

34) Сервер для реализации прикладных клиентских приложений называется:

- Коммуникационным сервером

+ Сервером приложений

- Вспомогательным

35) Серверы для передачи-приема e-mail называют:

- Приемо-передающим

+ Почтовым

- Файловым

36) Поток сетевых сообщений определяется:

- Транзакцией

+ Трафиком

- Трендом

37) Правильно утверждение "Звезда"

- Топологию «Звезда» можно собрать из нескольких топологий «Кольцо»

+ Топологию «Дерево» можно собрать из нескольких топологий «Звезда»

- Топологию «Шина» можно собрать из нескольких топологий «Дерево»

38) Сетевая топология определяется способом, структурой:

- Аппаратного обеспечения
- Программного обеспечения
+ Соединения узлов каналами сетевой связи

Итоговый тест МДК.01.02. Организация, принципы построения и функционирования компьютерных сетей

1. К основным программным средствам защиты информации относятся:

#программы шифрования информации
#программы разграничения доступа пользователей к ресурсам КС
#программы идентификации и аутентификации пользователей КС
программы архивации данных

2.К созданию чего привело появление персональных компьютеров?

Многотерминальных систем

*Первых локальных сетей
Систем пакетной обработки

Глобальных сетей
Стандартных технологий локальных сетей

3.Исторически первые сети технологии Ethernet были созданы на кабеле:

толстом коаксиале
витой паре
*тонком коаксиале

оптоволоконном

4.Кабель, способный передавать большие объемы данных на большие расстояния, - это:
Коаксиальный кабель
Витая пара
*Оптоволоконный кабель

5.К какому оборудованию относят кабели, коннекторы и сетевые розетки, повторители и усилители сигнала?
активному
канальному
физическому
*пассивному

6. Конфигурация (топология) локальной компьютерной сети, в которой все рабочие станции соединены с сервером, называется:
полносвязная звезда
Кольцо
Шина
*звезда

7. Коаксиальный кабель имеет жилу, изготовленную из:
Стекла

*Меди
Пластика
Стали

8. Какая подсистема состоит из внутренних горизонтальных кабелей между кроссовой этажа и информационными розетками рабочих мест?

*горизонтальная

внешних магистралей

внутренних магистралей

9. Какие сети появились раньше?

*Глобальные

Локальные

Персональные

10. Удаленные соединения типа «терминал - компьютер» появились с созданием чего?

*Многотерминальных систем

Стандартных технологий локальных сетей

Первых локальных сетей

Глобальных сетей

Систем пакетной обработки

11.Установите соответствие между типом сетевого кабеля и его описанием:

Коаксиальный кабель Состоит из медной жилы, окружающей ее изоляции, экрана в виде металлической оплетки
и внешней оболочки

Витая пара Состоит из нескольких перевитых друг вокруг друга изолированных медных проводов

Оптоволоконный кабель Состоит из тонкой стеклянной жилы, покрытой слоем стекла с иным, чем у жилы,
коэффициентом преломления

12. Как называют незаконный мониторинг сети, захват и анализ сетевых сообщений?

незаконное проникновение в один из компьютеров сети под видом легального пользователя

нелегальные действия легального пользователя

*«подслушивание» внутрисетевого графика

разрушение системы с помощью программ-вирусов

13. Всегда маскируется под какую-нибудь полезную утилиту или игру, а производит действия, разрушающие систему: Исключить неверное

#Червь

#Шпион

#Рукит

Троянский конь

14. Кто автор идеи связать несколько компьютеров в одну сеть?

*Пол Бэрэн

Рей Томлинсон

Роберт Тейлор

15. Для подключения витой пары к компьютеру не используется:

RG-45

#RG-44

#RG-55

#RG-54

16. К основным аппаратным средствам защиты информации относятся:

#устройства для шифрования информации

#устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы)

#устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т. п.)

программные средства блокировки несанкционированного доступа

17. Тип кабеля, обеспечивающий самую высокую скорость передачи информации...
коаксиальный
*оптоволоконный
витая пара

18 . Какой уровень сетевой коммуникации (OSI), не включает сетевое оборудование - сетевые кабели, разъемы, концентраторы и т.д.?
#канальный
#сетевой физический

19 . Выберите обозначение кабеля на основе неэкранированной витой пары:
10Base-T
10Base-2
10Base-FL
10Base-F

20.Он использует в качестве среды передачи данных коаксиальный кабель с волновым сопротивлением 50 Ом, диаметром центрального медного провода 2,17 мм и внешним диаметром около 10 мм
10Base-T

10Base-F

*10Base-5

10Base-2

21. Различают три типа беспроводных сетей, выберите:

#WPAN

BWA

#WMAN

#WLAN

22. Существует три основных группы стандартов **Internet,** укажите

#Отраслевые

Американские

#Европейские

#Международные

23 Процедура анализа накопленной в результате протоколирования информации. Этот анализ может осуществляться оперативно в реальном времени или периодически, процедура называется:

Аутентификация

*Аудит

Средство управления доступом

Протоколирование

24 Гарантирует длину связи между повторителями до 1 км при общей длине сети не более 2500 м. Максимальное число повторителей между любыми узлами сети - 4

10Base-5

10Base-T

10Base-2

*10Base-F

25 В каком типе сетей безопасность находится на более высоком уровне?

В сетях на основе сервера

*В одноранговых сетях

26. Какие устройства не принимают сигналы из одного сегмента кабеля и побитно синхронно повторяет их в другом сегменте, улучшая форму и мощность импульсов, а также синхронизируя импульсы?

Повторитель

#Концентратор

#Мост

#Шлюз

27 . Оборудование, которое способно обрабатывать или преобразовывать передаваемую по сети информацию называют:

пассивным сетевым оборудованием

интерактивным сетевым оборудованием

*активным сетевым оборудованием

28 Какие беспроводные сети работают в нелицензионных диапазонах частот 2,4 и 5 ГГц, т. е. при их развертывании не требуется частотного планирования и координации с другими радиосетями, работающими в том же диапазоне

#WPAN

BWA

WAN

#WLAN

30 . Какой протокол не предназначен для автоматизации назначения ip-адресов в локальных сетях?

#RIP

#PPP

#TCP/IP

DHCP

31. Подтверждение того, что предъявленное имя соответствует данному субъекту (подтверждение подлинности субъекта) называют:

*Аутентификация

Аккредитация

Идентификация

32 Что не относится к линии связи?

абоненты сети

#Станции

#передающая среда

33 Проектирование СКС разделяют на две основные стадии: телекоммуникационную и:

структурную

подготовительную

*архитектурную

35 Возможность радиоустройства перемещаться за пределы действия базовой станции и, находясь в зоне действия "гостевой" станции, иметь доступ к "домашней" сети называется:

Адаптируемость

Фишинг

*Роуминг

36 Компьютер, предоставляющий свои ресурсы другим компьютерам при совместной работе. Исключить неверное

#Адаптером

Сервером

#рабочей станцией

#коммутатором

37 Как называлась первая компьютерная сеть?

*Arpanet

Nercnet

Relcom

38 Какое устройство является основополагающим устройством в структуре беспроводной сети, которое отвечает за объединение всех элементов сети в единое целое?

*Точка доступа

маршрутизатор (router)

антенны Wi-Fi точек доступа

коммутатор (switch)

39 Весь входящий во внутреннюю сеть и выходящий во внешнюю сеть трафик должен проходить через единственный узел сети, например, через межсетевой экран (firewall) –

*это принцип политики безопасности:

использование комплексного подхода к обеспечению безопасности

принцип единого контрольно-пропускного пункта

использование средств, которые при отказе переходят в состояние максимальной защиты

40 Такая подсистема состоит из магистральных кабелей, положенных между кроссовой здания и кроссовыми этажей.
*Горизонтальная
внутренних магистралей
внешних магистралей

41 Укажите правильную аббревиатуру экранированной витой пары:
#STP
UDP
#FTP
#UTP

42 Включает требования заказчика по числу рабочих мест, их расположению, категории или классу системы. Этажные планы здания позволяют наглядно отобразить расположение различных элементов систем, оценить их параметры
#Технический проект
#Техническое задание
Техническая документация

43 Электронные и электронно-механические устройства, включаемые в состав технических средств КС и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности относят к:
*аппаратным средствам защиты
антивирусным средствам защиты
программным средствам защиты

44 Первое слово, которым обменялись по сети...

*Hello Wolld

Password

Login

45 .Такие угрозы в сети могут ограничиваться либо пассивным чтением данных или мониторингом системы, либо включать в себя активные действия, например, нарушение целостности и доступности информации:

*Умышленные

Спланированные

не умышленные

46 Для работы технологии Bluetooth наличие прямой видимости:

*Обязательно

Необязательно

Желательно

47. Что называют компьютерной сетью?

*Совокупность компьютеров, соединенных линиями связи

Совокупность компьютеров, находящихся в одном помещении

Совокупность всего коммуникационного оборудования, находящегося в одном помещении

48. Петлевидное соединение концентраторов в стандарте _____запрещено, так как оно приводит к некорректной работе сети.

10Base-2

*10Base-T

10Base-5

10Base-F

49. Какого типа коаксиального кабеля не существует?

Толстый

Тонкий

*Средний

50. Беспроводные локальные сети создаются на основе какого семейства стандартов?

*IEEE 802.11

IEEE 802.9

IEEE 802.4

IEEE 802.3

51 Wreless fidelity расшифровывается как:

Шифрование данных

*Беспроводная связь

Проводная связь

Сетевая активность

52. Какое сетевое устройство принимает сигнал от одного компьютера и рассылает его сразу на все свои порты, то есть всем компьютерам в сети?

Сетевой мост

Повторитель

*Концентратор

Сетевая карта

Маршрутизатор

53. Основной задачей этой стадии проектирования СКС является определение общей структуры, оптимальной по комплексу технико-экономических характеристик в процессе создания и последующей эксплуатации.

*Архитектурной

телекоммуникационной

54.Небольшая организация (5 сотрудников) собирается построить сеть. Какой тип сети является для нее наиболее приемлемым?

Сеть с выделенным сервером

#Одноранговая сеть

персональная сеть

55.Обычно состоит из разъема для сетевого проводника (обычно, витой пары) и микропроцессора, который кодирует/декодирует сетевые пакеты.

Терминатор

Маршрутизатор

Сетевой мост

*Сетевая карта

56. Программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами называют:

Провайдер

Webserver

*Firewall

Трафик

57. Укажите все характеристики компьютерной сети.

#Компьютерная сеть - группа компьютеров, соединенных с помощью специальной аппаратуры

#Компьютерная сеть - несколько компьютеров, используемых для схожих операций

#Обязательное наличие сервера

#В сети возможен обмен данными между любыми компьютерами

#Компьютеры должны соединяться непосредственно друг с другом

58. Представляет собой иерархическую кабельную систему здания или группы зданий, разделенную на структурные подсистемы.

ИКС

КСП

СКВ

*СКС

59.Предоставление каждому сотруднику предприятия того минимально уровня привилегий на доступ к данным, который необходим ему для выполнения его должностных обязанностей является принципом:

* Административной ответственности

Политики безопасности

Морально-этических норм в сети

60. Какой из уровней эталонной модели OSI не осуществляет управление потоком и восстановление после ошибки?

Транспортный уровень.

#Сетевой уровень.

#Уровень представлений.

#Уровень приложений.

61.Пропускная способность канала передачи информации измеряется в:

Мбайт

Кбайт

Мбит

Байт

Мбайт/с

Мбит/с

*Бит/с

Кбайт/с

62.Какие протоколы из перечисленных являются протоколами сжатия данных?

MNP-1

MNP-3

*MNP-5

MNP-9

V.42

MNP-7

*V.42bis

MNPX

MNP-8

63.HTML – это

*язык разметки гипертекста

Гиперссылка

протокол передачи данных

сервис Internet

64.Эталонная модель OSI является многоуровневой. Какое из положений неправильно характеризует причину многоуровневости модели?
Многоуровневая модель предотвращает влияние изменений в одной области на другие области.
*Многоуровневая модель увеличивает сложность.
Многоуровневая модель стандартизирует интерфейсы.
Многоуровневая модель дает возможность разработчикам сконцентрировать усилия на более специализированных направлениях.

65.Синонимом маршрутизатора является. Исключить неверное
#Хаб
Роутер
#Коммутатор
#Шлюз

66.Основными элементами модели OSI являются:
протоколы и прикладные процессы
*уровни, прикладные процессы и физические средства соединения
уровни и прикладные процессы
Уровни
протоколы, прикладные процессы и физические средства соединения

67.Протокол транспортного уровня с установлением соединения называется
SSL
IP
*TCP
FTP

68. Основные пути использования сети INTERNET:
*Удаленное управление - запрос и запуск программ на удаленном компьютере.

*Chat-разговор с помощью сети IRC и Электронной почты

*Отправка и получение файлов с помощью FTP

*Игры

*Электронная почта.

*Чтение и посылка текстов в USENET

*Поиск информации

69.Сколько бит содержит IP-адрес?

*32

16

8

4

70. Выбери корректный адрес электронной почты:

ivanpetrov@mail

ivan_petrov.mail.ru

ivan petrov.mail.ru

*ivan_petrov@mail.ru

71.Какой домен верхнего уровня означает «военная организация»?

com

gov

*mil

edu

72. Достоинство архитектуры TCP/IP

упрощение процедуры маршрутизации

возможность работы в реальном масштабе времени

введение процедур контроля и исправления ошибок в сообщениях

применение каналов хорошего качества

73.Комплекс аппаратных и программных средств, не позволяющие компьютерам обмениваться данными, это:

#магистраль

#интерфейс

#шины данных

компьютерная сеть

74.Какой кабель обеспечивает скоростью передачи данных до 10 Мбит/с?

*коаксиальный

витая пара

оптоволокно

нет правильного мнения

75.В домене google.com.ru домен «com» является:

доменом 1-го уровня

доменом 2-го уровня

*доменом 3-го уровня

76.Дан URL-адрес: http:\\zooclab.ru\cats\porody\index.html . Выбери правильные соответствия: http:\\ - это…

Доменное имя

Имя файла

*Протокол

Путь

77.Какие компоненты вычислительной сети необходимы для организации одноранговой локальной сети?

*Модем, компьютер-сервер

Сетевая плата, сетевое программное обеспечение

Компьютер-сервер, рабочие станции

Линии связи, сетевая плата, сетевое программное обеспечение

78.Дан URL-адрес: http:\\zooclab.ru\cats\porody\index.html . Выбери правильные соответствия: cats\parody\ - это…

Доменное имя

Имя файла

Протокол

*Путь

79.Какой кабель обеспечивает скоростью передачи данных до 10 Мбит/с?

*Коаксиальный

Витая пара

оптоволокно

Нет правильного ответа

80.Модем, передающий информацию со скоростью 28.800 бит/с, за 1 секунду сможет передать:

Видеофайл (3,6 Мбайт)

*Две страницы (3600 байт)

Аудиофайл (360 Кбайт)

Рисунок (36 Кбайт)

81.Для просмотра WEB-страниц предназначены:

Поисковые серверы

*Браузеры

Телеконференции

Провайдеры

82.Протокол HTTP служит для:

*Передачи гипертекста

Передачи файлов

Управления передачи сообщениями

Запуска программы с удаленного компьютера

83. Все многообразие компьютерных сетей можно классифицировать по следующим признакам

способ организации сети; территориальная распространенность; ведомственная принадлежность;

*скорость передачи информации; тип среды передачи; топология;

организация взаимодействия компьютеров.

все перечисленные варианты ответов

84. Доступом к сети называют:

*взаимодействие станции (узла сети) со средой передачи данных для обмена информацией с другими станциями;

взаимодействие станции со средой передачи данных для обмена информацией с друг с другом;

это установление последовательности, в которой станции получают доступ к среде передачи данных;

это установление последовательности, в которой серверы получают доступ к среде передачи данных.

85.К недостаткам иерархической сети, по сравнению с одноранговыми сетями, относятся:

необходимость дополнительной ОС для сервера

более высокая сложность установки и модернизации сети

необходимость выделения отдельного компьютера в качестве сервера

*все перечисленные варианты ответов

86. IP – адрес: (выберите несколько вариантов)
#может повторяться для разных серверов в Интернет
#уникальный адрес для каждого сервера в Интернет
состоит из 3-х чисел, находящихся в диапазоне от 0 до 255
состоит из 4-х чисел, находящихся в диапазоне от 0 до 255

87. Задан адрес электронной почты в сети Интернет: user_name@mtu- net. Ru. Каково имя владельца этого электронного адреса?
mtu-net.ru
*user_name
user_name@
Ru
mtu-net

Задачи:
A
1. Паше в институте дали задание проверить IP адрес на своём компьютере через терминал (командная строка), ведя стандартный код.
[IPCONFIG]

2. Паше в институте дали задание провести трассировку сайт института через терминал (командная строка), введя стандартный код.
[TRACERT]

3. Домен верхнего уровня учебного заведения в Internet
[edu]

4. Компьютер в сети Интернет, осуществляющий доступ к ресурсам другого компьютера, которые предоставляются в совместное использование, называется-

[клиентом]

5. Саша при обжимке кабеля не снял полностью верхнюю изоляцию и при этом потерял один провод. Какого провода не хватает Саше если он вытянул 7 цветов: бело-оранжевый, оранжевый, бело-зелёный, бело-синий, зелёный, бело-коричневый, коричневый.
[синий]

6. Саша при обжимке кабеля не снял полностью верхнюю изоляцию и при этом потерял один провод. Какого провода не хватает Саше если он вытянул 7 цветов: бело-оранжевый, бело-зелёный, синий, бело-синий, зелёный, бело-коричневый, коричневый.
[оранжевый]

7. На заводе при изготовлении кабеля, устройство подбирающий цвета проводов вышел из строя, и стал комплектовать лишь 7 цветов провода, какого провода не хватает, если есть цвета: бело-оранжевый, оранжевый, бело-зелёный, синий, бело-синий, бело-коричневый, коричневый.
[зеленый]

8. Конфигурация локальной сети, при которой все ПК подсоединяются к одной линии связи.
[шина]

9. Компьютерная сеть, созданная в 1969 году в США Агентством Министерства обороны США по перспективным исследованиям (DARPA) и явившаяся прототипом сети Интернет.
[ARPANET]

10. Это конфигурация графа, вершинам которого соответствуют конечные узлы сети (компьютеры) и коммуникационное оборудование (маршрутизаторы), а рёбрам — физические или информационные связи между вершинами. физической — описывает реальное расположение и связи между узлами сети.
[топология]

11. Какое устройство, принимая решение о дальнейшем перемещении пакета, выходит из информации о доступности канала и степенях его загрузки?
[маршрутизатор]

12. Задан адрес электронной почты в сети Интернет: fortuna@list.ru. Какое имя у почтового адреса?
[fortuna]

13. Какой домен верхнего уровня означает "образовательный сайт"?
[edu]

14. Определите номер компьютера в сети по IP 215.128.255.106
[106]

15.Общая схема соединения компьютеров в локальные сети называется...
[топология]

16. MAC -адрес представляет собой двоичное число длиной
[48]

17. Какой из уровней эталонной модели OSI осуществляет управление потоком и восстановление после ошибки?
[Транспортный]

18. Протокол Ethernet рассчитан на топологию:
[Звезда]

19. Протокол передачи файлов называется
[FTP]

20. Протокол транспортного уровня с установлением соединения называется
[TCP]

21. Протокол, который защищает данные, пересылаемые между Web-браузерами и Web-серверами, называется
[SSL]

22. Устройство, производящее преобразование аналоговых сигналов в цифровые и обратно, называется:
[сетевая карта]

23. Пропускная способность канала передачи информации измеряется в:
[Мбит/с]

24. совокупностью правил, регулирующих порядок обмена данными в сети
[Протокол]

25. В домене google.com.ru доменом какого уровня является ru?
[1]

26.В продуктовом магазине нужно данные внести в базу данных и после чего отправить ее на компьютер директора. Как и с помощью чего мы можем это сделать?

[Сети]

27.Данные передаются от одного компьютера к другому, если один компьютер получает данные, предназначенные для другого, то он их передает дальше. О какой топологии идет речь?

[кольцо]

28.Открыв организацию Иванов решил узнать у специалиста про топологию сети, сигналы по которым передается в одном направлении и проходят через каждый компьютер . Каким видом топологии сети интересуется Иванов?

[кольцо]

29.В корпорации при передачи данных с двух устройств произошла ошибки. При выявлении проблемы было обнаружено что сеть построена по топологии шина . Вопрос как называется эта ошибка?

[коллизия]

30.Абдуллаев приобрел компьютер и решил подключиться по локальной сети к ноутбуку брата. Какой вид кабеля необходим Абдуллаеву для подключения к локальной сети?

[витая]

31.Преподавателем компьютерных сетей была изложена студентам лекция топологии сетей, в ней рассматривалась одна из топологий сети, на основе которой находится сервер. Какая это топология сети?

[звезда]

32.После покупки компьютера Сидоров никак не мог подключиться к сети. Рассматривая системный блок, им было замечено отсутствие одной из плат. Назовите отсутствующую плату?

[сетевая]

33.Компьютер Магомедова взаимодействуют с компьютером Иванова, служившим с ним в армии; Какая плата компьютера, позволяет выходить в сеть и совершать это взаимодействие?

[сетевая]

34. Через дополнительную сетевую плату, подключенную к ноутбуку с USB интерфейса, Катя передала курсовую на свой компьютер. Назовите, какая сетевая плата разрешает совершить подключение через USB интерфейса?

[внешняя]

35.В офисе Дагнет не было возможности и удобства к каждому компьютеру подключить сетевой кабель для выхода в Интернет . И один из специалистов установил устройство позволяющее выход интернет без подключения сетевого кабеля . Какое это устройство ?

[роутер]

36. Вам необходимо объединить 5 компьютеров лечебного отделения ЛПУ в сеть. Какое оборудование для этого потребуется?

[Коммутатор]

37.Для того чтобы в процессе обмена информацией компьютеры Петра и Ивана могли найти друг друга в Интернете, существует единая система адресации. Как называется этот адрес?

[IP]

38. В университете потребовалось вести новые «IP адреса» для удобства адреса ввели следующие характеристики : если корпус находится на 10 улице, во 2 этаже и ввести адрес на 1 компьютер.

[10.2.0.1]

39.Компьютеры легко могли найти друг друга по числовому IP-Адресу, однако человеку запомнить числовой адрес было нелегко, и для удобства была введена система. Какая система была введена?

[DNS]

40.Компания Rumbler зарегистрирован домен второго уровня Rumbler в коммерческом домене верхнего уровня. Какой будет коммерческий домен?

[COM]

41.Компьютеры легко могли найти друг друга по числовому IP-Адресу,однако человеку запомнить числовой адрес было нелегко, и для удобства была введена система. Какая система была введена?

[домен]

42.Компания Microsoft зарегистрировали домен второго уровняMicrosoft в географическом домене России верхнего уровня. Какой будет географический домен России?

[RU]

43.Иванов имеет выход в Интернет или в мировую паутину ,обеспечивает доступ к специальным серверам информацией. Выход, в какую сеть имеет Петр Иванов?

[Глобальная сеть]

44. Ребенку 10 лет. Он живет в Якутии с родителями. Ему необходима консультация с директором Научного Центра сердечно-сосудистой хирургии им. А.Н.Бакулева академика Л. А. Бокерия. Но он находится

в Москве. Как можно проконсультироваться ребенку не выезжая в Москву?

[Интернет]

45.3 Друг Пети рассказал ему о корпоративной и региональной сети ,но не успел рассказать ему сеть, которая объединяет эти сети .Про какую сеть не узнал Петя?

[глобальная]

46.Какой кабель изображен на картинке?

[витая пара]

47.Конфигурация локальной сети, при которой все ПК подсоединяются к одной линии связи.

[шина]

48.Это конфигурация графа, вершинам которого соответствуют конечные узлы сети (компьютеры) и коммуникационное оборудование (маршрутизаторы), а рёбрам — физические или информационные связи между вершинами. физической — описывает реальное расположение и связи между узлами сети.

[топология]

49Какой кабель изображен на картинке?

[коаксиальный]

50.7. Как называется это устройство?

[кримпер]

51.Устройство, предназначенное для взаимодействия пользователя или оператора с ПК или автоматизированной системой, включающее в свой состав средства ввода и вывода данных

[терминал]

52.Домен верхнего уровня коммерческой организации в Internet

[com]

53.Какие две технологии улучшают способность удаленных сотрудников безопасно подключаться к внутренним ресурсам компании? [VPN]

54. Протокол предназначенный для передачи электронных сообщений

[POP]

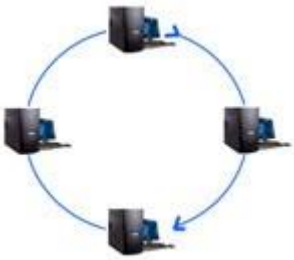
55. Набор правил, обусловливающих порядок обмена информации в сети

[протокол]

Задачи В

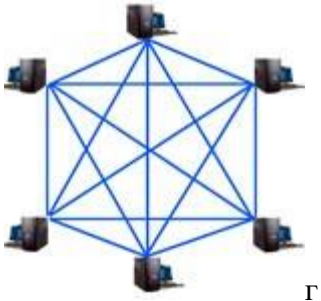
1.Выберите вариант топологии сети, типа "звезда":

а



б

в

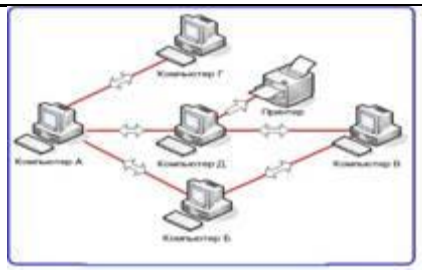


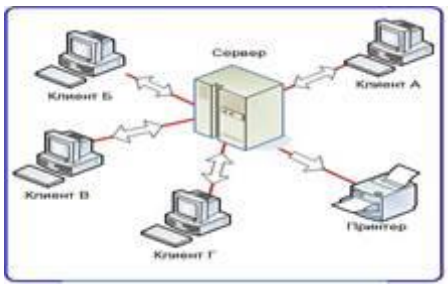
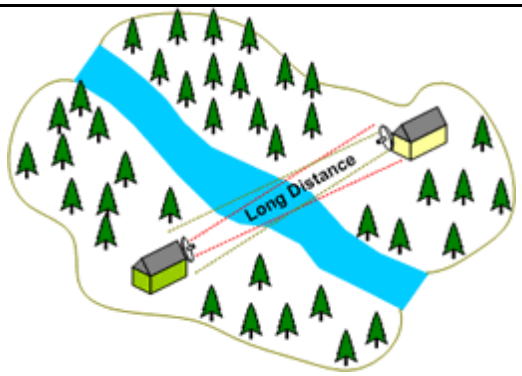
г

[а]

2.Установите соответствие:

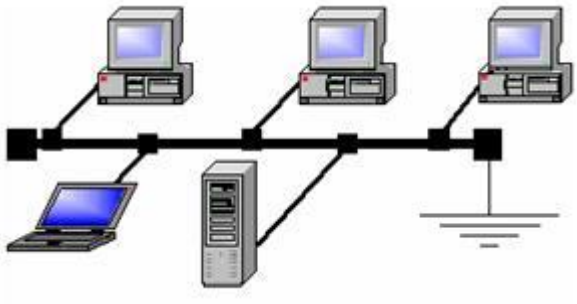
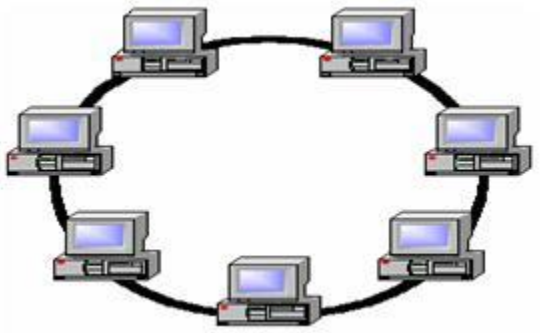
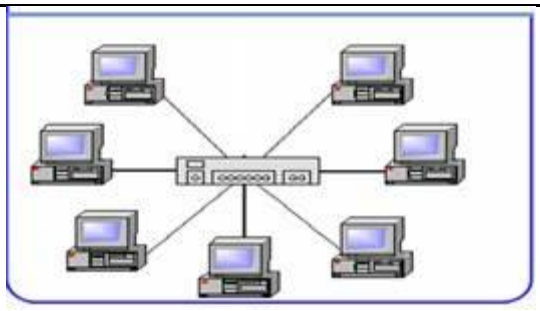
По типу организации компьютерные сети бывают:

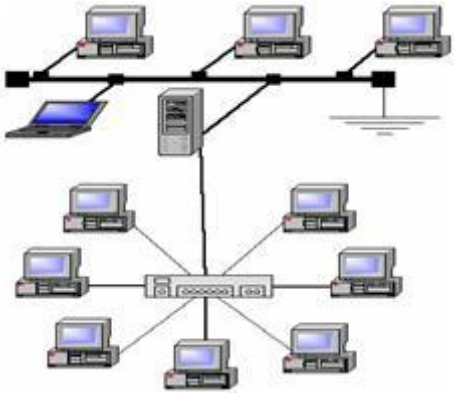
А		1	Беспроводная сеть

Б		2	Одноранговая сеть
В		3	Сеть на основе сервера

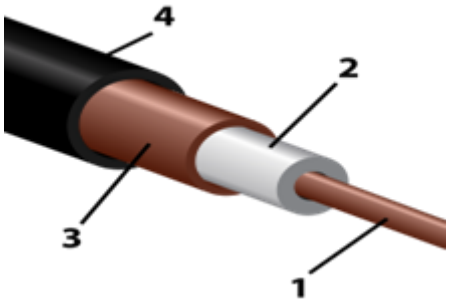
Ответ: а-2, б-3,в-1

3. Установите соответствие:

А		1	Топология «звезда»
Б		2	Топология «шина»
В		3	«Смешанная» топология

Г		4	Топология «кольцо»

Ответ: а-2, б-4, в-1, г-3

Установите соответствие передающих сред:А		1	Витая пара
Б		2	Коаксиальный кабель
В		3	Оптиковолокно

Ответ: а-2, б-1, в-3

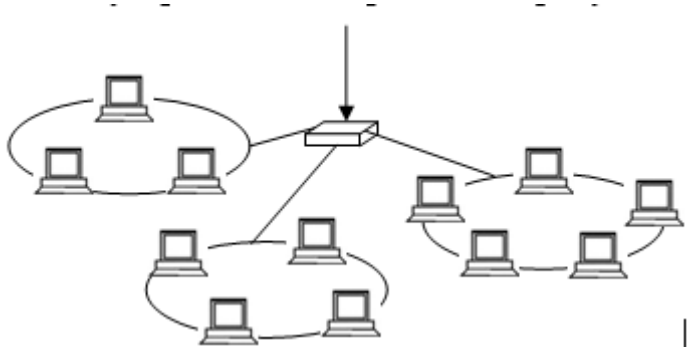
5. Установите соответствие:

1. Локальная сеть	а) объединяет в себе тысячи локальных, отраслевых, региональных глобальных компьютерных сетей в общее информационное пространство
2. Городские, региональные сети	б) объединяют сотни, тысячи узлов компьютерных сетей во многих странах мира

3. Глобальные сети	в) в пределах одного города, региона, связывающие множество локальных сетей
4. Интернет	г) соединение компьютеров в пределах одного помещения, предприятия протяженностью1-2 км

Ответ: 1-г,2-в,3-б, 4-а

6. Какое устройство изображено на рисунке?



[Концентратор]

7. Укажите уровень модели OSI, который не подписан на рисунке.

7	Прикладной
6	
5	Сеансовый
4	Транспортный
3	Сетевой
2	Канальный
1	Физический

[представительный]

8. Паше в институте дали задание проверить IP адрес на своём компьютере через терминал (командная строка), ведя стандартный код.
[IPCONFIG]

9. Паше в институте дали задание провести трассировку сайт института через терминал (командная строка), введя стандартный код.
[TRACERT]

10.. Саша при обжимке кабеля не снял полностью верхнюю изоляцию и при этом потерял один провод. Какого провода не хватает Саше если он вытянул 7 цветов: бело-оранжевый, оранжевый, бело-зелёный, бело-синий, зелёный, бело-коричневый, коричневый.

[синий]

11. Саша при обжимке кабеля не снял полностью верхнюю изоляцию и при этом потерял один провод. Какого провода не хватает Саше если он вытянул 7 цветов: бело-оранжевый, бело-зелёный, синий, бело-синий, зелёный, бело-коричневый, коричневый.

[оранжевый]

12. Задан адрес электронной почты в сети Интернет: fortuna@list.ru. Какое имя у почтового адреса?

[fortuna]

13. Дан URL-адрес: http:\\zooclab.ru\cats\porody\index.html. http:\\ - это....

[Протокол]

14. Конфигурация локальной сети, при которой все ПК подсоединяются к одной линии связи.

[шина]

15. В университете потребовалось вести новые «IP адреса» для удобства адреса ввели следующие характеристики : если корпус находится на 10 улице, во 2 этаже и ввести адрес на 1 компьютер.

[10.2.0.1]

16. В университете потребовалось вести новые «IP адреса» для удобства адреса ввели следующие характеристики : если корпус находится на 15 улице, во 3 этаже и ввести адрес на 5 компьютер.

[15.3.0.5]

17. Какой уровень эталонной модели OSI устанавливает, обслуживает и управляет сеансами взаимодействия прикладных программ?
[сеансовый]

18. Устройство, предназначенное для взаимодействия пользователя или оператора с ПК или автоматизированной системой, включающее в свой состав средства ввода и вывода данных
[терминал]

19. Это конфигурация графа, вершинам которого соответствуют конечные узлы сети (компьютеры) и коммуникационное оборудование (маршрутизаторы), а рёбрам — физические или информационные связи между вершинами. физической — описывает реальное расположение и связи между узлами сети.
[топология]

20. На заводе при изготовлении кабеля, устройство подбирающий цвета проводов вышел из строя, и стал комплектовать лишь 7 цветов провода, какого провода не хватает, если есть цвета: бело-оранжевый, оранжевый, бело-зелёный, синий, бело-синий, бело-коричневый, коричневый.
[зеленый]

21. Вам необходимо объединить 5 компьютеров лечебного отделения ЛПУ в сеть. Какое оборудование для этого потребуется?
[Коммутатор]

22. Допустим вы владелец крупной организации в городе Хасавюрт , а в других городах также есть филиалы, какую из сетей вы установите в вашей организации?
[Региональная]

23. Компьютер Магомедова взаимодействуют с компьютером Иванова, служившим с ним в армии; Какая плата компьютера, позволяет выходить в сеть и совершать это взаимодействие?
[сетевая]

24. Через дополнительную сетевую плату, подключенную к ноутбуку с USB интерфейса, Катя передала курсовую на свой компьютер. Назовите, какая сетевая плата разрешает совершить подключение через USB интерфейса?
[внешняя]

25. Вы решили создать адрес электронной почты. Для этого вам нужно задать имя пользователя и имя сервера. Но вы хотите создать электронную почту на коммерческом сервере. Какой будет домен коммерческого сервера?
[COM]

26. Набор правил, обусловливающих порядок обмена информации в сети
[протокол]

27. Данные передаются от одного компьютера к другому, если один компьютер получает данные, предназначенные для другого, то он их передает дальше. О какой топологии идечь речь?
[кольцо]

28. В компанию Мобильные Телесистемы (МТС) у системного администратора находиться компьютер высокопроизводительный, обслуживающий узел, с большим объемом памяти на жестком диске. Также этот компьютер обеспечивает связь между машинами- пользователями. Как называется этот компьютер?

[хост]

29. В новый открытый офис был вызван программист для объединения нескольких устройств Internet в общий сегмент. Как называется устройство для объединения этих сегментов
[хаб]

30. При установке IP- адресов в 2 компьютера были введены одинаковые числа, что при этом произойдёт?
[Конфликт]

31. Устройство, предназначенное для взаимодействия пользователя или оператора с ПК или автоматизированной системой, включающее в свой состав средства ввода и вывода данных
[Терминал]

32. Синонимом маршрутизатора является-
[Роутер]

33. Устройство, производящее преобразование аналоговых сигналов в цифровые и обратно, называется:
[сетевая карта]

34. Технология Ethernet определяется стандартом IEEE :
[802.3]

35. Какое устройство, принимая решение о дальнейшем перемещении пакета, выходит из информации о доступности канала и степенях его загрузки :
[Маршрутизатор]

36. Сети компьютеров, размещенные на небольшой территории и которые для связи используют высококачественные линии связи, это
[LAN]

37. Установите соответствие:
Компьютерные сети классифицируются по:

1. Типу организации компьютеров в сети	а) Одноранговая сеть и сеть на основе сервера
2. По топологии	г) Характеризует физическое расположение компьютеров, кабелей и других компонентов сети
3. По масштабам	б) Локальные, городские, глобальные
4. По типу передающей среды	в) Проводные, беспроводные

Ответ: 1-а, 2-г, 3-б, 4-в

38. Установите соответствие между организациями и их доменными именами :

А) организация которая работает с сетью	1)gov
Б) правительственная	2) com
В) некоммерческая	3) edy
Г) образование	4) net
Д) коммерческая	5) org

Ответ:а-4, б-1, в-5, г-3, д-2

39. Установите соответствие между видами сетей и их характеристиками охватывания территории сетью

А) персональная сеть	1) охватывает большие территории, соединяет отдельные сети и компьютеры для взаимодействия с другими объектами глобальной сети

Б) локальная	2) объединяет персональные электронные устройства (телефон, карманный компьютер, смартфон, ноутбук)
В) городская	3) охватывает отдельные сети и отдельные компьютера на территории определенного региона
Г) Глобальная	4) работает в нескольких или всех районах города
Д) Региональная	5) охватывает небольшую территорию или несколько строений

Ответ: а-2, б-5, в-4, г-1, д-3

40. Установите соответствие:

1. Локальная сеть	а) объединяет в себе тысячи локальных, отраслевых, региональных глобальных компьютерных сетей в общее информационное пространство
2. Городские, региональные сети	б) объединяют сотни, тысячи узлов компьютерных сетей во многих странах мира
3. Глобальные сети	в) в пределах одного города, региона, связывающие множество локальных сетей
4. Интернет	г) соединение компьютеров в пределах одного помещения, предприятия протяженностью1-2 км

Ответ: 1-г,2-в,3-б, 4-а

41. Установите соответствие между протоколом и его назначением:

1.HTTP	а) протокол передачи гипертекста
2. TCP	б) протокол маршрутизации
3. IP	в) транспортный протокол
4. FTP	г) протокол передачи файлов

Ответ:1-а,2-в,3-б,4-г

40. Установите соответствие:

1. Локальная сеть	а) объединяет в себе тысячи локальных, отраслевых, региональных глобальных компьютерных сетей в общее информационное пространство
2. Городские, региональные сети	б) объединяют сотни, тысячи узлов компьютерных сетей во многих странах мира
3. Глобальные сети	в) в пределах одного города, региона, связывающие множество локальных сетей
4. Интернет	г) соединение компьютеров в пределах одного помещения, предприятия протяженностью1-2 км

Ответ: 1-г,2-в,3-б, 4-а

41. Установите соответствие между протоколом и его назначением:

1.HTTP	а) протокол передачи гипертекста
2. TCP	б) протокол маршрутизации
3. IP	в) транспортный протокол
4. FTP	г) протокол передачи файлов

Ответ:1-а,2-в,3-б,4-г

42. Установите соответствие:

1	Сервер	в	специальный компьютер, который предназначен для удаленного запуска приложений, обработки запросов на получение информации из баз данных и обеспечения связи с общими внешними устройствами
2	Рабочая станция	а	это персональный компьютер, позволяющий пользоваться услугами, предоставляемыми серверами
3	Сетевая технология	г	согласованный набор стандартных протоколов, реализующих их программно-аппаратных средств, достаточный для построения компьютерной сети и обслуживания ее пользователей

4	Информационно-коммуникационная технология	б	это информационная технология работы в сети, позволяющая людям общаться, оперативно получать информацию и обмениваться ею

Ответ:1-в,2-а,3-г,4-б

43. В университете потребовалось вести новые «IP адреса» для удобства адреса ввели следующие характеристики : если корпус находится на 10 улице, во 2 этаже и ввести адрес на 1 компьютер.
[10.2.0.1]

44. В университете потребовалось вести новые «IP адреса» для удобства адреса ввели следующие характеристики : если корпус находится на 15 улице, во 3 этаже и ввести адрес на 5 компьютер.
[15.3.0.5]

45. В университете потребовалось вести новые «IP адреса» для удобства адреса ввели следующие характеристики : если корпус находится на 20 улице, во 1 этаже и ввести адрес на 10 компьютер.
[20.1.0.10]

46. Ученик продиктовал своей маме по телефону IP-адрес, мама его записала так: 2574125136. В ответе запишите IP-адрес с разделительными точками.
[25.74.125.136]

47. Определите скорость канала связи (радиодоступ) в Кбайтах/с, если передача изображения объемом 2 Мбайта заняла 1,2 мин. В ответе запишите целое число
[28]

48. Какой уровень модели OSI является самым верхним?

[прикладной]

49. Сети где все компьютеры равноправны
[Одноранговые]

50. Скорость передачи данных через ADSL-соединение равна 256000 бит/с. Передача файла через данное соединение заняла 3 минуты. Определите размер файла в килобайтах.
[5625]

51. Скорость передачи данных через ADSL-соединение равна 128000 бит/с. Через данное соединение передают файл размером 625 Кбайт. Определите время передачи файла в секундах
[40]

52. Скорость передачи данных через ADSL – соединение равна 1024000 бит/с. Передача
файла через данное соединение заняла 5 секунд. Определите размер файла в килобайтах
[625]

53. Текст подготовлен для передачи по сети и содержит 512000 символов. Каждый символ кодируется двумя байтами и во избежание искажений передается трижды. Время передачи текста составило 64 секунды. какова скорость передачи в “байтах в секунду”?
[4800]

54. Через ADSL-соединение файл размером 1000 Кбайт передавался 32 с. Сколько секунд потребуется для передачи файла размером 625 Кбайт
[20]

55. Скорость передачи данных скоростного ADSL соединения равна 1024000 бит/с, а скорость передачи данных через 3G-модем равна 512000 бит/с. Определите на сколько секунд дольше будет скачиваться файл размером 9000 Кбайт через 3G-модем, чем через ADSL-соединение. (Ответ дайте в секундах).
[72]
56. Сколько времени будет проходить передача файла размером 128 кбайт по сети, скорость которой составляет 128Кбит/с? (Ответ укажите в секундах)
[8]

57. Пропускная способность телефонной линии 8 Кб/с, специального оптического канала — 40 Мб/с. Сколько телефонных линий нужно задействовать, чтобы создать канал связи, эквивалентный оптическому по пропускной способности?
[5120]

58Скорость передачи данных через ADSL-соединение равна 256 000 бит/с. Передача файла через это соединение заняла 2 минуты. Определите размер файла в килобайтах.
[3750]
59.Задан адрес электронной почты в сети Интернет: name111@mtu-net.ru. Каково имя владельца этого электронного адреса?
[name111]
Задачи С

1. В компании XYZ была принята решение о внедрении новой системы управления проектами. Выбор был сделан в пользу централизованного метода, в котором все решения принимаются на высшем уровне управления. Главный проектный менеджер, Александр, был назначен ответственным за реализацию этой системы. Однако, при внедрении новой системы Александр столкнулся с рядом проблем. Он осознал, что принятие всех решений на центральном уровне замедляет

процесс и затрудняет оперативную реакцию на изменения внешней среды. Кроме того, команды, исполняющие проекты, испытывали трудности в связи с отсутствием возможности самостоятельно принимать решения и нести ответственность за свою работу. Александр решил провести встречу с руководителями всех отделов компании и предложить использовать децентрализованный подход в управлении проектами. Он привел примеры компаний, успешно внедривших данный метод и отметил, что они смогли повысить эффективность, сократить время выполнения проектов и улучшить коммуникацию внутри организации.

В результате перехода на децентрализованный метод управления проектами, компания XYZ что смогла улучшить?

[производительность]

2. Вы работаете в крупной IT-компании и вам поступил небольшой заказ от клиента. Клиент хочет создать локальную сеть в своем офисе для подключения всех компьютеров и устройств. Он хочет иметь возможность обмениваться данными между компьютерами, печатать на общем принтере, использовать общий доступ к интернету, а также обеспечить высокую безопасность своей сети. Вам предстоит разработать и реализовать план создания локальной сети для клиента. Для этого вам нужно определить подходящие протоколы и стандарты локальных сетей. Ваш ответ: Для создания локальной сети в офисе клиента, какой стандарт вы можете использовать?

[Ethernet]

3. Вы работаете в крупной компании, которая решает обновить свою локальную сеть для улучшения производительности и безопасности. Вам было поручено разработать проект стандартизированной сети для главного офиса, а

затем распространить его на все филиалы компании. Вы должны включать план проектирования стандартизированной сети, и что еще должны предоставить на реализацию проекта,
[бюджет]

4. Ваша компания растет и переезжает в новый офис. Вам предоставили план помещений, который включает несколько кабинетов, конференц-зал, приемную и серверную комнаты. В офисе будет работать более 100 сотрудников, из которых некоторые будут работать удаленно.
Ваша задача: 1. Разработать сетевую инфраструктуру, которая обеспечит быстрое и стабильное подключение к Интернету для всех сотрудников.
2. Определить, какое оборудование необходимо для создания локальной сети
3. Обеспечить безопасность сети, включая защиту от несанкционированного доступа, вредоносного ПО и утечек данных.
Для обеспечения быстрого и стабильного подключения к Интернету какое высокоскоростное соединение (FTTH) можно использовать?
[волоконно-оптическое]

5. Ваша компания решила провести обновление сетевой инфраструктуры и перейти на более современную технологию Ethernet. Вам было поручено исследовать историю разработки этой технологии и представить ее на совещании. Вы начали исследование и обнаружили, что первые прототипы технологии Ethernet были разработаны в 1970-х годах в лаборатории компании Xerox PARC. Эта технология представляла собой способ передачи данных в локальных сетях, используя метод передачи сигнала в виде постоянного потока битов.

На совещании вам задали следующий вопрос: "Какие критические моменты и препятствия возникли на пути разработки и внедрения технологии Ethernet?"

[Необходимость стандартизации]

6. В 1960-х годах компания Xyz принимает решение разработать новую технологию связи для своей корпоративной сети. Однако они сталкиваются с проблемой – кабельные соединения не способны передавать информацию на большие расстояния без существенных потерь сигнала. В то же время, сотрудник компании Xyz, по имени Джон, узнает о принципе работы коаксиального абонентского телевизионного кабеля, который передает сигналы с низкими потерями на большие расстояния. Он осознает, что такая технология может быть применена в сетях передачи данных. Джон решает провести эксперимент, соединив два компьютера через кабельное телевизионное соединение. Он успешно передает данные с одного компьютера на другой без значительных потерь сигнала. Джон понимает, что это может составить основу для разработки новой технологии связи.

Идея использования какого кабеля легли в основу разработки технологии Ethernet?

[коаксиального]

7. Вам нужно разработать сетевую архитектуру для небольшой компании, которая занимается разработкой программного обеспечения. В компании работают несколько отделов: разработки, тестирования, дизайна и администрации.

Основные требования к сети:

1. Безопасность: вся информация должна быть защищена от несанкционированного доступа, а также должна быть установлена защита от вредоносного ПО и хакерских атак.

2. Высокая производительность: сеть должна обеспечивать быстрый и стабильный доступ к ресурсам, таким как облачное хранилище, серверы баз данных и инструменты разработки.
3. Гибкость: сеть должна быть легко масштабируемой, чтобы можно было добавлять или изменять сетевое оборудование, не прерывая работу сотрудников.
4. Надежность: сеть должна быть надежной и иметь систему резервирования, чтобы минимизировать время простоя в случае сбоев.
5. Удобство использования: сотрудники должны иметь легкий доступ к сети из любого места в компании, даже если они работают удаленно или используют мобильные устройства.
Какую кабель будете использовать, учитывая вышеперечисленные требования?

[витая пара]

8. В небольшой компании, занимающейся разработкой программного обеспечения, возникла необходимость пересмотра своей сетевой инфраструктуры.
На текущий момент компания организована в виде одноранговой сети, в которой все компьютеры подключены непосредственно к одному роутеру. Однако, с увеличением количества сотрудников и объёма рабочей информации, возникли сложности в организации эффективного сетевого взаимодействия, а также проблемы с безопасностью.
Для решения данной проблемы, компания примет решение о переходе на какую сеть?
[серверную]

9. В большой компании были установлены беспроводные точки доступа, чтобы обеспечить сотрудникам стабильное подключение к сети интернет на всей территории офиса. Каждый сотрудник имел свой ноутбук с встроенным Wi-Fi модулем, чтобы подключаться к сети. Однако, в одном из отделов сотрудники стали жаловаться на проблемы с сетью — подключение к точкам доступа было низким, а скорость передачи данных была слишком медленной.

Сетевой администратор решил проверить состояние сети в данной зоне и обнаружил следующую ситуацию: в одной комнате располагалось несколько беспроводных принтеров, которые также использовали Wi-Fi для своей работы. К настоящему времени, принтеры были подключены к той же сети, что и ноутбуки сотрудников.

Сетевой администратор понял, что конфликтуют между собой присутствующие на одной частоте радиоволны, излучаемые точками доступа и принтерами, именно поэтому у сотрудников наблюдаются проблемы с подключением и скоростью передачи данных.

Чтобы решить данную проблему, сетевой администратор что должен установить на принтеры?

[сетевые адаптеры]

10. Вы являетесь техническим специалистом в компании, которая занимается предоставлением услуг интернета провайдерами. Вашей задачей является решить проблему, связанную с коммуникационным оборудованием в сети провайдера.

Получаете заявку от одного из клиентов провайдера, который сообщает, что у него нет доступа в Интернет. Вы знаете, что провайдер работает с помощью оптоволоконных линий и имеет свой центральный узел, откуда сигнал подается к клиентам по проводной линии.

При проверке вы обнаруживаете, что у клиента есть подключенный маршрутизатор, который включен и находится в рабочем состоянии. Вы также проверяете подключение провода от маршрутизатора к розетке и обнаруживаете, что все в порядке.Затем вы обращаете внимание на шкафчик, где маршрутизатор был установлен, и видите, что светодиодные индикаторы на коммутаторе в шкафчике не горят. Вы понимаете, что проблема может быть связана с коммуникационным оборудованием в самом шкафчике.
Чтобы решить эту проблему, что нужно перезагрузить?

[коммутатор]

11. Установите соответствие:

1. Всемирная паутина WWW	А. информационная система, основными компонентами которой являются гипертекстовые документы
2. Электронная почта e-mail	Б. система пересылки корреспонденции между пользователями в сети
3. Передача файлов FTP	В. система передачи электронной информации, позволяющая каждому пользователю сети получить доступ к программам и документам, хранящимся на удаленном компьютере

12. Фирма «Уют», которая специализируется на изготовлении изделий, делающих жилище уютным, комфортным, открывает свой новый магазин. На открытие магазина нужно пригласить более 100 гостей, среди которых есть частные лица, так и другие фирмы-друзья. Приглашение нужно послать за короткое время (1 рабочий день). Секретарь фирмы «Уют» смогла за рабочий день подготовить и отправить половину приглашений.
Вопрос: Какие способы решения проблемы вы можете предложить?
[Электронная почта]

13. Академия «Айти» имеет самую разветвленную сеть ограниченная в пределах одного города, континента филиалов в России в 20 крупнейших промышленных центрах: Владивостока, Волгограда, Воронежа и т.д. О какой из компьютерных сетей идет речь?
[региональная]

14. Вашим департаментом обороны разработано новое программное обеспечение для передачи конфиденциальной информации между двумя военными базами. Однако в процессе тестирования вы обнаружили, что передача данных нестабильна и может привести к потере или повреждению информации.
Как системный администратор, ваша задача состоит в том, чтобы исправить проблему и обеспечить безопасную передачу данных между базами.
Что нужно разработать для защиты конфиденциальной информации во время передачи?
[систему шифрования]

15. Существует небольшая компания, в которой работают несколько отделов: IT-отдел, отдел маркетинга, отдел продаж и отдел логистики. Каждый отдел использует различные программы и приложения для выполнения своих задач. Однако, сотрудники разных отделов часто нуждаются в обмене информацией между собой.
Руководство компании решает внедрить протоколы взаимодействия между отделами, чтобы обеспечить эффективное и безопасное обмен информацией.
Какой стек протоколов необходимо в компании использовать?
[OSI]

16. Установите соответствие:

1	Сервер	в	специальный компьютер, который предназначен для удаленного запуска приложений, обработки запросов на получение информации из баз данных и обеспечения связи с общими внешними устройствами
2	Рабочая станция	а	это персональный компьютер, позволяющий пользоваться услугами, предоставляемыми серверами
3	Сетевая технология	г	согласованный набор стандартных протоколов, реализующих их программно-аппаратных средств, достаточный для построения компьютерной сети и обслуживания ее пользователей
4	Информационно-коммуникационная технология	б	это информационная технология работы в сети, позволяющая людям общаться, оперативно получать информацию и обмениваться ею

Ответ:1-в,2-а,3-г,4-б

17. . В компании "ТехноСерв" развернута глобальная вычислительная сеть, которая используется для хранения и обработки конфиденциальной информации клиентов. Сеть поддерживается специализированной командой IT-специалистов, включающей системных администраторов, программистов и информационных безопасности.

Однажды ночью, во время проведения планового обслуживания сети, ведущий инженер по безопасности, Алексей, обнаруживает аномалию в системе безопасности. Он замечает необычную активность на одном из серверов, по которому проходит важное трафика информации. Алексей осознает, что это может быть попытка несанкционированного доступа к конфиденциальным данным.

Действуя быстро и внимательно, Алексей начинает проводить расследование. Он проверяет журналы системных логов и обнаруживает, что на удаленном сервере наблюдалась непрерывная попытка подбора пароля для доступа к

системе. Каждая попытка ввода пароля сопровождалась некорректным запросом, что подтверждает, что это атака на систему. Алексей знает, что ему необходимо прекратить эту атаку и защитить данные. Что он должен заблокировать для сохранения безопасности информации?
[удаленный доступ]

18. В офисе компании "ТехноПро" была проведена модернизация компьютерной сети. Ранее сеть работала на базе Фаст Итернет, но в связи с увеличением объема передаваемых данных руководство компании решило перейти на Гигабит Этернет. Во время модернизации было принято решение заменить старые аппаратные компоненты сети на более современные и производительные. Команде администраторов сети была поставлена задача выбрать подходящие компоненты. Однако, на месте команды возникла проблема с выбором видов сетевых сред передачи данных. В их распоряжении были витая пара, коаксиальный и оптоволоконный кабели. Учитывая все это оптимальным выбором будет использование каких коммутаторов, и учитывая что должны поддерживать работу как с витой парой, так и с оптоволокном

[гигабитных]

19. В компании "Техносервис" имеются три отдела: отдел разработки, отдел маркетинга и отдел снабжения. Каждый отдел имеет свою собственную локальную сеть для обмена данными и доступа в интернет. Однако, в последнее время сотрудники стали жаловаться на медленную скорость передачи данных в сети. Менеджмент решил обновить сетевую инфраструктуру и установить Gigabit Ethernet для повышения производительности сети. Для этого было решено провести анализ текущей сетевой инфраструктуры. Технический специалист выяснил, что в отделе разработки используется Fast Ethernet со скоростью передачи данных 100 Мбит/с, что является узким местом в сети. В отделе маркетинга также

используется Fast Ethernet, но скорость передачи данных на данный момент удовлетворительная. В отделе снабжения используется стандартный Ethernet. Для обновления сети в компании должна быть проведена замена каких коммутаторов и маршрутизаторов, поддерживающих Gigabit Ethernet.
[сетевых]
20. . Начальником транспортного отдела было создано электронная почта ,для получение тарифных планов, и расчетных документов , по месту своей работы. Назовите вид условного разделы адреса электронной почты?
[корпоративная]

21.Пользователь открывает приложение и отправляет сообщение другу в другую страну. Какой тип приложения при этом использовался?
[сетевая]

22. Вы – сотрудник фармацевтического учреждения. Ежедневно в базе данных происходит накопление большого количества информации.
Способ обеспечения целостности и предотвращения уничтожения данных
[Резервное копирование]

23. Вы являетесь администратором сети в одной компании, и у вас возникла задача построить сеть на базе маршрутизатора. Компания имеет несколько отделов, которые требуют раздельного доступа к ресурсам сети: 1. Отдел маркетинга должен иметь доступ к внешнему интернету и иметь возможность обмениваться данными с другими внешними компаниями. 2. Отдел разработки необходимо иметь доступ к внешним серверам для скачивания необходимых программ и обновлений, а также интернет-ресурсам для поиска необходимой информации. 3. Отдел бухгалтерии должен иметь доступ к внешним сервисам онлайн-банкинга и возможность обмениваться данными с другими финансовыми организациями путем создания защищенной подсети.

Для данной сети вы можете использовать маршрутизатор с какой функцией виртуальных локальных сетей
[VLAN]

24. Вы работаете в компании, которая занимается разработкой и продажей программного обеспечения для мониторинга работы компьютерных сетей. Ваша команда создала новый продукт - активный монитор, который помогает оперативно обнаруживать и анализировать проблемы в сети. Вашим клиентом является крупная финансовая организация, которая имеет высокие требования к надежности и безопасности своей сети. Они уже установили ряд мониторов на своих серверах, но столкнулись с проблемой - многие из них работают в пассивном режиме и не предоставляют оперативной информации о состоянии сети. Что можно предложить установить для того чтобы постоянно сканировать сеть, и фильтровать все входящие и исходящие пакеты данных?

[активные мониторы]

25. Вы являетесь системным администратором в крупной компании и вашей задачей является настройка IP-адресации для нового офиса. Офис состоит из 3-х этажей, на каждом этаже находится по 30 рабочих мест. Вам необходимо разделить доступные IP-адреса на сети для первого этажа и настроить маршрутизацию так, чтобы сотрудники с разных этажей могли свободно обмениваться данными. Ваша задача - разработать план IP-адресации для данного офиса.
[192.168.1.1 - 192.168.1.30]

26. В компании "Альфа" установлено сетевое оборудование, включающее в себя пассивные и активные концентраторы. Работники компании начали жаловаться на проблемы с интернет-соединением: скорость загрузки страниц

сильно снизилась, а некоторые устройства вообще перестали подключаться к сети. Определите, с чем может быть связана проблема?
[интернет-соединением]

27. Вы - инженер в компании, занимающейся разработкой компьютерных сетей. Вашей задачей является создание новой технологии FastEthernet, которая должна обеспечить более быструю передачу данных в локальных сетях. Ваша команда проводит серию экспериментов с различными компонентами и настройками сети. В процессе исследования вы обнаруживаете, что передача данных нестабильна и подвержена сильным помехам. Интенсивно работая вместе с командой, вы проводите анализ и определяете, что проблема в возникновении электрических помех на протяжении кабелей Ethernet. Чтобы решить эту проблему, вы ищете альтернативные материалы для кабелей, которые будут более устойчивы к помехам. Вы проводите многочисленные тесты и эксперименты с различными материалами, и в конечном итоге что вы сможете предложить?

[полимер]

28. Вы - IT-специалист, назначенный для проектирования и создания сети для малого предприятия, специализирующегося на продаже косметических товаров. Предприятие имеет один магазин и один склад, на котором хранятся товары для продажи.
Ваша задача создание надежной и безопасной сети, которая обеспечит связь между магазином и складом, а также с подключенными компьютерами и POS-терминалами в магазине. Самый первый пункт в решении этой задачи?

[Определение требований]

29. Вас попросили настроить маршрутизатор в офисе, который подключает сеть компьютеров к интернету. Во время настройки вы заметили, что один из компьютеров в сети имеет аномально высокий трафик данных, намного превышающий остальные устройства. В чем может быть причина высокого трафика и как вы будете решать эту проблему? Ответ: Причиной высокого трафика данных на одном из компьютеров может быть наличие вредоносного программного обеспечения, которое использовалось для сбора и передачи информации или для незаконного майнинга криптовалют. Для решения этой проблемы, первым делом что следует провести?
[анализ компьютера]

30. Установите соответствие между типом сетевого кабеля и его описанием:
1.Коаксиальный кабель Состоит из медной жилы, окружающей ее изоляции, экрана в виде металлической оплетки и внешней оболочки
2. Витая пара Состоит из нескольких перевитых друг вокруг друга изолированных медных проводов
3. Оптоволоконный кабель Состоит из тонкой стеклянной жилы, покрытой слоем стекла с иным, чем у жилы, коэффициентом преломления
Варианты ответов

31. В компании XYZ решено провести модернизацию локальной компьютерной сети для улучшения работы сотрудников. На данный момент сеть состоит из одного маршрутизатора и десяти компьютеров, но планируется добавить еще пять компьютеров. Между компьютерами требуется обеспечить высокую скорость передачи данных. Какая топология сети лучше всего подойдет для данной ситуации?
звезда]

32/ В компании "ABC" работает 100 сотрудников, которые регулярно обмениваются информацией и файлами при помощи компьютерных сетей. В некоторый момент сеть начала работать очень медленно, и сотрудники жалуются на постоянные задержки и сбои в работе. Вы - системный администратор компании "ABC" и вам поручено найти причину и решить проблему. Что для этого нужно протестировать?
[скорость сети]

33. В офисе небольшой компании работает 30 сотрудников, которые используют компьютеры для выполнения своей работы. В данный момент все компьютеры подключены к одной локальной сети через один коммутатор. Однако недавно сотрудники начали жаловаться на медленную работу сети и периодические проблемы с подключением к интернету. Как специалист по организации компьютерных сетей, вам необходимо решить эту проблему и улучшить работу сети. Что необходимо установить?
[дополнительные коммутаторы]

34. В офисе компании XYZ возникли проблемы с подключением к сети интернет. Пользователи жалуются на медленную скорость скачивания файлов и прерывания соединения. Администратор компьютерной сети решает проверить состояние оборудования. Какая проблема может быть выявлена?
[неисправность коммутатора]

35. В офисе компании произошел сбой в работе сети. Все сотрудники никак не могут подключиться к Интернету и получить доступ к общим файлам на сервере.
Какое решение предложите для восстановления работы сети и обеспечения подключения всех сотрудников к Интернету и общим файлам на сервере. В чем заключается проблема?
[сетевая карта]

36. Вы являетесь системным администратором крупной компании. Внезапно произошла непредвиденная ситуация - один из компьютерных серверов, отвечающих за хранение и обработку всех данных компании, вышел из строя. Это вызвало серьезные проблемы в работе всех подразделений компании, так как сотрудники не могут получить доступ к необходимым документам и программам. Необходимо принять меры для быстрого восстановления работы сервера и минимального нарушения работы компании. Однако, бюджет компании ограничен, поэтому необходимо выбрать оптимальное решение, которое удовлетворит потребности компании, но не приведет к необоснованным расходам.
[резервирование данных]

37. В компании, занимающейся разработкой программного обеспечения, произошел сбой в работе компьютерной сети. Сотрудникам необходимо подключиться к серверу для продолжения работы над текущим проектом. Один из сотрудников оборудовал свой компьютер в качестве временного сервера и установил на него необходимое программное обеспечение. Он дал доступ к этому временному серверу другим сотрудникам через локальную сеть. Остальные сотрудники использовали свои рабочие станции, чтобы подключиться к временному серверу. Они внесли необходимые изменения в настройки сети на своих компьютерах, чтобы они могли обмениваться данными и выполнять задачи, необходимые для проекта. Временный сервер был успешно запущен, и сотрудники продолжили работу над проектом, минуя основной сервер. Одна из команд проекта занималась тестированием и разработкой новой системы хранения данных. У них возникла необходимость в использовании базы данных, которая уже была сохранена на основном сервере и была доступна только в рамках основной сети. Сотрудники этой команды внесли в настройки своего компьютера изменения, чтобы они могли обратиться напрямую к основному серверу и использовать базу данных. Это

позволило им без проблем взаимодействовать с базой данных и проводить необходимые тесты и разработку. В результате какой-то времени сеть на основном сервере была восстановлена. Сотрудники переключили свои компьютеры обратно на основной сервер, а временный сервер был выключен. Какая архитектура использована?
[клиент-серверная]

38. Вы работаете системным администратором в небольшой компании. Ваша задача - подключить новый сетевой принтер к уже существующей локальной сети. В компании используется Ethernet-соединение. Что необходимо выполнить, какой кабель необходимо использовать?
[Ethernet]

39. В компании "Альфа" используется компьютерная сеть для связи между сотрудниками и передачи данных. В один день сотрудник Иванов обратился к администратору сети, жалуясь на то, что у него нет доступа к сети и не может работать. Администратор решил проверить причину проблемы и обнаружил, что у Иванова отсутствует IP-адрес. Далее, администратор обратился к сетевому администратору с просьбой присвоить Иванову новый IP-адрес. Однако, сетевой администратор сообщил, что все IP-адреса в сети уже используются и новый адрес выделить невозможно.

Как известно, IP-адрес служит для идентификации сетевых устройств, поэтому задача состоит в том, чтобы найти решение данной проблемы и предложить альтернативные варианты действий. Для решения данной проблемы можно предложить использовать какой механизм?
[DHCP]

40. В компании XYZ имеется несколько отделений, расположенных в разных городах. Каждое отделение имеет свою локальную компьютерную сеть,

включающую компьютеры, принтеры, сервера и другое оборудование. Все сети в каждом отделении оснащены маршрутизаторами для организации связи между ними. Однако недавно стало известно, что в отделении в городе А произошел сбой в компьютерной сети. Пользователи не могут подключиться к сети, а процессы и задачи, требующие обращения к удаленным ресурсам, работают очень медленно или вообще не выполняются. Ваша задача как сетевого администратора - выяснить и устранить причину сбоя в сети. Вы решаете проверить оборудование в отделении А и быстро обнаруживаете, что один из маршрутизаторов перегружен большим объемом сетевого трафика. Что будете делать, чтобы восстановить работоспособность сети в отделении А? Что нужно увеличить у маршрутизатора?
[пропускную способность]

41. Вы работаете системным администратором в небольшой компании. Сегодня весь офис столкнулся с проблемой отсутствия интернет-соединения. Пользователи не могут выходить в интернет, внутренняя сеть также не функционирует. После проведения первичной диагностики, вы обнаруживаете, что маршрутизатор, подключенный к провайдеру, перестал работать. Проверив внешние провода, вы приходите к выводу, что проблема находится именно в маршрутизаторе. Какие действия вы предпримите для решения данной ситуации?
[Перезагрузка маршрутизатора]

42. В офисе произошла сбойная ситуация в компьютерной сети. Сеть в офисе состоит из 50 компьютеров, которые подключены к одному коммутатору. Внезапно все компьютеры потеряли доступ к интернету и другим ресурсам в сети. Опишите, какой метод будете использовать, чтобы устранить данную ситуацию и восстановить работоспособность сети?
[Перезагрузка коммутатора]

43. В компании внедряют новую компьютерную сеть. В сети установлены несколько коммутаторов и маршрутизаторов. В результате одного из сбоев в сети, сотрудники больше не могут получать доступ к Интернету. Как вы, сетевой администратор, решите эту проблему? Какое проверите подключение маршрутизатора к Интернет-провайдеру?
[физическое]

44. В небольшой IT-компании решено провести обновление компьютерной сети для улучшения ее функционирования. Компания имеет 5 отделов, каждый из которых состоит из 20 сотрудников, расположенных на одном этаже здания. В настоящий момент в каждом отделе установлен маршрутизатор, однако сеть часто работает медленно, что в моменты пиковой нагрузки приводит к отключению и перегрузкам. Вам как специалисту предоставлено задание сделать необходимые изменения в структуре сети компании для устранения проблем и достижения более эффективного функционирования.
[Установка Wi-Fi]

45. Вы являетесь администратором компьютерной сети в офисе среднего размера. У вас есть два этажа, каждый из которых предоставляет рабочие места для 50 сотрудников. Каждый сотрудник должен иметь доступ к данным на общем сервере, а также к интернету. На первом этаже находятся отделы маркетинга и продаж, где сотрудники работают с большим объемом мультимедийных файлов и требуют высокой скорости интернета. На втором этаже находится отдел бухгалтерии, где сотрудники работают с большим объемом конфиденциальной информации и требуют безопасного доступа к серверу. Что вы установите для решения этой задачи?
[брандмауэр]

46. Вы являетесь администратором сети в небольшой компании, где работает около 70 сотрудников. Компания решила обновить свою сетевую

инфраструктуру, чтобы повысить производительность и обеспечить надежность и безопасность данных. Ваши задачи включают в себя: 1. Выбор архитектуры сети: Какую архитектуру сети вы предложите для компании?.
[клиент-серверную]

47. В офисе компании решили провести модернизацию сетевой инфраструктуры. У руководителя проекта было несколько предложений для принципов построения компьютерной сети, но он не мог выбрать самый оптимальный вариант. Работники офиса в значительной степени работают удаленно, используя VPN-соединение. Они также регулярно обмениваются большими объемами данных, включая графические и видеофайлы. Недавно в компании был заключен контракт с новым поставщиком интернет-услуг, который обеспечивает высокоскоростное подключение. Цель модернизации сети состоит в повышении ее производительности и надежности. Какие принципы построения компьютерной сети следует рассмотреть для этого проекта? [Принцип гибкости]

48. Вы являетесь администратором компьютерной сети в крупной компании. Ваш отдел недавно решил расшириться и переехать в новый офис, и вам необходимо построить новую компьютерную сеть со следующими требованиями: Обеспечить безопасность сети и защиту данных.
Какие принципы безопасности компьютерных сетей вы будете внедрять для решения данной задачи и почему?
[Виртуализация]

49. В офисе компании "Альфа" решили обновить свою компьютерную сеть. В компании работает 50 сотрудников, каждый из которых использует компьютер для своей работы. В офисе есть 5 отделов, каждый из которых имеет свою сеть печати и файловое хранилище. Компания хочет построить сеть, которая будет обеспечивать быструю передачу данных, надежную работу

и безопасность. Какой принцип построения компьютерной сети вы бы применили в данной ситуации?
[сегментация сети]

50. Фирма решила обновить свою существующую компьютерную сеть, чтобы повысить скорость передачи данных и обеспечить более безопасное соединение для своих сотрудников. Они наняли эксперта по компьютерным сетям, чтобы разработать новую инфраструктуру. Объясните принципы построения компьютерных сетей, которые вы учтете при разработке новой инфраструктуры, и предложите наиболее подходящие компоненты и настройки, которые помогут компании достичь своих целей. При проектировании новой компьютерной сети следует учитывать принципы:
1. Масштабируемость:
2. Надежность
3. Безопасность:
4. Производительность:
5. Гибкость:
Для достижения указанных целей, рекомендуется использовать высокоскоростные коммутаторы с какой поддержкой?
[VLANs]

51. В офисе компании есть несколько отделов, каждый из которых имеет свои компьютеры и сервера с различными данными. Недавно компания решила установить новую локальную сеть для более эффективного обмена информацией между отделами. Директор компании обратился к системному администратору с задачей разработать и построить оптимальную компьютерную сеть. Какой принцип построения компьютерной сети должен быть учтен в данном проекте.
[Иерархическая структура]

52. Компания уже имеет несколько офисов в разных городах и каждый офис имеет свою собственную локальную сеть. Вам необходимо связать все офисы в единую компьютерную сеть, чтобы сотрудники из разных городов могли без проблем обмениваться информацией.
Какую бы вы использовали сеть, чтобы обеспечить взаимодействие между ними?
[LAN]

53. В офисе компании возникла необходимость в установке новой компьютерной сети. Вас назначили ответственным за проектирование и настройку сети. Чтобы эффективно выполнить эту задачу, вы решили руководствоваться основными принципами построения компьютерных сетей.

Сеть должна обеспечивать высокую производительность, надежность и безопасность передачи данных. Ваши коллеги высоко ценят скорость связи между компьютерами и серверами, поэтому вы решили использовать гигабитные коммутаторы для обеспечения быстрой передачи данных.

Однако, вы столкнулись с проблемой: в здании компании отсутствует возможность проведения сетевых кабелей между этажами. Компания уже пару лет назад установила беспроводную сеть Wi-Fi на каждом этаже, но она не обладает достаточной пропускной способностью для обеспечения требуемой скорости.

Какую сеть вы будете использовать, соблюдая принципы построения компьютерных сетей?
[комбинированную]

54. Вы - системный администратор в небольшой компании, где используется локальная компьютерная сеть для обеспечения рабочих мест. В последнее

время сотрудники столкнулись с проблемой медленного доступа к сети и перебоев в работе Интернета.

Что вы первоначально проыерите?

[устройства]

Критерии и шкалы для интегрированной оценки уровнясформиров анности компетенций:

(Преподаватель вправе изменить содержание оценок в соответстви и с ФГОС и особенностями ОПОП)

Индикаторы компетенции	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**отлично**
Полнотазнаний	Уровень знаний ниже Минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущено много негрубых ошибки.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок.
Наличиеумений	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания но не в полном объеме.	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественным недочетами, выполнены все задания в полном

				объеме.
Характеристика **сформированности** **компетенции**	Компетенция вполной мере не сформирована. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач. Требуется повторное обучение	Сформированность компетенции соответствует минимальнымтребованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по большинству практических задач.	Сформированность компетенции в целом соответствует требованиям, но есть недочеты. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по некоторым профессиональным задачам.	Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач.
Уровень сформированности компетенций	Низкий	Ниже среднего	Средний	Высокий

Шкала оценивания

Количество баллов	**Отметка в 5 бальной системе**	**Качество усвоения предмета**
От 0 до 10	2	менее 50%

От 11 до 14	3	51%-70%
От 15 до 17	4	71%-85%
От 18 до 20	5	86%-100%

Шкала оценивания)

Количество баллов	**Отметка в 5 бальной системе**	**Качество усвоения предмета**
От 0 до 5	2	менее 50%
От 6 до 7	3	51%-70%
От 8 до 9	4	71%-85%
От 9 до 10	5	86%-100%

Шкала оценивания точных наук

Количество баллов	**Отметка в 5 бальной системе**	**Качество усвоения предмета**
От 0 до 8	2	менее 40%
От 9 до 12	3	41%-60%
От 13 до 16	4	61%-80%
От 17 до 20	5	81%-100%

Шкала оценивания

Количество баллов	**Отметка в 5 бальной системе**	**Качество усвоения предмета**
От 0 до 4	2	менее 40%
От 5 до 6	3	41%-60%
От 7 до 8	4	61%-80%
От 9 до 10	5	81%-100%

Практические задания для оценки степени усвоения дисциплины
(текущий контроль)
МДК 01.01. Компьютерные сети

Раздел 01. Компьютерные сети

Тема 1.1. Введение в сетевые технологии

Правила выполнения практических работ

При подготовке к выполнению практической работы студентам следует:

- изучить теоретические вопросы, изложенные в методических указаниях;

-ознакомиться с техникой безопасности при работе в кабинете №2 «Информатики и информационных технологий»;

-получить у преподавателя задание на выполнение практической работы, которое выдается после проверки теоретической подготовки обучающегося.

-внимательно слушать инструктаж на деловых играх и тренингах

-активно участвовать в обсуждениях, работать в группах

Результаты выполнения практической работы проверяются преподавателем.

Безопасность труда

Инструкция по охране труда для системного администратора

1. Общие требования охраны труда

1.1. К самостоятельной работе системным администратором допускаются лица, прошедшие при поступлении на работу вводный инструктаж по охране труда, инструктаж по электробезопасности на рабочем месте (с присвоением соответствующей группы по электробезопасности), обучение и проверку знаний по охране труда.

1.2. Системный администратор должен:

знать действие на человека опасных и вредных производственных факторов, возникающих во время работы;

соблюдать требования производственной санитарии, электробезопасности и пожарной безопасности;

знать место расположения огнетушителей и аптечек;

знать правила внутреннего трудового распорядка, установленные на предприятии;

знать назначение средств индивидуальной защиты (СИЗ);

уметь оказывать первую помощь пострадавшим, пользоваться средствами пожаротушения.

1.3. Во время работы на системного администратора могут воздействовать следующие опасные факторы:

повышенный уровень электромагнитных излучений;

повышенный уровень ионизирующих излучений (у мониторов на электронно-лучевых трубках);

повышенный уровень статического электричества;

повышенная напряженность электростатического поля; – повышенная или пониженная ионизация воздуха;

повышенная яркость света;

прямая и отраженная блесткость;

повышенное напряжение в электрической цепи, замыкание которой может произойти через тело человека;

статические перегрузки костно-мышечного аппарата и динамические локальные перегрузки мышц кистей рук;

повышенный уровень загазованности и запыленности воздуха (в первую очередь по углекислому газу и аммиаку, которые образуются при выдыхании), особенно в плохо вентилируемых помещениях;

перенапряжение органов зрения;

повышенный уровень шума от работающих вентилятора охлаждения ПК и принтера, от неотрегулированных источников люминесцентного освещения и др.;

умственное перенапряжение, эмоциональные перегрузки и монотонность труда.

1.4. Нормы и сроки выдачи СИЗ определяются согласно Типовым отраслевым нормам бесплатной выдачи рабочим и служащим специальной одежды, специальной обуви и других СИЗ.

1.5. Площадь на одно рабочее место с персональным компьютеров на базе электронно-лучевой трубки, должна составлять не менее 6 м, на базе плоских дискретных экранов (жидкокристаллические, плазменные) – не менее 4,5 м.

1.6. Оснащение светопроницаемых конструкций и оконных проёмов должно позволять регулировать параметры световой среды в помещении.

2. Требования охраны труда перед началом работы

2.1. Перед началом работы системный администратор обязан:

осмотреть и привести в порядок рабочее место;

отрегулировать освещенность на рабочем месте, убедиться в достаточности освещенности, отсутствии отражений на экране, отсутствии встречного светового потока;

проверить правильность подключения оборудования в электросеть;

проверить правильность установки стола, стула, подставки для ног, положения оборудования, угла наклона экрана, положение клавиатуры и, при необходимости, произвести регулировку рабочего стола и кресла, а также расположение элементов компьютера в соответствии с требованиями эргономики и в целях исключения неудобных поз и длительных напряжений тела.

2.2. При включении компьютера соблюдать правила электробезопасности.

2.3. Системному администратору запрещается приступать к работе при:

отсутствии информации о соответствии параметров данного оборудования требованиям санитарных норм;

обнаружении неисправности оборудования;

отсутствии защитного заземления электрооборудования;

отсутствии огнетушителя и аптечки первой помощи.

3. Требования охраны труда во время работы

3.1. Системный администратор во время работы обязан:

выполнять только ту работу, которая ему была поручена, и по которой он был

проинструктирован;

в течение всего рабочего дня содержать в порядке и чистоте рабочее место;

соблюдать санитарные нормы и режимы работы и отдыха;

соблюдать правила эксплуатации вычислительной техники в соответствии с инструкциями по эксплуатации;

соблюдать установленные режимом рабочего времени регламентированные перерывы в работе и выполнять упражнения для глаз, шеи, рук, туловища, ног.

3.2. Системному администратору во время работы запрещается:

прикасаться к задней панели системного блока (процессора) при включенном питании;

переключать разъемы интерфейсных кабелей периферийных устройств при включенном питании;

загромождать верхние панели устройств бумагами и посторонними предметами;

допускать захламленность рабочего места;

производить отключение питания во время выполнения активной задачи;

допускать попадание влаги на поверхность системного блока (процессора), монитора, рабочую поверхность клавиатуры, дисководов, принтеров и др. устройств;

включать сильноохлажденное (например, принесенное с улицы в зимнее время) оборудование;

производить самостоятельно вскрытие и ремонт оборудования (если это не входит в рабочие обязанности).

4. Требования охраны труда в аварийных ситуациях

4.1. Системный администратор обязан:

во всех случаях обнаружения обрыва проводов питания, неисправности заземления и других повреждений электрооборудования, появления запаха гари немедленно отключить питание и сообщить об аварийной ситуации своему непосредственному руководителю и дежурному электрику;

при обнаружении человека, попавшего под напряжение, немедленно освободить его от действия тока путем отключения электропитания и до прибытия врача оказать потерпевшему первую медицинскую помощь;

при обнаружении пострадавшего немедленно вызвать медицинских работников, до их прибытия оказать пострадавшему первую помощь и, по

возможности, сохранить текущую обстановку на месте происшествия для возможности дальнейшего расследования несчастного случая;

при любых случаях сбоя в работе технического оборудования или программного обеспечения немедленно вызвать представителя инженерно-технической службы эксплуатации вычислительной техники;

в случае появления недомогания (рези в глазах, резком ухудшении видимости, невозможности сфокусировать взгляд или навести его на резкость, появлении боли в пальцах и кистях рук, усилении сердцебиения и пр.) немедленно покинуть рабочее место, сообщить о происшедшем своему непосредственному руководителю и обратиться к врачу;

при возгорании оборудования отключить питание и принять меры к тушению очага пожара при помощи огнетушителя, если это не угрожает собственной жизни и здоровью, вызвать пожарную команду и сообщить о происшествии своему непосредственному руководителю.

5. Требования охраны труда по окончании работы

5.1. По окончании работ системный администратор обязан соблюдать следующую последовательность выключения техники:

произвести закрытие всех активных задач;

выключить питание системного блока (процессора);

выключить питание всех периферийных устройств;

привести в порядок свое рабочее место;

снять и убрать в предназначенное для этого место спецодежду, спецобувь и СИЗ.

5.2. По окончании работ системный администратор обязан осмотреть и привести в порядок рабочее место, вымыть с мылом руки и лицо.

Практическая работа №1

Тема: Составление карты сети Интернет с помощью утилит «ping» и «traceroute»

Цель: Исследование вероятностно-временных характеристик сети с использованием утилиты ping, исследование топологии фрагментов Internet с использованием утилиты traceroute.

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задание:

Проверка подключения к сети посредством эхо-запроса с помощью команды ping

1: Определите, доступен ли удалённый сервер. Для трассировки маршрута к удалённой сети используемый ПК должен быть подключён к Интернету.

a. Сначала мы воспользуемся эхо-запросом с помощью команды ping. Эхо-запрос с помощью команды ping — это средство для проверки доступности узла. Пакеты информации пересылаются удалённому узлу с требованием ответа. Локальный ПК определяет, получен ли ответ для каждого пакета, и рассчитывает, какое время заняла пересылка этих пакетов по сети. Название эхо-запрос пришло из области активной гидролокации, где оно обозначало звуковой сигнал, отправляемый под воду и отражающийся от дна или других кораблей.

b. Нажмите кнопку Пуск на экране компьютера, введите команду cmd в поле Найти программы и файлы и нажмите клавишу ВВОД.

c. В командной строке введите ping www.cisco.com.

d. В первой строке полученных данных отображается полное доменное имя (FQDN) e144.dscb.akamaiedge.net. Затем следует IP-адрес 23.1.48.170. Веб-узлы компании Cisco, содержащие одну и ту же информацию, размещаются на различных серверах (так называемых зеркалах) по всему миру. Это значит, что имя FQDN и IP-адрес будут отличаться в зависимости от вашего местонахождения.

e. Возьмём приведённую ниже часть полученных результатов.

```
Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

f. Теперь отправьте эхо-запрос с помощью команды ping на веб-сайты регионального интернетрегистратора (RIR), расположенные в различных частях мира.

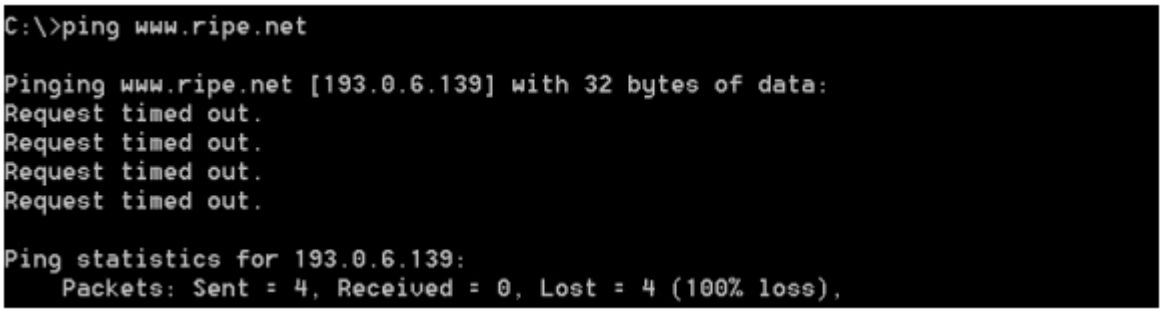
Африка: C:\> ping www.afrinic.net

```
C:\>ping www.afrinic.net

Pinging www.afrinic.net [196.216.2.136] with 32 bytes of data:
Reply from 196.216.2.136: bytes=32 time=314ms TTL=111
Reply from 196.216.2.136: bytes=32 time=312ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111

Ping statistics for 196.216.2.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 312ms, Maximum = 314ms, Average = 313ms
```

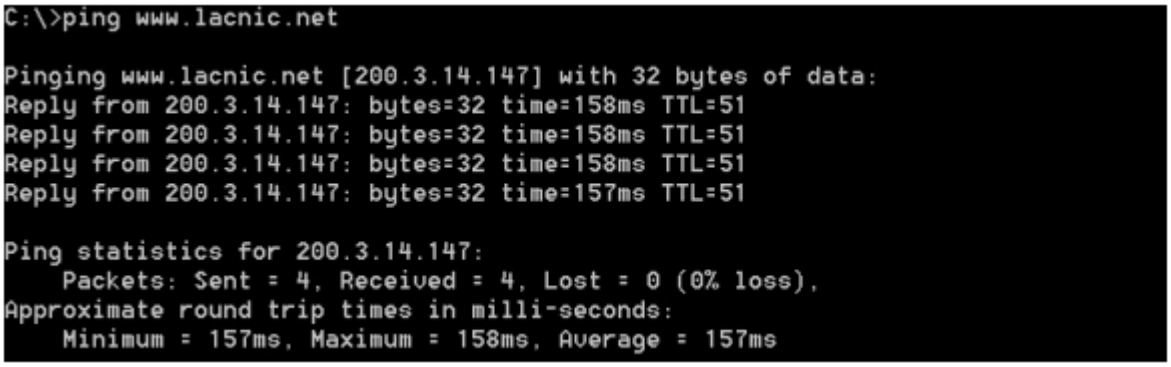
Австралия: C:\> ping www.apnic.net

```
C:\>ping www.apnic.net

Pinging www.apnic.net [202.12.29.194] with 32 bytes of data:
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=287ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49

Ping statistics for 202.12.29.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 286ms, Maximum = 287ms, Average = 286ms
```

Европа: C:\> ping www.ripe.net



Южная Америка: C:\> ping lacnic.net

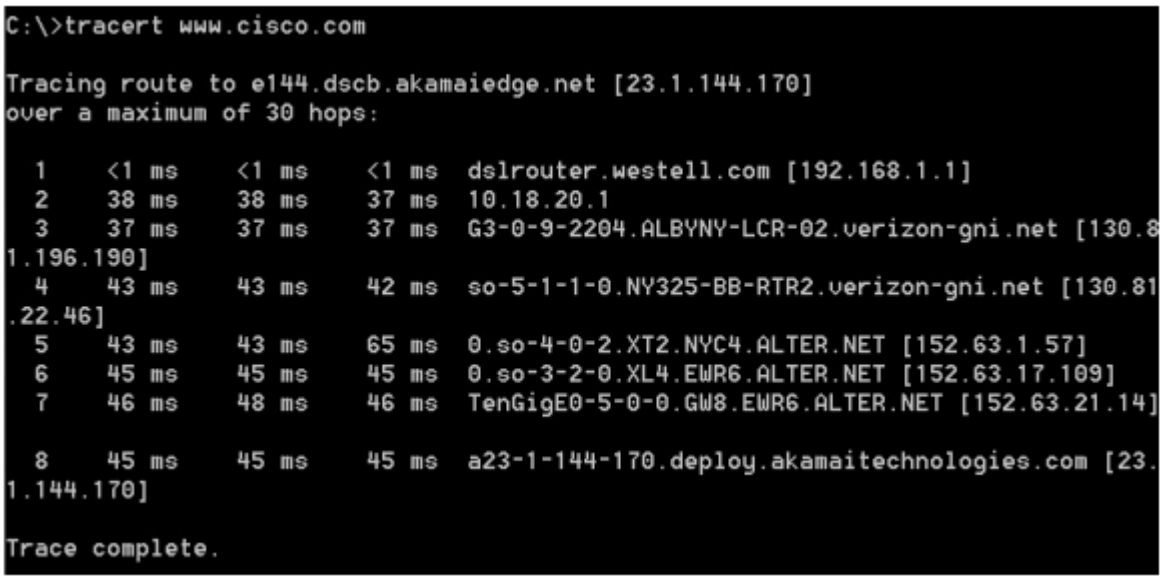


Все эти эхо-запросы с помощью команды ping были отправлены с компьютера, расположенного в США. Что происходит со средним временем эхо-запроса (в миллисекундах), когда данные передаются в пределах одного континента (Северной Америки), по сравнению с ситуацией, когда данные из Северной Америки пересылаются на другие континенты?

Отслеживание маршрута к удалённому серверу с помощью утилиты «traceroute»

1: Определите, какой маршрут из всего интернет-трафика направлен к удалённому серверу. Проверив достижимость с помощью утилиты «ping», стоит более внимательно рассмотреть каждый сегмент сети, через который проходят данные. Для этого воспользуемся утилитой tracert.

a. В командной строке введите tracert www.cisco.com.



b. Сохраните результаты, полученные после ввода команды «tracert», в текстовый файл, выполнив указанные ниже действия.

1) Нажмите правой кнопкой мыши на строку заголовка окна командной строки и выберите параметры Изменить > Выделить всё.

2) Ещё раз нажмите правой кнопкой мыши на строку заголовка окна командной строки и выберите параметры Изменить > Копировать.

3) Откройте Блокнот Windows. Для этого нажмите кнопку Пуск и выберите Все программы > Стандартные > Блокнот.

4) Чтобы вставить данные в Блокнот, выберите в меню Правка команду Вставить.

5) В меню Файл выберите команду Сохранить как и сохраните файл Блокнота на рабочий стол с названием tracert1.txt.

c. Запустите утилиту tracert для каждого веб-сайта назначения и сохраните полученные результаты в последовательно пронумерованные файлы. C:\> tracert www.afrinic.net C:\> tracert www.lacnic.net

d. Интерпретируйте данные, полученные с помощью утилиты tracert.

В зависимости от зоны охвата вашего интернет-провайдера и расположения узлов источника и назначения отслеженные маршруты могут пересекать множество переходов и сетей. Каждый переход — это один маршрутизатор. Маршрутизатор представляет собой особый компьютер, который используется для перенаправления трафика через Интернет. Представьте, что вы отправились в поездку по автодорогам нескольких стран.

Во время своего путешествия вы постоянно попадаете на развилки, где нужно выбирать одно из нескольких направлений. Теперь представьте себе, что на каждой такой развилке имеется устройство, которое указывает правильный путь к конечной цели вашего путешествия. То же самое делает маршрутизатор для пакетов в сети.

Поскольку компьютеры используют язык цифр, а не слов, маршрутизаторам присваиваются уникальные IP-адреса (номера в формате x.x.x.x). Утилита tracert показывает, по какому пути проходит пакет данных до конечного пункта назначения. Кроме того, с помощью утилиты tracert можно определить, с какой скоростью проходит трафик через каждый сегмент сети. Каждому маршрутизатору на пути прохождения данных отправляются три пакета, время ответа на которые измеряется в миллисекундах. Используя данную информацию, проанализируйте результаты, полученные с помощью утилиты tracert при отправке пакетов к www.cisco.com. Ниже представлен весь маршрут трассировки.

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

e. Существует интернет-сервис whois, с помощью которого можно узнать владельца доменного имени. Сервис whois доступен по адресу http://whois.domaintools.com/. Согласно информации, полученной с помощью whois, домен alter.net также принадлежит компании Verizon.

f. Теперь рассмотрим пример с пересылкой интернет-трафика через несколько интернетпровайдеров. Ниже представлены результаты применения утилиты «tracert» к узлу www.afrinic.net.

```
C:\>tracert www.afrinic.net

Tracing route to www.afrinic.net [196.216.2.136]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    39 ms    38 ms    37 ms  10.18.20.1
  3    40 ms    38 ms    39 ms  G4-0-0-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.197.182]
  4    44 ms    43 ms    43 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    42 ms  0.so-4-0-0.XT2.NYC4.ALTER.NET [152.63.9.249]
  6    43 ms    71 ms    43 ms  0.ae4.BR3.NYC4.ALTER.NET [152.63.16.185]
  7    47 ms    47 ms    47 ms  te-7-3-0.edge2.NewYork2.level3.net [4.68.111.137
]
  8    43 ms    55 ms    43 ms  vlan51.ebr1.NewYork2.Level3.net [4.69.138.222]
  9    52 ms    51 ms    51 ms  ae-3-3.ebr2.Washington1.Level3.net [4.69.132.89]

 10   130 ms   132 ms   132 ms  ae-42-42.ebr2.Paris1.Level3.net [4.69.137.53]
 11   139 ms   145 ms   140 ms  ae-46-46.ebr1.Frankfurt1.Level3.net [4.69.143.13
7]
 12   148 ms   140 ms   152 ms  ae-91-91.csw4.Frankfurt1.Level3.net [4.69.140.14
]
 13   144 ms   144 ms   146 ms  ae-92-92.ebr2.Frankfurt1.Level3.net [4.69.140.29
]
 14   151 ms   150 ms   150 ms  ae-23-23.ebr2.London1.Level3.net [4.69.148.193]

 15   150 ms   150 ms   150 ms  ae-58-223.csw2.London1.Level3.net [4.69.153.138]

 16   156 ms   156 ms   156 ms  ae-227-3603.edge3.London1.Level3.net [4.69.166.1
54]
 17   157 ms   159 ms   160 ms  195.50.124.34
 18   353 ms   340 ms   341 ms  168.209.201.74
 19   333 ms   333 ms   332 ms  csw4-pkl-gi1-1.ip.isnet.net [196.26.0.101]
 20   331 ms   331 ms   331 ms  196.37.155.180
 21   318 ms   316 ms   318 ms  fa1-0-1.ar02.jnb.afrinic.net [196.216.3.132]
 22   332 ms   334 ms   332 ms  196.216.2.136
```

Что происходит в переходе 7? Является ли level3.net тем же самым интернет-провайдером, что и в переходах 2–6? Чтобы ответить на этот вопрос, воспользуйтесь сервисом whois.

Как меняется время, необходимое для пересылки пакета данных между Вашингтоном и Парижем в переходе 10 по сравнению с предыдущими переходами 1–9?

Что происходит в переходе 18? С помощью сервиса whois выполните поиск по адресу 168.209.201.74. Кто является владельцем этой сети?

g. Введите команду tracert www.lacnic.net.

```
C:\>tracert www.lacnic.net

Tracing route to www.lacnic.net [200.3.14.147]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    38 ms    38 ms    39 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    42 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    82 ms    47 ms    47 ms  0.ae2.BR3.NYC4.ALTER.NET [152.63.16.49]
  6    46 ms    47 ms    56 ms  204.255.168.194
  7   157 ms   158 ms   157 ms  ge-1-1-0.100.gw1.gc.registro.br [159.63.48.38]
  8   156 ms   157 ms   157 ms  xe-5-0-1-0.core1.gc.registro.br [200.160.0.174]

  9   161 ms   161 ms   161 ms  xe-4-0-0-0.core2.nu.registro.br [200.160.0.164]

 10   158 ms   157 ms   157 ms  ae0-0.ar3.nu.registro.br [200.160.0.249]
 11   176 ms   176 ms   170 ms  gw02.lacnic.registro.br [200.160.0.213]
 12   158 ms   158 ms   158 ms  200.3.12.36
 13   157 ms   158 ms   157 ms  200.3.14.147

Trace complete.
```

3: Отслеживание маршрута к удалённому серверу с помощью программных и веб-средств

1: Воспользуйтесь веб-средством для трассировки маршрута.

a. С помощью сайта http://www.subnetonline.com/pages/network-tools/online-tracepath.php отследите маршрут к следующим веб-сайтам: www.cisco.com www.afrinic.net Скопируйте данные и сохраните их в файл Блокнота. Как меняется трассировка маршрута при переходе на www.cisco.com из командной строки (см. часть 1), а не через веб-сайт? (Полученные результаты могут изменяться в зависимости от местонахождения и того, с каким интернет-провайдером работает ваше учебное заведение.)

Сравните результаты трассировки маршрута в Африку из части 1 с результатами трассировки того же маршрута через веб-интерфейс. Какую разницу вы заметили?

В некоторых результатах трассировки маршрута можно увидеть сокращение «asymm». Есть идеи, что оно может означать? В чём его смысл?

Работа с программой VisualRoute Lite Edition VisualRoute — это проприетарная программа, позволяющая отобразить результаты трассировки маршрута наглядно.

a. Если программа VisualRoute Lite Edition на вашем компьютере не установлена, загрузите ее по следующей ссылке:

http://www.visualroute.com/download.html Если с загрузкой или установкой программы VisualRoute возникнут проблемы, обратитесь за помощью к инструктору. Убедитесь, что выполняется загрузка Lite Edition.

b. С помощью программы VisualRoute 2010 Lite Edition отследите маршруты к www.cisco.com.

c. Сохраните полученные IP-адреса в файле Блокнота.

Сравнените результы трассировки

Критерии оценки:

«5» (отлично): выполнены все задания самостоятельной работы без ошибок.

«4» (хорошо): выполнены все задания самостоятельной работы с замечаниями.

«3» (удовлетворительно): выполнены не все задания самостоятельной работы, имеются замечания.

«2» (не зачтено): студент не выполнил или выполнил неправильно задания самостоятельной работы.

Практическая работа 2

Тема: Создание простой сети

Цель: закрепить материал по базовым понятиям сетевых технологий, изученным в Главе 1 и Главе 2.

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

ЗАДАНИЕ

Ответьте на вопросы, приведенные ниже. Выберите один правильный ответ или дайте развернутый ответ там, где это необходимо.

1. **Дайте определение компьютерной сети.**

_____
_____
_____

2. **К какому классу относится сеть, объединяющая компьютеры разных городов, регионов, государств?**

локальная сеть; глобальная сеть; городская сеть.

3. **Что такое беспроводная сеть?**

сеть, в которой передача информации осуществляется при помощи электромагнитных волн в определенном частотном диапазоне;

сеть, в которой для передачи данных используется телефонный провод, коаксиальный кабель или витая пара.

4. **Какой тип взаимодействия между компьютерами показан на рисунке 1.1.**

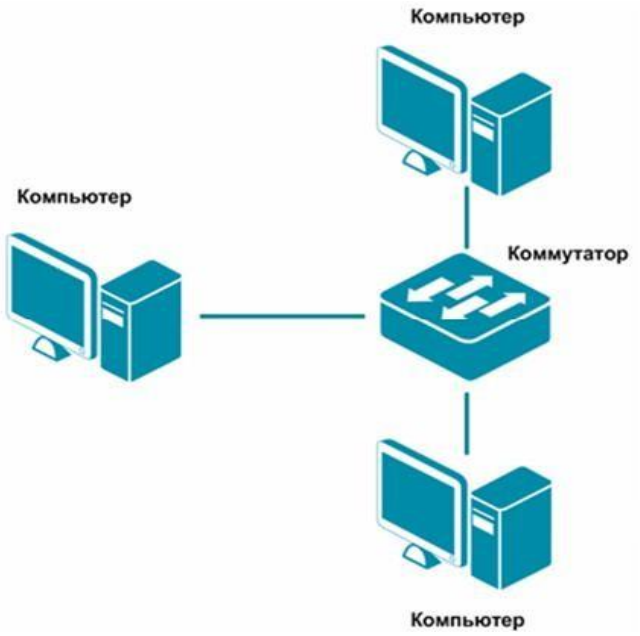


Рисунок 1.1 Взаимодействие между компьютерами

сеть типа «клиент-сервер»; одноранговая сеть; беспроводная сеть.

5. **Как называется установленное в компьютер устройство, которое позволяет ему подключаться к сети и взаимодействовать с другими устройствами?**

сетевой адаптер; маршрутизатор; коммутатор.

6. **Что такое проводная сеть?**

сеть, в которой передача информации осуществляется при помощи электромагнитных волн в определенном частотном диапазоне;

сеть, в которой для передачи данных используется телефонный провод, коаксиальный кабель или витая пара.

7. **Как называлась первая глобальная сеть, созданная в 1969 году Министерством обороны США?**

Internet; Arpanet; Intranet.

8. **Перечислите все уровни модели OSI?**

9. **Каким из перечисленных ниже терминов называют блок данных канального уровня?**

сегмент; пакет; кадр.

10. **Какой из перечисленных ниже терминов не является названием уровня в модели OSI?**

уровень приложений; уровень Интернет; сеансовый уровень.

11. **Перечислите основные достоинства и недостатки сетей типа «клиент-сервер».**

12. **Какой из уровней модели OSI отвечает за выбор наилучшего маршрута до сети назначения.**

уровень приложений; канальный уровень; сетевой уровень.

13. **Соотнесите перечисленные термины с уровнями модели OSI, к которым они относятся.**

а) кадр; Транспортный уровень _____

б) IP-адрес;

в) MAC-адрес; Сетевой уровень _____

г) пакет;

д) номер порта; Канальный уровень ___

е) сегмент; ж) биты.

14. Перечислите все уровни модели TCP/IP.

_____

_____

_____

15. Как называется процесс, при котором к данным добавляется заголовок определенного уровня перед отправкой в сеть?

декапсуляция; мультиплексирование; инкапсуляция.

16. Какие из перечисленных ниже протоколов относятся к транспортному уровню модели OSI? (Выберите 2 ответа).

IP;

Ethernet; TCP; UDP.

17. Какой из уровней модели OSI отвечает за логическую адресацию и маршрутизацию?

уровень приложений; канальный уровень; сетевой уровень.

18. Соотнесите перечисленные протоколы с уровнями модели OSI, к которым они относятся.

а) TCP; Транспортный уровень _____

б) IP;

в) Ethernet; Сетевой уровень _____

г) HTTP;

д) UDP; Уровень приложений _

е) FTP;

ж) Telnet.Физический уровень __

19. Каким из перечисленных ниже терминов называют блок данных сетевого уровня?

сегмент; пакет; кадр.

20. Какой из перечисленных ниже терминов не является названием уровня в модели TCP/IP?

уровень приложений; уровень Интернет; сеансовый уровень.

21. Каким из перечисленных ниже терминов называют блок данных транспортного уровня?

сегмент; пакет; кадр.

22. Какой из уровней модели OSI задает стандарты для кабельной системы?

уровень приложений; сеансовый уровень; физический уровень.

23. Какой из уровней модели OSI описывает стандарты форматов данных и шифрование трафика?

уровень представлений; сеансовый уровень; физический уровень; канальный уровень.

24. Когда протокол TCP передающего узла маркирует сегмент порядковым номером равным 1, а принимающий узел отправляет в ответ подтверждение приема с порядковым номером 1, такой процесс будет примером:

инкапсуляции данных;

взаимодействие двух систем на одинаковом уровне; взаимодействие двух смежных уровней;

ни один из указанных ответов не верен.

25. Какие из перечисленных ниже протоколов относятся к уровню приложений модели OSI? (Выберите 2 ответа).

IP;

Ethernet; TCP; HTTP; DNS.

Тема: Разработка топологии сети небольшого предприятия

Цель: разработать топологию сети небольшого предприятия.

При создании сети передачи данных, когда соединяются все компьютеры сети и другие сетевые устройства, формируется ***сетевая топология компьютерной сети.***

Сетевая топология — это способ описания конфигурации сети, схема расположения и соединения сетевых устройств. Существуют три базовые топологии, на основе которых строится большинство сетей:

- *«Шина» (Bus)* — все узлы соединяются между собой одним кабелем;
- *«Кольцо» (Ring)* — каждый компьютер соединяется с двумя другими так, чтобы от одного он получал информацию, а другому передавал ее. Последний компьютер подключается к первому;
- *«Звезда» (Star)* — каждый из узлов подключается к центральному соединительному устройству (коммутатору, концентратору).

Комбинированные топологии:

- *«Дерево» (Tree)* — объединение нескольких «звезд»;
- *Полносвязная топология* — каждый компьютер и другие устройства соединены друг с другом напрямую;
- *Топология неполной связности* — получается из полносвязной путем удаления некоторых возможных связей. Каждый узел сети соединяется с несколькими другими узлами сети.

При построении любой компьютерной сети используется ***коммуникационное*** или ***сетевое оборудование***. Основной его задачей является объединение компьютеров в сеть, подключение компьютерных сетей разных топологий и технологий друг к другу, увеличение расстояния передачи сигнала. Устройства, применяемые для построения компьютерной сети следующие:

Медиаконвертер (Mediaconverter) — это устройство физического уровня модели OSI, преобразующее среду распространения сигнала из одного типа в другой;

Повторитель (Repeater) — это устройство физического уровня модели OSI, используемое для соединения сегментов среды передачи данных с целью увеличения общей длины сети;

Концентратор (Concentrator) или *Хаб (Hub)* — это повторитель, который имеет несколько портов и соединяет несколько физических сегментов сети;

Мост (Bridge) — это устройство канального уровня модели OSI, которое соединяет между собой два сегмента локальной сети;

Коммутатор (Switch) — это устройство канального уровня модели OSI, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети;

Маршрутизатор (Router) — это устройство сетевого уровня модели OSI, пересылающее пакеты данных между различными сегментами сети (подсетями);

Шлюз (Gateway) — любое устройство, соединяющее разные сетевые архитектуры.

ЗАДАНИЕ 1

На рисунке 2.1 показан план 1-го этажа центрального офиса. В каждом кабинете по 6 рабочих станций. Требуется объединить в локальную сеть все сетевые устройства, находящиеся на 1-ом этаже, так, чтобы они могли обмениваться информацией друг с другом с меньшей вероятностью возникновения коллизий.

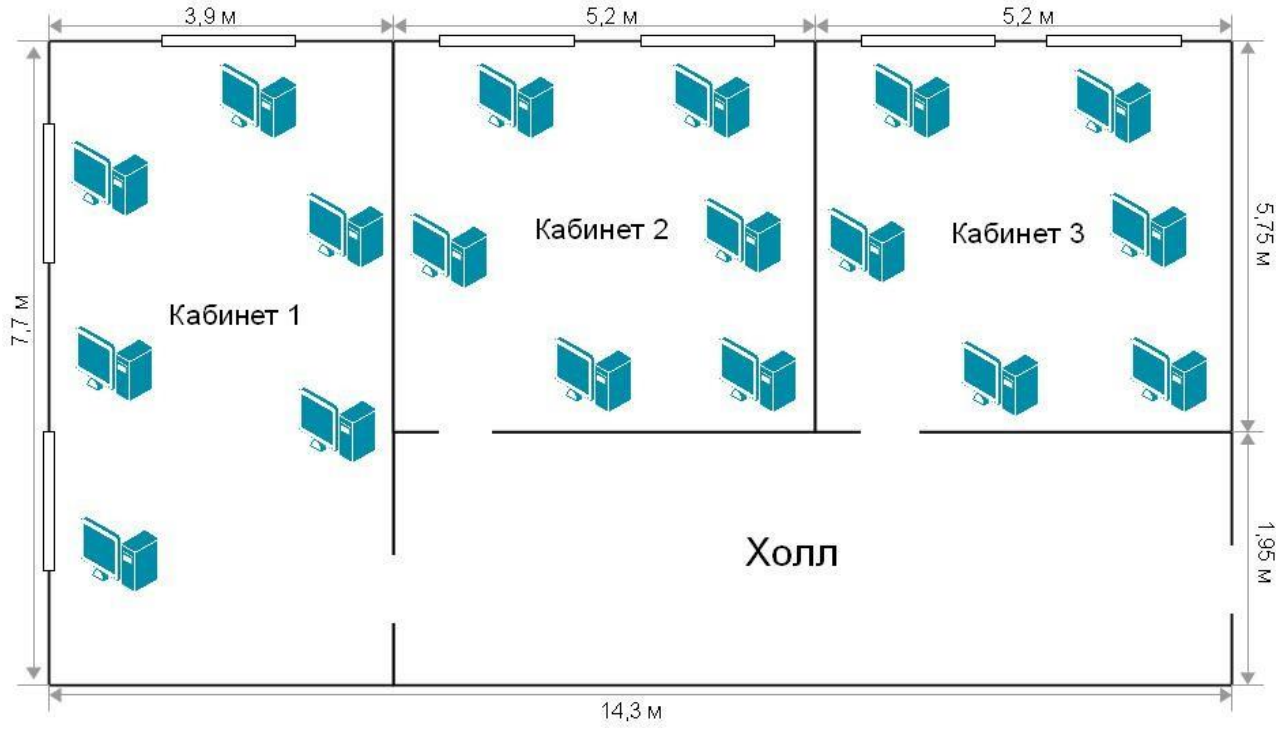


Рисунок 2.1 План 1-го этажа центрального офиса

Зарисуйте получившуюся топологию сети.

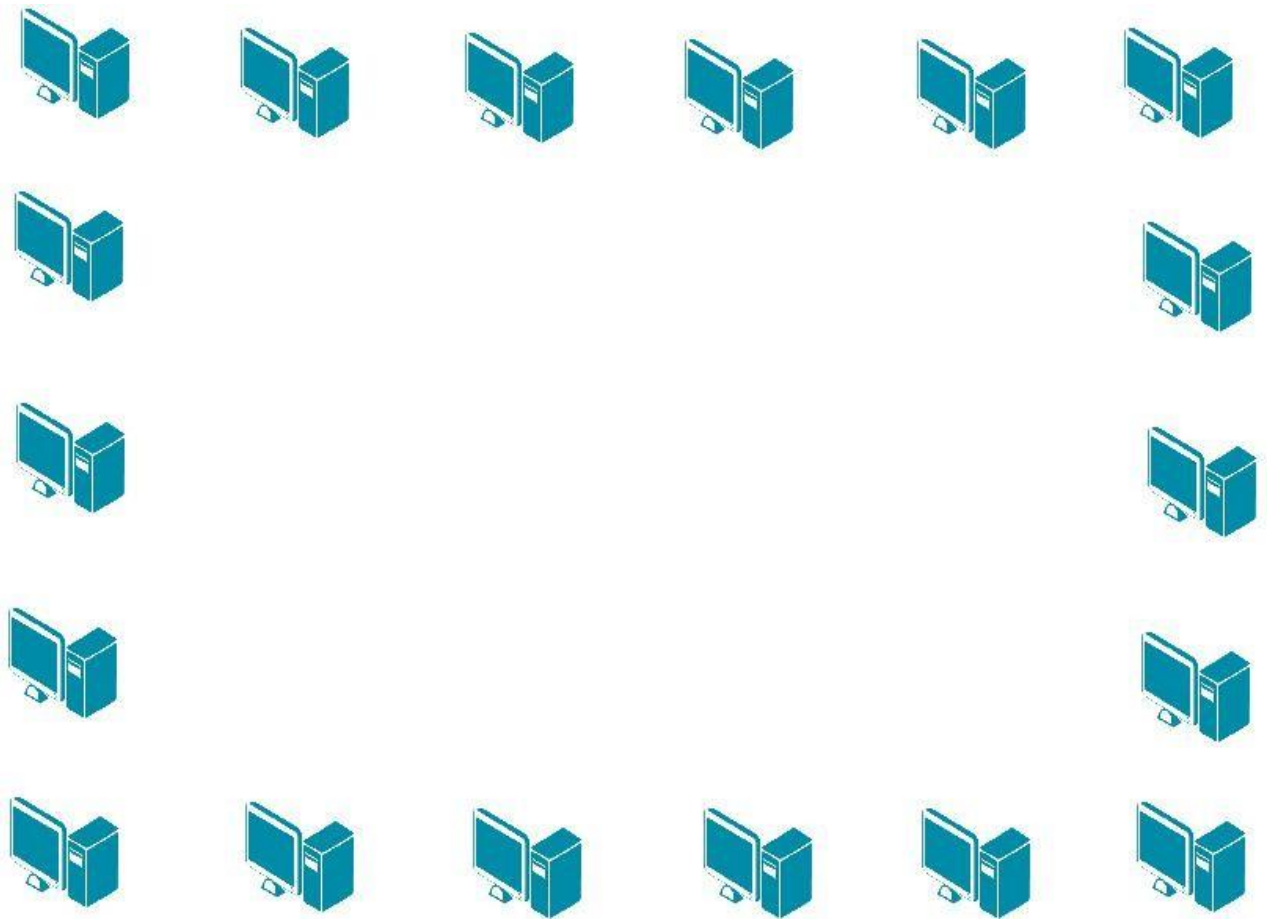


Рисунок 2.2 Топология сети центрального офиса

Какое сетевое оборудование необходимо использовать, чтобы избежать возникновения коллизий при передаче данных между компьютерами?_

Какое минимальное количество портов должно быть у сетевого оборудования? __

Обоснуйте выбор топологии сети. В чем преимущества данной топологии по сравнению с топологией «Общая шина»? __

_____

_____

ЗАДАНИЕ 2

Предположим, что компания расширилась и теперь занимает такое же помещение в соседнем здании на расстоянии 500 метров (рис. 2.3). Требуется объединить сеть центрального офиса и сеть подразделения так, чтобы сотрудники центрального офиса могли обмениваться данными с сотрудниками подразделения.

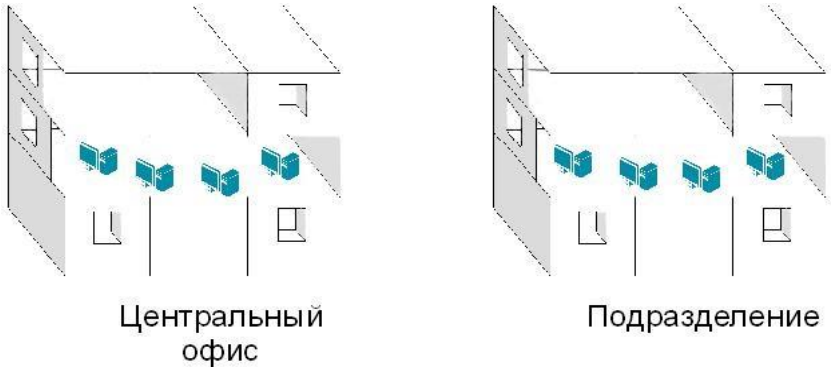


Рисунок 2.3

Зарисуйте получившуюся топологию сети.

Изучение элементов кабельной системы

Кабельная система — это система, элементами которой является *пассивное* сетевое оборудование, включающее в себя кабели, разъемы для кабелей, патч-панели, монтажные шкафы и телекоммуникационные стойки.

Кабель состоит из проводников, заключенных в несколько слоев изоляции и бывает трех типов:

- коаксиальный кабель;
- кабель на основе витой пары;
- волоконно-оптический (оптоволоконный)кабель.

Коаксиальный кабель — электрический кабель, состоящий из расположенных соосно центрального проводника и экрана. Центральная часть кабеля представляет собой монолитный или скрученный медный провод, заключенный в изолирующую пластиковую оболочку. Эту изоляцию окружает второй проводник в виде трубки (может быть из фольги), который служит экраном от электромагнитных помех. Снаружи он покрыт жесткой пластиковой трубкой, формирующей оболочку кабеля. В настоящее время коаксиальный кабель не используется для построения локальных сетей.

Кабель на основе витой пары (twisted pair) — вид кабеля, представляющий собой одну или несколько пар изолированных проводников, скрученных между собой (с небольшим числом витков на единицу длины), покрытых пластиковой оболочкой. Попарное скручивание проводов позволяет уменьшить воздействие перекрестных помех, так как электромагнитные волны, излучаемые каждым проводником, взаимно гасятся.

Различают два типа кабеля на основе витой пары:

- кабель на основе неэкранированной витой пары (unshielded twisted pair, UTP);

- кабель на основе экранированной витой пары (shielded twisted pair, STP).

Кабель на основе неэкранированной витой пары (UTP) состоит из четырех скрученных между собой пар проводов.

Кабели на основе экранированной витой пары (STP) имеют дополнительную защиту из алюминиевой фольги, которая позволяет уменьшить воздействие внешних электромагнитных полей.

Кабели на основе экранированной и неэкранированной витой пары подключаются к компьютерам и сетевым устройствам при помощи ***разъема 8P8C*** (ошибочное, но общепринятое название RJ-45).

Рисунок 3.1 Разъем 8P8C (RJ-45)

Последовательность распределения проводников в разъеме определяется стандартами EIA/TIA-568A и EIA/TIA-568B (рис.3.2).

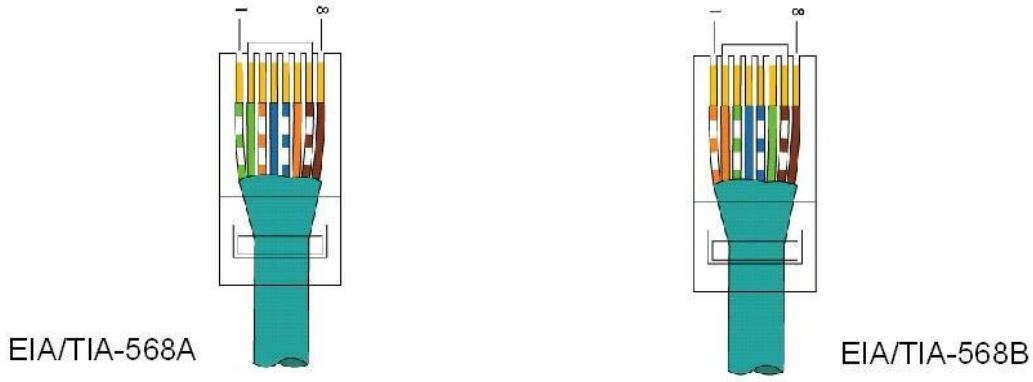


Рисунок 3.2 Распределение проводников в разъеме по стандартам EIA/TIA-568A и EIA/TIA-568B

В зависимости от схемы распределения проводников в разъемах с двух сторон кабеля, кабели делятся на:

- ***Прямые кабели (straight through cable)*** – витая пара с обеих сторон обжата одинаково, без перекрещивания пар внутри кабеля.

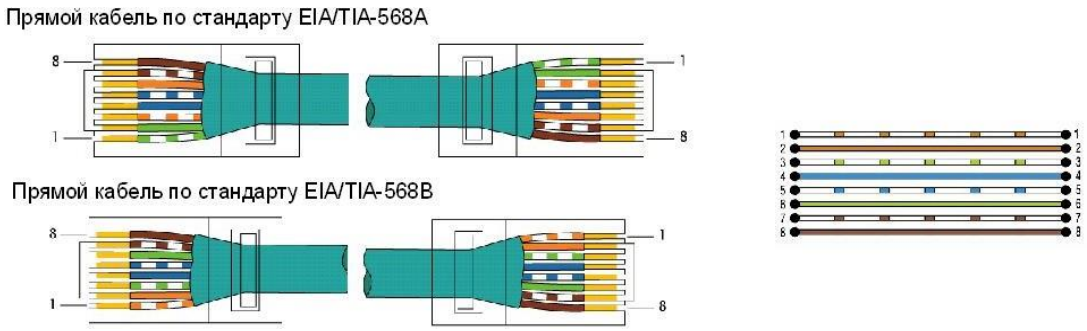


Рисунок 3.3 Прямой кабель

- ***Перекрестные кабели (crossover cable)***– инвертированная разводка с перекрещиванием пар внутри кабеля.

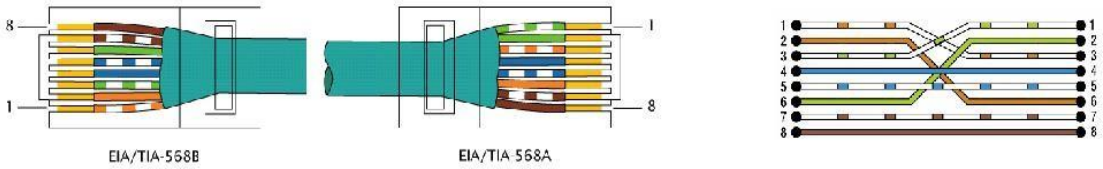


Рисунок 3.4 Перекрестный кабель

Для обжима кабеля разъемами RJ-45 используется специальный инструмент, который называется ***кримпер*** (рис. 3.5).

Рисунок 3.5 Инструмент для обжима кабеля разъемами RJ-45 (кримпер)

Оборудование (на 1 рабочее место):

Кабель Ethernet (UTP)	0,2 м.
Волоконно-оптический кабель	0,2 м.
Разъем RJ-45	2 шт.
Обжимной инструмент (кримпер)	1 шт.
Разъем типа SC-FC (или SC-ST)	1 шт.
Сетевой тестер	1 шт.

Цель:

1) Изучить волоконно-оптический кабель;
2) Научиться обжимать кабель UTP разъемами RJ-45;
3) Получить навыки в расчете кабельной сети.

3.1. Изучение волоконно-оптического кабеля

ЗАДАНИЕ

Так как заделка волоконно-оптического кабеля производится методом сварки и требует специальной подготовки, в данной работе производится только визуальное изучение образца волоконно-оптического кабеля и разъемов.

Волоконно-оптический (оптоволоконный) кабель состоит из светопроводящего стеклянного сердечника, окруженного стеклянной оболочкой с меньшим коэффициентом преломления.

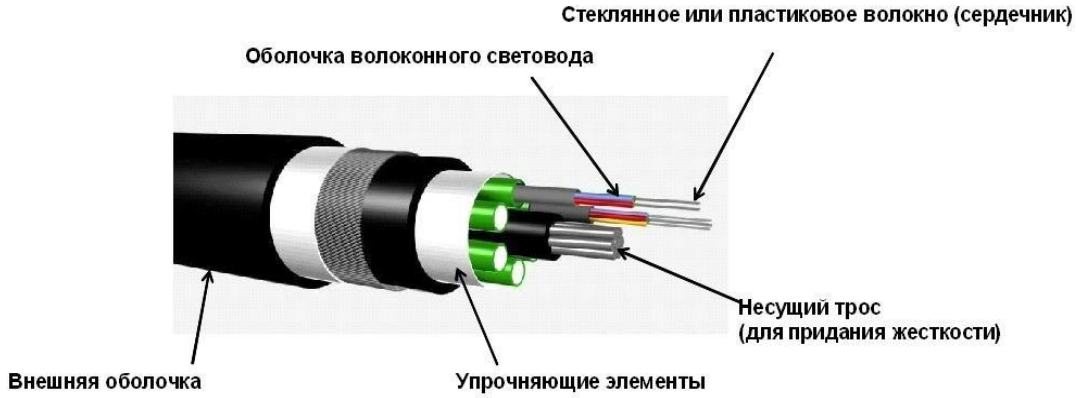


Рисунок 3.6 Волоконно-оптический кабель

В зависимости от распределения показателя преломления и от величины диаметра сердечника различают:

- одномодовый волокно-оптический кабель;
- многомодовый волокно-оптический кабель.

В ***одномодовом кабеле (Single Mode Fiber, SMF)*** оптический сигнал, распространяющийся по сердцевине, представлен одной модой. В одномодовом кабеле используется центральный сердечник очень малого диаметра, соизмеримого с длиной волны света — 5-10 мкм. В качестве источников излучения света в одномодовом кабеле применяются полупроводниковые лазеры с длиной волны 1300 нм, 1550 нм. Максимальная длина кабеля — 100 км, поэтому он используется, как правило, для протяженных линий связи, городских и региональных

сетей. Пропускная способность одномодового оптического кабеля превышает 10 Гбит/с.

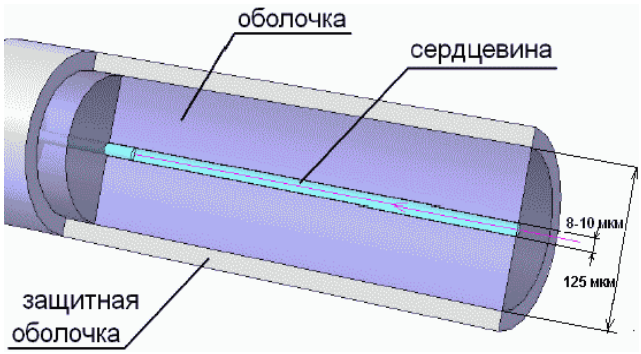


Рисунок 3.7 Одномодовый оптический кабель в разрезе

В ***многомодовом кабеле (Multi Mode Fiber, MMF)*** оптический сигнал, распространяющийся по сердцевине, представлен множеством мод. В многомодовых кабелях используются внутренние сердечники с диаметрами 62,5/125 мкм и 50/125 мкм, где 62,5 мкм или 50 мкм — это диаметр центрального проводника, а 125 мкм — диаметр внешнего проводника. В качестве источников излучения света в многомодовом кабеле применяются светодиоды с длиной волны 850 нм. Максимальная длина кабеля — 2 км. Используется в

локальных и домашних сетях небольшой протяженности.

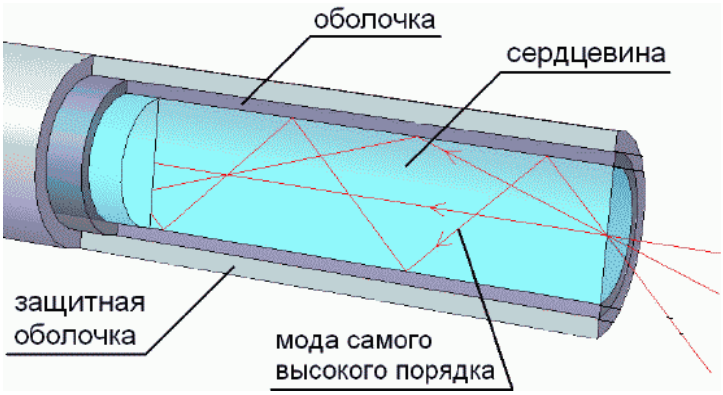


Рисунок 3.8 Многомодовый оптический кабель в разрезе

Волоконно-оптические кабели присоединяются к оборудованию разъемами: MT-RJ, ST, FC, SC, LC.

Разъем типа MT-RJ представляет собой миниатюрный дуплексный разъем.

Рисунок 3.9 Разъем типа MT-RJ

Разъем типа ST использует быстро сочленяемое байонетное

соединение, которое требует поворота разъема на четверть оборота для осуществления соединения/разъединения.

Рисунок 3.10 Разъем типа ST

Разъемы типа FC ориентированы на работу с одномодовым кабелем.

Рисунок 3.11 Разъем типа FC

Разъемы типа SC широко используются как для одномодового, так и для многомодового волокна. Относится к классу разъемов общего пользования. В разъеме используется механизм сочленения «push-pull». Может объединяться в модуль, состоящий из нескольких разъемов. В этом случае модуль может использоваться для дуплексного соединения, одно волокно которого используется для передачи в прямом, а другое в обратном направлениях.

Рисунок 3.12 Разъем типа SC

Разъем типа LC имеет размер примерно в два раза меньше, чем разъемы SC, FC, ST, что позволяет реализовать большую плотность при установке на коммутационной панели.

Рисунок 3.13 Разъем типа LC

3.2. Обжим UTP-кабеля разъемами RJ-45

ЗАДАНИЕ

Обожмите UTP-кабель с обеих сторон по стандарту EIA/TIA-568A или EIA/TIA-568B (прямой кабель) и проверьте его работоспособность при помощи сетевого тестера.

Шаг 1. Аккуратно снимите с одного конца кабеля 3-4 см внешней изоляции. После этого вы увидите восемь разноцветных проводов, скрученных попарно (рис.3.14).

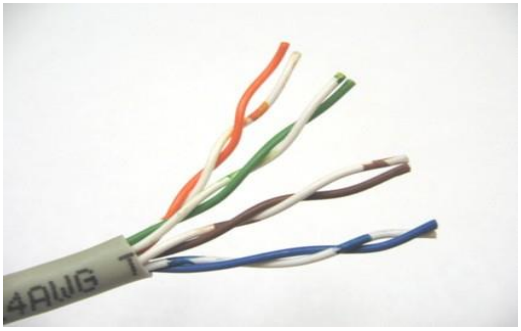


Рисунок 3.14 Кабель UTP без внешней изоляции

Шаг 2. Раскрутите каждый проводник до начала внешней изоляции. Все проводники должны быть ровными и прямыми.

Шаг 3. Расположите восемь цветных проводников плотно друг к другу в соответствии со стандартом EIA/TIA-568A или EIA/TIA-568B (рис.3.15).

Рисунок 3.15 Распределение проводников в разъеме по стандартам EIA/TIA-568A и EIA/TIA-568B

Шаг 4. Плотно прижимая проводники, обрежьте неровные края, оставляя примерно 1 см.

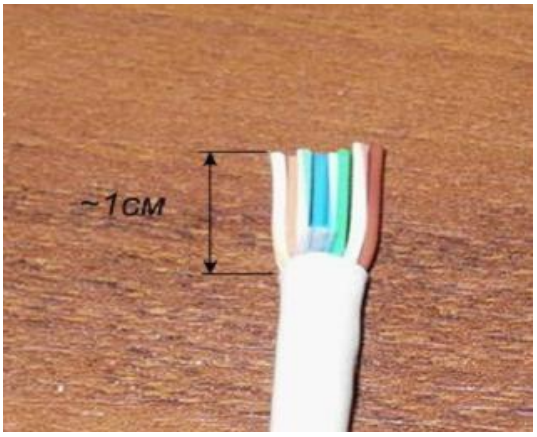


Рисунок 3.16 Выравнивание проводников

Шаг 5. Возьмите разъем RJ-45 и поверните его контактами вверх. Аккуратно вставьте проводники в разъем так, чтобы они попали в соответствующие дорожки и цветовое расположение не перепуталось. Следите за тем, чтобы все проводники доходили до конца разъема и внешняя изоляция кабеля выходила за фиксирующую защелку.

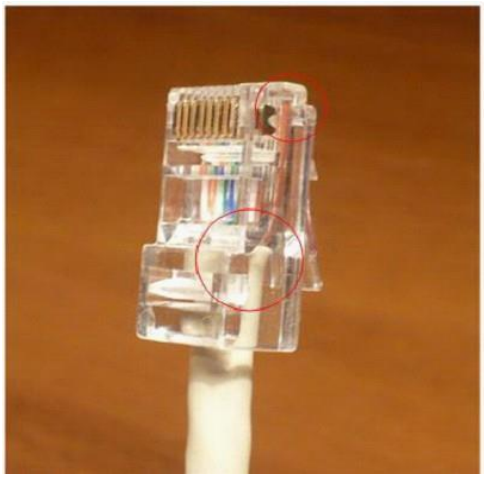


Рисунок 3.17 Места, на которые необходимо обратить внимание при обжиме кабеля

Внимание: часто на этом шаге проводники смещаются, особенно если используется некачественный кабель. В этом случае извлеките кабель из разъема и повторите шаг 5.

Шаг 6. Убедившись в правильном расположении проводников, вставьте разъем в обжимной инструмент (кримпер), как показано на рисунке 3.18, и аккуратно зажмите.

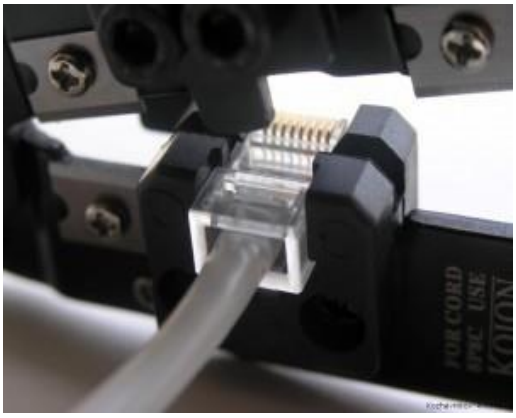


Рисунок 3.18 Обжим разъема RJ-45 кримпером

Шаг 7. Извлеките обжатый разъем из кримпера и еще раз проверьте расположение проводников. Правильно обжатый кабель показан на рисунке 3.19.

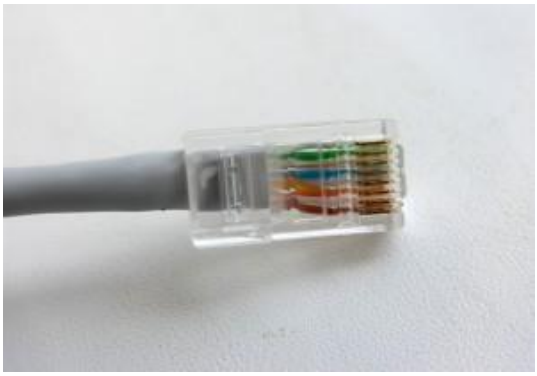


Рисунок 3.19 Правильно обжатый кабель

При неправильном обжиме внешняя изоляция кабеля не закреплена фиксирующей защелкой разъема и проводники могут смещаться. Пример неправильно обжатого кабеля показан на рисунке 3.20.

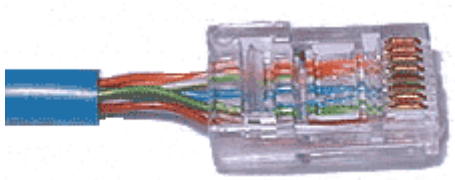


Рисунок 3.20 Неправильно обжатый кабель

Шаг 8. Повторите шаги 1-7 для обжима другого конца кабеля. Используйте ту же схему, что и для первого конца кабеля. Такой тип обжима называется ***прямой обжим***.

Прямой тип кабеля используется в тех случаях, когда устройства на противоположных концах используют разные номера проводников для приема и передачи информации. Например, прямым кабелем соединяются компьютер-коммутатор.

Для подключения друг к другу устройств, использующих одинаковые номера проводников для приема и передачи информации, в самом кабеле необходимо поменять местами пары проводников. Такой кабель

называется **перекрестным кабелем**. Таким типом кабеля соединяют, например, компьютер-компьютер.

Шаг 9. Подключите кабель к сетевому тестеру обоими концами.

Рисунок 3.21 Сетевой тестер

Сетевой тестер состоит из двух независимых частей, на каждой из которых расположены 8 индикаторов и по одному разъему RJ-45. Если кабель обжат правильно, то все индикаторы должны загораться последовательно, если кабель обжат неправильно, то индикатор не загорится.

3.3. Расчет кабельной сети

ЗАДАНИЕ

Для топологии сети из лабораторной работы №2 (задание 1) выберите тип кабельной системы и рассчитайте длину кабеля. На рисунке 3.22 обозначьте расположение коммутатора и соедините с ним каждый компьютер при помощи кабеля.

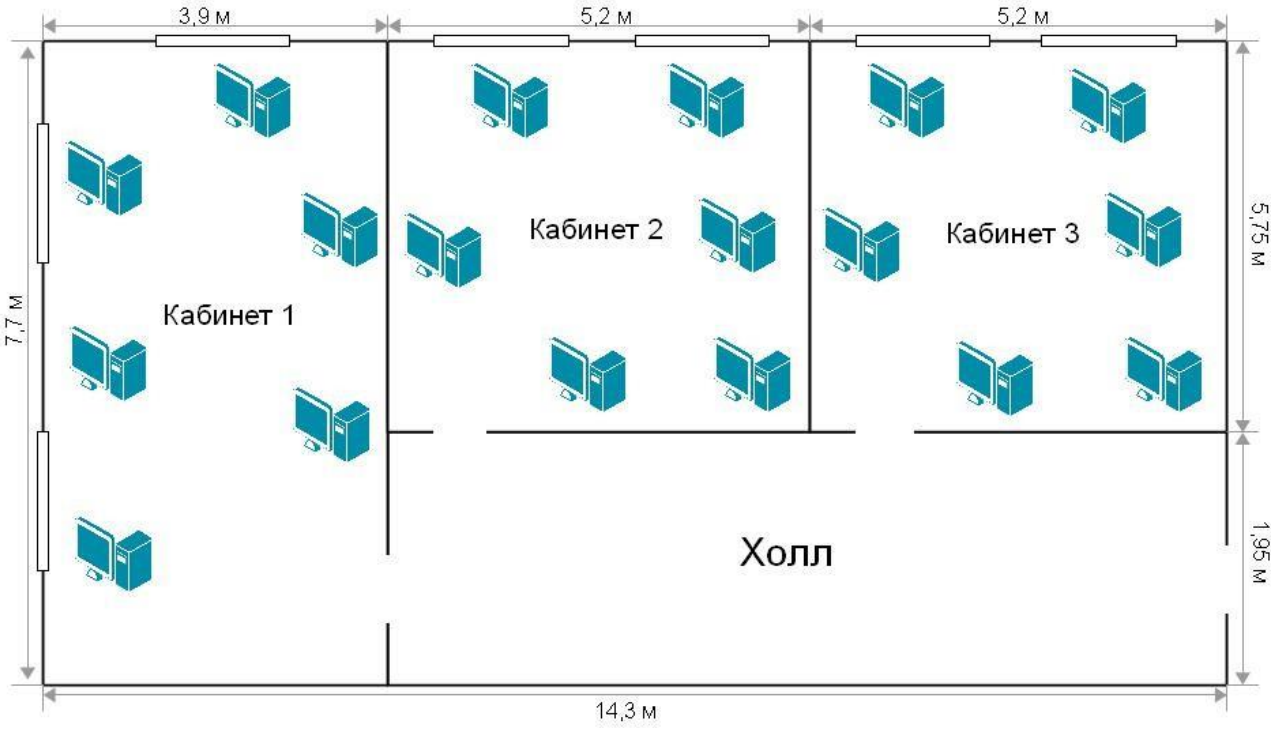


Рисунок 3.22 Схема 1-го этажа центрального офиса

Тип кабеля ___

Сколько кабеля (в метрах) понадобится для объединения компьютеров центрального офиса в сеть, если все компьютеры стоят у стен и коммутатор размещен в кабинете 3? (В межкомнатных перегородках запрещается просверливать отверстия) _____

Практическая работа 4

Тема: Монтаж кабельных сред технологий Ethernet

Цель: проанализовать схемы и таблицы для кабеля Ethernet стандарта TIA/EIA568-A и TIA/EIA568-B, получить навыки оконцевания неэкранированной «витой пары», получить навыки подключения кабеля «витая пара» к неэкранированным (экранированным) патч-панелям.

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Оборудование: кабель UTP, коннектор RJ-45, инструмент по зачистке кабеля, кримпер, кабельный тестер, ПК с операционной системой.

Ход работы

1. Ознакомиться с теоретической частью.
2. Выполнить задания.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Теоретическая часть

1. Анализ стандартов и схемы подключения кабелей Ethernet.

Стандарты TIA/EIA определяют правила использования неэкранированных витых пар в локальных средах. Стандарты TIA/EIA 568-A и 568-B обусловливают коммерческие кабельные стандарты для локальных сетей; они широко применяются в разводке локальных сетей для организаций и, кроме прочего, определяют цвет каждого кабеля для разных контактов.

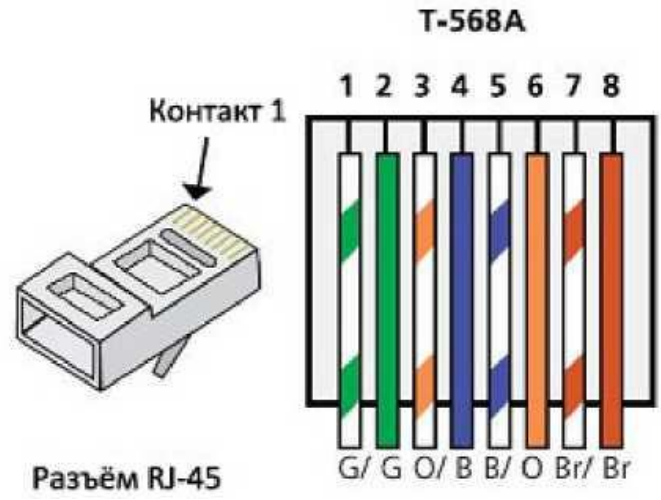
В кроссовом кабеле вторая и третья пары разъёма RJ-45 на одном конце кабеля переворачиваются на другом конце, что меняет местами пары отправки и приёма. На одном конце кабеля используется схема подключения кабеля со стандартом 568-A, а на другом — со стандартом 568-B. Кроссовые кабели обычно используются для подключения концентраторов к концентраторам или коммутаторов к коммутаторам, но могут применяться и для создания простой сети из двух узлов.

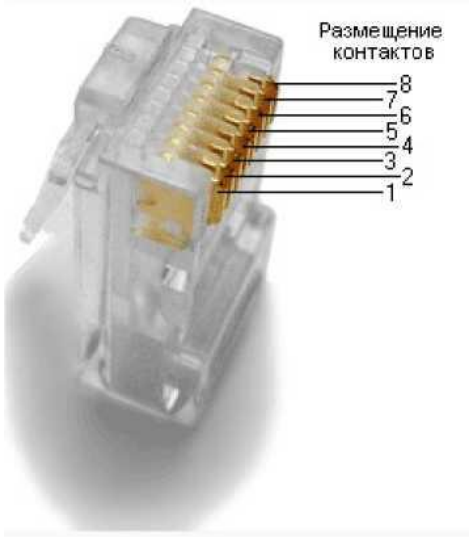
Приведённая ниже таблица и рисунки демонстрируют цветовую схему и расположение выводов, а также работу четырёх пар проводов, предусмотренных стандартом 568-A. ***Примечание****. В локальных сетях на основе стандарта 100Base-T (100 Мбит/с) используются только две пары из четырёх.*

Таблица 1 - 568-A 10/100/1000Base-TX Ethernet

Номер разводки	**Номер пары**	**Цвет провода**	**10Base-T 100Base-TX**	**1000Base-T**
1	2	Белый/зелёный	Передача	BI_DA+
2	2	Зелёный	Передача	BI_DA-
3	3	Белый/оранжевый	Приём	BI_DB+
4	1	Синий	Не используется	BI_DC+
5	1	Белый/синий	Не используется	BI_DC-
6	3	Оранжевый	Приём	BI_DB-
7	4	Белый/коричневый	Не используется	BI_DD+
8	4	Коричневый	Не используется	BI_DD-

На приведённых ниже рисунках показано, как цвета и расположение выводов разъёма RJ-45 соотносятся со стандартом 568-A.

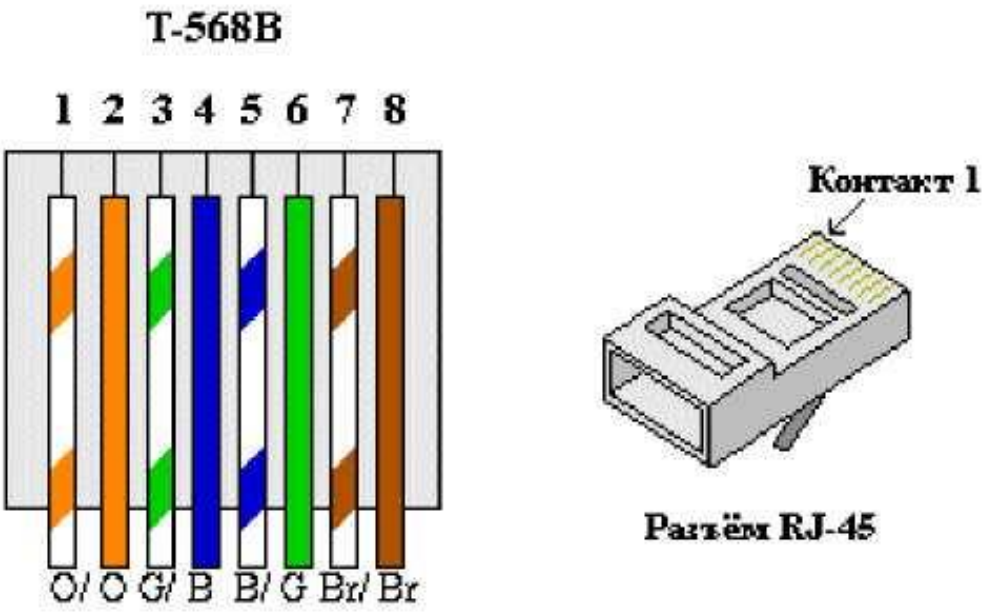




Приведённая ниже таблица и рисунок демонстрируют цветовую схему и расположение выводов для стандарта 568-B.

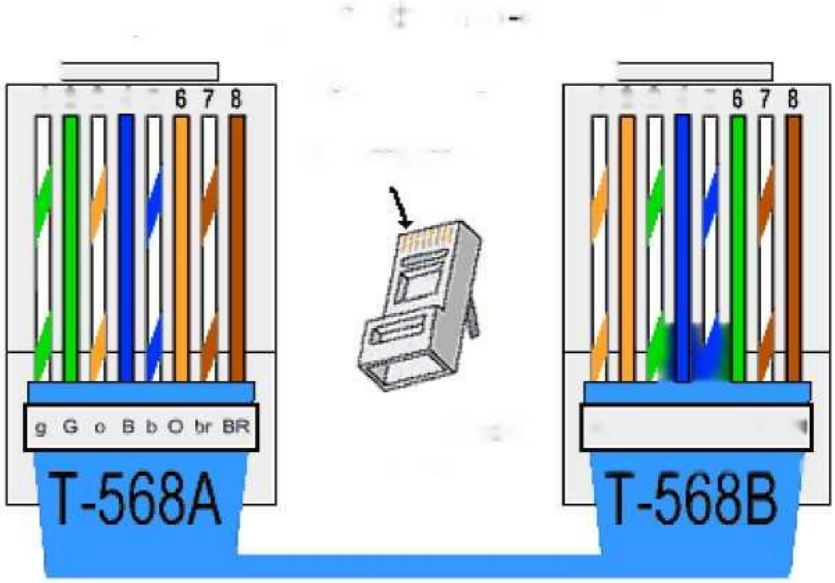
Таблица 2 - 568-B 10/100/1000-BaseTX Ethernet

Номер	**Номер пары**	**Цвет провода**	**10Base-T 100Base-**	**1000Base-T**
1	2	Белый/оранж	Передача	BI_DA+
2	2	Оранжевый	Передача	BI_DA-
3	3	Белый/зелён	Приём	BI_DB+
4	1	Синий	Не	BI_DC+
5	1	Белый/синий	Не	BI_DC-
6	3	Зелёный	Приём	BI_DB-
7	4	Белый/корич	Не	BI_DD+
8	4	Коричневый	Не	BI_DD-



2. Изготовление кроссового кабеля Ethernet

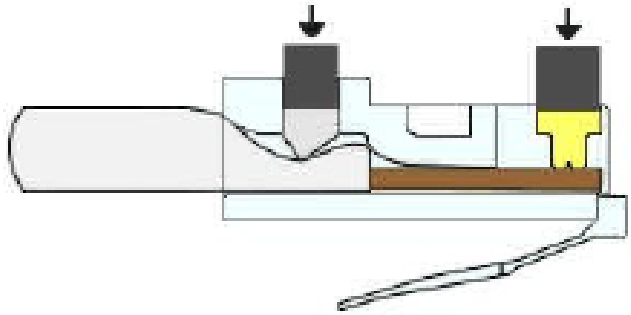
На кроссовом кабеле вторая и третья пары проводов в разъёме RJ-45 на одном конце обращены в обратную сторону (см. таблицу 2). На одном конце кабеля используется схема подключения кабеля со стандартом 568-A, а на другом — со стандартом 568-B. Два приведённых ниже рисунка иллюстрируют данный принцип.



Изготовление и обработка разъёма кабеля TIA/EIA 568-A.

1. Определить необходимую длину кабеля.

2. Отрезать кусок кабеля нужной длины и с помощью инструмента для снятия изоляции очистить от оболочки оба конца кабеля на 3...5 см.
3. В месте срезания оболочки плотно сжать все четыре пары витых кабелей. Поменять пары кабелей местами в порядке, соответствующем стандарту проводного подключения 568-А. При необходимости обращаться к рисунку. Не повредите витые пары кабеля; их целостность обеспечивает отсутствие помех.
4. Большим и указательным пальцами сплющить, выпрямить и выровнять провода.
5. Убедиться в том, что провода кабеля расположены в правильном порядке, соответствующем стандарту 568-А. С помощью кусачек обрезать четыре пары в прямую линию до длины 1...1,2 см.
6. На конце кабеля установить разъём RJ-45, выступ которого должен быть направлен вниз. Плотно вставить провода в разъём RJ-45. Все провода должны быть видны в конце разъёма на соответствующих местах. Если провода не достигают конца разъёма, извлечь кабель, поменять расположение проводов соответствующим образом и вставить провода обратно в разъём RJ-45.
7. Если всё сделано правильно, вставить разъём RJ-45 с кабелем в обжимной инструмент. Сжать кабель в инструменте достаточно сильно, так чтобы контакты на разъёме RJ-45 прошли через изоляцию проводов, закрывая таким образом проводной канал. См. пример на приведённом ниже рисунке.

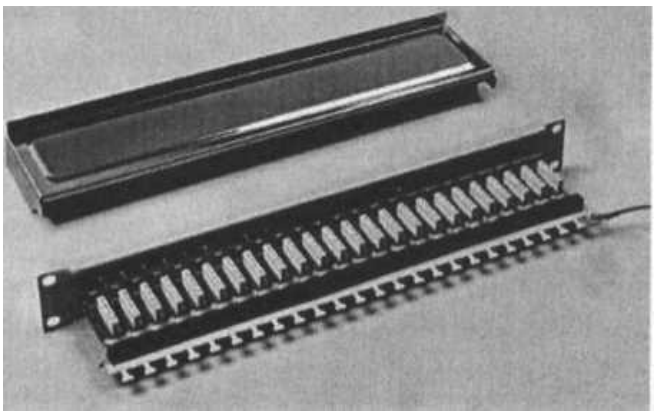


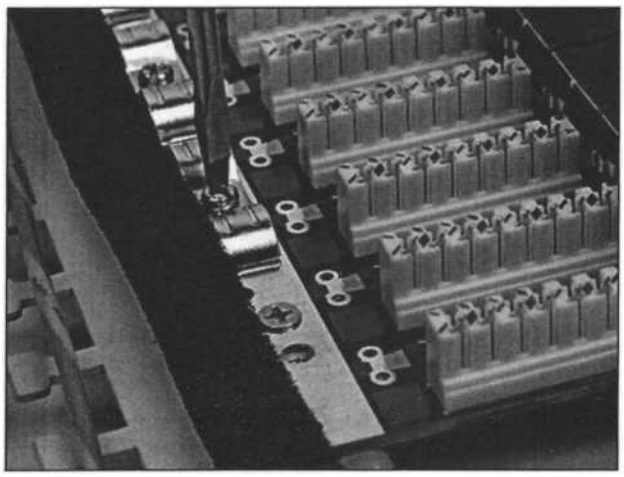
Изготовление и обработка разъёма кабеля TIA/EIA 568-B.

Выполнить шаги 1-7 из предыдущей инструкции, используя цветовую схему проводки 568-B, для другого конца.

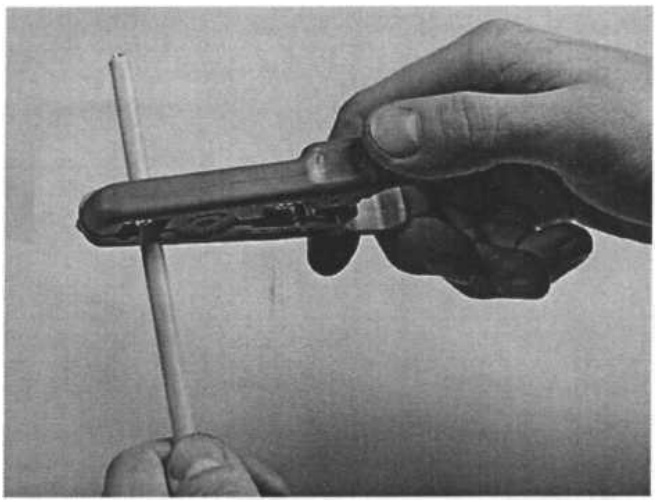
3. Инструкция по монтажу экранированной патч-панели

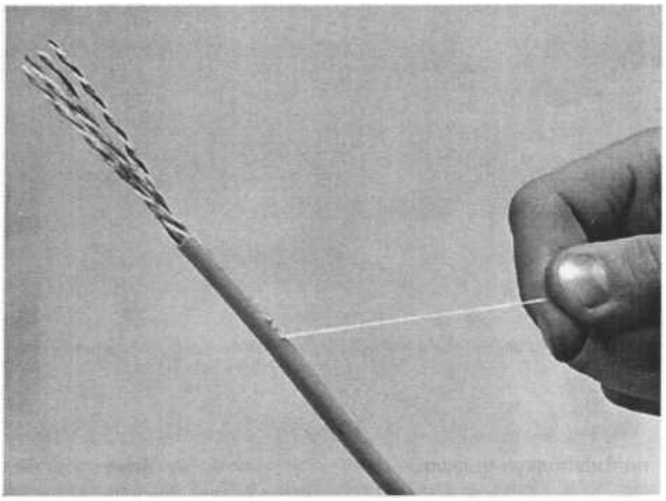
Снимите с патч-панели защитный экран и отложите его в сторону. Открутите прижимные клипсы, используя отвертку.



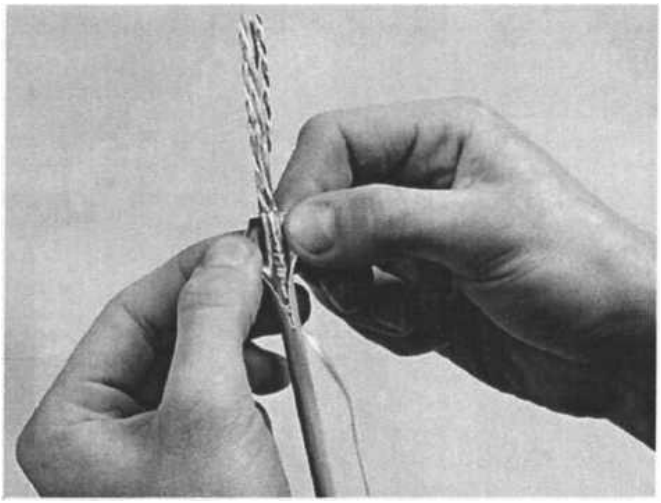


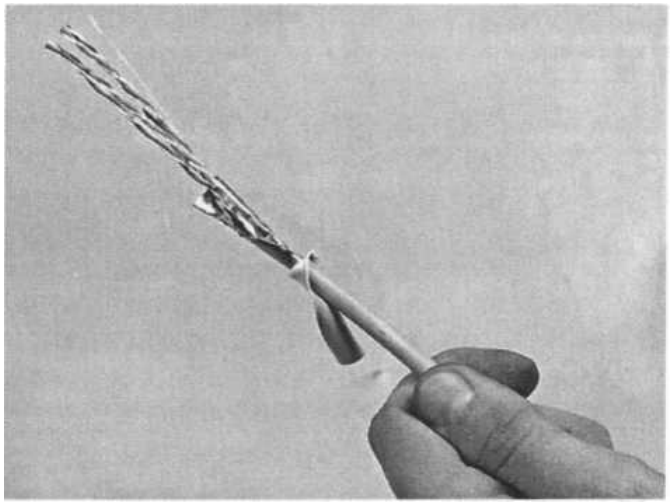
Выполните кольцевую подрезку оболочки кабеля для снятия верхней изоляции. Для этого нижним ножом обжимных клещей надо сделать один полный оборот вокруг кабеля и снять подрезанную часть изоляции. Для снятия верхней изоляции кабеля используйте шелковую нить (rip-cord), расположенную под оболочкой. Потяните ее в сторону с небольшим усилием, нить сделает на оболочке продольный разрез.



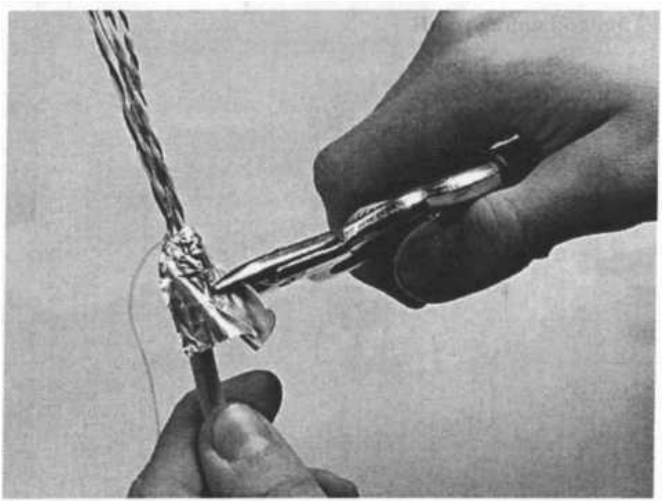


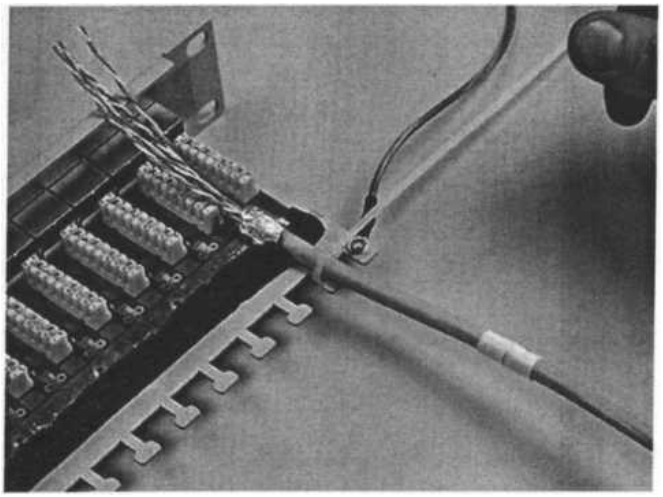
Разверните оболочку и загните ее вниз. Таким же образом разверните фольгу и загните ее вниз на внешнюю изоляцию. Фольга с дренажным проводом из луженой меди служит в качестве экрана.





Срежьте ножницами лишнюю часть оболочки с фольгой, оставив 1,5 см (соответствует ширине клипсы). Заведите подготовленный кабель на IDC модуль патч-панели. Поскольку для монтажа кабеля применяется метод "контакта со смещением изоляции" (IDC), не нужно зачищать изоляцию жил. Закрепите кабель на заднем органайзере при помощи пластиковой стяжки.

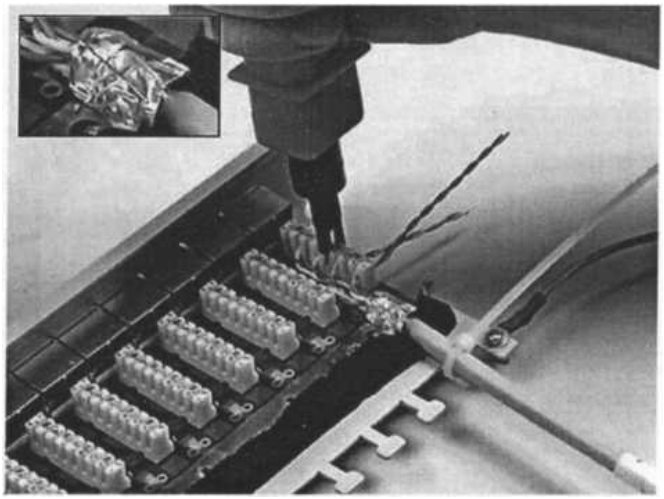


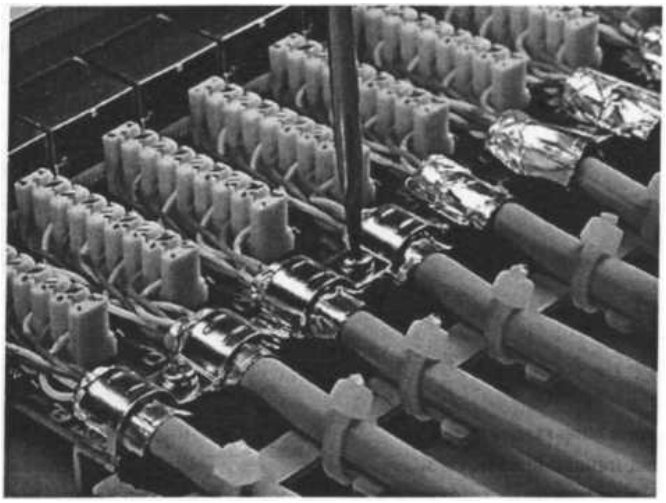


Разложите витые пары, ориентируясь по цветовой маркировке на патч-панели, в соответствии с выбранным вариантом T568A или T568B. Загните на фольгу дренажный провод, который страхует кабель от разрывов фольги и обеспечивает электрическую непрерывность экрана

Переведите кабель в рабочее положение при помощи специального инструмента. Чтобы вшить проводники в IDC модуль, необходимо до упора надавить на них инструментом. Нож IDC модуля прорезает изоляцию и врезается в металл жилы, что гарантирует надежный контакт

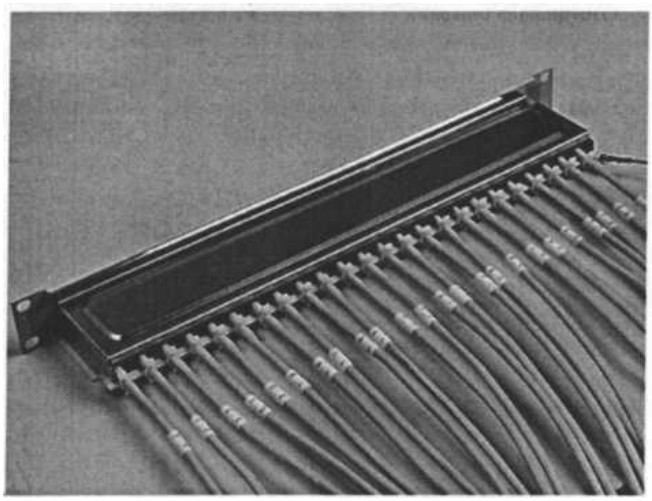
В данном случае использовалось устройство для заделки витой пары с ударным эффектом. Этот инструмент предназначен также для одновременной обрезки витой пары.

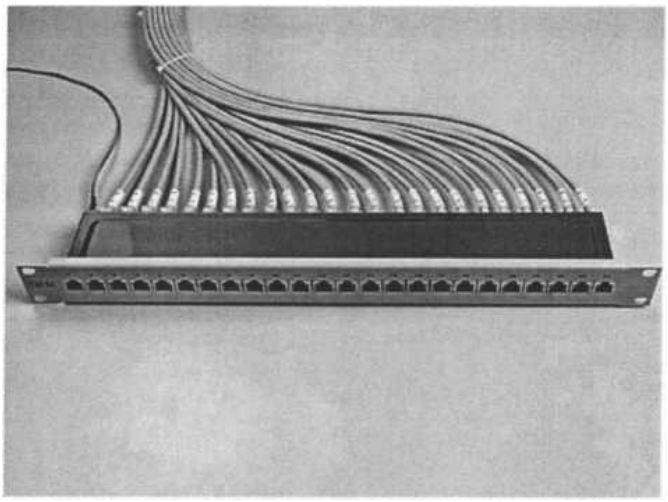




Таким же образом подготовьте и смонтируйте все кабели. Прикрутите прижимные клипсы до упора, чтобы они плотно соприкасались с фольгой и дренажным проводом. Обрежьте «хвосты» стяжек инструментом для затягивания стяжек.

Установите на место защитный экран. Аккуратно сгруппируйте все кабели и закрепите пластиковыми стяжками. Когда кабели жгутируются, обратите внимание на то, чтобы они не были слишком перетянуты. Можно жгутировать кабели как в одну сторону, так и в разные стороны.





Порядок выполнения работы

Задание 1. Изготовление неэкранированных коммутационных шнуров.

1. Ознакомьтесь с соответствующей инструкцией в теоретической части.
2. Отрежьте кабель «витой пары» категории 5е или 6 длиной 50 см.
3. Снимите 10 мм внешней оболочки с обоих концов.
4. Расплетите жилы.
5. Разложите жилы по схеме TIA568B.
6. Обрежьте жилы до ровных краёв.
7. Наденьте на жилы оконечивающий коннектор.
8. Закрепите коннектор обжимными клещами.

9. Повторите действия 2-7 для второго конца.
10. Проверьте качество изготовленного шнура кабельным тестером.

Задание 2. Подключение шнуров к экранированной патч-панели.

1. Ознакомьтесь с соответствующей инструкцией в теоретической части.
2. Возьмите экранированный кабель категории 6.
3. Снимите 5 см защитной оболочки.
4. С помощью рип-корда снимите еще 15 см защитной оболочки.
5. Аккуратно разверните фольгу и заверните ее на кабель ниже места подключения.
6. Оберните дренажный провод вокруг фольги.
7. Снимите защитную крышку патч-панели и прижимную планку.
8. Осуществите монтаж этого конца в патч-панель.
9. Поставьте на место прижимную планку и соберите патч-панель и розетку.
10. Проверьте качество выполненного монтажа кабельным тестером.

Контрольные вопросы

1. Последовательность расположения проводников по стандарту 568A.

2. Последовательность расположения проводников по стандарту 568B.

3. В чем заключается принцип врезного контакта?

4. Какие инструменты используются для оконцевания кабеля UTP, а какие для заделки в патч-панели?

Практическая работа 5

Тема: Сегментация IP-сетей, изучение калькуляторов подсетей, расчёт подсетей IPv4

Цель: научиться определять количество и диапазон адресов возможных узлов в подсетях; научиться структурировать сети с использованием масок

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задание:

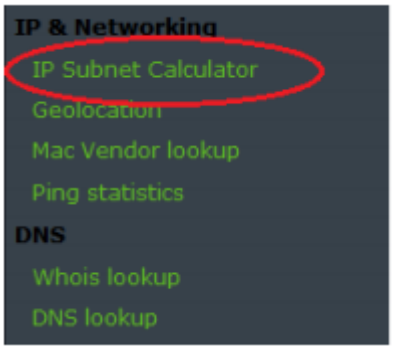
Обзор доступных калькуляторов подсетей

1: Рассмотрите некоторые программы для расчёта данных подсетей. Компания Solarwinds предлагает бесплатный калькулятор подсетей, который можно загрузить и установить на компьютер под управлением ОС Windows. Для загрузки этой программы необходимо указать личные данные (имя, компанию, страну, адрес электронной почты и номер телефона). Загрузить и установить калькулятор подсетей Solarwinds можно с веб-сайта компании www.solarwinds.com.

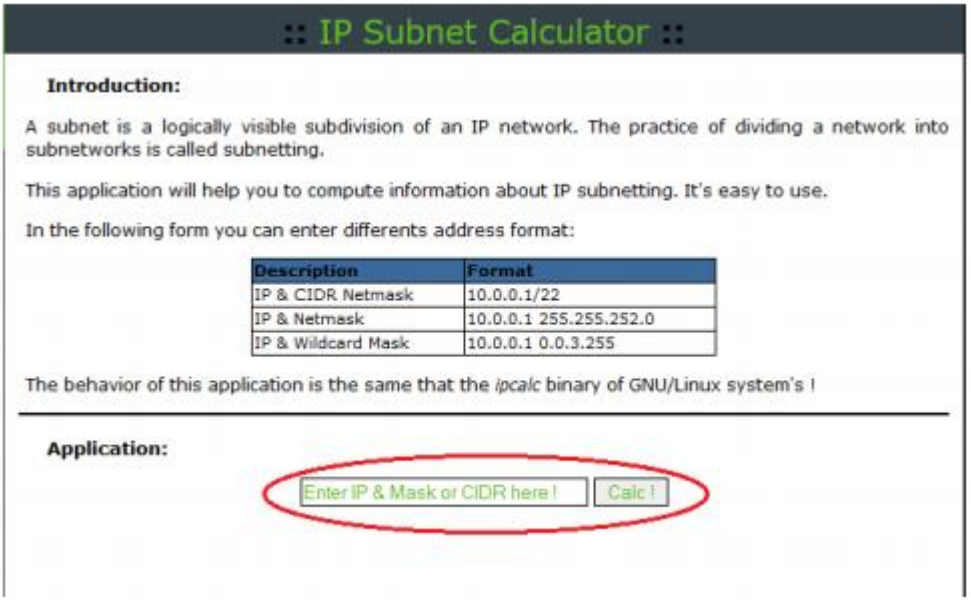
Если вы используете компьютер под управлением ОС Linux, рекомендуем утилиту ipcalc, которую можно найти в большинстве версий системы Linux. Для установки утилиты ipcalc на компьютер под управлением Linux воспользуйтесь командой apt-get install ipcalc.

2: Воспользуйтесь веб-калькулятором подсетей. Веб-калькуляторы подсетей не требуют установки, но для работы с ними необходимо подключение к Интернету. Указанный ниже веб-калькулятор подсетей можно использовать на любом устройстве с доступом к Интернету, включая смартфоны и планшеты.

a. Откройте браузер, перейдите на сайт www.ipcalc.org и выберите ссылку IP Subnet Calculator (Калькулятор IP-подсетей)



b. Нажмите ссылку IP Subnet Calculator (Калькулятор IP-подсетей), и введите в открывшемся окне IPадрес и маску подсети или IP-адрес и префиксную запись CIDR. Примеры ввода каждого из этих параметров показаны в разделе Introduction (Введение)



c. В поле Application (Приложение) введите 192.168.50.50/27 и нажмите кнопку Calc! (Рассчитать). Ниже появится таблица с информацией о сети в десятичном и двоичном форматах.

Application:

192.168.50.50/27 Calc !

Description	Value		Extra
Address	192.168.50.50	11000000.10101000.00110010.00110010	
Netmask	255.255.255.224	11111111.11111111.11111111.11100000	/27
Network	192.168.50.32	11000000.10101000.00110010.00100000	
Broadcast	192.168.50.63		
Host min	192.168.50.33	11000000.10101000.00110010.00100001	
Host max	192.168.50.62	11000000.10101000.00110010.00111110	
Host/net	30	Class C, Private Internet	

Используя приведённые выше данные, ответьте на вопросы.

Назовите сетевой адрес. _____

Назовите маску подсети. _____

Сколько узлов поддерживает эта сеть? _____

Назовите наименьший адрес узла. _____

Назовите наибольший адрес узла. _____

Назовите широковещательный адрес. _____

Расчёт сетевых данных с помощью калькулятора подсетей

1: Заполните приведённую ниже таблицу для адреса 10.223.23.136/10.

Описание	Десятичное	Двоичное
Адрес	10.223.23.136	
Маска подсети		
Сетевой адрес		
Широковещательный адрес		
Адрес первого узла		
Адрес последнего узла		
Число доступных узлов		Недоступно

Общий или частный тип адреса?

2. Заполните приведённую ниже таблицу для адреса 172.18.255.92 с маской подсети 255.255.224.0.

Описание	Десятичное	Двоичное
Адрес	172.18.255.92	
Маска подсети	255.255.224.0	
Сетевой адрес		
Широковещательный адрес		
Адрес первого узла		
Адрес последнего узла		
Число доступных узлов		Недоступно

Какова в данной сети префиксная запись CIDR?

Общий или частный тип адреса?

3: Заполните приведённую ниже таблицу, используя адрес 192.168.184.78 с маской подсети 255.255.255.252.

Описание	Десятичное	Двоичное
Адрес	192.168.184.78	
Маска подсети		
Сетевой адрес		
Широковещательный адрес		
Адрес первого узла		
Адрес последнего узла		
Число доступных узлов		Недоступно

Какова в данной сети префиксная запись CIDR?

Общий или частный тип адреса?

Где может использоваться такая сеть?

Задание 2.

Заполните приведенные ниже таблицы, зная заданный IPv4-адрес, исходную и новую маску подсети

Дано:	
IP-адрес узла	10.101.99.228
Исходная маска подсети	255.0.0.0
Новая маска подсети	255.255.128.0
Найти:	
Количество битов подсети	
Количество созданных подсетей	
Количество битов узлов в подсети	
Количество узлов в подсети	
Сетевой адрес этой подсети	
Адрес IPv4 первого узла в этой подсети	
Адрес IPv4 последнего узла в этой подсети	
Широковещательный адрес IPv4 в этой подсети	

Дано:	
IP-адрес узла	192.168.1.245
Исходная маска подсети	255.255.255.0
Новая маска подсети	255.255.255.252
Найти:	
Количество битов подсети	
Количество созданных подсетей	
Количество битов узлов в подсети	
Количество узлов в подсети	
Сетевой адрес этой подсети	
Адрес IPv4 первого узла в этой подсети	
Адрес IPv4 последнего узла в этой подсети	
Широковещательный адрес IPv4 в этой подсети	

Критерии оценки:

«5» (отлично): выполнены все задания самостоятельной работы без ошибок.

«4» (хорошо): выполнены все задания самостоятельной работы с замечаниями.

«3» (удовлетворительно): выполнены не все задания самостоятельной работы, имеются замечания.

«2» (не зачтено): студент не выполнил или выполнил неправильно задания самостоятельной работы.

Практическая работа 6

Тема: «Основы IP — адресации. Классы сетей и структура адресов»

Цель работы**:** научится решать следующие задачи:

- Идентифицировать 5 различных классов IP-адресов.
- Описывать характеристики и использование классов IP-адресов.
- Определять класс IP-адреса исходя из его значения.
- Определять, какая часть IP-адреса идентифицирует сеть (network ID) и какая – хост (host ID)
- Определять допустимые и недопустимые IP- адреса хостов, исходя из правил адресации
- Определять диапазон адресов и маску подсети по умолчанию для каждого класса адресов

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Ход работы:

Задание 1. Изучить теоретические основы IP-адресации

1. Сколько октетов в IP — адресе?
2. Сколько битов в октете?
3. Сколько бит в маске подсети?
4. В каких диапазонах десятичных и двоичных значений может быть значение первого октета IP-адресов класса «B»? Десятичные: от **128** до **191** Двоичные: от **1000 0000** до **1011 1111**
5. Какие октеты представляют сетевую часть IP-адреса класса «C»

6. Какие октеты представляют часть адреса хоста в IP-адресе класса «А»?

7. Какой из приведенных ниже адресов является примером широковещательного адреса для сети класса B?

	147.1.1.1
	147.255.255.255
	147.13.0.0
	147.14.255.255

8. Заполните таблицу:

Таблица 1 – характеристики классов IP адресации.

Класс адреса	Старшие биты первого	Диапазон дес. значений первого октета	Network / Host ID (N=Network, H=Host)	Маска подсети по умолч.	Количество сетей	Количество хостов (используемых адресов) в сети
A	0	1-126 (Значение 127 зарезервировано для организации внутренней петли устройств, которая используется при тестировании)	N.H.H.H	255.0.0.0	126	16777214
B	10	128-191	N.N.H.H	255.255.0.0	64	65534
C	110	192-223	N.N.N.H	255.255.255.0	32	254

D	1110	224-239	N.H.H.H		Используется для мультикастинга.
E	11110	240-255	N.H.H.H		Зарезервирован для экспериментальных целей.

Задание 2. Определение частей IP- адресов.

Заполнить таблицу об идентификации различных классов IP-адресов.

Таблица 2 – идентификация различных классов IP-адресов

IP-адреса хостов	Класс адреса	Адрес сети	Адреса хостов	Широковещательный (broadcast) адрес	Маска подсети по умолчанию
216.14.55.137					
123.1.1.15					
150.127.221.244					
194.125.35.199					
175.12.239.244					

2. Разбить каждую сеть на две подсети, вычислить диапазон каждой, адрес подсети , подкаст.
3. Дан IP- адрес 142.226.0.15
    1. Чему равен двоичный эквивалент второго октета?
    2. Какому классу принадлежит этот адрес?
    3. Чему равен адрес сети, в которой находится хост с этим адресом?
    4. Является ли этот адрес хоста допустимым в классической схеме адресации

Задание 3

Найти адрес сети, минимальный IP, максимальный IP и число хостов по IP-адресу и маске сети:

IP-адрес: 192.168.215.89

Маска: 255.255.255.0 /24

Задание 4

Что произойдет с данными из 1 задачи, если маску сети изменить на 255.255.255.128

Задание 5

Найти маску сети, минимальный IP, максимальный IP по IP-адресу и адресу сети:

IP-адрес: 124.165.101.45

Сеть: 124.128.0.0

Задание 6

Найти минимальный IP, максимальный IP по адресу сети и маске:

Маска: 255.255.192.0

Сеть: 92.151.0.0

Задание 7

Найти адрес сети, минимальный IP, максимальный IP и число хостов по IP-адресу и маске сети:

IP-адрес: 85.45.5.33

Маска: 255.252.0.0

Практическая работа 7

Тема: Построение схемы компьютерной сети

Цель: построение схемы компьютерной сети с помощью MS Visio 2016.

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Оборудование: ПК, ПО MS Visio 2016

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

Программный продукт Visio

Программный продукт Visio является разработкой компании VisioCorporation, которая была куплена в 2000-м году компанией Microsoft, а программа получила название MicrosoftVisio.

- VisioStandard – служит для создания бизнес-диаграмм, в том числе блок-схем, структурных схем, графиков работ, и др.

- VisioProfessional – средство моделирования и документирования бизнес-процессов, проектирования и построения схем сетей, планов помещений, схематических чертежей, предназначенных для IT-специалистов, инженеров, технических руководителей и разработчиков программного обеспечения.

Расширенные средства создания схем сетей выделены в дополнительный продукт –MicrosoftVisioEnterpriseNetworkTools, который предоставляет возможности автоматического создания схем сетей, документирование структур каталогов ActiveDirectory, и др.

Область применения

Программный продукт MicrosoftVisio (в дальнейшем - MS Visio) в последнее время активно завоевывает рынок, выступая в качестве эталона деловой графики.

Для рисования на компьютере существуют десятки различных приложений. Это и простейшие графические редакторы типа Paint, и профессиональные системы типа CorelDraw. Visio не заменяет существующих, особенно сильно развитых систем. Но в этой ситуации появляется много примеров, когда инженер, использующий скажем AutoCAD, начинает дополнительно применять MS Visio. Кроме того, существуют области, для которых нет специализированных продуктов кроме MS Visio, например, рисование химических структурных диаграмм.

Для IT-специалистов и разработчиков программного обеспечения особый интерес представляют такие функции пакета MS Visio:

- построение планов зданий и инженерных коммуникаций;
- разработка схем компьютерных сетей;
- разработка диаграмм баз данных;
- проектирование карт web-сайтов.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:

Задание 1.

Запустить *MicrosoftVisio* из группы программ *Microsoft Office.*

Запустить и ознакомиться с разделами справочной системы для работы с *MicrosoftVisio*. Открыть интересующий Вас раздел справки и изучить его.

Просмотреть образцы шаблонов схем, доступных для использования. Изучить интерфейс программы.

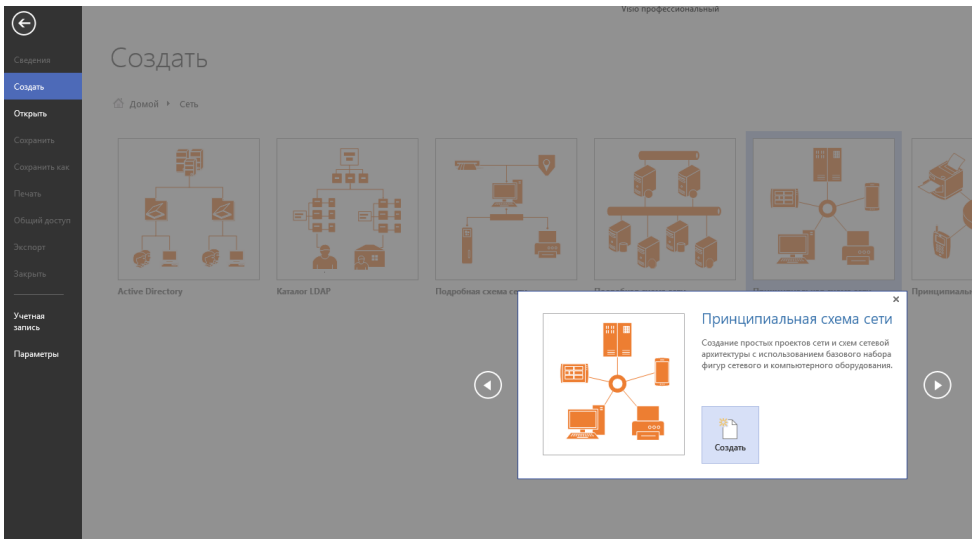
Добавить панели инструментов **Формат текста** и **Формат фигуры (**меню **Вид → Панели инструментов**).

Для добавления необходимой фигуры следует выбрать меню Файл → Фигуры → группа фигур (дополнительные фигуры).

Задание 2.

Программы Visio 2016 включают шаблон схемы сети, который называется Принципиальная схема сети. На основе этого шаблона можно построить схему простой корпоративной сети, что мы и продемонстрируем на примере.

1. Для этого щелкнем на вкладке **Файл** и выберем вкладку **Создать**. Щелкнем на **Категории**, затем на **Сеть** и дважды на миниатюре **Принципиальная схема сети**.



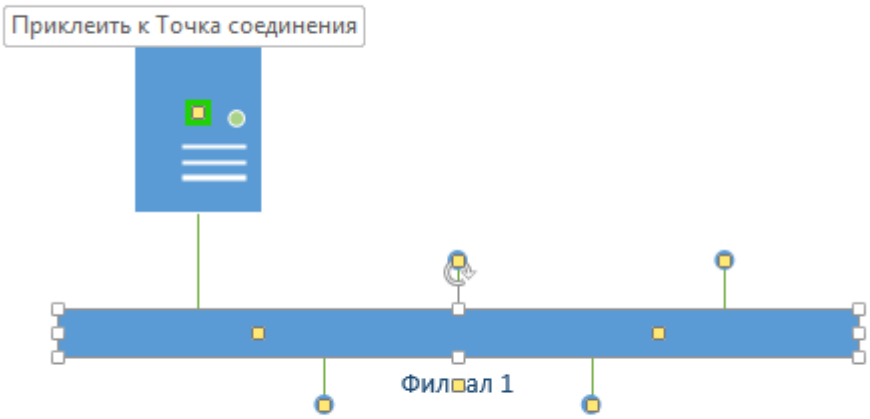
2. Перетащим фигурку **Ethernet** из набора элементов **Сеть и периферийные устройства** на страницу документа и сбросим ее по вертикали по центру чуть правее левого поля страницы.

3. Перетащим маркер изменения размера с правого края фигуры **Ethernet** вправо так, чтобы ее ширина стала 100 мм.

4. Не снимая выделение с фигуры **Ethernet**, введем *Филиал 1* в качестве подписи для сегмента сети, затем щелкнем на любой точке фона страницы.

5. Перетащим фигуру **Сервер** на страницу и поместим ее над фигурой Ethernet ближе к левому краю последней.

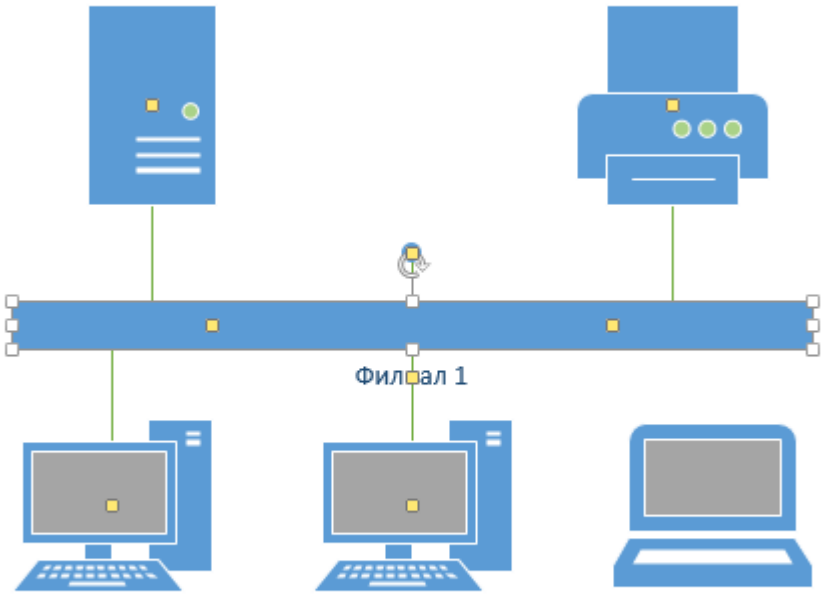
6. Щелкнем один раз на фигуре **Ethernet**, чтобы выделить ее, а затем перетащим любой и желтых управляющих маркеров в центр сервера, пока вокруг управляющего маркера не появится зеленый квадрат.



7. Перетащим фигуру **Принтер** над фигурой **Ethernet** ближе к ее правому краю, а затем соединим принтер с сетью, перетащив и приклеив желтый управляющий маркер к принтеру.

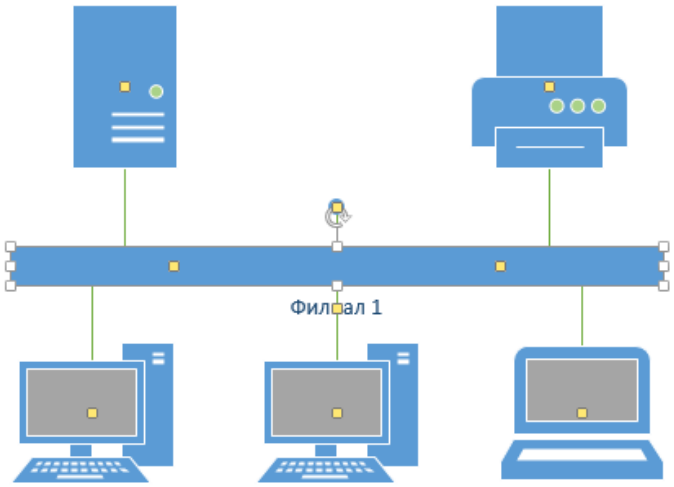
8. Перетащим на страницу две фигуры **ПК** и одну фигуру **Ноутбук** из набора **Компьютеры и мониторы** и сбросим их под фигурой **Ethernet**.

9. Перетащим желтый управляющий маркер к каждой из фигур **ПК**.



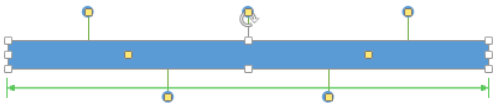
Сейчас только один управляющий маркер остается под фигурой **Ethernet**, но его назначение – перемещение блока текста. А, следовательно, его нельзя использовать для привязки ноутбука к сети.

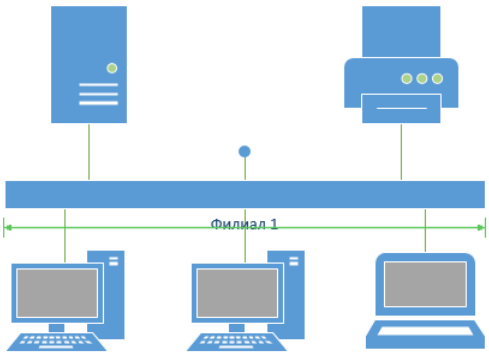
10. Перетащим управляющий маркер из середины фигуры **Ethernet** и приклеим его к ноутбуку. Теперь ноутбук подключен к сегменту **Ethernet**, но все еще доступны дополнительные управляющие маркеры, как показано на рисунке.



11. Перетащим другую фигуру **Ethernet** в верхний правый угол страницы, оставив достаточно места для того, чтобы над ней можно было разместить другие фигуры.

12. Перетащим левый маркер изменения размера влево, чтобы сделать сегмент **Ethernet** шире. Продолжим перетаскивать, пока не появится двунаправленная стрелка, показывая, что новый сегмент сети имеет такую же длину, как и уже существующий на странице.





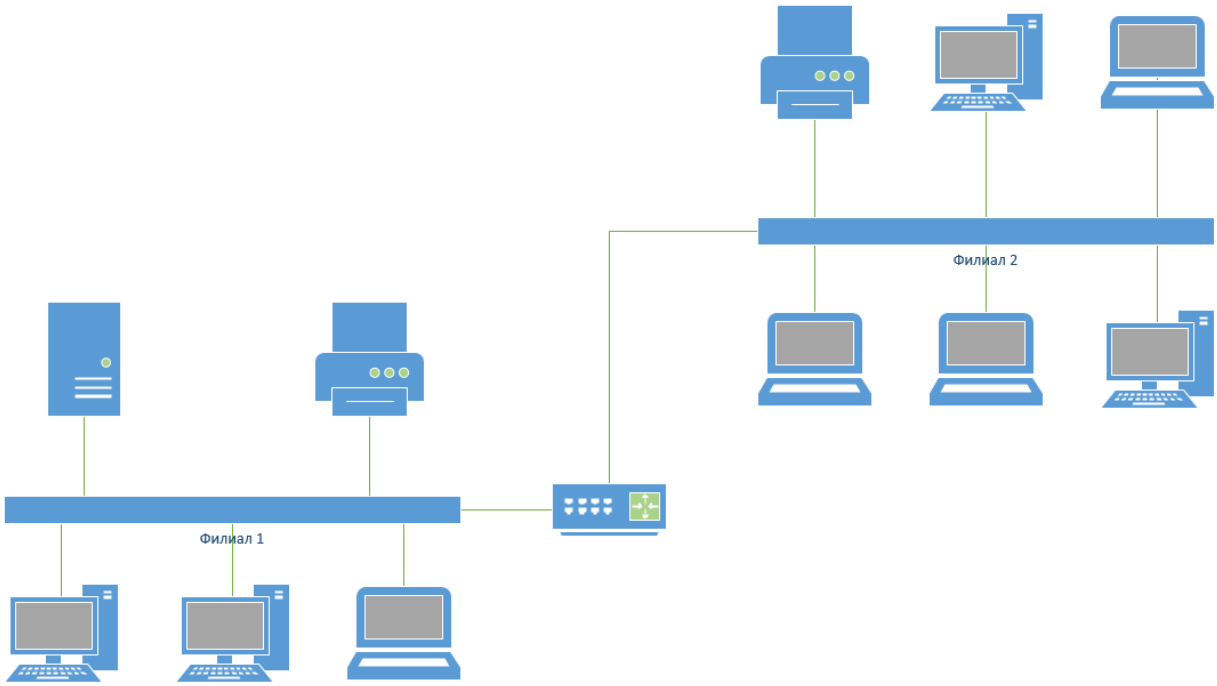
13. Не снимая выделения с фигуры **Ethernet**, введем **Филиал 2** и щелкнем на пустом месте страницы.

14. Перетащим фигуру **Принтер**, две фигуры **ПК** и три фигуры **Ноутбук** и соединим их с новым сегментом сети.

15. Перетащим фигуру **Маршрутизатор** из набора элементов **Сеть и периферийные устройства** и разместим ее по центру страницы.

16. Перетащим оставшийся неиспользованный управляющий маркер из фигуры сети **Филиал 1** и приклеим его к маршрутизатору.

17. Перетащим управляющий маркер из сети **Филиал 2** и приклеим его к маршрутизатору. Соединительная линия изгибается, когда мы перетаскиваем управляющий маркер к маршрутизатору – она ведет себя как динамическая соединительная, а не как простая линия. Получившаяся схема сети представлена на следующем рисунке.



Предоставьте результат работы преподавателю.

Контрольные вопросы:

1. Назначение и возможности *Microsoft Office Visio*.
2. Какие способы настройки окна и панели инструментов программы *MsVisio* вы знаете?
3. Какие группы фигур программы *MsVisio* используются для создания схем и других графических изображений?
4. Какие инструменты для работы с текстом доступны в программе *MsVisio*?

Практическая работа 8

Тема: Изучение маршрутизации IP

Цель: изучить правила адресации сетевого уровня, научиться распределять адреса между участниками сети передачи данных и организовывать маршрутизацию между сегментами сети

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Оборудование: персональный компьютер, включенный в сеть IP, Microsoft Windows

Ход работы:

1. Изучить теоретические сведения

Основные понятия

Сетевой уровень отвечает за возможность доставки пакетов по сети передачи данных – совокупности сегментов сети, объединенных в единую сеть любой сложности посредством узлов связи, в которой имеется возможность достижения из любой точки сети в любую другую.

Архитектуру сетевого уровня удобно рассматривать на примере сетевого протокола IP – самого распространенного в настоящее время, основного протокола сети Интернет. Термин «стек протоколов TCP/IP»

означает «набор протоколов, связанных с IP и TCP(протоколом транспортного уровня)».

Архитектура протоколов TCP/IP предназначена для объединенной сети, состоящей из соединенных друг с другом шлюзами отдельных разнородных пакетных подсетей, к которым подключаются разнородные машины.

Каждая из подсетей работает в соответствии со своими специфическими требованиями и имеет свою природу средств связи.

Однако предполагается, что каждая подсеть может принять пакет информации (данные с соответствующим сетевым заголовком) и доставить его по указанному адресу в этой конкретной подсети. Не требуется, чтобы подсеть гарантировала обязательную доставку пакетов и имела надежный сквозной протокол. Таким образом, две машины, подключенные к одной подсети, могут обмениваться пакетами.

Когда необходимо передать пакет между машинами, подключенными к разным подсетям, то машина-отправитель посылает пакет в соответствующий шлюз (шлюз подключен к подсети также как обычный узел). Шлюз (gateway)– любое сетевое оборудование с несколькими сетевыми интерфейсами и осуществляющее продвижение пакетов между сетями на уровне протоколов сетевого уровня.

Из шлюза пакет направляется по определенному маршруту через систему шлюзов и подсетей, пока не достигнет шлюза, подключенного к той же подсети, что и машина-получатель; там пакет направляется к получателю.

Таким образом, шлюз выполняет маршрутизацию – процедуру нахождения в структуре сети пути достижения получателя (построение пути доставки пакетов).

Если хост подключен к нескольким сетям, он должен иметь несколько сетевых адресов, как минимум столько, сколько каналов к нему подключено.

Даже если хост не является шлюзом между подсетями, все равно в нем присутствует таблица маршрутизации, ведь любой хост должен отправлять пакеты напрямую членам своей подсети, через какой-то шлюз другим подсетям и не передавать в сеть пакеты, предназначенные самому себе (заворачивать их по внутренней петле 127.0.0.1).

Правила маршрутизации

Правила маршрутизации определяют куда и как должны посылаться пакеты для разных сетей.

Каждое правило состоит из следующих компонентов:

- Начальный адрес подсети, порядок достижения которой описывает правило.
- Маска подсети, которую описывает правило.
- Шлюз показывает, на какой адрес будут посланы пакеты, идущие в сеть назначения. Если пакеты будут идти напрямую, то указывается собственный адрес (точнее тот адрес того канала, через который будут передаваться пакеты).
- Интерфейс показывает через какой сетевой адаптер (его номер или IPадрес) должен посылаться пакет в заданную сеть;
- Метрика показывает время за которое пакет может достигнуть сети получателя (величина условная и может быть изменена при маршрутизации). Если имеется несколько правил достижения одной сети, пакеты посылаются по правилу с наименьшей метрикой.

Применение правила заключается в определении, принадлежит ли хост назначения сети, указанной в правиле, и если принадлежит, то пакет отправляется на адрес шлюза через интерфейс.

Правила маршрутизации сведены в таблицу маршрутизации (где расположены по степени уменьшения маски), которую можно посмотреть с помощью команды ROUTE PRINT.

Правила применяются в порядке уменьшения масок.

Правила с равными масками применяются в порядке увеличения метрики.

Пример таблицы маршрутизации

Рассмотрим таблицу маршрутизации, имеющую следующий вид:

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
0.0.0.0	0.0.0.0	192.168.200.1	192.168.200.47	30
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.192.0	255.255.240.0	192.168.200.47	192.168.200.47	30
192.168.200.47	255.255.255.255	127.0.0.1	127.0.0.1	30
192.168.200.255	255.255.255.255	192.168.200.47	192.168.200.47	30
224.0.0.0	240.0.0.0	192.168.200.47	192.168.200.47	30
255.255.255.255	255.255.255.255	192.168.200.47	192.168.200.47	1

Проанализируем вышеприведенную таблицу маршрутизации, пересортировав правила:

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика

255.255.255.255	255.255.255.255	192.168.200.47	192.168.200.47	1
192.168.200.47	255.255.255.255	127.0.0.1	127.0.0.1	30
192.168.200.255	255.255.255.255	192.168.200.47	192.168.200.47	30
192.168.192.0	255.255.240.0	192.168.200.47	192.168.200.47	30
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
224.0.0.0	240.0.0.0	192.168.200.47	192.168.200.47	30
0.0.0.0	0.0.0.0	192.168.200.1	192.168.200.47	30

255.255.255.255	255.255.255.255	192.168.200.47	192.168.200.47	1

Обратите внимание на маску сети в первом правиле. Она описывает подсеть размером в 1 хост с адресом 255.255.255.255 – это широковещательный адрес. Пакеты будут посылаться на адрес 192.168.200.47 через интерфейс 192.168.200.47. Это наш адрес, т.е. пакеты будут отправляться напрямую.

192.168.200.255	255.255.255.255	192.168.200.47	192.168.200.47	30

Опять широковещательный адрес. Смотри предыдущий комментарий.

192.168.200.47	255.255.255.255	127.0.0.1	127.0.0.1	30

Опять такая же маска, но адрес нашего хоста. Отправлять будем через внутреннюю петлю.

192.168.192.0	255.255.240.0	192.168.200.47	192.168.200.47	30

А вот и наша подсеть. Отправляем напрямую.

127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1

Все, что начинается со 127, отправляем через внутреннюю петлю.

224.0.0.0	240.0.0.0	192.168.200.47	192.168.200.47	30

Класс D – отправляем напрямую.

0.0.0.0	0.0.0.0	192.168.200.1	192.168.200.47	30

Самое интересное правило. Маска покрывает ВСЕ возможные адреса! Пакеты отправляются через наш интерфейс на адрес 192.168.200.1. Правило применяется последним, поэтому его можно озвучить так: по всем адресам, которые не подошли по предыдущим правилам, пакеты отправляем на адрес 192.168.200.1. Такой адрес обычно имеется в любой сети и называется шлюзом по умолчанию (default gateway). Этот адрес скрывает от хостов и пользователей структуру сети и позволяет упростить таблицы маршрутизации и снять нагрузку с хостов, перенеся маршрутизацию на специально выделенные шлюзы – маршрутизаторы.

Нетрудно догадаться, что все адреса в колонке Адрес шлюза должны достигаться напрямую, т.е. входить в нашу подсеть.

Разбиение сети на подсети

Одной из основных задач, стоящих при проектировании сетей, является распределение по подсетям сетевых адресов из заданного диапазона, т.е. разделение сети на подсети.

При разделении сети на подсети следует учитывать следующие правила:

- Размер подсетей должен быть степенью двойки.
- Имеются запрещенные адреса.
- Начальный адрес подсети должен быть кратен ее размеру.

В качестве шлюза по умолчанию можно использовать любой узел, но, исходя из увеличения пропускной способности сети и уменьшения времени передачи пакетов, следует в качестве шлюза по умолчанию использовать либо ближайший узел, либо узел, соединенный с максимальным количеством сетей, т.е. следует учитывать топологию сети.

Программа ROUTE

Для работы с таблицами маршрутизации в составе ОС имеется программа route (упоминалась ранее). Выводит на экран и изменяет записи в локальной таблице IP-маршрутизации.

route [-f] [-p] [команда [конечная_точка] [mask маска_сети] [шлюз] [metric метрика]] [if интерфейс]]

Параметры:

-f – Очищает таблицу маршрутизации от всех записей, которые не являются узловыми маршрутами (маршруты с маской подсети 255.255.255.255), сетевым маршрутом замыкания на себя (маршруты с конечной точкой 127.0.0.0 и маской подсети 255.0.0.0) или маршрутом многоадресной рассылки (маршруты с конечной точкой 224.0.0.0 и маской подсети 240.0.0.0). При использовании данного параметра совместно с одной из команд (таких, как add, change или delete) таблица очищается перед выполнением команды.

-p – При использовании данного параметра с командой add указанный маршрут добавляется в реестр и используется для инициализации таблицы IP-маршрутизации каждый раз при запуске протокола TCP/IP. При использовании параметра с командой print выводит на экран список постоянных маршрутов. Все другие команды игнорируют этот параметр.

команда – Указывает команду, которая будет запущена на удаленной системе. В следующей таблице представлен список допустимых параметров.

Команда	Назначение
Add	Добавление маршрута
change	Изменение существующего маршрута
Delete	Удаление маршрута или маршрутов
Print	Печать маршрута или маршрутов

конечная_точка – Определяет конечную точку маршрута. Конечной точкой может быть сетевой IP-адрес (где разряды узла в сетевом адресе имеют значение 0), IP-адрес маршрута к узлу, или значение 0.0.0.0 для маршрута по умолчанию.

mask маска_сети – Указывает маску сети в соответствии с точкой назначения. Маска сети может быть маской подсети соответствующей сетевому

шлюз – Указывает IP-адрес пересылки или следующего перехода, по которому доступен набор адресов, определенный конечной точкой и маской подсети

metric метрика – Задает целочисленную метрику стоимости маршрута (в пределах от 1 до 9999) для маршрута, которая используется при выборе в таблице маршрутизации одного из нескольких маршрутов, наиболее близко соответствующего адресу назначения пересылаемого пакета.

if интерфейс – Указывает индекс интерфейса, через который доступна точка назначения. В случае, когда параметр if пропущен, интерфейс определяется из адреса шлюза.

/? – Отображает справку в командной строке.

2. **Выполнить задания**
3. С помощью программы route print посмотрите таблицу маршрутизации Вашего компьютера. Объясните все правила.
4. Посмотрите таблицу маршрутизации хоста, имеющего несколько каналов. Объясните все правила.
5. Посмотрите таблицу маршрутизации маршрутизатора. Объясните все правила.
6. Добавьте новое правило в таблицу маршрутизации для сети 192.168.0.0/24 через шлюз в вашей сети с последним байтом в адресе 125 и метрикой 12.
7. Удалите это правило.
8. В соответствии с таблицей и схемами выполните задание на распределение адресов по подсетям (согласно варианта). Постройте таблицы маршрутизации для всех шлюзов и для одного хоста для каждого сегмента.

№ Варианта	Количество хостов в подсети					Диапазон адресов	
	A	B	C	D	E	от	до
1	5	10	20	15	50	10.0.20.0	10.0.20.255
2	20	15	6	70	25	192.168.0.0	192.168.0.255

3	15	25	5	40	5	112.38.25.128	112.38.25.255
4	24	32	8	10	2	196.13.49.0	196.13.49.128
5	50	16	64	20	15	68.76.115.0	68.76.115.255
6	40	6	10	12	5	211.3.45.0	211.3.45.128

7. Разделите сеть, состоящую из трех сегментов, имеющую диапазон адресов 192.168.0.32 – 192.168.0.159 на подсети, содержащие 64, 20 и 44 хостов (включая шлюзы).

Практическая работа 9

Тема: «Сетевые утилиты ОС Windows»

Цель**:** изучить утилиты командной строки Windows, предназначенные для контроля и мониторинга сетей, построенных на базе стека протоколов TCP/IP.

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Оборудование: персональный компьютер, Windows с установленной сетью IP

Сетевая операционная система Windows содержит набор утилит, полезных при диагностике сети. Основными задачами этих программ является:

Определение работоспособности сети

Определение параметров и характеристик сети

В случае неправильного функционирования сети – локализация службы или сервиса, вызывающих неисправность.

Главными параметрами сетевых подключений являются их канальные и сетевые адреса и параметры, влияющие на работу сетевого уровня.

Единственным параметром канального уровня, который может быть просмотрен, являются MAC адреса сетевых адаптеров. Для их просмотра можно воспользоваться утилитой IPCONFIG, которая покажет MAC адреса для каждого адаптера, или, для последних версий Windows, с помощью ROUTE PRINT. Для изменения MAC адресов следует воспользоваться драйверами соответствующих сетевых адаптеров, если, конечно, они допускают подобную операцию.

1. IPCONFIG

Параметры IP просматривают с помощью утилиты IPCONFIG.

Использование:

ipconfig [/? | /all | /release [адаптер] | /renew [адаптер] |

/flushdns | /displaydns /registerdns |

/showclassid адаптер |

/setclassid адаптер [устанавливаемый_код_класса_dhcp]]

Параметры:

адаптер – полное имя или имя, содержащие подстановочные знаки «*» и «?» (* – любое количество знаков, ? – один любой знак). См. примеры

ключи:

/? – отобразить это справочное сообщение.

/all – отобразить полную информацию о настройке параметров.

/release – освободить IP–адрес для указанного адаптера.

/renew – обновить IP–адрес для указанного адаптера.

/flushdns– очистить кэш разрешений DNS.

/registerdns – обновить все DHCP–аренды и перерегистрировать DNS–имена

/displaydns – отобразить содержимое кэша разрешений DNS.

/showclassid – отобразить все допустимые для этого адаптера коды (IDs)
DHCP–классов.

/setclassid – изменить код (ID) DHCP–класса.

По умолчанию отображается только IP–адрес, маска подсети и стандартный шлюз для каждого подключенного адаптера, для которого выполнена привязка с TCP/IP.

Для ключей /release и /renew, если не указано имя адаптера, то будет освобожден или обновлен IP–адрес, выданный для всех адаптеров, для которых существуют привязки с TCP/IP.

Для ключа /setclassid, если не указан код класса (ID), то существующий код класса будет удален.

Примеры:

ipconfig – отображает краткую информацию.

Настройка протокола IP для Windows

Подключение по локальной сети 2 – Ethernet адаптер:

DNS–суффикс этого подключения . . :

IP–адрес автонастройки. . . . . : 169.254.236.138

Маска подсети . . . . . : 255.255.0.0

Основной шлюз . . . . . :

Main – PPP адаптер:

DNS–суффикс этого подключения . . :

IP–адрес. . . . . : 82.209.222.238

Маска подсети . . . . . : 255.255.255.255

Основной шлюз . . . . . : 82.209.222.238

ipconfig /all – отображает полную информацию.

Настройка протокола IP для Windows

Имя компьютера. . . . . : home

Основной DNS–суффикс. . . . . :

Тип узла. . . . . : неизвестный

IP–маршрутизация включена . . . . : нет

WINS–прокси включен . . . . . : нет

Подключение по локальной сети 2 – Ethernet адаптер:

DNS–суффикс этого подключения . . :

Описание. . . . . : Realtek RTL8029(AS)–based

Ethernet адаптер (Универсальный) #2

Физический адрес. . . . . : 52–54–05–E2–77–88

Dhcp включен. . . . . : да

Автонастройка включена. . . . . : да

IP–адрес автонастройки. . . . . : 169.254.236.138

Маска подсети . . . . . : 255.255.0.0

Основной шлюз . . . . . :

Main – PPP адаптер:

DNS–суффикс этого подключения . . :

Описание. . . . . : WAN (PPP/SLIP) Interface

Физический адрес. . . . . : 00–53–45–00–00–00

Dhcp включен. . . . . : нет

IP–адрес. . . . . : 82.209.222.238

Маска подсети . . . . . : 255.255.255.255

Основной шлюз . . . . . : 82.209.222.238

DNS–серверы . . . . . : 194.158.206.206

193.232.248.2

NetBIOS через TCP/IP. . . . . : отключен

ipconfig /renew– обновляет сведения для всех адаптеров.

ipconfig /renew EL* – обновляет сведения для адаптеров, начинающихся с EL

ipconfig /release *ELINK?21* – освобождает IP–адреса для всех адаптеров, имена которых удовлетворяют запросу: ELINK–21 или myELELINKi21adapter и т.п.

2 ARP

Соответствие MAC и IP адресов производится службой ARP. Для работы с этой службой имеется утилита ARP.

Служба ARP работает с таблицей ARP, состоящей из двух колонок: IP адрес и MAC адрес (физический адрес). При необходимости отправить пакет по какому–то IP адресу в таблице ARP находят соответствующий ему MAC адрес и на канальном уровне передают информацию. Если передача производится через шлюз, то в таблице ищут MAC адрес шлюза и передают пакет с IP адресом получателя и MAC адресом шлюза.

Если в таблице ARP нет нужного IP адреса, то посылается запрос – специальный пакет ARP по IP адресу получателя с широковещательным MAC адресом. Получатель, получив такой пакет,

посылает ответ от своего IP адреса и своего MAC адреса. Отправитель, получив этот ответ, добавляет запись в ARP таблицу.

Таблица ARP динамическая, поэтому запись в ней «живет» некоторое время, после которого удаляется, но имеется возможность создавать в таблице и постоянные (статические) записи.

Отображение и изменение таблиц преобразования IP–адресов в физические, используемые протоколом разрешения адресов (ARP).

Использование:

ARP –s inet_addr eth_addr [if_addr]

ARP –d inet_addr [if_addr]

ARP –a [inet_addr] [–N if_addr]

Параметры:

–a – отображает текущие ARP–записи, опрашивая текущие данные протокола. Если задан inet_addr, то будут отображены IP и и физический адреса только для заданного компьютера. Если более одного сетевого интерфейса используют ARP, то будут отображаться записи для каждой таблицы.

–g – то же, что и ключ –a.

inet_addr – определяет IP–адрес.

–N if_addr – отображает ARP–записи для заданного в if_addr сетевого интерфейса.

–d – удаляет узел, задаваемый inet_addr. inet_addr может содержать символ шаблона * для удаления всех узлов.

–s – добавляет узел и связывает internet адрес inet_addr с физическим адресом eth_addr. Физический адрес задается 6 байтами (в шестнадцатеричном виде), разделенных дефисом. Эта связь является постоянной.

eth_addr – определяет физический адрес.

if_addr – если параметр задан – он определяет интернет адрес интерфейса, чья таблица преобразования адресов должна измениться. Если не задан – будет использован первый доступный интерфейс.

Пример:

arp –s 157.55.85.212 00–aa–00–62–c6–09 – добавляет статическую запись.

arp –a – выводит ARP–таблицу.

3 Протокол ICMP

Для мониторинга и управления сетями передачи данных разработан и используется протокол ICMP. На его базе можно:

1. Проверить доступность адресов сети
2. Определить маршрут
3. Определить время достижения пакетами узлов сети.

Решается это посылкой специальных пакетов.

Опции маршрутизации и временных меток являются весьма интересными, так как они обеспечивают способ наблюдения или управления тем, как межсетевые шлюзы маршрутизируют дейтаграммы.

Опция запись маршрута позволяет источнику создать пустой список IP–адресов и заставить каждый шлюз, обрабатывающий дейтаграмму, добавлять свой IP–адрес к этому списку. Всякий раз, когда машина обрабатывает дейтаграмму, имеющую опцию записи маршрута, она добавляет свой адрес к списку записи маршрута (в опции должно быть выделено достаточно места исходным отправителем для того, чтобы поместились все нужные элементы).

При прибытии дейтаграммы машина–получатель должна выделить и обработать список IP–адресов.

Если получатель обрабатывает дейтаграмму обычным образом, он будет игнорировать записанный путь.

Отметим, что отправитель должен разрешить наличие опции записи маршрута, а получатель должен быть согласен обработать полученный список; сама по себе машина не получит автоматически информацию о пройденном пути автоматически, если она включит опцию записи маршрута.

Опция временных меток работает аналогично опции записи маршрута в том отношении, что опция временных меток содержит вначале пустой список, а каждый шлюз на всем протяжении пути от источника к назначению заполняет элемент в этом списке.

Каждый элемент в списке состоит из двух 32–битных частей: IP–адреса шлюза, заполнившего этот элемент, и 32–битового целого числа – временной метки.

Временные метки определяют время и дату, когда шлюз обрабатывал дейтаграмму, и выражаются в миллисекундах после полуночи по Гринвичу. Если стандартное представление времени невозможно, шлюз может использовать любое представление локального времени.

4 TRACERT

Для оценки маршрута прохождения пакетов используют утилиту TRACERT (trace route)

В отличие от PING на пробные пакеты постоянного размера отвечает каждый узел, через который этот пакет проходит. Программа измеряет и показывает время между отправкой пакета и получением ответа.

Использование:

tracert [–d] [–h максЧисло] [–j списокУзлов] [–w интервал] имя

Параметры:

–d – без разрешения в имена узлов.

–h максЧисло – максимальное число прыжков при поиске узла.

–j списокУзлов – свободный выбор маршрута по списку узлов.

–w интервал – интервал ожидания каждого ответа в миллисекундах.

Примеры:

tracert www.lycos.com

Трассировка маршрута к mia–search.mia.lycos.com [209.202.248.101]
с максимальным числом прыжков 30:

1 136 ms 149 ms 149 ms194.158.206.83

2 136 ms 209 ms 139 ms194.158.206.197

3 164 ms 149 ms 149 ms193.232.249.18

4 132 ms 149 ms 219 ms193.232.248.128

5 160 ms 149 ms 169 ms80.77.105.197

6 158 ms 149 ms 149 mssl–bb21–sto–8–0.sprintlink.net [80.77.96.41]

7 185 ms 159 ms 189 mssl–bb21–cop–12–0.sprintlink.net
[213.206.129.33]

8 163 ms 159 ms 189 mssl–bb20–cop–15–0.sprintlink.net [80.77.64.33]

9 270 ms 269 ms 229 mssl–bb21–msq–10–0.sprintlink.net
[144.232.19.29]

10 257 ms 249 ms 259 mssl–bb20–msq–15–0.sprintlink.net
[144.232.9.109]

11 235 ms 249 ms 249 mssl–bb25–nyc–6–0.sprintlink.net
[144.232.20.75]

12 232 ms 239 ms 252 mssl–bb21–nyc–15–0.sprintlink.net
[144.232.13.2]

13 239 ms 239 ms 299 mssl–bb23–nyc–3–0.sprintlink.net
[144.232.7.109]

14 246 ms 239 ms 339 mssl–gw31–nyc–0–0.sprintlink.net
[144.232.13.32]

15 244 ms 249 ms 259 mssl–tiws–2–0.sprintlink.net [144.232.230.2]

16 296 ms 319 ms 279 msSo7–2–0–0–grtmiabr4.red.telefonica–wholesale.net[213.140.38.254]

17 296 ms 289 ms 299 msSo2–0–0–0–grtmiana2.red.telefonica–wholesale.net[213.140.36.89]

18 274 ms 289 ms 299 msteusa–7–3–0–0–grtmiana2.red.telefonica–wholesale.net[213.140.39.50]

19 271 ms 298 ms 299 ms66.119.71.166

20 283 ms 319 ms 279 msmia–search.mia.lycos.com [209.202.248.101]

Трассировка завершена.

TRACERT позволяет обнаружить некоторые ошибки маршрутизации в сети. Такими ошибками являются отсутствие правила маршрутизации в каком либо шлюзе, или петля маршрутов по умолчанию.

Пример отсутствия правила на узле:

tracert 10.249.0.100

Трассировка маршрута к 10.249.0.100

с максимальным числом прыжков 30:

1 13 ms 14 ms 14 ms10.7.11.11

2 * * *Сеть недоступна [10.7.11.11]

Трассировка завершена.

Пример петли маршрутизации:

tracert 10.250.0.100

Трассировка маршрута к 10.250.0.100

с максимальным числом прыжков 30:

1 13 ms 14 ms 14 ms10.7.11.11

2 18 ms 17 ms 17 ms10.7.10.11

3 19 ms 18 ms 24 ms10.7.11.11

4 28 ms 14 ms 19 ms10.7.10.11

5 23 ms 14 ms 22 ms10.7.11.11

6 19 ms 16 ms 33 ms10.7.10.11

…

Хорошо видно, что шлюз 10.7.11.11 посылает пакет на 10.7.10.11, а 10.7.11.11 на 10.7.10.11. Это возможно, если либо для сети, к которой принадлежит адрес 10.250.0.100 неправильно прописаны правила маршрутизации, либо неправильно прописана маршрутизация по умолчанию на одном или обоих узлах.

5 NSLOOKUP

Имеется специальная служба, сопоставляющая доменные адреса Интернет с IP адресами – DNS (domain name service). Для проверки ее работоспособности используют утилиту NSLOOKUP. Для работы этой утилиты должен быть определен сервер DNS в параметрах IP компьютера. С его помощью и будет производиться распознавание имен.

Использование:

nslookup [–подкоманда …] [{искомый_компьютер| [–сервер]}]

Параметры:

–подкоманда … – задает одну или несколько подкоманд nslookup как параметры командной строки.

искомый_компьютер – ищет данные для параметра искомый_компьютер, используя текущий, заданный по умолчанию сервер имен DNS, если никакого другого сервера не указано

–сервер – указывает, что данный сервер следует использовать в качестве сервера имен DNS. Если параметр –сервер не указан, используется сервер DNS, заданный по умолчанию.

–help|? – Выводит краткое описание подкоманд nslookup.

Пример:

nslookup

Default Server:mail.mogilev.by

Address:194.158.206.206

> lycos.com

Server:mail.mogilev.by

Address:194.158.206.206

Non–authoritative answer:

Name:lycos.com

Address:209.202.248.101

> hp.com

Server:mail.mogilev.by

Address:194.158.206.206

DNS request timed out.

timeout was 2 seconds.

Non–authoritative answer:

Name:hp.com

Addresses:192.6.234.8, 192.6.234.9, 192.6.234.10, 192.151.52.187
161.114.22.105

> bru.mogilev.by
Server:mail.mogilev.by
Address:194.158.206.206

Name:bru.mogilev.by
Address:82.209.221.110

> exit

Задания для выполнения

1. Используя утилиту PING определить пропускную способность сети до адресов 192.168.0.1, 192.168.0.201, 192.168.0.254, 192.168.1.1. Объясните разницу в результатах.

2. Используя утилиту TRACERT и таблицу маршрутизации (адрес server.af), постройте схему сеть филиала.

3. Передайте пакеты участникам сети напрямую и через шлюз. Объясните полученные записи в таблице ARP.

4. Определите IP адреса
www.microsoft.com, www.hp.com, www.tut.by, ftp.cdrom.ru при помощи утилиты NSLOOKUP.

Практическая работа 10

Тема: Изучение протоколов высших уровней модели OSI

Цель: ознакомиться с принципами работы текстовых протоколов высших уровней на примере протоколов электронной почты.

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Оборудование: персональный компьютер, включенный в сеть; Microsoft Windows; утилита TELNET; сервер электронной почты в сети

Ход работы: изучить теоретические сведения**.**

Основные понятия

Большинство протоколов высших уровней – текстовые – запросы и ответы передаются в виде текста, т.е. в запросах и ответах могут присутствовать только печатные символы.

Во многих протоколах ответы начинаются со специальной строки, состоящей из трехзначного числа и, возможно, текстового описания типа ответа. Трехзначное число разделяется на две части: 1-ый символ рассматривается как код класса сообщения; два последние – как тип сообщения данной важности.

Коды классов следующие:

1 – информационное сообщение. Обычно игнорируется программными клиентами.

2 – удачное завершение запроса. Рассматривается программами-клиентами как успех обработки запроса и обычно игнорируется.

Часто программы-серверы не различают сообщения первого и второго типа, т.е. информационное сообщение проходит по второй категории.

3 – сообщение об удачной обработке запроса, но требующее дополнительных действий клиента.

4 – ошибка со стороны клиента, т.е. клиент послал запрос, который не может обработать сервер вследствие ошибочности или недостаточности данных.

5 – ошибка со стороны сервера. Клиент послал правильный запрос, но сервер не смог его выполнить в силу каких-то причин.

Трехзначные коды ответов очень удобны для программного распознавания, нет необходимости распознавать текст ответа, который, в общем случае, может прийти на разных языках, достаточно распознать только 3 цифры.

Программа TELNET

Для работы с текстовыми протоколами воспользуемся программой TELNET, входящей в состав Windows. Эта программа предназначена для работы с протоколом TELNET, задачей которого является обмен информацией между клиентом и сервером без каких либо преобразований, т.е. организация прозрачного канала между клиентом и сервером.

Синтаксис команды TELNET следующий:

TELNET адрес_сервера [порт]

Если порт не указан, используется 23 — стандартный порт протокола TELNET.

Протокол SMTP

Для начала попробуем поработать с протоколом SMTP. Обычно он работает, используя порт 25.

Для наглядности команды пользователя выделены красным цветом, а ответы сервера – синим.

Даем команду на подключение:

telnet 192.168.200.1 25

Получаем ответ

220 home VPOP3 SMTP Server Ready

Работает! Обратите внимание на число 220 в начале строки ответа. Это нормальный ответ, сервер ответил на наш запрос на подключение.

Многие серверы, работающие по текстовым протоколам, поддерживают команду HELP. Проверим.

Help

Дадим серверу неправильный запрос

abrakadabra

500 Command Unrecognised

Как ни странно, но код ответа 5 – ошибка на стороне сервера!

Попробуем написать письмо

Поздороваемся J

helo home

250 home VPOP3 SMTP Server — Hello home, pleased to meet you

Укажем отправителя письма

mail from: user1

250 <user1>… Sender ok

Укажем получателя письма

rcpt to: user2

250 <user2>… Recipient ok

Перейдем в режим ввода письма

data

354 Start Mail input, end with <CRLF>.<CRLF>

Обратите внимание на код ответа 354.

Это нормальное завершение, но требуются дополнительные данные – само письмо, которое, как видно, должно заканчиваться строкой, состоящей из одной точки «.».

А теперь само письмо. Формат письма описан стандартами. Их изучение не входит в нашу задачу, но наиболее важные служебные строки вкратце рассмотрим:

Date: Tue, 22 Nov 2005 19:55:07 +0200

Дата создания по GMT и часовой пояс

From: User user1@home.my

От кого

Reply-To: User user1@home.my

Кому отвечать

To: user2@home.my

Кому

Subject: Test

Тема письма

MIME-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

Информация почтовой программе, как закодировано письмо – с помощью этих строк почтовая программа клиент сможет реализовать шестой уровень – представить информацию пользователю в читабельном виде

Hello user2,

It’s a test message.

Best regards,

User mailto:user1@home.my

Само письмо

.

250 OK

Письмо принято!

Теперь выходим

quit

221 home VPOP3 Server Closing Connection

Протокол SMTP (Simple Mail Transfer Protocol) используется для передачи электронной почты от клиента серверу или между серверами. Не содержит встроенных средств идентификации и преобразования.

Протокол POP3

Теперь поработаем с протоколом POP3. Обычно он работает, используя порт 110.

Даем команду на подключение:

telnet 192.168.200.1 25

Получаем ответ

+OK VPOP3 Server Ready <1.7b0.435a37>

Работает, но трехсимвольного кода ответа нет!

Попробуем help

help

-ERR Unrecognised command

Видим, что помощи нет, заодно и посмотрели, как сервер отвечает на ошибочный для него запрос.

Как мы знаем, POP3 требует аутентификации, поэтому представимся:

user user2

+OK User Accepted, PASSword required

А теперь пароль.

pass 2

+OK user2 has 1 message(s) (580 octets)

Нам есть почта! Посмотрим.

list

+OK 1 messages (580 octets)

1 580

.

Одно письмо 580 символов. Если бы было несколько писем, было бы несколько строк с указанием номеров и размеров писем. Точка в последней строке показывает, что это окончание ответа.

Теперь прочитаем (получим) первое письмо.

retr 1

+OK 580 octets

Received: from 192.168.200.1 by home ([192.168.200.1] running VPOP3) with SMTP

or <user2>; Tue, 22 Nov 2005 20:31:07 +0200

Date: Tue, 22 Nov 2005 19:55:07 +0200

From: User <user1@home.my>

Reply-To: User <user1@home.my>

To: user2@home.my

Subject: Test

MIME-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

Message-Id: <VPOP31.3.0c.20051122203134.814.e.1.40132205@home>

X-Server: VPOP3 V1.3.0c — Registered to: Collega

Hello user2,

It’s a test message.

Best regards,

User mailto:user1@home.my

.

Служебных полей стало больше – их добавил сервер.

Обратите внимание на последнюю строку ответа

Теперь удалим письмо с сервера, ведь оно уже прочитано:

dele 1

+OK message 1 deleted

Проверим, есть ли что еще

list

+OK 0 messages (0 octets)

.

Ничего нет. А можно и так, для программы это будет более удобным

list 1

-ERR Invalid Message Number

Ну, и теперь выходим

quit

+OK VPOP3 Server Closing Connection

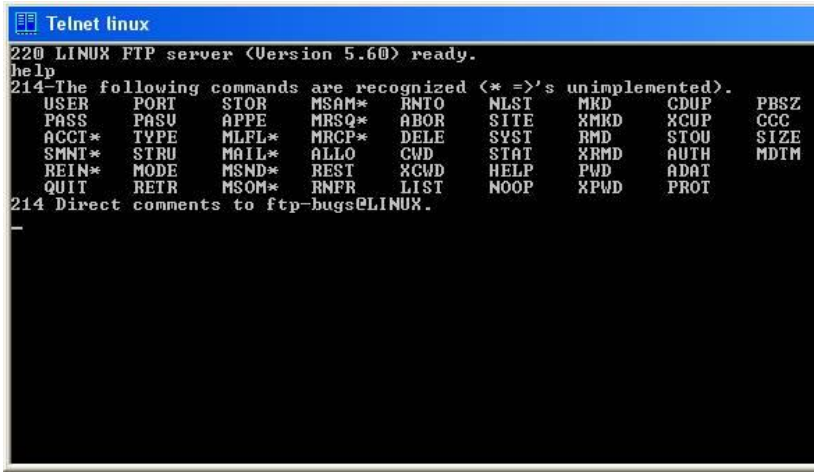
В приведенном выше примере было отправлено письмо от пользователя «user1» пользователю «user2» и получена почта пользователя «user2» с помощью утилиты TELNET, т.е. без использования почтового клиента.

Протокол POP3 (Post Office Protocol) предназначен для получения электронной почты от сервера к клиенту. Содержит средства идентификации клиента, использует факультативные средства преобразования.

Протокол FTP

Протокол FTP (File Transfer Protocol) – протокол передачи файлов.

Он использует 20-ый порт для установления соединений и 21-ый порт для установления соединений и передачи файлов. Этот протокол содержит встроенные средства идентификации клиента. Все распознаваемые им команды состоят из 3-х или 4-х символов, являющихся сокращениями или аббревиатурами выполняемых действий.



Протокол HTTP

Протокол HTTP (Hyper Text Transfer Protocol) – протокол передачи гипертекста, т.е. данных разного представления (текст, изображения, видео, звук). Обычно этот протокол работает на 80-ом порту. Он содержит средства идентификации и перекодирования передаваемой информации.

Как видим работа с текстовыми протоколами не представляет особых трудностей. Правда некоторые протоколы содержат большое число команд и чтобы узнать их формат требуется использовать их стандарт и описания RFC.

2. Выполнить задания:

Во всех заданиях адрес сервера: 10.203.0.120.

Где необходимо требуется пояснить трехсимвольные коды ответов, например, при первом появлении такого кода.

В пятом и шестом заданиях, после аутентификации (если она необходима) рекомендуется в первую очередь вызвать помощь командой help и посмотреть информацию о других командах, поддерживаемых данным протоколом.

1. Получить у преподавателя адрес сервера электронной почты, имена и пароли пользователей. Отправить и получить почту без использования почтового клиента (для аутентификации использовать имя пользователя типа: user№, тогда паролем будет №, в качестве номера № использовать номер Вашей подгруппы).
2. Поработать с POP3 без аутентификации. Сделать соответствующие выводы.
3. Определить, является ли протокол FTPтекст-ориентированным и поддерживает ли он трехсимвольные коды ответов. Подтвердить и объяснить полученные результаты.
4. Подключиться к HTTPсерверу и определить, является ли протокол HTTP текст-ориентированным и поддерживает ли он трехсимвольные коды ответов. Подтвердить и объяснить полученные результаты.
5. Получить у преподавателя адрес и порт неизвестного для вас протокола и сервера. Получите список его команд, объясните, что делает каждая команда. Попробовать некоторые из них и проанализировать результаты. (использовать 1000-ый порт, при аутентификации имя пользователя и пароль: admin).
6. Поработайте с FTP-сервером с помощью TELNETи программы FTP. Объясните и подтвердите на конкретном примере разницу между ними (при аутентификации имя пользователя: anonymous и пароль: a). Для запуска

программы FTP в командной строке вызвать ftp>open (узел) 10.203.0.120)

Практическая работа 11

Тема: Работа в сети с использованием визуальных средств ОС и командной строки

Цель: научиться работе в сети с использованием встроенных визуальных средств Windows

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Оборудование: персональный компьютер, включенный в сеть; Microsoft Windows

Ход работы: Изучить теоретические сведения

Подключение компьютера к сети позволяет организовать общий доступ к файлам и принтерам на других компьютерах, а также обмен электронной почтой. В этой работе рассматривается, как настроить компьютер для работы в сети, и описывается выполнение некоторых сетевых операций.

Настройка компьютера для работы в сети

Для большинства компьютеров настройка на работу в сети производится при установке операционной системы. Если в процессе установки подключение к сети произведено не было, это можно сделать позднее с помощью значка “Сеть” Панели управления.

Перед установкой сетевого программного обеспечения необходимо убедиться, что сетевое оборудование (сетевая плата, кабели и другие устройства) правильно установлено и соединено.

Установка сетевого программного обеспечения

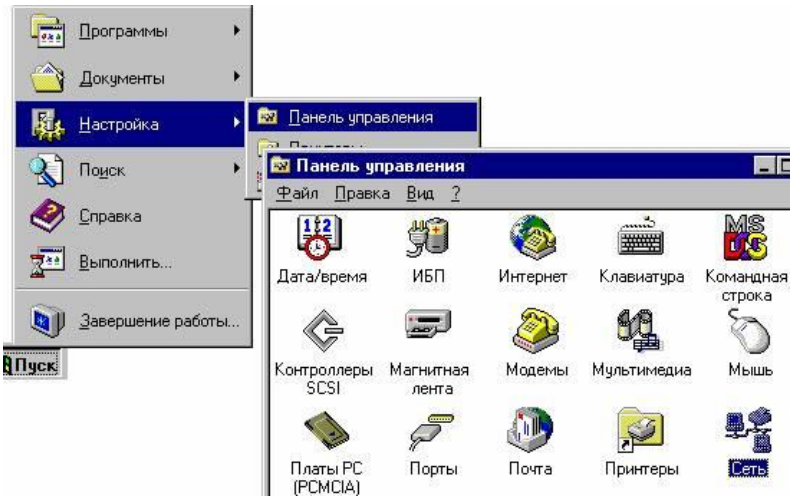
1. Нажмите кнопку “Пуск” и выберите в меню Настройка команду Панель управления

2. Дважды щелкните значок “Сеть”.
3. На экране появится первое окно мастера установки сети. Для подключения компьютера к сети следуйте выводимым на экран указаниям.

Замена сетевого программного обеспечения и оборудования

Иногда возникает необходимость замены или добавления нового сетевого программного обеспечения или оборудования, например служб, протоколов, привязок и сетевых плат. Для этого также используется значок “Сеть” Панели управления.

Изменение сетевых программ или оборудования



1. Нажмите кнопку “Пуск” и выберите в меню Настройка команду Панель управления.
2. Дважды щелкните значок “Сеть”. На экране появится диалоговое окно Сеть с набором вкладок, позволяющих внести необходимые изменения:

- вкладка “Компьютер” отображает имя компьютера и домена, заданные во время установки системы.
- вкладка “Службы” содержит список используемых сетевых служб.
- вкладка “Протоколы” содержит список сетевых протоколов.
- вкладка “Адаптеры” содержит список установленных в компьютере сетевых плат.

- вкладка “Привязки” является дополнительным средством Windows NT. Она позволяет включить и отключить отдельные привязки, а также изменить порядок существующих привязок.

3. Чтобы добавить сетевой компонент выберите нужную вкладку и нажмите кнопку “Добавить”.
4. Чтобы обновить существующий драйвер компонента выберите нужную вкладку и нажмите кнопку “Обновить”. В процессе обновления потребуется диск с новым драйвером.

Подключение к компьютерам в сети

	Чтобы просмотреть файлы и каталоги на компьютерах, подсоединенных к сети или входящих в домен, дважды щелкните значок “Сетевое окружение” на рабочем столе.
	Первый значок в списке компьютеров, “Вся сеть”, имеет особое назначение.
	Этот значок позволяет вывести полный список доступных служб доступа к сетям, а также список других доступных доменов и локальных сетей. Содержимое списка всей сети определяется системным администратором.

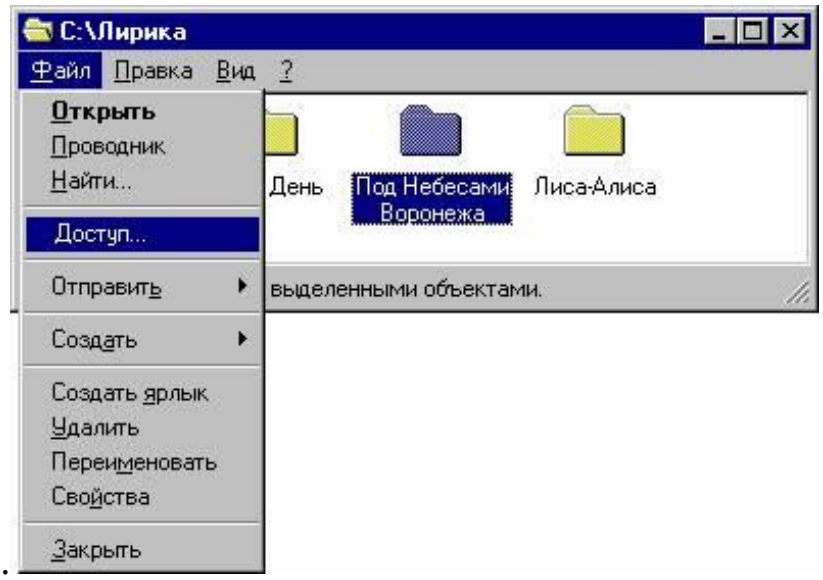
Общий доступ к файлам и папкам

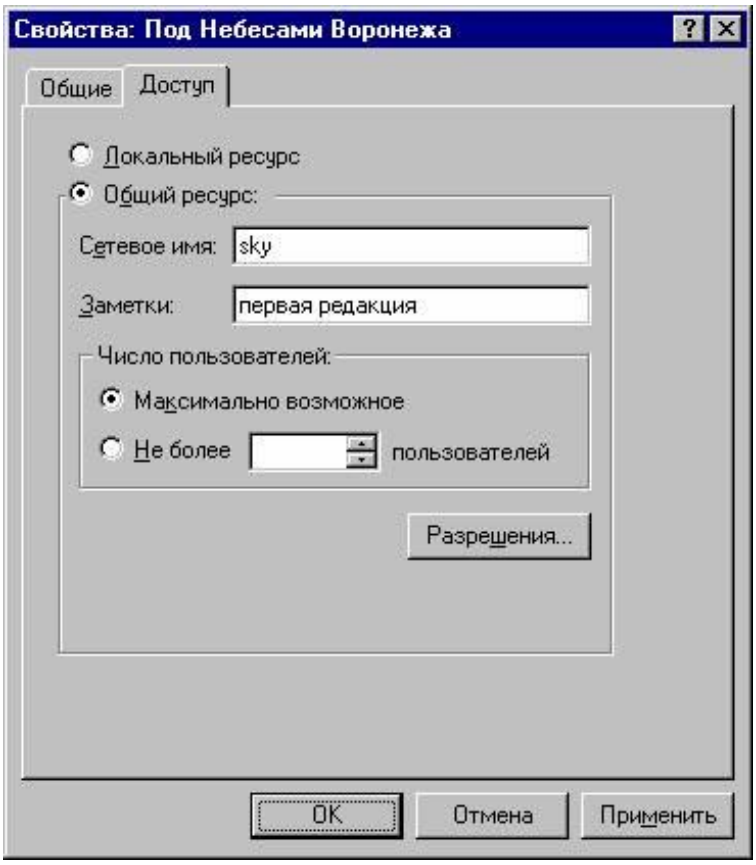
Файлы и папки на локальном компьютере можно сделать общими, разрешив доступ к ним для других пользователей сети.

Для организации общего доступа к папкам или файлам:

1. Найдите папку, которую нужно сделать общей, и выделите ее.
2. Выберите в меню Файл команду Доступ. Если эта команда отсутствует в меню, необходимо сначала установить поддержку сети для Windows NT

3. .



4. На вкладке «Доступ» окна свойств папки установите нужные параметры общего доступа, введите имя общего ресурса и заметки.
5. 

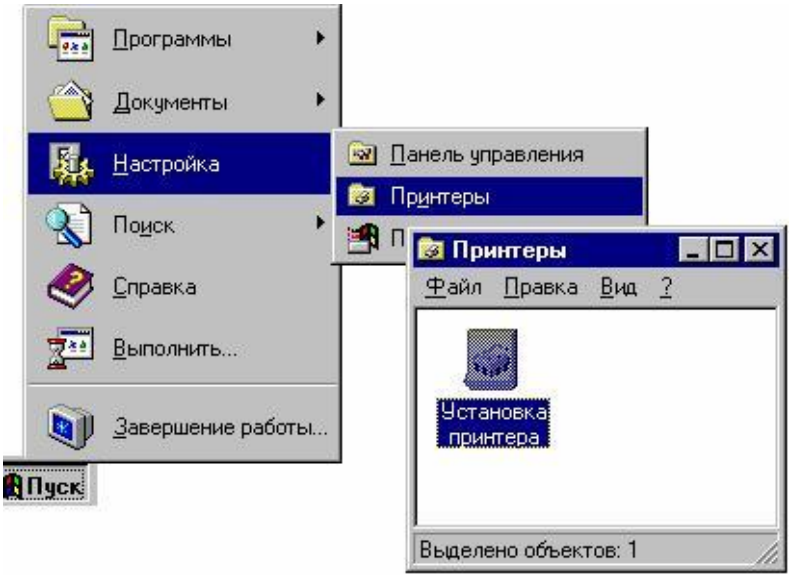
6. Чтобы ограничить доступ к папке, нажмите кнопку «Разрешения».

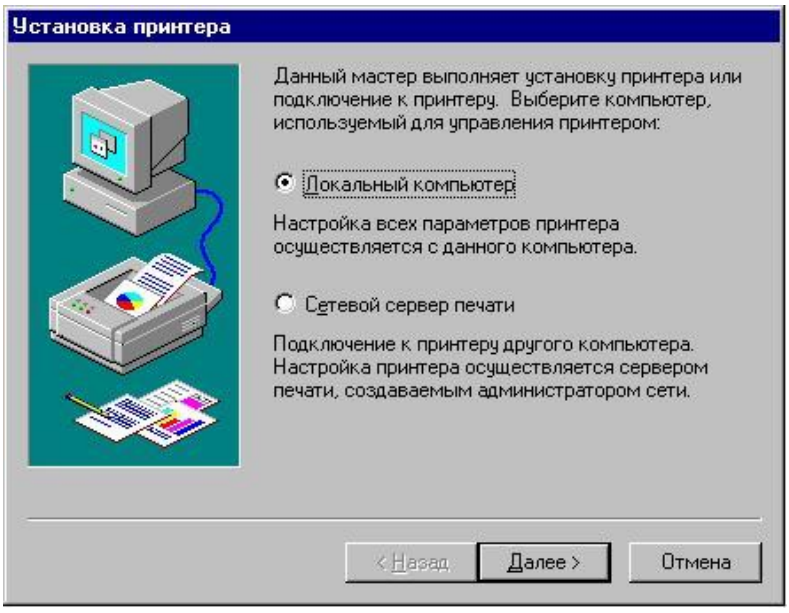
Теперь другие пользователи сети смогут просмотреть содержимое общей папки.

Подключение к сетевым принтерам

Для подключения к сетевому принтеру, как и для установки принтера, подсоединенного к локальному компьютеру, используется мастер установки принтеров, специальная пошаговая программа установки. Чтобы выбрать в сети нужный принтер, необходимо задать полный сетевой путь к нему, однако можно просто найти принтер с помощью значка «Сетевое окружение» и дважды щелкнуть его значок для запуска установки.

Для установки сетевого принтера:

1. Нажмите кнопку “Пуск” и выберите в меню Настройка команду Принтеры**.**
2. Дважды щелкните значок “Установка принтера”. На экране появится первое окно мастера установки принтеров.
3. 

4. Следуйте выводимым на экран указаниям.
5. 

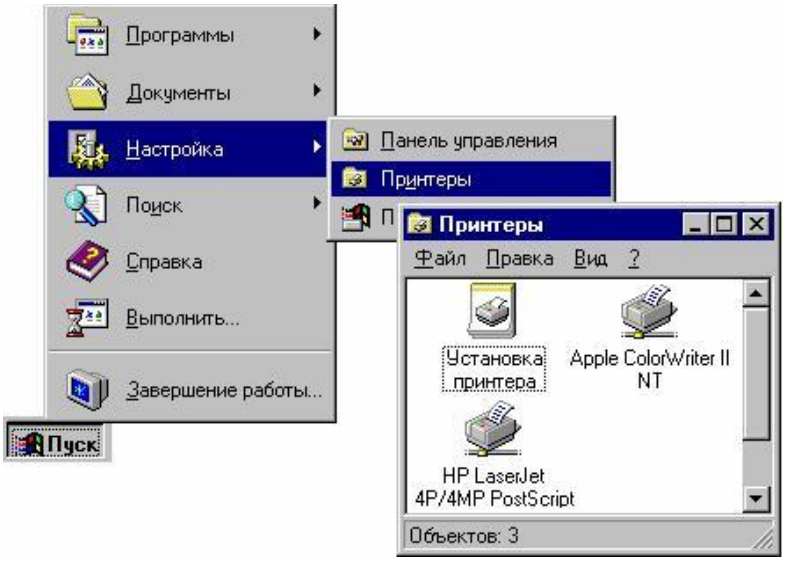
По окончании установки в папке “Принтеры” появится значок нового принтера. Теперь принтер готов к печати документов.

Общий доступ к локальному принтеру

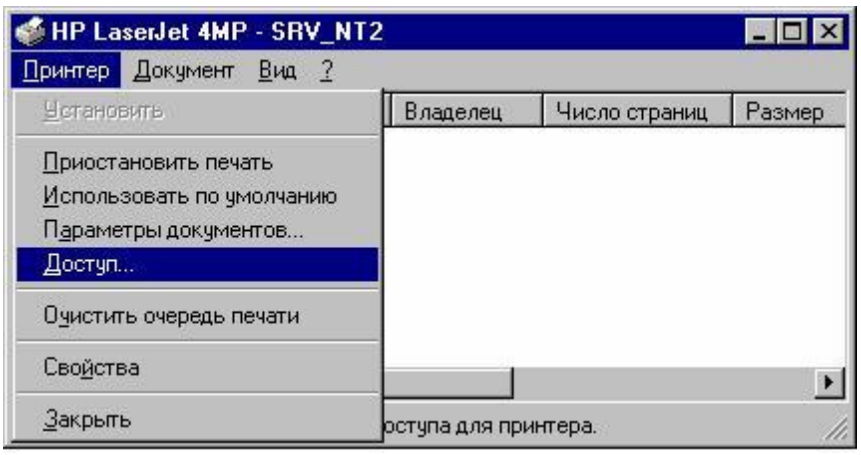
Принтер, подсоединенный к локальному компьютеру, можно сделать общим, разрешив доступ к нему для других пользователей сети.

Чтобы сделать принтер общим:

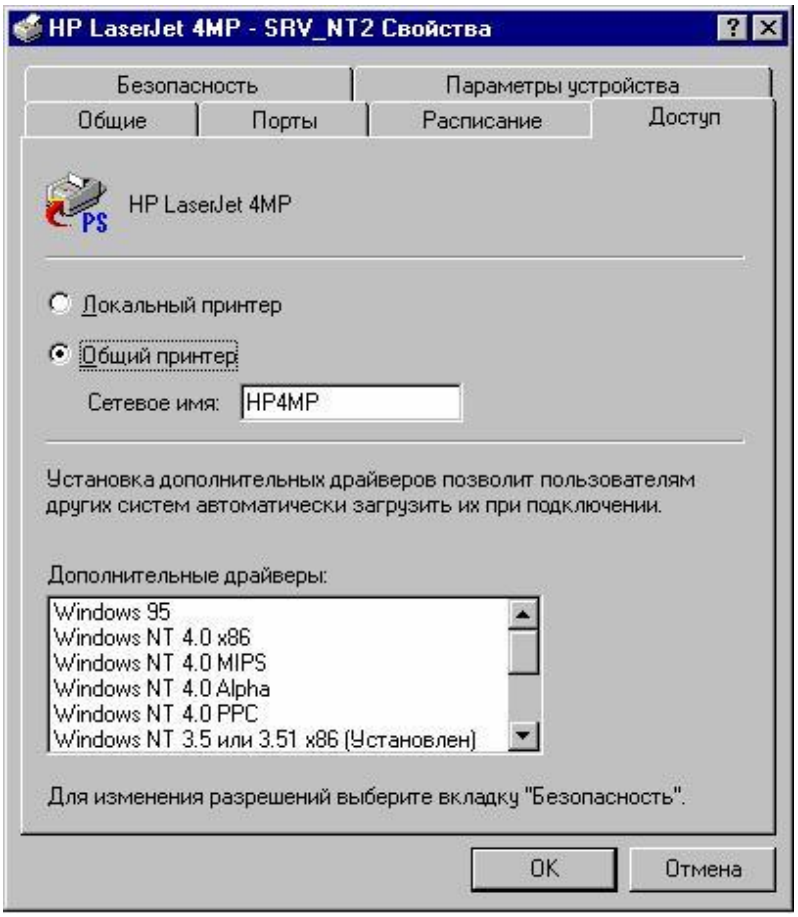
1. Нажмите кнопку “Пуск” и выберите в меню Настройка команду Принтеры.



2.
3. Выберите нужный принтер в папке “Принтеры”.

4. 

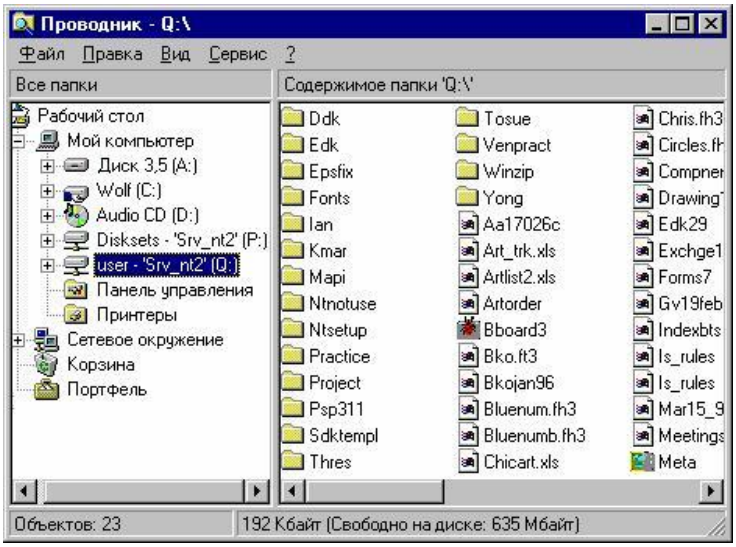
5. Выберите в меню Файл команду Доступ.
6. Установите нужные параметры в окне свойств принтера.



Просмотр сетевых дисков с помощью проводника Windows NT

Для просмотра содержимого подключенных сетевых дисков можно воспользоваться проводником Windows NT. Содержимое сети в окне проводника отображается в виде иерархической структуры. Это окно позволяет увидеть, что находится на подключенных сетевых дисках, а также на любых локальных дисках компьютера.

Просмотр содержимого сети:

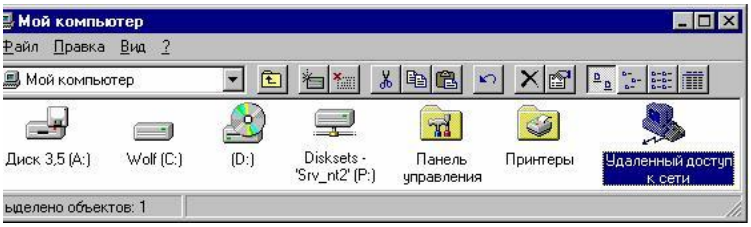
1. Нажмите кнопку “Пуск” и выберите в меню Программы команду Проводник. В левой области окна появится список сетевых дисков.
2. 

3. Выберите диск и просмотрите его содержимое в правой области окна.

Удаленный доступ к сети

Средства удаленного доступа к сети позволяют работать через модем с общими ресурсами другой сети, например с файлами или принтерами.

Для использования удаленного доступа к сети:

1. Дважды щелкните значок “Мой компьютер”, а затем значок “Удаленный доступ к сети”.
2. 

   Следуйте выводимым на экран указаниям.

Средства командной строки

Для работы в сети в Windows имеется мощная утилита командной строки NET.

С ее помощью можно управлять сетевыми ресурсами и производить основные действия в сети.

Синтаксис данной команды:

Можно использовать следующие имена команд:

NET ACCOUNTS NET HELP NET SHARE
NET COMPUTER NET HELPMSG NET START
NET CONFIG NET LOCALGROUP NET STATISTICS
NET CONFIG SERVER NET NAME NET STOP
NET CONFIG WORKSTATION NET PAUSE NET TIME
NET CONTINUE NET PRINT NET USE
NET FILE NET SEND NET USER
NET GROUP NET SESSION NET VIEW

NET HELP SERVICES – эта команда выводит список служб, которые можно запустить.

NET HELP SYNTAX – эта команда выводит объяснения синтаксических

правил, используемых при описании команд в Справке.

NET HELP имя_команды | MORE – просмотр справки по одному экрану за раз.

Далее рассмотрим команды утилиты NET с примерами.

NET ACCOUNTS

NET ACCOUNTS – эта команда используется для обновления базы данных регистрационных записей и изменения параметров входа в сеть (LOGON) и требований к паролям для всех регистрационных записей.

Синтаксис данной команды:

NET ACCOUNTS [/FORCELOGOFF:{минуты | NO}] [/MINPWLEN:длина]

[/MAXPWAGE:{дни | UNLIMITED}] [/MINPWAGE:дни]

[/UNIQUEPW:число] [/DOMAIN]

При использовании этой команды без указания параметров NET ACCOUNTS выводит текущие значения параметров, определяющих требования к паролям и входу в сеть, а также информацию о домене.

Должны быть выполнены два условия для того, чтобы изменения параметров с помощью команды NET ACCOUNTS вступили в силу:

1. Требования к паролям и параметрам входа в сеть можно применять только в том случае, если были определены регистрационные записи пользователей (с помощью Диспетчера пользователей или команды NET USER).
2. На всех серверах домена, проверяющих полномочия при входе в сеть, должна быть запущена служба входа в сеть. Эта служба запускается автоматически при запуске Windows.

Параметры:

/FORCELOGOFF:{минуты | NO} – Устанавливает время в минутах, через которое пользователь будет принудительно отключен по истечении срока действия его регистрационной записи или разрешенного интервала времени.

По умолчанию используется значение NO, т.е. принудительное отключение не используется.

/MINPWLEN:длина – Устанавливает минимальное количество знаков, которое должен иметь пароль. Допустимый диапазон значений: 0–14 знаков, по умолчанию используется значение 6.

/MAXPWAGE:{дни | UNLIMITED} – Устанавливает максимальный срок жизни пароля (в днях). Для указания бессрочного действия пароля используется значение UNLIMITED.

Значение параметра /MAXPWAGE не может быть меньше /MINPWAGE.

Допустимый диапазон значений: 1–999 дней; по умолчанию используется 90 дней.

/MINPWAGE:дни – Устанавливает минимальный срок жизни пароля (в днях), по истечении которого пользователь может изменить пароль. Значение 0 позволяет менять пароль как угодно часто. Допустимый диапазон значений: 1–999 дней; по умолчанию используется 0 дней. Значение параметра /MINPWAGE не может быть больше /MAXPWAGE.

/UNIQUEPW:число – Устанавливает требование, чтобы определяемый пользователем новый пароль не повторял ни одного из последних использовавшихся ранее паролей. Максимальное значение – 24.

/DOMAIN – Выполняет данную операцию на контроллере домена текущего активного домена. В противном случае, операция производится на локальном компьютере.

Пример использования:

net accounts

Принудительный выход по истечении времени через: Никогда

Минимальный срок действия пароля (дней): 0

Максимальный срок действия пароля (дней): 42

Минимальная длина пароля: 0

Хранение неповторяющихся паролей: Нет

Блокировка после ошибок ввода пароля: Никогда

Длительность блокировки (минут): 30

Сброс счетчика блокировок через (минут): 30

Роль компьютера: РАБОЧАЯ СТАНЦИЯ

Команда выполнена успешно.

NET COMPUTER

NET COMPUTER – эта команда добавляет или удаляет компьютеры из базы данных домена, и используется только на серверах Windows NT Server.

Синтаксис данной команды:

NET COMPUTER \\имя_компьютера {/ADD | /DEL}

Параметры:

\\имя_компьютера – Указывает компьютер, который нужно добавить к домену или удалить из домена.

/ADD – Добавляет указанный компьютер к домену.

/DEL – Удаляет указанный компьютер из домена.

NET CONFIG

NET CONFIG – отображает информацию о настройке служб рабочей станции или сервера. Когда эта команда используется без указания переключателяSERVER или WORKSTATION, то выводится список настраиваемых служб. Для того, чтобы получить справку о том, как выполнить настройку конкретной службы, введите команду HELP CONFIG имя_службы.

Синтаксис данной команды:

NET CONFIG [SERVER | WORKSTATION]

Параметры:

SERVER – Отображает информацию о настройке службы сервера.

WORKSTATION – Отображает информацию о настройке службы рабочей станции.

Пример использования:

net config server

Имя сервера \\HOME

Комментарий для сервера

Версия программы Windows 2002

Активный сервер на

NetBT_Tcpip_{6B78BD8E–F521–4197–8189–EF5BD6601473} (525405e27788)

NetbiosSmb (000000000000)

Скрытый сервер No

Максимальное число пользователей 10

Максимальное число открытых файлов в сеансе 16384

Время холостого хода сеанса (мин) 15

Команда выполнена успешно.

или

net config workstation

Имя компьютера \\HOME

Полное имя компьютера home

Имя пользователя Collega

Активная рабочая станция на

NetbiosSmb (000000000000)

NetBT_Tcpip_{6B78BD8E–F521–4197–8189–EF5BD6601473} (525405E27788)

Версия программы Windows 2002

Домен рабочей станции WORKGROUP
DNS–имя домена рабочей станции (null)
Домен входа HOME

Интервал ожидания открытия COM–порта (с) 0
Отсчет передачи COM–порта (байт) 16
Таймаут передачи COM–порта (мс) 250
Команда выполнена успешно.

NET CONTINUE

NET CONTINUE – активизирует службу Windows, ранее приостановленную с помощью команды NET PAUSE.

Синтаксис данной команды:

NET CONTINUE имя_службы

Параметры:

имя_службы Имя приостановленной службы. Например, это может быть одно из следующих имен:

NETLOGON (Сетевой вход в систему)
NTLMSSP (Поставщик поддержки безопасности NT LM)
SCHEDULE (Планировщик заданий)
SERVER (Сервер)
WORKSTATION (Рабочая станция)

NET FILE

NET FILE – эта команда закрывает совместно используемый файл и снимает блокировки файла. Когда используется без параметров, выводит список открытых файлов на сервере. Этот список включает идентификационный номер, присвоенный открытому файлу, путь к этому файлу, имя пользователя, количество блокировок.

Эта команда работает только на компьютерах с запущенной службой сервера.

Синтаксис данной команды:

NET FILE [номер [/CLOSE]]

Параметры:

номер – Задает идентификационный номер файла.

/CLOSE – Закрывает открытый файл и снимает блокировки этого файла. Эту команду следует вводить на том сервере, где располагается совместно используемый файл.

NET GROUP

NET GROUP – эта команда добавляет, выводит на экран или изменяет глобальные группы на сервере. Когда используется без параметров, отображает список глобальных групп на сервере.

Синтаксис данной команды:

NET GROUP [имя_группы [/COMMENT:»текст»]] [/DOMAIN]

имя_группы {/ADD [/COMMENT:»текст»] | /DELETE} [/DOMAIN]

имя_группы имя_пользователя […] {/ADD | /DELETE} [/DOMAIN]

Параметры:

Имя_группы – Задает имя группы, которую нужно добавить, расширить или удалить. Для того чтобы получить список пользователей в группе, задайте только имя группы.

/COMMENT:»текст» – Добавляет комментарий для новой или существующей группы. Длина комментария не должна превышать 48 знаков. Текст комментария должен быть заключен в кавычки.

/DOMAIN – Выполняет операцию на контроллере домена в текущем домене. В противном случае операция выполняется на локальном компьютере.

имя_пользователя […]– Задает одно или несколько имен, которые нужно добавить или удалить из группы. Имена пользователей разделяются пробелом.

/ADD – Добавляет группу, или добавляет пользователя в группу.

/DELETE – Удаляет группу, или удаляет пользователя из группы.

NET LOCALGROUP

NET LOCALGROUP – эта команда служит для изменения локальных групп на компьютере. Когда используется без параметров, отображает список локальных групп на данном компьютере.

Синтаксис данной команды:

NET LOCALGROUP [имя_группы [/COMMENT:»текст»]] [/DOMAIN]

имя_группы {/ADD [/COMMENT:»текст»] | /DELETE} [/DOMAIN]

имя_группы имя […] {/ADD | /DELETE} [/DOMAIN]

Параметры:

имя_группы – Задает имя локальной группы, которую необходимо добавить, расширить или удалить. Если указать только имя группы, то будет выведен список пользователей или глобальных групп, являющихся членами этой локальной группы.

/COMMENT:»текст» – Добавляет комментарий для новой или существующей группы. Текст должен быть заключен в кавычки.

/DOMAIN – Выполняет операцию на основном контроллере домена в текущем домене. В противном случае операция выполняется на локальном компьютере.

имя […] – Список из одного или нескольких имен пользователей, которых необходимо добавить или удалить из локальной группы.

Имена разделяются пробелом. Эти имена могут быть именами пользователей или глобальных групп, но не именами других локальных групп. Если пользователь зарегистрирован в другом домене, его имени должно предшествовать имя домена (например, SALES\RALPHR).

/ADD – Добавляет имя группы или имя пользователя в локальную группу. Регистрационная запись для добавляемых пользователей или глобальных групп должна быть создана заранее.

/DELETE – Удаляет имя группы или пользователя из локальной группы.

NET NAME

NET NAME – эта команда добавляет или удаляет используемое для получения сообщений имя (псевдоним) данного компьютера. На это имя отсылаются сообщения. Когда команда NET NAME используется без параметров, она отображает имена, принимающие сообщения на этом компьютере.

Список имен компьютера имеет три источника:

1. Имена для сообщений, которые добавляются с помощью команды NET NAME.
2. Имя компьютера, которое добавляется в момент запуска службы рабочей станции. Это имя не может быть удалено.
3. Имя пользователя, которое добавляется в тот момент, когда пользователь входит в систему, в том случае, если это имя не

используется на другом компьютере. Это имя может быть удалено.

Синтаксис данной команды:

NET NAME [имя [/ADD | /DELETE]]

Параметры:

Имя – Задает имя для получения сообщений. Это имя может иметь длину до 15 знаков.

/ADD – Добавляет имя для этого компьютера. Этот параметр может быть опущен, команда ‘NET NAME имя’ приводит к тому же результату, что и команда ‘NET NAME имя /ADD’.

/DELETE – Удаляет указанное имя на компьютере.

NET PAUSE

NET PAUSE – эта команда приостанавливает службу Windows или ресурс.

Синтаксис данной команды:

NET PAUSE имя_службы

Параметры:

имя_службы – Это имя приостанавливаемой службы. Например, это может быть одно из следующих имен:

NETLOGON (Сетевой вход в систему)

NTLMSSP (Поставщик поддержки безопасности NT LM)

SCHEDULE (Планировщик заданий)

SERVER (Сервер)

WORKSTATION (Рабочая станция)

NET PRINT

NET PRINT – эта команда отображает список заданий для печати и совместно используемых очередей. Для каждой очереди отображается список заданий с указанием размера и статуса каждого задания, и статус очереди.

Синтаксис данной команды:

NET PRINT \\имя_компьютера\имя_ресурса [\\имя_компьютера] №_задания [/HOLD | /RELEASE | /DELETE]

Параметры:

\\имя_компьютера – Задает имя компьютера, на котором находятся совместно используемые очереди заданий на печать.

имя_ресурса – Задает имя совместно используемой очереди принтера. №_задания Задает идентифицирующий номер, присвоенный заданию на печать.Компьютер, на котором находятся одна или несколько очередей принтеров, присваивает каждому заданию уникальный номер.

/HOLD – Задерживает задание в очереди, предотвращая печать. Задание остается в очереди принтера, другие задания обходят его, пока оно не будет освобождено.

/RELEASE – Вновь активизирует задержанное ранее задание.

/DELETE – Удаляет задание из очереди.

NET SEND

NET SEND – эта команда отправляет сообщения другим пользователям, компьютерам или иным именам для получения сообщений в сети. Для того, чтобы получить сообщение, должна быть запущена служба сообщений (MESSENGER).

Отправить сообщение на конкретное имя можно только в том случае, если это имя активно в сети. Если сообщение отсылается на имя пользователя, то этот пользователь должен к этому моменту войти в сеть и запустить службу сообщений для того, чтобы получить это сообщение.

Синтаксис данной команды:

NET SEND {имя | * | /DOMAIN[:имя] | /USERS} сообщение

Параметры:

имя – Задает имя пользователя, компьютера или имя для получения сообщений, на которое отправляется данное сообщение. Если это имя компьютера, которое содержит пробелы, то оно должно быть заключено в кавычки (» «).

* – Используется для отправки сообщения по всем именам в текущей группе.

/DOMAIN[:имя] – Направляет сообщение по всем именам домена данной рабочей станции. Если указано имя, то сообщение отправляется по всем именам указанного домена или рабочей группы.

/USERS – Направляет сообщение всем пользователям, подключенным в настоящий момент к серверу.

сообщение – Представляет собой текст отправляемого сообщения.

NET SESSION

NET SESSION – эта команда выводит список или завершает текущие сеансы связи между данным компьютером и другими компьютерами сети. Когда используется без параметров, выводит информацию о всех текущих сеансах связи с интересующим компьютером.

Эта команда используется только на серверах.

Синтаксис данной команды:

NET SESSION [\\имя_компьютера] [/DELETE]

Параметры:

\\имя_компьютера – выводит информацию о текущих сеансах связи указанного компьютера.

/DELETE – Завершает сеанс связи между локальным компьютером и компьютером с указанным именем, при этом закрывает все открытые на

этом компьютере файлы для этого сеанса связи. Если имя компьютера опущено, то закрываются все сеансы связи.

NET SHARE

NET SHARE – эта команда разрешает использовать ресурсы другим пользователям в сети. Когда используется без параметров, выводит информацию обо всех ресурсах данного компьютера, которые могут быть совместно использованы.

Для каждого ресурса Windows NT выводит имя устройства или путь и соответствующий комментарий.

Синтаксис данной команды:

NET SHARE имя_ресурса имя_ресурса=диск:путь

[/USERS:число | /UNLIMITED]

[/REMARK:»текст»]

[/CACHE:Manual | Automatic | No]

[/CACHE:Manual | Documents| Programs | None]

имя_ресурса

[/USERS:число | /UNLIMITED]

[/REMARK:»текст»]

[/CACHE:Manual | Documents | Programs | None] {имя_ресурса | имя_устройства | диск:путь} /DELETE

Параметры:

имя_ресурса – Задает сетевое имя данного совместно используемого ресурса. Если ввести в качестве параметра только имя ресурса, то выводится информация об этом ресурсе.

диск:путь – Указывает абсолютный путь к совместно используемому каталогу.

/USERS:число – Устанавливает максимальное число пользователей, которые могут одновременно получить доступ к совместно используемому ресурсу.

/UNLIMITED – Определяет, что ограничения на число пользователей, которые могут получить доступ к совместно используемому ресурсу, отсутствует.

/REMARK:»текст» – Задает краткое примечание, описывающее ресурс. Текст должен быть заключен в кавычки.

имя_устройства – Задает один или несколько принтеров (от LPT1: до LPT9:) совместно используемых под данным именем ресурса.

/DELETE – Прекращает совместное использование данного ресурса.

/CACHE:Manual – Задает ручное кэширование программ и документов на этом общем ресурсе.

/CACHE:Documents – Задает автоматическое кэширование документов на этом общем ресурсе.

/CACHE:Programs – Задает автоматическое кэширование документов и программ на этом общем ресурсе.

/CACHE:None – Отключает кэширование на этом общем ресурсе.

NET START

NET START – эта команда выводит список запущенных служб.

При запуске из командной строки можно использовать либо приведенные выше сокращенные английские названия, либо полные русские названия служб, при этом они должны быть заключены в кавычки и не допускается изменение прописных букв на строчные и наоборот.

Например, команда NET START «Сетевой вход в систему» запускает службу сетевого входа в систему.

Команда NET START может также использоваться для запуска служб, не входящих в состав Windows.

Синтаксис данной команды:

NET START [служба]

Параметры:

[служба] – может быть одной из следующих служб:

ALERTER (Оповещатель)

BROWSER (Обозреватель компьютеров)

NWCWORKSTATION (Клиент для сетей NetWare)

CLIPSRV (Сервер папки обмена)

DHCP (DHCP–клиент)

EVENTLOG (Журнал событий)

MESSENGER (Служба сообщений)

NETLOGON (Сетевой вход в систему)

NTLMSSP (Поставщик поддержки безопасности NT LM)

RASMAN (Диспетчер подключений удаленного доступа)

REMOTEACCESS (Маршрутизация и удаленный доступ)

RPCLOCATOR (Локатор удаленного вызова процедур (RPC))

RPCSS (Удаленный вызов процедур (RPC))

SCHEDULE (Планировщик заданий)

SERVER (Сервер)

SPOOLER (Диспетчер очереди печати)

LMHOSTS (Поддержка NetBIOS через TCP/IP)

UPS (Источник бесперебойного питания)

WORKSTATION (Рабочая станция)

NET STATISTICS

NET STATISTICS – выводит журнал статистики для локальной службы рабочей станции или службы сервера. Если используется без

параметров, то эта команда выводит список служб, для которых может накапливаться статистика.

Синтаксис данной команды:

NET STATISTICS [WORKSTATION | SERVER]

Параметры:

SERVER – Выводит статистику для службы сервера.

WORKSTATION – Выводит статистику для службы рабочей станции.

Примеры использования:

net statistics server

Статистика сервера для \\HOME

Статистика после 11/30/2005 1:20 PM

Принятые сеансы 1

Сеансы с истекшим интервалом 0

Сеансы с ошибками 0

Послано КБ 0

Принято КБ 0

Среднее время отклика (мс) 0

Системные ошибки 0

Нарушение разрешений 0

Нарушение паролей 0

Доступ к файлам 0

Доступ к устройствам связи 0

Задания печати в очереди 0

Исчерпанные буферы времени

Большие буферы 0

Затребованные буферы 0

Команда выполнена успешно.

или

net statistics workstation

Статистика рабочей станции для \\HOME

Статистика после 11/30/2005 1:19 PM

Получено байт 0

Принятые блоки сообщений сервера SMB 1

Передано байт 0

Переданные блоки сообщений сервера SMB 0

Операции чтения 0

Операции записи 0

Отказано в чтении 0

Отказано в записи 0

Ошибки сети 0

Выполненные подключения 0

Повторные подключения 0

Отключений от сервера 0

Запущенные сеансы 0

Зависание сеансов 0

Сбои в сеансах 0

Сбои в операциях 0

Счетчик использования 0

Счетчик сбоев при использовании 0

Команда выполнена успешно.

NET STOP

NET STOP – эта команда останавливает одну из служб Windows.

Остановка одной из служб может привести к отключению сетевых соединений, используемых этой службой. Кроме того, некоторые службы зависят от других служб. Остановка одной из служб может привести к остановке других служб.

Некоторые службы не могут быть остановлены.

Команда NET STOP может также использоваться для остановки служб, не входящих в состав Windows.

Синтаксис данной команды:

NET STOP служба

Параметры:

[служба] – может быть одной из следующих служб:

ALERTER (Оповещатель)

BROWSER (Обозреватель компьютеров)

NWCWORKSTATION (Клиент для сетей NetWare)

CLIPSRV (Сервер папки обмена)

DHCP (DHCP–клиент)

EVENTLOG (Журнал событий)

MESSENGER (Служба сообщений)

NETLOGON (Сетевой вход в систему)

NTLMSSP (Поставщик поддержки безопасности NT LM)

RASMAN (Диспетчер подключений удаленного доступа)

REMOTEACCESS (Маршрутизация и удаленный доступ)

RPCLOCATOR (Локатор удаленного вызова процедур (RPC))

RPCSS (Удаленный вызов процедур (RPC))

SCHEDULE (Планировщик заданий)

SERVER (Сервер)

SPOOLER (Диспетчер очереди печати)

LMHOSTS (Поддержка NetBIOS через TCP/IP)

UPS (Источник бесперебойного питания)

WORKSTATION (Рабочая станция)

NET TIME

NET TIME – синхронизирует показания часов компьютера с другим компьютером или доменом. Если используется без параметров в домене Windows Server, выводит текущую дату и время дня, установленные на компьютере, который назначен сервером времени для данного домена.

Эта команда позволяет задать сервер времени NTP для компьютера.

Синтаксис данной команды:

NET TIME [\\компьютер | /DOMAIN[:домен]|

/RTSDOMAIN[:домен]] [/SET]

[\\компьютер] /QUERYSNTP

[\\компьютер] /SETSNTP[:список серверов NTP]

Параметры:

\\компьютер – Задает имя компьютера, который нужно проверить или с которым нужно синхронизировать показания часов.

/DOMAIN[:домен] – Задает домен, с которым нужно синхронизировать показания часов.

/RTSDOMAIN[:домен] – Задает синхронизацию времени с сервером времени (Reliable Time Server) из указанного домена.

/SET – Синхронизирует показания часов компьютера со временем указанного компьютера или домена.

/QUERYSNTP – Отображает назначенный этому компьютеру сервер NTP

/SETSNTP[:ntp server list] – Задает список серверов времени NTP этого компьютера. Это может быть список IP–адресов или DNS–имен, разделенных пробелами. Если задано несколько серверов, список должен быть заключен в кавычки.

NET USE

NET USE – эта команда подключает компьютер к совместно используемому ресурсу или отключает компьютер от совместно

используемого ресурса. Когда используется без параметров, выводит список соединений для данного компьютера.

Синтаксис данной команды:

NET USE [имя_устройства | *] [\\имя_компьютера\имя_ресурса[\том] [пароль | *]]

[/USER:[имя_домена\]имя_пользователя]

[/USER:[имя_домена_с_точками\]имя_пользователя]

[/USER:[имя_пользователя@имя_домена_с_точками]

[/SMARTCARD]

[/SAVECRED]

[[/DELETE] | [/PERSISTENT:{YES | NO}]]

NET USE {имя_устройства | *} [пароль | *] /HOME

NET USE [/PERSISTENT:{YES | NO}]

Параметры:

имя_устройства – Назначает имя для подключения к ресурсу или задает устройство, от которого нужно выполнить отключение. Используется два типа имен устройств: дисковые устройства (буквы от D: до Z:) и принтеры (от LPT1: до LPT3:). Если ввести звездочку (*) вместо имени устройства, то назначается следующее незанятое имя.

\\имя_компьютера – Указывает имя компьютера, контролирующего совместно используемый ресурс. Если в имени компьютера используются пробелы, то нужно заключить весь этот параметр в кавычки, вместе с двумя символами обратной косой черты (\\). Длина имени компьютера может быть от 1 до 15 знаков.

\имя_ресурса – Указывает сетевое имя совместно используемого ресурса.

\volume – Задает том NetWare на сервере. Для того, чтобы иметь доступ к серверам NetWare, необходимо установить и запустить службу клиента для NetWare(на Windows Workstation) или службу шлюза для NetWare (на Windows Server).

пароль – Указывает пароль, который нужен для доступа к совместно используемому ресурсу.

* – Вызывает открытие специальной строки ввода пароля. Пароль не выводится на экран во время его ввода в этой строке.

/USER – Указывает другое имя пользователя, с помощью которого устанавливается соединение.

имя_домена – Указывает другой домен. Если указание домена опущено, то подразумевается текущий домен, использовавшийся при входе в сеть.

имя_пользователя – Указывает имя пользователя для входа в сеть.

/SMARTCARD – Указывает, что это подключение использует личные данные со смарт–карты.

/SAVECRED – Указывает, что имя пользователя и пароль следует сохранить. Этот параметр игнорируется, если команда не запрашивает имя пользователя и пароль. Эта возможность отсутствует на Windows XP Home Edition и поэтому игнорируется.

/HOME – Подключает пользователя к его домашнему каталогу.

/DELETE – Разрывает сетевое соединение и удаляет его из списка постоянных соединений.

/PERSISTENT – Управляет режимом установления постоянных соединений, автоматически подключаемых при входе в систему. По умолчанию используется режим предыдущего соединения.

YES – Запоминает устанавливаемое соединение и обеспечивает его автоматическое подключение при следующем входе в систему.

NO – Не запоминает устанавливаемое соединение или последующие соединения, в результате эти соединения не будут автоматически подключены при следующем входе в систему.

/DELETE – Используется для удаления постоянных соединений.

NET USER

NET USER – эта команда создает и изменяет учетные записи пользователей на компьютере. Когда используется без параметров, выводит список учетных записей пользователей для данного компьютера. Информация об учетных записях пользователей хранится в базе данных учетных записей.

Эта команда используется только на серверах.

Синтаксис данной команды:

NET USER [имя_пользователя [пароль | *] [параметры]] [/DOMAIN]

имя_пользователя {пароль | *} /ADD [параметры] [/DOMAIN]

имя_пользователя [/DELETE] [/DOMAIN]

Параметры:

имя_пользователя – Задает имя пользователя, которое необходимо добавить, удалить, изменить или вывести на экран. Длина имени пользователя не должна превосходить 20 знаков.

пароль – Назначает или изменяет пароль для учетной записи пользователя. Пароль должен отвечать установленным требованиям на длину – быть не короче, чем значение, установленное параметром /MINPWLEN в команде NET ACCOUNTS, и в то же время не длиннее 14 знаков.

* – Вызывает открытие специальной строки ввода пароля. Пароль не выводится на экран во время его ввода в этой строке.

/DOMAIN – Выполняет операцию на контроллере домена в текущем домене.

/ADD – Добавляет учетную запись пользователя в базу данных учетных записей.

/DELETE – Удаляет учетную запись пользователя из базы данных учетных записей.

Параметры – Допустимые параметры перечислены в следующем списке:

/ACTIVE:{YES | NO} Активизирует учетную запись или делает ее не активной. Если учетная запись не активна, пользователь не может получить доступ к серверу. По умолчанию используется значение YES (т.е. учетная запись активна).

/COMMENT:»текст» Добавляет описательный комментарий об учетной записи (длиной не более 48 знаков). Текст должен быть заключен в кавычки.

/COUNTRYCODE:nnn Использует кодовую страницу нужного языка для вывода справки и сообщений об ошибках. Значение 0 означает выбор кодовой страницы по умолчанию.

/EXPIRES:{дата | NEVER} Устанавливает дату истечения срока действия ученой записи. Если используется значение NEVER, то время действия учетной записи не имеет ограничений срока действия. Дата истечения срока действия задается в формате дд/мм/гг или мм/дд/гг, в зависимости от того, какая кодовая страница используется. Месяц может быть указан цифрами, названием месяца или трехбуквенным его сокращением. В качестве разделителя полей должен использоваться знак косой черты (/).

/FULLNAME:»имя» Указывает настоящее имя пользователя (а не кодовое имя, заданное параметром имя_пользователя). Настоящее имя следует заключить в кавычки.

/HOMEDIR:путь Указывает путь к домашнему каталогу пользователя. Этот каталог должен существовать.

/PASSWORDCHG:{YES | NO} Определяет, может ли пользователь изменять свой пароль. По умолчанию используется значение YES (т.е. изменение пароля разрешено).

/PASSWORDREQ:{YES | NO} Определяет, является ли указание пароля обязательным. По умолчанию используется значение YES (т.е. пароль обязателен).

/PROFILEPATH[:путь] Устанавливает путь к профилю пользователя.

/SCRIPTPATH:путь Устанавливает расположение пользовательского сценария для входа в систему.

/TIMES:{промежуток | ALL} Устанавливает промежуток времени, во время которого пользователю разрешен вход в систему. Этот параметр задается в следующем формате:

день[–день][,день[–день]],время[–время][,время[–время]]

Время указывается с точностью до одного часа. Дни являются днями недели и могут указываться как в полном, так и в сокращенном виде. Время можно указывать в 12– и 24–часовом формате. Если используется 12–часовой формат, то можно использовать am, pm, a.m. или p.m. Значение ALL указывает, что пользователь может войти в систему в любое время, а пустое значение указывает, что пользователь не может войти в систему никогда. Разделителем полей указания дней недели и времени является запятая, разделителем при использовании нескольких частей является точка с запятой.

/USERCOMMENT:»текст» Позволяет администратору добавлять или изменять текст комментария к учетной записи.

/WORKSTATIONS:{имя_компьютера[,…] | *} Перечисляет до восьми различных компьютеров, с которых пользователь может войти в сеть. Если данный параметр имеет пустой список или указано значение *, пользователь может войти в сеть с любого компьютера.

NET VIEW

NET VIEW – эта команда выводит список доступных для совместного использования ресурсов данного компьютера. Когда используется без параметров, отображает список компьютеров текущего домена или сети.

Синтаксис данной команды:

NET VIEW [\\имя_компьютера [/CACHE] | /DOMAIN[:имя_домена]]

NET VIEW /NETWORK:NW [\\имя_компьютера]

Параметры:

\\имя_компьютера – Указывает имя компьютера, для которого нужно вывести список совместно используемых ресурсов.

/DOMAIN:имя_домена – Указывает домен, для которого нужно вывести список доступных компьютеров. Если имя домена опущено, выводит все домены данной локальной сети.

/NETWORK:NW – Выводит все доступные серверы в сети NetWare. Если указано имя компьютера, то выводятся ресурсы, доступные на этом компьютере в сети NetWare.

/CACHE – Отображает параметры автономного клиентского кэширования для ресурсов указанного компьютера.

Тема 1.2. Принципы маршрутизации и коммутации

Практическая работа 1

Тема: Настройка статической маршрутизации

Цель: настроить *связь* двух сетей через *маршрутизатор* (роутер).

Сеть на двух маршрутизаторах

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Далее мы изучим статическую маршрутизацию в локальных сетях, рассмотрев этот вопрос на двух практических примерах.

Схема сети для настройки статической маршрутизации приведена на рис. 25.

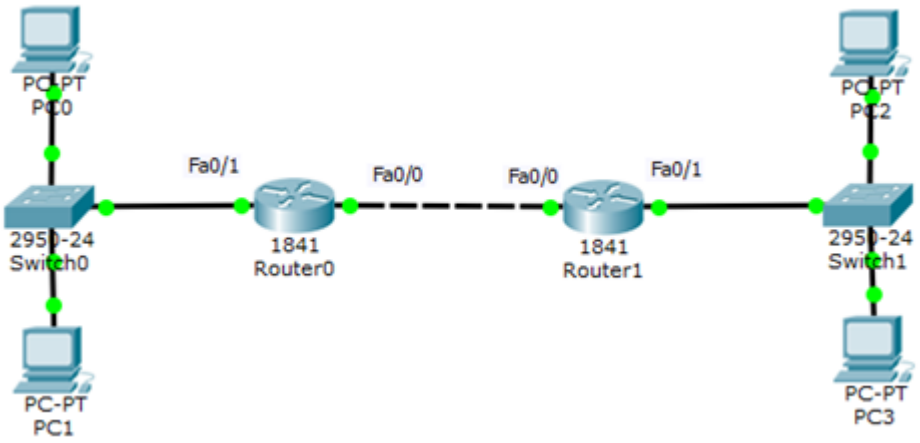


Рис. 25. Схема сети

Если сейчас командой show ip route посмотреть таблицу маршрутизации на R0 и R1, то увидим следующее (рис. 26 и рис. 27).

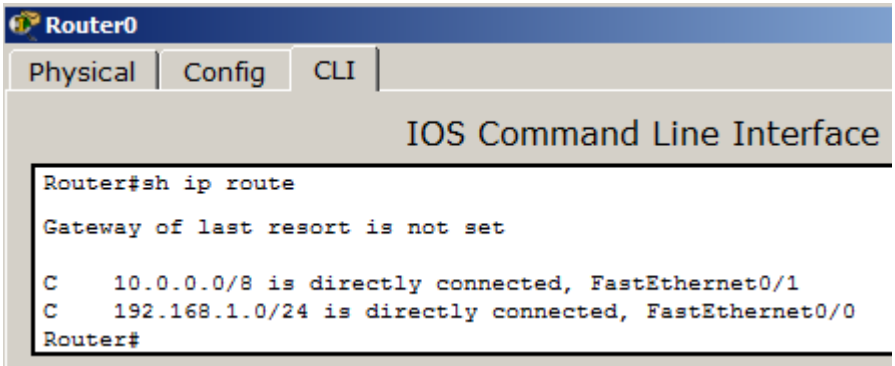


Рис. 26. Таблица маршрутизации на 1-м маршрутизаторе

```
Router>en
Router#sh ip route
Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
Router#
```

Рис. 27. Таблица маршрутизации на 2-м маршрутизаторе

Мы видим, что в данный момент в нашей таблице есть только сети, подключенные напрямую. R0 не знает сеть 10.1.2.0, а R1 не знает сеть 10.1.1.0. Поэтому, чтобы настроить маршрутизацию, следует добавим эти маршруты в таблицы маршрутизаторов:

R0 (config)#ip route 10.1.2.0 255.255.255.0 192.168.1.2

R1 (config)#ip route 10.1.1.0 255.255.255.0 192.168.1.1

Теперь снова выведем таблицы маршрутизации наших устройств (рис. 28).

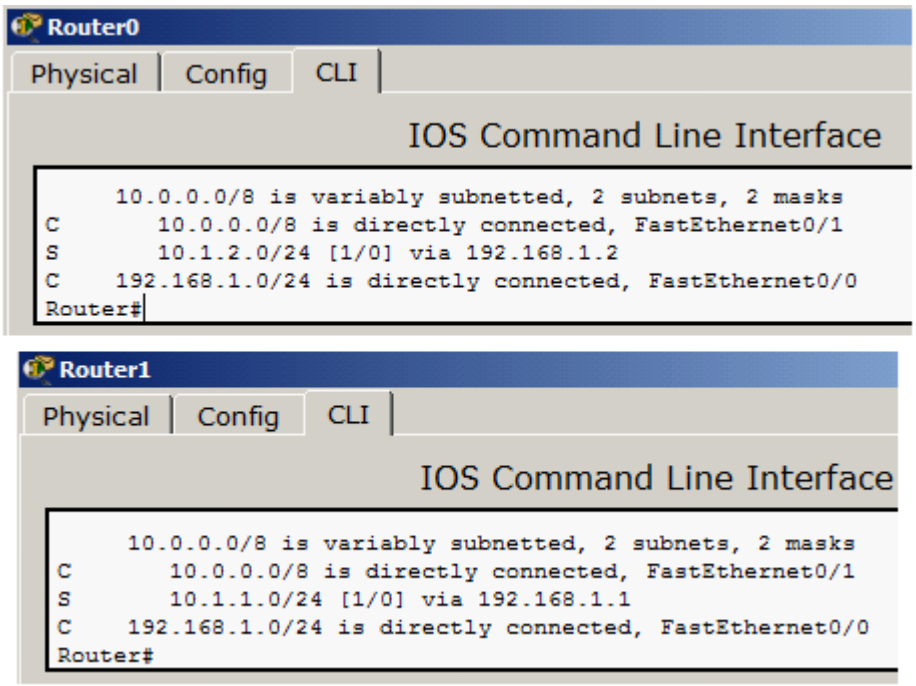


Рис. 28. Маршрутизация настроена

Теперь 1-й маршрутизатор знает, что пакеты, направляемые в подсеть 10.1.2.0 можно переслать маршрутизатору с ip адресом 192.168.1.2, а 2-й маршрутизатор знает, что пакеты, направляемые

в подсеть 10.1.1.0 можно переслать маршрутизатору с ip адресом 192.168.1.1. Проверяем связь ПК из разных сетей (рис. 29).

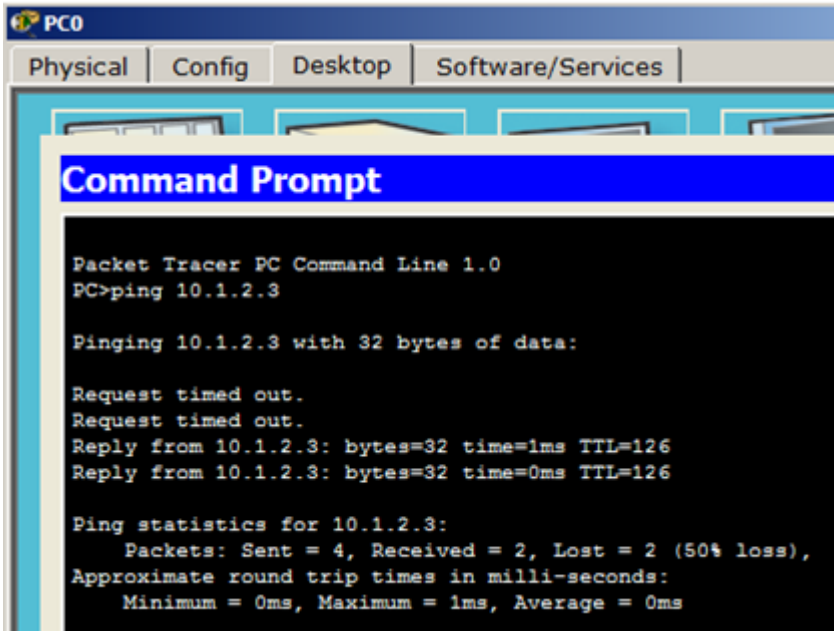


Рис. 29. Статическая маршрутизация настроена – PC0 может общаться с PC3

Описанная сеть на двух маршрутизаторах (файл task-7-3.pkt) прилагается.

Задание 5. Статическая маршрутизация для пяти сетей и роутеров с тремя портами

В этом примере мы соберем и настроим следующую схему сети (рис. 30).

Схема сети

На данной схеме имеется пять сетей: 192.168.1.0, 172.20.20.0, 192.168.100.0, 10.10.10.0 и 192.168.2.0. В качестве шлюза по умолчанию у каждого компьютера указан интерфейс маршрутизатора, к которому он подключен. Маска у всех ПК одна - 255.255.255.0. Маска маршрутизаторов для каждого порта своя: Fa0/0 -255.255.255.0, Fa0/1 - 255.255.0.0, Fa1/0 - 255.255.255.252.

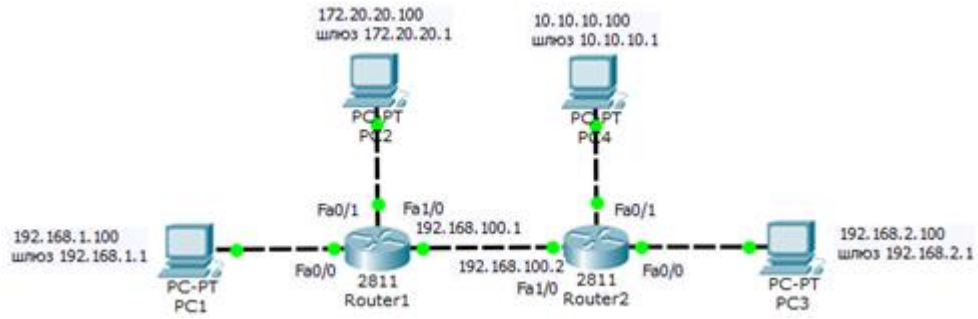


Рис. 30. Связь сетей посредством маршрутизаторов

Далее соединим маршрутизаторы между собой нам потребуется добавить к маршрутизатору интерфейсную плату NM-1FE-TX (NM – Network module, 1FE – содержит один порт FastEthernet, TX – поддерживает 10/100MBase-TX). Чтобы это сделать перейдите к окну конфигурации маршрутизатора0, выключите его, щелкнув на кнопке питания. После этого перетяните интерфейсную плату NM-1FE-TX в разъем маршрутизатора (рис. 31). После того как карта добавлена, еще раз щелкните по тумблеру маршрутизатора, чтобы включить его. Повторите аналогичные действия со вторым маршрутизатором.

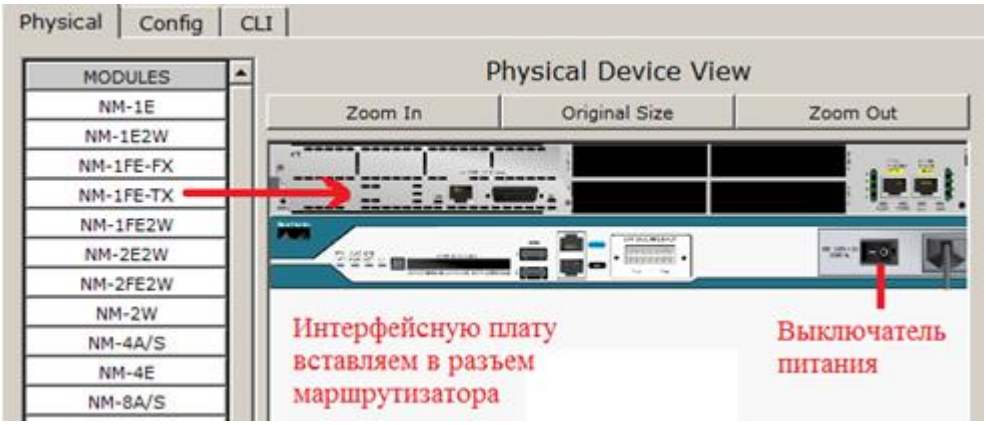


Рис. 31. Вставляем интерфейсную плату в маршрутизатор

Постановка задачи

Нам требуется произвести необходимые настройки для того, чтобы все ПК могли общаться друг с другом, то есть, необходимо обеспечить доступность компьютеров из разных сетей между собой.

Настройка маршрутизации (маршрута по умолчанию)

В настоящий момент если мы отправим с компьютера PC1 с IP адресом 192.168.1.100 пакет на интерфейс Fa1/0 с IP адресом

192.168.100.2 маршрутизатора R2, то ICMP пакет слева дойдет до этого маршрутизатора, но при отправке ICMP пакетов в обратном направлении с адреса 192.168.100.2 на адрес 192.168.1.100 возникнет проблема. Дело в том, что маршрутизатор R2 не имеет в своей таблице маршрутизации информации о сети 172.20.20.0, так как шлюз по умолчанию мы еще не прописывали и маршрутизатор R2 не знает, куда отправлять ответы на запрос. В небольших сетях самым простым способом настроить маршрутизацию, является добавление маршрута по умолчанию. Для того чтобы это сделать выполните на маршрутизаторе R1 в режиме конфигурирования следующие команды (рис. 32).

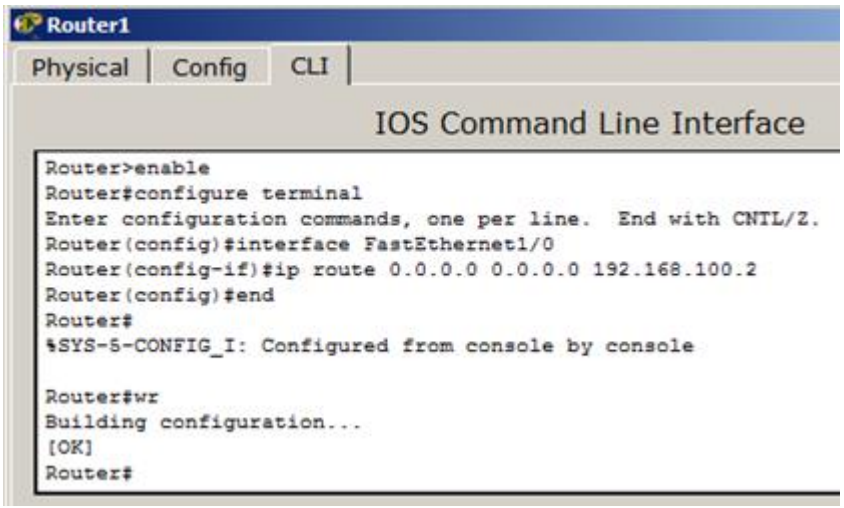


Рис. 32. Настройка маршрута по умолчанию на R1

Примечание. В этих командах первая группа цифр 0.0.0.0 обозначают IP адрес сети назначения, следующая группа цифр 0.0.0.0 обозначает её маску, а последние цифры – 192.168.100.2 это IP адрес интерфейса, на который необходимо передать пакеты, чтобы попасть в данную сеть. Если мы указываем в качестве адреса сети 0.0.0.0 с маской 0.0.0.0, то данный маршрут становится маршрутом по умолчанию, и все пакеты, адреса назначения которых, прямо не указаны в таблице маршрутизации будут отправлены на него.

На правом маршрутизаторе R2 поступаем аналогично (рис. 33).

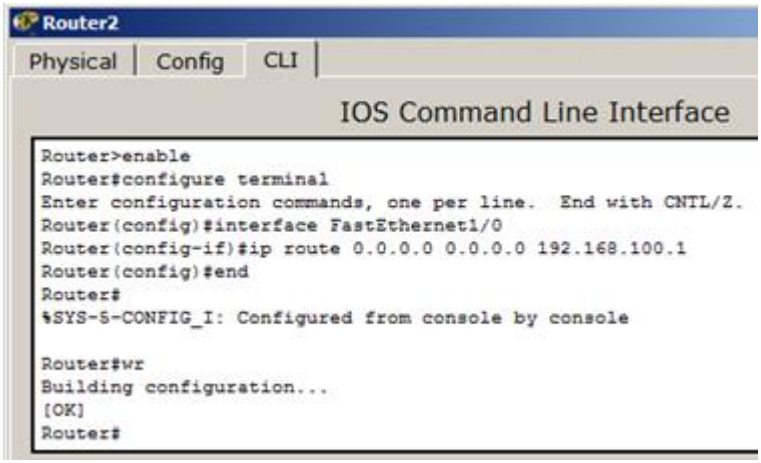


Рис. 33. Настройка маршрута по умолчанию на R2

Отправим с компьютера PC1 с IP адресом 192.168.1.100 пакет на интерфейс Fa1/0 с IP адресом 192.168.100.2 маршрутизатора R2 и посмотрим, что изменилось (рис. 34).

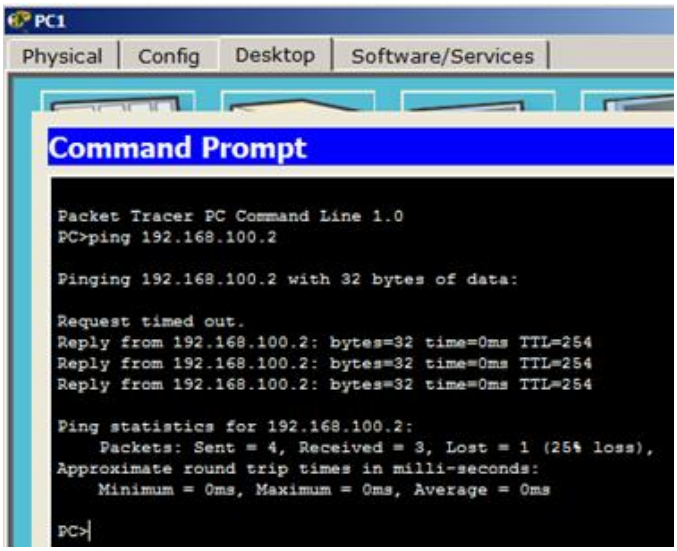


Рис. 34. С компьютера PC1 с IP адресом 192.168.1.100 успешно пингуем интерфейс Fa1/0 с IP адресом 192.168.100.2 маршрутизатора R2

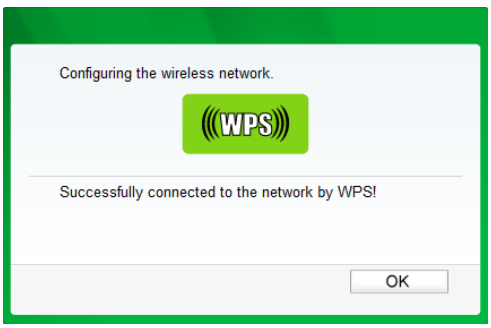


Рис. 32. ПК к сети Итернет подключен

Практическая работа 13

Тема: Динамическая настройка маршрутизации на основе протоколов RIP, EIGRP, OSPF и BGP.

Цель: приобрести навыки по обеспечению безопасности сети на основе динамической маршрутизации протоколов RIP, EIGRP, OSPF и BGP.

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Теоретическая часть:

Как настроить RIP на маршрутизаторе Cisco. RIP (Routing Information Protocol) — это один из протоколов маршрутизации, которые необходимо понять, если вы хотите пройти экзамен Cisco CCNA. Если вы не знаете, как работает RIP, я предлагаю сначала прочитать предыдущую статью, где я объясню, как работает RIP. В этой статье я покажу вам, как настроить RIP на маршрутизаторе Cisco. Вот топология, которую я буду использовать:

Рис. 1. Топология исследуемой сети

Выше мы видим 3 маршрутизатора под названием R1, R2 и R3. У нас несколько сетей, поэтому будет возможность объявлять через RIP. Сначала давайте настроим все интерфейсы:

Ход работы настройка R1 маршрутизатора

```
R1>enable
R1#configure terminal
R1(config)#interface fastEthernet 0/0
R1(config-if)#no shutdown
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface fastEthernet 1/0
```

R1(config-if)#ip address 192.168.12.1 255.255.255.0

R1(config-if)#no shutdown

Настройка R2 маршрутизатора

R2>enable

R2#configure terminal

R2(config)#interface fastEthernet 0/0

R2(config-if)#no shutdown

R2(config-if)#ip address 192.168.12.2 255.255.255.0

R2(config-if)#exit

R2(config)#interface FastEthernet 1/0

R2(config-if)#no shutdown

R2(config-if)#ip address 192.168.23.2 255.255.255.0

R2(config-if)#exit

Настройка R3 маршрутизатора

R3>enable

R3#configure terminal

R3(config)#interface fastEthernet 0/0

R3(config-if)#no shutdown

R3(config-if)#ip address 172.16.2.3 255.255.255.0

R3(config-if)#exit

R3(config)#interface fastEthernet 1/0

R3(config-if)#no shutdown

R3(config-if)#ip address 192.168.23.3 255.255.255.0

R3(config-if)#exit

Прежде чем продолжить RIP, мы проверим таблицы маршрутизации:

Рис. 2. Результат конфигурации маршрутизатора

R1(config)#router rip

R1(config-router)#network 192.168.12.0
R1(config-router)#network 172.16.1.0
R2(config)#router rip
R2(config-router)#network 192.168.12.0
Мы используем команду router rip для перехода к конфигурации RIP. Следующим шагом является использование команды, которая делает две вещи. Давайте увеличим R1 и R2, чтобы я мог объяснить это немного больше: network

На R2 я использовал только команду network. Это означает, что R2 поместит 192.168.12.0/24 в базу данных RIP и отправит обновления RIP на свой интерфейс FastEthernet 0/0. В настоящий момент он не будет объявлять сеть 192.168.23.0/24 в RIP и не будет отправлять обновления RIP на интерфейс FastEthernet 1/0.
Вместо того, чтобы вводить show ip route вы также можете использовать show ip route rip. Это покажет только информацию RIP в таблице маршрутизации. Как вы можете видеть, R1 не узнал ничего от R2. Это связано с тем, что сеть 192.168.23.0/24 не объявлена на R2.
R2 узнал сеть 172.16.0.0/16. Почему мы видим 172.16.0.0/16, а не 172.16.1.0/24? Имейте в виду, что по умолчанию в RIP работает версия 1, которая является классовой. Он НЕ отправляет маску подсети вместе с обновлениями маршрутизации. Поскольку 172.16.1.0/24 находится в диапазоне сетей класса B, она будет объявляться как 172.16.0.0/16.
Я настрою RIP версию 2 позже, чтобы вы могли видеть разницу между бесклассовой и классовой версиями протокола.
В любом случае давайте посмотрим, можем ли мы сделать так, чтобы R1 узнал о 192.168.23.0/24:
Давайте проверим таблицы маршрутизации R1 и R2!
Вместо того, чтобы вводить show ip route вы также можете

использовать show ip route rip. Это покажет только информацию RIP в таблице маршрутизации. Как вы можете видеть, R1 не узнал ничего от R2. Это связано с тем, что сеть 192.168.23.0/24 не объявлена на R2. R2 узнал сеть 172.16.0.0/16. Почему мы видим 172.16.0.0/16, а не 172.16.1.0/24? Имейте в виду, что по умолчанию в RIP работает версия 1, которая является классовой. Он НЕ отправляет маску подсети вместе с обновлениями маршрутизации. Поскольку 172.16.1.0/24 находится в диапазоне сетей класса B, она будет объявляться как 172.16.0.0/16.

BGP (англ. Border Gateway Protocol, протокол пограничного шлюза)

Это основной протокол динамической маршрутизации в интернете. Протокол BGP отличается от других протоколов динамической маршрутизации, информация о маршруте передается между отдельными маршрутизаторами, а не между целыми маршрутизаторами предназначен для переключения между автономными системами и по этой причине, помимо информации о маршрутах в сети, к автономным системам относятся также несет информацию о маршрутах.

Рис. 3. Топология сети, построенная по протоколу BGP

Порядок выполнения работы для сети, построенной по протоколу BGP

Введите IP адреса к компьютерам по топологии, показанной на рисунке 3.

BGP-100(config)#router bgp 100

BGP-100(config-router)#ne

```
BGP-100(config-router)#nei
BGP-100(config-router)#neighbor 1.1.1.0 mas
BGP-100(config-router)#neighbor 1.1.1.0 ma
BGP-100(config-router)#neighbor 1.1.1.2 re
BGP-100(config-router)#neighbor 1.1.1.2 remote-as 400
BGP-100(config-router)#net
BGP-100(config-router)#network 192.168.2.0 mas
BGP-100(config-router)#network 192.168.2.0 mask 255.255.255.0
BGP-100(config-router)#net
BGP-100(config-router)#network 1.1.1.0 ,as
BGP-100(config-router)#network 1.1.1.0 m
BGP-100(config-router)#network 1.1.1.0 mask s
BGP-100(config-router)#network 1.1.1.0 mask 255.255.255.0
BGP-100(config-router)#do wr
Building configuration...
[OK]
BGP-100(config-router)#%BGP-5-ADJCHANGE: neighbor 1.1.1.2 Up
```

BGP-200(config)#router bgp 200

```
BGP-200(config-router)#ne
BGP-200(config-router)#nei
BGP-200(config-router)#neighbor 2.2.2.2 re
BGP-200(config-router)#neighbor 2.2.2.2 remote-as 400
BGP-200(config-router)#net
BGP-200(config-router)#network 192.168.3.0 ma
BGP-200(config-router)#network 192.168.3.0 mask 255.255.255.0
BGP-200(config-router)#net
BGP-200(config-router)#network 2.2.2.0 mas
BGP-200(config-router)#network 2.2.2.0 mask 255.255.255.0
BGP-200(config-router)#do wr
```

Building configuration...

[OK]

BGP-200(config-router)#%BGP-5-ADJCHANGE: neighbor 2.2.2.2 Up

BGP-300(config)#router bgp 300

BGP-300(config-router)#nei

BGP-300(config-router)#neighbor 3.3.3.2 re

BGP-300(config-router)#neighbor 3.3.3.2 remote-as 400

BGP-300(config-router)#%BGP-5-ADJCHANGE: neighbor 3.3.3.2 Up

BGP-300(config-router)#net

BGP-300(config-router)#network 192.168.4.0 mas

BGP-300(config-router)#network 192.168.4.0 mask 255.255.255.0

BGP-300(config-router)#net

BGP-300(config-router)#network 3.3.3.0 ,as

BGP-300(config-router)#network 3.3.3.0 mas

BGP-300(config-router)#network 3.3.3.0 mask 255.255.255.0

BGP-300(config-router)#

Рис. 4. Результат конфигурации маршрутизатора с помощи протокола BGP

Отчет о лабораторной работе должен состоять из:

- нумерация и название дела;
- цель работы;
- задание;
- Изображение сетевой модели в Cisco Packet Tracer;
- а распределение IP-адресов в сети, схема подключения (интерфейсы
- нумерации), содержащие описание;
- состоит из списков конфигураций элементов сети

Контрольные вопросы

1. По какому алгоритму работает протокол RIP?
2. На основании чего протокол RIP вычисляет метрику?
3. Каково административное расстояние протокола RIP?
4. В чем разница между протоколами RIPv1 и RIPv2?
5. По какому алгоритму работает протокол OSPF?
6. По какому алгоритму работает протокол EIGRP?
7. Каковы преимущества протокола EIGRP?
8. Что вы подразумеваете под административной дистанцией?
9. Назовите типы протоколов динамической маршрутизации?
10. В чем разница между динамической маршрутизацией и статической маршрутизацией?
11. Опишите протокол внешней маршрутизации BGP.
12. Протокол BGP сколько административное расстояние.
13. На основе какого алгоритма работает протокол BGP.
14. Что вы подразумеваете под автономной системой?

Практическая работа 2

Тема: Настройка базовых параметров маршрутизатора с помощью интерфейса командной строки (CLI) системы Cisco IOS

Цель: настроить базовые параметры маршрутизатора с помощью интерфейса

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задание:

Топология

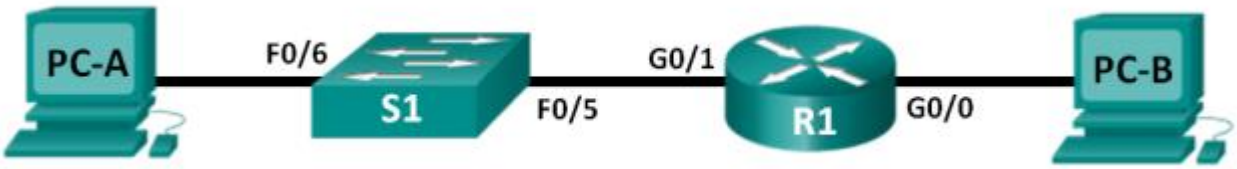


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Настройка топологии и инициализация устройств

1: Подключите кабели в сети в соответствии с топологией.

a. Подключите устройства в соответствии с топологией и проведите все необходимые кабели.

b. Включите все устройства в топологии.

2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Настройка устройств и проверка подключения

1: Настройте интерфейсы ПК.

a. На PC-A настройте IP-адрес, маску подсети и параметры шлюза по умолчанию.

b. На PC-B настройте IP-адрес, маску подсети и параметры шлюза по умолчанию.

2: Настройте маршрутизатор.

a. Подключитесь к маршрутизатору с помощью консольного подключения и активируйте привилегированный режим.

Router> enable Router#

b. Войдите в режим глобальной конфигурации маршрутизатора.

Router# config terminal

Router(config)#

c. Назначьте маршрутизатору имя устройства.

Router(config)# hostname R1

d. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовать введённые команды так, как если бы они были узлами.

R1(config)# no ip domain-lookup e.

Пароли должны содержать не менее 10 символов.

R1(config)# security passwords min-length 10

Укажите способы усиления защиты паролей, кроме установки минимальной длины.

f. Назначьте cisco12345 в качестве зашифрованного пароля привилегированного режима.

R1(config)# enable secret cisco12345

g. В качестве пароля консоли назначьте ciscoconpass, установите лимит времени, активируйте вход в систему и добавьте команду logging synchronous. Команда logging synchronous позволяет синхронизировать выходные данные отладки и программного обеспечения Cisco IOS, а также запрещает этим сообщениям прерывать ввод команд с клавиатуры.

```
R1(config)# line con 0
R1(config-line)# password ciscoconpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
R1(config-line)# exit
R1(config)#
```

h. В качестве пароля vty назначьте ciscovtypass, установите лимит времени, активируйте вход в систему и добавьте команду logging synchronous.

R1(config)# line vty 0 4

```
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
R1(config-line)# exit
R1(config)#
```

i. Зашифруйте незашифрованные пароли.

R1(config)# service password-encryption j. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

R1(config)# banner motd #Unauthorized access prohibited!#

k. Настройте IP-адрес и описание интерфейса. Активируйте оба интерфейса на маршрутизаторе.

```
R1(config)# int g0/0
R1(config-if)# description Connection to PC-B
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# int g0/1
R1(config-if)# description Connection to S1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# exit
R1#
```

l. Настройте часы на маршрутизаторе. R1# clock set 17:00:00 18 Feb 2013

m. Сохраните файл текущей конфигурации в файл загрузочной конфигурации.

R1# copy running-config startup-config

3. Проверьте сетевое соединение.

4. Настройте маршрутизатор для доступа по протоколу SSH.

Отображение данных маршрутизатора

1: Установите сеанс SSH с маршрутизатором R1. На компьютере PC-B с помощью Tera Term создайте сеанс SSH с маршрутизатором R1 по IP-адресу 192.168.0.1 и войдите в систему, используя имя пользователя admin и пароль adminpass1.

2: Получите основные данные об аппаратном и программном обеспечении.

a. Используйте команду show version, чтобы ответить на вопросы о маршрутизаторе. Как называется образ IOS, под управлением которой работает маршрутизатор?

Какой объём энергонезависимого ОЗУ (NVRAM) имеет маршрутизатор?

Какой объём флеш-памяти имеет маршрутизатор?

b. Зачастую команды show могут выводить несколько экранов данных. Фильтрация выходных данных позволяет пользователю отображать лишь нужные разделы выходных данных. Чтобы включить команду фильтрации, после команды show введите прямую черту (|), после которой следует ввести параметр и выражение фильтрации. Чтобы отобразить все строки выходных данных, которые содержат выражение фильтрации, можно согласовать выходные данные с оператором фильтрации с помощью ключевого слова include. Настройте фильтрацию для команды show version и используйте команду show version | include register, чтобы ответить на следующий вопрос.

Отобразите загрузочную конфигурацию. Выполните команду show startup-config на маршрутизаторе, чтобы ответить на следующие вопросы. Как пароли представлены в выходных данных?

Используйте show startup-config | begin vty. Что происходит в результате выполнения этой команды?

4: Отобразите таблицу маршрутизации на маршрутизаторе. Выполните команду show ip route на маршрутизаторе, чтобы ответить на следующие вопросы. Какой код используется в таблице маршрутизации для отображения сети с прямым подключением?

Сколько записей маршрутов закодированы с кодом C в таблице маршрутизации? _____ Шаг 5: Отобразите на маршрутизаторе сводный список интерфейсов. Выполните команду show ip interface brief на

маршрутизаторе, чтобы ответить на следующий вопрос. Какая команда позволяет изменить состояние портов Gigabit Ethernet с DOWN на UP?

Настройка протокола IPv6 и проверка подключения

1: Назначьте IPv6-адреса интерфейсу G0/0 маршрутизатора R1 и включите IPv6- маршрутизацию.

Примечание. Назначение IPv6-адрес в дополнение к IPv4-адресам на интерфейсе называют двойным стеком, поскольку активным является как протокол IPv4, так и протокол IPv6. Благодаря включению IPv6-маршрутизации одноадресной передачи на маршрутизаторе R1 компьютер PC-B получает сетевой IPv6-префикс для интерфейса G0/0 маршрутизатора R1 и может автоматически настраивать свой IPv6-адрес и шлюз по умолчанию.

a. Назначьте интерфейсу G0/0 глобальный индивидуальный IPv6-адрес, в дополнение к индивидуальному адресу на интерфейсе назначьте локальный адрес канала и включите IPv6- маршрутизацию. R1# configure terminal

```
R1(config)# interface g0/0
R1(config-if)# ipv6 address 2001:db8:acad:a::1/64
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# ipv6 unicast-routing
R1(config)# exit
```

b. Чтобы проверить параметры IPv6 на маршрутизаторе R1 выполните команду show ipv6 int brief. Если интерфейсу G0/1 не назначен IPv6-адрес, то почему он отображается как [up/up] (ВКЛ/ВКЛ)?

c. На компьютере PC-B выполните команду ipconfig, чтобы проверить настройки IPv6. Какой IPv6-адрес назначен компьютеру PC-B?

Какой шлюз по умолчанию назначен компьютеру PC-B?

От компьютера PC-B отправьте эхо-запрос на локальный адрес канала шлюза по умолчанию маршрутизатора R1. Был ли запрос успешным?

От компьютера PC-B отправьте эхо-запрос на индивидуальный IPv6-адрес маршрутизатора R1 2001:db8:acad:a::1. Был ли запрос успешным?

Критерии оценки:

«5» (отлично): выполнены все задания самостоятельной работы без ошибок.

«4» (хорошо): выполнены все задания самостоятельной работы с замечаниями.

«3» (удовлетворительно): выполнены не все задания самостоятельной работы, имеются замечания.

«2» (не зачтено): студент не выполнил или выполнил неправильно задания самостоятельной работы.

Практическая работа 3

Тема: Развертывание коммутируемой сети с резервными каналами

Цели: Развернуть коммутируемую сеть с резервными каналами

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задачи

Часть 1. Создание сети и настройка базовых параметров устройств

Часть 2. Настройка сетей VLAN, native VLAN и транковых каналов

Часть 3. Настройка корневого моста и проверка сходимости PVST+

Исходные данные/сценарий

Протокол spanning-tree для VLAN (PVST) является проприетарным протоколом Cisco. По умолчанию коммутаторы Cisco используют

протокол PVST. Rapid PVST+ (IEEE 802.1w) является усовершенствованной версией PVST+ и обеспечивает более быстрые вычисления протокола spanning-tree и более быструю сходимость после изменений топологии 2 уровня. Rapid PVST+ определяет три состояния порта: отбрасывание, обучение и пересылка, а также представляет ряд нововведений в целях оптимизации производительности сети.

В этой лабораторной работе вам предстоит настроить основной и вспомогательный корневые мосты, изучить сходимость PVST+, настроить Rapid PVST+ и сравнить его сходимость с PVST+. Кроме того, необходимо будет настроить пограничные порты для немедленного перехода в состояние пересылки с помощью PortFast, а также блокировать пересылку BDPU из пограничных портов, используя BDPU guard.

Примечание. В данной лабораторной работе содержится минимальный набор команд, необходимых для настройки. Список требуемых команд приведен в приложении А. Проверьте свои знания: настройте устройства, не обращаясь к информации, приведённой в приложении.

Примечание. В лабораторной работе используются коммутаторы Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9). Допускается использование других моделей коммутаторов и других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и их результаты могут отличаться от приведённых в описании лабораторных работ.

Примечание. Убедитесь, что прежние настройки коммутаторов были удалены, и они не содержат конфигурации загрузки. Если вы не уверены в этом, обратитесь к инструктору.

Топология

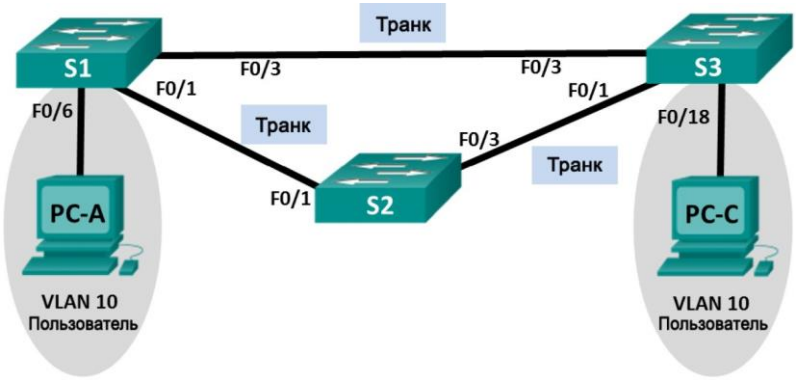


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
S1	VLAN 99	192.168.1.11	255.255.255.0
S2	VLAN 99	192.168.1.12	255.255.255.0
S3	VLAN 99	192.168.1.13	255.255.255.0
PC-A	NIC	192.168.0.2	255.255.255.0
PC-C	NIC	192.168.0.3	255.255.255.0

Назначения сети VLAN

VLAN	Имя
10	Пользователь
99	Management (Руководство)

Необходимые ресурсы:

- 3 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Создание сети и настройка базовых параметров устройств

В первой части вам предстоит настроить топологию сети и настроить базовые параметры, такие как IP-адреса интерфейсов, статическая маршрутизация, доступ к устройствам и пароли.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузку коммутаторов.

Шаг 4: Настройте базовые параметры каждого коммутатора.

a. Отключите поиск DNS.

Присвойте имена устройствам в соответствии с топологией.

a. Установите **cisco** в качестве пароля консоли и виртуального терминала VTY и включите вход по паролю.

b. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

c. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд. f. Отключите все порты коммутатора.

g. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Часть 2: Настройка сетей VLAN, native VLAN и транковых каналов

В части 2 рассматриваются создание сетей VLAN, назначения сетям VLAN портов коммутатора, настройка транковых портов и изменение native VLAN для всех коммутаторов.

Примечание. Команды, необходимые для выполнения заданий второй части лабораторной работы, приведены в приложении A. Чтобы проверить свои знания, попробуйте настроить сети VLAN, native VLAN и транковые каналы, не обращаясь к приложению.

Шаг 1: Создайте сети VLAN.

Используйте соответствующие команды, чтобы создать сети VLAN 10 и 99 на всех коммутаторах. Присвойте сети VLAN 10 имя **User**, а сети VLAN 99 — имя **Management**.

S1(config)# **vlan 10**

S1(config-vlan)# **name User**

S1(config-vlan)# **vlan 99**

S1(config-vlan)# **name Management**

S2(config)# **vlan 10** S2(config-vlan)# **name User**

S2(config-vlan)# **vlan 99**

S2(config-vlan)# **name Management**

S3(config)# **vlan 10**

S3(config-vlan)# **name User**

S3(config-vlan)# **vlan 99**

S3(config-vlan)# **name Management**

Шаг 2: Переведите пользовательские порты в режим доступа и назначьте сети VLAN.

Для интерфейса F0/6 S1 и интерфейса F0/18 S3 включите порты, настройте их в качестве портов доступа и назначьте их сети VLAN 10.

Шаг 3: Настройте транковые порты и назначьте их сети native VLAN 99.

Для портов F0/1 и F0/3 на всех коммутаторах включите порты, настройте их в качестве транковых и назначьте их сети native VLAN 99.

Шаг 4: Настройте административный интерфейс на всех коммутаторах.

Используя таблицу адресации, настройте на всех коммутаторах административный интерфейс с соответствующим IP-адресом.

Шаг 5: Проверка конфигураций и возможности подключения.

Используйте команду **show vlan brief** на всех коммутаторах, чтобы убедиться в том, что все сети VLAN внесены в таблицу VLAN и назначены правильные порты.

Используйте команду **show interfaces trunk** на всех коммутаторах, чтобы проверить транковые интерфейсы.

Используйте команду **show running-config** на всех коммутаторах, чтобы проверить все остальные конфигурации.

Какие настройки используются для режима протокола spanning-tree на коммутаторах Cisco?

_____

_____

Проверьте подключение между PC-A и PC-C. Удалось ли выполнить эхо-запрос? _____

Если эхо-запрос выполнить не удалось, следует выполнять отладку до тех пор, пока проблема не будет решена.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Часть 3: Настройка корневого моста и проверка сходимости PVST+

В части 3 вам предстоит определить корневой мост по умолчанию в сети, назначить основной и вспомогательный корневые мосты и использовать команду **debug** для проверки сходимости PVST+.

Примечание. Команды, необходимые для выполнения заданий третьей части лабораторной работы, приведены в приложении A. Проверьте свои знания: попробуйте настроить корневой мост, не обращаясь к приложению.

Шаг 1: Определите текущий корневой мост.

С помощью какой команды пользователи определяют состояние протокола spanning-tree коммутатора Cisco Catalyst для всех сетей VLAN? Запишите команду в строке ниже.

_____

_____ Выполните команду на всех трех коммутаторах, чтобы ответить на следующие вопросы:

Примечание. На каждом коммутаторе доступно три экземпляра протокола spanning-tree. По умолчанию на коммутаторах Cisco используется конфигурация STP PVST+, которая позволяет создавать отдельный экземпляр протокола spanning-tree для каждой сети VLAN (VLAN 1 и все остальные настроенные пользователем сети VLAN).

Какой приоритет моста используется для коммутатора S1 в сети VLAN 1? _____

Какой приоритет моста используется для коммутатора S2 в сети VLAN 1? _____

Какой приоритет моста используется для коммутатора S3 в сети VLAN 1? _____

Какой коммутатор является корневым мостом? _____ Почему этот коммутатор выбран в качестве корневого моста?

_____

_____

Шаг 2: Настройте основной и вспомогательный корневые мосты для всех существующих сетей VLAN.

При выборе корневого моста (коммутатора) по MAC-адресу может образоваться условно оптимальная конфигурация. В этой лабораторной работе вам необходимо настроить коммутатор S2 в качестве корневого моста и коммутатор S1 — в качестве вспомогательного корневого моста.

a. Настройте коммутатор S2 в качестве основного корневого моста для всех существующих сетей VLAN. Запишите команду в строке ниже.

_____

_____

b. Настройте коммутатор S1 в качестве вспомогательного корневого моста для всех существующих сетей VLAN. Запишите команду в строке ниже.

_____

_____ Используйте команду **show spanning-tree** для ответа на следующие вопросы:

Какой приоритет моста используется для коммутатора S1 в сети VLAN 1? _____ Какой приоритет моста используется для коммутатора S2 в сети VLAN 1? _____ Какой интерфейс в сети находится в состоянии блокировки?

_____

Шаг 3: Измените топологию 2 уровня и проверьте сходимость.

Чтобы проверить сходимость PVST+, необходимо создать изменение топологии 2 уровня, используя команду **debug** для отслеживания событий протокола spanning-tree.

a. Выполните команду **debug spanning-tree events** в привилегированном режиме на коммутаторе S3.

S3# **debug spanning-tree events**

Spanning Tree event debugging is on

b. Измените топологию, отключив интерфейс F0/1 на коммутаторе S3.

S3(config)# **interface f0/1**

S3(config-if)# **shutdown**

*Mar 1 00:58:56.225: STP: VLAN0001 new root port Fa0/3, cost 38

*Mar 1 00:58:56.225: STP: VLAN0001 Fa0/3 -> listening

*Mar 1 00:58:56.225: STP[1]: Generating TC trap for port FastEthernet0/1

*Mar 1 00:58:56.225: STP: VLAN0010 new root port Fa0/3, cost 38

*Mar 1 00:58:56.225: STP: VLAN0010 Fa0/3 -> listening

*Mar 1 00:58:56.225: STP[10]: Generating TC trap for port FastEthernet0/1

*Mar 1 00:58:56.225: STP: VLAN0099 new root port Fa0/3, cost 38

*Mar 1 00:58:56.225: STP: VLAN0099 Fa0/3 -> listening

*Mar 1 00:58:56.225: STP[99]: Generating TC trap for port FastEthernet0/1

*Mar 1 00:58:56.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down

*Mar 1 00:58:56.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down

*Mar 1 00:58:58.214: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down *Mar 1 00:58:58.230: STP: VLAN0001 sent Topology Change Notice on Fa0/3

*Mar 1 00:58:58.230: STP: VLAN0010 sent Topology Change Notice on Fa0/3

*Mar 1 00:58:58.230: STP: VLAN0099 sent Topology Change Notice on Fa0/3

*Mar 1 00:58:59.220: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down *Mar 1 00:59:11.233: STP: VLAN0001 Fa0/3 -> learning

*Mar 1 00:59:11.233: STP: VLAN0010 Fa0/3 -> learning

*Mar 1 00:59:11.233: STP: VLAN0099 Fa0/3 -> learning

*Mar 1 00:59:26.240: STP[1]: Generating TC trap for port FastEthernet0/3

*Mar 1 00:59:26.240: STP: VLAN0001 Fa0/3 -> forwarding

*Mar 1 00:59:26.240: STP[10]: Generating TC trap for port FastEthernet0/3

*Mar 1 00:59:26.240: STP: VLAN0010 sent Topology Change Notice on Fa0/3

*Mar 1 00:59:26.240: STP: VLAN0010 Fa0/3 -> forwarding

*Mar 1 00:59:26.240: STP[99]: Generating TC trap for port FastEthernet0/3

*Mar 1 00:59:26.240: STP: VLAN0099 Fa0/3 -> forwarding

*Mar 1 00:59:26.248: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

*Mar 1 00:59:26.248: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

Примечание. Прежде чем продолжить, исходя из выходных данных команды **debug** убедитесь, что все сети VLAN на интерфейсе F0/3 перешли в состояние пересылки, после чего используйте команду **no debug spanning-tree events**, чтобы остановить вывод данных командой **debug**.

Через какие состояния портов проходит каждая сеть VLAN на интерфейсе F0/3 в процессе схождения сети?

_____

_____

Используя временную метку из первого и последнего сообщений отладки STP, рассчитайте время (округляя до секунды), которое потребовалось для схождения сети. **Рекомендация**. Формат временной метки сообщений отладки: чч.мм.сс.мс

_____

_____

Часть 4: Настройка Rapid PVST+, PortFast, BPDU Guard и проверка сходимости

В части 4 вам предстоит настроить Rapid PVST+ на всех коммутаторах. Вам необходимо будет настроить функции PortFast и BPDU guard на всех портах доступа, а затем использовать команду **debug** для проверки сходимости Rapid PVST+.

Примечание. Команды, необходимые для выполнения заданий в четвертой части, приведены в приложении A. Проверьте свои знания. Для этого попробуйте настроить Rapid PVST+, PortFast и BPDU guard, не обращаясь к материалам в приложении.

Шаг 1: Настройте Rapid PVST+.

a. Настройте S1 для использования Rapid PVST+. Запишите команду в строке ниже.

_____

_____ b. Настройте S2 и S3 для Rapid PVST+.

c. Проверьте конфигурации с помощью команды **show running-config | include spanning-tree mode**.

S1# **show running-config | include spanning-tree mode** spanning-tree mode rapid-pvst

S2# **show running-config | include spanning-tree mode** spanning-tree mode rapid-pvst

S3# **show running-config | include spanning-tree mode** spanning-tree mode rapid-pvst

Шаг 2: Настройте PortFast и BPDU Guard на портах доступа.

PortFast является функцией протокола spanning-tree, которая переводит порт в состояние пересылки сразу после его включения. Эту функцию рекомендуется использовать при подключении узлов, чтобы они могли начать обмен данными по сети VLAN немедленно, не дожидаясь протокола spanning-tree.

Чтобы запретить портам, настроенным с использованием PortFast, пересылать кадры BPDU, которые могут изменить топологию протокола spanning-tree, можно включить функцию BPDU guard. После получения BPDU функция BPDU Guard отключает порт, настроенный с помощью функции PortFast.

a. Настройте F0/6 на S1 с помощью функции PortFast. Запишите команду в строке ниже.

_____

_____

b. Настройте F0/6 на S1 с помощью функции BPDU Guard. Запишите команду в строке ниже.

_____

_____

c. Глобально настройте все нетранковые порты на коммутаторе S3 с помощью функции PortFast. Запишите команду в строке ниже.

_____

_____

d. Глобально настройте все нетранковые порты на коммутаторе S3 с помощью функции BPDU. Запишите команду в строке ниже.

_____

_____

Шаг 3: Проверьте сходимость Rapid PVST+.

a. Выполните команду **debug spanning-tree events** в привилегированном режиме на коммутаторе S3.

b. Измените топологию, отключив интерфейс F0/1 на коммутаторе S3.

S3(config)# **interface f0/1** S3(config-if)# **no shutdown**

*Mar 1 01:28:34.946: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up

*Mar 1 01:28:37.588: RSTP(1): initializing port Fa0/1

*Mar 1 01:28:37.588: RSTP(1): Fa0/1 is now designated

*Mar 1 01:28:37.588: RSTP(10): initializing port Fa0/1

*Mar 1 01:28:37.588: RSTP(10): Fa0/1 is now designated

*Mar 1 01:28:37.588: RSTP(99): initializing port Fa0/1

*Mar 1 01:28:37.588: RSTP(99): Fa0/1 is now designated

*Mar 1 01:28:37.597: RSTP(1): transmitting a proposal on Fa0/1

*Mar 1 01:28:37.597: RSTP(10): transmitting a proposal on Fa0/1

*Mar 1 01:28:37.597: RSTP(99): transmitting a proposal on Fa0/1

*Mar 1 01:28:37.597: RSTP(1): updt roles, received superior bpdu on Fa0/1

*Mar 1 01:28:37.597: RSTP(1): Fa0/1 is now root port

*Mar 1 01:28:37.597: RSTP(1): Fa0/3 blocked by re-root

*Mar 1 01:28:37.597: RSTP(1): synced Fa0/1

*Mar 1 01:28:37.597: RSTP(1): Fa0/3 is now alternate

*Mar 1 01:28:37.597: RSTP(10): updt roles, received superior bpdu on Fa0/1

*Mar 1 01:28:37.597: RSTP(10): Fa0/1 is now root port

*Mar 1 01:28:37.597: RSTP(10): Fa0/3 blocked by re-root

*Mar 1 01:28:37.597: RSTP(10): synced Fa0/1

*Mar 1 01:28:37.597: RSTP(10): Fa0/3 is now alternate

*Mar 1 01:28:37.597: RSTP(99): updt roles, received superior bpdu on Fa0/1

*Mar 1 01:28:37.605: RSTP(99): Fa0/1 is now root port

*Mar 1 01:28:37.605: RSTP(99): Fa0/3 blocked by re-root

*Mar 1 01:28:37.605: RSTP(99): synced Fa0/1

*Mar 1 01:28:37.605: RSTP(99): Fa0/3 is now alternate

*Mar 1 01:28:37.605: STP[1]: Generating TC trap for port FastEthernet0/1

*Mar 1 01:28:37.605: STP[10]: Generating TC trap for port FastEthernet0/1

*Mar 1 01:28:37.605: STP[99]: Generating TC trap for port FastEthernet0/1

*Mar 1 01:28:37.622: RSTP(1): transmitting an agreement on Fa0/1 as a response to a proposal

*Mar 1 01:28:37.622: RSTP(10): transmitting an agreement on Fa0/1 as a response to a

proposal

*Mar 1 01:28:37.622: RSTP(99): transmitting an agreement on Fa0/1 as a response to a

proposal

*Mar 1 01:28:38.595: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Используя временную метку из первого и последнего сообщений отладки RSTP, рассчитайте время, которое потребовалось для схождения сети.

_____

_____

Вопросы на закрепление

1. В чем заключается главное преимущество Rapid PVST+?

_____

_____

2. Каким образом настройка порта с помощью функции PortFast обеспечивает более быстрое схождение?

_____

_____

3. Какую защиту обеспечивает функция BPDU Guard?

_____

_____

Приложение А. Команды настройки коммутатора

Коммутатор S1

S1(config)# **vlan 10**

S1(config-vlan)# **name User**

S1(config-vlan)# **vlan 99**

S1(config-vlan)# **name Management**

S1(config-vlan)# **exit**

S1(config)# **interface f0/6** S1(config-if)# **no shutdown**

S1(config-if)# **switchport mode access**

S1(config-if)# **switchport access vlan 10**

S1(config-if)# **interface f0/1**

S1(config-if)# **no shutdown**

S1(config-if)# **switchport mode trunk**

S1(config-if)# **switchport trunk native vlan 99**

S1(config-if)# **interface f0/3**

S1(config-if)# **no shutdown**

S1(config-if)# **switchport mode trunk**

S1(config-if)# **switchport trunk native vlan 99**

S1(config-if)# **interface vlan 99**

S1(config-if)# **ip address 192.168.1.11 255.255.255.0**

S1(config-if)# **exit**

S1(config)# **spanning-tree vlan 1,10,99 root secondary**

S1(config)# **spanning-tree mode rapid-pvst**

S1(config)# **interface f0/6**

S1(config-if)# **spanning-tree portfast**

S1(config-if)# **spanning-tree bpduguard enable**

Коммутатор S2

S2(config)# **vlan 10**

S2(config-vlan)# **name User**

S2(config-vlan)# **vlan 99**

S2(config-vlan)# **name Management**

S2(config-vlan)# **exit**

S2(config)# **interface f0/1** S2(config-if)# **no shutdown** S2(config-if)# **switchport mode trunk**

S2(config-if)# **switchport trunk native vlan 99**

S2(config-if)# **interface f0/3**

S2(config-if)# **no shutdown**

S2(config-if)# **switchport mode trunk**

S2(config-if)# **switchport trunk native vlan 99**

S2(config-if)# **interface vlan 99**

S2(config-if)# **ip address 192.168.1.12 255.255.255.0**

S2(config-if)# **exit**

S2(config)# **spanning-tree vlan 1,10,99 root primary**

S2(config)# **spanning-tree mode rapid-pvst**

Коммутатор S3

S3(config)# **vlan 10**

S3(config-vlan)# **name User**

S3(config-vlan)# **vlan 99**

S3(config-vlan)# **name Management**

S3(config-vlan)# **exit**

S3(config)# **interface f0/18**

S3(config-if)# **no shutdown** S3(config-if)# **switchport mode access**

Практическая работа 4

Тема: Определение типовых ошибок конфигурации STP

Цели: Определить типовые ошибки при конфигурации STP

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задачи

Часть 1. Создание сети и настройка основных параметров устройства

Часть 2. Выбор корневого моста

Часть 3. Наблюдение за процессом выбора протоколом STP порта, исходя из стоимости портов

Часть 4. Наблюдение за процессом выбора протоколом STP порта, исходя из приоритета портов

Общие сведения/сценарий

Избыточность позволяет увеличить доступность устройств в топологии сети за счёт устранения единой точки отказа. Избыточность в коммутируемой сети обеспечивается посредством использования нескольких коммутаторов или нескольких каналов между коммутаторами. Когда в проекте сети используется физическая избыточность, возможно возникновение петель и дублирование кадров.

Протокол spanning-tree (STP) был разработан как механизм предотвращения возникновения петель на 2-м уровне для избыточных каналов коммутируемой сети. Протокол STP обеспечивает наличие только одного логического пути между всеми узлами назначения в сети путем намеренного блокирования резервных путей, которые могли бы вызвать петлю.

В этой лабораторной работе команда **show spanning-tree** используется для наблюдения за процессом выбора протоколом STP

корневого моста. Также вы будете наблюдать за процессом выбора портов с учетом стоимости и приоритета.

Примечание. Используются коммутаторы Cisco Catalyst 2960s с Cisco IOS версии 15.0(2) (образ lanbasek9). Допускается использование других моделей коммутаторов и других версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах.

Примечание. Убедитесь, что все настройки коммутатора удалены и загрузочная конфигурация отсутствует. Если вы не уверены, обратитесь к инструктору.

Топология

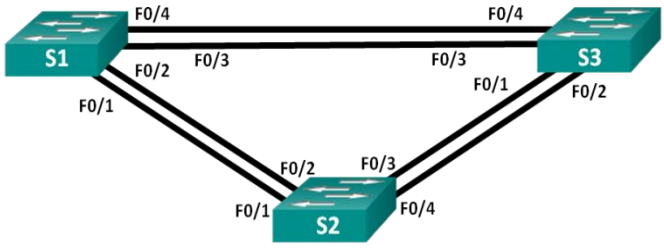


Таблица адресации

Устройство	**Интерфейс**	**IP-адрес**	**Маска подсети**
S1	VLAN 1	192.168.1.1	255.255.255.0
S2	VLAN 1	192.168.1.2	255.255.255.0
S3	VLAN 1	192.168.1.3	255.255.255.0

Необходимые ресурсы

- 3 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты

- Кабели Ethernet, расположенные в соответствии с топологией

Часть 1: Создание сети и настройка основных параметров устройства

В части 1 вам предстоит настроить топологию сети и основные параметры маршрутизаторов.

Шаг 1: Создайте сеть согласно топологии.

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

Шаг 2: выполните инициализацию и перезагрузку коммутаторов.

Шаг 3: Настройте базовые параметры каждого коммутатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

d. Назначьте **cisco** в качестве паролей консоли и VTY и активируйте вход для консоли и VTY каналов.

e. Настройте logging synchronous для консольного канала.

f. Настройте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.

g. Задайте IP-адрес, указанный в таблице адресации для VLAN 1 на обоих коммутаторах.

h. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Проверьте связь.

Проверьте способность компьютеров обмениваться эхо-запросами.

Успешно ли выполняется эхо-запрос от коммутатора S1 на коммутатор S2? _____ Успешно ли выполняется эхо-запрос от коммутатора S1 на коммутатор S3? _____

Успешно ли выполняется эхо-запрос от коммутатора S2 на коммутатор S3? _____ Выполняйте отладку до тех пор, пока ответы на все вопросы не будут положительными.

Часть 2: Определение корневого моста

Для каждого экземпляра протокола spanning-tree (коммутируемая сеть LAN или широковещательный домен) существует коммутатор, выделенный в качестве корневого моста. Корневой мост служит точкой привязки для всех расчётов протокола spanning-tree, позволяя определить избыточные пути, которые следует заблокировать.

Процесс выбора определяет, какой из коммутаторов станет корневым мостом. Коммутатор с наименьшим значением идентификатора моста (BID) становится корневым мостом. Идентификатор BID состоит из значения приоритета моста, расширенного идентификатора системы и MAC-адреса коммутатора. Значение приоритета может находиться в диапазоне от 0 до 65535 с шагом 4096. По умолчанию используется значение 32768.

Шаг 1: отключите все порты на коммутаторах.

Шаг 2: настройте подключенные порты в качестве транковых.

Шаг 3: включите порты F0/2 и F0/4 на всех коммутаторах.

Шаг 4: отобразите данные протокола spanning-tree.

Введите команду **show spanning-tree** на всех трех коммутаторах. Приоритет идентификатора моста рассчитывается путем сложения значений приоритета и расширенного идентификатора системы. Расширенным идентификатором системы всегда является номер сети VLAN. В примере ниже все три коммутатора имеют равные значения приоритета идентификатора моста (32769 = 32768 + 1, где приоритет по умолчанию = 32768, номер сети VLAN = 1); следовательно, коммутатор с самым низким значением MAC-адреса становится корневым мостом (в примере — S2).

S1# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0cd9.96d2.4000

Cost 19

Port 2 (FastEthernet0/2)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0cd9.96e8.8a00

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300 sec

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/2	Root	FWD	19	128.2	P2p
Fa0/4	Altn	BLK	19	128.4	P2p

S2# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee Root ID Priority 32769

Address 0cd9.96d2.4000

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

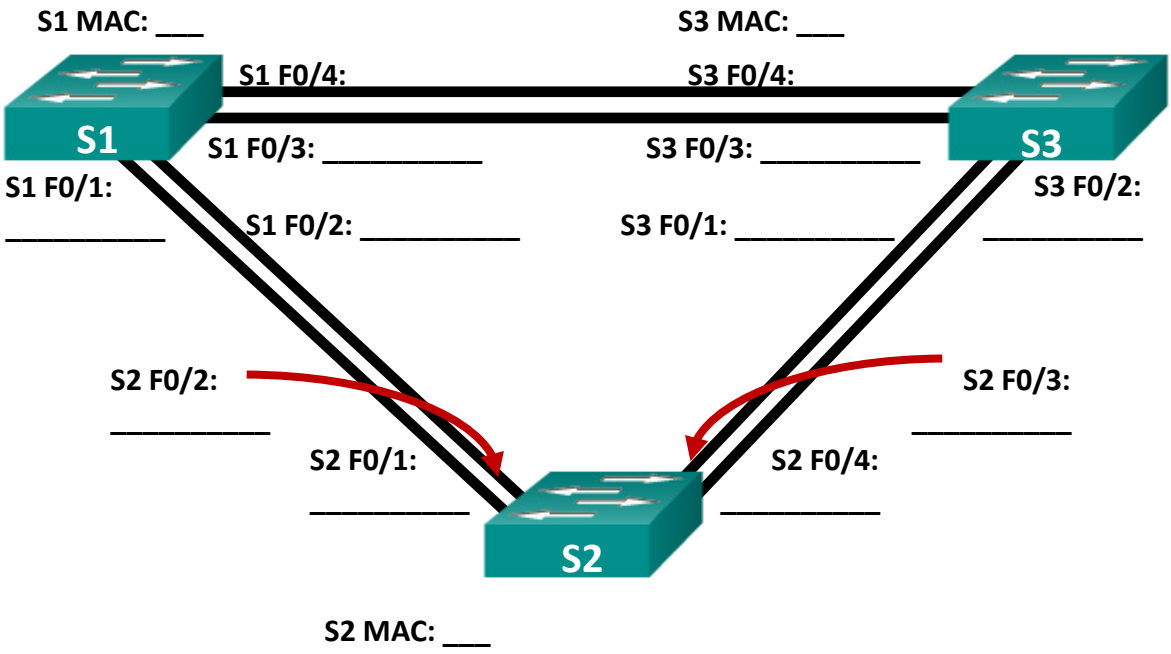
Address 0cd9.96d2.4000

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

```
        Aging Time  300 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/4            Desg FWD 19        128.4    P2p

S3# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
        Address     0cd9.96d2.4000
        Cost        19
        Port        2 (FastEthernet0/2)
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
        Address     0cd9.96e8.7400
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
        Aging Time  300 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Root FWD 19        128.2    P2p
Fa0/4            Desg FWD 19        128.4    P2p
```

Примечание. Режим STP по умолчанию на коммутаторе 2960 — протокол STP для каждой сети VLAN (PVST).

В схему ниже запишите роль и состояние (Sts) активных портов на каждом коммутаторе в топологии.



С учетом выходных данных, поступающих с коммутаторов, ответьте на следующие вопросы.

Какой коммутатор является корневым мостом? _____

Почему этот коммутатор был выбран протоколом spanning-tree в качестве корневого моста?

_____

_____

Какие порты на коммутаторе являются корневыми портами? _____

Какие порты на коммутаторе являются назначенными портами? _____

Какой порт отображается в качестве альтернативного и в настоящее время заблокирован? _____

Почему протокол spanning-tree выбрал этот порт в качестве невыделенного (заблокированного) порта?

_____

_____

Часть 3: Наблюдение за процессом выбора протоколом STP порта, исходя из стоимости портов

Алгоритм протокола spanning-tree (STA) использует корневой мост как точку привязки, после чего определяет, какие порты будут заблокированы, исходя из стоимости пути. Порт с более низкой стоимостью пути является предпочтительным. Если стоимости портов равны, процесс сравнивает BID. Если BID равны, для определения корневого моста используются приоритеты портов. Наиболее низкие значения являются предпочтительными. В части 3 вам предстоит изменить стоимость порта, чтобы определить, какой порт будет заблокирован протоколом spanning-tree.

Шаг 1: определите коммутатор с заблокированным портом.

При текущей конфигурации только один коммутатор может содержать заблокированный протоколом STP порт. Выполните команду **show spanning-tree** на обоих коммутаторах некорневого моста. В примере ниже протокол spanning-tree блокирует порт F0/4 на коммутаторе с самым высоким идентификатором BID (S1).

S1# **show spanning-tree**

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID Priority 32769
        Address 0cd9.96d2.4000
        Cost 19
        Port 2 (FastEthernet0/2)
        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
  Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
        Address 0cd9.96e8.8a00
        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
        Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type

---------- ---- --- --------- -------- ------------------------------

Fa0/2 Root FWD 19 128.2 P2p

Fa0/4 Altn BLK 19 128.4 P2p

S3# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0cd9.96d2.4000

Cost 19

Port 2 (FastEthernet0/2)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0cd9.96e8.7400

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 15 sec

Interface Role Sts Cost Prio.Nbr Type

---------- ---- --- --------- -------- ------------------------------

Fa0/2 Root FWD 19 128.2 P2p Fa0/4 Desg FWD 19 128.4 P2p

Примечание. В конкретной топологии корневой мост может отличаться от выбора порта.

Шаг 2: измените стоимость порта.

Помимо заблокированного порта, единственным активным портом на этом коммутаторе является порт, выделенный в качестве порта корневого моста. Уменьшите стоимость этого порта корневого моста до

18, выполнив команду **spanning-tree cost 18** режима конфигурации интерфейса.

S1(config)# **interface f0/2** S1(config-if)# **spanning-tree cost 18**

Шаг 3: просмотрите изменения протокола spanning-tree.

Повторно выполните команду **show spanning-tree** на обоих коммутаторах некорневого моста. Обратите внимание, что ранее заблокированный порт (S1 – F0/4) теперь является назначенным портом, и протокол spanning-tree теперь блокирует порт на другом коммутаторе некорневого моста (S3 – F0/4).

S1# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0cd9.96d2.4000

Cost 18

Port 2 (FastEthernet0/2)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0cd9.96e8.8a00

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300 sec

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/2	Root	FWD	18	128.2	P2p
Fa0/4	Desg	FWD	19	128.4	P2p

S3# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0cd9.96d2.4000

Cost 19

Port 2 (FastEthernet0/2)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0cd9.96e8.7400

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type

---------- ---- --- --------- -------- --------------------------------

Fa0/2 Root FWD 19 128.2 P2p Fa0/4 Altn BLK 19 128.4 P2p

Почему протокол spanning-tree заменяет ранее заблокированный порт на назначенный порт и блокирует порт, который был назначенным портом на другом коммутаторе?

_____

_____

Шаг 4: удалите изменения стоимости порта.

a. Выполните команду **no spanning-tree cost 18** режима конфигурации интерфейса, чтобы удалить запись стоимости, созданную ранее.

S1(config)# **interface f0/2** S1(config-if)# **no spanning-tree cost 18**

b. Повторно выполните команду **show spanning-tree**, чтобы подтвердить, что протокол STP сбросил порт на коммутаторе некорневого моста, вернув исходные настройки порта. Протоколу STP

требуется примерно 30 секунд, чтобы завершить процесс перевода порта.

Часть 4: Наблюдение за процессом выбора протоколом STP порта, исходя из приоритета портов

Если стоимости портов равны, процесс сравнивает BID. Если BID равны, для определения корневого моста используются приоритеты портов. Значение приоритета по умолчанию — 128. STP объединяет приоритет порта с номером порта, чтобы разорвать связи. Наиболее низкие значения являются предпочтительными. В части 4 вам предстоит активировать избыточные пути до каждого из коммутаторов, чтобы просмотреть, каким образом протокол STP выбирает порт с учетом приоритета портов.

a. Включите порты F0/1 и F0/3 на всех коммутаторах.

b. Подождите 30 секунд, чтобы протокол STP завершил процесс перевода порта, после чего выполните команду **show spanning-tree** на коммутаторах некорневого моста. Обратите внимание, что порт корневого моста переместился на порт с меньшим номером, связанный с коммутатором корневого моста, и заблокировал предыдущий порт корневого моста.

S1# **show spanning-tree**

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID   Priority   32769
             Address   0cd9.96d2.4000
             Cost   19
  Port   1 (FastEthernet0/1)
Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority   32769 (priority 32768 sys-id-ext 1)
Address   0cd9.96e8.8a00

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 15 sec

Interface Role Sts Cost Prio.Nbr Type

---------- ---- --- --------- -------- --------------------------------

Fa0/1 Root FWD 19 128.1 P2p

Fa0/2 Altn BLK 19 128.2 P2p Fa0/3 Altn BLK 19 128.3 P2p

Fa0/4 Altn BLK 19 128.4 P2p

S3# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0cd9.96d2.4000

Cost 19

Port 1 (FastEthernet0/1)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0cd9.96e8.7400

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 15 sec

Interface Role Sts Cost Prio.Nbr Type

---------- ---- --- --------- -------- --------------------------------

Fa0/1 Root FWD 19 128.1 P2p

Fa0/2 Altn BLK 19 128.2 P2p Fa0/3 Desg FWD 19 128.3 P2p Fa0/4 Desg FWD 19 128.4 P2p

Какой порт выбран протоколом STP в качестве порта корневого моста на каждом коммутаторе некорневого моста? _____

Почему протокол STP выбрал эти порты в качестве портов корневого моста на этих коммутаторах?

_____
_____

Вопросы для повторения

1. Какое значение протокол STP использует первым после выбора корневого моста, чтобы определить выбор порта?

_____
_____

2. Если первое значение на двух портах одинаково, какое следующее значение будет использовать протокол STP при выборе порта?

_____
_____

3. Если оба значения на двух портах равны, каким будет следующее значение, которое использует протокол STP при выборе порта?

_____
_____

Практическая работа 5

Тема: Настройка EtherChannel

Цели: Произвести настройку EtherChannel

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задачи

Часть 1. Построение сети и проверка соединения

Часть 2. Настройка обеспечения избыточности на первом хопе с помощью VRRP

Общие сведения/сценарий

Связующее дерево обеспечивает резервирование коммутаторами в локальной сети, не допуская возникновения петель. Но оно не позволяет организовать в сети резервирование шлюзов по умолчанию для устройств конечных пользователей на случай сбоя одного из маршрутизаторов. Протоколы обеспечения избыточности на первом хопе (First Hop Redundancy Protocols, FHRP) предоставляют избыточные шлюзы по умолчанию для конечных устройств. При этом конфигурация конечного пользователя не требуется. В этой лабораторной работе предстоит настроить протокол VRRP, являющийся протоколом FHRP.

Агрегирование каналов позволяет создавать логические каналы, состоящие из двух или более физических каналов. Таким образом увеличивается пропускная способность, а также используется только один физический канал. Агрегирование каналов также обеспечивает избыточность в случае сбоя одного из каналов.

В этой лабораторной работе вам предстоит настроить EtherChannel — тип агрегирования каналов, который используется в коммутируемых сетях. Вы настроите EtherChannel с помощью протокола агрегирования портов (PAgP) и протокола управления агрегированием каналов (LACP).

Примечание. PAgP является проприетарным протоколом Cisco, который можно использовать только на коммутаторах Cisco и коммутаторах лицензированных поставщиков, поддерживающих PAgP. Протокол LACP является протоколом агрегирования каналов, который определен стандартом IEEE 802.3ad и не связан с конкретным поставщиком.

Протокол LACP позволяет коммутаторам Cisco осуществлять управление каналами Ethernet между коммутаторами в соответствии с протоколом 802.3ad. В создании канала могут участвовать до 16 портов. Восемь из

портов находятся в активном режиме (active), а остальные восемь — в режиме ожидания (standby). В случае сбоя любого из активных портов задействуется порт, пребывающий

в режиме ожидания. Режим ожидания (standby mode) доступен только для протокола LACP, но не для протокола PAgP.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сетевыми сервисами (ISR) Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Точные идентификаторы интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что у маршрутизаторов и коммутаторов были удалены начальные конфигурации. Если вы не уверены, обратитесь к инструктору.

Топология

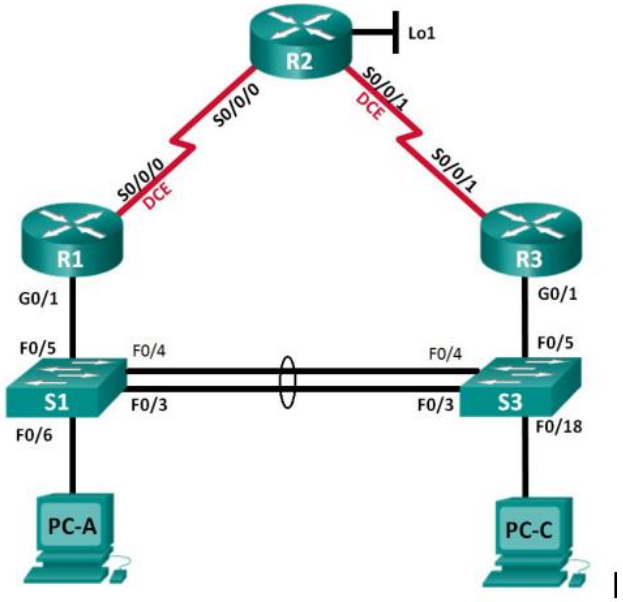


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	—
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	—
R2	S0/0/0	10.1.1.2	255.255.255.252	—
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	—
	Lo1	209.165.200.225	255.255.255.224	—
R3	G0/1	192.168.1.3	255.255.255.0	—
	S0/0/1	10.2.2.1	255.255.255.252	—
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.13	255.255.255.0	192.168.1.3
PC-A	NIC	192.168.1.31	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.33	255.255.255.0	192.168.1.3

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3
  (универсальный образ) или аналогичная модель)

- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- 2 компьютера (Windows 8, 7 или Vista с программой эмуляции терминала, например Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet и последовательные кабели согласно топологии

Часть 1: Построение сети и проверка связи

В первой части вам предстоит настроить топологию сети и выполнить базовую настройку, например IP-адреса интерфейсов, статическую маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Создайте сеть согласно топологии.

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 4: Произведите базовую настройку маршрутизаторов.

a. Отключите поиск DNS.
b. Присвойте имена устройствам в соответствии с топологией.
c. Настройте IP-адреса для маршрутизаторов, указанных в таблице адресации.
d. Установите тактовую частоту на **128000** для всех последовательных интерфейсов маршрутизатора DCE.
e. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.
f. Назначьте **cisco** в качестве пароля консоли и VTY и включите запрос пароля при подключении.
g. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.
h. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 5: Настройте базовые параметры каждого коммутатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

d. Настройте IP-адреса для коммутаторов, указанных в таблице адресации.

e. На каждом коммутаторе настройте шлюз по умолчанию.

f. Назначьте **cisco** в качестве пароля консоли и VTY и включите запрос пароля при подключении.

g. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.

h. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 6: Проверьте подключение между PC-A и PC-C.

Отправьте ping-запрос с компьютера PC-A на компьютер PC-C. Удалось ли получить ответ? _____

Если команды ping завершились неудачно и связь установить не удалось, исправьте ошибки в основных настройках устройства.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Шаг 7: Настройте маршрутизацию.

a. Настройте RIP версии 2 на всех маршрутизаторах. Добавьте в процесс RIP все сети, кроме 209.165.200.224/27.

b. Настройте маршрут по умолчанию на маршрутизаторе R2 с использованием Lo1 в качестве интерфейса выхода в сеть 209.165.200.224/27.

c. На маршрутизаторе R2 используйте следующие команды для перераспределения маршрута по умолчанию в процесс RIP.

R2(config)# **router rip**
R2(config-router)# **default-information originate**

Шаг 8: Проверьте подключение.

a. Необходимо получить ответ на ping-запросы с компьютера PC-A от каждого интерфейса на маршрутизаторах R1, R2 и R3, а также от компьютера PC-C. Удалось ли получить все ответы?

_____

Если команды ping завершились неудачно и связь установить не удалось, исправьте ошибки в основных настройках устройства.

b. Необходимо получить ответ на ping-запросы с компьютера PC-C от каждого интерфейса на маршрутизаторах R1, R2 и R3, а также от компьютера PC-A. Удалось ли получить все ответы?

_____

Если команды ping завершились неудачно и связь установить не удалось, исправьте ошибки в основных настройках устройства.

Часть 2: Настройка обеспечения избыточности на первом хопе с помощью VRRP

Даже если топология спроектирована с учетом избыточности (два маршрутизатора и два коммутатора в одной сети LAN), оба компьютера, PC-A и PC-C, необходимо настраивать с одним адресом шлюза.

PC-A использует R1, а PC-C — R3. В случае сбоя на одном из этих маршрутизаторов или интерфейсов маршрутизаторов компьютер может потерять подключение к сети Интернет.

В части 2 вам предстоит изучить поведение сети до и после настройки протокола VRRP. Для этого вам понадобится определить путь, по которому проходят пакеты, чтобы достичь loopback-адрес на R2.

Шаг 1: Определите путь интернет-трафика для PC-A и PC-C.

a. В командной строке на PC-A введите команду **tracert** для loopback-адреса 209.165.200.225 на маршрутизаторе R2.

C:\ **tracert 209.165.200.225**
Tracing route to 209.165.200.225 over a maximum of 30 hops

1 1 ms 1 ms 1 ms 192.168.1.1
2 13 ms 13 ms 13 ms 209.165.200.225

Trace complete.

Какой путь прошли пакеты от PC-A до 209.165.200.225?

_____

b. В командной строке на PC-C введите команду **tracert** для loopback-адреса 209.165.200.225 на маршрутизаторе R2.

Какой путь прошли пакеты от PC-C до 209.165.200.225?

_____

Шаг 2: Запустите сеанс эхо-тестирования на PC-A и разорвите соединение между S1 и R1.

a. В командной строке на PC-A введите команду **ping –t** для адреса **209.165.200.225** на маршрутизаторе R2. Убедитесь, что окно командной строки открыто.

Примечание. Чтобы прервать отправку эхо-запросов, нажмите комбинацию клавиш **Ctrl+C** или закройте окно командной строки.

C:\ **ping –t 209.165.200.225**
Pinging 209.165.200.225 with 32 bytes of data:
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
<выходные данные опущены>

b. В процессе эхо-тестирования отсоедините кабель Ethernet от интерфейса F0/5 на S1. Отключение интерфейса F0/5 на S1 приведет к тому же результату.

Что произошло с трафиком эхо-запросов?

_____
_____

c. Какими были бы результате при повторении шагов 2a и 2b на компьютере PC-C и коммутаторе S3?

_____
_____

d. Повторно подсоедините кабели Ethernet к интерфейсу F0/5 или включите интерфейс F0/5 на S1 и S3, соответственно. Повторно отправьте эхо-запросы на 209.165.200.225 с компьютеров PC-A и PC-C, чтобы убедиться в том, что подключение восстановлено.

Шаг 3: Настройте VRRP на R1 и R3.

В этом шаге вам предстоит настроить VRRP и изменить адрес шлюза по умолчанию на компьютерах PC-A, PC-C, S1 и коммутаторе S2 на виртуальный IP-адрес для VRRP. R1 назначается активным

маршрутизатором с помощью команды приоритета VRRP. a. Настройте протокол VRRP на маршрутизаторе R1.

R1(config)# **interface g0/1**
R1(config-if)# **vrrp 1 ip 192.168.1.254**
R1(config-if)# **vrrp 1 priority 150**

b. Настройте протокол VRRP на маршрутизаторе R3.

R3(config)# **interface g0/1**
R3(config-if)# **vrrp 1 ip 192.168.1.254**

c. Проверьте VRRP, выполнив команду **show vrrp** на R1 и R3.

R1# **show vrrp**

Используя указанные выше выходные данные, ответьте на следующие вопросы:

Какой маршрутизатор является активным? _____

Какой MAC-адрес используется для виртуального IP-адреса?

_____

Какой IP-адрес и приоритет используются для резервного маршрутизатора?

_____

_____

d. Используйте команду **show vrrp brief** на R1 и R3, чтобы просмотреть сводку состояния VRRP. Выходные данные приведены ниже.

R1# **show vrrp brief**

e. Измените адрес шлюза по умолчанию для PC-A, PC-C, S1 и S3. Какой адрес следует использовать?

_____

_____

f. Проверьте новые настройки. Отправьте эхо-запрос с PC-A и с PC-C на loopback-адрес маршрутизатора R2. Успешно ли выполнены эхо-запросы? _____

Шаг 4: Запустите сеанс эхо-тестирования на PC-A и разорвите соединение с коммутатором, подключенным к активному маршрутизатору VRRP (R1).

a. В командной строке на PC-A введите команду **ping –t** для адреса 209.165.200.225 на маршрутизаторе R2. Убедитесь, что окно командной строки открыто.

b. Во время отправки эхо-запроса отсоедините кабель Ethernet от интерфейса F0/5 на коммутаторе S1 или выключите интерфейс F0/5.

Что произошло с трафиком эхо-запросов?

_____
_____

Шаг 5: Проверьте настройки VRRP на маршрутизаторах R1 и R3.

a. Выполните команду **show vrrp brief** на маршрутизаторах R1 и R3.

Какой маршрутизатор является активным?

_____ Повторно подключите кабель, соединяющий коммутатор и маршрутизатор, или включите интерфейс F0/5. Какой маршрутизатор теперь является активным? Поясните ответ.

_____
_____

Шаг 6: Изменение приоритетов VRRP.

a. Измените приоритет VRRP на 200 на маршрутизаторе R3. Какой маршрутизатор является активным? _____

b. Выполните команду, чтобы сделать активным маршрутизатор R3 без изменения приоритета. Какую команду вы использовали?

_____
_____

c. Используйте команду **show**, чтобы убедиться, что R3 является активным маршрутизатором.

Часть 1: Настройка протокола LACP

Протокол LACP является открытым протоколом агрегирования каналов, разработанным на базе стандарта IEEE. В части 3 необходимо выполнить настройку канала между S1 и S3 с помощью протокола LACP. Кроме того, отдельные каналы необходимо настроить в качестве транковых, прежде чем они будут объединены в каналы EtherChannel.

Шаг 1: Настройте LACP между S1 и S3.

S1(config)# **interface range f0/3-4**
S1(config-if-range)# **switchport mode trunk**
S1(config-if-range)# **switchport trunk native vlan 99**

S1(config-if-range)# **channel-group 2 mode active**
Creating a port-channel interface Port-channel 2

S1(config-if-range)# **no shutdown**

S3(config)# **interface range f0/3-4**
S3(config-if-range)# **switchport mode trunk**
S3(config-if-range)# **switchport trunk native vlan 99**
S3(config-if-range)# **channel-group 2 mode passive**
Creating a port-channel interface Port-channel 2

S3(config-if-range)# **no shutdown**

Шаг 2: Убедитесь, что порты объединены.

Какой протокол использует Po2 для агрегирования каналов? Какие порты агрегируются для образования Po2? Запишите команду, используемую для проверки.

_____
_____

Шаг 3: Проверьте наличие сквозного соединения.

Убедитесь в том, что все устройства могут передавать друг другу эхо-запросы в пределах одной сети VLAN. Если нет, устраните неполадки, чтобы установить связь между конечными устройствами.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение межсетевого экрана.

Шаг 4: Проверьте конфигурации на портах.

В настоящее время интерфейсы F0/3, F0/4 и Po1 (Port-channel1) на коммутаторах S1 и S3 находятся в режиме доступе, а режим управления установлен на динамический автоматический режим (dynamic auto). Проверьте конфигурацию с помощью соответствующих команд **show run interface** *идентификатор-интерфейса* и **show interfaces** *идентификатор-интерфейса* **switchport**. Для интерфейса F0/3 на S1 отображаются следующие выходные данные конфигурации:

S1# **show run interface f0/3**
Building configuration...

Current configuration : 103
bytes !
interface FastEthernet0/3
channel-group 1 mode active

S1# **show interfaces f0/3 switchport**
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access (member of bundle Po1)
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

Шаг 5: Убедитесь, что порты объединены.

S1# **show etherchannel summary**
Flags: D - down P - bundled in port-channel

I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator

M - not in use, minimum links
not met u - unsuitable for
bundling w - waiting to be
aggregated d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+-----------+---
1 Po1(SU) LACP Fa0/3(P) Fa0/4(P)

S3# **show etherchannel summary**
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator

M - not in use, minimum links
not met u - unsuitable for
bundling w - waiting to be
aggregated d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+-----------+---

1 Po1(SU) LACP Fa0/3(P)

Fa0/4(P) Что означают флаги «SU» и «P» в

сводных данных по Ethernet?

_____

_____

Вопросы для повторения

Для чего в локальной сети может потребоваться избыточность?

Что может препятствовать образованию каналов EtherChannel?

_____

_____

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet № 1**	**Интерфейс Ethernet № 2**	**Последовательный интерфейс № 1**	**Последовательный интерфейс № 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах Cisco IOS для обозначения интерфейса.				

Практическая работа 6

Тема: Поиск неполадок в работе EtherChannel

Цели работы: Произвести поиск и устранить неполадки в работе EtherChannel

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задачи

Часть 1. Построение сети и загрузка конфигураций устройств

Часть 2. Отладка EtherChannel

Исходные данные/сценарий

Маршрутизаторы в сети вашей компании были настроены неопытным сетевым администратором. В результате ошибок в конфигурации возникли проблемы со скоростью и подключением. Начальник попросил вас найти и устранить неполадки в настройке и задокументировать работу. Найдите и исправьте ошибки, используя свои знания EtherChannel и стандартные методы тестирования. Убедитесь в том, что все каналы EtherChannel используют протокол агрегирования портов (PAgP) и все узлы доступны.

Примечание. В лабораторной работе используются коммутаторы Cisco Catalyst 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование других моделей коммутаторов и других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и их результаты могут отличаться от приведённых в описании лабораторных работ.

Примечание. Убедитесь, что прежние настройки коммутаторов были удалены, и они не содержат конфигурации загрузки. Если вы не уверены в этом, обратитесь к инструктору.

Топология

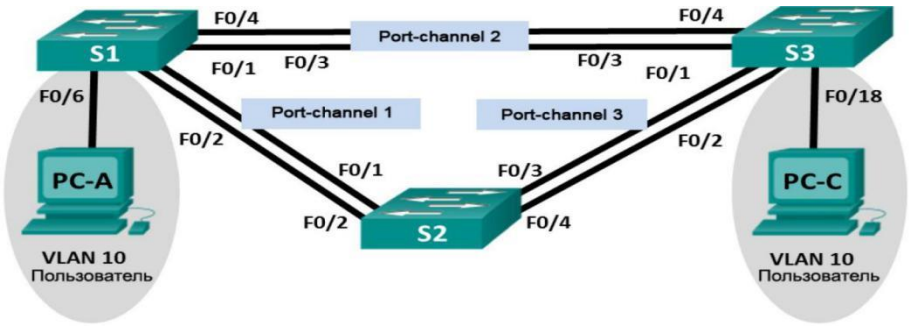


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
S1	VLAN 99	192.168.1.11	255.255.255.0
S2	VLAN 99	192.168.1.12	255.255.255.0
S3	VLAN 99	192.168.1.13	255.255.255.0
PC-A	NIC	192.168.0.2	255.255.255.0
PC-C	NIC	192.168.0.3	255.255.255.0

Назначения сети VLAN

VLAN	Имя
10	Пользователь
99	Management (Руководство)

Необходимые ресурсы:

- 3 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);
- 2 ПК (Windows 7, Vista и XP с программой эмуляции терминала, например Tera Term)
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Построение сети и загрузка конфигураций устройств

В части 1 вам предстоит настроить топологию сети и базовые параметры для ПК, а также загрузить конфигурации на коммутаторы.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Настройте узлы ПК.

Шаг 3: Удалите загрузочную конфигурацию и настройки VLAN, а затем перезагрузите коммутаторы.

Шаг 4: Загрузите конфигурации коммутаторов.

Загрузите следующие конфигурации в соответствующий коммутатор. Все коммутаторы используют одинаковые пароли. Пароль привилегированного режима — **class**. Пароль для консоли и доступа vty — **cisco**. Поскольку все коммутаторы являются устройствами Cisco, сетевой администратор решил использовать протокол PAgP Cisco для всех агрегированных каналов, настроенных с использованием EtherChannel. Коммутатор S2 является корневым мостом для всех сетей VLAN в топологии.

Конфигурация коммутатора S1:

hostname S1

interface range f0/1-24, g0/1-2 shutdown exit

enable secret class no ip domain lookup line vty 0 15 password cisco login line con 0 password cisco logging synchronous login exit vlan 10 name User vlan 99 Name Management interface range f0/1-2 switchport mode trunk channel-group 1 mode active switchport trunk native vlan 99 no shutdown interface range f0/3-4

channel-group 2 mode desirable switchport trunk native vlan 99 no shutdown interface f0/6 switchport mode access switchport access vlan 10 no shutdown interface vlan 99 ip address 192.168.1.11 255.255.255.0 interface port-channel 1 switchport trunk native vlan 99 switchport mode trunk interface port-channel 2 switchport trunk native vlan 99 switchport mode access **Конфигурация коммутатора S2:**

hostname S2 interface range f0/1-24, g0/1-2 shutdown exit enable secret class no ip domain lookup line vty 0 15 password cisco login line con 0 password cisco logging synchronous

login exit vlan 10 name User vlan 99 name Management spanning-tree vlan 1,10,99 root primary interface range f0/1-2 switchport mode trunk channel-group 1 mode desirable switchport trunk native vlan 99 no shutdown interface range f0/3-4

switchport mode trunk channel-group 3 mode desirable switchport trunk native vlan 99 interface vlan 99 ip address 192.168.1.12 255.255.255.0 interface port-channel 1 switchport trunk native vlan 99 switchport trunk allowed vlan 1,99 interface port-channel 3 switchport trunk native vlan 99 switchport trunk allowed vlan 1,10,99 switchport mode trunk

Конфигурация коммутатора S3:

hostname S3 interface range f0/1-24, g0/1-2 shutdown exit enable secret class no ip domain lookup line vty 0 15 password cisco login line con 0 password cisco logging synchronous login exit vlan 10 name User vlan 99 name Management

interface range f0/1-2

interface range f0/3-4

switchport mode trunk channel-group 3 mode desirable switchport trunk native vlan 99 no shutdown interface f0/18 switchport mode access switchport access vlan 10 no shutdown interface vlan 99 ip address 192.168.1.13 255.255.255.0 interface port-channel 3 switchport trunk native vlan 99 switchport mode trunk

Шаг 5: Сохраните конфигурацию.

Часть 2: Отладка EtherChannel

В части 2 необходимо проверить конфигурации на всех коммутаторах, исправить при необходимости и проверить их работоспособность.

Шаг 1: Выполните поиск и устранение неполадок в работе маршрутизатора S1.

a. Используйте команду **show interfaces trunk**, чтобы убедиться в том, что агрегированные каналы работают, как транковые порты.

Отображаются ли агрегированные каналы 1 и 2, как транковые порты?

_____

b. Используйте команду **show etherchannel summary**, чтобы убедиться в том, что интерфейсы входят в состав соответствующего агрегированного канала, применен правильный протокол и интерфейсы задействованы.

Есть ли в выходных данных сведения о неполадках в работе EtherChannel? В случае обнаружения неполадок запишите их в отведённом ниже месте.

_____

_____

c. Используйте команду **show run | begin interface Port-channel** для просмотра текущей конфигурации, начиная с первого интерфейса агрегированного канала.

d. Устраните все ошибки, найденные в выходных данных из предыдущих команд **show**. Запишите команды, используемые для исправления конфигураций.

_____

_____

e. Используйте команду **show interfaces trunk** для проверки настроек транковой связи.

f. Используйте команду **show etherchannel summary**, чтобы убедиться в том, что агрегированные каналы работают и задействованы.

Шаг 2: Выполните поиск и устранение неполадок в работе маршрутизатора S2.

a. Выполните команду для того, чтобы убедиться, что агрегированные каналы работают в качестве транковых портов. Ниже запишите команду, которую вы использовали.

_____

_____

Есть ли в выходных данных сведения о неполадках в конфигурациях? В случае обнаружения неполадок запишите их в отведённом ниже месте.

_____

_____

b. Выполните команду, чтобы убедиться в том, что интерфейсы настроены в правильном агрегированном канале и настроен соответствующий протокол.

Есть ли в выходных данных сведения о неполадках в работе EtherChannel? В случае обнаружения неполадок запишите их в отведённом ниже месте.

_____

_____

c. Используйте команду **show run | begin interface Port-channel** для просмотра текущей конфигурации, начиная с первого интерфейса канала порта.

d. Устраните все ошибки, найденные в выходных данных из предыдущих команд **show**. Запишите команды, использованные для внесения изменений в конфигурацию.

_____

_____

e. Выполните команду для проверки параметров транковой связи.

f. Выполните команду для проверки правильного функционирования агрегированных каналов.

Помните, что проблемы с агрегированным каналом могут возникнуть на любом конце канала.

Шаг 3: Выполните поиск и устранение неполадок в работе маршрутизатора S3.

a. Выполните команду для того, чтобы убедиться, что агрегированные каналы работают в качестве транковых портов.

Есть ли в выходных данных сведения о неполадках в конфигурациях? В случае обнаружения неполадок запишите их в отведённом ниже месте.

_____

_____

b. Выполните команду, чтобы убедиться в том, что интерфейсы настроены в правильном агрегированном канале и применен соответствующий протокол.

Есть ли в выходных данных сведения о неполадках в работе EtherChannel? В случае обнаружения неполадок запишите их в отведённом ниже месте.

_____

_____

c. Используйте команду **show run | begin interface Port-channel** для просмотра текущей конфигурации, начиная с первого интерфейса агрегированного канала.

d. Устраните все обнаруженные неполадки. Запишите команды, использованные для внесения изменений в конфигурацию.

_____

_____

e. Выполните команду для проверки параметров транковой связи. Ниже запишите команду, которую вы использовали.

_____

_____

f. Выполните команду для проверки правильного функционирования агрегированных каналов. Ниже запишите команду, которую вы использовали.

_____

_____

Шаг 4: Проверка EtherChannel и подключения

a. Используйте команду **show interfaces etherchannel** для проверки работоспособности агрегированных каналов.

b. Проверьте подключение сети VLAN Management.

Успешно ли выполняется эхо-запрос от коммутатора S1 на коммутатор S2? _____ Успешно ли выполняется эхо-запрос от коммутатора S1 на коммутатор S3? _____

Успешно ли выполняется эхо-запрос от коммутатора S2 на коммутатор S3? _____

c. Проверка подключения компьютеров

Успешно ли выполняется эхо-запрос от узла PC-A на узел PC-C? _____

Если каналы EtherChannel не полностью работоспособны, отсутствует соединение между коммутаторами или между узлами. Выполните окончательную отладку.

Примечание. Для успешной передачи эхо-запросов между компьютерами может потребоваться отключение межсетевого экрана.

Практическая работа 7

Тема: Агрегирование каналов

Цели работы: Изучить протоколы агрегирования каналов

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задачи

Часть 1. Настройка базовых параметров коммутатора

Часть 2. Настройка PAgP

Часть 3. Настройка LACP

Общие сведения/сценарий

Агрегирование каналов позволяет создавать логические каналы, состоящие из двух или более физических каналов. Таким образом увеличивается пропускная способность, а также используется только один физический канал. Агрегирование каналов также обеспечивает избыточность в случае сбоя одного из каналов.

В этой лабораторной работе вам предстоит настроить EtherChannel — тип агрегирования каналов, который используется в коммутируемых сетях. Вы настроите EtherChannel с помощью протокола агрегирования портов (PAgP) и протокола управления агрегированием каналов (LACP).

Примечание. PAgP является проприетарным протоколом Cisco, который можно использовать только на коммутаторах Cisco и коммутаторах лицензированных поставщиков, поддерживающих PAgP. Протокол LACP является протоколом агрегирования каналов, который определен стандартом IEEE 802.3ad и не связан с конкретным поставщиком.

Протокол LACP позволяет коммутаторам Cisco осуществлять управление каналами Ethernet между коммутаторами в соответствии с протоколом 802.3ad. В создании канала могут участвовать до 16 портов. Восемь из портов находятся в активном режиме (active), а остальные восемь — в режиме ожидания (standby). В случае сбоя любого из активных портов задействуется порт, пребывающий в режиме

ожидания. Режим ожидания (standby mode) доступен только для протокола LACP, но не для протокола PAgP.

Примечание. В практических лабораторных работах CCNA используются коммутаторы Cisco Catalyst 2960s с операционной системой Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование других моделей коммутаторов и других версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах.

Примечание. Убедитесь, что все настройки коммутатора удалены и загрузочная конфигурация отсутствует. Если вы не уверены, обратитесь к инструктору.

Топология

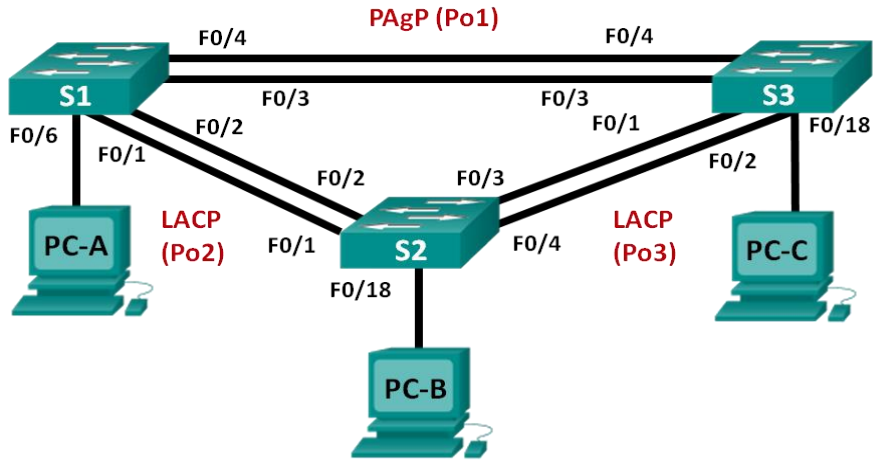


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
S1	VLAN 99	192.168.99.11	255.255.255.0
S2	VLAN 99	192.168.99.12	255.255.255.0
S3	VLAN 99	192.168.99.13	255.255.255.0
PC-A	NIC	192.168.10.1	255.255.255.0

PC-B	NIC	192.168.10.2	255.255.255.0
PC-C	NIC	192.168.10.3	255.255.255.0

Необходимые ресурсы

- 3 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- 3 ПК (Windows 7, Vista или XP с программой эмуляции терминалов, например Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet, расположенные в соответствии с топологией

Часть 1: Настройка основных параметров коммутатора

В части 1 вы настроите топологию сети и такие базовые параметры, как IP-адреса интерфейсов, доступ к устройствам и пароли.

Шаг 1: Создайте сеть согласно топологии.

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

Шаг 2: Выполните инициализацию и перезагрузку коммутаторов.

Шаг 3: Настройте базовые параметры каждого коммутатора.

a. Отключите поиск DNS.

b. Настройте имя устройства в соответствии с топологией.

c. Зашифруйте незашифрованные пароли.

d. Создайте баннерное сообщение дня MOTD, предупреждающее пользователей о том, что несанкционированный доступ запрещен.

e. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

f. Назначьте **cisco** в качестве пароля консоли и VTY и включите запрос пароля при подключении.

g. Настройте logging synchronous, чтобы предотвратить прерывание ввода команд сообщениями консоли.

h. Отключите все порты коммутатора, кроме портов, подключенных к компьютерам.

i. Настройте сеть VLAN 99 и присвойте ей имя **Management**.

j. Настройте сеть VLAN 10 и присвойте ей имя **Staff**.

k. Настройте порты коммутатора с присоединёнными узлами в качестве портов доступа в сети VLAN 10.

l. Назначьте IP-адреса в соответствии с таблицей адресации.

m. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 4: Настройте компьютеры.

Назначьте IP-адреса компьютерам в соответствии с таблицей адресации.

Часть 2: Настройка протокола PAgP

Протокол PAgP является проприетарным протоколом агрегирования каналов Cisco. В части 2 вам предстоит настроить канал между S1 и S3 с использованием протокола PAgP.

Шаг 1: Настройте PAgP на S1 и S3.

Для создания канала между S1 и S3 настройте порты на S1 с использованием рекомендуемого режима (desirable), а порты на S3 — с использованием автоматического режима (auto). Включите порты после настройки режимов PAgP.

S1(config)# **interface range f0/3-4**

S1(config-if-range)# **channel-group 1 mode desirable**

Creating a port-channel interface Port-channel 1

S1(config-if-range)# **no shutdown**

S3(config)# **interface range f0/3-4**

S3(config-if-range)# **channel-group 1 mode auto**

Creating a port-channel interface Port-channel 1

S3(config-if-range)# **no shutdown**

*Mar 1 00:09:12.792: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up *Mar 1 00:09:12.792: %LINK-3-UPDOWN: Interface FastEthernet0/4, changed state to up S3(config-if-range)#

*Mar 1 00:09:15.384: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

*Mar 1 00:09:16.265: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

S3(config-if-range)#

*Mar 1 00:09:16.357: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up

*Mar 1 00:09:17.364: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to u p

*Mar 1 00:09:44.383: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Шаг 2: Проверьте конфигурации на портах.

В настоящее время интерфейсы F0/3, F0/4 и Po1 (Port-channel1) на коммутаторах S1 и S3 находятся в режиме доступе, а режим управления установлен на динамический автоматический режим (dynamic auto). Проверьте конфигурацию с помощью соответствующих команд **show run interface** *идентификатор-интерфейса* и **show interfaces**

идентификатор-интерфейса **switchport**. Для интерфейса F0/3 на S1 отображаются следующие выходные данные конфигурации:

S1# **show run interface f0/3**

Building configuration...

Current configuration : 103 bytes ! interface FastEthernet0/3 channel-group 1 mode desirable

S1# **show interfaces f0/3 switchport**

Name: Fa0/3

Switchport: Enabled

Administrative Mode: dynamic auto

Operational Mode: static access (member of bundle Po1)

Administrative Trunking Encapsulation: dot1q Operational Trunking Encapsulation: native

Negotiation of Trunking: On

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: 1 (default)

Administrative Native VLAN tagging: enabled

Voice VLAN: none

Administrative private-vlan host-association: none

Administrative private-vlan mapping: none

Administrative private-vlan trunk native VLAN: none

Administrative private-vlan trunk Native VLAN tagging: enabled

Administrative private-vlan trunk encapsulation: dot1q

Administrative private-vlan trunk normal VLANs: none

Administrative private-vlan trunk associations: none

Administrative private-vlan trunk mappings: none

Operational private-vlan: none

Trunking VLANs Enabled: ALL

Pruning VLANs Enabled: 2-1001

Capture Mode Disabled

Capture VLANs Allowed: ALL

Protected: false

Unknown unicast blocked: disabled

Unknown multicast blocked: disabled Appliance trust: none

Шаг 3: Убедитесь, что порты объединены.

S1# **show etherchannel summary**

Flags: D - down P - bundled in port-channel

I - stand-alone s - suspended

H - Hot-standby (LACP only)

R - Layer3 S - Layer2

U - in use f - failed to allocate aggregator

M - not in use, minimum links not met u - unsuitable for bundling

w - waiting to be aggregated d - default port

Number of channel-groups in use: 1 Number of aggregators: 1

Group Port-channel Protocol Ports

------+-------------+-----------+---

1 Po1(SU) PAgP Fa0/3(P) Fa0/4(P)

S3# **show etherchannel summary**

Flags: D - down P - bundled in port-channel

I - stand-alone s - suspended

H - Hot-standby (LACP only)

R - Layer3 S - Layer2

U - in use f - failed to allocate aggregator

M - not in use, minimum links not met u - unsuitable for bundling w - waiting to be aggregated d - default port

Number of channel-groups in use: 1 Number of aggregators: 1

Group Port-channel Protocol Ports

------+-------------+-----------+---

1 Po1(SU) PAgP Fa0/3(P) Fa0/4(P) Что означают флаги «SU» и «P» в сводных данных по Ethernet?

_____

_____

Шаг 4: Настройте транковые порты.

После агрегирования портов команды, применённые на интерфейсе Port Channel, влияют на все объединённые в группу каналы. Вручную настройте порты Po1 на S1 и S3 в качестве транковых и назначьте их сети native VLAN 99.

S1(config)# **interface port-channel 1** S1(config-if)# **switchport mode trunk**

S1(config-if)# **switchport trunk native vlan 99**

S3(config)# **interface port-channel 1** S3(config-if)# **switchport mode trunk**

S3(config-if)# **switchport trunk native vlan 99**

Шаг 5: Убедитесь в том, что порты настроены в качестве транковых.

a. Выполните команды **show run interface** *идентификатор-интерфейса* на S1 и S3. Какие команды включены в список для интерфейсов F0/3 и F0/4 на обоих коммутаторах? Сравните результаты с текущей конфигурацией для интерфейса Po1. Запишите наблюдения.

_____

_____

b. Выполните команды **show interfaces trunk** и **show spanning-tree** на S1 и S3. Какой транковый порт включен в список? Какая используется сеть native VLAN? Какой вывод можно сделать на основе выходных данных?

_____

_____

Какие значения стоимости и приоритета порта для агрегированного канала отображены в выходных данных команды **show spanning-tree**?

_____

_____

Часть 3: Настройка протокола LACP

Протокол LACP является открытым протоколом агрегирования каналов, разработанным на базе стандарта IEEE. В части 3 необходимо выполнить настройку канала между S1 и S2 и канала между S2 и S3 с помощью протокола LACP. Кроме того, отдельные каналы необходимо настроить в качестве транковых, прежде чем они будут объединены в каналы EtherChannel.

Шаг 1: Настройте LACP между S1 и S2.

S1(config)# **interface range f0/1-2**

S1(config-if-range)# **switchport mode trunk**

S1(config-if-range)# **switchport trunk native vlan 99**

S1(config-if-range)# **channel-group 2 mode active**

Creating a port-channel interface Port-channel 2

S1(config-if-range)# **no shutdown**

S2(config)# **interface range f0/1-2**

S2(config-if-range)# **switchport mode trunk**

S2(config-if-range)# **switchport trunk native vlan 99**

S2(config-if-range)# **channel-group 2 mode passive**

Creating a port-channel interface Port-channel 2

S2(config-if-range)# **no shutdown**

Шаг 2: Убедитесь, что порты объединены.

Какой протокол использует Po2 для агрегирования каналов? Какие порты агрегируются для образования Po2? Запишите команду, используемую для проверки.

_____

_____

Шаг 3: Настройте LACP между S2 и S3.

a. Настройте канал между S2 и S3 как Po3, используя LACP как протокол агрегирования каналов.

S2(config)# **interface range f0/3-4**

S2(config-if-range)# **switchport mode trunk**

S2(config-if-range)# **switchport trunk native vlan 99** S2(config-if-range)# **channel-group 3 mode active** Creating a port-channel interface Port-channel 3

S2(config-if-range)# **no shutdown**

S3(config)# **interface range f0/1-2**

S3(config-if-range)# **switchport mode trunk**

S3(config-if-range)# **switchport trunk native vlan 99**

S3(config-if-range)# **channel-group 3 mode passive**

Creating a port-channel interface Port-channel 3

S3(config-if-range)# **no shutdown**

b. Убедитесь в том, что канал EtherChannel образован.

Шаг 4: Проверьте наличие сквозного соединения.

Убедитесь в том, что все устройства могут передавать друг другу эхо-запросы в пределах одной сети VLAN. Если нет, устраните неполадки, чтобы установить связь между конечными устройствами.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение межсетевого

Практическая работа 6

Тема: Настройка беспроводного маршрутизатора

Цели: Произвести настройку беспроводного маршрутизатора и клиента

Задачи

Часть 1. Настройка основных параметров маршрутизатора Linksys серии EA

Часть 2. Настройка защиты беспроводной сети

Часть 3. Настройка дополнительных функций маршрутизатора Lynksys сериiEA

Часть 4. Подключение беспроводного клиента

Исходные данные/сценарий

В наши дни доступ к сети Интернет из любого места, будь то дом или офис — широко распространенное явление. Без беспроводной связи пользователи были бы ограничены возможностью подключения только при наличии проводного соединения. Пользователи по достоинству

оценили гибкость и возможности, которые предоставляют беспроводные маршрутизаторы в рамках доступа к сети и Интернету.

В этой лабораторной работе вам предстоит настроить маршрутизатор Linksys Smart Wi-Fi, применить настройки безопасности WPA2 и активировать службы DHCP. Вы рассмотрите некоторые дополнительные функции, доступные на этих маршрутизаторах, например, USB-накопители, родительский контроль и ограничения по времени. Вам также предстоит настроить беспроводной клиент для компьютера.

Топология

Настройки маршрутизатора Linksys

Имя сети (SSID)	Сеть CCNA
Пароль сети	cisconet
Пароль маршрутизатора	cisco123

Необходимые ресурсы:

- 1 маршрутизатор Linksys EA Series (EA4500 с версией микропрограммного обеспечения 2.1.39.145204 или сопоставимой версией);
- 1 кабельный или DSL-модем (необязательно; требуется для работы интернет-службы и обычно предоставляется интернет-провайдером);

- 1 компьютер с беспроводным сетевым адаптером (ОС Windows 7, Vista или XP);
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Настройка основных параметров маршрутизатора Linksys EA Series

Самым эффективным способом настройки основных параметров маршрутизатора EA Series является запуск установочного компакт-диска Linksys EA Series, поставляемого в комплекте с маршрутизатором. Если установочный компакт-диск отсутствует, следует загрузить программу установки с веб-сайта http://Linksys.com/support.

Шаг 1: Вставьте установочный компакт-диск Linksys EA-Series в компьютер.

Когда отобразится соответствующий запрос, выберите **Set up your Linksys Router (Настройка маршрутизатора Linksys)**. Вам будет предложено ознакомиться с условиями лицензии на использование программного обеспечения и принять их. После того, как вы примете условия лицензии нажмите **Next > (Далее >)**.

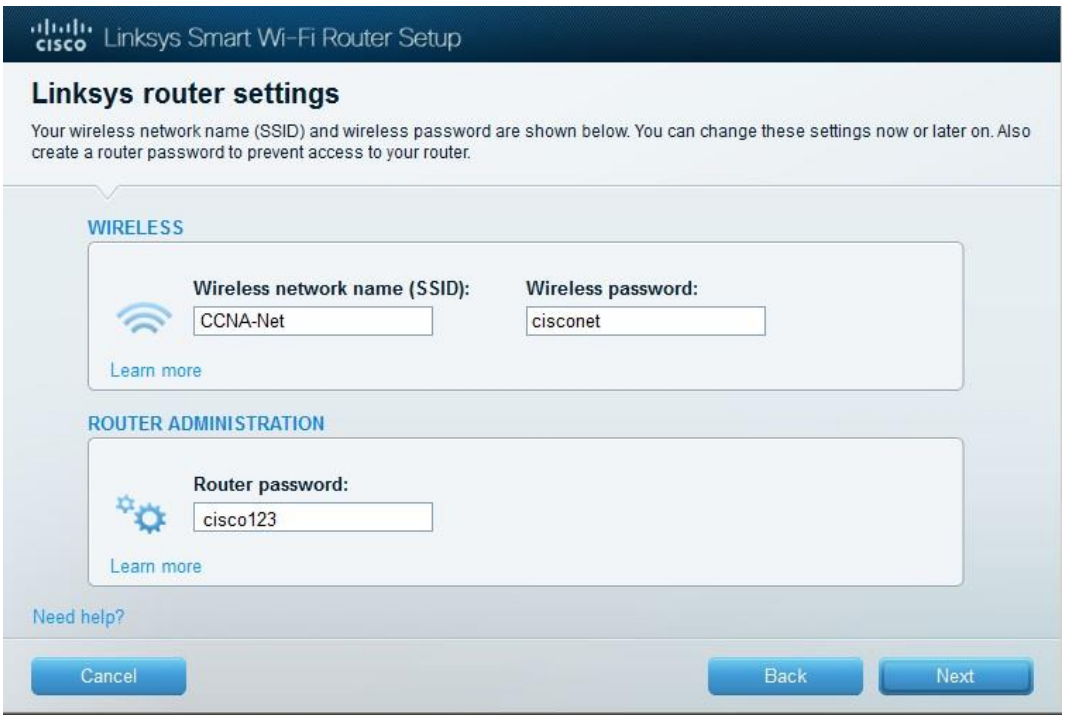
Шаг 2: Подключите кабели в сети в соответствии с топологией.

Следуйте инструкциям по подключению кабеля питания и кабельного модема или DSL-модема с помощью Ethernet-кабеля, которые отобразятся в следующем окне. Можно подключить компьютер к одному из четырех неиспользуемых Ethernet-портов на задней стенке маршрутизатора. После подключения всех необходимых элементов нажмите **Next > (Далее >)**.

Шаг 3: Настройте параметры маршрутизатора Linksys.

a. Дождитесь, когда отобразится окно **Linksys router settings (Настройки маршрутизатора Linksys)**. Для заполнения полей в этом окне используйте данные таблицы **Linksys router settings (Настройки маршрутизатора Linksys)**, приведённой в начале лабораторной работы. Нажмите **Next (Далее)**, чтобы отобразить экран со сводной информацией о настройках маршрутизатора.

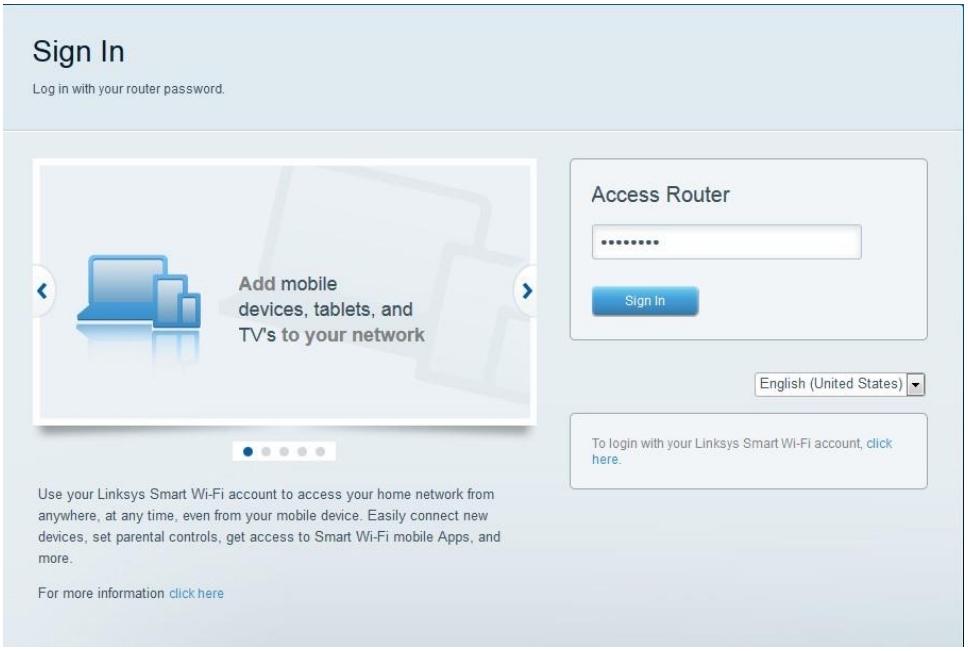
Нажмите **Next (Далее)**.



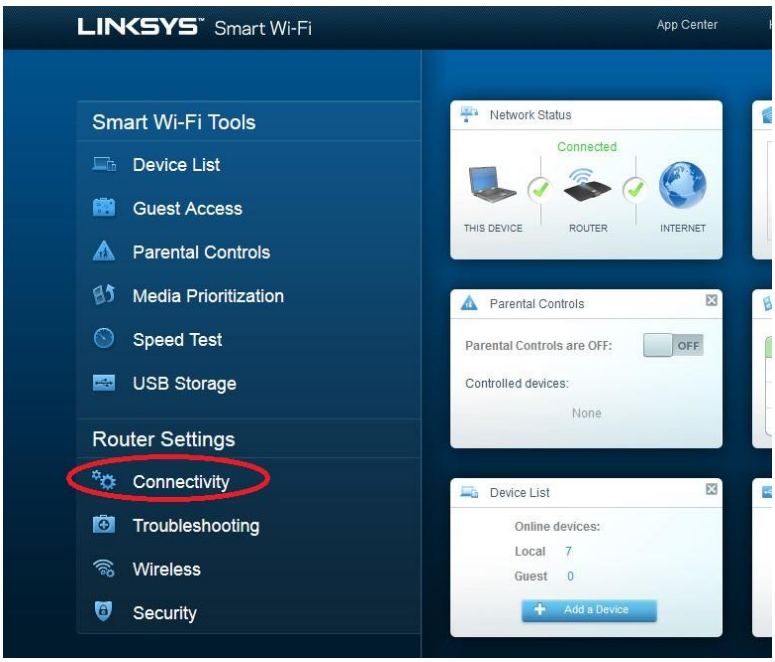
b. Отобразится окно **Create your Linksys Smart Wi-Fi account (Создание учетной записи Linksys Smart Wi-Fi)**. Учетная запись Linksys Smart Wi-Fi используется для ассоциации маршрутизатора к учетной записи, что позволяет удалённо управлять маршрутизатором с помощью браузера или мобильного устройства, на котором запущено приложение Smart Wi-Fi. В рамках этой лабораторной работы пропустите процесс настройки учетной записи. Щелкните поле **No, thanks (Нет, спасибо)** и нажмите **Continue (Продолжить)**.

Примечание. Чтобы настроить учетную запись, перейдите на веб-сайт www.linksyssmartwifi.com.

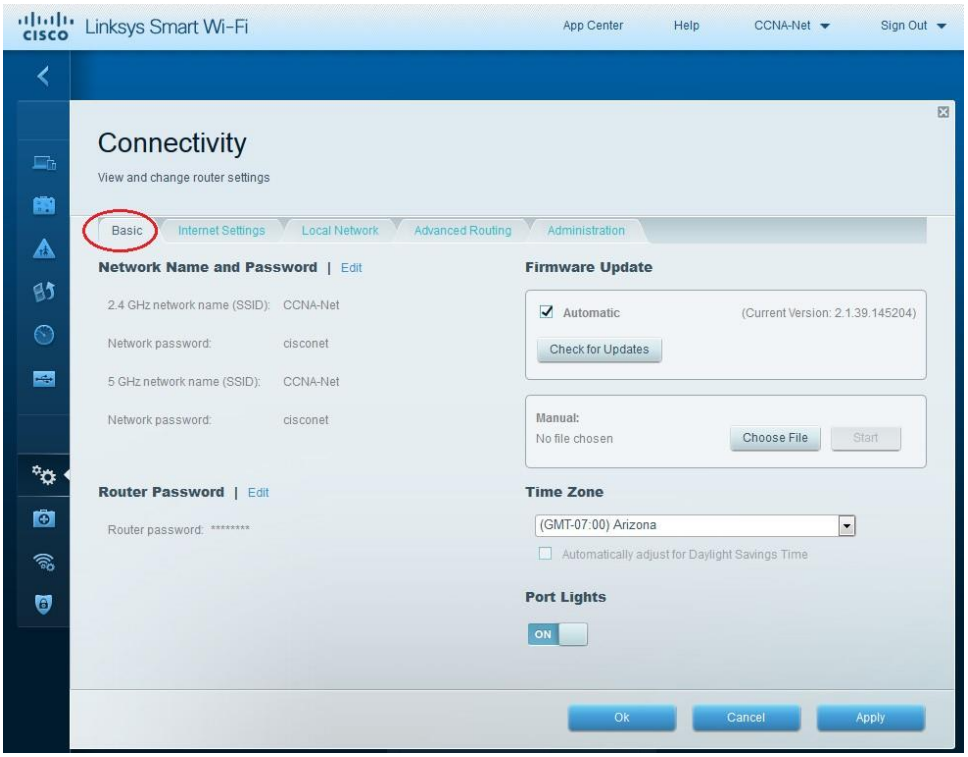
c. Отобразится окно **Sign in (Вход в систему)**. В поле **Access Router (Доступ к маршрутизатору)** введите **cisco123** и нажмите **Sign in (Войти)**.



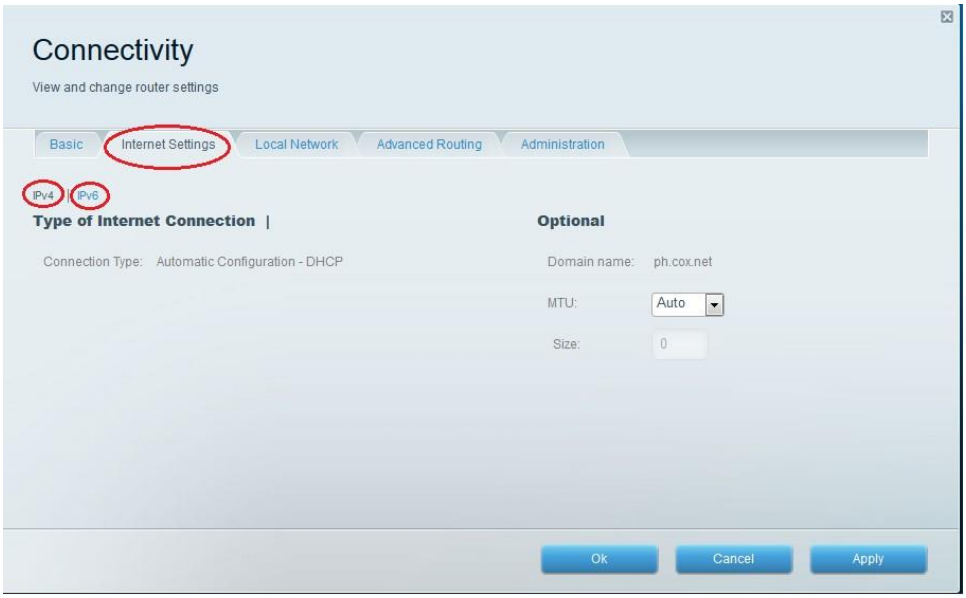
d. На домашней странице Linksys Smart Wi-Fi нажмите **Connectivity (Соединение)** чтобы просмотреть и изменить основные настройки маршрутизатора.



e. На вкладке **Basic (Основные настройки)** можно изменить имя и пароль сети, изменить пароль маршрутизатора, выполнить обновление микропрограммного обеспечения и задать часовой пояс для маршрутизатора. Пароль маршрутизатора и данные о сети настроены в шаге 3a. В раскрывающемся списке выберите соответствующий часовой пояс для маршрутизатора и нажмите **Apply (Применить)**.

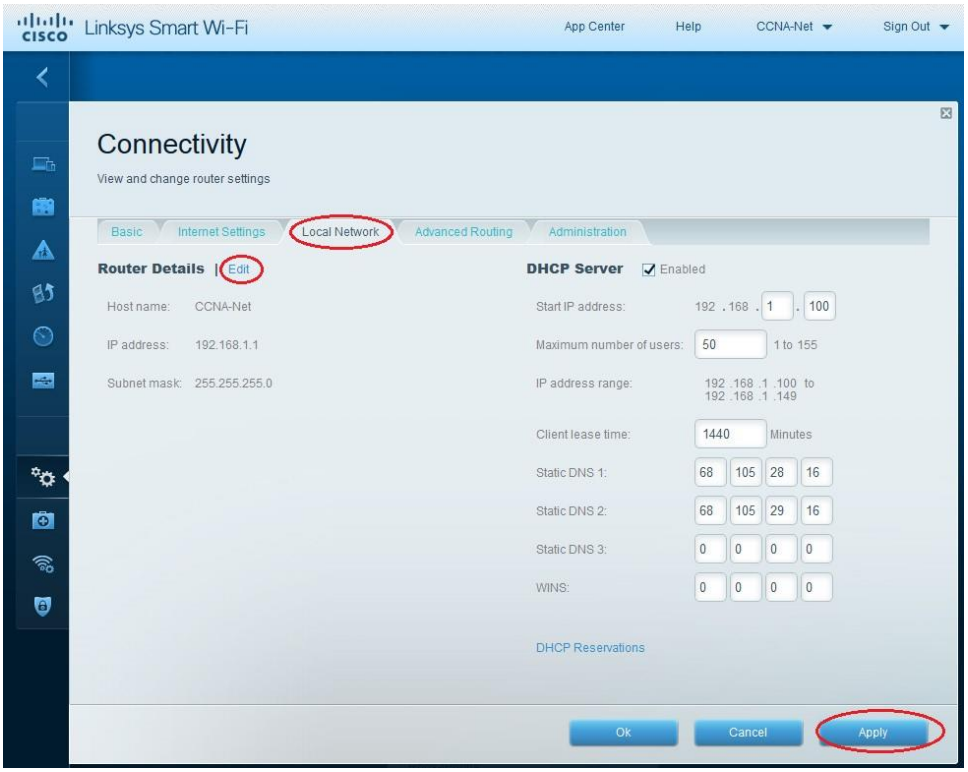


f. На вкладке **Internet Settings (Настройки Интернета)** отображены сведения об интернетподключении. В этом примере маршрутизатор автоматически настраивает подключение для DHCP. На этом экране можно отобразить сведения как об IPv4, так и об IPv6.

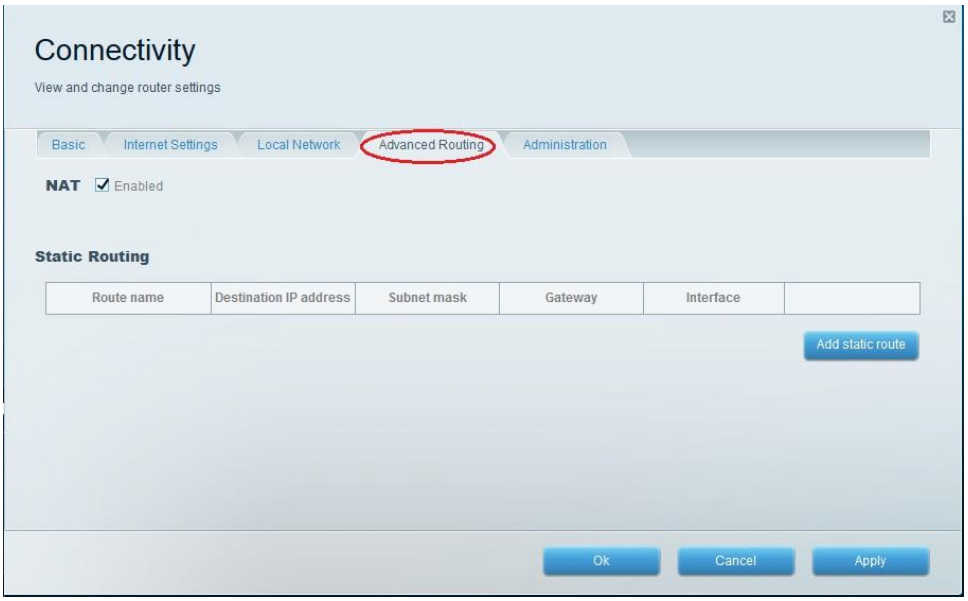


g. На вкладке **Local Network (Локальная сеть)** доступны параметры настройки локального DHCPсервера. В настройках локальной сети по умолчанию задана сеть 192.168.1.0/24 и локальный IPадрес маршрутизатора по умолчанию 192.168.1.1. Эти настройки можно изменить, нажав **Edit (Изменить)** рядом с разделом **Router Details (Сведения о маршрутизаторе)**. На этом экране можно изменить настройки DHCP-сервера. Можно задать начальный адрес DHCP, максимальное число пользователей DHCP, срок аренды клиента и статические DNS-серверы. Нажмите **Apply (Применить)**, чтобы принять все изменения, внесённые на этом экране.

Примечание. Если DHCP используется для получения данных о подключении к сети интернетпровайдера, эти DNS-адреса, наиболее вероятно, будут заполняться данными DNS-сервера интернет-провайдера.

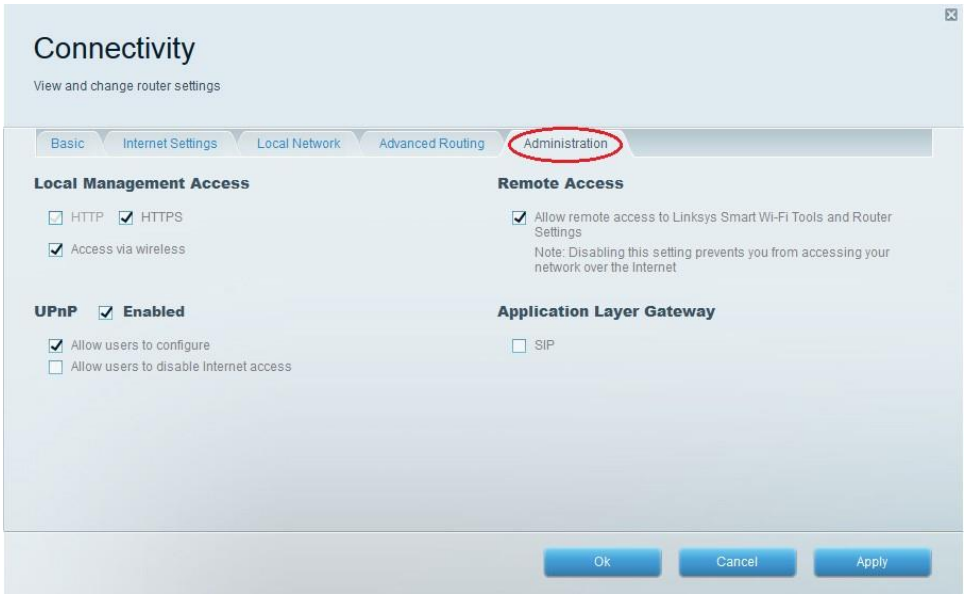


h. На вкладке **Advanced Routing (Дополнительная маршрутизация)** можно отключить функцию преобразования сетевых адресов (NAT), которая по умолчанию включена. На этом экране также можно добавить статические маршруты. Нажмите **Apply (Применить)**, чтобы принять все изменения, внесённые в этом окне.



i. На вкладке **Administration (Администрирование)** доступны элементы управления, с помощью которых

осуществляется управление программным обеспечением Smart Wi-Fi. Щелкнув соответствующее поле, можно активировать доступ к удалённому управлению маршрутизатором. Также можно активировать доступ по HTTPS и ограничить возможности управления беспроводной сетью. На этом экране также доступны элементы управления Universal Plug and Play (UPnP) и шлюза уровня приложения. Нажмите **Apply (Применить)**, чтобы принять все изменения, внесённые в этом окне.

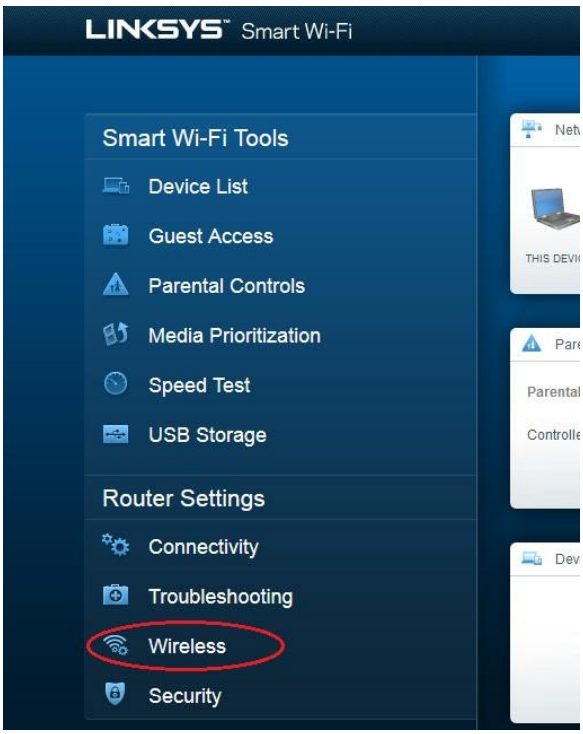


Часть 2: Защита беспроводной сети

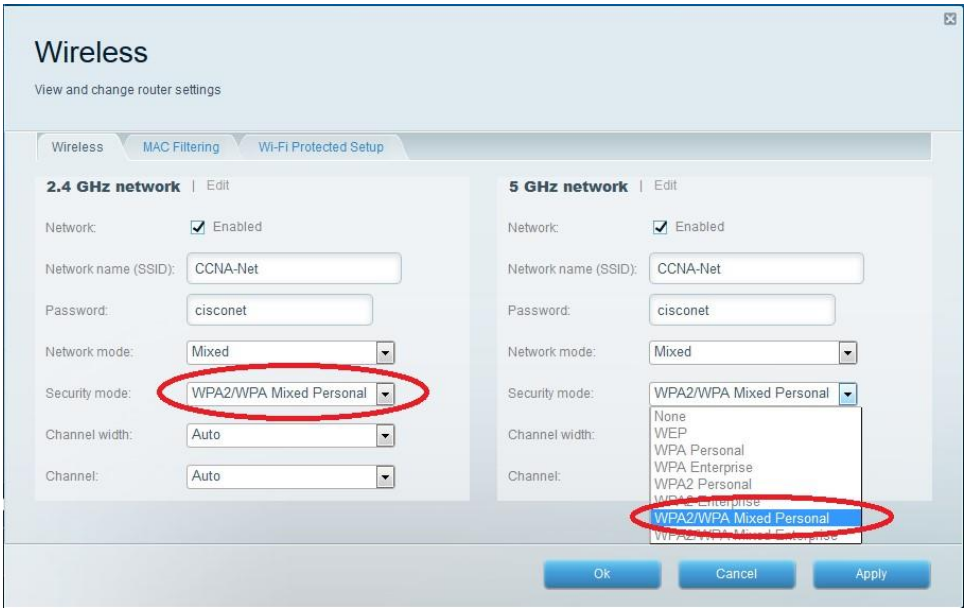
В части 2 вам предстоит настроить функции защиты маршрутизатора Linksys EA Series и рассмотреть параметры межсетевого экрана и переадресации портов на маршрутизаторе Linksys Smart Wi-Fi.

Шаг 1: Добавьте функции безопасности WPA на беспроводные маршрутизаторы.

a. На главной странице Linksys Smart Wi-Fi нажмите **Wireless (Беспроводная связь)**.



b. В окне **Беспроводная связь (Wireless)** отображаются настройки для полос 2,4 и 5 ГГц. Используйте кнопку **Edit (Изменить)** рядом с каждым из столбцов, чтобы изменить настройки безопасности для каждого частотного диапазона беспроводной сети. Имя и пароль сети ранее настроены в части 1. Нажмите раскрывающийся список **Security mode (Режим безопасности)**, чтобы выбрать параметр **WPA2/WPA Mixed Personal** для каждого из диапазонов. Нажмите **Apply (Применить)**, чтобы сохранить свои настройки, после чего нажмите **ОК**.



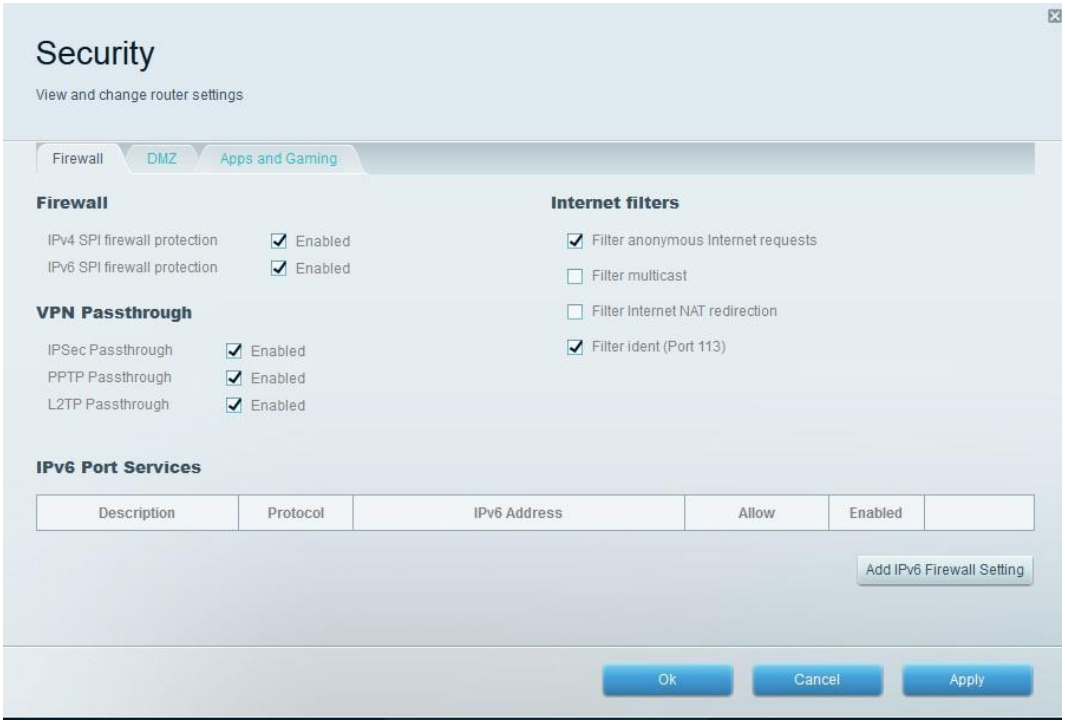
Шаг 2: Примените настройки межсетевого экрана и переадресации портов.

a. На главной странице Linksys Smart Wi-Fi нажмите **Security (Безопасность)**. В окнах

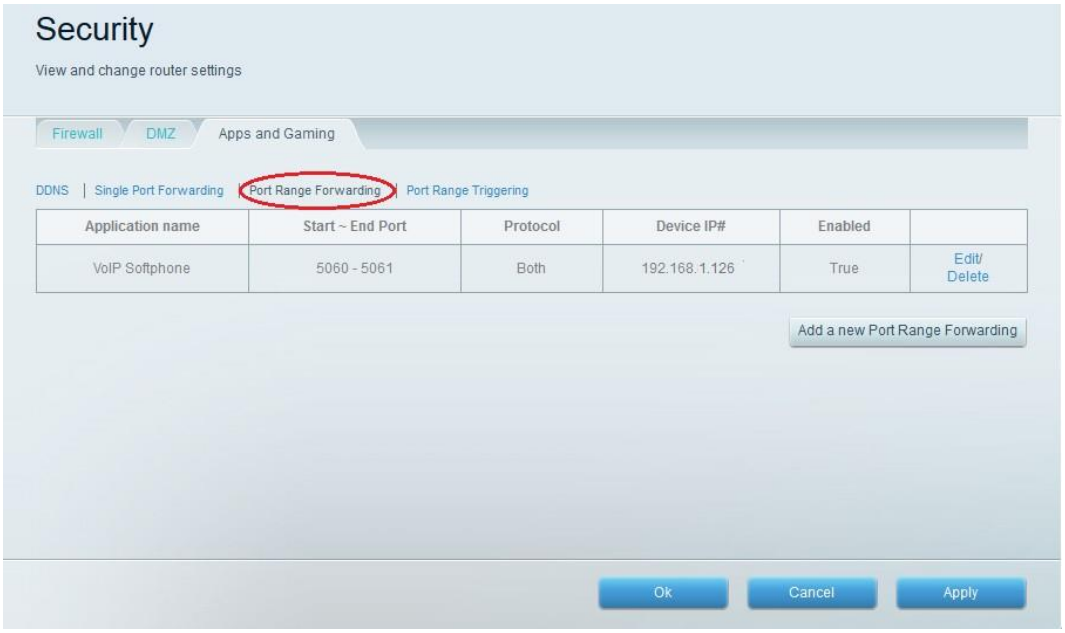
Безопасность (Security) доступны вкладки **Firewall (Межсетевой экран)**, **DMZ** и **Apps and Gamig (Приложения и игры)**, на которых можно просмотреть и изменить настройки безопасности маршрутизатора.

b. На вкладке **Firewall (Межсетевой экран)** отображается раздел настроек межсетевого экрана, где можно включить или отключить защиту межсетевого экрана с анализом пакетов с учетом состояния соединений (SPI) для IPv4 и IPv6, параметры транзитной пересылки по виртуальной частной сети (VPN) и

интернет-фильтры. Нажмите **Apply (Применить)**, чтобы принять все изменения, внесённые в этом окне.



c. На вкладке **Apps and Gamig (Приложения и игры)** доступны функции переадресации портов. В этом примере порты 5060 и 5061 открыты для программного телефона VoIP, запущенного на локальном устройстве с IP-адресом 192.168.1.126. Нажмите **Apply (Применить)**, чтобы принять все изменения, внесённые в этом окне.

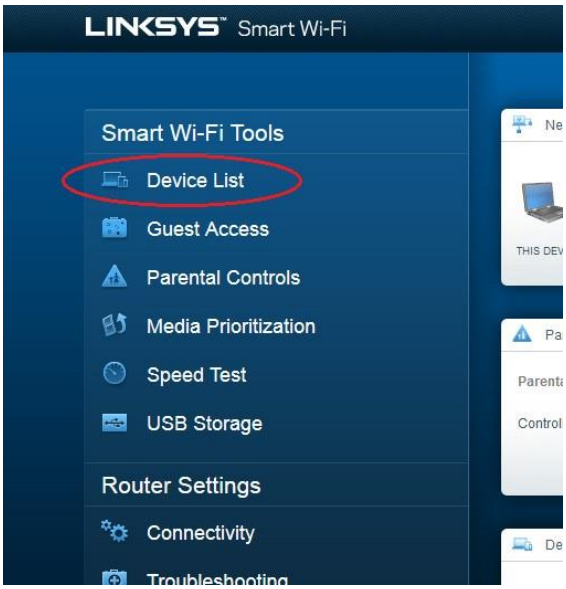


Часть 3: Изучение дополнительных функций на маршрутизаторе Lynksys серии EA

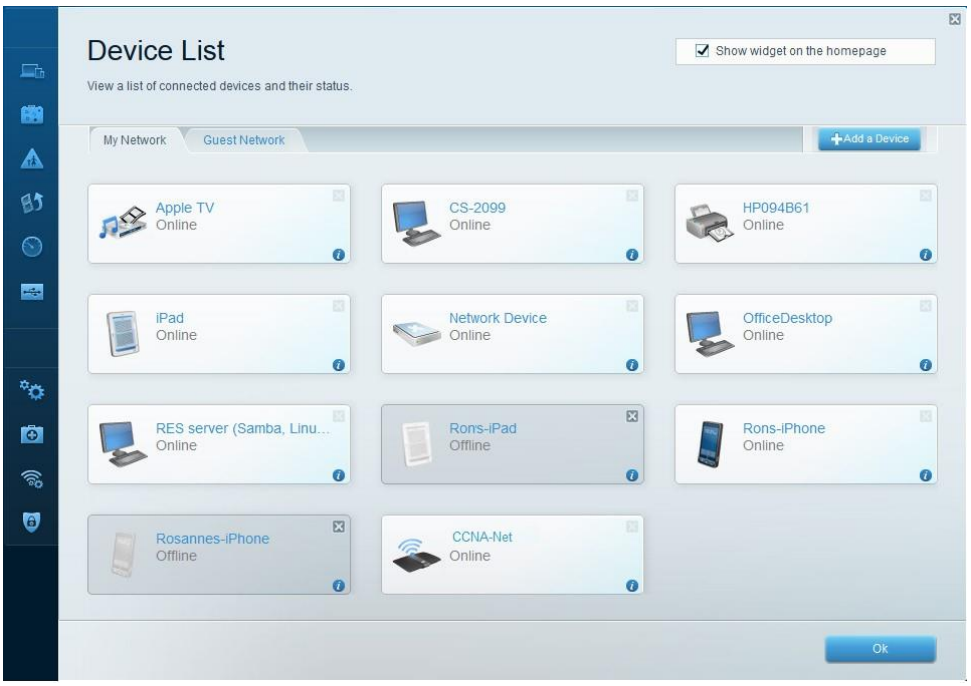
В части 3 вам предстоит рассмотреть ряд дополнительных функций, доступных на маршрутизаторе Linksys EA Series.

Шаг 1: Изучите инструменты Smart Wi-Fi.

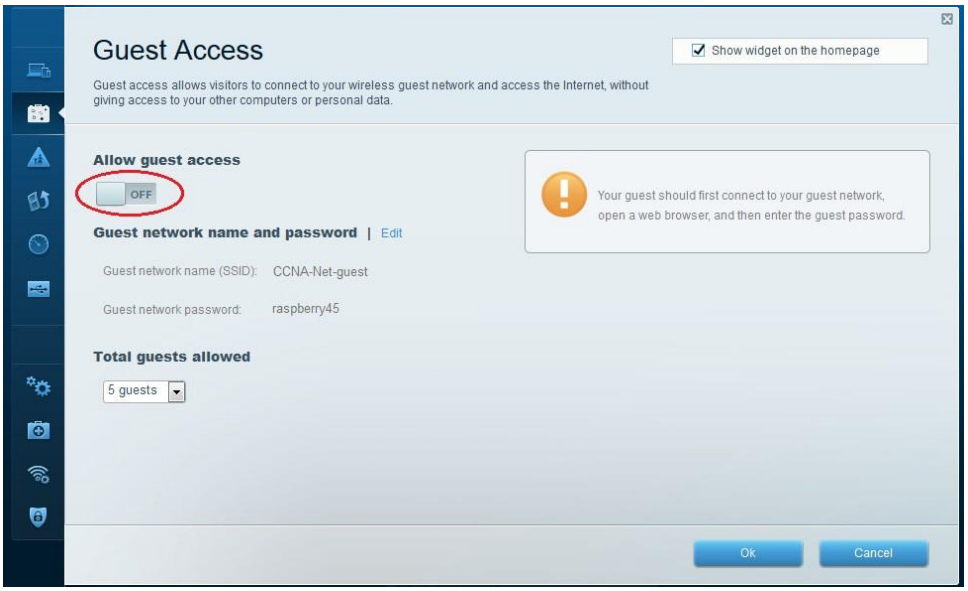
a. На главной странице Linksys Smart Wi-Fi нажмите **Device List (Список устройств)**.



В окне **Список устройств (Device List)** отображается список клиентов в локальной сети. Обратите внимание на вкладку **Guest Network (Гостевая сеть)**. Если гостевая сеть активирована, клиенты этой сети отображаются на вкладке **Guest Network (Гостевая сеть)**.

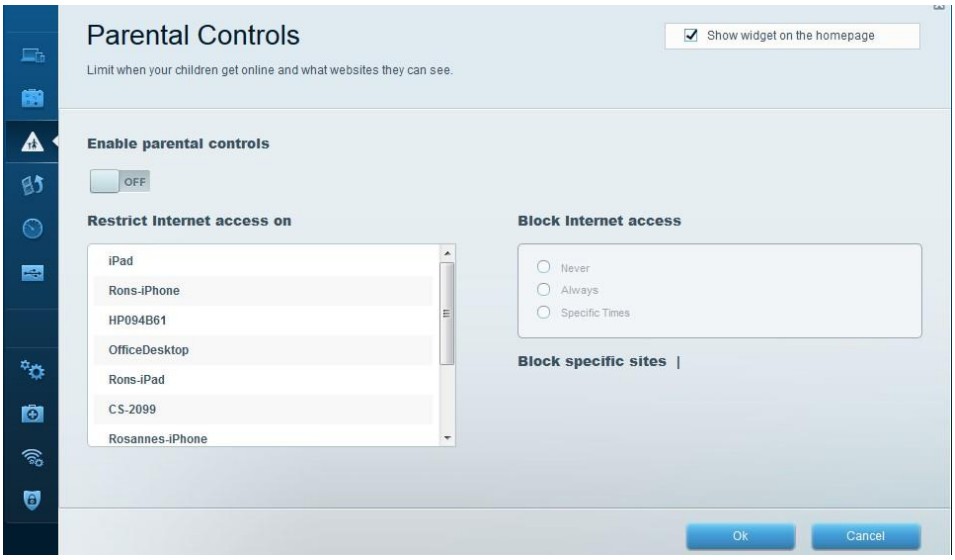


b. На главной странице Linksys Smart Wi-Fi нажмите **Guest Access (Гостевой доступ)**. Клиенты гостевой сети имеют доступ только к сети Интернет и не имеют доступа к другим клиентам локальной сети. Чтобы разрешить гостевой доступ, нажмите на кнопку **Allow guest access (Разрешить гостевой доступ)**. Щелкните ссылку **Edit (Изменить)** (рядом с именем и паролем гостевой сети), чтобы изменить пароль гостевой сети, и нажмите **ОК**, чтобы принять и сохранить изменения.

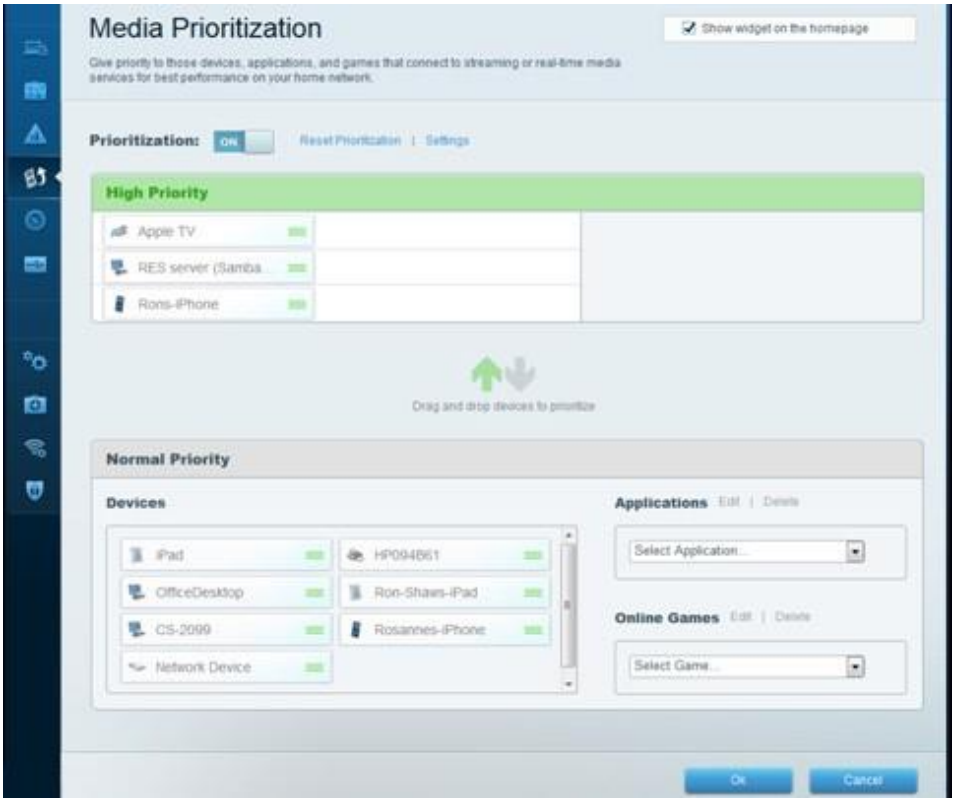


c. На главной странице Linksys Smart Wi-Fi нажмите **Parental Control (Родительский контроль)**. Эти параметры можно

использовать для ограничения доступа к Интернету на отдельных устройствах, а также чтобы ограничить доступ по времени и доступ к веб-сайтам. Нажмите **OK**, чтобы сохранить настройки.



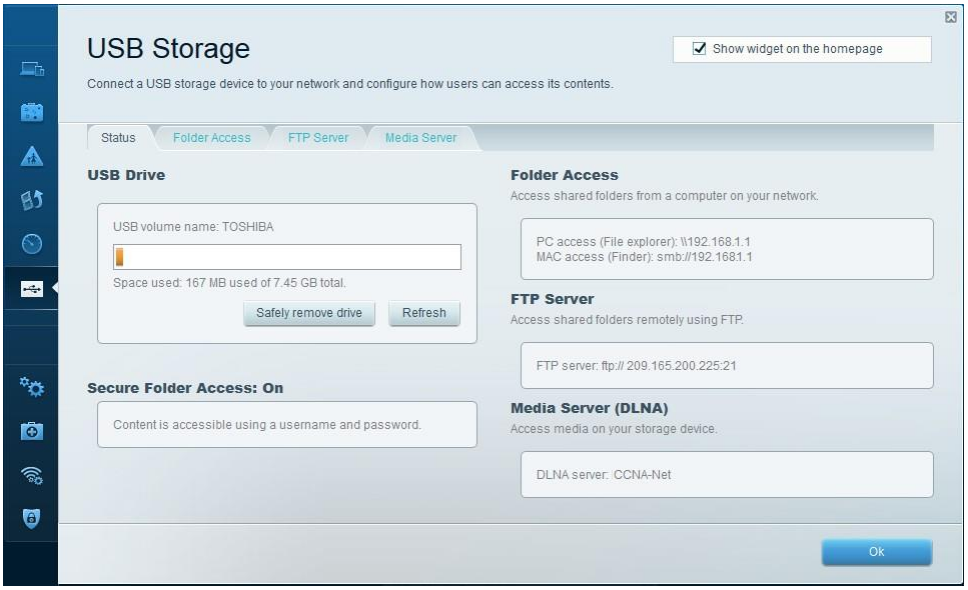
d. На главной странице Linksys Smart Wi-Fi выберите **Media Prioritization (Приоритизация мультимедиа)**. С помощью этих параметров можно назначить приоритет пропускной способности сети для выбранных устройств в локальной сети. В этом примере устройству, помеченному как «Apple TV», назначается самый высокий приоритет для ресурсов сети. Чтобы изменить настройки приоритетов, просто перетащите устройства в списке и нажмите **OK**, чтобы сохранить настройки.



e. На главной странице Linksys Smart Wi-Fi нажмите **Speed Test (Проверка скорости)**. Эта утилита используется для проверки скорости доступа к Интернету. В этом примере показаны результаты проверки скорости. Маршрутизатор сохраняет результаты всех проверок скорости и предоставляет возможность вывода этих журналов на экран.

f. На главной странице Linksys Smart Wi-Fi нажмите **USB Storage (Устройство хранения USB)**. Этот экран используется

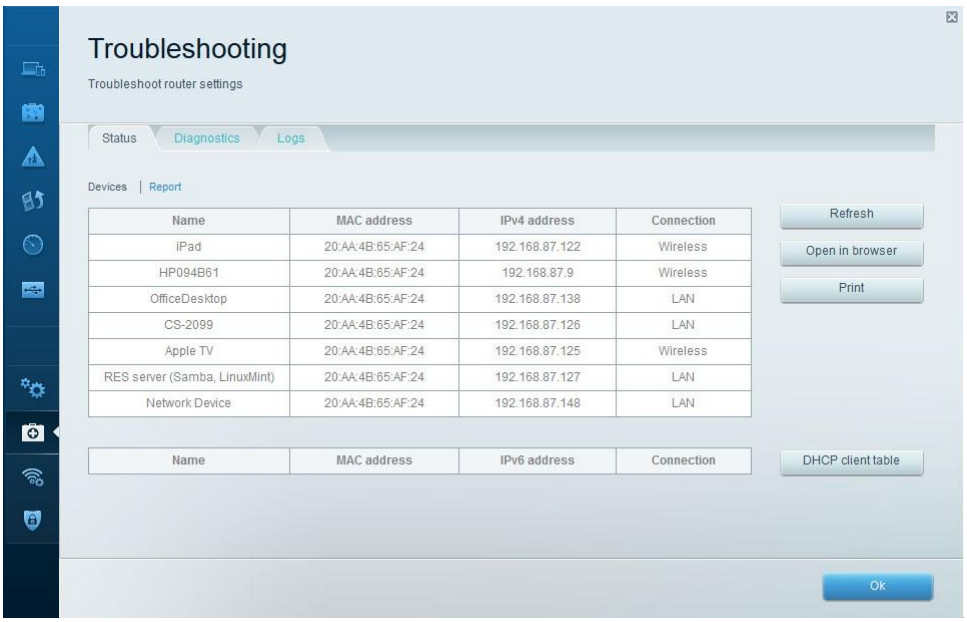
для просмотра настроек USB-накопителя. Отсюда можно перейти на соответствующую вкладку для настройки FTP-серверов и серверов мультимедиа. Также можно настроить отдельные учетные записи пользователей для доступа к этим серверам. Для этого нажмите вкладки в верхней части данного экрана. Чтобы использовать этот параметр, необходимо подсоединить USB-накопитель к задней стенке маршрутизатора. Нажмите **OK**, чтобы сохранить все внесённые изменения.



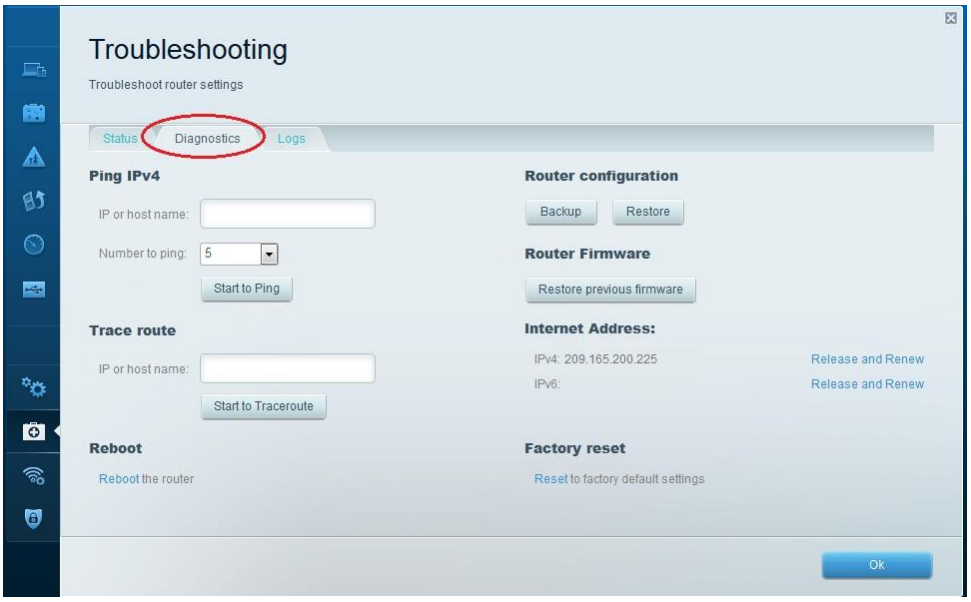
Шаг 2: Поиск и устранение неполадок в работе маршрутизатора.

На главной странице Linksys Smart Wi-Fi нажмите **Troubleshooting (Поиск и устранение неполадок)**.

a. На вкладке **Status (Состояние)** представлен список клиентов локальной сети, а также MAC-адреса и IP-адреса их сетевых адаптеров. На этой вкладке также отображается способ их подключения к сети. Нажмите **OK**, чтобы сохранить все внесённые изменения.

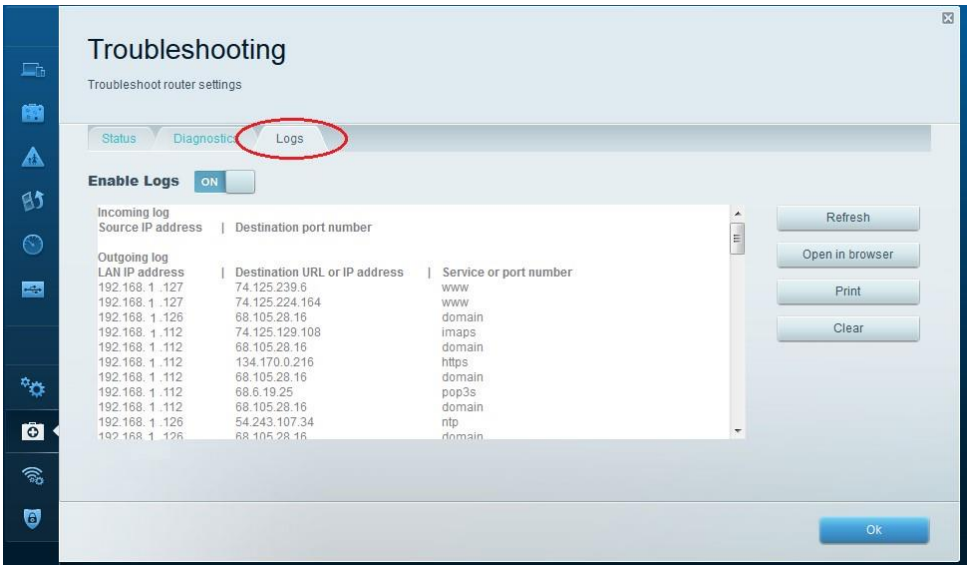


b. На вкладке **Diagnostics (Диагностика)** представлены утилиты ping и traceroute. С помощью этой вкладки также можно перезагрузить маршрутизатор, выполнить резервное копирование или восстановление конфигурации маршрутизатора, восстановить предыдущую версию микропрограммного обеспечения, опубликовать и обновить интернет-адреса на своем маршрутизаторе и выполнить сброс до заводских настроек по умолчанию. Нажмите **OK**, чтобы сохранить все внесённые изменения.



На вкладке **Logs (Журналы)** доступны журналы «Входящие», «Исходящие», «Безопасность» и «DHCP». С этого экрана можно

отправить журналы на печать или удалить их. Нажмите **OK**, чтобы сохранить все внесённые изменения.



Часть 4: Подключение клиента беспроводной сети

В части 4 вам предстоит настроить адаптер беспроводной сети на компьютере для подключения к маршрутизатору Linksys EA Series.

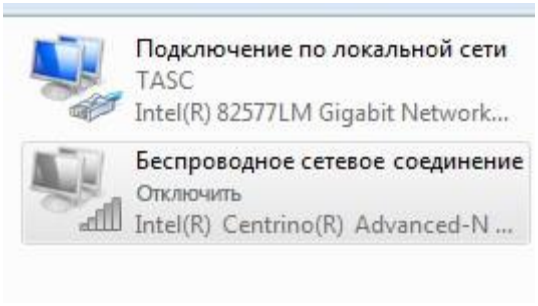
Примечание. Данная лабораторная работа была выполнена на ПК под управлением ОС Windows 7. Ее можно выполнить и с любой другой из указанных версий операционной системы Windows, однако параметры меню и окна в этом случае могут отличаться.

Шаг 3: Используйте «Центр управления сетями и общим доступом».

a. Откройте **Центр управления сетями и общим доступом**, нажав кнопку **Пуск > Панель управления > Просмотр состояния сети и задач** под заголовком «Сеть и Интернет» в представлении по категориям.

b. В левой части экрана нажмите на ссылку **Изменение параметров адаптера**.

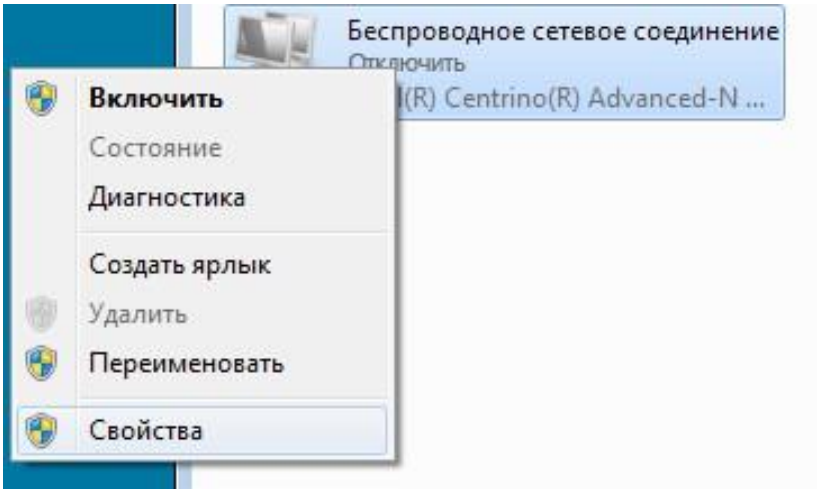
Откроется окно **Сетевые подключения** со списком доступных сетевых адаптеров на этом компьютере. В данном окне найдите адаптеры **Подключение по локальной сети** и **беспроводное сетевое соединение**.



Примечание. В этом окне могут отображаться также адаптеры виртуальной частной сети (VPN) и другие типы сетевых подключений.

Шаг 4: Поработайте с беспроводным сетевым адаптером.

a. Выберите и щелкните правой кнопкой мыши параметр **беспроводное сетевое соединение**, чтобы отобразить раскрывающийся список. Если сетевой адаптер отключен, необходимо **Включить** его.



b. Нажмите правой кнопкой мыши на **Wireless Network Connection (беспроводное сетевое соединение)**, и выберите **Connect/Disconnect (Подключить/Отключить)**. Здесь показан список идентификаторов SSID в диапазоне действия сетевого адаптера. Выберите **CCNA-Net**, затем нажмите **Connect (Подключить)**.

c. Когда отобразится соответствующий запрос, введите **cisconet**, чтобы указать ключ безопасности сети, после чего нажмите **OK**.

d. Если доступно подключение к беспроводной сети, на панели задач должен отображаться значок беспроводной сети. Нажмите на этот значок, чтобы отобразить список идентификаторов SSID в диапазоне действия сетевого адаптера.

e. Идентификатор SSID **CCNA-Net** теперь должен показывать подключение к беспроводной сети CCNA.

Вопросы на закрепление

Почему вам не стоит использовать инструменты безопасности WEP для своей беспроводной сети?

_____

_____

Практическая работа 8

Тема: Настройка базового протокола OSPFv2 для одной области

Цели: Провести настройку OSPFv2 для одной области

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задачи

Часть 1. Построение сети и настройка базовых параметров устройства

Часть 2. Настройка и проверка маршрутизации OSPF

Часть 3. Изменение значения ID маршрутизатора

Часть 4. Настройка пассивных интерфейсов OSPF Часть 5. Изменение метрик OSPF

Исходные данные/сценарий

Алгоритм кратчайшего пути (OSPF) — протокол маршрутизации для IP-сетей на базе состояния канала. Версия OSPFv2 используется для сетей протокола IPv4, а OSPFv3 - для сетей IPv6. OSPF обнаруживает изменения в топологии, например сбой канала, и быстро сходится в новой беспетлевой структуре маршрутизации. OSPF рассчитывает каждый маршрут с помощью алгоритма Дейкстры, т.е. алгоритма кратчайшего пути.

В данной лабораторной работе необходимо настроить топологию сети с маршрутизацией OSPFv2, изменить значения ID маршрутизатора, настроить пассивные интерфейсы, установить метрики OSPF и использовать несколько команд интерфейса командной строки для вывода и проверки данных маршрутизации OSPF.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсах маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Топология

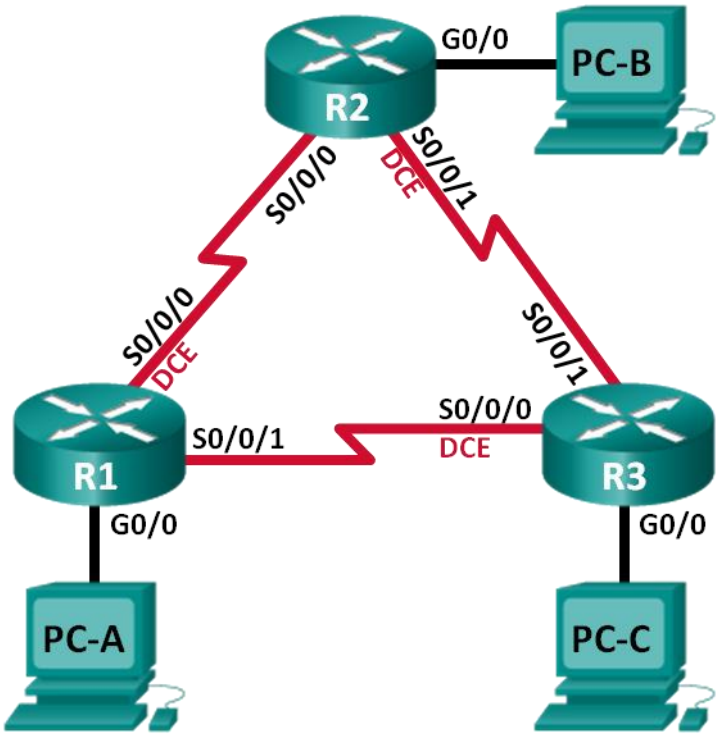


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252	N/A
	S0/0/1	192.168.13.1	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	192.168.12.2	255.255.255.252	N/A
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	N/A
	S0/0/1	192.168.23.2	255.255.255.252	N/A

PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и настройка базовых параметров устройства

В первой части вам предстоит создать топологию сети и настроить основные параметры для узлов и маршрутизаторов.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните запуск и перезагрузку маршрутизаторов.

Шаг 3: Настройте базовые параметры каждого маршрутизатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте **class** в качестве пароля привилегированного режима EXEC.

d. Назначьте **cisco** в качестве паролей консоли и VTY.

e. Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.

f. Настройте **logging synchronous** для консольного канала.

g. Назначьте IP-адреса всем интерфейсам в соответствии с таблицей адресации.

h. Установите значение тактовой частоты на всех последовательных интерфейсах DCE на **128000**.

i. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 4: Настройте узлы ПК.

Шаг 5: Проверка соединения.

Маршрутизаторы должны иметь возможность отправлять успешные эхо-запросы друг другу, и все ПК должны иметь возможность отправлять успешные эхо-запросы на свои шлюзы по умолчанию. Компьютеры не могут отправлять успешные эхо-запросы на другие ПК, пока не настроена маршрутизация OSPF. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.

Часть 2: Настройка и проверка маршрутизации OSPF

Во второй части вам предстоит настроить маршрутизацию OSPFv2 на всех маршрутизаторах в сети, а затем убедиться, что таблицы маршрутизации обновляются верным образом. После проверки OSPF, для повышения уровня безопасности необходимо настроить на каналах аутентификацию протокола OSPF.

Шаг 1: Настройте маршрутизацию OSPF на маршрутизаторе R1.

a. Используйте команду **router ospf** в режиме глобальной конфигурации, чтобы активировать OSPF на маршрутизаторе R1.

R1(config)# **router ospf 1**

Примечание. Идентификатор процесса OSPF хранится локально и не имеет отношения к другим маршрутизаторам в сети.

b. Используйте команду **network** для сетей маршрутизатора R1. Используйте идентификатор области, равный 0.

R1(config-router)# **network 192.168.1.0 0.0.0.255 area 0**

R1(config-router)# **network 192.168.12.0 0.0.0.3 area 0**

R1(config-router)# **network 192.168.13.0 0.0.0.3 area 0**

Шаг 2: Настройте OSPF на маршрутизаторах R2 и R3.

Используйте команду **router ospf** и добавьте команду **network** для сетей маршрутизаторов R2 и R3. Когда маршрутизация OSPF будет настроена на R2 и R3, на маршрутизаторе R1 появятся сообщения об установленных отношениях смежности.

R1#

00:22:29: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on Serial0/0/0 from LOADING to

FULL, e

Loading

Don

R1#

00:23:14: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.2 on Serial0/0/1 from LOADING to

FULL, e

Loading

Don

R1#

Шаг 3: Проверьте информацию о соседях и маршрутизации OSPF.

a. Используйте команду **show ip ospf neighbor** для проверки списка смежных маршрутизаторов на каждом маршрутизаторе в соответствии с топологией.

R1# **show ip ospf neighbor**

Neighbor ID Pri State Dead Time Address Interface

192.168.23.2 0 FULL/ - 00:00:33 192.168.13.2 Serial0/0/1

192.168.23.1 0 FULL/ - 00:00:30 192.168.12.2 Serial0/0/0

b. Выполните команду **show ip route**, чтобы убедиться, что в таблицах маршрутизации всех маршрутизаторов отображаются все сети.

R1# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, GigabitEthernet0/0

L 192.168.1.1/32 is directly connected, GigabitEthernet0/0

O 192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0

O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:31:48, Serial0/0/1

192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.12.0/30 is directly connected, Serial0/0/0

L 192.168.12.1/32 is directly connected, Serial0/0/0

192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.13.0/30 is directly connected, Serial0/0/1

L 192.168.13.1/32 is directly connected, Serial0/0/1

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0/30 [110/128] via 192.168.12.2, 00:31:38, Serial0/0/0

[110/128] via 192.168.13.2, 00:31:38, Serial0/0/1

Какую команду вы бы применили, чтобы просмотреть только маршруты OSPF в таблице маршрутизации?

_____

_____

Шаг 4: Проверьте настройки протокола OSPF.

Команда **show ip protocols** обеспечивает быструю проверку критически важных данных конфигурации OSPF. К таким данным относятся идентификатор процесса OSPF, идентификатор маршрутизатора, сети, объявляемые маршрутизатором, соседние устройства, от которых маршрутизатор принимает обновления, и значение административной дистанции по умолчанию, равное 110 для OSPF.

R1# **show ip protocols**

*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 192.168.13.1

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4 Routing for Networks:

192.168.1.0 0.0.0.255 area 0

192.168.12.0 0.0.0.3 area 0

192.168.13.0 0.0.0.3 area 0 Routing Information Sources:

Gateway Distance Last Update

192.168.23.2 110 00:19:16

192.168.23.1 110 00:20:03

Distance: (default is 110)

Шаг 5: Проверьте данные процесса OSPF.

Используйте команду **show ip ospf**, чтобы просмотреть идентификаторы процесса OSPF и маршрутизатора. Данная команда отображает данные о зоне OSPF и показывает время, когда последний раз выполнялся алгоритм поиска кратчайшего пути SPF.

R1# **show ip ospf**

Routing Process "ospf 1" with ID 192.168.13.1

Start time: 00:20:23.260, Time elapsed: 00:25:08.296

Supports only single TOS(TOS0) routes

Supports opaque LSA

Supports Link-local Signaling (LLS)

Supports area transit capability

Supports NSSA (compatible with RFC 3101)

Event-log enabled, Maximum number of events: 1000, Mode: cyclic

Router is not originating router-LSAs with maximum metric

Initial SPF schedule delay 5000 msecs

Minimum hold time between two consecutive SPFs 10000 msecs

Maximum wait time between two consecutive SPFs 10000 msecs

Incremental-SPF disabled

Minimum LSA interval 5 secs

Minimum LSA arrival 1000 msecs

LSA group pacing timer 240 secs

Interface flood pacing timer 33 msecs

Retransmission pacing timer 66 msecs

Number of external LSA 0. Checksum Sum 0x000000

Number of opaque AS LSA 0. Checksum Sum 0x000000

Number of DCbitless external and opaque AS LSA 0

Number of DoNotAge external and opaque AS LSA 0

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Number of areas transit capable is 0

External flood list length 0

IETF NSF helper support enabled

Cisco NSF helper support enabled

Reference bandwidth unit is 100 mbps

Area BACKBONE(0)

Number of interfaces in this area is 3

Area has no authentication

SPF algorithm last executed 00:22:53.756 ago

SPF algorithm executed 7 times

Area ranges are

Number of LSA 3. Checksum Sum 0x019A61

Number of opaque link LSA 0. Checksum Sum 0x000000

Number of DCbitless LSA 0

Number of indication LSA 0

Number of DoNotAge LSA 0

Flood list length 0

Шаг 6: Проверьте настройки интерфейса OSPF.

a. Выполните команду **show ip ospf interface brief**, чтобы отобразить сводку об интерфейсах, на которых активирован алгоритм OSPF.

R1# **show ip ospf interface brief**

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs F/C
Se0/0/1	1	0	192.168.13.1/30	64	P2P	1/1
Se0/0/0	1	0	192.168.12.1/30	64	P2P	1/1
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0

b. Для того чтобы увидеть более подробные данные об интерфейсах, на которых активирован OSPF, выполните команду **show ip ospf interface**.

R1# **show ip ospf interface**

Serial0/0/1 is up, line protocol is up

Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement

Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT, Cost: 64

Topology-MTID Cost Disabled Shutdown Topology Name

0 64 no no Base

Transmit Delay is 1 sec, State POINT_TO_POINT Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 oob-resync timeout 40 Hello due in 00:00:01

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 3/3, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 192.168.23.2

Suppress hello for 0 neighbor(s)

Serial0/0/0 is up, line protocol is up

Internet Address 192.168.12.1/30, Area 0, Attached via Network Statement

Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT, Cost: 64

Topology-MTID Cost Disabled Shutdown Topology Name

0 64 no no Base

Transmit Delay is 1 sec, State POINT_TO_POINT Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 oob-resync timeout 40 Hello due in 00:00:03

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 2/2, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 192.168.23.1

Suppress hello for 0 neighbor(s)

GigabitEthernet0/0 is up, line protocol is up

Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement

Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost: 1

Topology-MTID Cost Disabled Shutdown Topology Name

0 1 no no Base

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 192.168.13.1, Interface address 192.168.1.1

No backup designated router on this network Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 oob-resync timeout 40 Hello due in 00:00:01

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 0, maximum is 0

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

Шаг 7: Проверьте наличие сквозного соединения.

Все компьютеры должны успешно выполнять эхо-запросы ко всем остальным компьютерам, указанным в топологии. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Часть 3: Изменение значения ID маршрутизатора

Идентификатор OSPF-маршрутизатора используется для уникальной идентификации маршрутизатора в домене маршрутизации OSPF. Маршрутизаторы компании Cisco получают ID маршрутизатора одним из трёх способов в следующем порядке:

1) IP-адрес, установленный с помощью команды OSPF **router-id** (при наличии)
2) Наивысший IP-адрес любого из loopback-адресов маршрутизатора (при наличии)
3) Наивысший активный IP-адрес любого из физических интерфейсов маршрутизатора

Поскольку ни на одном из трёх маршрутизаторов не настроены идентификаторы маршрутизатора или loopback-интерфейсы, идентификатор каждого маршрутизатора определяется наивысшим IP-адресом любого активного интерфейса.

В третьей части вам необходимо изменить значение ID идентификатора OSPF-маршрутизатора с помощью loopback-адресов. Также вам предстоит использовать команду **router-id** для изменения идентификатора маршрутизатора.

Шаг 1: Измените идентификаторы маршрутизатора, используя loopback-адреса.

a. Назначьте IP-адрес loopback 0 для маршрутизатора R1.

R1(config)# **interface lo0**

R1(config-if)# **ip address 1.1.1.1 255.255.255.255**

R1(config-if)# end

b. Назначьте IP-адреса loopback 0 для маршрутизаторов R2 и R3. Используйте IP-адрес 2.2.2.2/32 для R2 и 3.3.3.3/32 для R3.

c. Сохраните текущую конфигурацию в загрузочную на всех трёх маршрутизаторах.

d. Для того чтобы идентификатор маршрутизатора получил значение loopback-адреса, необходимо перезагрузить маршрутизаторы. Выполните команду **reload** на всех трёх маршрутизаторах. Нажмите клавишу Enter, чтобы подтвердить перезагрузку.

e. После перезагрузки маршрутизатора выполните команду **show ip protocols**, чтобы просмотреть новый идентификатор маршрутизатора

R1# **show ip protocols**

*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 1.1.1.1

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4 Routing for Networks:

192.168.1.0 0.0.0.255 area 0

192.168.12.0 0.0.0.3 area 0

192.168.13.0 0.0.0.3 area 0 Routing Information Sources:

Gateway Distance Last Update

3.3.3.3 110 00:01:00

2.2.2.2 110 00:01:14

Distance: (default is 110)

f. Выполните **show ip ospf neighbor**, чтобы отобразить изменения идентификатора маршрутизатора для соседних маршрутизаторов.

R1# **show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	0	FULL/ -	00:00:35	192.168.13.2	Serial0/0/1
2.2.2.2	0	FULL/ -	00:00:32	192.168.12.2	Serial0/0/0

R1#

Шаг 2: Измените идентификатор маршрутизатора R1 с помощью команды router-id.

Наиболее предпочтительным способом изменения ID маршрутизатора осуществляется с помощью команды **router-id**.

a. Чтобы переназначить идентификатор маршрутизатора, выполните команду **router-id 11.11.11.11** на маршрутизаторе R1. Обратите внимание на уведомление, которое появляется при выполнении команды **router-id**.

R1(config)# **router ospf 1**

R1(config-router)# **router-id 11.11.11.11**

Reload or use "clear ip ospf process" command, for this to take effect

R1(config)# end

b. Вы получите уведомление о том, что для того, чтобы изменения вступили в силу, вам необходимо либо перезагрузить маршрутизатор, либо использовать команду **clear ip ospf process**. Выполните команду **clear ip ospf process** на всех трёх

маршрутизаторах. Введите **yes**, чтобы подтвердить сброс, и нажмите клавишу Enter.

c. Для маршрутизатора R2 настройте идентификатор **22.22.22.22**, а для маршрутизатора R3 - идентификатор **33.33.33.33**. Затем используйте команду **clear ip ospf process**, чтобы сбросить процесс маршрутизации OSPF.

d. Выполните команду **show ip protocols**, чтобы проверить изменился ли идентификатор маршрутизатора R1.

R1# **show ip protocols**

*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 11.11.11.11

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4 Routing for Networks:

192.168.1.0 0.0.0.255 area 0

192.168.12.0 0.0.0.3 area 0

192.168.13.0 0.0.0.3 area 0 Passive Interface(s):

GigabitEthernet0/1 Routing Information Sources:

Gateway Distance Last Update

33.33.33.33 110 00:00:19

22.22.22.22 110 00:00:31

3.3.3.3 110 00:00:41

2.2.2.2 110 00:00:41

Distance: (default is 110)

е. Выполните команду **show ip ospf neighbor** на маршрутизаторе R1, чтобы убедиться, что новые идентификаторы маршрутизаторов R2 и R3 содержатся в списке.

R1# **show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:36	192.168.13.2	Serial0/0/1
22.22.22.22	0	FULL/ -	00:00:32	192.168.12.2	Serial0/0/0

Часть 4: Настройка пассивных интерфейсов OSPF

Команда **passive-interface** запрещает отправку обновлений маршрутизации из определённого интерфейса маршрутизатора. В большинстве случаев команда используется для уменьшения трафика в сетях LAN, поскольку им не нужно получать сообщения протокола динамической маршрутизации. В четвёртой части вам предстоит использовать команду **passive-interface** для настройки интерфейса в качестве пассивного. Также вы настроите OSPF таким образом, чтобы все интерфейсы маршрутизатора были пассивными по умолчанию, а затем включите объявления протокола маршрутизации OSPF на выбранных интерфейсах.

Шаг 1: Настройте пассивный интерфейс.

а. Выполните команду **show ip ospf interface g0/0** на маршрутизаторе R1. Обратите внимание на таймер, указывающий время получения очередного пакета приветствия. Пакеты приветствия отправляются каждые 10 секунд и используются маршрутизаторами OSPF для проверки работоспособности соседних устройств.

R1# **show ip ospf interface g0/0**

GigabitEthernet0/0 is up, line protocol is up

Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement

Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1

Topology-MTID Cost Disabled Shutdown Topology Name

0 1 no no Base

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1

No backup designated router on this network Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 oob-resync timeout 40 Hello due in 00:00:02

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 0, maximum is 0

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

b. Выполните команду **passive-interface**, чтобы интерфейс G0/0 маршрутизатора R1 стал пассивным.

R1(config)# **router ospf 1**

R1(config-router)# **passive-interface g0/0**

c. Повторно выполните команду **show ip ospf interface g0/0**, чтобы убедиться, что интерфейс G0/0 стал пассивным.

R1# **show ip ospf interface g0/0**

GigabitEthernet0/0 is up, line protocol is up

Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement

Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1

Topology-MTID Cost Disabled Shutdown Topology Name

0 1 no no Base

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1

No backup designated router on this network Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 oob-resync timeout 40 No Hellos (Passive interface)

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 0, maximum is 0

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

d. Выполните команду **show ip route** на маршрутизаторах R2 и R3, чтобы убедиться, что маршрут к сети 192.168.1.0/24 по-прежнему доступен.

R2# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP + - replicated route, % - next hop override

Gateway of last resort is not set

2.0.0.0/32 is subnetted, 1 subnets

C 2.2.2.2 is directly connected, Loopback0

O 192.168.1.0/24 [110/65] via 192.168.12.1, 00:58:32, Serial0/0/0

192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.2.0/24 is directly connected, GigabitEthernet0/0

L 192.168.2.1/32 is directly connected, GigabitEthernet0/0

O 192.168.3.0/24 [110/65] via 192.168.23.2, 00:58:19, Serial0/0/1

192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.12.0/30 is directly connected, Serial0/0/0

L 192.168.12.2/32 is directly connected, Serial0/0/0

192.168.13.0/30 is subnetted, 1 subnets

O 192.168.13.0 [110/128] via 192.168.23.2, 00:58:19, Serial0/0/1

[110/128] via 192.168.12.1, 00:58:32, Serial0/0/0

192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.23.0/30 is directly connected, Serial0/0/1

L 192.168.23.1/32 is directly connected, Serial0/0/1

Шаг 2: Настройте маршрутизатор так, чтобы все его интерфейсы были пассивными по умолчанию.

a. Выполните команду **show ip ospf neighbor** на маршрутизаторе R1, чтобы убедиться, что R2 указан в качестве соседа OSPF.

R1# **show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:31	192.168.13.2	Serial0/0/1
22.22.22.22	0	FULL/ -	00:00:32	192.168.12.2	Serial0/0/0

b. Выполните команду **passive-interface default** на R2, чтобы по умолчанию настроить все интерфейсы OSPF в качестве пассивных.

R2(config)# **router ospf 1**

R2(config-router)# **passive-interface default**

R2(config-router)#

*Apr 3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from

FULL to DOWN, Neighbor Down: Interface down or detached

*Apr 3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from

FULL to DOWN, Neighbor Down: Interface down or detached

c. Повторно выполните команду **show ip ospf neighbor** на R1. После истечения таймера простоя маршрутизатор R2 больше не будет указан, как сосед OSPF.

R1# **show ip ospf neighbor**

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.33.33.33	0	FULL/ -	00:00:34	192.168.13.2	Serial0/0/1

d. Выполните команду **show ip ospf interface S0/0/0** на маршрутизаторе R2, чтобы просмотреть состояние OSPF интерфейса S0/0/0.

R2# **show ip ospf interface s0/0/0**

Serial0/0/0 is up, line protocol is up

Internet Address 192.168.12.2/30, Area 0, Attached via Network Statement

Process ID 1, Router ID 22.22.22.22, Network Type POINT_TO_POINT, Cost: 64

Topology-MTID	Cost	Disabled	Shutdown	Topology Name
0	64	no	no	Base

Transmit Delay is 1 sec, State POINT_TO_POINT Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 oob-resync timeout 40 No Hellos (Passive interface)

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 2/2, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 0, maximum is 0

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

e. В случае если все интерфейсы маршрутизатора R2 являются пассивными, маршрутизирующая информация объявляться не будет. В этом случае маршрутизаторы R1 и R3 больше не должны иметь маршрут к сети 192.168.2.0/24. Это можно проверить с помощью команды **show ip route**.

f. На маршрутизаторе R2 выполните команду **no passive-interface**, чтобы маршрутизатор отправлял и получал обновления маршрутизации OSPF. После ввода этой команды появится уведомление о том, что на маршрутизаторе R1 были установлены отношения смежности.

R2(config)# **router ospf 1**

R2(config-router)# **no passive-interface s0/0/0**

R2(config-router)#

*Apr 3 00:18:03.463: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from

LOADING to FULL, Loading Done

g. Повторно выполните команды **show ip route** и **show ipv6 ospf neighbor** на маршрутизаторах R1 и R3 и найдите маршрут к сети 192.168.2.0/24.

Какой интерфейс использует R3 для прокладки маршрута к сети 192.168.2.0/24? _____

Чему равна суммарная стоимость для сети 192.168.2.0/24 на R3? _____

Отображается ли маршрутизатор R2 как сосед OSPF на маршрутизаторе R1? _____ Отображается ли маршрутизатор R2 как сосед OSPF на маршрутизаторе R3? _____ Что даёт вам эта информация?

_____

_____

h. Настройте интерфейс S0/0/1 маршрутизатора R2 таким образом, чтобы он мог объявлять маршруты OSPF. Ниже запишите используемые команды.

_____

_____

i. Повторно выполните команду **show ip route** на маршрутизаторе R3.

Какой интерфейс использует R3 для прокладки маршрута к сети 192.168.2.0/24? _____ Чему равна суммарная стоимость для сети 192.168.2.0/24 на R3? Как она была рассчитана?

_____

_____

Отображается ли маршрутизатор R2 как сосед OSPF для маршрутизатора R3? _____

Часть 5: Изменение метрик OSPF

В части 3 необходимо изменить метрики OSPF с помощью команд **auto-cost reference-bandwidth**, **bandwidth** и **ip ospf cost**.

Примечание. В части 1 на всех интерфейсах DCE нужно было установить значение тактовой частоты 128000.

Шаг 1: Измените заданную пропускную способность на маршрутизаторах.

Заданная пропускная способность по умолчанию для OSPF равна 100 Мб/с (скорость Fast Ethernet).

Однако скорость каналов в большинстве современных устройств сетевой инфраструктуры превышает 100 Мб/с. Поскольку метрика стоимости OSPF должна быть целым числом, стоимость во всех каналах со скоростью передачи 100 Мб/с и выше равна 1. Вследствие этого интерфейсы Fast Ethernet, Gigabit Ethernet и 10G Ethernet имеют одинаковую стоимость. Поэтому, для правильного использования сетей со скоростью канала более 100 Мб/с, заданную пропускную способность необходимо установить на большее значение.

a. Выполните команду **show interface** на маршрутизаторе R1, чтобы просмотреть значение пропускной способности по умолчанию для интерфейса G0/0.

R1# **show interface g0/0**

GigabitEthernet0/0 is up, line protocol is up

Hardware is CN Gigabit Ethernet, address is c471.fe45.7520 (bia c471.fe45.7520) MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 100 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set

Keepalive set (10 sec)

Full Duplex, 100Mbps, media type is RJ45

output flow-control is unsupported, input flow-control is unsupported ARP type: ARPA, ARP Timeout 04:00:00

Last input never, output 00:17:31, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

0 packets input, 0 bytes, 0 no buffer

Received 0 broadcasts (0 IP multicasts)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

0 watchdog, 0 multicast, 0 pause input

279 packets output, 89865 bytes, 0 underruns

0 output errors, 0 collisions, 1 interface resets

0 unknown protocol drops

0 babbles, 0 late collision, 0 deferred

1 lost carrier, 0 no carrier, 0 pause output

0 output buffer failures, 0 output buffers swapped out

Примечание. Пропускная способность на интерфейсе G0/0 может отличаться от значения, приведённого выше, если интерфейс узла ПК может поддерживать только скорость Fast Ethernet. Если интерфейс узла ПК не поддерживают скорость передачи 1 Гб/с, то пропускная способность, скорее всего, будет отображена как 100000 Кб/с.

b. Выполните команду **show ip route ospf** на R1, чтобы определить маршрут к сети 192.168.3.0/24.

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP + - replicated route, % - next hop override

Gateway of last resort is not set

O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:57, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/128] via 192.168.13.2, 00:00:57, Serial0/0/1
[110/128] via 192.168.12.2, 00:01:08, Serial0/0/0

Примечание. Суммарная стоимость маршрута к сети 192.168.3.0/24 от маршрутизатора R1 должна быть равна 65.

c. Выполните команду **show ip ospf interface** на маршрутизаторе R3, чтобы определить стоимость маршрутизации для интерфейса G0/0.

R3# **show ip ospf interface g0/0**

GigabitEthernet0/0 is up, line protocol is up

Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement

Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1

Topology-MTID Cost Disabled Shutdown Topology Name

0 1 no no Base

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1

No backup designated router on this network Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 oob-resync timeout 40 Hello due in 00:00:05

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 0, maximum is 0

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

d. Выполните команду **show ip ospf interface s0/0/1** на маршрутизаторе R1, чтобы просмотреть стоимость маршрутизации для интерфейса S0/0/1.

R1# **show ip ospf interface s0/0/1**

Serial0/0/1 is up, line protocol is up

Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement

Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 64

Topology-MTID Cost Disabled Shutdown Topology Name

0 64 no no Base

Transmit Delay is 1 sec, State POINT_TO_POINT Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 oob-resync timeout 40 Hello due in 00:00:04

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 3/3, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 192.168.23.2

Suppress hello for 0 neighbor(s)

Как видно из выходных данных команды **show ip route**, сумма метрик стоимости этих двух интерфейсов и суммарная стоимость маршрута к сети 192.168.3.0/24 на маршрутизаторе R3 рассчитывается по формуле 1 + 64 = 65.

e. Выполните команду **auto-cost reference-bandwidth 10000** на маршрутизаторе R1, чтобы изменить параметр заданной пропускной способности по умолчанию. С подобной установкой стоимость интерфейсов 10 Гб/с будет равна 1, стоимость интерфейсов 1 Гбит/с будет равна 10, а стоимость интерфейсов 100 Мб/с будет равна 100.

R1(config)# **router ospf 1**

R1(config-router)# **auto-cost reference-bandwidth 10000**

% OSPF: Reference bandwidth is changed.

Please ensure reference bandwidth is consistent across all routers.

f. Выполните команду **auto-cost reference-bandwidth 10000** на маршрутизаторах R2 и R3.

g. Повторно выполните команду **show ip ospf interface**, чтобы просмотреть новую стоимость интерфейса G0/0 на R3 и интерфейса S0/0/1 на R1.

R3# **show ip ospf interface g0/0**

GigabitEthernet0/0 is up, line protocol is up

Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement

Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 10

Topology-MTID	Cost	Disabled	Shutdown	Topology Name
0	10	no	no	Base

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1

No backup designated router on this network Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 oob-resync timeout 40 Hello due in 00:00:02

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 0, maximum is 0

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

Примечание. Если устройство, подключённое к интерфейсу G0/0, не поддерживает скорость Gigabit Ethernet, то стоимость будет отличаться от отображаемых выходных данных. Например, для скорости Fast Ethernet (100 Мб/с) стоимость будет равна 100.

R1# **show ip ospf interface s0/0/1**

Serial0/0/1 is up, line protocol is up

Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement

Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 6476

Topology-MTID Cost Disabled Shutdown Topology Name

0 6476 no no Base

Transmit Delay is 1 sec, State POINT_TO_POINT Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 oob-resync timeout 40 Hello due in 00:00:05

Supports Link-local Signaling (LLS)

Cisco NSF helper support enabled

IETF NSF helper support enabled

Index 3/3, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 192.168.23.2

Suppress hello for 0 neighbor(s)

h. Повторно выполните команду **show ip route ospf**, чтобы просмотреть новую суммарную стоимость для маршрута 192.168.3.0/24 (10 + 6476 = 6486).

Примечание. Если устройство, подключённое к интерфейсу G0/0, не поддерживает скорость Gigabit Ethernet, то стоимость будет отличаться от того, что отображается в выходных данных. Например, если интерфейс G0/0 работает на скорости Fast Ethernet (100 Мб/с), то суммарная стоимость будет равна 6576.

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP + - replicated route, % - next hop override

Gateway of last resort is not set

O 192.168.2.0/24 [110/6486] via 192.168.12.2, 00:05:40, Serial0/0/0

O 192.168.3.0/24 [110/6486] via 192.168.13.2, 00:01:08, Serial0/0/1

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0 [110/12952] via 192.168.13.2, 00:05:17, Serial0/0/1

[110/12952] via 192.168.12.2, 00:05:17, Serial0/0/

Примечание. Изменение заданной пропускной способности по умолчанию на маршрутизаторах с 100 на 10 000 изменяет суммарные стоимости всех маршрутизаторов в 100 раз, но стоимость каждого канала и маршрута интерфейса рассчитывается точнее.

i. Для того чтобы восстановить заданную пропускную способность до значения по умолчанию, на всех трёх маршрутизаторах выполните команду **auto-cost reference-bandwidth 100**.

R1(config)# **router ospf 1**

R1(config-router)# **auto-cost reference-bandwidth 100**

% OSPF: Reference bandwidth is changed.

Please ensure reference bandwidth is consistent across all routers.

Для чего имеет смысл изменять заданную пропускную способность OSPF?

_____

_____

Шаг 2: Измените пропускную способность для интерфейса.

На большинстве последовательных каналов метрика пропускной способности имеет значение по умолчанию, равное 1544 Кбит (T1). В случае если реальная скорость последовательного канала другая, то для правильного расчёта стоимости маршрута в OSPF параметр пропускной способности нужно будет изменить, чтобы она была равна фактической скорости. Используйте команду **bandwidth**, чтобы откорректировать значение пропускной способности на интерфейсе.

Примечание. Согласно распространённому заблуждению, команда **bandwidth** может изменить физическую пропускную способность (или скорость) канала. Команда изменяет метрику пропускной способности, используемой алгоритмом OSPF для расчёта стоимости маршрутизации, но **не** изменяет фактическую пропускную способность (скорость) канала.

a. Выполните команду **show interface s0/0/0** на маршрутизаторе R1, чтобы просмотреть установленное значение пропускной способности на интерфейсе S0/0/0. Реальная скорость передачи данных на этом интерфейсе, установленная командой clock rate, составляет 128 Кб/с, при этом установленное значение пропускной способности по-прежнему равно 1544 Кб/с.

R1# **show interface s0/0/0**

Serial0/0/0 is up, line protocol is up

Hardware is WIC MBRD Serial

Internet address is 192.168.12.1/30 MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation HDLC, loopback not set

Keepalive set (10 sec)

<Output omitted>

b. Выполните команду **show ip route ospf** на маршрутизаторе R1, чтобы просмотреть суммарную стоимость для маршрута к сети 192.168.23.0/24 через интерфейс S0/0/0. Обратите внимание, что к сети 192.168.23.0/24 есть два маршрута с равной стоимостью (128): один через интерфейс S0/0/0, другой через интерфейс S0/0/1.

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP + - replicated route, % - next hop override

Gateway of last resort is not set

O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:26, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/128] via 192.168.13.2, 00:00:26, Serial0/0/1
[110/128] via 192.168.12.2, 00:00:42, Serial0/0/0

c. Выполните команду **bandwidth 128**, чтобы установить на интерфейсе S0/0/0 пропускную способность равную 128 Кб/с.

R1(config)# **interface s0/0/0**
R1(config-if)# bandwidth 128

d. Повторно выполните команду **show ip route ospf**. В таблице маршрутизации больше не отображается маршрут к сети 192.168.23.0/24 через интерфейс S0/0/0. Это связано с тем, что оптимальный маршрут с наименьшей стоимостью проложен через S0/0/1.

R1# **show ip route ospf**
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic

downloaded static route, H - NHRP, l - LISP + - replicated route, % - next hop override

Gateway of last resort is not set

O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:04:51, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/128] via 192.168.13.2, 00:04:51, Serial0/0/1

e. Выполните **show ip ospf interface brief**. Стоимость для интерфейса S0/0/0 изменилась с 64 на 781, что является более точным представлением стоимости скорости канала.

R1# **show ip ospf interface brief**

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs F/C
Se0/0/1	1	0	192.168.13.1/30	64	P2P	1/1
Se0/0/0	1	0	192.168.12.1/30	781	P2P	1/1
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0

f. Измените пропускную способность для интерфейса S0/0/1 на значение, установленное для интерфейса S0/0/0 маршрутизатора R1.

g. Повторно выполните команду **show ip route ospf**, чтобы просмотреть суммарную стоимость обоих маршрутов к сети 192.168.23.0/24. Обратите внимание, что к сети 192.168.23.0/24 есть два маршрута с одинаковой стоимостью (845): один через интерфейс S0/0/0, другой через интерфейс S0/0/1.

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-

IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP + - replicated route, % - next hop override

Gateway of last resort is not set

O 192.168.3.0/24 [110/782] via 192.168.13.2, 00:00:09, Serial0/0/1
192.168.23.0/30 is subnetted, 1 subnets
O 192.168.23.0 [110/845] via 192.168.13.2, 00:00:09, Serial0/0/1
[110/845] via 192.168.12.2, 00:00:09, Serial0/0/0

Объясните, как были рассчитаны стоимости для сетей 192.168.3.0/24 и 192.168.23.0/30 от маршрутизатора R1.

_____

_____Стоимость маршрута к сети 192.168.3.0/24: R1 S0/0/1 + R3 G0/0 (781+1=782). Стоимость маршрута к сети 192.168.23.0/30: R1 S0/0/1 + R3 S0/0/1 (781+64=845).

h. Выполните команду **show ip route ospf** на R3. Суммарная стоимость сети 192.168.1.0/24 попрежнему равна 65. В отличие от команды **clock rate**, команду **bandwidth** следует выполнить на каждом конце последовательного канала.

R3# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP + - replicated route, % - next hop override

Gateway of last resort is not set

O 192.168.1.0/24 [110/65] via 192.168.13.1, 00:30:58, Serial0/0/0
192.168.12.0/30 is subnetted, 1 subnets
O 192.168.12.0 [110/128] via 192.168.23.1, 00:30:58, Serial0/0/1
[110/128] via 192.168.13.1, 00:30:58, Serial0/0/0

i. Выполните команду **bandwidth 128** на всех остальных последовательных интерфейсах в топологии.

Чем равна новая суммарная стоимость для сети 192.168.23.0/24 на R1? Почему?

_____

_____

Шаг 3: Измените стоимость маршрута.

Для расчёта стоимости канала OSPF использует значение, установленное командой bandwidth. Рассчитанную стоимость можно изменить, настроив вручную стоимость канала с помощью команды **ip ospf cost**. Как и команда **bandwidth**, команда **ip ospf cost** действует только на той стороне канала, на которой она была применена.

a. Введите команду **show ip route ospf** на маршрутизаторе R1.

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP + - replicated route, % - next hop override

Gateway of last resort is not set

O 192.168.2.0/24 [110/782] via 192.168.12.2, 00:00:26, Serial0/0/0

O 192.168.3.0/24 [110/782] via 192.168.13.2, 00:02:50, Serial0/0/1

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0 [110/1562] via 192.168.13.2, 00:02:40, Serial0/0/1

[110/1562] via 192.168.12.2, 00:02:40, Serial0/0/0

b. Выполните команду **ip ospf cost 1565** на интерфейсе S0/0/1 маршрутизатора R1. Стоимость 1565 является выше суммарной стоимости маршрута, проходящего через R2 (1562).

R1(config)# int s0/0/1

R1(config-if)# **ip ospf cost 1565**

c. Повторно выполните команду **show ip route ospf** на R1, чтобы отобразить изменения в таблице маршрутизации. Теперь все маршруты OSPF для маршрутизатора R1 направляются через маршрутизатор R2.

R1# **show ip route ospf**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP + - replicated route, % - next hop override

Gateway of last resort is not set

O 192.168.2.0/24 [110/782] via 192.168.12.2, 00:02:06, Serial0/0/0

O 192.168.3.0/24 [110/1563] via 192.168.12.2, 00:05:31, Serial0/0/0

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0 [110/1562] via 192.168.12.2, 01:14:02, Serial0/0/0

Примечание. Изменение метрик стоимости канала с помощью команды **ip ospf cost** — это наиболее простой и предпочтительный способ изменения стоимости маршрутов OSPF. Помимо изменения стоимости в связи с реальным значением пропускной способности, у сетевого администратора могут быть другие причины для изменения стоимости маршрута, например, известная пропускная способность, предоставляемой оператором связи или фактическая стоимость канала или маршрута.

Почему маршрут к сети 192.168.3.0/24 маршрутизатора R1 теперь проходит через R2?

_____

_____

Вопросы на закрепление

1. Почему так важно контролировать значение ID маршрутизатора при использовании протокола OSPF?

_____

_____

2. Почему процесс выбора DR/BDR не рассматривается в этой лабораторной работе?

_____

_____

3. Почему имеет смысл устанавливать интерфейс OSPF в качестве пассивного?

_____

_____

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов

Модель маршрутизатора	**Интерфейс Ethernet №1**	**Интерфейс Ethernet №2**	**Последовательный интерфейс №1**	**Последовательный интерфейс №2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Практическая работа9

Тема: Настройка OSPFv2 в сети множественного доступа

Цели: Произвести настройку OSPFv2 в сети множественного доступа

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задачи

Часть 1. Создание сети и настройка базовых параметров устройств

Часть 2. Настройка и проверка OSPFv2 на DR, BDR и DROther

Часть 3. Настройка приоритета интерфейса OSPFv2 для определения DR и BDR

Исходные данные/сценарий

Сеть с множественным доступом — это сеть, содержащая более двух устройств в общей среде передачи данных. К таким сетям относятся Ethernet и Frame Relay. В сетях с множественным доступом протокол OSPFv2 назначает выделенный маршрутизатор (DR) в качестве точки сбора и распределения отправленных и принятых объявлений о состоянии канала (LSA). На случай отказа выделенного маршрутизатора (DR) также выбирается резервный назначенный маршрутизатор (BDR). Все остальные маршрутизаторы станут маршрутизаторами DROther. Это состояние показывает, что маршрутизатор не является ни DR, ни BDR.

Поскольку DR играет роль центральной точки для сообщений протокола маршрутизации OSPF, выбранный маршрутизатор должен поддерживать больший трафик, чем другие маршрутизаторы сети. На роль DR, как правило, подходит маршрутизатор с мощным ЦП и достаточным объёмом динамической памяти.

В этой лабораторной работе вам предстоит настроить OSPFv2 на маршрутизаторах DR, BDR и DROther. Затем вам необходимо изменить приоритет маршрутизаторов, чтобы повлиять на результаты выбора DR/BDR и обеспечить назначение роли DR нужному маршрутизатору.

Примечание. В лабораторной работе используются маршрутизаторы с интеграцией сервисов серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3

(образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и их результаты могут отличаться от приведённых в описании лабораторных работ. Точные идентификаторы интерфейсов приведены в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что информация из маршрутизаторов и коммутаторов удалена и в них нет начальной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.

Топология

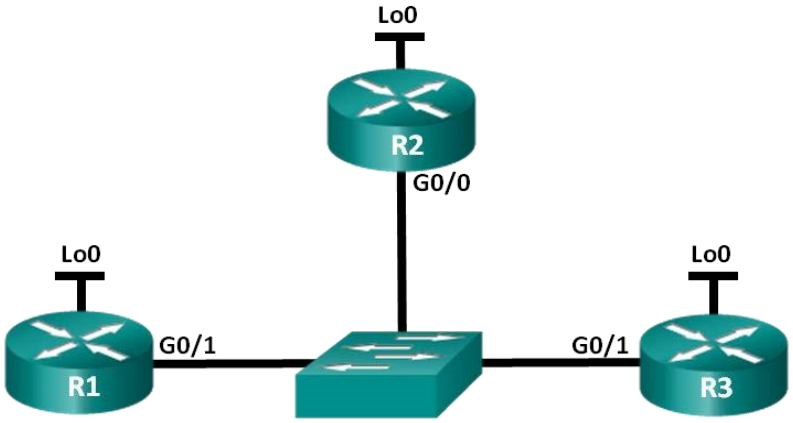


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
R1	G0/1	192.168.1.1	255.255.255.0
	Lo0	192.168.31.11	255.255.255.255
R2	G0/0	192.168.1.2	255.255.255.0
	Lo0	192.168.31.22	255.255.255.255
R3	G0/1	192.168.1.3	255.255.255.0
	Lo0	192.168.31.33	255.255.255.255

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 1 коммутатор (серия Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный)
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Создание сети и настройка базовых параметров устройств

В части 1 необходимо настроить топологию сети и выполнить базовые настройки маршрутизаторов.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Подключите устройства в соответствии с диаграммой топологии и выполните разводку кабелей по необходимости.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов.

Шаг 3: Настройте базовые параметры каждого маршрутизатора.

a. Отключите поиск DNS.
b. Настройте имена устройств в соответствии с топологией.
c. Назначьте **class** в качестве пароля привилегированного режима.
d. Назначьте **cisco** в качестве паролей консоли и VTY.
e. Зашифруйте пароли.
f. Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.
g. Настройте **logging synchronous** для консольного канала.
h. Назначьте IP-адреса всем интерфейсам в соответствии с таблицей адресации.
i. Выполните команду **show ip interface brief**, чтобы убедиться в правильности IP-адресации и активности интерфейсов.
j. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Часть 2: Настройка и проверка OSPFv2 на DR, BDR и DROther

В части 2 вам предстоит настроить OSPFv2 на маршрутизаторах DR, BDR и DROther. Процедура выбора DR и BDR начинается сразу после появления в сети с множественным доступом первого маршрутизатора с работающим интерфейсом. Это может случиться после включения питания маршрутизаторов или выполнения команды OSPF **network** на интерфейсе. Если новый маршрутизатор входит в сеть после выбора маршрутизаторов DR и BDR, он не становится маршрутизатором DR или BDR, даже если приоритет его OSPF-интерфейса или идентификатор маршрутизатора выше, чем у действующих маршрутизаторов DR и BDR. Настройте OSPF-процесс сначала на маршрутизаторе с наивысшим идентификатором, чтобы именно он стал маршрутизатором DR.

Шаг 1: Настройте протокол OSPF на маршрутизаторе R3.

Настройте OSPF-процесс сначала на маршрутизаторе R3 (с наивысшим идентификатором), чтобы именно он стал маршрутизатором DR.

a. Назначьте 1 в качестве идентификатора процесса OSPF. Настройте для маршрутизатора объявление сети 192.168.1.0/24. Для параметра OSPF *area-id* выражения **network** введите идентификатор области 0.

По какой причине идентификатор маршрутизатора R3 является наивысшим?

_____

_____

b. Убедитесь, что OSPF настроен, а маршрутизатор R3 исполняет роль DR.

Какую команду необходимо выполнить, чтобы убедиться в правильности настройки OSPF и в том, что R3 исполняет роль DR?

_____

_____

Шаг 2: Настройте протокол OSPF на маршрутизаторе R2.

Настройте OSPF-процесс сначала на маршрутизаторе R2 (со вторым по величине значением идентификатора), чтобы именно он стал маршрутизатором BDR.

a. Назначьте 1 в качестве идентификатора процесса OSPF. Настройте для маршрутизатора объявление сети 192.168.1.0/24. Для параметра OSPF *area-id* выражения **network** введите идентификатор области 0.

b. Убедитесь, что OSPF настроен, а маршрутизатор R2 исполняет роль BDR. Запишите команду, используемую для проверки.

_____

_____

c. Выполните команду **show ip ospf neighbor** для просмотра сведений о других маршрутизаторах в области OSPF.

R2# **show ip ospf neighbor**

Neighbor ID Pri State Dead Time Address Interface

192.168.31.33 1 FULL/DR 00:00:33 192.168.1.3 GigabitEthernet0/0

Обратите внимание, что R3 является маршрутизатором DR.

Шаг 3: Настройте протокол OSPF на маршрутизаторе R1.

Настройте OSPF-процесс на маршрутизаторе R1 (с самым низким идентификатором). Этот маршрутизатор станет маршрутизатором DROther, а не DR или BDR.

a. Назначьте 1 в качестве идентификатора процесса OSPF. Настройте для маршрутизатора объявление сети 192.168.1.0/24. Для параметра OSPF *area-id* выражения **network** введите идентификатор области 0.

b. Выполните команду **show ip ospf interface brief**, чтобы убедиться, что OSPF настроен, а маршрутизатору R1 назначена роль DROther.

R1# **show ip ospf interface brief**

Interface PID Area IP Address/Mask Cost State Nbrs F/C

Gi0/1 1 0 192.168.1.1/24 1 DROTH 2/2

c. Выполните команду **show ip ospf neighbor** для просмотра сведений о других маршрутизаторах в области OSPF.

R1# **show ip ospf neighbor**

Neighbor ID Pri State Dead Time Address Interface

192.168.31.22 1 FULL/BDR 00:00:35 192.168.1.2 GigabitEthernet0/1

192.168.31.33 1 FULL/DR 00:00:30 192.168.1.3 GigabitEthernet0/1

Каким приоритетом обладают оба маршрутизатора, DR и BDR? _____

Часть 3: Настройка приоритета интерфейса OSPFv2 для определения DR и BDR

В части 3 вам предстоит настроить приоритет интерфейса маршрутизатора для того, чтобы предопределить выбор DR/BDR, перезапустить процесс OSPFv2, а также убедиться в изменении маршрутизаторов DR и BDR. Приоритет интерфейса OSPF является основным параметром при определении ролей маршрутизаторов DR и BDR.

Шаг 1: Для интерфейса G0/1 маршрутизатора R1 настройте приоритет OSPF 255.

Значение 255 — это максимально возможный приоритет интерфейса.

R1(config)# **interface g0/1**

R1(config-if)# **ip ospf priority 255** R1(config-if)# **end**

Шаг 2: Для интерфейса G0/1 маршрутизатора R3 настройте приоритет OSPF 100.

R3(config)# **interface g0/1**

R3(config-if)# **ip ospf priority 100** R3(config-if)# **end**

Шаг 3: Для интерфейса G0/0 маршрутизатора R2 настройте приоритет OSPF 0.

Маршрутизатор с приоритетом 0 не может участвовать в процессе выбора OSPF, поэтому он не станет ни DR, ни BDR.

R2(config)# **interface g0/0**

R2(config-if)# **ip ospf priority 0**

R2(config-if)# **end**

Шаг 4: Перезапустите процесс OSPF

a. Используйте команду **show ip ospf neighbor** для определения DR и BDR.
b. Изменилось ли назначение DR? _____
c. Какой маршрутизатор исполняет роль DR? _____

Изменилось ли назначение BDR? _____

Какой маршрутизатор выполняет роль BDR? _____

Какую роль выполняет маршрутизатор R2? _____

Объясните немедленные изменения, вызванные командой **ip ospf priority**.

_____

_____

Примечание. Если назначения DR и BDR не изменились, выполните команду **clear ip ospf 1 process** на всех маршрутизаторах, чтобы сбросить процессы OSPF и инициировать новый выбор.

Если команда **clear ip ospf process** не привела к сбросу DR и BDR, то, сохранив текущую конфигурацию как загрузочную, выполните команду **reload** на всех маршрутизаторах.

d. Выполните команду **show ip ospf interface** на маршрутизаторах R1 и R3 для проверки заданных приоритетов и статуса DR/BDR маршрутизаторов.

```
R1# show ip ospf interface
GigabitEthernet0/1 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.31.11, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 255
  Designated Router (ID) 192.168.31.11, Interface address 192.168.1.1
  Backup Designated router (ID) 192.168.31.33, Interface address 192.168.1.3
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40      Hello due in 00:00:00
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 192.168.31.22
    Adjacent with neighbor 192.168.31.33  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)

R3# show ip ospf interface
GigabitEthernet0/1 is up, line protocol is up
  Internet Address 192.168.1.3/24, Area 0
```

Process ID 1, Router ID 192.168.31.33, Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State BDR, Priority 100

Designated Router (ID) 192.168.31.11, Interface address 192.168.1.1

Backup Designated router (ID) 192.168.31.33, Interface address 192.168.1.3

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

oob-resync timeout 40 Hello due in 00:00:00

Supports Link-local Signaling (LLS)

Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 0, maximum is 2

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 2, Adjacent neighbor count is 2

Adjacent with neighbor 192.168.31.22

Adjacent with neighbor 192.168.31.11 (Designated Router)

Suppress hello for 0 neighbor(s)

Какой из маршрутизаторов теперь является DR? _____

Какой из маршрутизаторов теперь является BDR? _____

Важнее ли приоритет интерфейса, чем идентификатор маршрутизатора при определении DR/BDR? _____

Вопросы на закрепление

1. Перечислите критерии, используемые для определения DR в сети OSPF, в порядке убывания их важности.

_____

_____2. Что означает приоритет интерфейса 255?

_____

_____

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов

Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества его интерфейсов. Не существует эффективного способа перечислить все комбинации настроек для каждого класса маршрутизаторов. В этой таблице содержатся идентификаторы для возможных сочетаний интерфейсов Ethernet и последовательных интерфейсов в устройстве. В таблицу не включены никакие иные типы интерфейсов, даже если они присутствуют на конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Практическая работа 10

Настройка базового PPP с аутентификацией

Цели: Произвести настройку базового PPP с аутентификацией

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задачи

Часть 1. Базовая настройка устройств

Часть 2. Настройка инкапсуляции PPP

Часть 3. Настройка аутентификации CHAP PPP

Исходные данные/сценарий

PPP — очень распространенный протокол WAN уровня 2. PPP можно использовать для подключения из локальной сети к WAN-провайдеру и для подключения сегментов LAN в рамках корпоративной сети.

В этой лабораторной работе требуется настроить инкапсуляцию PPP на выделенных последовательных каналах между маршрутизаторами филиалов и центральным маршрутизатором. Требуется настроить протокол аутентификации по квитированию вызова (CHAP) PPP на последовательных каналах PPP. Вы также изучите влияние, оказываемое изменениями инкапсуляции и аутентификации на состояние последовательного канала.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы Cisco Catalyst серии 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены и они не имеют загрузочных настроек. Если вы не уверены в этом, обратитесь к инструктору.

Топология

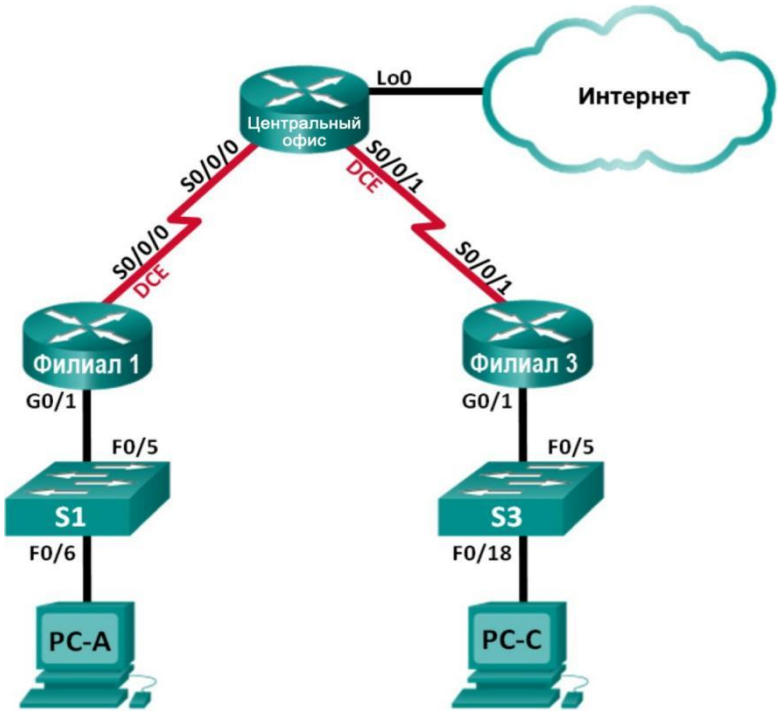


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Филиал 1	G0/1	192.168.1.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Недоступно
Central	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Недоступно
	Lo0	209.165.200.225	255.255.255.224	Недоступно
Филиал 3	G0/1	192.168.3.1	255.255.255.0	Недоступно
	S0/0/1	10.2.2.1	255.255.255.252	Недоступно
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Базовая настройка устройств

В части 1 вам предстоит настроить топологию сети и базовые параметры маршрутизатора, например, IP-адреса интерфейсов, маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

a. Отключите поиск DNS.
b. Настройте имя устройства.
c. Зашифруйте незашифрованные пароли.
d. Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.
e. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.
f. Назначьте **cisco** в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.
g. Настройте ведение журнала состояния консоли на синхронный режим.

h. Примените IP-адреса к интерфейсам Serial и Gigabit Ethernet в соответствии с таблицей адресации и включите физические интерфейсы.

i. Настройте тактовую частоту на **128000** для всех последовательных интерфейсов DCE.

j. На маршрутизаторе «Главный» создайте **Loopback 0** для имитации доступа в Интернет и назначьте IP-адрес согласно таблице адресации.

Шаг 4: Настройте маршрутизацию.

a. Включите на маршрутизаторах использование протокола OSPF для одной области и используйте в качестве идентификатора процесса значение 1. Добавьте в процесс OSPF все сети, за исключением 209.165.200.224/27.

b. На маршрутизаторе «Главный» настройте маршрут по умолчанию к симулируемому Интернету, используя Lo0 в качестве выходного интерфейса, и перераспределите маршрут в процесс OSPF.

c. На всех маршрутизаторах выполните команды **show ip route ospf**, **show ip ospf interface brief** и **show ip ospf neighbor**, чтобы проверить правильность настройки OSPF. Обратите внимание на идентификатор каждого маршрутизатора.

Шаг 5: Настройте компьютеры.

Настройте IP-адреса и шлюзы по умолчанию на всех ПК в соответствии с таблицей адресации.

Шаг 6: Проверьте связь между конечными устройствами.

Все устройства должны успешно выполнять эхо-запросы ко всем остальным устройствам, указанным в топологии. Если это не так, выполняйте поиск и устранение неполадок то до тех пор, пока не удастся установить сквозное соединение.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение межсетевого экрана.

Шаг 7: Сохраните настройки.

Часть 2: Настройка инкапсуляции PPP

Шаг 1: Отобразите инкапсуляцию, используемую в последовательном интерфейсе по умолчанию.

На маршрутизаторах выполните команду **show interfaces serial** *идентификатор_интерфейса* для отображения текущей инкапсуляции, используемой в последовательном интерфейсе.

Branch1# **show interfaces s0/0/0**

Serial0/0/0 is up, line protocol is up

Hardware is WIC MBRD Serial

Internet address is 10.1.1.1/30 MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation HDLC, loopback not set

Keepalive set (10 sec)

Last input 00:00:02, output 00:00:05, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

1003 packets input, 78348 bytes, 0 no buffer

Received 527 broadcasts (0 IP multicasts)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

1090 packets output, 80262 bytes, 0 underruns

0 output errors, 0 collisions, 3 interface resets

0 unknown protocol drops

0 output buffer failures, 0 output buffers swapped out

2 carrier transitions

DCD=up DSR=up DTR=up RTS=up CTS=up

Укажите тип инкапсуляции, используемой в последовательном интерфейсе по умолчанию, для маршрутизатора Cisco. _____

Шаг 2: Измените инкапсуляцию на PPP.

a. Для изменения инкапсуляции HDLC на PPP введите команду **encapsulation ppp** на интерфейсе S0/0/0 маршрутизатора «Филиал 1».

Branch1(config)# **interface s0/0/0**

Branch1(config-if)# **encapsulation ppp**

Branch1(config-if)#

Jun 19 06:02:33.687: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

Branch1(config-if)#

Jun 19 06:02:35.687: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

b. Введите команду для отображения состояния канала и протокола канала для интерфейса S0/0/0 маршрутизатора «Филиал 1». Задокументируйте выполненную команду. Укажите текущее состояние интерфейса S0/0/0.

_____

_____

c. Для исправления разночтений в настройках инкапсуляции для последовательного интерфейса ведите команду **encapsulation ppp** на интерфейсе S0/0/0 для маршрутизатора Central.

Central(config)# **interface s0/0/0**

Central(config-if)# **encapsulation ppp**

Central(config-if)#

.Jun 19 06:03:41.186: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,

changed state to up

.Jun 19 06:03:41.274: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done

d. Убедитесь, что интерфейс S0/0/0 как на маршрутизаторе «Филиал 1», так и на маршрутизаторе «Главный» находится в активном состоянии и настроен с инкапсуляцией PPP.

Укажите состояние протокола PPP (LCP). _____

Укажите, согласование каких протоколов NCP было выполнено.

_____

_____

Branch1# **show interfaces s0/0/0**

Serial0/0/0 is up, line protocol is up

Hardware is WIC MBRD Serial

Internet address is 10.1.1.1/30 MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation PPP, LCP Open

Open: IPCP, CDPCP, loopback not set

Keepalive set (10 sec)

Last input 00:00:00, output 00:00:00, output hang never

Last clearing of "show interface" counters 00:03:58

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

77 packets input, 4636 bytes, 0 no buffer

Received 0 broadcasts (0 IP multicasts)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

117 packets output, 5800 bytes, 0 underruns

0 output errors, 0 collisions, 8 interface resets

22 unknown protocol drops

0 output buffer failures, 0 output buffers swapped out

18 carrier transitions

DCD=up DSR=up DTR=up RTS=up CTS=up

Central# **show interfaces s0/0/0**

Serial0/0/0 is up, line protocol is up

Hardware is WIC MBRD Serial

Internet address is 10.1.1.2/30 MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation PPP, LCP Open

Open: IPCP, CDPCP, loopback not set

Keepalive set (10 sec)

Last input 00:00:02, output 00:00:03, output hang never

Last clearing of "show interface" counters 00:01:20

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

41 packets input, 2811 bytes, 0 no buffer

Received 0 broadcasts (0 IP multicasts)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

40 packets output, 2739 bytes, 0 underruns

0 output errors, 0 collisions, 0 interface resets

0 unknown protocol drops

0 output buffer failures, 0 output buffers swapped out

0 carrier transitions

DCD=up DSR=up DTR=up RTS=up CTS=up

Шаг 3: Намеренно разорвите последовательное подключение.

a. Выполните команды **debug ppp**, чтобы понаблюдать за влиянием изменения настройки PPP на маршрутизаторы «Филиал 1» и «Главный».

Branch1# **debug ppp negotiation**

PPP protocol negotiation debugging is on

Branch1# **debug ppp packet** PPP packet display debugging is on

Central# **debug ppp negotiation**

PPP protocol negotiation debugging is on

Central# **debug ppp packet**

PPP packet display debugging is on

b. Наблюдайте за сообщениями команды debug PPP при проходе трафика по последовательному каналу между маршрутизаторами «Филиал 1» и «Главный».

Branch1#

Jun 20 02:20:45.795: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84

Jun 20 02:20:49.639: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]

Jun 20 02:20:50.147: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 45 len 12 magic 0x73885AF2

Jun 20 02:20:50.147: Se0/0/0 LCP-FS: O ECHOREP [Open] id 45 len 12 magic 0x8CE1F65F

Jun 20 02:20:50.159: Se0/0/0 LCP: O ECHOREQ [Open] id 45 len 12 magic 0x8CE1F65F

Jun 20 02:20:50.159: Se0/0/0 LCP-FS: I ECHOREP [Open] id 45 len 12 magic 0x73885AF2

Jun 20 02:20:50.159: Se0/0/0 LCP-FS: Received id 45, sent id 45, line up

Central#

Jun 20 02:20:49.636: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84

Jun 20 02:20:50.148: Se0/0/0 LCP: O ECHOREQ [Open] id 45 len 12 magic 0x73885AF2

Jun 20 02:20:50.148: Se0/0/0 LCP-FS: I ECHOREP [Open] id 45 len 12 magic 0x8CE1F65F

Jun 20 02:20:50.148: Se0/0/0 LCP-FS: Received id 45, sent id 45, line up

Jun 20 02:20:50.160: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 45 len 12 magic 0x8CE1F65F

Jun 20 02:20:50.160: Se0/0/0 LCP-FS: O ECHOREP [Open] id 45 len 12 magic 0x73885AF2

Jun 20 02:20:55.552: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]

c. Разорвите последовательное подключение путем возвращения HDLC в качестве инкапсуляции для последовательного интерфейса S0/0/0 маршрутизатора «Филиал 1». Запишите команду, использованную для изменения инкапсуляции на HDLC.

_____

_____

d. Наблюдайте за сообщениями команды debug PPP на маршрутизаторе «Филиал 1».

Последовательное подключение завершено, и протокол линии связи не функционирует. Маршрут к 10.1.1.2 («Главный») удалён из таблицы маршрутизации.

Jun 20 02:29:50.295: Se0/0/0 PPP DISC: Lower Layer disconnected Jun 20 02:29:50.295: PPP: NET STOP send to AAA.

Jun 20 02:29:50.299: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]

Jun 20 02:29:50.299: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 02:29:50.299: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]

Jun 20 02:29:50.299: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 02:29:50.29

Branch1(config-if)#9: Se0/0/0 LCP: O TERMREQ [Open] id 7 len 4

Jun 20 02:29:50.299: Se0/0/0 LCP: Event[CLOSE] State[Open to Closing]

Jun 20 02:29:50.299: Se0/0/0 PPP: Phase is TERMINATING

Jun 20 02:29:50.299: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address 10.1.1.2

Jun 20 02:29:50.299: Se0/0/0 IPCP: Remove route to 10.1.1.2

Jun 20 02:29:50.299: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]

Jun 20 02:29:50.299: Se0/0/0 PPP: Phase is DOWN

Branch1(config-if)#

Jun 20 02:30:17.083: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Jun 20 02:30:17.083: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

e. Наблюдайте за сообщениями команды debug PPP на маршрутизаторе «Главный». Маршрутизатор «Главный» продолжает попытки установить подключение к маршрутизатору «Филиал 1», как видно из сообщений команды debug. Если интерфейсы не могут установить подключение, интерфейсы снова прекращают работу. Кроме того, OSPF не может сформировать отношения смежности с соседним с ним устройством вследствие несоответствия инкапсуляции для последовательного канала.

Jun 20 02:29:50.296: Se0/0/0 PPP: Sending cstate DOWN notification

Jun 20 02:29:50.296: Se0/0/0 PPP: Processing CstateDown message

Jun 20 02:29:50.296: Se0/0/0 PPP DISC: Lower Layer disconnected Jun 20 02:29:50.296: PPP: NET STOP send to AAA.

Jun 20 02:29:50.296: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]

Jun 20 02:29:50.296: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 02:29:50.296: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]

Jun 20 02:29:50.296: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 02:29:50.296: Se0/0/0 LCP: O TERMREQ [Open] id 2 len 4

Jun 20 02:29:50.296: Se0/0/0 LCP: Event[CLOSE] State[Open to Closing]

Jun 20 02:29:50.296: Se0/0/0 PPP: Phase is TERMINATING

Jun 20 02:29:50.296: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address 10.1.1.1

Jun 20 02:29:50.296: Se0/0/0 IPCP: Remove route to 10.1.1.1

Jun 20 02:29:50.296: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

Jun 20 02:29:50.296: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]

Jun 20 02:29:50.296: Se0/0/0 PPP: Phase is DOWN

Jun 20 02:29:52.296: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

.Jun 20 02:29:52.296: Se0/0/0 PPP: Sending cstate UP notification

.Jun 20 02:29:52.296: Se0/0/0 PPP: Processing CstateUp message

.Jun 20 02:29:52.296: PPP: Alloc Context [29F9F32C]

.Jun 20 02:29:52.296: ppp3 PPP: Phase is ESTABLISHING

.Jun 20 02:29:52.296: Se0/0/0 PPP: Using default call direction

.Jun 20 02:29:52.296: Se0/0/0 PPP: Treating connection as a dedicated line

.Jun 20 02:29:52.296: Se0/0/0 PPP: Session handle[60000003] Session id[3]

.Jun 20 02:29:52.296: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]

.Jun 20 02:29:52.296: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10

.Jun 20 02:29:52.296: Se0/0/0 LCP: MagicNumber 0x7397843B (0x05067397843B)

.Jun 20 02:29:52.296: Se0/0/0 LCP:Event[UP] State[Starting to REQsent]

.Jun 20 02:29:54.308: Se0/0/0 LCP: O CONFREQ [REQsent] id 2 len 10

.Jun 20 02:29:54.308: Se0/0/0 LCP: MagicNumber 0x7397843B (0x05067397843B)

.Jun 20 02:29:54.308: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]

.Jun 20 02:29:56.080: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24 link[illegal]

.Jun 20 02:29:56.080: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet, discarding

<Данные опущены>

.Jun 20 02:30:10.436: Se0/0/0 LCP: O CONFREQ [REQsent] id 10 len 10

.Jun 20 02:30:10.436: Se0/0/0 LCP: MagicNumber 0x7397843B (0x05067397843B)

.Jun 20 02:30:10.436: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]

.Jun 20 02:30:12.452: Se0/0/0 PPP DISC: LCP failed to negotiate .Jun 20 02:30:12.452: PPP: NET STOP send to AAA.

.Jun 20 02:30:12.452: Se0/0/0 LCP: Event[Timeout-] State[REQsent to Stopped]

.Jun 20 02:30:12.452: Se0/0/0 LCP: Event[DOWN] State[Stopped to Starting]

.Jun 20 02:30:12.452: Se0/0/0 PPP: Phase is DOWN

.Jun 20 02:30:14.452: PPP: Alloc Context [29F9F32C]

.Jun 20 02:30:14.452: ppp4 PPP: Phase is ESTABLISHING

.Jun 20 02:30:14.452: Se0/0/0 PPP: Using default call direction

.Jun 20 02:30:14.452: Se0/0/0 PPP: Treating connection as a dedicated line

.Jun 20 02:30:14.452: Se0/0/0 PPP: Session handle[6E000004] Session id[4]

.Jun 20 02:30:14.452: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]

.Jun 20 02:30:14.452: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10

.Jun 20 02:30:14.452: Se0/0/0 LCP: MagicNumber 0x7397DADA (0x05067397DADA)

.Jun 20 02:30:14.452: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]

.Jun 20 02:30:16.080: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24 link[illegal]

.Jun 20 02:30:16.080: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet, discarding

<Данные опущены>

.Jun 20 02:30:32.580: Se0/0/0 LCP: O CONFREQ [REQsent] id 10 len 10

.Jun 20 02:30:32.580: Se0/0/0 LCP: MagicNumber 0x7397DADA (0x05067397DADA)

.Jun 20 02:30:32.580: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]

.Jun 20 02:30:34.596: Se0/0/0 PPP DISC: LCP failed to negotiate .Jun 20 02:30:34.596: PPP: NET STOP send to AAA.

.Jun 20 02:30:34.596: Se0/0/0 LCP: Event[Timeout-] State[REQsent to Stopped]

.Jun 20 02:30:34.596: Se0/0/0 LCP: Event[DOWN] State[Stopped to Starting]

.Jun 20 02:30:34.596: Se0/0/0 PPP: Phase is DOWN

.Jun 20 02:30:36.080: Se0/0/0 PPP: I pkt type 0x008F, discarded, PPP not running

.Jun 20 02:30:36.596: PPP: Alloc Context [29F9F32C]

.Jun 20 02:30:36.596: ppp5 PPP: Phase is ESTABLISHING

.Jun 20 02:30:36.596: Se0/0/0 PPP: Using default call direction

.Jun 20 02:30:36.596: Se0/0/0 PPP: Treating connection as a dedicated line

.Jun 20 02:30:36.596: Se0/0/0 PPP: Session handle[34000005] Session id[5]

.Jun 20 02:30:36.596: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]

Что происходит в случае, если на одном конце последовательного канала используется инкапсуляция PPP, а на другом — HDLC?

_____

_____

f. Введите команду **encapsulation ppp** на интерфейсе S0/0/0 маршрутизатора «Филиал 1», чтобы исправить несоответствующую инкапсуляцию.

Branch1(config)# **interface s0/0/0**

Branch1(config-if)# **encapsulation ppp**

g. Наблюдайте за сообщениями команды debug PPP от маршрутизатора «Филиал 1» при установке подключения между маршрутизаторами «Филиал 1» и «Главный».

Branch1(config-if)#

Jun 20 03:01:57.399: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

Jun 20 03:01:59.399: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Jun 20 03:01:59.399: Se0/0/0 PPP: Sending cstate UP notification

Jun 20 03:01:59.399: Se0/0/0 PPP: Processing CstateUp message

Jun 20 03:01:59.399: PPP: Alloc Context [30F8D4F0]

Jun 20 03:01:59.399: ppp9 PPP: Phase is ESTABLISHING

Jun 20 03:01:59.399: Se0/0/0 PPP: Using default call direction

Jun 20 03:01:59.399: Se0/0/0 PPP: Treating connection as a dedicated line

Jun 20 03:01:59.399: Se0/0/0 PPP: Session handle[BA000009] Session id[9]

Jun 20 03:01:59.399: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]

Jun 20 03:01:59.399: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10

Jun 20 03:01:59.399: Se0/0/0 LCP: MagicNumber 0x8D0EAC44 (0x05068D0EAC44)

Jun 20 03:01:59.399: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]

Jun 20 03:01:59.407: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]

Jun 20 03:01:59.407: Se0/0/0 LCP: I CONFREQ [REQsent] id 1 len 10

Jun 20 03:01:59.407: Se0/0/0 LCP: MagicNumber 0x73B4F1AF (0x050673B4F1AF)

Jun 20 03:01:59.407: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 10

Jun 20 03:01:59.407: Se0/0/0 LCP: MagicNumber 0x73B4F1AF (0x050673B4F1AF)

Jun 20 03:01:59.407: Se0/0/0 LCP: Event[Receive ConfReq+] State[REQsent to ACKsent]

Jun 20 03:01:59.407: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]

Jun 20 03:01:59.407: Se0/0/0 LCP: I CONFACK [ACKsent] id 1 len 10

Jun 20 03:01:59.407: Se0/0/0 LCP: MagicNumber 0x8D0EAC44 (0x05068D0EAC44)

Jun 20 03:01:59.407: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]

Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is FORWARDING, Attempting Forward

Jun 20 03:01:59.439: Se0/0/0 LCP: State is Open

Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP

Jun 20 03:01:59.439: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

Jun 20 03:01:59.439: Se0/0/0 PPP: Outbound cdp packet dropped, line protocol not up

Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is UP

Jun 20 03:01:59.439: Se0/0/0 IPCP: Protocol configured, start CP. state[Initial]

Jun 20 03:01:59.439: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]

Jun 20 03:01:59.439: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10

Jun 20 03:01:59.439: Se0/0/0 IPCP: Address 10.1.1.1 (0x03060A010101)

Jun 20 03:01:59.439: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]

Jun 20 03:01:59.439: Se0/0/0 CDPCP: Protocol configured, start CP. state[Initial]

<Данные опущены>

Jun 20 03:01:59.471: Se0/0/0 Added to neighbor route AVL tree: topoid 0, address 10.1.1.2

Jun 20 03:01:59.471: Se0/0/0 IPCP: Install route to 10.1.1.2

Jun 20 03:01:59.471: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80

Jun 20 03:01:59.479: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]

Jun 20 03:01:59.479: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84

Jun 20 03:01:59.483: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]

Jun 20 03:01:59.483: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68

Jun 20 03:01:59.491: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]

Jun 20 03:01:59.491: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 148

Jun 20 03:01:59.511: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 148 link[ip]

Jun 20 03:01:59.511: %OSPF-5-ADJCHG:Process 1, Nbr 209.165.200.225 on Serial0/0/0 from LOADING to FULL, Loading Done

Jun 20 03:01:59.511: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68

Jun 20 03:01:59.519: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 60 link[ip]

h. Наблюдайте за сообщениями команды debug PPP от маршрутизатора «Главный» при установке подключения между маршрутизаторами «Филиал 1» и «Главный».

Jun 20 03:01:59.393: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]

Jun 20 03:01:59.393: Se0/0/0 LCP: I CONFREQ [Open] id 1 len 10

Jun 20 03:01:59.393: Se0/0/0 LCP: MagicNumber 0x8D0EAC44 (0x05068D0EAC44)

Jun 20 03:01:59.393: Se0/0/0 PPP DISC: PPP Renegotiating Jun 20 03:01:59.393: PPP: NET STOP send to AAA.

Jun 20 03:01:59.393: Se0/0/0 LCP: Event[LCP Reneg] State[Open to Open]

Jun 20 03:01:59.393: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]

Jun 20 03:01:59.393: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 03:01:59.393: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]

Jun 20 03:01:59.393: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 03:01:59.393: Se0/0/0 LCP: Event[DOWN] State[Open to Starting]

Jun 20 03:01:59.393: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

Jun 20 03:01:59.393: Se0/0/0 PPP: Outbound cdp packet dropped, NCP not negotiated

.Jun 20 03:01:59.393: Se0/0/0 PPP: Phase is DOWN

.Jun 20 03:01:59.393: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address 10.1.1.1

.Jun 20 03:01:59.393: Se0/0/0 IPCP: Remove route to 10.1.1.1

.Jun 20 03:01:59.393: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

.Jun 20 03:01:59.397: PPP: Alloc Context [29F9F32C]

.Jun 20 03:01:59.397: ppp38 PPP: Phase is ESTABLISHING

.Jun 20 03:01:59.397: Se0/0/0 PPP: Using default call direction

.Jun 20 03:01:59.397: Se0/0/0 PPP: Treating connection as a dedicated line

<Данные опущены>

.Jun 20 03:01:59.401: Se0/0/0 LCP: MagicNumber 0x73B4F1AF (0x050673B4F1AF)

.Jun 20 03:01:59.401: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]

.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is FORWARDING, Attempting Forward

.Jun 20 03:01:59.433: Se0/0/0 LCP: State is Open

.Jun 20 03:01:59.433: Se0/0/0 PPP: I pkt type 0x8021, datagramsize 14 link[ip]

.Jun 20 03:01:59.433: Se0/0/0 PPP: Queue IPCP code[1] id[1]

.Jun 20 03:01:59.433: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8 link[cdp]

.Jun 20 03:01:59.433: Se0/0/0 PPP: Discarded CDPCP code[1] id[1]

.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP

.Jun 20 03:01:59.433: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

.Jun 20 03:01:59.433: Se0/0/0 PPP: Outbound cdp packet dropped, line protocol not up

.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is UP

.Jun 20 03:01:59.433: Se0/0/0 IPCP: Protocol configured, start CP. state[Initial]

.Jun 20 03:01:59.433: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]

.Jun 20 03:01:59.433: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10

.Jun 20 03:01:59.433: Se0/0/0 IPCP: Address 10.1.1.2 (0x03060A010102)

.Jun 20 03:01:59.433: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]

.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Protocol configured, start CP. state[Initial]

.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Event[OPEN] State[Initial to Starting]

.Jun 20 03:01:59.433: Se0/0/0 CDPCP: O CONFREQ [Starting] id 1 len 4

.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Event[UP] State[Starting to REQsent]

<Данные опущены>

.Jun 20 03:01:59.465: Se0/0/0 IPCP: State is Open

.Jun 20 03:01:59.465: Se0/0/0 Added to neighbor route AVL tree: topoid 0, address 10.1.1.1

.Jun 20 03:01:59.465: Se0/0/0 IPCP: Install route to 10.1.1.1

.Jun 20 03:01:59.465: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80

.Jun 20 03:01:59.465: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]

.Jun 20 03:01:59.469: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84

.Jun 20 03:01:59.477: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]

.Jun 20 03:01:59.477: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68

.Jun 20 03:01:59.481: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]

.Jun 20 03:01:59.489: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 148 link[ip]

.Jun 20 03:01:59.493: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 148

.Jun 20 03:01:59.505: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]

.Jun 20 03:01:59.505: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 60

.Jun 20 03:01:59.517: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 88 link[ip]

.Jun 20 03:01:59.517: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done

.Jun 20 03:01:59.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80

.Jun 20 03:01:59.569: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]

Jun 20 03:02:01.445: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8 link[cdp]

Jun 20 03:02:01.445: Se0/0/0 CDPCP: I CONFREQ [ACKrcvd] id 2 len 4

Jun 20 03:02:01.445: Se0/0/0 CDPCP: O CONFACK [ACKrcvd] id 2 len 4

Jun 20 03:02:01.445: Se0/0/0 CDPCP: Event[Receive ConfReq+] State[ACKrcvd to Open]

Jun 20 03:02:01.449: Se0/0/0 CDPCP: State is Open

Jun 20 03:02:01.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80

Jun 20 03:02:01.569: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]

Jun 20 03:02:02.017: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68

Jun 20 03:02:02.897: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 112 link[ip]

Jun 20 03:02:03.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80

Основываясь на сообщении команды debug, укажите, через какие этапы проходит PPP, если другой конец последовательного канала на маршрутизаторе Central настроен с инкапсуляцией PPP.

_____

_____

Что произойдет, если инкапсуляция PPP настроена на обоих концах последовательного канала?

_____

_____

i. Введите команду **undebug all** (или **u all**) на маршрутизаторах «Филиал 1» и «Главный» и отключите всю отладку на обоих маршрутизаторах.

j. После стабилизации сети выполните команду **show ip interface brief** на маршрутизаторах «Филиал 1» и «Главный». Укажите состояние интерфейса S0/0/0 на обоих маршрутизаторах.

_____

_____

k. Убедитесь, что интерфейс S0/0/0 как на маршрутизаторе «Филиал 1», так и на маршрутизаторе «Главный» настроен на инкапсуляцию PPP.

Ниже запишите команду для проверки инкапсуляции PPP.

_____

_____

l. Инкапсуляцию в последовательном интерфейсе для связи между маршрутизаторами «Главный» и «Филиал 3» измените на инкапсуляцию PPP.

Central(config)# **interface s0/0/1**

Central(config-if)# **encapsulation ppp**

Central(config-if)#

Jun 20 03:17:15.933: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from

FULL to DOWN, Neighbor Down: Interface

down or detached

Jun 20 03:17:17.933: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,

changed

state to

down

Jun 20 03:17:23.741: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,

changed

state to up

Jun 20 03:17:23.825: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from

LOADING to FULL,

Loading Done

Branch3(config)# **interface s0/0/1**

Branch3(config-if)# **encapsulation ppp**

Branch3(config-if)#

Jun 20 03:17:21.744: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1

from FULL to DOWN, Neighbor Down: Interface

down or detached

Jun 20 03:17:21.948: %LINEPROTO-5-UPDOWN: Line protocol on

Interface Serial0/0/1,

changed

state to

down

.Jun 20 03:17:21.964: %LINEPROTO-5-UPDOWN: Line protocol on

Interface Serial0/0/1,

changed

state to up

.Jun 20 03:17:23.812: %OSPF-5-ADJCHG: Process 1, Nbr

209.165.200.225 on Serial0/0/1

from LOADING to FULL,

Loading Done

m. Перед переходом к части 3 убедитесь в том, что сквозное соединение восстановлено.

Часть 3: Настройка аутентификации CHAP PPP

Шаг 1: Убедитесь, что инкапсуляция PPP настроена на всех последовательных интерфейсах.

Запишите команды, используемые для подтверждения того, что настроена инкапсуляция PPP.

_____

_____

Шаг 2: Настройте аутентификацию CHAP PPP для канала между маршрутизатором «Главный» и маршрутизатором «Филиал 3».

a. Настройте имя пользователя для аутентификации CHAP.

Central(config)# **username Branch3 password cisco**

Branch3(config)# **username Central password cisco**

b. Выполните команды **debug ppp** на маршрутизаторе «Филиал 3» для наблюдения за процессом, который связан с аутентификацией.

Branch3# **debug ppp negotiation**

PPP protocol negotiation debugging is on

Branch3# **debug ppp packet**

PPP packet display debugging is on

c. Настройте интерфейс S0/0/1 на маршрутизаторе «Филиал 3» для аутентификации CHAP.

Branch3(config)# **interface s0/0/1**

Branch3(config-if)# **ppp authentication chap**

d. Изучите сообщения команды debug PPP на маршрутизаторе «Филиал 3», выдаваемые во время согласования с маршрутизатором «Главный».

Branch3(config-if)#

Jun 20 04:25:02.079: Se0/0/1 PPP DISC: Authentication configuration changed Jun 20 04:25:02.079: PPP: NET STOP send to AAA.

Jun 20 04:25:02.079: Se0/0/1 IPCP: Event[DOWN] State[Open to Starting]

Jun 20 04:25:02.079: Se0/0/1 IPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 04:25:02.079: Se0/0/1 CDPCP: Event[DOWN] State[Open to Starting]

Jun 20 04:25:02.079: Se0/0/1 CDPCP: Event[CLOSE] State[Starting to Initial]

Jun 20 04:25:02.079: Se0/0/1 LCP: Event[DOWN] State[Open to Starting]

Jun 20 04:25:02.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down

Jun 20 04:25:02.079: Se0/0/1 PPP: Outbound cdp packet dropped, NCP not negotiated

.Jun 20 04:25:02.079: Se0/0/1 PPP: Phase is DOWN

.Jun 20 04:25:02.079: Se0/0/1 Deleted neighbor route from AVL tree: topoid 0, address

10.2.2.2

.Jun 20 04:25:02.079: Se0/0/1 IPCP: Remove route to 10.2.2.2

.Jun 20 04:25:02.079: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

.Jun 20 04:25:02.083: PPP: Alloc Context [29F4DA8C]

.Jun 20 04:25:02.083: ppp73 PPP: Phase is ESTABLISHING

.Jun 20 04:25:02.083: Se0/0/1 PPP: Using default call direction

.Jun 20 04:25:02.083: Se0/0/1 PPP: Treating connection as a dedicated line

.Jun 20 04:25:02.083: Se0/0/1 PPP: Session handle[2700004D] Session id[73]

<Данные опущены>

.Jun 20 04:25:02.091: Se0/0/1 PPP: I pkt type 0xC021, datagramsize 19 link[ppp]

.Jun 20 04:25:02.091: Se0/0/1 LCP: I CONFACK [ACKsent] id 1 len 15

.Jun 20 04:25:02.091: Se0/0/1 LCP: AuthProto CHAP (0x0305C22305)

.Jun 20 04:25:02.091: Se0/0/1 LCP: MagicNumber 0xF7B20F10 (0x0506F7B20F10)

.Jun 20 04:25:02.091: Se0/0/1 LCP: Event[Receive ConfAck] State[ACKsent to Open]

.Jun 20 04:25:02.123: Se0/0/1 PPP: Phase is AUTHENTICATING, by this end

.Jun 20 04:25:02.123: Se0/0/1 CHAP: O CHALLENGE id 1 len 28 from "Branch3"

.Jun 20 04:25:02.123: Se0/0/1 LCP: State is Open

.Jun 20 04:25:02.127: Se0/0/1 PPP: I pkt type 0xC223, datagramsize 32 link[ppp]

.Jun 20 04:25:02.127: Se0/0/1 CHAP: I RESPONSE id 1 len 28 from "Central"

.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is FORWARDING, Attempting Forward

.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is AUTHENTICATING, Unauthenticated User

.Jun 20 04:25:02.127: Se0/0/1 PPP: Sent CHAP LOGIN Request

.Jun 20 04:25:02.127: Se0/0/1 PPP: Received LOGIN Response PASS

.Jun 20 04:25:02.127: Se0/0/1 IPCP: Authorizing CP

.Jun 20 04:25:02.127: Se0/0/1 IPCP: CP stalled on event[Authorize CP]

.Jun 20 04:25:02.127: Se0/0/1 IPCP: CP unstall

.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is FORWARDING, Attempting Forward

.Jun 20 04:25:02.135: Se0/0/1 PPP: Phase is AUTHENTICATING, Authenticated User

.Jun 20 04:25:02.135: Se0/0/1 CHAP: O SUCCESS id 1 len 4

.Jun 20 04:25:02.135: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

.Jun 20 04:25:02.135: Se0/0/1 PPP: Outbound cdp packet dropped, line protocol not up

.Jun 20 04:25:02.135: Se0/0/1 PPP: Phase is UP

.Jun 20 04:25:02.135: Se0/0/1 IPCP: Protocol configured, start CP. state[Initial]

.Jun 20 04:25:02.135: Se0/0/1 IPCP: Event[OPEN] State[Initial to Starting]

.Jun 20 04:25:02.135: Se0/0/1 IPCP: O CONFREQ [Starting] id 1 len 10

<Данные опущены>

.Jun 20 04:25:02.143: Se0/0/1 CDPCP: I CONFACK [ACKsent] id 1 len 4

.Jun 20 04:25:02.143: Se0/0/1 CDPCP: Event[Receive ConfAck] State[ACKsent to Open]

.Jun 20 04:25:02.155: Se0/0/1 IPCP: State is Open

.Jun 20 04:25:02.155: Se0/0/1 CDPCP: State is Open

.Jun 20 04:25:02.155: Se0/0/1 Added to neighbor route AVL tree: topoid 0, address 10.2.2.2

.Jun 20 04:25:02.155: Se0/0/1 IPCP: Install route to 10.2.2.2

.Jun 20 04:25:02.155: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 80

.Jun 20 04:25:02.155: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 80 link[ip]

.Jun 20 04:25:02.155: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 84

.Jun 20 04:25:02.167: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 84 link[ip]

.Jun 20 04:25:02.167: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 68

.Jun 20 04:25:02.171: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 68 link[ip]

.Jun 20 04:25:02.171: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 148

.Jun 20 04:25:02.191: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 148 link[ip]

.Jun 20 04:25:02.191: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1 from LOADING to FULL, Loading Done

.Jun 20 04:25:02.191: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 68

.Jun 20 04:25:02.571: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 80

.Jun 20 04:25:03.155: Se0/0/1 PPP: I pkt type 0x0207, datagramsize 333 link[cdp]

.Jun 20 04:25:03.155: Se0/0/1 PPP: O pkt type 0x0207, datagramsize 339

.Jun 20 04:25:04.155: Se0/0/1 PPP: O pkt type 0x0207, datagramsize 339

Основываясь на сообщениях команды debug для PPP, укажите, какие этапы проходит маршрутизатор «Филиал 3», прежде чем будет установлена связь с маршрутизатором «Главный».

_____

_____

e. Введите команду **debug ppp authentication** для наблюдения за сообщениями аутентификации CHAP на маршрутизаторе Central.

Central# **debug ppp authentication**

PPP authentication debugging is on

f. Настройте аутентификацию CHAP на интерфейсе S0/0/1 на маршрутизаторе «Главный».

g. Наблюдайте за сообщениями команд debug PPP, относящихся к аутентификации CHAP на маршрутизаторе «Главный».

Central(config-if)#

.Jun 20 05:05:16.057: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down

.Jun 20 05:05:16.061: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

.Jun 20 05:05:16.061: Se0/0/1 PPP: Using default call direction

.Jun 20 05:05:16.061: Se0/0/1 PPP: Treating connection as a dedicated line

.Jun 20 05:05:16.061: Se0/0/1 PPP: Session handle[12000078] Session id[112]

.Jun 20 05:05:16.081: Se0/0/1 CHAP: O CHALLENGE id 1 len 28 from "Central"

.Jun 20 05:05:16.089: Se0/0/1 CHAP: I CHALLENGE id 1 len 28 from "Branch3"

.Jun 20 05:05:16.089: Se0/0/1 PPP: Sent CHAP SENDAUTH Request

.Jun 20 05:05:16.089: Se0/0/1 PPP: Received SENDAUTH Response PASS

.Jun 20 05:05:16.089: Se0/0/1 CHAP: Using hostname from configured hostname

.Jun 20 05:05:16.089: Se0/0/1 CHAP: Using password from AAA

.Jun 20 05:05:16.089: Se0/0/1 CHAP: O RESPONSE id 1 len 28 from "Central"

.Jun 20 05:05:16.093: Se0/0/1 CHAP: I RESPONSE id 1 len 28 from "Branch3"

.Jun 20 05:05:16.093: Se0/0/1 PPP: Sent CHAP LOGIN Request

.Jun 20 05:05:16.093: Se0/0/1 PPP: Received LOGIN Response PASS

.Jun 20 05:05:16.093: Se0/0/1 CHAP: O SUCCESS id 1 len 4

.Jun 20 05:05:16.097: Se0/0/1 CHAP: I SUCCESS id 1 len 4

.Jun 20 05:05:16.097: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

.Jun 20 05:05:16.165: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from LOADING to FULL, Loading Done

h. Введите команду **undebug all** (или **u all**) на маршрутизаторах «Главный» и «Филиал 3» и отключите всю отладку.

Central# **undebug all**

All possible debugging has been turned off

Шаг 3: Намеренно разорвите последовательный канал, настроенный с использованием аутентификации.

a. На маршрутизаторе «Главный» настройте имя пользователя для использования с «Филиал 1».

Назначьте **cisco** в качестве пароля.

Central(config)# **username Branch1 password cisco**

b. На маршрутизаторах «Главный» и «Филиал 1» настройте аутентификацию CHAP на интерфейсе S0/0/0. Что происходит с интерфейсом?

_____

_____ **Примечание**. Для ускорения процесса выключите интерфейс и снова его включите.

c. Для исследования возникшего процесса используйте команду **debug ppp negotiation**.

Central# **debug ppp negotiation**

PPP protocol negotiation debugging is on

Central(config-if)#

.Jun 20 05:25:26.229: Se0/0/0 PPP: Missed a Link-Up transition, starting PPP

.Jun 20 05:25:26.229: Se0/0/0 PPP: Processing FastStart message

.Jun 20 05:25:26.229: PPP: Alloc Context [29F9F32C]

.Jun 20 05:25:26.229: ppp145 PPP: Phase is ESTABLISHING

.Jun 20 05:25:26.229: Se0/0/0 PPP: Using default call direction

.Jun 20 05:25:26.229: Se0/0/0 PPP: Treating connection as a dedicated line

.Jun 20 05:25:26.229: Se0/0/0 PPP: Session handle[6000009C] Session id[145]

.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]

.Jun 20 05:25:26.229: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 15

.Jun 20 05:25:26.229: Se0/0/0 LCP: AuthProto CHAP (0x0305C22305)

.Jun 20 05:25:26.229: Se0/0/0 LCP: MagicNumber 0x74385C31 (0x050674385C31)

.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]

.Jun 20 05:25:26.229: Se0/0/0 LCP: I CONFREQ [REQsent] id 1 len 10

.Jun 20 05:25:26.229: Se0/0/0 LCP: MagicNumber 0x8D920101 (0x05068D920101)

.Jun 20 05:25:26.229: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 10

.Jun 20 05:25:26.229: Se0/0/0 LCP: MagicNumber 0x8D920101 (0x05068D920101)

.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[Receive ConfReq+] State[REQsent to ACKsent]

.Jun 20 05:25:26.233: Se0/0/0 LCP: I CONFACK [ACKsent] id 1 len 15

.Jun 20 05:25:26.233: Se0/0/0 LCP: AuthProto CHAP (0x0305C22305)

.Jun 20 05:25:26.233: Se0/0/0 LCP: MagicNumber 0x74385C31 (0x050674385C31)

.Jun 20 05:25:26.233: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]

.Jun 20 05:25:26.261: Se0/0/0 PPP: Phase is AUTHENTICATING, by this end

.Jun 20 05:25:26.261: Se0/0/0 CHAP: O CHALLENGE id 1 len 28 from "Central"

.Jun 20 05:25:26.261: Se0/0/0 LCP: State is Open

.Jun 20 05:25:26.265: Se0/0/0 LCP: I TERMREQ [Open] id 2 len 4

.Jun 20 05:25:26.265: Se0/0/0 PPP DISC: Received LCP TERMREQ from peer .Jun 20 05:25:26.265: PPP: NET STOP send to AAA.

.Jun 20 05:25:26.265: Se0/0/0 PPP: Phase is TERMINATING

.Jun 20 05:25:26.265: Se0/0/0 LCP: O TERMACK [Open] id 2 len 4

.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[Receive TermReq] State[Open to Stopping]

.Jun 20 05:25:26.265: Se0/0/0 PPP: Sending cstate DOWN notification

.Jun 20 05:25:26.265: Se0/0/0 PPP: Processing CstateDown message

.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[CLOSE] State[Stopping to Closing]

.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]

.Jun 20 05:25:26.265: Se0/0/0 PPP: Phase is DOWN

Объясните, что приводит к окончательному завершению канала. Запишите ниже команду, выполненную для устранения неполадки.

_____

_____

d. Введите команду **undebug all** на всех маршрутизаторах, чтобы отключить отладку.

e. Проверьте связь между конечными устройствами.

Вопросы на закрепление

1. Каковы признаки того, что на канале последовательной связи настроена несоответствующая инкапсуляция?

_____

_____

2. Каковы признаки того, что на канале последовательной связи настроена несоответствующая аутентификация?

_____

_____

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet № 1**	**Интерфейс Ethernet № 2**	**Последовательный интерфейс № 1**	**Последовательный интерфейс № 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует.

В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Практическая работа 10

Тема: Проверка PPP

Цели: Произвести проверку протокола PPP

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задачи

Часть 1. Построение сети и загрузка конфигурации устройств

Часть 2. Поиск и устранение неполадок канального уровня

Часть 3. Поиск и устранение неполадок сетевого уровня

Общие сведения/сценарий

Маршрутизаторы в сети вашей компании были настроены неопытным сетевым инженером. В результате нескольких ошибок в настройках возникли проблемы с подключением. Ваш начальник поручил вам найти и устранить неполадки конфигурации и задокументировать работу. Найдите и исправьте ошибки, используя свои знания PPP и стандартные методы тестирования. Убедитесь, что на всех последовательных каналах используется аутентификация CHAP PPP и что все сети доступны.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии 15.2(4)M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии

Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Точные идентификаторы интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что у всех маршрутизаторов и коммутаторов была удалена начальная конфигурация. Если вы не уверены, обратитесь к инструктору.

Топология

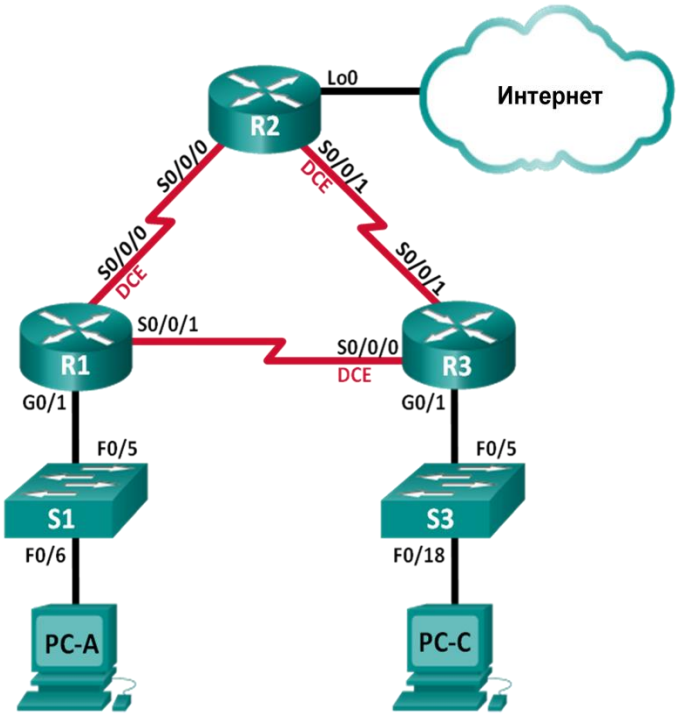


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Н/Д (недоступно)
	S0/0/0 (DCE)	192.168.2.1	255.255.255.252	Н/Д (недоступно)
	S0/0/1	192.168.3.1	255.255.255.252	Н/Д (недоступно)

R2	Lo0	209.165.200.225	255.255.255.252	Н/Д (недоступно)
	S0/0/0	192.168.12.2	255.255.255.252	Н/Д (недоступно)
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	Н/Д (недоступно)
R3	G0/1	192.168.3.1	255.255.255.0	Н/Д (недоступно)
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	Н/Д (недоступно)
	S0/0/1	192.168.23.2	255.255.255.252	Н/Д (недоступно)
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3

(универсальный образ) или аналогичная модель)

- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- 2 ПК (ОС Windows с программой эмуляции терминалов, такой как Tera Term)
- Консольные кабели для настройки устройств на базе Cisco IOS через консольные порты
- Кабели Ethernet и последовательные кабели в соответствии с топологией

Часть 1: Построение сети и загрузка настроек устройств

В части 1 вам предстоит создать топологию сети, настроить базовые параметры для хостов ПК и загрузить настройки маршрутизаторов.

Шаг 1: Подключите кабели сети согласно приведенной топологии.

Шаг 2: Настройте узлы ПК.

Шаг 3: Загрузите настройки маршрутизатора.

Загрузите в соответствующий маршрутизатор следующие настройки. На всех маршрутизаторах настроены одинаковые пароли. Пароль привилегированного режима — **class**. Пароль для консоли и доступа vty — **cisco**. Все последовательные интерфейсы должны быть настроены с инкапсуляцией PPP и аутентификацией по протоколу CHAP с паролем **chap123**.

Конфигурация маршрутизатора R1:

hostname R1 enable secret class no ip domain lookup banner motd #Unauthorized Access is Prohibited!# username R2 password chap123 username R3 password chap123 interface g0/1 ip address 192.168.1.1 255.255.255.0 no shutdown interface s0/0/0 ip address 192.168.12.1 255.255.255.252 clock rate 128000 encapsulation ppp ppp authentication chap interface s0/0/1 ip address 192.168.31.1 255.255.255.252 encapsulation ppp ppp authentication pap exit router ospf 1 router-id 1.1.1.1 network 192.168.1.0 0.0.0.255 area 0 network 192.168.12.0 0.0.0.3 area 0 network 192.168.13.0 0.0.0.3 area 0 passive-interface g0/1 exit line con 0 password cisco logging synchronous login line vty 0 4 password cisco login

Конфигурация маршрутизатора R2:

hostname R2 enable secret class no ip domain lookup banner motd #Unauthorized Access is Prohibited!# username R1 password chap123 username r3 password chap123 interface lo0 ip address 209.165.200.225 255.255.255.252 interface s0/0/0 ip address 192.168.12.2 255.255.255.252 encapsulation ppp ppp authentication chap no shutdown interface s0/0/1 ip address 192.168.23.1 255.255.255.252 clock rate 128000 no shutdown exit router ospf 1 router-id 2.2.2.2 network 192.168.12.0 0.0.0.3 area 0 network 192.168.23.0 0.0.0.3 area 0 default-information originate exit

ip route 0.0.0.0 0.0.0.0 loopback0 line con 0 password cisco logging synchronous login line vty 0 4

password cisco login

Конфигурация маршрутизатора R3:

hostname R3 enable secret class no ip domain lookup banner motd #Unauthorized Access is Prohibited!# username R2 password chap123 username R3 password chap123 interface g0/1 ip address 192.168.3.1 255.255.255.0 no shutdown interface s0/0/0 ip address 192.168.13.2 255.255.255.252 clock rate 128000 encapsulation ppp ppp authentication chap no shutdown interface s0/0/1 ip address 192.168.23.2 255.255.255.252 encapsulation ppp ppp authentication chap no shutdown exit router ospf 1 router-id 3.3.3.3 network 192.168.13.0 0.0.0.3 area 0 network 192.168.23.0 0.0.0.3 area 0 passive-interface g0/1 line con 0 password cisco logging synchronous login line vty 0 4

password cisco login

Шаг 4: Сохраните текущую конфигурацию.

Часть 2: Поиск и устранение неполадок на канальном уровне

В части 2 вы будете использовать команды **show** для поиска и устранения неполадок на канальном уровне. Не забудьте проверить такие параметры, как тактовая частота, инкапсуляция, CHAP и имена и пароли пользователей.

Шаг 1: Проверьте конфигурацию маршрутизатора R1.

a. Используйте команду **show interfaces**, чтобы определить, установлен ли PPP на обоих последовательных каналах.

Основываясь на результатах работы команды **show interfaces** для S0/0/0 и S0/0/1, укажите возможные неполадки в каналах PPP.

_____

_____

b. В ходе поиска и устранения неполадок используйте команду **debug ppp authentication** для просмотра сведений об аутентификации PPP в режиме реального времени.

R1# **debug ppp authentication**

PPP authentication debugging is on

c. Для исследования параметров на S0/0/0 используйте команду **show run interface s0/0/0**.

Устраните все неполадки, связанные с S0/0/0. Запишите команды, использованные для исправления конфигурации.

_____

_____

Укажите выходные данные команды debug, выполненной после устранения неполадки.

_____

_____

d. Для исследования параметров на S0/0/1 используйте команду **show run interface s0/0/1**.

Устраните все неполадки, связанные с S0/0/1. Запишите команды, использованные для исправления конфигурации.

Укажите выходные данные команды debug, выполненной после устранения неполадки.

_____

_____

e. Для отключения вывода данных команды debug PPP используйте команду **no debug ppp authentication** или **undebug all**.

f. Для проверки правильности настроек имени и пароля пользователя используйте команду **show running-config | include username**.

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления конфигурации.

_____

_____

Шаг 2: Проверьте конфигурацию маршрутизатора R2.

a. Используя команду **show interfaces**, определите, установлен ли PPP на обоих последовательных каналах.

Все ли каналы установлены? _____

Если ответ отрицательный, то какие каналы следует проверить? В чем заключаются возможные причины неполадок?

_____

_____

b. Для исследования связей, которые не были установлены, используйте команду **show run interface**.

Устраните все обнаруженные неполадки, относящиеся к интерфейсам. Запишите команды, использованные для исправления конфигурации.

_____

_____

c. Для проверки правильности настроек имени и пароля пользователя используйте команду **show running-config | include username**.

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления конфигурации.

_____

_____

d. Используйте команду **show ppp interface serial** для того последовательного интерфейса, который вы отлаживаете.

Связь установлена? _____

Шаг 3: Проверьте конфигурацию маршрутизатора R3.

a. Используйте команду **show interfaces**, чтобы определить, установлен ли PPP на обоих последовательных каналах.

Все ли каналы установлены? _____

Если ответ отрицательный, то какие каналы следует проверить? В чем заключаются возможные причины неполадок?

_____

_____

b. Используйте команду **show run interface** для проверки всех последовательных каналов, соединение для которых не было установлено.

Устраните все неполадки, обнаруженные на интерфейсах. Запишите команды, использованные для исправления конфигурации.

_____

_____

c. Для проверки правильности настроек имени и пароля пользователя используйте команду **show running-config | include username**.

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления конфигурации.

_____

_____

d. Используйте команду **show interface**, чтобы убедиться, что последовательные связи установлены.

e. По всем ли каналам PPP установлены соединения? _____

f. Эхо-запрос от узла ПК A к Lo0 выполняется успешно? _____

g. Успешно ли выполняется эхо-запрос от узла ПК A на узел ПК C? _____

Примечание. Чтобы успешно получать ответы на ping-запросы между ПК, может потребоваться отключить межсетевой экран.

Часть 3: Поиск и устранение неполадок сетевого уровня

В части 3 вам предстоит убедиться, что подключения уровня 3 установлены на всех интерфейсах, исследуя для этого настройки IPv4 и OSPF.

Шаг 1: Убедитесь, что интерфейсы, указанные в таблице адресации, активны и настроены с правильными IP-адресами.

Выполните команду **show ip interface brief** на всех маршрутизаторах, чтобы убедиться, что все интерфейсы находятся в рабочем состоянии (up/up).

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления конфигурации.

_____

_____

Шаг 2: Проверка маршрутизации OSPF

Выполните команду **show ip protocols** и убедитесь, что протокол OSPF работает и все сети анонсированы.

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления конфигурации.

_____

_____

Успешно ли выполняется эхо-запрос от узла ПК А на узел ПК С? _____

Если между некоторыми хостами нет связи, продолжите поиск и устранение неполадок, чтобы устранить все имеющиеся неполадки.

Примечание. Чтобы успешно получать ответы на ping-запросы между ПК, может потребоваться отключить межсетевой экран.

Сводная таблица по интерфейсам маршрутизаторов

Сводка по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet № 1**	**Интерфейс Ethernet № 2**	**Последовательный интерфейс № 1**	**Последовательный интерфейс № 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах Cisco IOS для обозначения интерфейса.

Практическая работа 11

Тема: Настройка маршрутизатора в качестве клиента PPPoE для подключения DSL

Цели: Произвести настройку маршрутизатора в качестве клиента PPPoE для подключение DSL

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задачи

Часть 1. Развёртывание сети

Часть 2. Настройка маршрутизатора ISP

Часть 3. Настройка маршрутизатора Cust1

Исходные данные/сценарий

Интернет-провайдеры часто используют протокол PPPoE для передачи данных по каналам DSL своим заказчикам. PPP поддерживает назначение IP-адреса устройству на удаленном конце канала PPP. Что ещё более важно, PPP поддерживает аутентификацию CHAP. Интернет-провайдеры могут проверять учётные записи, чтобы определить, оплатил ли заказчик свой счёт, прежде чем позволить ему подключиться к Интернету

В этой лабораторной работе выполняется настройка подключения на стороне клиента и интернетпровайдера для настройки PPPoE. В большинстве случаев достаточно выполнить настройку на стороне клиента.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы Cisco Catalyst серии 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь в том, что маршрутизаторы и коммутаторы очищены от данных и на них нет стартовых конфигураций. Если вы не уверены в этом, обратитесь к инструктору.

Топология

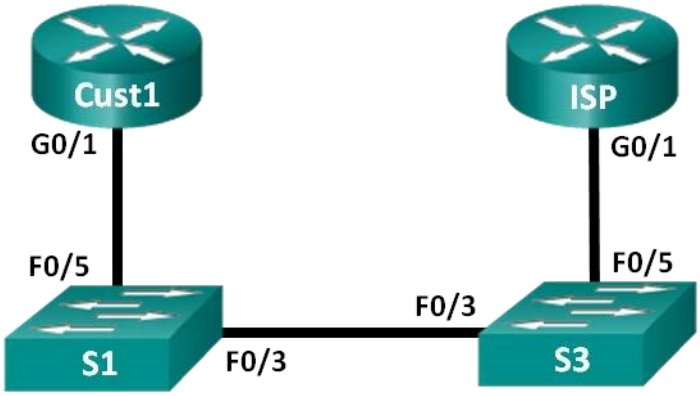


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Cust1	G0/1	Получен с помощью PPP	Получен с помощью PPP	Получен с помощью PPP

ISP	G0/1	Недосту пно	Нед оступн о	Недоступн о

Необходимые ресурсы:

- 2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Построение сети

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

a. Отключите поиск DNS.
b. Настройте имя устройств в соответствии с топологией.
c. Зашифруйте незашифрованные пароли.
d. Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.
e. Назначьте class в качестве зашифрованного пароля доступа к привилегированному режиму.
f. Назначьте cisco в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.
g. Настройте ведение журнала состояния консоли на синхронный режим.
h. Сохраните настройку.

Часть 2: Настройка маршрутизатора интернет-провайдера ISP

В части 2 необходимо настроить маршрутизатор ISP с использованием параметров PPPoE для приёма подключений от маршрутизатора Cust1.

Примечание. Многие из команд настройки PPPoE для маршрутизатора интернет-провайдера выходят за рамки курса; однако они необходимы для выполнения лабораторной работы. Их можно скопировать и вставить в Маршрутизатор ISP в командной строке режима глобальной конфигурации.

a. Создайте в локальной базе учётных записей имя пользователя Cust1 с паролем ciscopppoe.

```
ISP(config)# username Cust1 password ciscopppoe
```

b. Создайте пул адресов, которые будут назначены пользователям.

```
ISP(config)# ip local pool PPPoEPOOL 10.0.0.1 10.0.0.10
```

c. Создайте виртуальный шаблон Virtual Template и свяжите с ним IP-адрес G0/1. Свяжите виртуальный шаблон с пулом адресов. Настройте CHAP для аутентификации пользователей.

```
ISP(config)# interface virtual-template 1
ISP(config-if)# ip address 10.0.0.254 255.255.255.0
ISP(config-if)# mtu 1492
ISP(config-if)# peer default ip address pool PPPoEPOOL
ISP(config-if)# ppp authentication chap callin
ISP(config-if)# exit
```

d. Назначьте шаблон группе PPPoE.

```
ISP(config)# bba-group pppoe global
ISP(config-bba-group)# virtual-template 1
ISP(config-bba-group)# exit
```

e. Свяжите группу bba-group с физическим интерфейсом G0/1.

```
ISP(config)# interface g0/1
ISP(config-if# pppoe enable group global ISP(config-if)# no shutdown
```

Часть 3: Настройка маршрутизатора Cust1

В части 3 необходимо настроить маршрутизатор Cust1 с использованием параметров PPPoE.

a. Настройте интерфейс G0/1 для подключения PPPoE.

```
Cust1(config)# interface g0/1
```

Cust1(config-if)# pppoe enable

Cust1(config-if)# pppoe-client dial-pool-number 1

Cust1(config-if)# exit

b. Свяжите интерфейс G0/1 с интерфейсом номеронабирателя Dialer. Используйте имя пользователя Cust1 и пароль ciscopppoe, настроенные в части 2.

Cust1(config)# interface dialer 1

Cust1(config-if)# mtu 1492

Cust1(config-if)# ip address negotiated

Cust1(config-if)# encapsulation ppp

Cust1(config-if)# dialer pool 1

Cust1(config-if)# ppp authentication chap callin

Cust1(config-if)# ppp chap hostname Cust1

Cust1(config-if)# ppp chap password ciscopppoe

Cust1(config-if)# exit

c. Настройте статический маршрут по умолчанию через интерфейс номеронабирателя.

Cust1(config)# ip route 0.0.0.0 0.0.0.0 dialer 1

d. Настройте отладку на маршрутизаторе Cust1 для отображения согласования PPP и PPPoE.

Cust1# debug ppp authentication

Cust1# debug pppoe events

e. Включите интерфейс G0/1 на маршрутизаторе Cust1 и проверьте выходные данные отладки при установлении сеанса номеронабирателя PPPoE и во время аутентификации CHAP.

*Jul 30 19:28:42.427: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down

*Jul 30 19:28:46.175: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up

*Jul 30 19:28:47.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface

GigabitEthernet0/1, changed state to up

*Jul 30 19:29:03.839: padi timer expired

*Jul 30 19:29:03.839: Sending PADI: Interface = GigabitEthernet0/1

*Jul 30 19:29:03.839: PPPoE 0: I PADO R:30f7.0da3.0b01 L:30f7.0da3.0bc1 Gi0/1

*Jul 30 19:29:05.887: PPPOE: we've got our pado and the pado timer went off

*Jul 30 19:29:05.887: OUT PADR from PPPoE Session

*Jul 30 19:29:05.895: PPPoE 1: I PADS R:30f7.0da3.0b01 L:30f7.0da3.0bc1 Gi0/1

*Jul 30 19:29:05.895: IN PADS from PPPoE Session

*Jul 30 19:29:05.899: %DIALER-6-BIND: Interface Vi2 bound to profile Di1 *Jul 30 19:29:05.899: PPPoE: Virtual Access interface obtained.

*Jul 30 19:29:05.899: PPPoE : encap string prepared

*Jul 30 19:29:05.899: [0]PPPoE 1: data path set to PPPoE Client

*Jul 30 19:29:05.903: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up

*Jul 30 19:29:05.911: Vi2 PPP: Using dialer call direction

*Jul 30 19:29:05.911: Vi2 PPP: Treating connection as a callout

*Jul 30 19:29:05.911: Vi2 PPP: Session handle[C6000001] Session id[1]

*Jul 30 19:29:05.919: Vi2 PPP: No authorization without authentication

*Jul 30 19:29:05.939: Vi2 CHAP: I CHALLENGE id 1 len 24 from "ISP"

*Jul 30 19:29:05.939: Vi2 PPP: Sent CHAP SENDAUTH Request

*Jul 30 19:29:05.939: Vi2 PPP: Received SENDAUTH Response FAIL

*Jul 30 19:29:05.939: Vi2 CHAP: Using hostname from interface CHAP

*Jul 30 19:29:05.939: Vi2 CHAP: Using password from interface CHAP

*Jul 30 19:29:05.939: Vi2 CHAP: O RESPONSE id 1 len 26 from "Cust1"

*Jul 30 19:29:05.955: Vi2 CHAP: I SUCCESS id 1 len 4

*Jul 30 19:29:05.955: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state to up *Jul 30 19:29:05.983: PPPoE : ipfib_encapstr prepared

*Jul 30 19:29:05.983: PPPoE : ipfib_encapstr prepared

f. Введите команду show ip interface brief на маршрутизаторе Cust1, чтобы отобразить IP-адрес, назначенный маршрутизатором ISP. Выходные данные

приведены ниже. Каким способом был получен этот IP-адрес?

_____

```
Cust1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         unassigned      YES unset  up                    up
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                unassigned      YES unset  administratively down down
Dialer1                    10.0.0.1        YES IPCP   up                    up
Virtual-Access1            unassigned      YES unset  up                    up
Virtual-Access2            unassigned      YES unset  up                    up
```

g. Введите команду show ip route на маршрутизаторе Cust1. Выходные данные приведены ниже.

```
Cust1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2       E1 - OSPF external type 1, E2 - OSPF external type 2       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2       ia - IS-IS inter area, * - candidate default, U - per-user static route       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, Dialer1
      10.0.0.0/32 is subnetted, 2 subnets
C        10.0.0.1 is directly connected, Dialer1
C        10.0.0.254 is directly connected, Dialer1
```

h. Введите команду show pppoe session на маршрутизаторе Cust1. Выходные данные приведены ниже.

Cust1# show pppoe session

1 client session

Uniq ID PPPoE RemMAC Port VT VA State

SID LocMAC VA-st Type

N/A 1 30f7.0da3.0b01 Gi0/1 Di1 Vi2 UP

30f7.0da3.0bc1 UP

i. Отправьте эхо-запрос на адрес 10.0.0.254 с маршрутизатора Cust1. Эхо-запрос должен быть успешным. В противном случае устраните неполадки, пока не будет установлено подключение.

Cust1# ping 10.0.0.254

Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.0.0.254, timeout is 2 seconds: !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

Вопросы на закрепление

Почему интернет-провайдеры, использующие технологию DSL, главным образом используют протокол PPPoE?

_____

_____

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	Последовательный интерфейс № 1	Последовательный интерфейс № 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet	Gigabit Ethernet	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

	0/0 (G0/0)	0/1 (G0/1)		
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует.

В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Практическая работа 12

Тема: Настройка туннеля VPN GRE по схеме «точка-точка»

Цели: Произвести настройку туннеля VPN GRE по схеме «точка-точка»

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задачи

Часть 1. Базовая настройка устройств

Часть 2. Настройка туннеля GRE

Часть 3. Включение маршрутизации через туннель GRE

Исходные данные/сценарий

Универсальная инкапсуляция при маршрутизации (GRE) — это протокол туннелирования, способный инкапсулировать различные протоколы сетевого уровня между двумя объектами по общедоступной сети, например, в Интернете.

GRE можно использовать с:

- подключением сети IPv6 по сетям IPv4
- пакетами групповой рассылки, например, OSPF, EIGRP и приложениями потоковой передачи данных

В этой лабораторной работе необходимо настроить незашифрованный туннель GRE VPN «точкаточка» и убедиться, что сетевой трафик использует туннель. Также будет нужно настроить протокол маршрутизации OSPF внутри туннеля GRE VPN. Туннель GRE существует между маршрутизаторами WEST и EAST в области 0 OSPF. Интернет-провайдер не знает о туннеле GRE. Для связи между маршрутизаторами WEST и EAST и интернет-провайдером применяются статические маршруты по умолчанию.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы Cisco Catalyst серии 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены и они не имеют загрузочных настроек. Если вы не уверены в этом, обратитесь к инструктору.

Топология

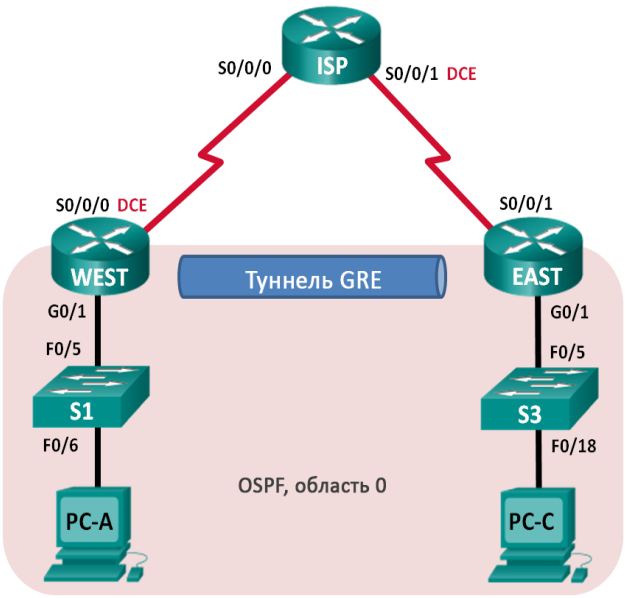


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
WEST	G0/1	172.16.1.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Недоступно
	Tunnel0	172.16.12.1	255.255.255.252	Недоступно
ISP	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Недоступно
EAST	G0/1	172.16.2.1	255.255.255.0	Недоступно
	S0/0/1	10.2.2.1	255.255.255.252	Недоступно
	Tunnel0	172.16.12.2	255.255.255.252	Недоступно
PC-A	NIC	172.16.1.3	255.255.255.0	172.16.1.1
PC-C	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Базовая настройка устройств

В части 1 вам предстоит настроить топологию сети и базовые параметры маршрутизатора, например, IP-адреса интерфейсов, маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

a. Отключите поиск DNS.

b. Назначьте имена устройств.

c. Зашифруйте незашифрованные пароли.

d. Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.

e.

f. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

g. Назначьте cisco в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.

h. Настройте ведение журнала состояния консоли на синхронный режим.

i. Примените IP-адреса к интерфейсам Serial и Gigabit Ethernet в соответствии с таблицей адресации и активируйте физические интерфейсы. На данном этапе не настраивайте интерфейсы Tunnel0.

j. Настройте тактовую частоту на **128000** для всех последовательных интерфейсов DCE.

Шаг 4: Настройте маршруты по умолчанию к маршрутизатору интернет-провайдера.

WEST(config)# **ip route 0.0.0.0 0.0.0.0 10.1.1.2**

EAST(config)# **ip route 0.0.0.0 0.0.0.0 10.2.2.2**

Шаг 5: Настройте компьютеры.

Настройте IP-адреса и шлюзы по умолчанию на всех ПК в соответствии с таблицей адресации.

Шаг 6: Проверьте соединение.

На данный момент компьютеры не могут отправлять друг другу эхо-запросы. Каждый ПК должен получать ответ на эхо-запрос от своего шлюза по умолчанию. Маршрутизаторы могут отправлять эхозапросы на последовательные интерфейсы других маршрутизаторов в топологии. Если это не так, устраните неполадки и убедитесь в наличии связи.

Шаг 7: Сохраните текущую конфигурацию.

Часть 2: Настройка туннеля GRE

В части 2 необходимо настроить туннель GRE между маршрутизаторами WEST и EAST.

Шаг 1: Настройка интерфейса туннеля GRE.

a. Настройте интерфейс туннеля на маршрутизаторе WEST. Используйте S0/0/0 на маршрутизаторе WEST в качестве интерфейс источника туннеля и 10.2.2.1 как назначение туннеля на маршрутизаторе EAST.

WEST(config)# **interface tunnel 0**

WEST(config-if)# **ip address 172.16.12.1 255.255.255.252**

WEST(config-if)# **tunnel source s0/0/0** WEST(config-if)# **tunnel destination 10.2.2.1**

b. Настройте интерфейс туннеля на маршрутизаторе EAST. Используйте S0/0/1 на маршрутизаторе EAST в качестве интерфейс источника туннеля и 10.1.1.1 как назначение туннеля на маршрутизаторе WEST.

EAST(config)# **interface tunnel 0**

EAST(config-if)# **ip address 172.16.12.2 255.255.255.252**

EAST(config-if)# **tunnel source 10.2.2.1**

EAST(config-if)# **tunnel destination 10.1.1.1**

Примечание. Для команды **tunnel source** в качестве источника можно использовать имя интерфейса или IP-адрес.

Шаг 2: Убедитесь, что туннель GRE работает.

a. Проверьте состояние интерфейса туннеля на маршрутизаторах WEST и EAST.

WEST# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Embedded-Service-Engine0/0 unassigned YES unset administratively down down

GigabitEthernet0/0 unassigned YES unset administratively down down

GigabitEthernet0/1 172.16.1.1 YES manual up up

Serial0/0/0 10.1.1.1 YES manual up up

Serial0/0/1 unassigned YES unset administratively down down Tunnel0 172.16.12.1 YES manual up up

EAST# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Embedded-Service-Engine0/0 unassigned YES unset administratively down down

GigabitEthernet0/0 unassigned YES unset administratively down down

GigabitEthernet0/1 172.16.2.1 YES manual up up

Serial0/0/0 unassigned YES unset administratively down down

Serial0/0/1 10.2.2.1 YES manual up up

Tunnel0 172.16.12.2 YES manual up up

b. С помощью команды **show interfaces tunnel 0** проверьте протокол туннелирования, источник туннеля и назначение туннеля, используемые в этом туннеле.

Какой протокол туннелирования используется? Какие IP-адреса источника и назначения туннеля связаны с туннелем GRE на каждом маршрутизаторе?

_____

c. Отправьте эхо-запрос по туннелю из маршрутизатора WEST на маршрутизатор EAST с использованием IP-адреса интерфейса туннеля.

WEST# **ping 172.16.12.2**

Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.12.2, timeout is 2 seconds: !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/36 ms

d. С помощью команды **traceroute** на маршрутизаторе WEST определите тракт к интерфейсу туннеля на маршрутизаторе EAST. Укажите путь до маршрутизатора EAST.

_____

e. Отправьте эхо-запрос и сделайте трассировку маршрута через туннель от маршрутизатора EAST к маршрутизатору WEST с использованием IP-адреса интерфейса туннеля.

Укажите путь от маршрутизатора EAST до маршрутизатора WEST?

_____

_____

С какими интерфейсами связаны эти IP-адреса? Почему?

_____

f. Команды **ping** и **traceroute** должны успешно выполняться. Если это не так, устраните неполадки и перейдите к следующей части.

Часть 3: Включение маршрутизации через туннель GRE

В части 3 необходимо настроить протокол маршрутизации OSPF таким образом, чтобы локальные сети (LAN) на маршрутизаторах WEST и EAST могли обмениваться данными с помощью туннеля GRE.

После установления туннеля GRE можно реализовать протокол маршрутизации. Для туннелирования GRE команда network будет включать сеть IP туннеля, а не сеть, связанную с последовательным интерфейсом. точно так же, как и с другими интерфейсами, например, Serial и Ethernet. Следует помнить, что маршрутизатор ISP в этом процессе маршрутизации не участвует.

Шаг 1: Настройка маршрутизации по протоколу OSPF для области 0 по туннелю.

a. Настройте идентификатор процесса OSPF 1, используя область 0 на маршрутизаторе WEST для сетей 172.16.1.0/24 и 172.16.12.0/24.

WEST(config)# **router ospf 1**

WEST(config-router)# **network 172.16.1.0 0.0.0.255 area 0**

WEST(config-router)# **network 172.16.12.0 0.0.0.3 area 0**

b. Настройте идентификатор процесса OSPF 1, используя область 0 на маршрутизаторе EAST для сетей 172.16.2.0/24 и 172.16.12.0/24.

EAST(config)# **router ospf 1**

EAST(config-router)# **network 172.16.2.0 0.0.0.255 area 0** EAST(config-router)# **network 172.16.12.0 0.0.0.3 area 0**

Шаг 2: Проверка маршрутизации OSPF.

a. Отправьте с маршрутизатора WEST команду **show ip route** для проверки маршрута к локальной сети 172.16.2.0/24 на маршрутизаторе EAST.

WEST# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP + - replicated route, % - next hop override

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 10.1.1.2

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 10.1.1.0/30 is directly connected, Serial0/0/0

L 10.1.1.1/32 is directly connected, Serial0/0/0

172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks

C 172.16.1.0/24 is directly connected, GigabitEthernet0/1

L 172.16.1.1/32 is directly connected, GigabitEthernet0/1

O 172.16.2.0/24 [110/1001] via 172.16.12.2, 00:00:07, Tunnel0

C 172.16.12.0/30 is directly connected, Tunnel0

L 172.16.12.1/32 is directly connected, Tunnel0

Какой выходной интерфейс и IP-адрес используются для связи с сетью 172.16.2.0/24?

_____

b. Отправьте с маршрутизатора EAST команду для проверки маршрута к локальной сети 172.16.1.0/24 на маршрутизаторе WEST.

Какой выходной интерфейс и IP-адрес используются для связи с сетью 172.16.1.0/24?

_____

Шаг 3: Проверьте связь между конечными устройствами.

a. Отправьте эхо-запрос с ПК A на ПК C. Эхо-запрос должен пройти успешно. Если это не так, устраните неполадки и убедитесь в наличии связи между конечными узлами.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение межсетевого экрана.

b. Запустите трассировку от ПК A к ПК C. Каков путь от ПК A до ПК C?

_____

_____

Вопросы на закрепление

1. Какие еще настройки необходимы для создания защищенного туннеля GRE?

_____

2. Если вы добавили дополнительные локальные сети к маршрутизатору WEST или EAST, то что нужно сделать, чтобы сеть использовала туннель GRE для трафика?

_____

_____

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet № 1**	**Интерфейс Ethernet № 2**	**Последовательный интерфейс № 1**	**Последовательный интерфейс № 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует.

В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Практическая работа 13

Тема: Разработка технического обслуживания сети

Цели работы: Разработать техническое обслуживание сети

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задачи

Опишите различные уровни сообщений в журнале маршрутизатора.

Сценарий

В настоящее время официальные политики и процедуры для регистрации проблем, возникших в сети компании, отсутствуют. Кроме того, при возникновении проблем с сетью приходится применять различные методы для установления причины – и этот способ поиска и устранения неисправностей занимает много времени.

Вам известно, что существует лучший способ решения подобных проблем. Вы решаете создать план технического обслуживания сети, чтобы сохранить записи о ремонте и определить причины ошибок в сети.

Ресурсы:

- программа редактирования текстов.

Указания:

Шаг 1: Обсудите в группе различные типы записей технического обслуживания сети, которые вы хотели бы регистрировать.

Шаг 2: Разделите типы записей на несколько основных категорий. Это могут быть следующие категории:

- Оборудование (маршрутизаторы и коммутаторы)
- Трафик
- Безопасность

Шаг 3: Создайте краткое руководство по процессу планирования технического обслуживания сети для компании.

Практическая работа 14

Тема: Настройка Syslog и NTP

Цели работы: Произвести настройку Syslog и NTP

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задачи

Часть 1. Базовая настройка устройств

Часть 2. Настройка NTP

Часть 3. Настройка Syslog

Исходные данные/сценарий

Сообщения Syslog, создаваемые сетевыми устройствами, могут собираться и архивироваться на сервере Syslog. Эту информацию можно использовать для наблюдения, отладки и поиска и устранения неполадок. Администратор может настраивать место сохранения и отображения сообщений. Сообщения Syslog могут сопровождаться метками времени для анализа последовательности сетевых событий; поэтому важно синхронизировать часы всех сетевых устройств с помощью сервера NTP.

В этой лабораторной работе необходимо настроить маршрутизатор R1 в качестве сервера NTP, а маршрутизатор R2 в качестве клиента Syslog и NTP. Приложение сервера Syslog, например Tftp32d или другая аналогичная программа, будет выполняться на ПК B. Кроме того, необходимо настроить уровень важности сообщений журнала, которые будут собираются и архивироваться на сервере Syslog.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не содержат файла загрузочной конфигурации. Если вы не уверены в этом, обратитесь к инструктору.

Топология

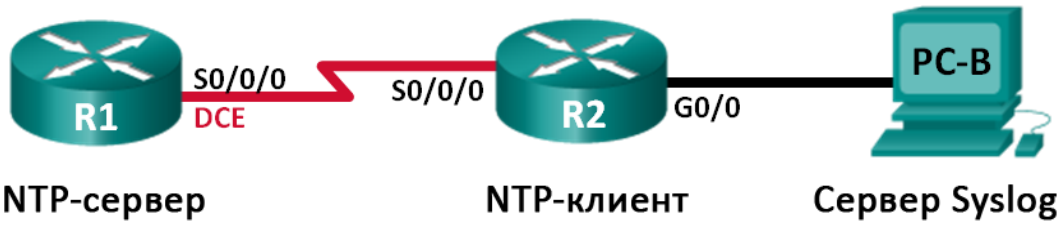


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Недоступно
R2	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
	G0/0	172.16.2.1	255.255.255.0	Недоступно
PC-B	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Необходимые ресурсы:

- 2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 1 компьютер (с ОС Windows 7, Vista или XP или с программой эмуляции терминала, например Tera Term, и ПО Syslog, например tftpd32);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Базовая настройка устройств

В части 1 необходимо настроить топологию сети и базовые параметры, например IP-адреса интерфейса, маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните запуск и перезагрузку маршрутизаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

a. Отключите поиск DNS.

b. Настройте имя устройства.

c. Зашифруйте незашифрованные пароли.

d. Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.

e. Назначьте class в качестве зашифрованного пароля доступа к привилегированному режиму.

f. Назначьте cisco в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.

g. Настройте ведение журнала состояния консоли на синхронный режим.

h. Примените IP-адреса к интерфейсам Serial и Gigabit Ethernet в соответствии с таблицей адресации и включите физические интерфейсы.

i. Установите тактовую частоту 128000 для последовательного интерфейса DCE.

Шаг 4: Настройте маршрутизацию.

Включите на маршрутизаторах протокол OSPF с одной областью с идентификатором процесса 1. Добавьте все сети в процесс OSPF для области 0.

Шаг 5: Настройте ПК B.

Настройте IP-адрес и шлюз по умолчанию для ПК B согласно таблице адресации.

Шаг 6: Проверьте связь между конечными устройствами.

Убедитесь, что все устройства могут отправлять эхо-запросы на каждое другое устройство в сети. Если нет, устраните неполадки, чтобы установить связь между конечными устройствами.

Шаг 7: Сохраните текущую конфигурацию в загрузочную.

Часть 2: Настройка NTP

В части 2 необходимо настроить маршрутизатор R1 в качестве сервера NTP, а маршрутизатор R2 в качестве клиента NTP маршрутизатора R1. Необходимо выполнить синхронизацию времени для Syslog и отладочных функций. Если время не синхронизировано, сложно определить, какое сетевое событие стало причиной данного сообщения.

Шаг 1: Выведите на экран текущее время.

Введите команду show clock для отображения текущего времени на R1.

R1# show clock

*12:30:06.147 UTC Tue May 14 2013

Запишите отображаемые сведения о текущем времени в следующей таблице.

Дата	
Время	
Часовой пояс	

Шаг 2: Установите время.

С помощью команды clock set установите время на маршрутизаторе R1. Ниже приводится пример настройки даты и времени.

R1# clock set 9:39:00 05 july 2013

R1#

*Jul 5 09:39:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 12:30:54

UTC Tue May 14 2013 to 09:39:00 UTC Fri Jul 5 2013, configured from console by console.

Примечание. Время можно также настроить с помощью команды clock timezone в режиме глобальной конфигурации. Для получения дополнительной информации о команде clock timezone посетите веб-сайт www.cisco.com и определите часовой пояс для вашего региона.

Шаг 3: Настройте главный сервер NTP.

Настройте маршрутизатор R1 в качестве главного сервера NTP с помощью команды ntp master *stratum-number* в режиме глобальной конфигурации. Значение stratum показывает в каком количестве переходов NTP от доверенного источника времени находится сервер. В этой лабораторной работе в качестве stratum данного сервера NTP используется число 5.

R1(config)# ntp master 5

Шаг 4: Настройте клиент NTP.

a. Введите команду show clock на маршрутизаторе R2. Запишите текущее время, отображаемое на маршрутизаторе R2, в следующей таблице.

Дата	
Время	
Часовой пояс	

b. Настройте R2 в качестве клиента NTP. Используйте команду ntp server, чтобы указать на IP-адрес или имя компьютера сервера NTP. Команда ntp update-calendar периодически обновляет календарь на основе времени NTP.

R2(config)# ntp server 10.1.1.1

R2(config)# ntp update-calendar

Шаг 5: Проверьте настройку NTP.

a. Используйте команду show ntp associations, чтобы проверить, что маршрутизатор R2 связан через NTP с маршрутизатором R1.

R2# show ntp associations

address ref clock st when poll reach delay offset disp *~10.1.1.1 127.127.1.1 5 11 64 177 11.312 -0.018 4.298

* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

b. Введите команду show clock на маршрутизаторах R1 и R2 и сравните метку времени.

Примечание. Синхронизация метки времени на маршрутизаторе R2 с меткой времени на маршрутизаторе R1 может занять несколько минут.

R1# show clock

09:43:32.799 UTC Fri Jul 5 2013 R2# show clock

09:43:37.122 UTC Fri Jul 5 2013

Часть 3: Настройте Syslog

Сообщения Syslog от сетевых устройств могут собираться и архивироваться на сервере Syslog. В этой лабораторной работе в качестве программного обеспечения сервера Syslog используется Tftpd32.

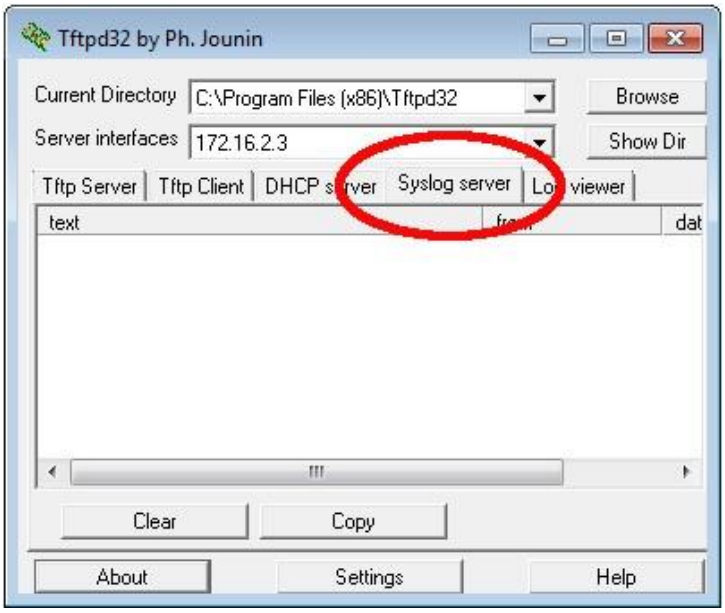
Администратор может настраивать типы сообщений, которые можно отправлять на сервер Syslog.

Шаг 1: (Дополнительно) Установите сервер Syslog.

Если сервер Syslog еще не установлен на компьютере, загрузите и установите последнюю версию сервера Syslog, например Tftpd32. Последнюю версию Tftpd32 можно найти по следующей ссылке: http://tftpd32.jounin.net/

Шаг 2: Запустите сервер Syslog на компьютере ПК B.

После запуска приложения Tftpd32 перейдите на вкладку Syslog server.



Шаг 3: Убедитесь, что на маршрутизаторе R2 включена служба меток времени.

С помощью команды show run проверьте, что служба меток времени включена для журналирования на маршрутизаторе R2.

R2# show run | include timestamp service timestamps debug datetime msec service timestamps log datetime msec

Если служба меток времени не включена, используйте следующую команду, чтобы включить её.

R2(config)# service timestamps log datetime msec

Шаг 4: Настройте R2 для сохранения сообщений журнала на сервере Syslog.

Настройте R2 для отправки сообщений Syslog на сервер Syslog — ПК B. IP-адрес сервера Syslog ПК B — 172.16.2.3.

R2(config)# logging host 172.16.2.3

Шаг 5: Выведите на экран параметры по умолчанию для журналирования.

Используйте команду show logging, чтобы вывести на экран параметры журналирования по умолчанию.

R2# show logging

Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled) No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 47 messages logged, xml disabled, filtering disabled Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled Buffer logging: level debugging, 47 messages logged, xml disabled, filtering disabled Exception Logging: size (4096 bytes)

Count and timestamp logging messages: disabled

Persistent logging: disabled

No active filter modules.

Trap logging: level informational, 49 message lines logged Logging to 172.16.2.3 (udp port 514, audit disabled, link up), 6 message lines logged,

0 message lines rate-limited, 0 message lines dropped-by-MD, xml disabled, sequence number disabled filtering disabled Logging Source-Interface: VRF Name:

Назовите IP-адрес сервера Syslog. _____

Какие протокол и порт использует сервер Syslog? _____

Какой уровень сообщений настроен? _____

Шаг 6: Настройте и проверьте результат настройки уровней важности для журналирования на маршрутизаторе R2.

a. Используйте команду logging trap ? для определения доступности различных уровней ловушек. При настройке уровня сообщений, отправляемые на сервер Syslog, будут включать сообщения настроенного уровня и сообщение более низких уровней.

R2(config)# logging trap ?

<0-7> Logging severity level alerts Immediate action needed (severity=1) critical Critical conditions (severity=2) debugging Debugging messages (severity=7) emergencies System is unusable (severity=0) errors Error conditions (severity=3) informational Informational messages (severity=6) notifications Normal but significant conditions (severity=5) warnings Warning conditions (severity=4) <cr>

Если введена команда logging trap warnings, сообщения с какими уровнями важности будут регистрироваться?

_____

_____

b. Укажите уровень важности для журналирования равный 4.

R2(config)# logging trap warnings или

R2(config)# logging trap 4

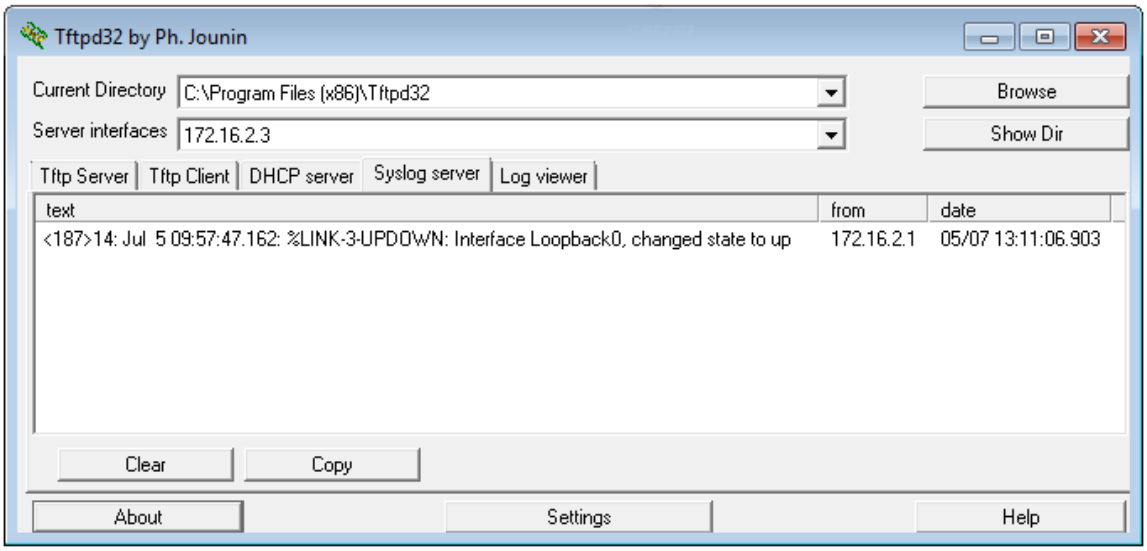
c. Создайте интерфейс Loopback0 на маршрутизаторе R2 и просмотрите сообщения журнала как в окне терминала, так и в окне сервера Syslog на ПК B.

R2(config)# interface lo 0

R2(config-if)#

Jul 5 09:57:47.162: %LINK-3-UPDOWN: Interface Loopback0, changed state to up

Jul 5 09:57:48.162: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up



d. Удалите интерфейс Loopback 0 на маршрутизаторе R2 и просмотрите сообщения журнала.

R2(config-if)# no interface lo 0

R2(config)#

Jul 5 10:02:58.910: %LINK-5-CHANGED: Interface Loopback0, changed state to administratively down

Jul 5 10:02:59.910: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to down

Отображаются ли какие-либо сообщения на сервере Syslog при выборе уровня серьёзности 4? Если какие-либо сообщения журнала отображаются, объясните, какие сообщения отображаются и почему.

_____

_____

e. Укажите уровень важности для журналирования равный 6.

R2(config)# logging trap informational или

R2(config)# logging trap 6

f. Удалите записи Syslog на ПК B. Нажмите кнопку Clear (Очистить) в диалоговом окне Tftpd32.

g. Создайте интерфейс Loopback 1 на маршрутизаторе R2.

R2(config)# interface lo 1

Jul 5 10:05:46.650: %LINK-3-UPDOWN: Interface Loopback1, changed state to up

Jul 5 10:05:47.650: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

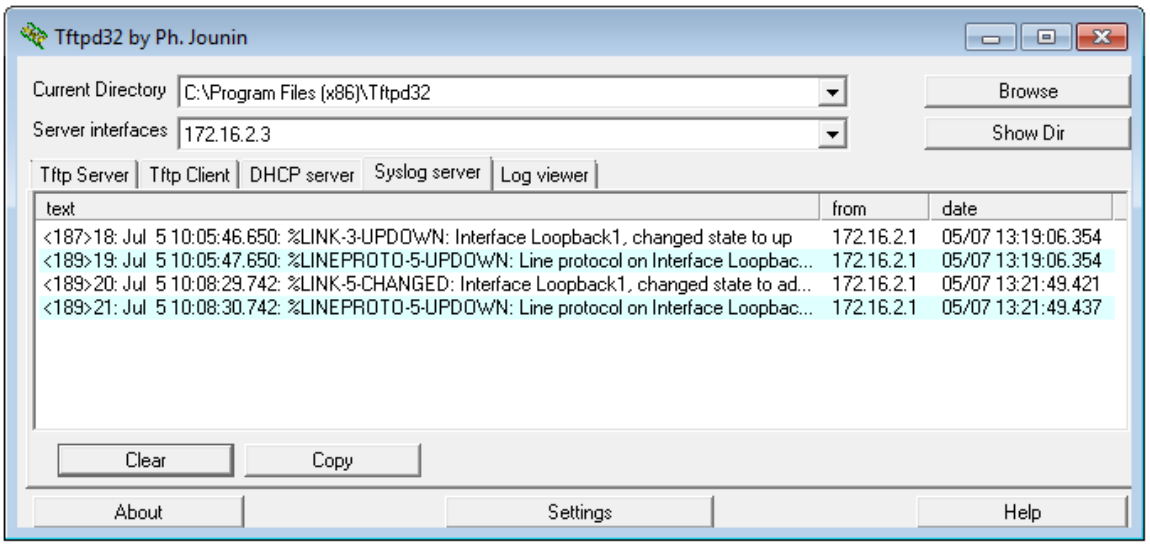
h. Удалите интерфейс Loopback 1 с маршрутизатора R2.

R2(config-if)# no interface lo 1

R2(config-if)#

Jul 5 10:08:29.742: %LINK-5-CHANGED: Interface Loopback1, changed state to administratively down

Jul 5 10:08:30.742: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to down



i. Проанализируйте выходные данные сервера Syslog. Сравните эти результаты с результатами на уровне важности 4. Каковы ваши наблюдения?

_____

_____

Вопросы на закрепление

Какая проблема возникает при настройке слишком высокого (самый маленький номер) или слишком низкого (самый большой номер) уровня важности для Syslog?

_____

_____

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	Последовательный интерфейс № 1	Последовательный интерфейс № 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует.

В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.

Практическая работа 15

Тема: Изучение программного обеспечения для мониторинга сети

Цели: Изучить программное обеспечение для мониторинга сети

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задачи

Часть 1. Проверка знаний по мониторингу сетей

Часть 2. Изучение инструментов мониторинга сетей

Часть 3. Выбор инструмента для мониторинга сетей

Общие сведения/сценарий

Мониторинг необходим для сетей любого размера. Профилактическое наблюдение за сетевой инфраструктурой поможет администраторам сети выполнять ежедневные обязанности. Существуют различные средства мониторинга сети, которые отличаются по стоимости в зависимости от возможностей, количества сетей и поддерживаемых узлов.

В этой лабораторной работе будет исследоваться доступное ПО для мониторинга сети. Вашей задачей будет сбор информации о программных продуктах и их функциях. Один продукт вы рассмотрите более подробно и перечислите некоторые из его основных функций.

Необходимые ресурсы

- ПК с доступом к Интернету.

Часть 1: Проверка знаний по мониторингу сетей

Опишите, в чем, по вашему мнению, заключается процесс мониторинга сети. Приведите пример его использования в сети организации.

_____

_____

Часть 2: Изучение инструментов мониторинга сети

Шаг 1: Проведите исследование и найдите три инструмента мониторинга сети.

Перечислите эти три найденных инструмента.

_____

_____

Шаг 2: Заполните следующую форму для выбранных инструментов мониторинга сети.

Поставщик	Название продукта	Особенности

Часть 3: Выберите средство мониторинга сети

Шаг 1: Выберите одно или несколько средств мониторинга из исследования.

Укажите одно или несколько средств из исследования, которые бы вы выбрали для мониторинга сети. Назовите эти средства и объясните свой выбор, перечислив конкретные функциональные возможности, которые, по вашему мнению, важны.

_____

_____

Шаг 2: Изучите средство мониторинга сети PRTG.

Перейдите на веб-страницу www.paessler.com/prtg.

В следующих полях приведите примеры некоторых функций PRTG.

_____

_____

Вопросы для повторения

Какие выводы вы можете сделать на основании проведенного исследования в отношении программного обеспечения для мониторинга сети?

_____

_____

МДК.01.02. Организация, принципы построения и функционирования компьютерных сетей

Раздел 2. Организация, прин ципы построения и функционирования компьютерных се тей

Тема 2.1. Маршрутизация и коммутация. Масштабирование сетей

Практическая работа 1

Тема: Определение топологии и протоколов для указанной сети. Поиск и устранение неполадок в работе СКС

Цели: изучить виды топологий компьютерных сетей

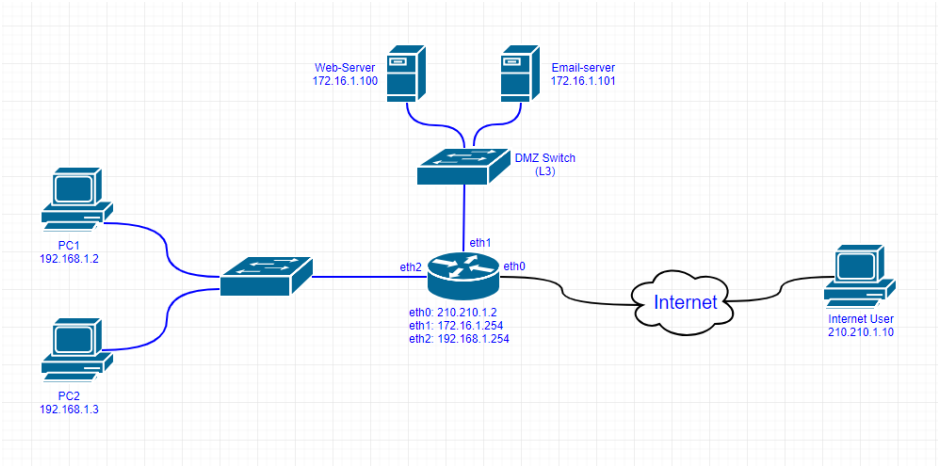
ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задание:

1. Изучить теоретический материал по определению топологии и протоколов для указанной сети
2. Можно ли определить топологию сети средствами OS Windows? Если можно,

то опишите эти средства.

3. Дать ответы на вопросы:
    1. Дайте определение топологии.
    2. Опишите физические топологии.
    3. Опишите логические топологии.
    4. Перечислите программные средства для определения топологии сети, опишите функции трех программных средств.
4. Определите недостатки указанной сети (рисунок 1). Дайте рекомендации по



устранению недостатков.

Рисунок 1 - Схема сети

5. Сделать выводы о проделанной работе.

Практическая работа 2

Тема: Настройка беспроводного маршрутизатора и клиента

Цели: научиться устанавливать беспроводное соединение и подключаться к беспроводной сети.

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задание:

Настройки маршрутизатора Linksys

Имя сети (SSID)	Сеть CCNA
Пароль сети	cisconet
Пароль маршрутизатора	cisco123

Исходные данные/сценарий

В наши дни доступ к сети Интернет из любого места, будь то дом или офис — широко распространенное явление. Без беспроводной связи пользователи были бы ограничены

возможностью подключения только при наличии проводного соединения. Пользователи по достоинству оценили гибкость и возможности, которые предоставляют беспроводные маршрутизаторы в рамках доступа к сети и Интернету.

В этой лабораторной работе вам предстоит настроить маршрутизатор Linksys Smart Wi-

Fi, применить настройки безопасности WPA2 и активировать службы DHCP. Вы

рассмотрите некоторые дополнительные функции, доступные на этих маршрутизаторах, например, USB-накопители, родительский контроль и ограничения по времени. Вам

также предстоит настроить беспроводной клиент для компьютера.

Необходимые ресурсы:

- 1 маршрутизатор Linksys EA Series (EA4500 с версией микропрограммного обеспечения

  2.1.39.145204 или сопоставимой версией);
- 1 кабельный или DSL-модем (необязательно; требуется для работы интернет-службы и обычно предоставляется интернет-провайдером);
- 1 компьютер с беспроводным сетевым адаптером (ОС Windows 7, Vista или XP);
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Настройка основных параметров маршрутизатора Linksys EA Series

Самым эффективным способом настройки основных параметров маршрутизатора EA Series является запуск установочного компакт-диска Linksys EA Series, поставляемого в комплекте с маршрутизатором. Если установочный компакт-диск отсутствует, следует загрузить программу установки с веб-сайта http://Linksys.com/support.

Шаг 1: Вставьте установочный компакт-диск Linksys EA-Series в компьютер.

Когда отобразится соответствующий запрос, выберите **Set up your Linksys Router (Настройка маршрутизатора Linksys)**. Вам будет предложено ознакомиться с

условиями лицензии на использование программного обеспечения и принять их. После того, как вы примете условия лицензии нажмите **Next > (Далее >)**.

Шаг 2: Подключите кабели в сети в соответствии с топологией.

Следуйте инструкциям по подключению кабеля питания и кабельного модема или DSL-модема с помощью Ethernet-кабеля, которые отобразятся

в следующем окне. Можно подключить компьютер к одному из четырех неиспользуемых Ethernet-портов на задней стенке маршрутизатора. После подключения всех необходимых элементов нажмите **Next > (Далее >)**.

Шаг 3: Настройте параметры маршрутизатора Linksys.

a. Дождитесь, когда отобразится окно **Linksys router settings**

(Настройки маршрутизатора Linksys). Для заполнения полей в этом окне используйте данные таблицы **Linksys router settings (Настройки маршрутизатора Linksys)**, приведённой в начале лабораторной работы.

Нажмите **Next (Далее)**, чтобы отобразить экран со сводной информацией о настройках маршрутизатора.

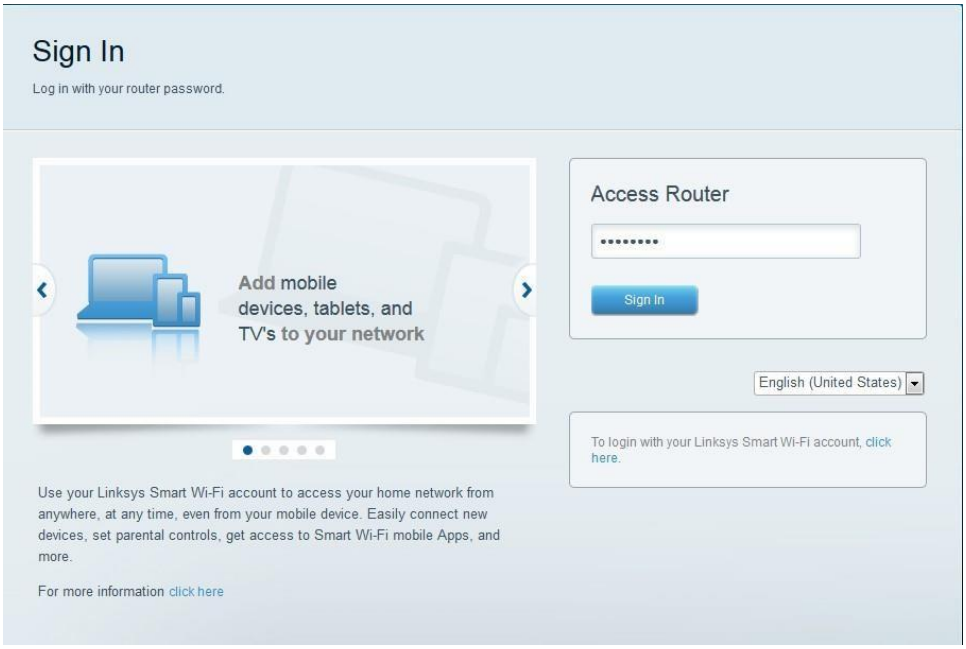
Нажмите **Next (Далее)**.

b. Отобразится окно **Create your Linksys Smart Wi-Fi account (Создание учетной записи Linksys Smart Wi-Fi)**. Учетная запись Linksys Smart Wi-Fi используется для ассоциации маршрутизатора к учетной записи, что позволяет удалённо управлять маршрутизатором с помощью браузера или мобильного устройства, на котором запущено приложение Smart Wi-Fi. В рамках этой лабораторной работы пропустите процесс настройки учетной записи. Щелкните поле **No, thanks (Нет, спасибо)** и нажмите **Continue**

(Продолжить).

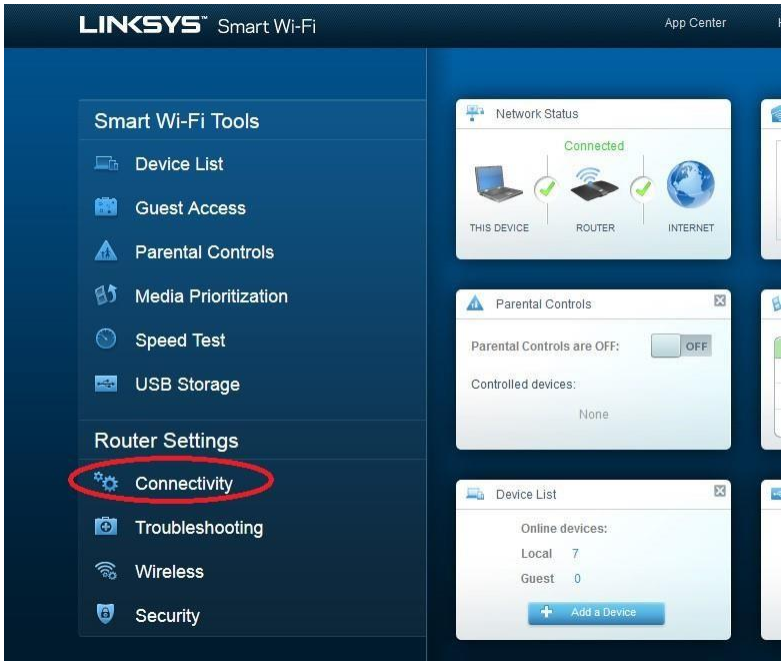
Примечание. Чтобы настроить учетную запись, перейдите на веб-сайт www.linksyssmartwifi.com.

c. Отобразится окно **Sign in (Вход в систему)**. В поле **Access Router (Доступ к маршрутизатору)** введите **cisco123** и нажмите **Sign in (Войти)**.



d. На домашней странице Linksys Smart Wi-Fi нажмите **Connectivity (Соединение)**

чтобы просмотреть и изменить основные настройки маршрутизатора.

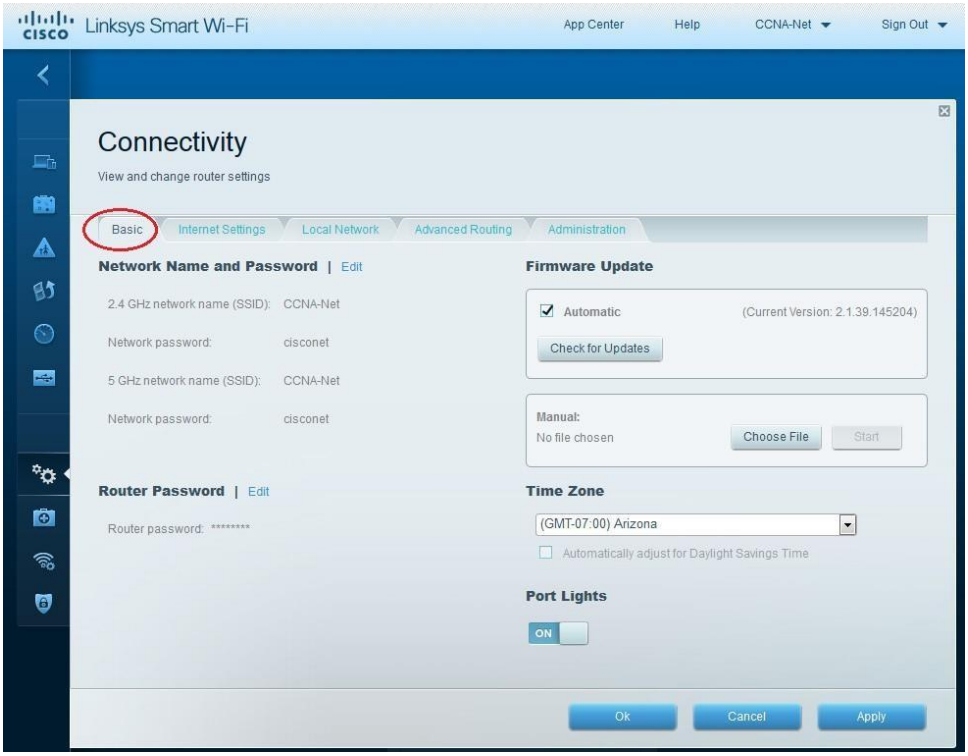


e. На вкладке **Basic (Основные настройки)** можно изменить имя и пароль сети, изменить пароль

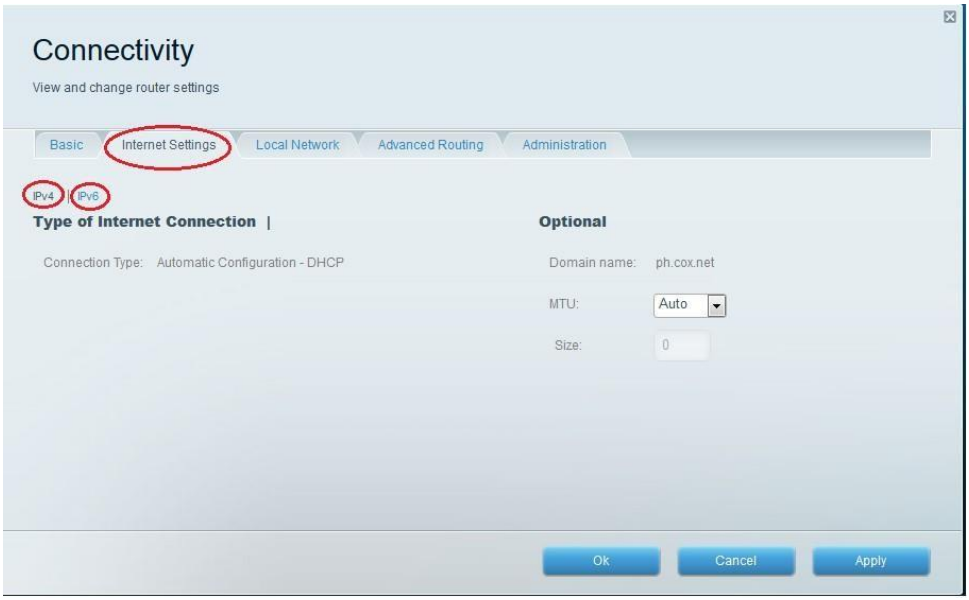
маршрутизатора, выполнить обновление микропрограммного

обеспечения и задать часовой пояс для маршрутизатора. Пароль маршрутизатора и данные о сети настроены в шаге 3a. В раскрывающемся списке выберите

соответствующий часовой пояс для маршрутизатора и нажмите **Apply (Применить)**.



f. На вкладке **Internet Settings (Настройки Интернета)** отображены сведения об интернетподключении. В этом примере маршрутизатор автоматически настраивает подключение для DHCP. На этом экране можно отобразить сведения как об IPv4, так и об IPv6.



g. На вкладке **Local Network (Локальная сеть)** доступны параметры настройки локального DHCPсервера. В настройках локальной сети по умолчанию задана сеть 192.168.1.0/24 и локальный IPадрес маршрутизатора по умолчанию 192.168.1.1. Эти настройки можно изменить, нажав **Edit (Изменить)** рядом с разделом **Router Details (Сведения о маршрутизаторе)**. На этом экране можно изменить настройки DHCP- сервера. Можно задать начальный адрес DHCP, максимальное число пользователей DHCP, срок аренды клиента и статические DNS-серверы. Нажмите **Apply (Применить)**, чтобы принять все изменения, внесённые на этом экране.

Примечание. Если DHCP используется для получения данных о подключении к сети интернетпровайдера, эти DNS-адреса, наиболее вероятно, будут заполняться данными DNS- сервера интернет-провайдера.

Практическая работа 3

Тема: Работа с технической документацией проекта сети. Выбор оборудования для проекта сети

Цели: изучение аппаратных и программных средств для построения локальной сети.

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задание:

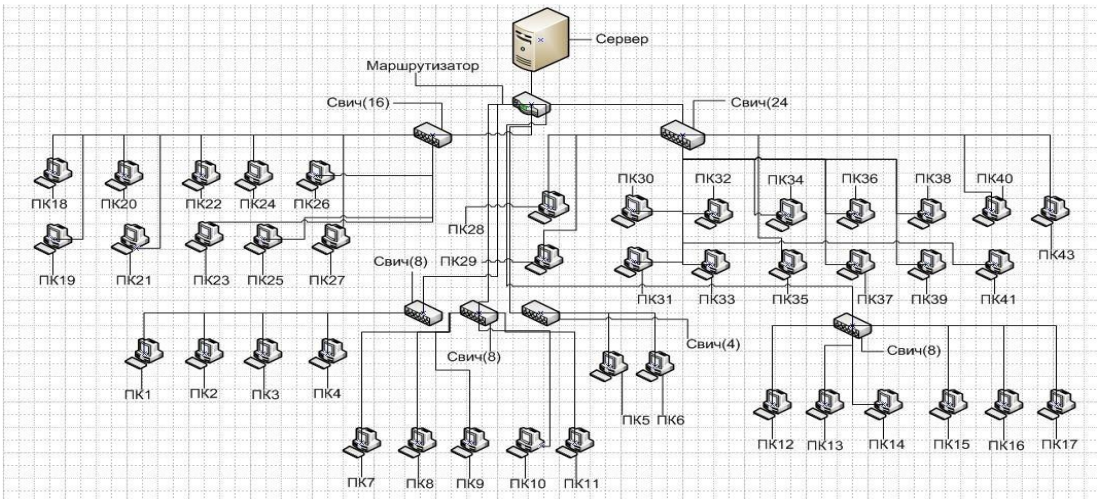
1. Изучить состав технической документации сети.
2. Дать краткие ответы на вопросы:
   - По каким ГОСТам составляется техническая документация сети?
   - Какие документы входят в технический проект сети?
   - Чем структурно-функциональная схема сети отличается от плана кабельной структуры сети?
   - Какие спецификации входят в состав проекта?
   - Какой процент от стоимости сети отводится на монтаж и настройку сети?
3. Выполнить проект сети из разрозненных документов, находящихся в папке дисциплины ОППиФКС на диске Z. Не забудьте скопировать все документы в свою рабочую папку.
4. Дан план офиса. Необходимо спроектировать план компьютерной сети. Исходными данными для этого является: количество комнат на этаже офисного помещения, рабочие места пользователей компьютерной сети и распределение рабочих мест в офисном помещении.

№ комнаты	Кол-во рабочих мест
1	7
2	6
3	9
4	1
5	5
6	2
7	1

5. На основе исходных данных необходимо спроектировать план одного этажа офисного здания, учитывая, что одна из комнат офисного здания должна являться серверной комнатой с один рабочим местом для администратора сети. Также необходимо учесть все требования относительно расположения серверной комнаты (двери, окна и т.д.).
6. При проектировании сети необходимо определить рабочие места для персонала, оснащенные офисной мебелью и персональными компьютерами. Также необходимо определить месторасположение для сетевого оборудования.
7. С помощью глобальной компьютерной сети подобрать сетевое оборудование для кабельной сети и составить спецификацию аппаратного обеспечения.
8. Разработать структурно-функциональную схему локальной вычислительной сети. На структурно-функциональной схеме необходимо указать все сетевое оборудование.

Структурно-функциональная схема локальной вычислительной сети выполняется в любой программе на формате А1.

Пример структурно-функциональной схемы сети



9. Сохранить схемы в свою рабочую папку.

Практическая работа 4

Тема: Проектирование подсистемы рабочего места. Расчет основных параметров локальной сети

Цели: расчет технических характеристик разрабатываемой сети, определение аппаратных и программных средств, расчет стоимости внедрения сети.

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задание:

1. Дан план офиса. Необходимо спроектировать подсистему рабочего места. Исходными данными для этого является практическая работа №6.
2. Необходимо на плане офиса указать рабочее место (компьютер, ноутбук),

1 штепсельную и 1 сетевую розетки. На всех планах указать имя компьютера (план с указанием рабочих мест, структурно-функциональная схема).

3. С помощью глобальной компьютерной сети подобрать сетевое оборудование для подсистемы рабочего места, указать его характеристики. Составить список необходимого ПО, указать системные требования для каждого вида ПО, стоимость лицензии.
4. Составить спецификацию для рабочего места (сетевое оборудование и программное обеспечение).

Таблица 1 - Конфигурация рабочей станции (пример)

Наименование	Тип	Цена,руб.
Материнская плата	AsusTek P3V133	2759.00
Процессор	Intel Pentium II – 400 512k MMX	2790.00
Память	64Mb (DIMM)	868.00
Видеокарта	SVGA 8Mb	961.00
HDD	10,2Gb Fujitsu MPF3102AT	3813.00
FDD	3.5”	341.00
CD-ROM	Asus 50-X	1441.50
Клавиатура	Turbo RUS, Win’95	127.10
Мышь	Genius Easy COM / PS/2	93.00
Монитор	Scott 570 15”	4557.00
Сетевая карта	NE-2000 Acorp UTP (10Base-T; 100Base-TX)	272.80
Итого:		18023.40

Таблица 2 – Спецификация программного обеспечения

Наименование	Описание	Стоимость лицензии	Кол-во	Цена,руб.

5. Сохранить схемы и спецификации в свою рабочую папку.
6. Составить кабельный журнал. На формате А4 заполнить кабельный журнал, в котором необходимо указать соответствие сетевого устройства, порта сетевого устройства, сетевой компьютерной розетки, номера комнаты и имя компьютера. Пример кабельного журнала представлен в табл. 3.

Таблица 3 - Пример кабельного журнала (в номере розетки первая цифра – номер комнаты, вторая цифра – номер сетевого устройства, третья цифра – номер компьютера)

№ п/п	Название устройства	№ порта	№ розетки	Имя компьютера	№ комнаты
1	КМ01	01	01-01-01	ПК01	01
		02	01-01-02	ПК02	
		03	01-01-03	ПК03	
2	КМ02	01	01-02-04	ПК04	
		02			
		03			

7. Описать спецификацию персональныхкомпьютеров,серверов, сетевого и периферийного оборудования, необходимого для развертывания

локальной вычислительной сети. Для каждого вида приобретаемого оборудования составить таблицу спецификации.

8. Сохранить журналы и спецификации в свою рабочую папку.

Практическая работа 5

Тема: Проектирование высокоскоростной локальной сети

Цели: Научиться проектировать локальные сети с учетом планировки помещения, количества необходимых рабочих мест и имеющегося оборудования.

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задание:

1. Дан план офиса. Имеются 2 схемы компьютерной сети (схема размещения рабочих мест, структурно-функциональная схема), спецификации и необходимые журналы. Разработать кабельную схему. Из разрозненных документов собрать технический проект кабельной локальной сети, оформить в соответствии с ГОСТами.
2. Сохранить все схемы, спецификации и проект в свою рабочую папку.
3. Заполнить отчет, показать преподавателю и защитить работу.

Содержание проекта

Графическая часть проекта сети включает в себя:

- План помещения, включающий в себя кабельную систему, проводку, формата А1, выполняется в программе Microsoft Visio либо чертится на ватмане по ГОСТ (1 лист на 1 этаж).
- План помещения, включающий в себя ПК, оргтехнику, сетевое оборудование, формата А1, выполняется в программе Microsoft Visio либо чертится на ватмане по ГОСТ (1 лист на 1 этаж).
- Условные обозначения (формат А4).
- Структурно-функциональная схема локальной вычислительной сети

1. ПЛАНИРОВАНИЕ РАЗМЕЩЕНИЯ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

1.1. План помещения (поэтажный) с указанием кабельной структуры

Поэтажный план помещения (структурная схема сети), включающий в себя кабельную систему, проводку, розетки выполняется в программе Microsoft Visio либо чертится на

ватмане по ГОСТ на формате А1 (1 лист на 1 этаж). На структурной схеме сети с учетом ее будущего размещения в помещении необходимо представить компоненты сети и их

соединения.

Условные обозначения на отдельном листе формата А4.

1.2. Перечень кабинетов на планах помещений На формате А4 в таблице указать № кабинета и его назначение.

Таблица 1 - Перечень кабинетов.

№ на плане	Назначение кабинета
1	
2	
...	

1.3. Структурно-функциональная схема локальной вычислительной сети

На структурно-функциональной схеме необходимо указать название рабочей группы и имена ПК из состава сети, адресацию сетевого уровня, тип адресации (статическое

распределение или динамическое) и прочие настройки. Структурно-функциональная схема локальной вычислительной сети выполняется в любой программе на формате А1.

1.4. Описание размещения рабочих мест и оборудования

Поэтажный план помещения, включающий в себя ПК, оргтехнику, сетевое оборудование, формата А1, выполняется в программе Microsoft Visio либо чертится на

ватмане по ГОСТ (1 лист на 1 этаж). Условные обозначения на отдельном листе формата А4.

1.5. Кабельный журнал

На формате А4 заполнить кабельный журнал, в котором необходимо указать соответствие сетевого устройства, порта сетевого устройства, сетевой компьютерной розетки, номера комнаты и имя компьютера. Пример кабельного журнала представлен в табл. 2.

Таблица 2 - Пример кабельного журнала

№ п/п	**Название устройства**	**№ порта**	**№ розетки**	**Имя компьютера**	**№ комнаты**
1	КМ01	01	01-01-К1	01-01-01	01
		02	01-01-К2	01-01-02	
		03	01-01-К3	01-01-03	
2	КМ02	01	01-01-Т1	01-01-01	
		02	01-01-Т2	01-01-02	
		03	01-01-Т3	01-01-03	
3	КМ03	01	01-02-К4	01-02-04	02
		02	01-02-К5	01-02-05	
		03	01-02-К6	01-02-06	
		04	01-02-К7	01-02-07	
			01-05-Т36		
		07	01-08-Т35	01-08-35	

2. РАСЧЕТ СТОИМОСТИ РАЗВЕРТЫВАНИЯ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

2.1. Спецификация аппаратного и программного обеспечения

Разработать спецификацию персональных компьютеров, серверов, сетевого и периферийного оборудования, необходимого для развертывания локальной вычислительной сети.

Для рабочих станций и сервера разработать конфигурацию.

Таблица 5 - Конфигурация рабочей станции

Наименование	Тип	Цена,руб.
Материнская плата	AsusTek P3V133	2759.00
Процессор	Intel Pentium II – 400 512k MMX	2790.00
Память	64Mb (DIMM)	868.00
Видеокарта	SVGA 8Mb	961.00
HDD	10,2Gb Fujitsu MPF3102AT	3813.00
FDD	3.5”	341.00
CD-ROM	Asus 50-X	1441.50
Клавиатура	Turbo RUS, Win’95	127.10
Мышь	Genius Easy COM / PS/2	93.00

Монитор	Scott 570 15”	4557.00
Сетевая карта	NE-2000 Acorp UTP (10Base-T; 100Base-TX)	272.80
Итого:		18023.40

Определение необходимого программного обеспечения производится исходя из перечня тех должностных обязанностей работника, для которых могут понадобиться какие- либо технические средства. Составить список необходимого ПО, указать системные

требования для каждого вида ПО, стоимость лицензии.

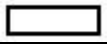
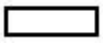
2.2. Расчет длины кабеля

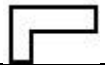
Рассчитать длину кабеля и кабелепровода для закупки и прокладки, данные о кабеле и его стоимости занести в таблицу. При покупке кабеля необходимо учесть, что необходимая длина кабеля составит на 5 % больше длины кабеля расчётной.

Таблица 3 - Пример спецификации кабельной системы

Наименование, тип	Кол-во	Цена за единицу, руб.	Стоимость, руб.
Кабель UTP, кат.5	120 м	8.37	1004.40
Патч-корд 0.5м RJ-45 UTP кат.5	7	46.50	325.50
Патч-корд 2м RJ-45 UTP кат.5	7	62.00	434.00
Патч-корд 1.5м RJ-45 UTP кат.5	1	55.80	55.80
Разъем RJ-45 кат.5	14	17.05	238.70
Патч-панель настенная, 12-порт. для UTP кат.5	1	1860.00	1860.00
Итого:			3918.40

Таблица 4 - Пример спецификации кабелепровода

Наименование	Условное обозначение	Условное изображение	Кол-во	Тип	Цена, руб.	Стоимость, руб.
Короб 30х20	К.1.1-К.1.11		8х2м	Односекционный	54.25	868.00
Короб 60х20	К.2.1, К.2.2		2х2м	Двухсекционный	65.10	260.00
Внешний угол	КЕ.1		1	Для короба 30х20	24.80	24.80

Плоский угол	KL.1		1	Для короба 30х20	24.80	24.80
Внутренний угол	KI.1-KI.2		2	Для короба 30х20	24.80	49.60
Соединитель коробов на стык	KS.1-KS.6		6	Для короба 30х20	9.30	55.80
Соединитель коробов на стык	K S.7		1	Для короба 60х20	10.85	10.85
Розетка RJ-45 кат.5	R1.1-R1.7		7		80.60	564.20
Заглушка	RZ.1, RZ.2		2	Для короба	9.3	18.60
Итого:						1876.65

2.3. Примерная стоимость развертывания локальной вычислительной сети Для оценки стоимости сведите в единую таблицу (табл. 6) стоимость всех

составляющих сети, рассчитайте общую стоимость и оцените возможность ее уменьшения. Если это возможно, вернитесь к предыдущим этапам разработки и внесите необходимые изменения.

Таблица 6 - Расчет стоимости проекта

Наименование	Обозначение, тип	Кол-во	Цена, руб.	Стоимость, руб.
Сервер	C1	1	24031.00	24031.00
Рабочая станция	PC1,..., PC6	6	18023.40	108140.40
Кабельная система		1		3918.40
Кабелепровод		1		1876.65
Коммутатор		1		14321.60
Модем		1		5321.10
Всего:				157609.15
Монтаж и наладка 30...40% от п. "Всего"				35% (55163.20)
Итого:				212772.35

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

В конце описания проекта указать 15 источников, включая книги, справочники, стандарты. Список литературы описать согласно ГОСТу.

Оформление пояснительной записки

Пояснительная записка может быть написана при помощи средств вычислительной техники на формате А4, обязательно используется рамка (см. пример титульного листа).

Текст пояснительной записки располагается на одной стороне листа.

При выполнении пояснительной записки в текстовом редакторе Microsoft Word рекомендуется шрифт Times New Roman размером 14, междустрочный интервал - полуторный.

Не допускается в пояснительной записке применять цветные шрифты, подчеркивание и т.п.

Каждый лист пояснительной записки должен иметь поля, указанные в приложении. Расстояние от рамки формата до границ текста следует оставлять в начале строк

менее 5 мм, в конце строк - не менее 3 мм.

Расстояние от верхней или нижней строки текста до верхней или нижней рамки формата должно быть не менее 10 мм.

Абзац в тексте - 1,25 см.

Практическая работа 6

Тема: Прокладка сетевого кабеля. Контроль соответствия проекта локальной сети нормативно-технической документации

Цели: аучиться проектированию локальных сетей в соответствии с поставленной задачей.

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задание:

1. Имеется проект сети. В нем недостает спецификации кабеля и кабелепровода, на схемах недостает сегментов кабеля.
2. Рассчитать длину кабеля и кабелепровода для закупки и прокладки, данные о кабеле и его стоимости занести в таблицу. При покупке кабеля необходимо учесть, что необходимая длина кабеля составит на 5 % больше длины кабеля расчётной.

3. С помощью глобальной сети найти стоимость 1 метра кабеля, стоимость кабелепровода, монтажа. Составить спецификацию.

Таблица 1 - Пример спецификации кабельной системы

Наименование, тип	Кол-во	Цена за единицу, руб.	Стоимость, руб.
Кабель UTP, кат.5	120 м	8.37	1004.40
Патч-корд 0.5м RJ-45 UTP кат.5	7	46.50	325.50
Патч-корд 2м RJ-45 UTP кат.5	7	62.00	434.00
Патч-корд 1.5м RJ-45 UTP кат.5	1	55.80	55.80
Разъем RJ-45 кат.5	14	17.05	238.70
Патч-панель настенная, 12-порт. для UTP кат.5	1	1860.00	1860.00
Итого:			3918.40

Таблица 2 - Пример спецификации кабелепровода

Наименование	Условное обозначение	Условное изображение	Кол-во	Тип	Цена, руб.	Стоимость, руб.
Короб 30х20	К.1.1-К.1.11		8х2м	Односекционный	54.25	868.00
Короб 60х20	К.2.1, К.2.2		2х2м	Двухсекционный	65.10	260.00
Внешний угол	КЕ.1		1	Для короба 30х20	24.80	24.80
Плоский угол	KL.1		1	Для короба 30х20	24.80	24.80
Внутренний угол	KI.1-KI.2		2	Для короба 30х20	24.80	49.60
Соединитель коробов на стык	KS.1-KS.6		6	Для короба 30х20	9.30	55.80
Соединитель коробов на стык	К S.7		1	Для короба 60х20	10.85	10.85
Розетка RJ-45 кат.5	R1.1-R1.7		7		80.60	564.20
Заглушка	RZ.1, RZ.2		2	Для короба	9.3	18.60
Итого:						1876.65

4. Выполнить расчет стоимости проекта и монтажа всей сети.
5. Сохранить схему, спецификации и расчеты в свою рабочую папку, заполнить отчет, показать преподавателю и защитить работу5.Имеющиеся схемы, спецификации, таблицы расчетов структурированной кабельной сети оформить в один файл проекта в соответствии с ГОСТами.
6. Сохранить проект в свою рабочую папку, заполнить отчет, показать

преподавателю и защитить работу.

Практическая работа 7

Тема: Настройка локальной сети

Цели: Изучить варианты организации локальных компьютерных сетей

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задание:

Изучить самостоятельно возможности ОС Windows 10 по настройке локальной сети (теоретический материал).

Письменно ответить на вопросы:

1. Какие параметры сетевых протоколов необходимы для настройки локальной сети?
2. Параметры какого протокола настраиваются?
3. Раскройте понятие DNS-сервер, WINS-сервер.

Самостоятельно составьте алгоритм настройки локальной сети и ОС Windows 7. Заполните отчет. Покажите результат работы преподавателю.

Настройка локальной сети в Windows 10

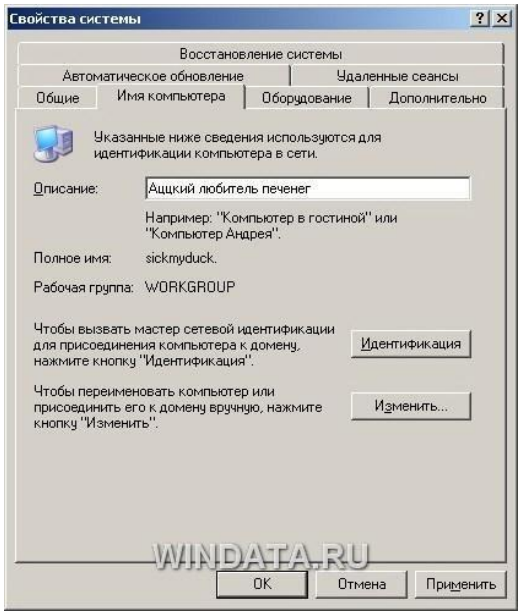
Если у вас дома два компьютера и более, пришло время заняться настройкой доступа к

локальной сети. К счастью, не нужно быть системным администратором, чтобы настроить все, как надо. В Windows 10 достаточно ввести лишь несколько параметров, и компьютер будет готов к работе. Посмотрим, как это можно сделать.

Первый этап настройки локальной сети не займет много времени. Щелкните правой кнопкой мыши на значке Мой компьютер и выберите команду Свойства. Перейдите на

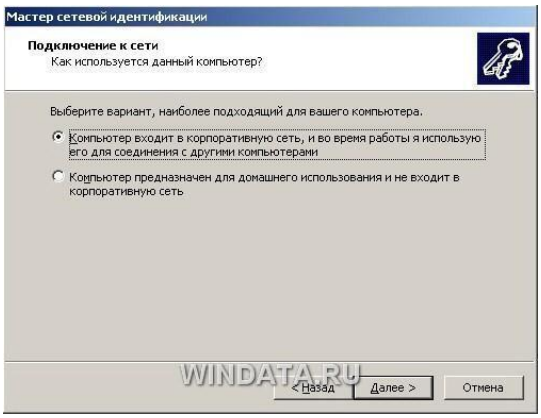
вкладку Имя компьютера и щелкните на кнопке Идентификация, чтобы запустить мастер сетевой

идентификации.



В первом окне мастера просто щелкните на кнопке Далее. В новом окне следует выбрать

вариант подключения к локальной сети. Если компьютер подключен к небольшой домашней сети, выберите переключатель Компьютер предназначен для домашнего использования и не входит в корпоративную сеть.

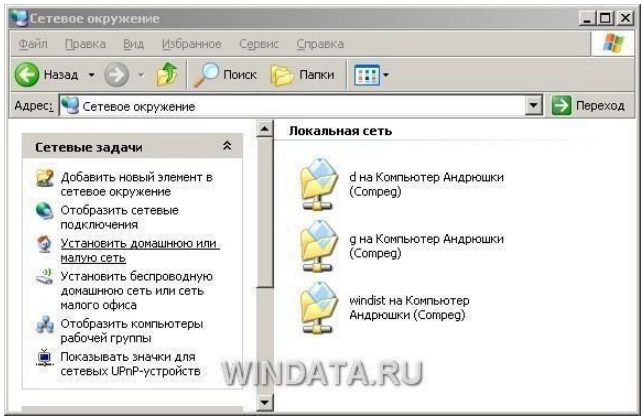


Щелкните на кнопке Далее. Осталось щелкнуть на кнопке Готово, и первый этап настройки локальной сети будет завершен.

После перезагрузки можно приступить ко второму этапу настройки локальной сети.

Выберите команду Пуск->Мой компьютер, после чего щелкните на ссылке Сетевое

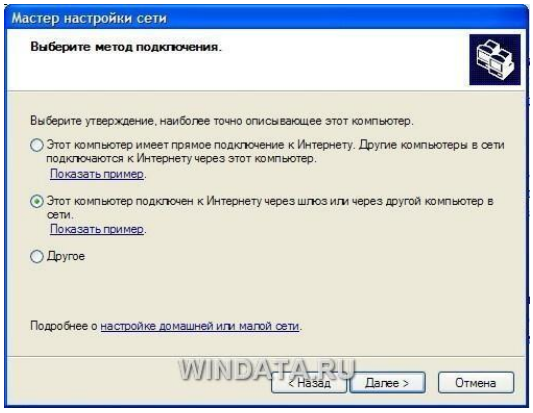
окружение, расположенной в левой панели. Теперь щелкните в поле Сетевые задачи на ссылке Установить домашнюю или малую сеть.



На экране появится окно мастера Настройка сети. Щелкните в первом окне на кнопке Далее. В следующем окне мастер сообщит о возможных вариантах сетевых настроек и о необходимости установить на компьютере соответствующее оборудование до того, как вы начнете процедуру подключения к локальной сети. Снова щелкните на кнопке Далее.

В новом окне, позволяющем выбрать метод подключения к сети, выберите переключатель Этот компьютер подключен к Интернету через шлюз или другой компьютер в сети. Данный вариант следует выбирать для типичной домашней локальной сети топологии «звезда» с

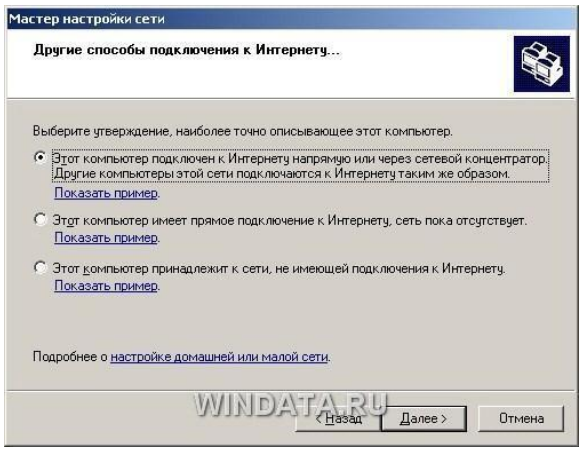
коммутатором и подключением к Интернету через общий модем. Если же подключение



производится через другой компьютер то выберите, соответственно, первый переключатель.

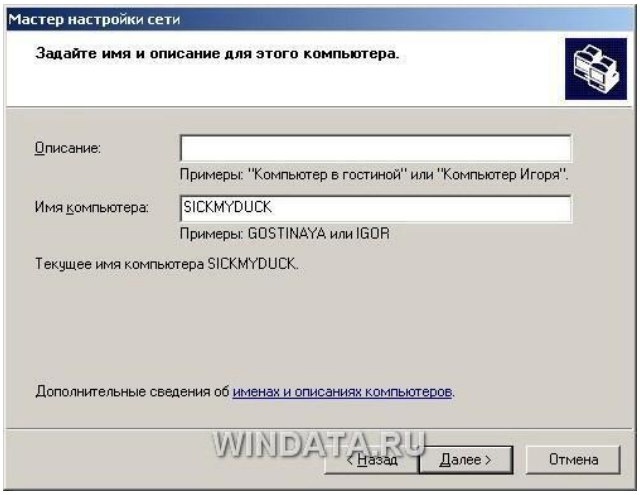
Если выбрать переключатель Другое, то станут доступными еще дополнительных три варианта, которые обычно не используются и описание которых говорит само за себя, например, «Этот компьютер имеет прямое подключение к Интернету, сеть пока

отсутствует». Выбрав необходимый вариант, щелкните на кнопке Далее.



В следующем окне нужно указать сетевое имя и дать описание компьютера. Введите произвольное описание компьютера в поле Описание например «Мой железный супермонстр» или «Покоритель цифровой вселенной». Сетевое имя компьютера будет

отображаться в папке Сетевое окружение, и предназначено для идентификации компьютера в локальной сети. Введите имя в поле Имя компьютера и щелкните на кнопке Далее.



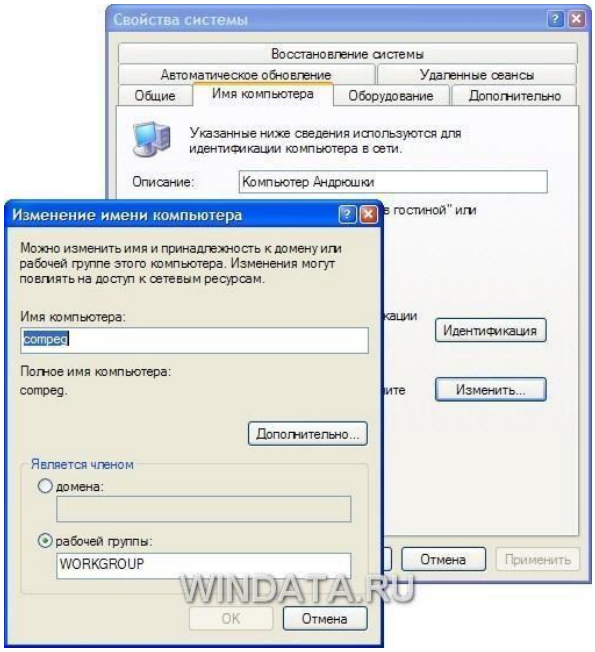
В новом окне укажите название сетевой рабочей группы, к которой принадлежит компьютер. Введите название рабочей группы в поле Рабочая группа.

Все компьютеры в домашней локальной сети должны иметь **одинаковое название рабочей группы**. Можно оставить без изменений базовое название WORKGROUP, автоматически указываемое Windows XP, либо выбрать и свое название, не забыв указать его для других компьютеров.

В следующем окне мастер настройки сети продемонстрирует все указанные вами сведения. Если что-либо введено неправильно, воспользуйтесь кнопкой Назад, чтобы отредактировать соответствующие настройки. Когда все будет готово, щелкните на кнопке Далее. Теперь Windows XP автоматически протестирует конфигурацию локальной сети и настроит сетевое подключение на вашем компьютере. Щелкните на кнопке Готово. Изменить сетевое имя

компьютера, его описание и название рабочей группы можно и без помощи мастера настройки. Щелкните на кнопке Пуск, затем правой кнопкой мыши на значке Мой

компьютер и выберите команду Свойства. Перейдите на вкладку Имя компьютера. В поле описание можно ввести любое текстовое описание компьютера (делать это не обязательно). В этом же окне указано название рабочей группы. Щелкните на кнопке Изменить и введите в поле Имя компьютера сетевое обозначение компьютера, а в поле Рабочая группа – название рабочей группы.



Осталось настроить аналогичное подключение для других компьютеров в локальной сети, в которых следует воспользоваться услугами описанного в данном разделе мастера настройки сети.

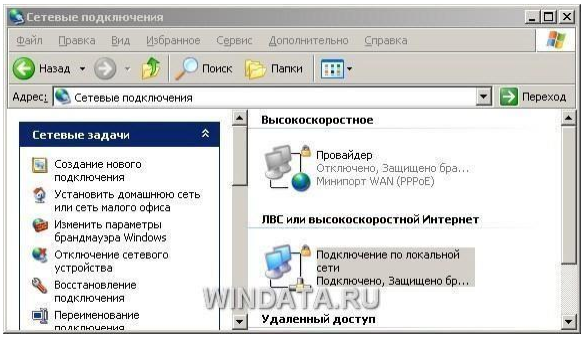
Настройка конфигурации сети

Несмотря на то что мастер настройки сети автоматически создает все необходимые сетевые параметры, свойства сетевых протоколов могут не соответствовать текущей конфигурации локальной сети. Иными словами, мастер не всегда на «отлично» справляется со своей работой. Если, открыв папку Сетевое окружение, вы не увидите в ней значков подключенных к локальной сети компьютеров, придется изменять настройки сетевых протоколов вручную. Для этого понадобятся следующие параметры:

- IP-адрес вашего компьютера;
- маска подсети;
- IP-адрес основного шлюза доступа к Интернету.

Откройте папку Сетевое окружение и щелкните на ссылке Отобразить сетевые подключения в левой панели Сетевые задачи. Откроется окно Сетевые подключения, содержащее значки всех настроенных в системе сетевых подключений. Дважды щелкните на значке

соответствующего сетевого подключения, чтобы открыть окно с данными о состоянии



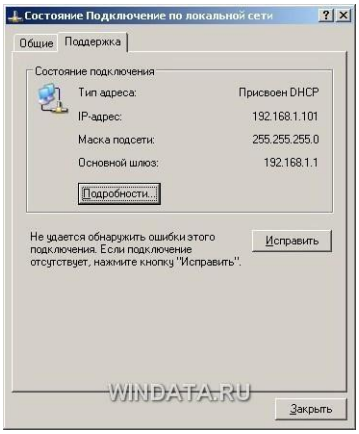
подключения локальной сети.

В частности, в окне указана длительность активного сетевого соединения, скорость

соединения, активность (сколько байтов информации отправлено и принято). Все параметры сетевого соединения представлены в этом же окне на вкладке Поддержка.

Там можно узнать тип IP-адреса (введен вручную или назначен DHCP), IP-адрес компьютера, маску подсети и IP-адрес основного шлюза.

Вкладка Поддержка.

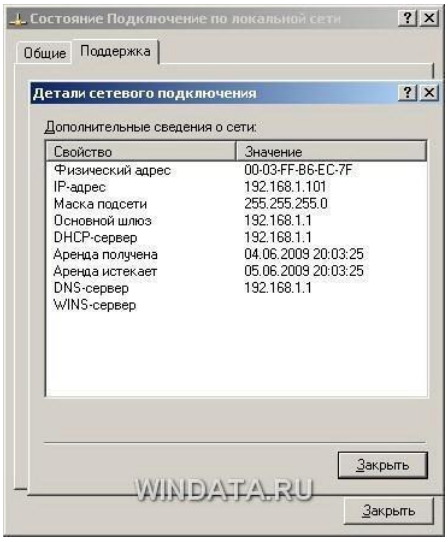


Кроме того, если щелкнуть на кнопке Подробности, можно получить дополнительные

сведения, такие как физический MAC-адрес сетевого адаптера. В окне также расположена кнопка Исправить, позволяющая исправить некоторые проблемы, связанные с

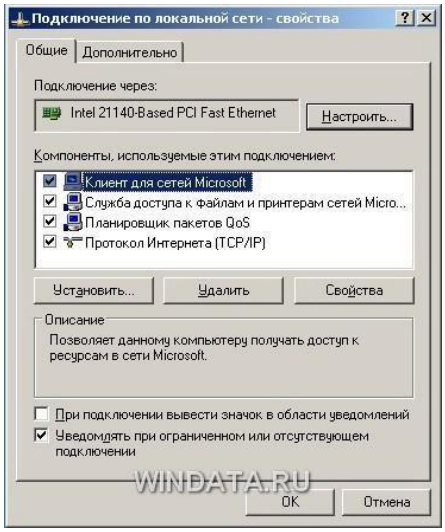
подключением.

Щелкните на кнопке Подробности, чтобы открыть это окно.



Щелкните на кнопке Исправить, чтобы исправить проблемы с сетевым подключением. Порой действительно помогает :)

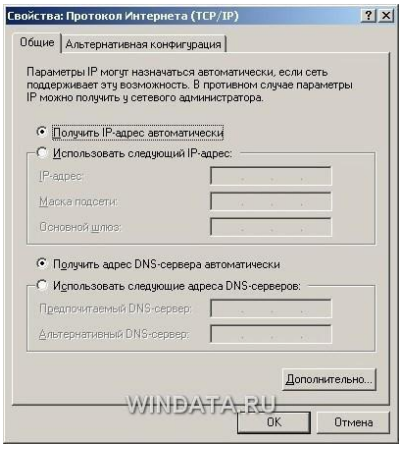
Чтобы внести какие-либо изменения в конфигурацию локальной сети, щелкните на кнопке Свойства. Откроется окно со свойствами сетевого подключения.



Чтобы изменить аппаратные настройки сетевой платы, щелкните на кнопке Настроить.

Кроме того, установите флажок При подключении вывести значок в области уведомлений, чтобы при подключении к локальной сети в области уведомления Windows 10 отображался специальный значок.

Настройка параметров TCP/IP – основной шаг, позволяющий добиться работоспособности локальной сети. В окне Подключение по локальной сети выберите пункт Протокол Интернета (TCP/IP) и щелкните на кнопке Свойства. Откроется окно Свойства: Протокол Интернета (TCP/IP).



Для стандартной домашней сети можно рекомендовать такие параметры. Адреса

компьютеров указывайте в диапазоне 192.168.0.2-192.168.0.50, т.е. первый компьютер получает адрес 192.168.0.2, второй – 192.168.0.3 и т.д. Адрес 192.168.0.1, как правило,

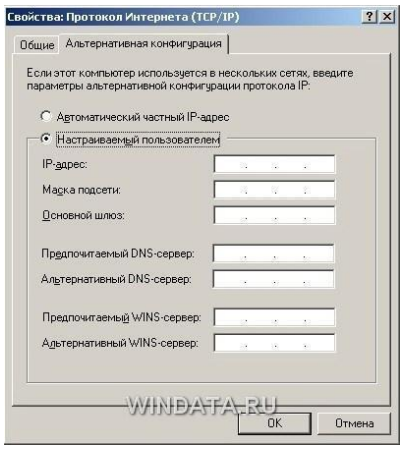
присваивается основному шлюзу сети. Маску подсети укажите как 255.255.255.0. Во многих случаях такая конфигурация подойдет для организации работы локальной сети. Если мастер настройки сети выполнил свою работу, то IP-адрес компьютеру назначается автоматически. В противном случае адрес придется указать вручную. Для этого выберите переключатель

Использовать следующий IP-адрес и введите IP-адрес компьютера в поле Использовать следующий IP-адрес, а в поле Маска подсети – маску подсети. Если в сети используется

определенный шлюз, такой как маршрутизатор, укажите его IP-адрес в поле Основной шлюз.

Вводить IP-адреса первичного и вторичного DNS-серверов, как правило, не обязательно (хотя порой и требуется).

Если компьютер используется в нескольких сетях, щелкните на вкладке Альтернативная конфигурация. В ней можно, выбрав переключатель ввести параметры альтернативной конфигурации IP, включая IP-адрес, маску подсети и основной шлюз, а также



предпочитаемые и альтернативные DNS-серверы.

Щелкните на кнопке ОК, чтобы сохранить произведенные изменения. Для того чтобы изменения вступили в силу, потребуется перезагрузка компьютера. Если все параметры были указаны верно, после перезагрузки локальная сеть будет активизирована, и компьютеры смогут обмениваться данными.

Практическая работа 8

Тема: Проектирование беспроводной локальной сети

Цели: проектирование локальной вычислительной сети на основе технологии беспроводной передачи данных по стандарту

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задание:

1. На основе разработанного проекта структурированной кабельной сети разработать проект беспроводной сети.
2. Провести необходимые изменения в схемах, вместо компьютеров установить ноутбуки, изменить спецификации и кабельный журнал.
3. Произвести расчет стоимости беспроводной сети.
4. Сохранить проект в свою рабочую папку, показать преподавателю, заполнить отчет и защитить работу.

Практическая работа 9

Тема: Оформление технической документации для проекта беспроводной сети. Контроль соответствия проекта беспроводной сети
нормативно-технической документации

Цели: Изучить техническую документацию для проекта беспроводной сети.

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задание:

1. Повторить состав технической документации сети.
2. Дать краткие ответы на вопросы:

1. По каким ГОСТам составляется техническая документация сети?
2. Какие документы входят в технический проект сети?
3. Чем структурно-функциональная схема сети отличается от плана структуры сети?
4. Какие спецификации входят в состав проекта?

3. Имеющиеся схемы, спецификации, таблицы расчетов структурированной кабельной сети оформить в один файл проекта в соответствии с ГОСТами.
4. Сохранить проект в свою рабочую папку, заполнить отчет, показать преподавателю и защитить работу.

Оформление пояснительной записки проекта

Пояснительная записка может быть написана при помощи средств вычислительной техники на формате А4, обязательно используется рамка.

Текст пояснительной записки располагается на одной стороне листа.

При выполнении пояснительной записки в текстовом редакторе Microsoft Word рекомендуется шрифт Gost type B, размером 14 (в таблицах размер шрифта 12), междустрочный интервал - полуторный.

Не допускается в пояснительной записке применять цветные шрифты, подчеркивание

и т.п.

Каждый лист пояснительной записки должен иметь поля (слева 3 см, сверху и снизу 2

см, справа 1,5 см).

Расстояние от рамки формата до границ текста следует оставлять в начале строк не менее 5 мм, в конце строк - не менее 3 мм.

Расстояние от верхней или нижней строки текста до верхней или нижней рамки формата должно быть не менее 10 мм.

Абзац в тексте - 1,25 см.

Нумерация листов и содержание

Нумерация листов в проекте выполняется арабскими цифрами, способ нумерации сквозной.

Нумерация листов начинается с титульного, на котором единица не ставится, затем следует лист «Содержание» (всегда лист «2»), и затем продолжается последовательная нумерация до последнего листа.

В содержании перечисляются номера, наименования разделов и страниц, на которых эти разделы начинаются. Наименования разделов в содержании должны точно соответствовать наименованиям разделов в тексте проекта.

Слово «Содержание» записывается в виде заголовка (симметрично тексту) прописными буквами.

Наименования, включённые в содержание, записывают строчными буквами (кроме первой прописной).

Построение текста проекта

Текст проекта при необходимости разбивают на разделы и подразделы. Каждый раздел рекомендуется начинать с нового листа.

Наименования разделов должны соответствовать содержанию и записываться в виде заголовка (симметрично тексту) прописными буквами.

Наименования подразделов должны соответствовать содержанию и записываться в виде заголовков строчными буквами (кроме первой прописной).

Содержащиеся в тексте пункта перечисления требований, указаний положений обозначают арабскими цифрами со скобкой: 1), 2), 3) и т.д. Каждый пункт перечисления записывают с новой строки.

Переносы слов в заголовках не допускаются. Точку в конце заголовка не ставят.

Термины и определения должны быть едиными, общепринятыми и соответствовать установленным стандартам.

Условные буквенные и графические обозначения должны соответствовать установленным стандартам.

Расстояние между заголовком и последующим текстом должно составлять 2 межстрочных интервала.

Наименования обозначения, приводимые в тексте, в расчетах на схемах должны быть одинаковыми. Не допускается сокращение обозначения единиц физических величин, если они употребляются без цифр.

Построение и заполнение таблиц

Цифровой материал, как правило, оформляют в виде таблиц.

Заголовки граф таблицы начинаются с прописных букв, а подзаголовки со строчных. Заголовки указывают в единственном числе. В конце заголовка и подзаголовков таблиц знаки препинания не ставят. Для облегчения ссылок в тексте проекта допускается нумерация граф. Графу **«номер по порядку»** в таблицу не включают. При необходимости порядковые номера указывают в одной (строке) графе с наименованием.

Нумерация таблиц в проекте сквозная.

Если цифровые данные в графах таблицы выражены в различных единицах физических величин, то их указывают в заголовке каждой графы. Если все параметры выражены в одной и той же единице физической величины, то еѐ сокращённое

обозначение помещают в заголовке над таблицей. Ставить кавычки вместо повторяющихся цифр не допускается. Если цифровые данные в таблице не приведены, то в графе ставится прочерк.

Таблица 3 – Название таблицы

Наименование	**Длина, м**			
1	2	3	4	5
1. …	7	5		

При переносе таблицы на другой лист головку таблицы повторяют, над ней пишут

«**Продолжение таблицы…»**. Ссылки в тексте на таблицу даются следующим образом: **см. табл. 3** или **в табл. 3.**

Основная надпись чертежа

Все графические материалы к проекту сети должны иметь основную надпись, которая располагается в правом нижнем углу. Расположение, размеры и содержание основной надписи на чертежах должны соответствовать ГОСТ 2.104-68. Наименование чертежа выполняется согласно ГОСТ 102-68 и ГОСТ 2.701-76. Устанавливается следующий порядок заполнения основной надписи:

Наименование изделия. Оно должно быть кратким и лаконичным. В наименованиях, состоящих из двух и более слов имя существительное, например: «Схема помещения», ниже мелким шрифтом пишется вид документа, например: «Планирование вычислительной системы организации».

Шифр присваиваемый документу: например **БПК.230111.41КС**

На каждом листе пояснительной записки, выполненной студентом группы 41 КС должен быть написан шифр. **Оформление иллюстраций в проекте**

Число иллюстраций должно быть достаточным для пояснения излагаемого текста. К иллюстрациям в проекте относятся: рисунки, схемы и т.д.

Все иллюстрации должны быть выполнены в соответствии с требованием стандартов, ЕСКД и пронумерованы арабскими цифрами в пределах раздела. Например: рис. 1.1 рис 2.4...

В тексте проекта делаются ссылки на необходимую иллюстрацию, например: см. рис. 1.2.

Каждый рисунок должен иметь так называемый подрисуночный текст, который располагается под рисунком по центру. Сокращения слов не допускаются. Первая буква в подрисуночном тексте - прописная.

Наименование иллюстраций помещают над иллюстрациями, поясняющие данные под ней. Номер иллюстрации помещают ниже поясняющих данных.

Практическая работа 10

Тема: Настройка беспроводного оборудования. Диагностика работоспособности сети

Цели: Изучить средства настройки беспроводной сети средствами ОС Windows (теоретический материал).

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задание:

1. Какие стандарты беспроводной сети массово используются в наше время?
2. В чем состоит технология Super G? В каком оборудовании используется данная технология?
3. Раскройте понятия:

SSID

Channel

Data

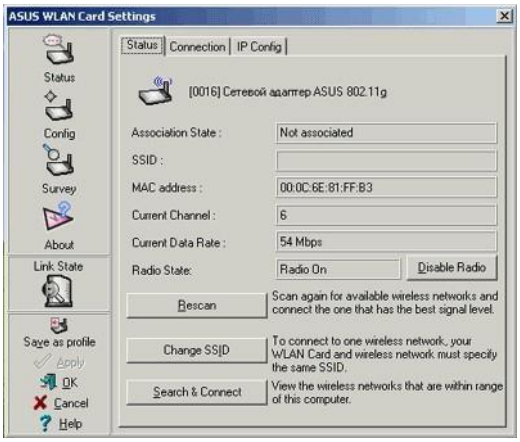
Rate

Encryption Самостоятельно составьте алгоритм настройки беспроводного оборудования в ОС Windows 8. Покажите результат работы преподавателю.

Настройка беспроводного оборудования ASUS WLAN Control Center — ASUS WL-100g

При первом запуске ASUS WLAN Control Center (после установки этой утилиты) она спрашивает, будет ли управление данной беспроводной картой осуществляться через нее или нужно предоставить эти функции Windows (ее сервису Zero Wireless Configuration). Подтверждаем, что хотим использовать утилиту от ASUS.

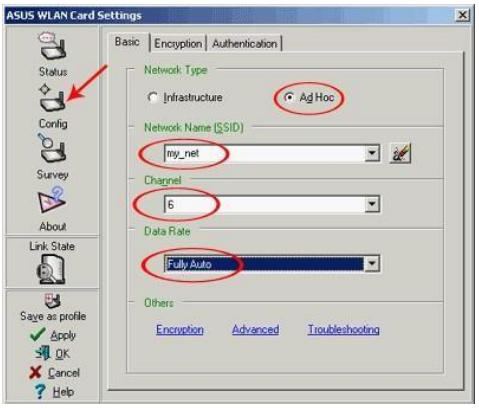
Не будет лишним отметить, что устанавливаемые интерфейсы от некоторых других производителей такой вопрос не задают, автоматически беря на себя управление адаптером.



При запуске интерфейс выглядит примерно так, как показано на скриншоте.

- Assotiation State: подключена ли карта к беспроводной сети (пока не подключена)
- SSID: имя сети тоже отсутствует
- Current Channel: на каком канале карта пытается найти сеть

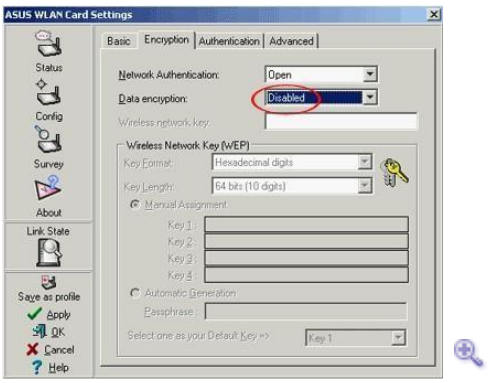
- Current Data Rate: на какой скорости работает адаптер, в данном



случае число 54 ничего не означает, так как карта не подключена к беспроводной сети

Для перехода к конфигурированию адаптера, надо щелкнуть на **Config**. В открывшемся окне выставляем:

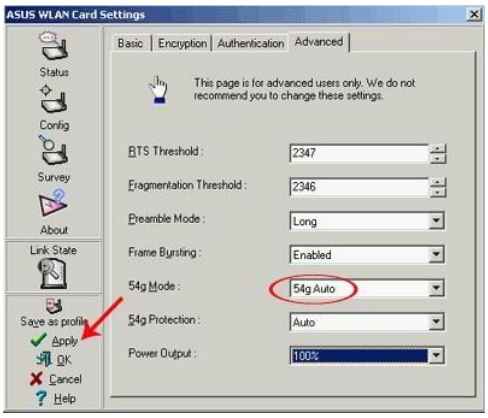
- Network Type (тип сети): Ad Hoc, одноранговая беспроводная сеть, в сети одни лишь адаптеры, устройства типа «точка доступа» не используются;
- SSID: имя сети выставили в **my_net**;
- Channel: установили шестой канал;
- Data Rate: скорость работы беспроводного адаптера установили



в автоматический режим

В следующей закладке, **Encryption**, настраивается шифрование. Во время первичной настройки беспроводной сети шифрование лучше отключить (так как если ничего не

заработает, то будет ясно, что дело точно не в шифровании). Рекомендуется



активировать шифрование сразу после того, как все компьютеры в беспроводной сети увидят друг друга.

В закладке **Advanced** настраиваются специфические параметры беспроводных сетей. Лучше оставить их в том состоянии, в котором они и стоят по умолчанию. Рассмотрю лишь пару из них: 54g Mode и Protection (у разных производителей названия могут отличаться). Они

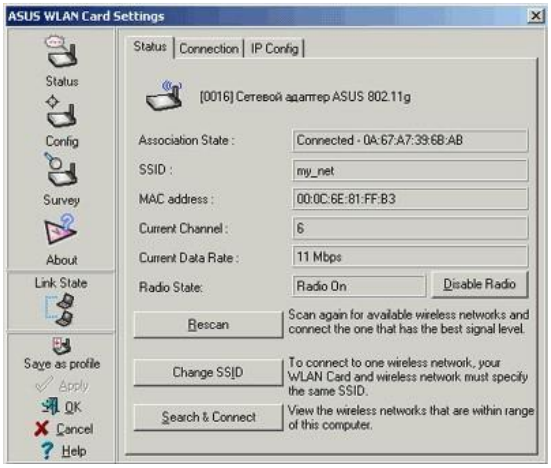
отвечают за режимы работы (совместимость) в смешанных беспроводных сетях, где одновременно работают 802.11b и 802.11g адаптеры. Лучше ставить режим **Auto** или же читать документацию по конкретным адаптерам и драйверам к ним для выставления

правильных параметров для работы устройств. В противном случае параметры, отличные от auto, могут не только увеличить скорость работы беспроводной сети, но и сделать ее

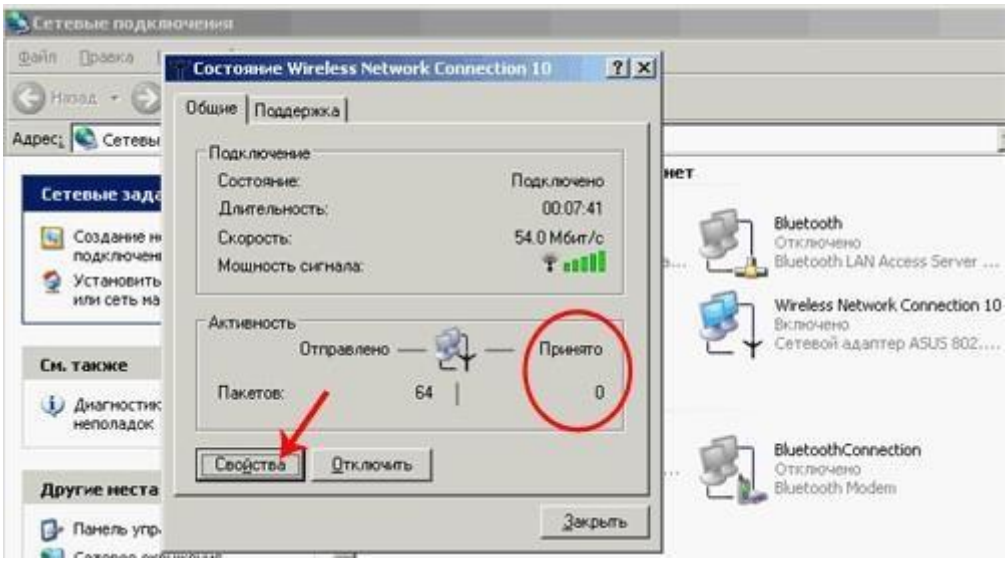
полностью неработоспособной. Это касается и остальных опций в разделе **Advanced**.

После выставления всех нужных опций, надо кликнуть на **Apply** для применения установок к адаптеру.

После этого шага в трее выскочит информационное сообщение, что мы подключились к беспроводной сети,



а раздел **Status** интерфейса драйверов ASUS, примет примерно такой вид, как на скриншоте. Информация о том, что мы подсоединились к беспроводной сети, в данном случае не означает, что компьютер действительно куда-то подключился. Сообщение о подключении может выскочить даже в том случае, если у нас лишь один компьютер с беспроводным
адаптером.



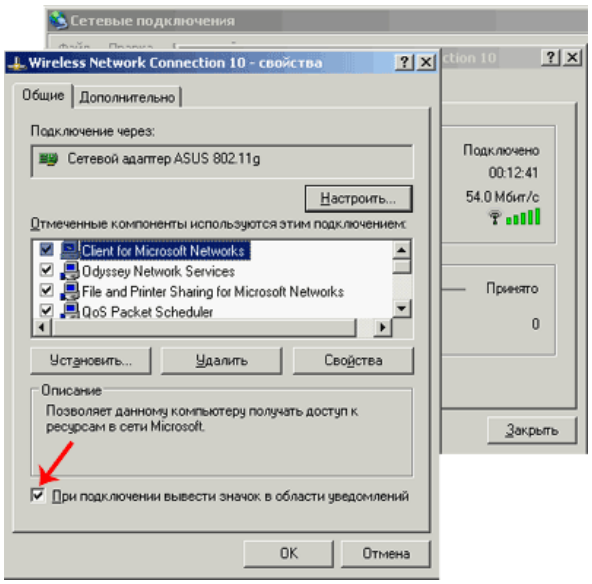
Передаются ли (а точнее — принимаются ли) данные в сети можно узнать, кликнув на иконку беспроводного соединения в трее. Или выбрав ее в разделе **Сетевые подключения**, в которые можно попасть через панель управления, или меню Пуск, или райткликнув на иконке **Сетевое**

окружение на рабочем столе и выбрав в появившемся меню пункт **Свойства**.

В появившемся окне свойств сетевого подключения нужно обратить внимание на счетчик принятых пакетов. Если там стоит число, отличное от нуля, значит, беспроводная сеть

работает, точнее беспроводной адаптер принимает пакеты, т.е. слышит другие адаптеры в той же беспроводной сети. Счетчик же отправленных пакетов показателем

работоспособности сети не является. Адаптер (точнее его драйвер) может отправлять пакеты



«в никуда», даже в случае неработоспособности беспроводной сети.

Кстати говоря, за появление значка сетевого соединения в трее отвечает галочка, помеченная на вышеприведенном скриншоте. Обычно она включена по умолчанию. Попасть в свойства сетевого соединения можно, кликнув по кнопке **свойства** в окне состояния соединения.

Тут же, в свойствах TCP/IP, проверяем автоматическую настройку IP адреса и DNS серверов (обычно так и стоит).

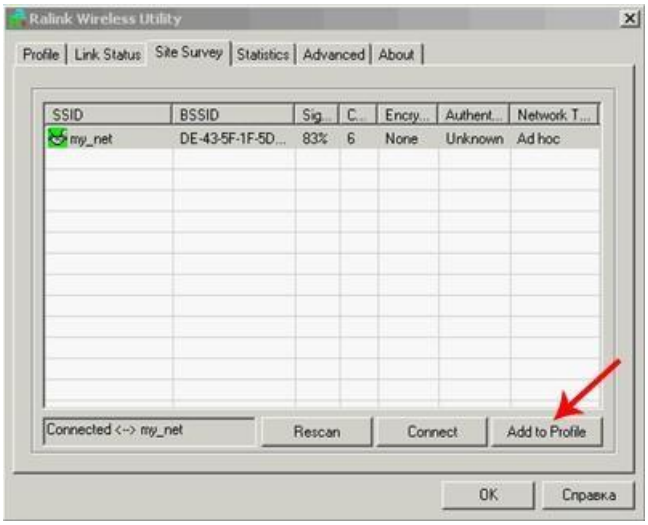
В ASUS WLAN Control Center есть еще одна полезная опция — сохранение текущих

настроек в профайл. Таким образом, можно создать несколько профилей (один — для дома, другой — для работы) и подгружать тот или другой (например, через Asus Mobile Manager) по мере необходимости. Возможность сохранения профилей есть в интерфейсах к

беспроводным картам у многих производителей. В том числе и в интерфейсе Zero Wireless Configuration (встроенный в Windows интерфейс управления беспроводными устройствами). Беспроводной адаптер на ноутбуке настроен (исключая шифрование). Переходим к настройке адаптера с PCI интерфейсом.

Интерфейс управления в реализации от Ralink — Asus WL-130g

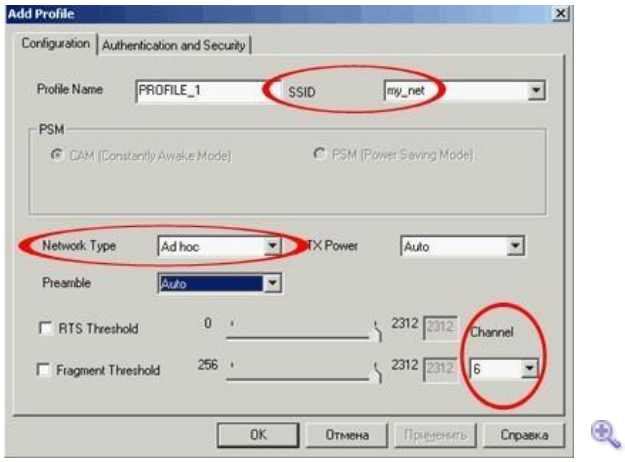
Ralink Configuration Utility помещает себя в трей в виде вот такого симпатичного значка. При райтклике на него появляется меню, позволяющее выбрать, кто будет управлять



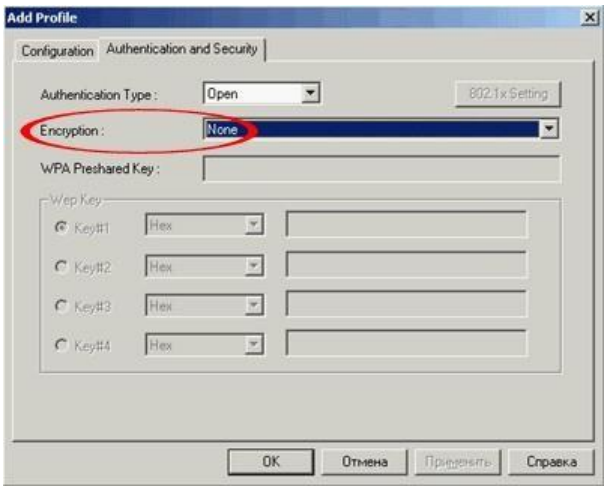
беспроводным адаптером — Windows или Ralink Utility.

При запуске интерфейса мы попадаем в раздел **Site Survey**, где показываются находящиеся поблизости беспроводные сети. В данном случае видна лишь одна сеть — my_net, так как сеть с этим именем уже настроена на ноутбуке. Достаточно выделить ее и кликнуть на кнопку **Add to Profile** (создать профиль настроек для этой сети).

Если в **Site Survey** нет списка доступных сетей (допустим, это первый компьютер, на котором настраивается беспроводная сеть), не страшно — достаточно перейти в закладку **Profile** (профили), и нажать **Add** (добавить).

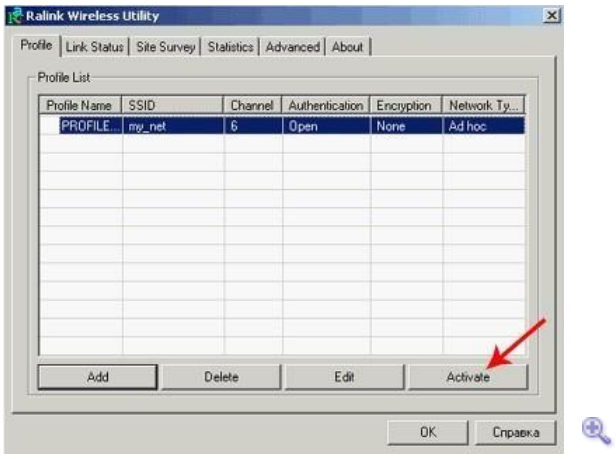


При создании профиля мы, как и в случае с картой на ноутбуке, ставим тип

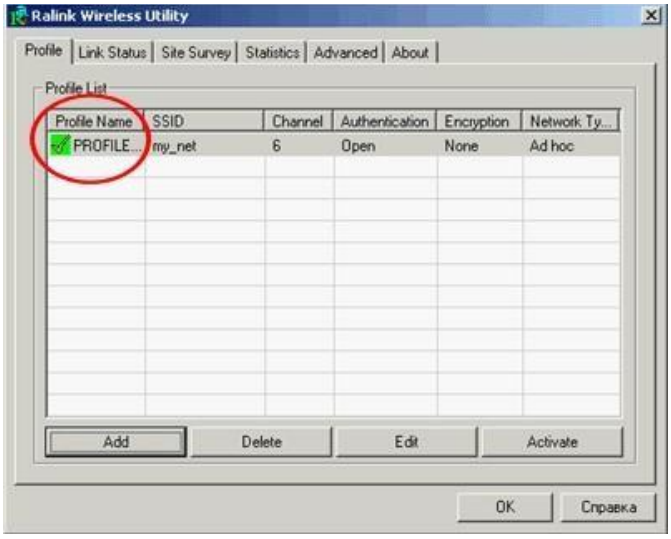


сети в Ad Hoc, SSID — my_net, и устанавливаем рабочим шестой канал.

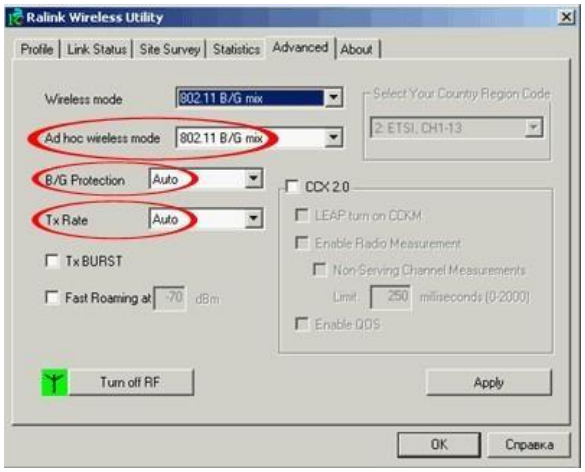
В разделе **Authentification and Security** временно отключаем шифрование.



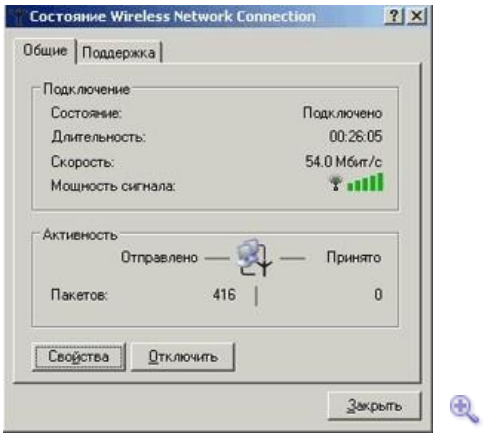
Осталось лишь активировать настроенный профиль, нажав кнопку **Activate**.



Напротив созданного профиля появилась пометка, говорящая о том, что в беспроводном адаптере используются настройки именно из этого профиля.



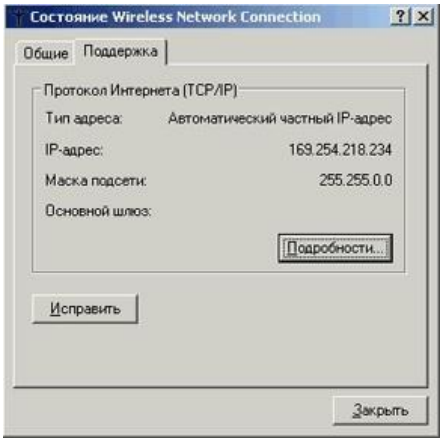
Так же имеет смысл зайти в раздел **Advanced**, дополнительных настроек. В нем установим типы адаптеров, которые могут работать в нашей беспроводной сети (**Wireless mode**) в
состояние 802.11 B/G mix, т.е. беспроводной адаптер на данном компьютере сможет общаться как с 802.11b, так и с 802.11g картами, установленными на других машинах
(возможно, что для совместимости со старыми 802.11b адаптерами, возможно, понадобится вместо Auto, установить эту опцию в 54G LRS). Опцию **B/G Protection**, относящуюся к той же области, поставим в состояние Auto. **TX Rate** — скорость работы адаптера, то же установим в автоматический режим.



Теперь мы имеем два компьютера, подключенных к общей беспроводной сети. Имеет смысл проверить, видят ли они друг друга. Для этого, вызываем окно

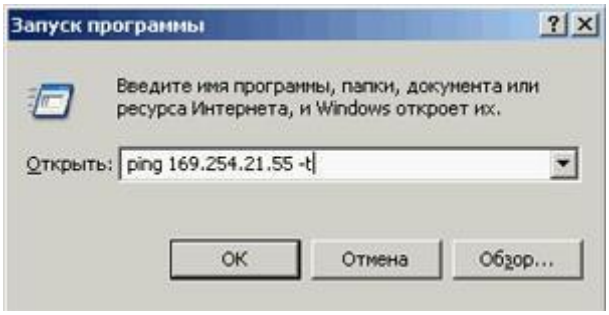
Состояния беспроводного адаптера (кликнув на беспроводной адаптер в **Сетевых подключениях**). Видим нулевое

количество принятых пакетов — это нормально, мы пока не обменивались



информацией с другим компьютером.

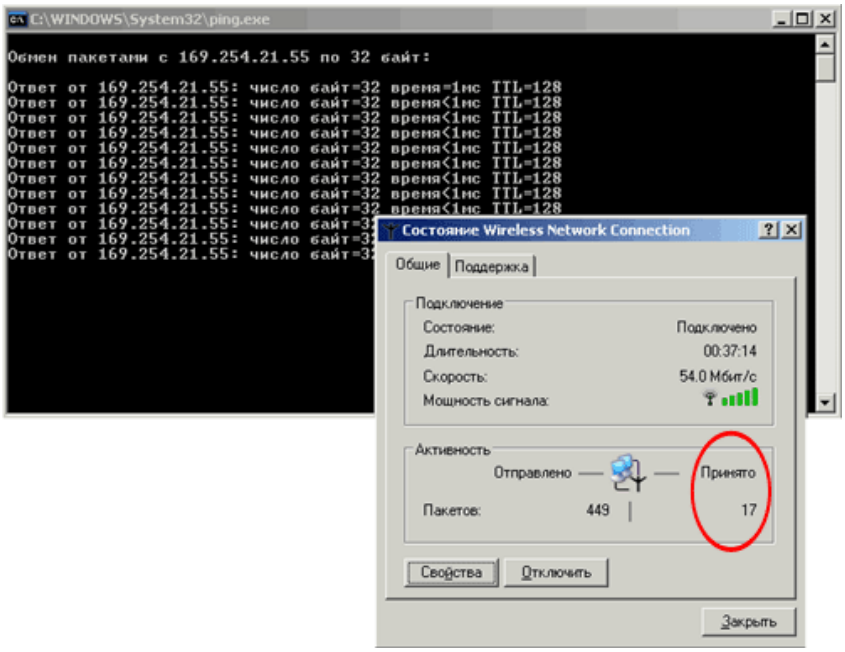
Выясняем IP адреса обоих компьютеров, перейдя на закладку **Поддержка**. Разумеется, на обоих адаптерах должно стоять автоматическое определение IP-адреса и DNS серверов. Ноутбук у нас имеет адрес 169.254.21.55, стационарных компьютер с PCI беспроводным адаптером — 169.254.218.234. Пингуем ноутбук со стационарного компьютера.



Для этого в **Пуск** —> **Выполнить** пишем:

ping 169.254.21.55 -t и жмем

Enter или кнопку **Ok**.



Удаленный компьютер должен отвечать на ping-запросы, а счетчик полученных пакетов — увеличиваться. Если этого не происходит, то беспроводная сеть не функционирует.

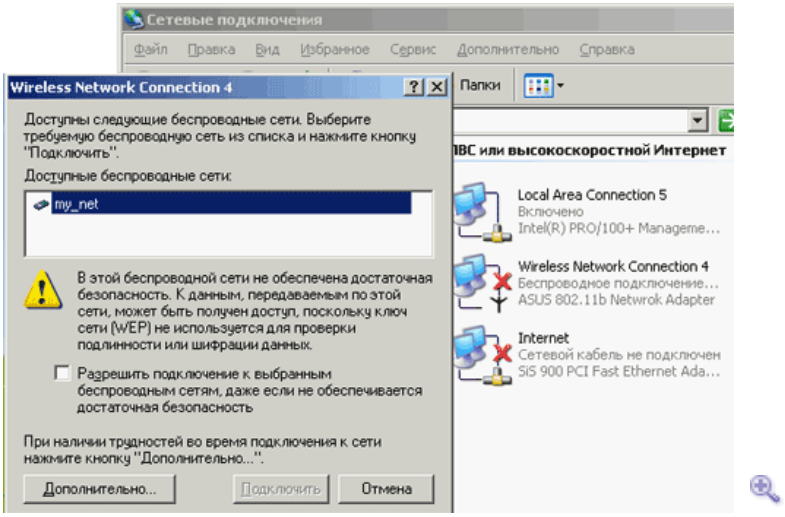
Возможные причины — разные каналы, разные SSID, разные ключи/типы шифрования, или на одном компьютере оно включено, на втором — нет. Так же возможно, что на каком-то из

компьютеров установлен 802.11b адаптер, а на другом — 802.11g, а также на втором отключена работа в режиме совместимости с 802.11b (возможно, также вместо

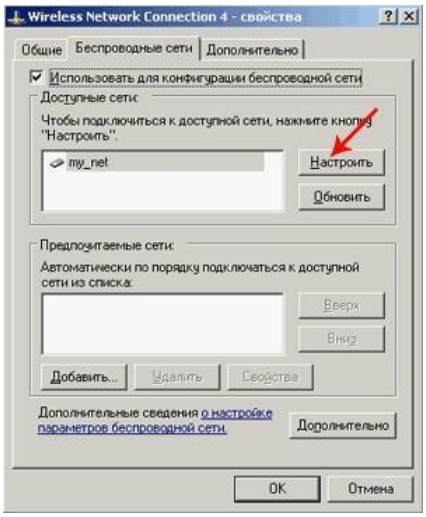
54G Auto нужно поставить 54G LRS или даже перевести все адаптеры в режим 802.11b Only).

Zero Wireless Configuration (встроенный в Windows интерфейс) — ASUS WL-140

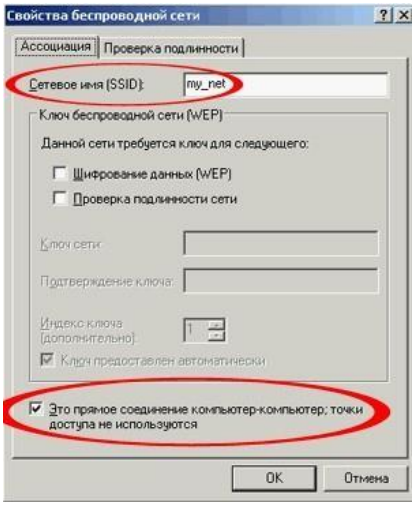
Последний рассматриваемый сегодня интерфейс конфигурирования — встроенный в Windows. Его мы рассмотрим, настраивая внешний адаптер с USB интерфейсом ASUS WL- 140.



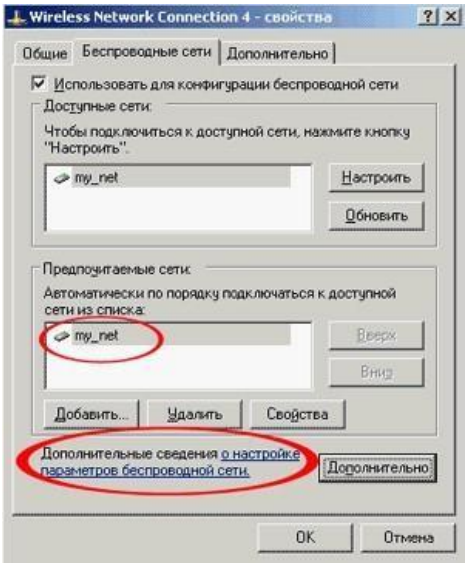
При клике на значок беспроводного адаптера операционная система предупреждает (если она увидела беспроводную сеть), что в выбранной сети отсутствует шифрование. Все верно, мы его отключили на этапе конфигурирования (о его включении и настройке — в следующей статье). Можно установить флажок **Разрешить подключение** и нажать кнопку подключить — Windows установит параметры самостоятельно и мы попадем (скорее всего) в беспроводную сеть. А можно нажать кнопку **Дополнительно**, что и сделаем.



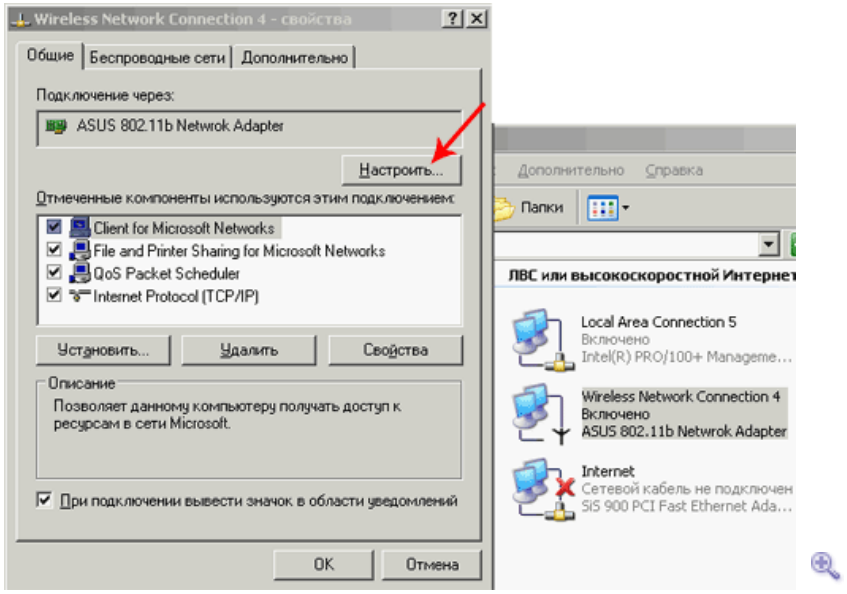
Выбираем доступную сеть из списка и жмем **Настроить** (если сети нет, то можно создать профиль для нее, нажав кнопку **Добавить**).



Тут проверяем, что бы SSID сети был верным, а флажок **Прямое соединение компьютеркомпьютер** (режим Ad Hoc) — активен. Шифрование пока отключено.



После нажатия **Ok**, в списке **Предпочитаемых сетей** появится наш новый профиль. Не помешает кликнуть на **Дополнительные сведения** — это ссылка на систему помощи Windows по настройке беспроводных сетей. Там написано довольно много интересного.



До расширенных (Advanced) настроек беспроводного адаптера можно добраться, зайдя на закладку **Общие** и нажав **Настроить**.

По большому счету, тут ничего трогать не следует. Большинство опций, обведенным

красным, все равно игнорируются, так как используются данные из профиля, настраиваемого в Zero-утилите.

На этом настройку последнего адаптера можно считать законченной. Опять же имеет смысл проверить работу беспроводной сети, пропинговав с каждого компьютера. Именно так,

потому что в Ad Hoc сети все машины для обмена данными друг с другом, соединяются напрямую. Поэтому вполне возможна ситуация, что в сети из трех машин (A, B, C), машина A пингует машину B, машина B пингует

машину С (т.е. вроде бы сеть работает), но машина С не пингует машину А! Как раз с подобным я столкнулся при написании этого материала. Беспроводная сеть (в вышеописанном режиме) работала, в качестве машины А выступал ноутбук с адаптером WL-100g, в качестве С — компьютер с USB адаптером WL-140. Так вот WL-100g и WL-140 не видели друг друга, хотя оба успешно общались с WL-130g.

Проблема быстро решилась выставлением опции **54g mode** в режим 54g LRS в настройках WL-100g адаптера. Это было связано со старой версией чипсета WL-140, он понимал не все скоростные режимы, в которых пытался работать WL-100g адаптер.

Изучить программные средства диагностики работоспособности сети, встроенные в ОС Windows (теоретический материал).

Письменно ответить на вопросы:

1. Какие существуют программные средства диагностики работоспособности сети, встроенные в ОС Windows? Опишите их использование.
2. Перечислите основные конфигурационные и диагностические команды набора протоколов TCP/IP.
3. Что относится к диагностическим онлайн сервисам?

Самостоятельно опишите программные средства диагностики работоспособности сети, встроенные в ОС Windows 10.

Опишите диагностические утилиты VisualRoute 2010 14.0a, 3D Traceroute 2.4.39.2. Покажите результат работы преподавателю.

Практическая работа 11

Тема: Использование приборов и программных средств мониторинга сети и технического контроля

Цели: Изучить аппаратные и программные средства мониторинга сети, функциональное использование приборов мониторинга сети

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задание:

Разработать презентацию по теме занятия. Письменно ответить на вопросы:

1. Опишите группы оборудования для диагностики и сертификации кабельных систем.
2. Опишите по одному прибору из каждой группы приборов мониторинга сети.
3. Опишите основные электромагнитные характеристики кабельных систем.
4. Какую информацию можно получить с помощью программ для мониторинга сети?
5. Опишите группу агентов SNMP.
6. Опишите группу агентов RMON. Заполните отчет, покажите результат работы преподавателю, защитите работу.

Приборы мониторинга сети

Оборудование для диагностики и сертификации кабельных систем. Условно это оборудование можно поделить на четыре основные группы: сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры (мультиметры).

- Сетевые мониторы (называемые также сетевыми анализаторами) предназначены для тестирования кабелей различных категорий. Следует различать сетевые мониторы и анализаторы протоколов. Сетевые мониторы собирают данные только о статистических показателях трафика - средней интенсивности общего трафика сети, средней интенсивности потока пакетов с определенным типом ошибки и т.п.
- Назначение устройств для сертификации кабельных систем, непосредственно следует из их названия. Сертификация выполняется в соответствии с требованиями одного из международных стандартов на кабельные системы.
- Кабельные сканеры используются для диагностики медных кабельных систем. ·

Тестеры предназначены для проверки кабелей на отсутствие физического разрыва.

Оборудование для диагностики и сертификации кабельных систем

К оборудованию данного класса относятся сетевые анализаторы, приборы для сертификации кабелей, кабельные сканеры и тестеры.

Основные электромагнитные характеристики кабельных систем

Основными электрическими характеристиками, влияющими на работу кабеля, являются: затухание, импеданс (волновое сопротивление),

перекрестные наводки двух витых пар и уровень внешнего электромагнитного излучения.

Сетевые анализаторы

Сетевые анализаторы (не следует путать их с анализаторами протоколов) представляют собой эталонные измерительные инструменты для диагностики и сертификации кабелей и кабельных систем. В качестве примера можно привести сетевые анализаторы компании HewlettPackard - HP 4195A и HP 8510C.

Сетевые анализаторы содержат высокоточный частотный генератор и узкополосный приемник. Передавая сигналы различных частот в передающую пару и измеряя сигнал в приемной паре, можно измерить затухание и NEXT. Сетевые анализаторы - это

прецизионные крупногабаритные и дорогие (стоимостью более $20'000) приборы,

предназначенные для использования в лабораторных условиях специально обученным техническим персоналом.

Кабельные сканеры

Данные приборы позволяют определить длину кабеля, NEXT, затухание, импеданс, схему разводки, уровень электрических шумов и провести оценку полученных результатов. Цена на эти приборы варьируется от $1'000 до $3'000. Существует достаточно много устройств данного класса, например, сканерыкомпаний MicrotestInc., FlukeCorp., DatacomTechnologiesInc., ScopeCommunicationInc. В отличие от сетевых анализаторов сканеры могут быть использованы не только специально обученным техническим персоналом, но даже администраторами-новичками.

Для определения местоположения неисправности кабельной системы (обрыва, короткого замыкания, неправильно установленного разъема и т.д.) используется метод "кабельного

радара", или TimeDomainReflectometry (TDR). Суть этого метода состоит в том, что сканер излучает в кабель короткий электрический импульс и измеряет время задержки до прихода отраженного сигнала. По полярности отраженного импульса определяется характер повреждения кабеля (короткое замыкание или обрыв). В правильно установленном и подключенном кабеле отраженный импульс совсем отсутствует. Точность измерения расстояния зависит от того, насколько точно известна скорость распространения электромагнитных волн в кабеле. В различных кабелях она будет разной. Скорость распространения электромагнитных волн в кабеле (NVP - nominalvelocityofpropagation) обычно задается в процентах к скорости света в вакууме. Современные сканеры содержат в себе электронную таблицу данных о NVP для всех основных типов кабелей и позволяют пользователю устанавливать эти параметры самостоятельно после предварительной калибровки.

Наиболее известными производителями компактных (их размеры обычно не превышают размеры видеокассеты стандарта VHS) кабельных сканеров являются компании MicrotestInc., WaveTekCorp., ScopeCommunicationInc.

Тестеры

Тестеры кабельных систем - наиболее простые и дешевые приборы для диагностики кабеля. Они позволяют определить непрерывность кабеля, однако, в отличие от кабельных сканеров, не дают ответа на вопрос о том, в каком месте произошел сбой.

Программы для мониторинга сети

Программы для мониторинга сети отображают всевозможную информацию о статусе разнообразных сервисов интернета или локальной сети, сетевого оборудования и серверов.

Так же, они могут проверять доступность HTTP, FTP и SMTP сервисов, отображать данные об использовании сети, нагрузке на процессор, дисковом пространстве, строить списки компьютеров в локальной сети, проводить поиск и проверку паролей, просмотр и подключение сетевых ресурсов, осуществлять доступ к расшаренным папкам. Некоторые программы подобного типа способны не только вести статистику всех процессов сетевой деятельности, но и отслеживать их качество, анализировать ошибки, и делать выводы, на основании собранной информации.

Агенты SNMP

На сегодня существует несколько стандартов на базы данных управляющей информации. Основными являются стандарты MIB-I и MIB-II, а также версия базы данных для удаленного управления RMONMIB. Кроме этого, существуют стандарты для специальных MIB устройств конкретного типа (например, MIB для концентраторов или MIB для модемов), а также частные MIB конкретных фирм-производителей оборудования.

Первоначальная спецификация MIB-I определяла только операции чтения значений переменных. Операции изменения или установки значений объекта являются частью спецификаций MIB-II.

Версия MIB-I (RFC 1156) определяет до 114 объектов, которые подразделяются на 8 групп:

- System - общие данные об устройстве (например, идентификатор поставщика, время последней инициализации системы).

- Interfaces - описываются параметры сетевых интерфейсов устройства (например, их количество, типы, скорости обмена, максимальный размер пакета).
- AddressTranslationTable - описывается соответствие между сетевыми и физическими адресами (например, по протоколу ARP).
- InternetProtocol - данные, относящиеся к протоколу IP (адреса IP-шлюзов, хостов, статистика об IP-пакетах).
- ICMP - данные, относящиеся к протоколу обмена управляющими сообщениями ICMP.
- TCP - данные, относящиеся к протоколу TCP (например, о TCP-соединениях). · UDP - данные, относящиеся к протоколу UDP (число переданных, принятых и ошибочных UPD- дейтаграмм).
- EGP - данные, относящиеся к протоколу обмена маршрутной информацией ExteriorGatewayProtocol, используемому в сети Internet (число принятых с ошибками и без ошибок сообщений).

Из этого перечня групп переменных видно, что стандарт MIB-I разрабатывался с жесткой ориентацией на управление маршрутизаторами, поддерживающими протоколы стека TCP/IP.

В версии MIB-II (RFC 1213), принятой в 1992 году, был существенно (до 185) расширен набор стандартных объектов, а число групп увеличилось до 10.

Агенты RMON

Новейшим добавлением к функциональным возможностям SNMP является спецификация RMON, которая обеспечивает удаленное взаимодействие с базой MIB. До появления RMON протокол SNMP не мог использоваться удаленным образом, он допускал

только локальное управление устройствами. База RMONMIB обладает улучшенным набором свойств для удаленного управления,

так как содержит агрегированную информацию об устройстве, что не требует передачи по сети больших объемов информации. Объекты RMONMIB включают дополнительные счетчики ошибок в пакетах, более гибкие средства анализа графических трендов и статистики, более мощные средства фильтрации для захвата и анализа отдельных пакетов, а также более сложные условия установления сигналов
предупреждения. Агенты RMONMIB более интеллектуальны по сравнению с агентами MIB-I или MIB-II и выполняют значительную часть работы по обработке информации об
устройстве, которую раньше выполняли менеджеры. Эти агенты могут располагаться внутри различных коммуникационных устройств, а также быть выполнены в виде отдельных
программных модулей, работающих на универсальных ПК и ноутбуках (примером может служить
LANalyzerNovell).

Объекту RMON присвоен номер 16 в наборе объектов MIB, а сам объект RMON объединяет 10 групп следующих объектов:

- Statistics - текущие накопленные статистические данные о характеристиках пакетов, количестве коллизий и т.п.
- History - статистические данные, сохраненные через определенные промежутки времени для последующего анализа тенденций их изменений.
- Alarms - пороговые значения статистических показателей, при превышении которых агент RMON посылает сообщение менеджеру.
- Host - данных о хостах сети, в том числе и об их MAC-адресах.
- HostTopN - таблица наиболее загруженных хостов сети.
- TrafficMatrix - статистика об интенсивности трафика между

каждой парой хостов сети, упорядоченная в виде матрицы.

- Filter - условия фильтрации пакетов.
- PacketCapture - условия захвата пакетов.
- Event - условия регистрации и генерации событий.

Данные группы пронумерованы в указанном порядке, поэтому, например, группа Hosts имеет числовое имя 1.3.6.1.2.1.16.4.

Десятую группу составляют специальные объекты протокола TokenRing. Всего стандарт RMONMIB определяет около 200 объектов в 10 группах, зафиксированных в двух документах - RFC 1271 для сетей Ethernet и RFC 1513 для сетей TokenRing.

Отличительной чертой стандарта RMONMIB является его независимость от протокола сетевого уровня (в отличие от стандартов MIB-I и MIB-II, ориентированных на протоколы TCP/IP). Поэтому, его удобно использовать в гетерогенных средах, использующих различные протоколы сетевого уровня.

Анализаторы протоколов

В ходе проектирования новой или модернизации старой сети часто возникает необходимость в количественном измерении некоторых характеристик сети таких, например, как интенсивности потоков данных по сетевым линиям связи, задержки, возникающие на различных этапах обработки пакетов, времена реакции на запросы того или иного вида, частота возникновения определенных событий и других характеристик.

Для этих целей могут быть использованы разные средства и прежде всего - средства мониторинга в системах управления сетью, которые уже обсуждались в предыдущих

разделах. Некоторые измерения на сети могут быть выполнены и встроенными в операционную систему программными измерителями, примером тому служит компонента ОС WindowsNTPerformanceMonitor. Даже кабельные тестеры в их современном исполнении способны вести захват пакетов и анализ их содержимого.

Но наиболее совершенным средством исследования сети является анализатор протоколов. Процесс анализа протоколов включает захват циркулирующих в сети пакетов, реализующих тот или иной сетевой протокол, и изучение содержимого этих пакетов.

Основываясь на результатах анализа, можно осуществлять обоснованное и взвешенное изменение каких-либо компонент сети, оптимизацию ее производительности, поиск и устранение неполадок. Очевидно, что для того, чтобы можно было сделать какиелибо выводы о влиянии некоторого изменения на сеть, необходимо выполнить анализ протоколов и до, и после внесения изменения.

Анализатор протоколов представляет собой либо самостоятельное специализированное устройство, либо персональный компьютер, обычно переносной, класса Notebook, оснащенный специальной сетевой картой и соответствующим программным обеспечением. Применяемые сетевая карта и программное обеспечение должны соответствовать топологии сети (кольцо, шина, звезда). Анализатор подключается к сети точно также, как и обычный узел. Отличие состоит в том, что анализатор может принимать все пакеты данных, передаваемые по сети, в то время как обычная станция - только

адресованные ей. Программное обеспечение анализатора состоит из ядра, поддерживающего работу сетевого адаптера и декодирующего получаемые данные, и дополнительного
программного кода, зависящего от типа топологии исследуемой сети. Кроме того,
поставляется ряд процедур декодирования, ориентированных на определенный протокол, например, IPX. В состав некоторых анализаторов может входить также экспертная система, которая может выдавать пользователю рекомендации о том, какие эксперименты следует проводить в данной ситуации, что могут означать те или иные результаты измерений, как устранить некоторые виды неисправности сети.

Несмотря на относительное многообразие анализаторов протоколов, представленных на рынке, можно назвать некоторые черты, в той или иной мере присущие всем им:

- Пользовательский интерфейс. Большинство анализаторов имеют развитый дружественный интерфейс, базирующийся, как правило, на Windows или Motif. Этот интерфейс позволяет пользователю: выводить результаты анализа интенсивности трафика; получать мгновенную и усредненную статистическую оценку

производительности сети; задавать определенные события и критические ситуации для
отслеживания их возникновения; производить декодирование протоколов разного уровня и представлять в понятной форме содержимое пакетов.

- Буфер захвата. Буферы различных анализаторов отличаются по объему. Буфер может располагаться на устанавливаемой сетевой карте, либо для него может быть отведено место в оперативной памяти одного из компьютеров сети. Если буфер расположен на сетевой карте, то управление им осуществляется аппаратно, и за

счет этого скорость ввода повышается. Однако это приводит к удорожанию анализатора. В случае недостаточной производительности процедуры захвата, часть информации будет теряться, и анализ будет невозможен. Размер буфера определяет возможности анализа по более или менее представительным выборкам захватываемых данных. Но каким бы большим ни был буфер захвата, рано или поздно он заполнится. В этом случае либо прекращается захват, либо заполнение начинается с начала буфера.

- Фильтры. Фильтры позволяют управлять процессом захвата данных, и, тем самым, позволяют экономить пространство буфера. В зависимости от значения определенных полей пакета, заданных в виде условия фильтрации, пакет либо игнорируется, либо записывается в буфер захвата. Использование фильтров значительно ускоряет и упрощает анализ, так как исключает просмотр ненужных в данный момент пакетов.
- Переключатели - это задаваемые оператором некоторые условия начала и прекращения процесса захвата данных из сети. Такими условиями могут быть выполнение ручных команд запуска и остановки процесса захвата, время суток, продолжительность процесса захвата, появление определенных значений в кадрах данных. Переключатели могут использоваться совместно с фильтрами, позволяя более детально и тонко проводить анализ, а также продуктивнее использовать ограниченный объем буфера захвата. · Поиск. Некоторые анализаторы протоколов позволяют автоматизировать просмотр информации, находящейся в буфере, и находить в ней данные по заданным критериям. В то время, как фильтры проверяют входной поток на предмет соответствия условиям фильтрации, функции поиска применяются к уже накопленным в буфере данным.

Практическая работа 12

Тема: Резервное копирование информации

Цели: реализация метода обратного инкрементального резервного копирования для предотвращения потери информации при реализации угроз на информационную систему.

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задание:

1. Изучить теоретический материал по резервному копированию информации и восстановлению данных.
2. Описать процесс резервного копирования информации в Windows 7 и Windows 10 Pro.
3. Описать процесс восстановления данных.
4. Дать краткие ответы на вопросы:
    1. Дайте определение резервному копированию информации.
    2. Зачем нужно резервное копирование данных.
    3. Какие бывают резервные копии?
    4. Перечислите средства Windows для резервного копирования.
    5. Перечислите программы для резервного копирования данных.
    6. Опишите рекомендации по резервному копированию данных.

5. Выполнить резервное копирование своей папки на диске X: на рабочий стол своего компьютера средствами Windows (не забудьте, сделать скриншоты своих действий и вставить их в презентацию).

Выполнить восстановление своего архива с данными (не забудьте, сделать скриншоты своих действий и вставить их в презентацию).

Тема 2.2. Соединение сетей.

Практическая работа 1

Тема: Создание корпоративной сети из нескольких сетей

с Web сайтом в каждой сети

Цели: создание эффективной внутренней и внешней работы этой организации

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задание:

Рассмотрим использование Virtual Host-Only Ethernet Adapter, применение которого позволяет обеспечить **полное взаимодействие машин** между собой и **выход обеих во внешний мир**, хотя описание настройки будет приведено для каждого типа сетевого интерфейса.

Настройка Host-части VirtualBox

В качестве host-системы в данном случае выступает операционная система Windows Vista Home Premium SP2 (Windows Server 2008), а качестве гостевой Windows XP Pro SP3.

Итак, первым делом определимся с реальным подключением host-машины к сети Интернет и самое главное и нужное свойство — это тип IP-адреса – статический или динамический.

В настройках приложения VirtualBox через меню «File» («Файл») открываем вкладку «Network» («Сеть») и производим следующие действия.

Сначала выставляем IPv4-адрес и IPv4-маску подсети (рис. 1).

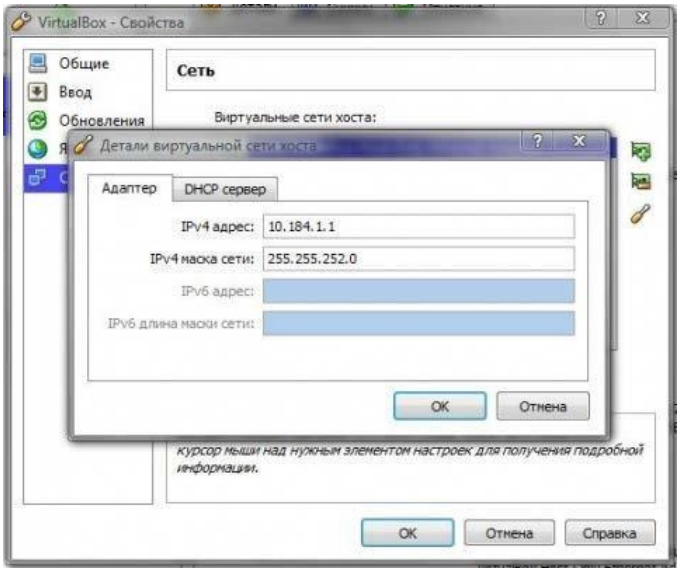


Рис.1: параметры адаптера.

Вводимый здесь IPv4-адрес обязательно должен находиться в диапазоне адресов реальных адаптеров;

IPV4-маска подсети должна соответствовать маске, используемой реальным адаптером.

Включаем DHCP-сервер (независимо от того, статический или динамический IPадрес Вашего реального сетевого адаптера), рис.2.

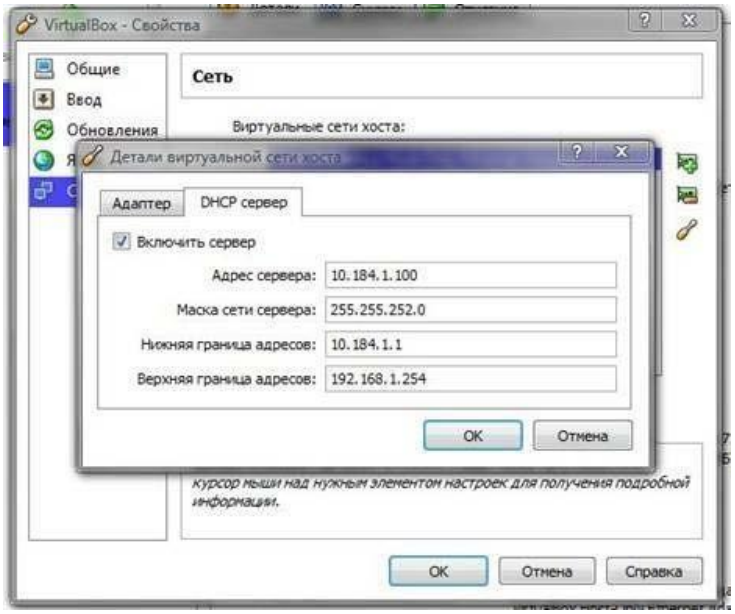


Рис.2: параметры DHCP-сервера.

Адрес сервера также должен находиться в диапазоне адресов реальных

адаптеров, IPv4маска подсети должна соответствовать маске, используемой реальным адаптером, верхняя и нижняя границы адресов должны захватывать все адреса, используемые в системе.

Сетевые настройки виртуальной машины

В настройках Settings (Настройки) установленной виртуальной машины открываем вкладку Network (Сеть) и производим следующие действия:

1. Включаем адаптер Host-only adapter;
2. Включаем адаптер NAT;
3. Включаем адаптер Bridge Adapter и для него выбираем Ваш реальный интерфейс сети Интернет, но т.к. речь идет о настройке именно для Virtual Host-Only

   Ethernet Adapter, то пока не важно, что там выбрано;

4. Включаем адаптер Internal Network;
5. Для каждого адаптера выбираем тип сетевой карты PCnet-Fast III (Am79C973), т.к. операционная система Windows XP, установленная гостевой, поддерживает только этот адаптер;
6. В настройках каждого адаптера ставим флаг о подключении кабеля.

Пояснение по каждому адаптеру:

- NAT – наипростейший способ предоставить гостевой ОС доступ в интернет, при таком режиме осуществляется просто перенаправление (транзакции) пакетов;
- Bridge Adapter - сетевой адаптер виртуальной машины получает такой же доступ в сеть, как и сетевой адаптер host-машины, но нет доступа во внешний мир;
- Internal Network - внутренняя сеть для объединения виртуальных машин в локальную сеть, без наружу и к host-машине;
- Host-only adapter - Ваша виртуалка как живая, она имеет доступ к сети Интернет, находится в одной локальной сети с реальной и имеет к ней доступ.

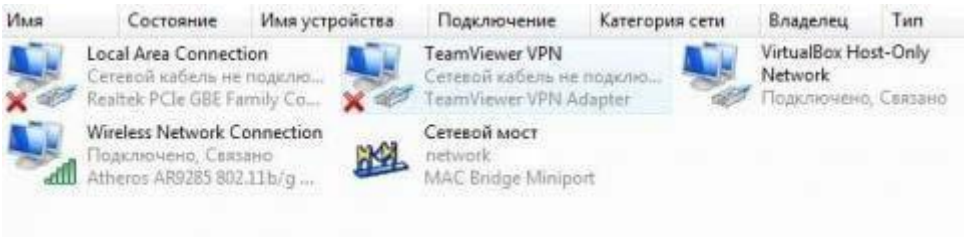
Настройка сетевого моста и шлюза Интернет

Теперь открываем папку «Сетевые подключения», с помощью клавиши «Ctrl» выделяем реальное подключение к сети интернет и VirtualBox Host-Only Network, созданный

программой VirtualBox, и через контекстное меню правой кнопки мыши

выбираем пункт «Сетевой мост». После этого это соглашаемся с сообщением о том, что данному адаптеру (сетевому мосту) присвоен адрес шлюза 192.168.0.1.

Примечание. Если Вы решили ограничиться сетевым интерфейсом NAT или Bridge, то сетевой мост Вам не нужен и эту часть настроек Вы можете пропустить. В папке



«Сетевые подключения» должна быть следующая картина:

Рис.3: «Сетевые подключения»

Но это еще не все, открываем «Карту сети» и видим там следующее:

Рис.4: «Карта сети»

И самое теперь самое неприятное - у нас пропало подключение к Интернету. Для того чтобы привести положение дел в порядок, нужно настроить сетевой мост, рис.5:

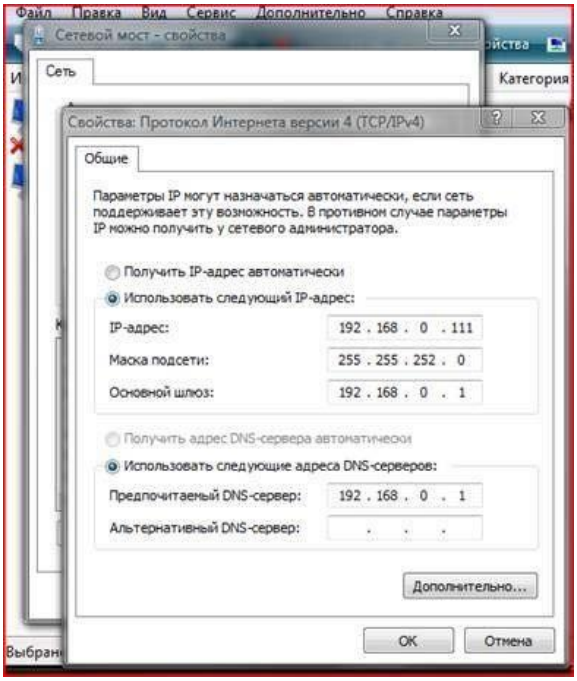


Рис.5: Настройка сетевого моста

Для IPv4-адреса используем любой адрес из установленного ранее диапазона адресов в

DHCP-сервере VirtualBox, маску подсети берем ту же, шлюз уже выставлен, а адрес DNScервера **выставляем таким же, как и адрес шлюза**. Применяем настройки, нажимая кнопку OK.

Примечание. Если Ваш реальный сетевой адаптер использует динамический IPv4- адрес, то в настройках сетевого моста, а также для всех сетевых интерфейсов виртуальной машины (их настройки будут приведены далее) следует выбрать пункт

«Получить IP-адрес автоматически», но в случае отсутствия подключения к интернету Вам следует произвести настройки, указанные для статического IP-адреса.

Снова открываем «Карту сети» и теперь видим там следующее, рис.6:

Рис.6: «Карта сети» после настройки сетевого моста

Примечание. Возможно, что у Вас в «Карте сети» элемент коммутатор отображаться не будет, но это не важно, а важно то, что наше подключение к Интернету снова активно! **Настройка сетевых подключений виртуальной машины**

Теперь пора заняться настройками виртуальной машины, для

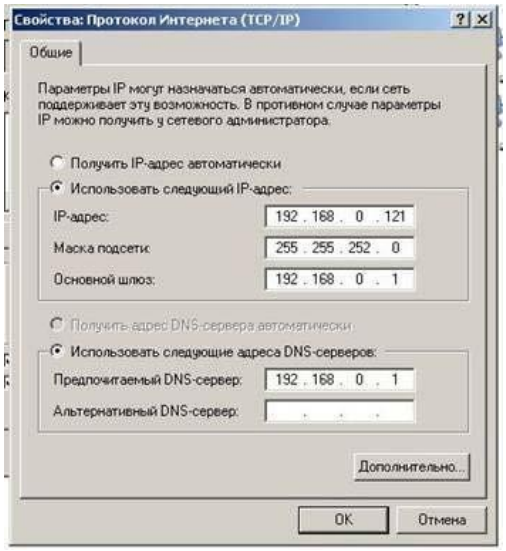
чего запускаем её и переходим к папке «Сетевые подключения», рис.7.

Рис.7: «Сетевые подключения» виртуальной машины

Все созданные подключения на месте – давайте настроим каждое из них, для этого

щелкнем правой кнопкой мыши на интерфейсе и в контекстном меню выберем пункт

«Свойства»:



1. Для адаптера Virtual Host-Only Ethernet Adapter:

Рис.8: Virtual Host-Only Ethernet Adapter

2. Для адаптера NAT Ethernet Adapter просто выставляем получить IP- адрес автоматически;
3. Для адаптера Intranet Ethernet Adapter:

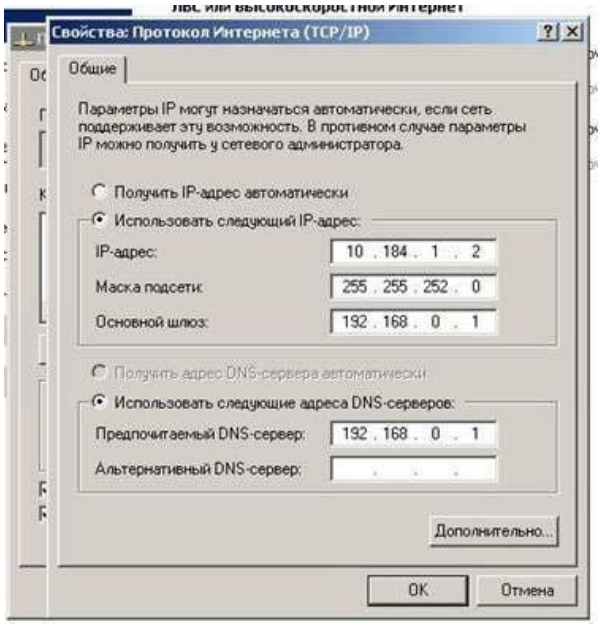
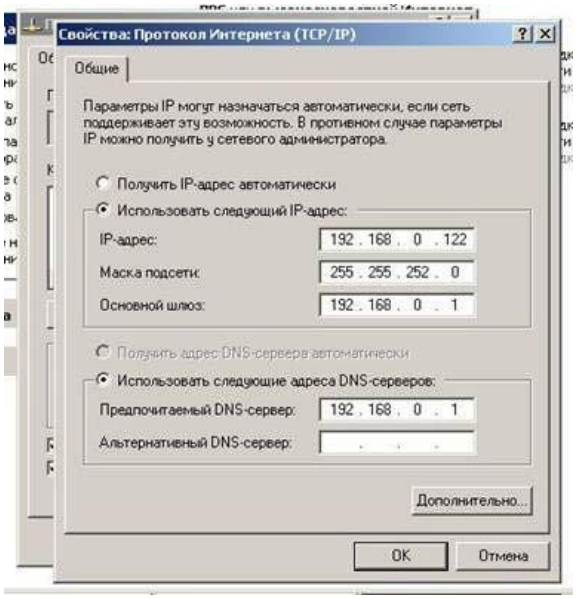


Рис.9: Intranet Ethernet Adapter



4. Для адаптера Bridge Ethernet Adapter:

Рис.10: Bridge Ethernet Adapter

Примечание. Обратите внимание, что все использованные IPv4-адреса берутся из установленного ранее диапазона адресов в DHCP-сервере VirtualBox, при этом используется диапазон от адреса шлюза (192.168.0.1) до верхней границы адресов. Ни в

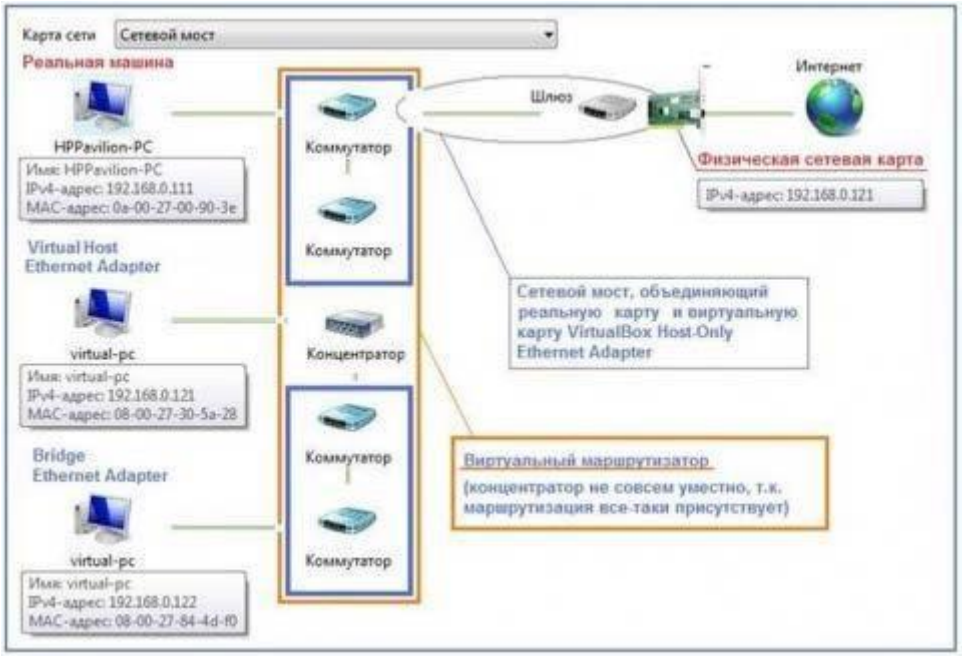
коем случае не выставляйте адреса, не входящие в указанную область. Например,

адаптер виртуальной машины с установленным для него IP-адресом 192.167.0.111 не позволит Вам подключиться настраиваемой сети. Адреса маски подсети, шлюза и DNS- сервера соответствуют адресам, заданным для сетевого моста для host-машины.

После того, как Вы произвели все указанные операции, в системном лотке появится уведомление «Интернет сейчас подключен», но это мы проверим в самом конце.

Настройка рабочих групп

После проведенных нами операций перезагружаем сначала виртуальную машину, а затем и host-машину. После



того как наша реальная операционная система загрузилась, запускаем VirtualBox и включаем нашу виртуальную машину и на host- машине (Windows Vista) открываем «Карту сети»:

Рис.11: «Карта сети» после настроек виртуальной машины

Тут мы видим host-машину (HPPavilion-PC) и подключенную через два адаптера (Bridge Ethernet Adapter и Virtual Host-Only Ethernet Adapter) виртуальную машину

(VirtualPC). Для большей наглядности на изображении приведены краткие комментарии.

Самое главное – мы видим наши обе машины, то же самое можно определить, запустив сеанс командной строки на обеих машинах и выполнив в нем команду **net view**. На

изображении ниже (рис.12) приведены результаты отработки данной команды – справа для Windows Vista, слева для Windows XP.

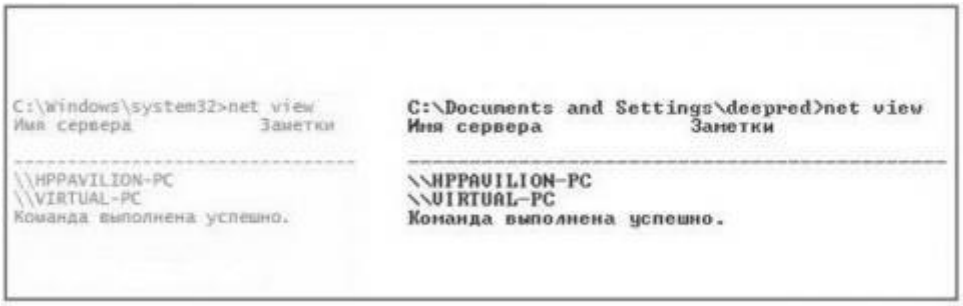


Рис.12: Результат выполнения команды net view

Теперь определимся с рабочими группами – в сети Интернет часто приводится некое требование, согласно которому обе машины должны находиться в одной рабочей группе, но это не так. В нашем случае рабочие группы разные, т.к. по

умолчанию ОС Windows XP включена в Workgroup, а Windows Vista в MShome.

Чтобы увидеть, что это означает, перейдем в папку «Сетевое окружение» на нашей виртуальной машине. В данном расположении мы видим две рабочие группы - Workgroup и MShome:

Рис.13: Разные рабочие группы

Откроем рабочую группу MShome и увидим нашу host-машину (HPPavilion-PC).

Рис.14: Рабочая группа MShome и host-машина (HPPavilion-PC).

Вернемся на шаг назад и откроем рабочую группу Workgroup, в ней мы увидим нашу виртуальную машину (Virtual-PC).

Рис.15: Рабочая группа Workgroup и виртуальная машина (Virtual-PC).

Несмотря на то, что все работает, перенесем Virtual-PC, т.е. нашу виртуальную машину, в ту же рабочую группу, что и host-машина (HPPavilion-PC). Для этого откроем

свойства Мой Компьютер, перейдем на вкладку «Имя компьютера» и нажмем кнопку

«Изменить». В открывшемся окне в поле «Рабочая группа» введем имя рабочей группы, в которой состоит реальная машина (в нашем случае MShome), чтобы увидеть результат перейдем в папку «Сетевое окружение» обеих машин и убедимся, что обе станции находятся в одной рабочей группе. Посмотрим, что у нас получилось сначала на нашей виртуальной машине Windows XP:

Рис.16: Общая рабочая группа на виртуальной машине А теперь на host-машине Windows Vista:

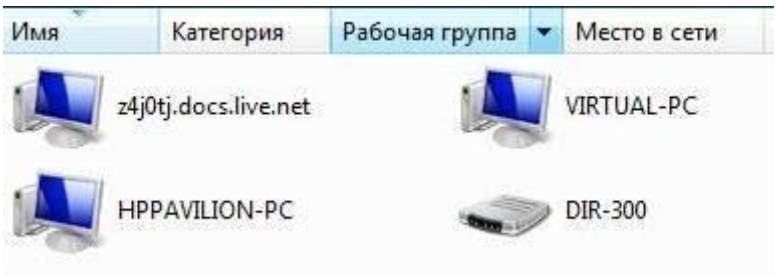


Рис.17: Общая рабочая группа на host-машине

Завершение настройки

Конечно, использовать все четыре адаптера в виртуальной машине нет никакого смысла, поэтому мы оставляем только один, но самый нужный - Virtual Host-Only Ethernet Adapter. Для этого на нашей виртуальной машине откроем папку «Сетевые подключения» и отключим ненужные нам интерфейсы. Дополнительно проверим, сохранились ли настройки указанного адаптера, выполнив команду **ipconfig** в окне

командной строки. На изображении ниже приведен вид папки «Сетевые подключения», в которой мы обязательно должны видеть все наши четыре адаптера и Шлюз Интернета, который должен находиться в подключенном состоянии.

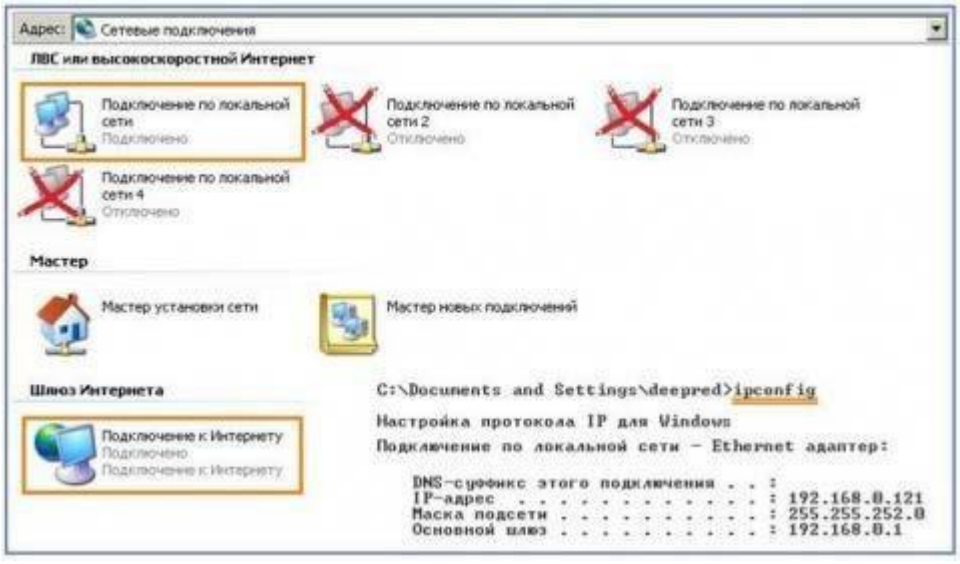
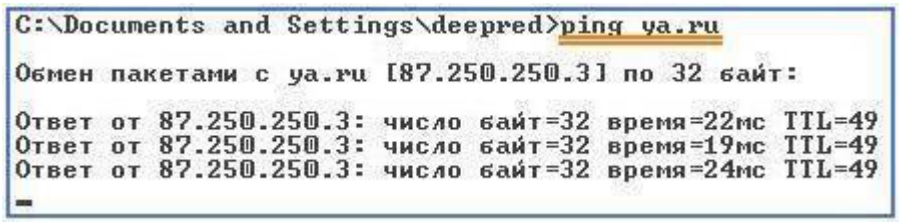


Рис.18: Окончательная конфигурация сетевого интерфейса.

Для того чтобы удостовериться, что подключение к Интернету действительно активно, снова откроем окно командной строки и выполним команду **ping** для узла ya.ru,



результат вывода команды должен быть таким:

Рис.19: Вывод команды ping

Таким образом, все работает, взаимодействует, находится в одной сети, и обе машины имеют доступ к глобальной сети.

Примечание. Если при запуске Вашей host-машины или виртуальной машины Вы обнаружили, что на одной из них или на обеих отсутствует подключение к Интернету, следует проверить настройки Вашего сетевого моста, как правило, проблема заключается в отсутствии записи адреса основного шлюза и решается вводом оного (198.162.0.1).

Практическая работа 2

Тема: Создание схемы сети предприятия. Создание корпоративной сети, настройка служб Web и FTP

Цели: обобщение и систематизация знаний по теме «Разработка корпоративных компьютерных сетей».

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задание:

Краткие теоретические сведения

Программа 10-Strike LANState , позволяет осуществлять мониторинг сетевых служб и устройств, устранять неполадки в их работе, и сокращать простои.

Внезапные сбои в работе ответственных служб и протоколов сервера или активного сетевого оборудования часто оборачивается для компании немалыми убытками и подорванным доверием клиентов. В обязанности системного администратора входит задача своевременного обнаружения таких неполадок и их быстрого устранения. Но справиться с этой задачей без специальных программных инструментов подчас очень нелегко, и, можно сказать, невозможно. Решением проблемы автоматического мониторинга сети является программа 10-Strike LANState. Из под ее контроля не уйдет ни один сбой в работе сетевой службы или протокола. Программа вовремя обнаружит неполадку и сообщит о ней системному администратору.

В основе работы программы лежит механизм периодического выполнения заданных проверок контролируемых служб и протоколов

на серверах и другом сетевом оборудовании. О результате проверок системный администратор оповещается несколькими альтернативными способами: электронной почтой, SMS, звуковым сигналом. Кроме этого, программой ведется фиксация всех событий в журналах с подробной расшифровкой неполадок и временем их происшествия.

10-Strike LANState обладает возможностями мониторинга работы серверов баз данных, систем управления базами данных, значений некоторых параметров производительности сетевого оборудования (например, трафик на коммутаторах), а также оперативного доведения информации до системного администратора о достижении критических значений этих параметров. Для устранения неполадок программа может автоматически выполнить заданные администратором действия: перезагрузку служб и компьютеров, запустить программу или скрипт. Кроме этого, отличительной особенностью 10-Strike LANState является то, что она наглядно отображает контролируемые устройства в виде графической карты сети со связями и условными обозначениями (имеется веб-интерфейс). Карта призвана визуализировать результаты мониторинга, и позволяет быстро определить местонахождение сбойного устройства.

В новой версии 10-Strike LANState реализована возможность отслеживания изменений в списке установленного программного обеспечения на серверах и рабочих станциях локальной сети. Системный администратор будет оповещен о фактах установки пользователями новых программ и удаления старых.

Порядок выполнения работы

Часть I. Построение схемы сети 1. Установите на свой компьютер программу

LANState

2. Запустите программу.

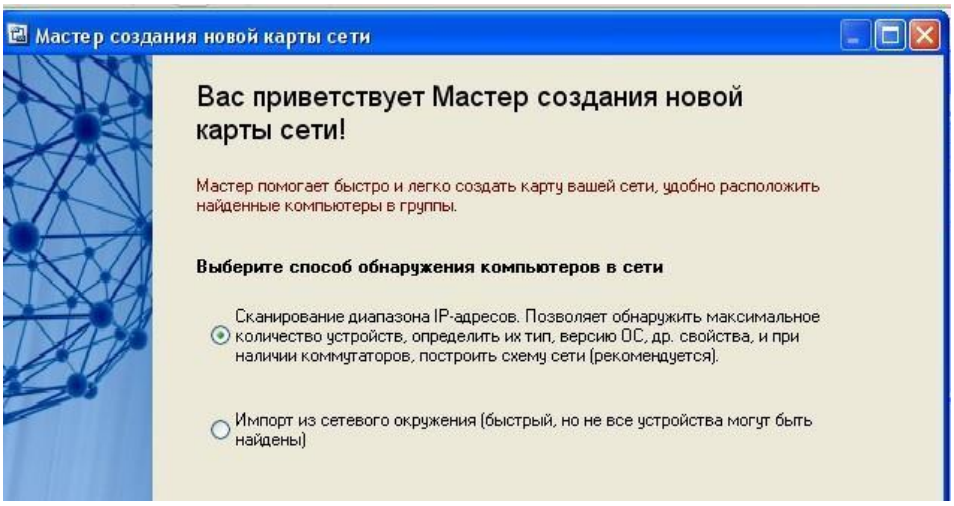
Создание схемы сети автоматически

Начиная с версии 3.3, LANState поддерживает сканирование SNMP-устройств и

может рисовать схему сети автоматически с созданием линий, соединяющих хосты. При этом номера портов коммутаторов проставляются в подписях к линиям.

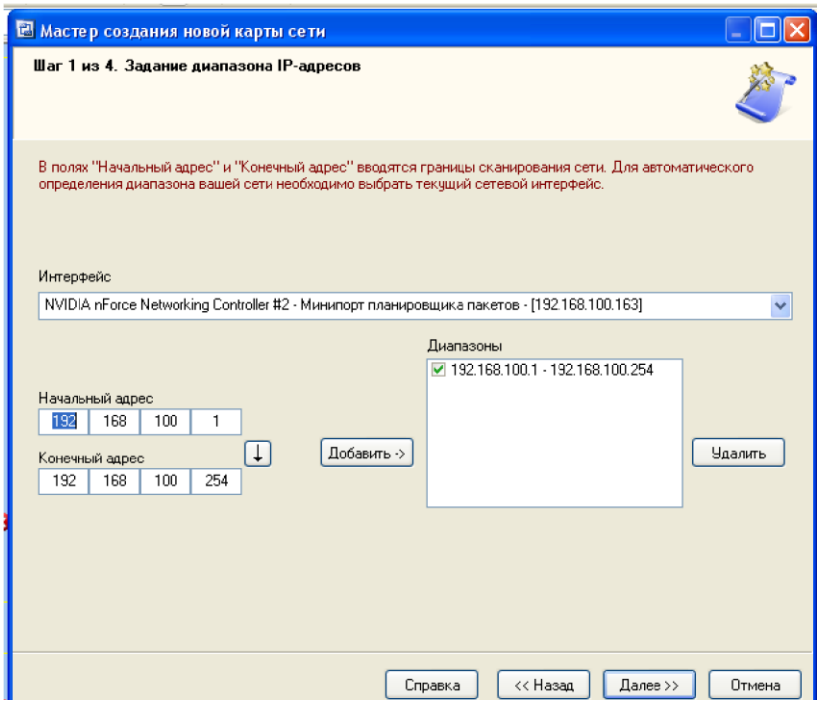
Итак, как построим схему сети автоматически:

1. **SNMP** должен быть включен на коммутаторах. Программа должна быть разрешена в брандмауэре для успешной работы по протоколу SNMP.
2. Запустите **Мастер Создания Карты Сети (Файл – Мастер создания карты)**.

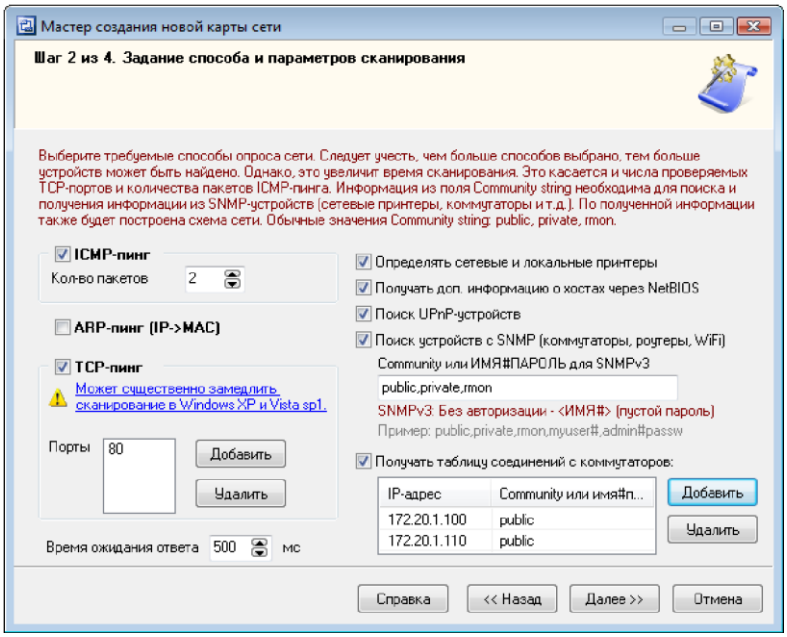


3. В открывшемся окне выберите пункт Сканирование диапазона IP-адресов

4. Выберите сканирование сети по диапазону IP-адресов. Укажите диапазоны (от 192.168.100.1 до 192.168.100.254) Устройства с SNMP должны находиться внутри указанных диапазонов.

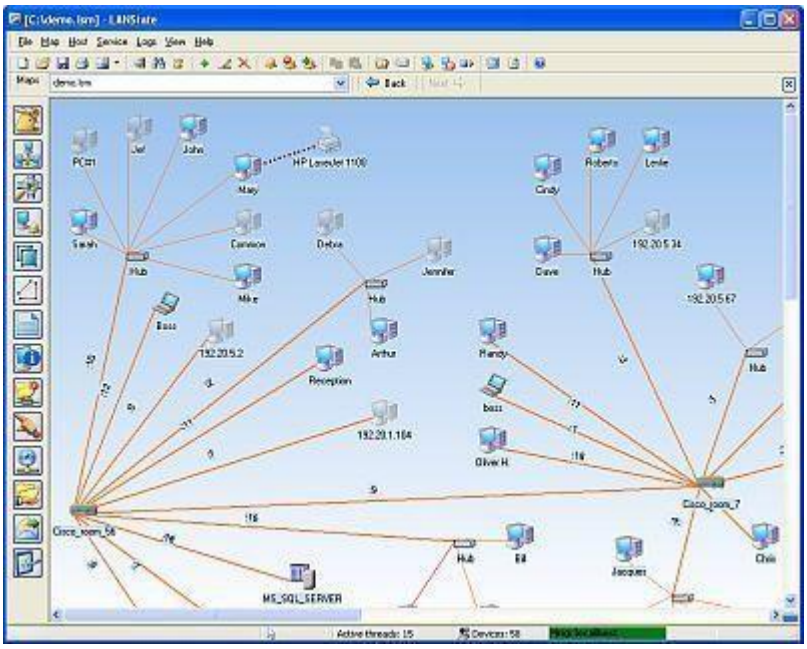


4. Выберите методы сканирования и настройте их параметры. Не забудьте поставить галочку рядом с опцией "**Поиск устройств с SNMP...**" и укажите правильные community strings для подключения к коммутаторам.



-
-

5. После сканирования программа должна нарисовать схему сети. Если сканирование SNMP прошло успешно, соединения между



сетевыми устройствами будут нарисованы автоматически. Передвиньте мышкой устройства для лучшего восприятия схемы.

6. Схема сети может быть выгружена в картинку, либо в схему Microsoft Visio (только в LANState Pro). Полученную схему сохраните в отдельный файл.

Часть II. Построение диаграмм сети

Краткие теоретические сведения

Программа построения диаграмм сети EDraw Network Diagrammer

При проектировании сетей иногда используется EDraw Network Diagrammer – программа создания диаграмм сети с большим количеством примеров и шаблонов.

Основные диаграммы:

- Топологические схемы сети
-
-

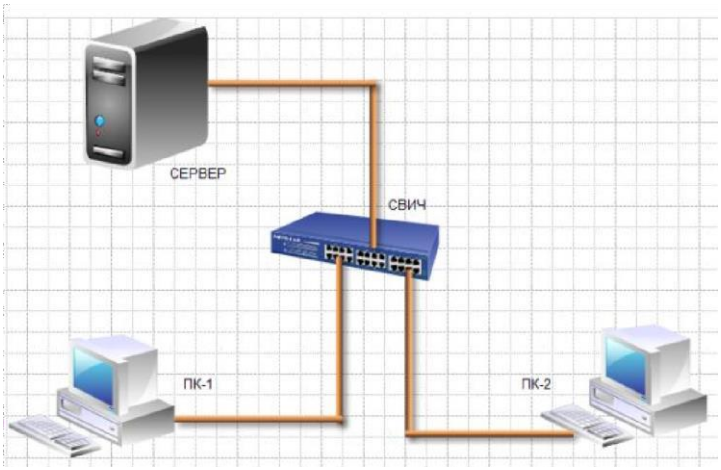
Проектирование сетей Cisco Диаграммы кабельных сетей

Диаграммы LAN (локальная компьютерная сеть) Диаграммы сетей WAN (глобальная сеть)

Сетевая диаграмма (граф сети) - графическое отображение работ проекта сети и их взаимосвязей. Отличием от блок-схемы является то, что сетевая диаграмма

моделирует только логические зависимости между элементарными работами. Она не отображает входы, процессы и выходы.

Программа имеет как сходство с программой 10 Страйк: Схема



Сети, так и принципиальные отличия. Например, в ней можно нарисовать не только изображение сети (рис. 1), но и изображение помещения, где эту сеть планируется установить (рис. 2).

Рис. 1. Пример элементарной схемы сети, выполненной в EDraw Network Diagrammer

Задание 1

1. Постройте схему, изображенную на рисунке 1.
2. Для выбора компьютеров и мониторов из библиотеки (Libraries) нужно выбрать команду **NetworkComputers and Monitors**, а для выбора кабелей – команду **Network and Peripherals**.

Задание 2 Нарисуйте схему помещения, изображенного на рисунке 2.

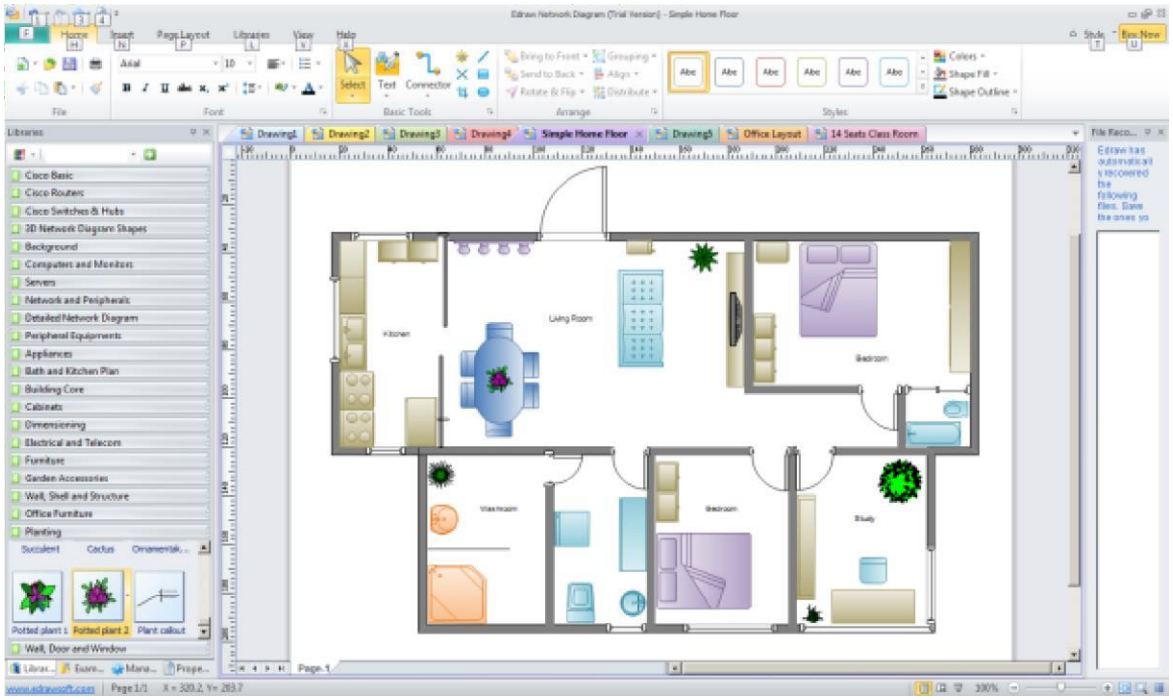
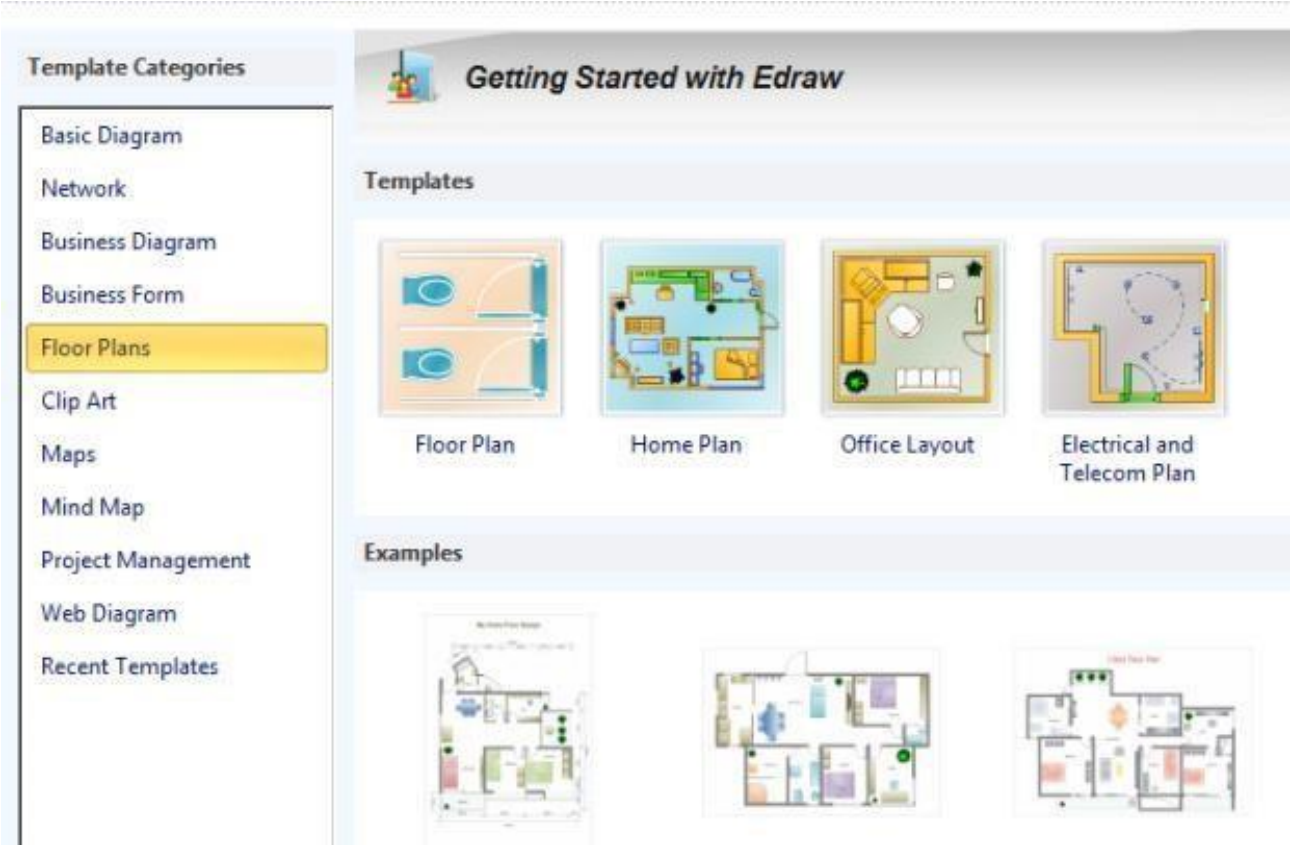


Рис.2. Изображение офисного помещения, нарисованного в EDraw Network Diagrammer



В этом случае из библиотеки нужно выбрать вариант **Floor Plans** (рис. 3).

Рис 3. Различные схемы офисов, для размещения в них ПК

Задание 3. В программе EDraw Network Diagrammer повторите

схему, показанную на рис.4. Поясните, что за устройства присутствуют в данной сети и как они работают.

Рис. 4. Схема сети небольшого офиса

Задание 3. Повторите рисунок, изображающий расположение компьютеров в компьютерном классе

(рис.5).

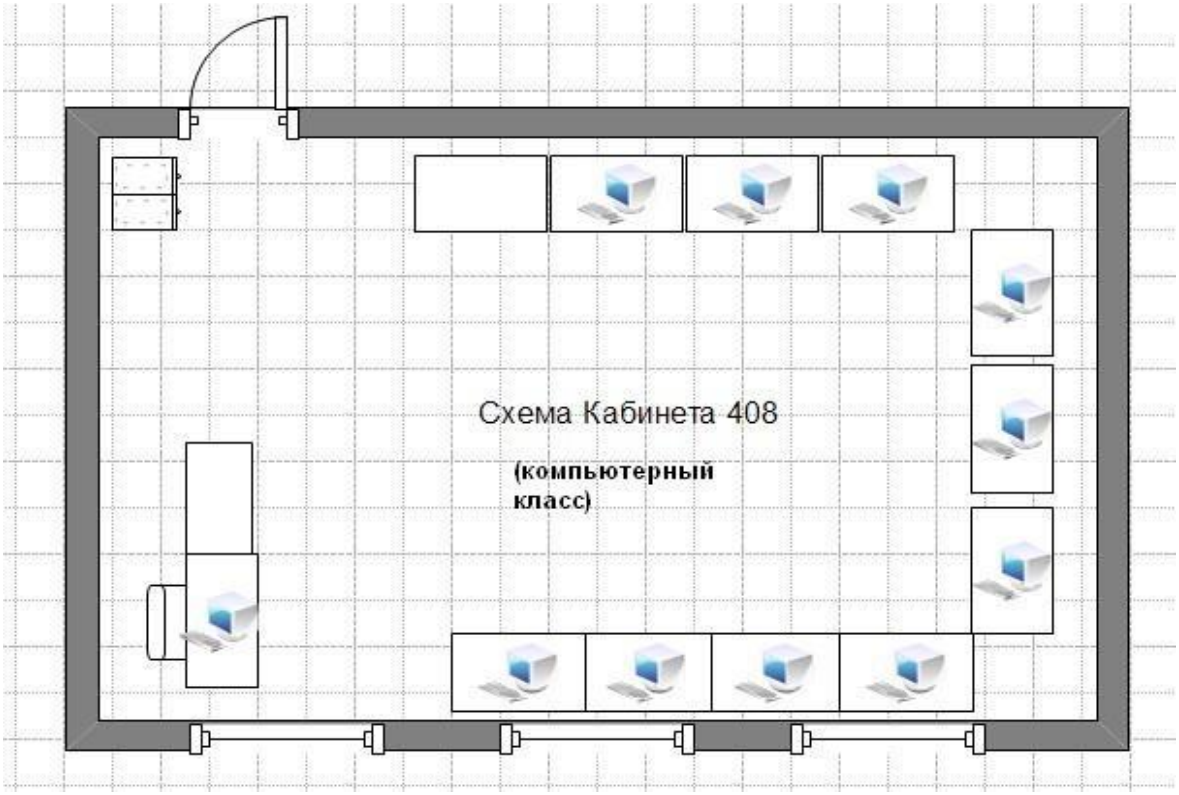


Рис. 5. Расположение компьютеров в компьютерном классе

Контрольное задание

Используя возможности программы **EDraw Network Diagrammer** создайте схему

помещения и расположения компьютерной техники в кабинете № 402 (по аналогии с рис. 5)

Практическая работа 3

Тема: Топологии сети и ROUTING-диаграмма

Цели: Изучить топологии сети и ROUTING-диаграмма

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задание:

Правила маршрутизации

Правила маршрутизации определяют куда и как должны посылаться пакеты для разных сетей.

Каждое правило состоит из следующих компонентов:

- Начальный адрес подсети, порядок достижения которой описывает правило.
- Маска подсети, которую описывает правило.
- Шлюз показывает, на какой адрес будут посланы пакеты, идущие в сеть назначения. Если пакеты будут идти напрямую, то указывается собственный адрес (точнее тот адрес того канала, через который будут передаваться пакеты).
- Интерфейс показывает через какой сетевой адаптер (его номер или IPадрес) должен посылаться пакет в заданную сеть;
- Метрика показывает время за которое пакет может достигнуть сети получателя (величина условная и может быть изменена при маршрутизации). Если имеется несколько правил достижения одной сети, пакеты посылаются по правилу с наименьшей метрикой. Применение правила заключается в определении, принадлежит ли хост назначения сети, указанной в правиле, и если принадлежит, то пакет отправляется на адрес

шлюза через интерфейс.

Правила маршрутизации сведены в таблицу маршрутизации (где расположены по степени уменьшения маски), которую можно посмотреть с помощью команды ROUTE PRINT.

Правила применяются в порядке уменьшения масок.

Правила с равными масками применяются в порядке увеличения метрики.

Пример таблицы маршрутизации

Рассмотрим таблицу маршрутизации, имеющую следующий вид:

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика

0.0.0.0	0.0.0.0	192.168.200.1	192.168.200.47	30
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.192.0	255.255.240.0	192.168.200.47	192.168.200.47	30
192.168.200.47	255.255.255.255	127.0.0.1	127.0.0.1	30
192.168.200.255	255.255.255.255	192.168.200.47	192.168.200.47	30
224.0.0.0	240.0.0.0	192.168.200.47	192.168.200.47	30
255.255.255.255	255.255.255.255	192.168.200.47	192.168.200.47	1

Проанализируем вышеприведенную таблицу маршрутизации, пересортировав правила:

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
255.255.255.255	255.255.255.255	192.168.200.47	192.168.200.47	1
192.168.200.47	255.255.255.255	127.0.0.1	127.0.0.1	30
192.168.200.255	255.255.255.255	192.168.200.47	192.168.200.47	30
192.168.192.0	255.255.240.0	192.168.200.47	192.168.200.47	30
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
224.0.0.0	240.0.0.0	192.168.200.47	192.168.200.47	30
0.0.0.0	0.0.0.0	192.168.200.1	192.168.200.47	30

255.255.255.255	255.255.255.255	192.168.200.47	192.168.200.47	1

Обратите внимание на маску сети в первом правиле. Она описывает подсеть размером в 1 хост с адресом 255.255.255.255 – это широковещательный адрес. Пакеты будут посылаться на адрес 192.168.200.47 через интерфейс 192.168.200.47. Это наш адрес, т.е. пакеты будут отправляться напрямую.

192.168.200.255	255.255.255.255	192.168.200.47	192.168.200.47	30

Опять широковещательный адрес. Смотри предыдущий комментарий.

192.168.200.47	255.255.255.255	127.0.0.1	127.0.0.1	30

Опять такая же маска, но адрес нашего хоста. Отправлять будем через внутреннюю петлю.

192.168.192.0	255.255.240.0	192.168.200.47	192.168.200.47	30

А вот и наша подсеть. Отправляем напрямую.

127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1

Все, что начинается со 127, отправляем через внутреннюю петлю.

224.0.0.0	240.0.0.0	192.168.200.47	192.168.200.47	30

Класс D – отправляем напрямую.

0.0.0.0	0.0.0.0	192.168.200.1	192.168.200.47	30

Самое интересное правило. Маска покрывает ВСЕ возможные адреса! Пакеты отправляются через наш интерфейс на адрес 192.168.200.1. Правило применяется последним, поэтому его можно озвучить так: по всем адресам, которые не подошли по предыдущим правилам, пакеты отправляем на адрес 192.168.200.1. Такой адрес обычно имеется в любой сети и называется шлюзом по умолчанию (default gateway). Этот адрес скрывает от хостов и пользователей структуру сети и позволяет упростить таблицы маршрутизации и снять нагрузку с хостов, перенеся маршрутизацию на специально выделенные шлюзы – маршрутизаторы.

Нетрудно догадаться, что все адреса в колонке Адрес шлюза должны достигаться напрямую, т.е. входить в нашу подсеть.

Разбиение сети на подсети

Одной из основных задач, стоящих при проектировании сетей, является распределение по подсетям сетевых адресов из заданного диапазона, т.е. разделение сети на подсети.

При разделении сети на подсети следует учитывать следующие правила:

- Размер подсетей должен быть степенью двойки.
- Имеются запрещенные адреса.
- Начальный адрес подсети должен быть кратен ее размеру.

В качестве шлюза по умолчанию можно использовать любой узел, но, исходя из увеличения пропускной способности сети и уменьшения времени передачи пакетов, следует в качестве шлюза по умолчанию использовать либо ближайший узел, либо узел, соединенный с максимальным количеством сетей, т.е. следует учитывать топологию сети.

Программа ROUTE

Для работы с таблицами маршрутизации в составе ОС имеется программа route (упоминалась ранее). Выводит на экран и изменяет записи в локальной таблице IP-маршрутизации.

route [-f] [-p] [команда [конечная_точка] [mask маска_сети] [шлюз] [metric метрика]] [if интерфейс]]

Параметры:

-f – Очищает таблицу маршрутизации от всех записей, которые не являются узловыми маршрутами (маршруты с маской подсети 255.255.255.255), сетевым маршрутом замыкания на себя (маршруты с конечной точкой 127.0.0.0 и маской подсети 255.0.0.0) или маршрутом многоадресной рассылки (маршруты с конечной точкой 224.0.0.0 и маской подсети

240.0.0.0). При использовании данного параметра совместно с одной из команд (таких, как add, change или delete) таблица очищается перед выполнением команды.

-p – При использовании данного параметра с командой add указанный маршрут добавляется в реестр и используется для инициализации таблицы IP-маршрутизации каждый раз при запуске протокола TCP/IP. При использовании параметра с командой print выводит на экран список постоянных маршрутов. Все другие команды игнорируют этот параметр.

команда – Указывает команду, которая будет запущена на удаленной системе. В следующей таблице представлен список допустимых параметров.

Команда	Назначение
Add	Добавление маршрута
change	Изменение существующего маршрута
Delete	Удаление маршрута или маршрутов
Print	Печать маршрута или маршрутов

конечная_точка – Определяет конечную точку маршрута. Конечной точкой может быть сетевой IP-адрес (где разряды узла в сетевом адресе имеют значение 0), IP-адрес маршрута к узлу, или значение 0.0.0.0 для маршрута по умолчанию.

mask маска_сети – Указывает маску сети в соответствии с точкой назначения. Маска сети может быть маской подсети соответствующей сетевому

шлюз – Указывает IP-адрес пересылки или следующего перехода, по которому доступен набор адресов, определенный конечной точкой и маской подсети

metric метрика – Задает целочисленную метрику стоимости маршрута (в пределах от 1 до 9999) для маршрута, которая используется при выборе в таблице маршрутизации одного из нескольких маршрутов, наиболее близко соответствующего адресу назначения пересылаемого пакета.

if интерфейс – Указывает индекс интерфейса, через который доступна точка назначения. В случае, когда параметр if пропущен, интерфейс определяется из адреса шлюза.

/? – Отображает справку в командной строке.

2. **Выполнить задания**

1) С помощью программы route print посмотрите таблицу маршрутизации Вашего компьютера. Объясните все правила.
2) Посмотрите таблицу маршрутизации хоста, имеющего несколько каналов. Объясните все правила.
3) Посмотрите таблицу маршрутизации маршрутизатора. Объясните все правила.
4) Добавьте новое правило в таблицу маршрутизации для сети 192.168.0.0/24 через шлюз в вашей сети с последним байтом в адресе 125 и метрикой 12.
5) Удалите это правило.
6) В соответствии с таблицей и схемами выполните задание на распределение адресов по подсетям (согласно варианта). Постройте таблицы маршрутизации для всех шлюзов и для одного хоста для каждого сегмента.

№ Варианта	Количество хостов в подсети					Диапазон адресов	
	A	B	C	D	E	от	до

1	5	10	20	15	50	10.0.20.0	10.0.20.255
2	20	15	6	70	25	192.168.0.0	192.168.0.255
3	15	25	5	40	5	112.38.25.128	112.38.25.255
4	24	32	8	10	2	196.13.49.0	196.13.49.128
5	50	16	64	20	15	68.76.115.0	68.76.115.255
6	40	6	10	12	5	211.3.45.0	211.3.45.128

7) Разделите сеть, состоящую из трех сегментов, имеющую диапазон адресов 192.168.0.32 – 192.168.0.159 на подсети, содержащие 64, 20 и 44 хостов (включая шлюзы).

Практическая работа 4

Тема: Глобальная сеть интернет

Цели: Изучение основных функциональных возможностей, предоставляемых глобальной сетью Интернет, и общей методологией их использования в медицинских информационных системах.

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

1. Порядок выполнения работы

1. Самостоятельно изучить основные сведения глобальной сети Интернет (см. раздел 3).
2. Получить допуск к выполнению практической работы, ответив на вопросы преподавателя или пройдя компьютерное тестирование.
3. Выполнить задания к практической работе, приведенные в разделе 4.
4. Выполнить индивидуальное задание согласно варианту, выданному преподавателем.
5. Оформить отчет по результатам выполнения индивидуального задания.
6. Защитить результаты работы.

3. Общие сведения о глобальной сети Интернет

Компьютерные вычислительные сети

История развития глобальных компьютерных сетей

Разработка компьютерных сетей велась во многих странах, и в частности, в СССР и России, начиная с конца 50-х годов. Так, в Санкт-Петербурге в Институте информатики и автоматизации Академии Наук проводилась большая работа по созданию «Академсети»; в ЦНИИ робототехники и технической кибернетики продолжаются работы по созданию сверхскоростных линий передачи данных; велись и ведутся работы в других организациях. Долгое время в России и СССР основной и практически единственной региональной сетью была сеть Релком.

В это же время в мире постепенно складывалась глобальная компьютерная сеть. Как же возникла эта сеть сетей? Подобно многим самым совершенным технологиям сегодняшнего дня она развилась из военных проектов.

Все началось в 60-х годах с проводившихся в Агентстве перспективных исследований США (Advanced Research Projects Agency — ARPA) научных разработок. Правительство США поставило задачу и финансировало работу по развитию сети, позволяющей обеспечивать связь во время ядерной войны. Пакеты информации должны были передаваться на различных уровнях системы, которые постоянно функционировали бы даже в условиях уничтожения ее центра управления.

В 1968 г. основные принципы построения децентрализованных сетей были опробованы в Национальной физической лаборатории в Великобритании.

Первая крупная национальная сеть США была образована в 1969 г. соединением 4 академических компьютерных центров (Калифорнийского университета в Санта-Барбаре, Калифорнийского университета в Лос-Анджелесе, университета штата Юта и Стэндфордского университета) с помощью специального телефонного кабеля со скоростью передачи 56000 бит/с. Эта основа получила тогда название ARPAnet. Спустя некоторое время все больше компьютеров стало подключаться к ARPAnet, формируя все увеличивающуюся сеть. К 1980 г. сеть объединяла 200 компьютеров которые были подключены к 5 суперкомпьютерам Национального научного фонда (National Science Foundation — NSF). Ученые по всей территории США могли использовать вычислительные ресурсы суперкомпьютеров, если они подключались к NSFnet. По мере того, как все больше сетей подключалось к ARPAnet, обеспечивая их межсетевое взаимодействие, эту общую сеть стали называть Интернет (Internet), что означает "между сетей". К маю 1994 более 2,2 млн. компьютеров были включены в Интернет, к которому имело доступ более 25 млн. человек. В настоящее время число пользователей, возможно, составляет более 100 млн. человек!

Распределенная обработка данных

Современная медицина требует высоких скоростей обработки информации, удобных форм ее хранения и передачи. Необходимо также иметь динамичные способы обращения к информации, способы поиска данных в заданные временные интервалы; реализовывать сложную

математическую и логическую обработку данных. Управление медицинскими предприятиями, управление медициной на уровне страны требуют участия в этом процессе достаточно крупных коллективов. Такие коллективы могут располагаться в различных районах города, в различных регионах страны и даже в различных странах. Для решения задач управления, обеспечивающих реализацию экономической стратегии, становятся важными и актуальными скорость и

удобство обмена информацией, а также возможность тесного взаимодействия всех участвующих в процессе выработки управленческих решений.

В эпоху централизованного использования ЭВМ с пакетной обработкой информации пользователи вычислительной техники предпочитали приобретать компьютеры, на которых можно было бы решать почти все классы их задач. Однако сложность решаемых задач обратно пропорциональна их количеству, и это приводило к неэффективному использованию вычислительной мощности ЭВМ при значительных материальных затратах. Нельзя не учитывать и тот факт, что доступ к ресурсам компьютеров был затруднен из-за существующей политики централизации вычислительных средств в одном месте.

Компьютерная (вычислительная) сеть — совокупность компьютеров и терминалов, соединенных с помощью каналов связи в единую систему, удовлетворяющую требованиям распределенной обработки данных.

С течением времени различные производители разрабатывают программы для быстрого и удобного обмена информацией. Особенно в современный период развития медицины, где информация играет очень важную роль. Одной из таких программ

стал Skype. Эта программа позволяет почти бесплатно связаться с человеком на другом конце света, что облегчает передачу информации. Так же эта программа позволяет передавать файлы, правда на малой скорости и, соответственно, малого объёма. Skype является бесплатной программой, которую можно скачать при помощи браузеров, о которых мы поговорим чуть позже.

Классификация вычислительных сетей

В зависимости от территориального расположения абонентских систем вычислительные сети можно разделить на три основных класса:

- глобальные сети (WAN — Wide Area Network);
- региональные сети (MAN — Metropolitan Area Network);
- локальные сети (LAN — Local Area Network).

Глобальная вычислительная сеть объединяет абонентов, расположенных в различных странах, на различных континентах. Взаимодействие между абонентами такой сети может осуществляться на базе телефонных линий связи, радиосвязи и систем спутниковой связи. Глобальные вычислительные сети позволят решить проблему объединения информационных ресурсов всего человечества и организации доступа к этим ресурсам.

Региональная вычислительная сеть связывает абонентов, расположенных на значительном расстоянии друг от друга. Она может включать абонентов внутри большого города, экономического региона, отдельной страны. Обычно расстояние между абонентами региональной вычислительной сети составляет десятки — сотни километров.

Локальная вычислительная сеть объединяет абонентов, расположенных в пределах небольшой территории. В настоящее

время не существует четких ограничений на территориальный разброс абонентов локальной вычислительной сети. Обычно такая сеть привязана к конкретному месту. К классу локальных вычислительных сетей относятся сети отдельных предприятий, фирм, банков, офисов и т.д. Протяженность такой сети можно ограничить пределами 2 - 2,5 км. Аппаратное обеспечение локальной вычислительной сети включает рабочие станции, сервер, коммуникационное оборудование. Топологиями локальных вычислительных сетей являются: звезда, шина, кольцо.

Объединение глобальных, региональных и локальных вычислительных сетей позволяет создавать многосетевые иерархии. Они обеспечивают мощные, экономически целесообразные средства обработки огромных информационных массивов и доступ к неограниченным информационным ресурсам. На рис. 3.2 приведена одна из возможных иерархий вычислительных сетей. Локальные вычислительные сети могут входить как компоненты в состав региональной сети, региональные сети — объединяться в составе глобальной сети и, наконец, глобальные сети могут также образовывать сложные структуры.

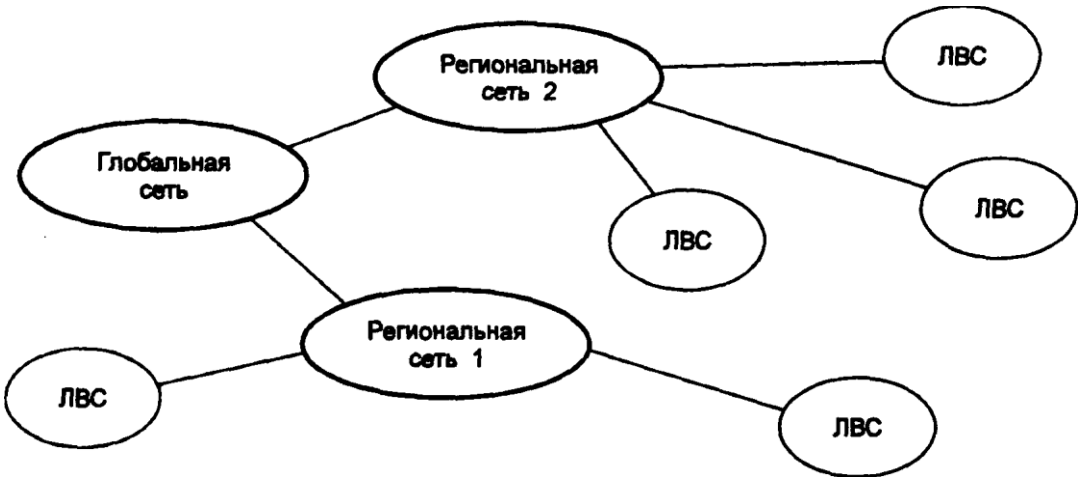


Рис. 3.2. Иерархия компьютерных сетей

Пример. Компьютерная сеть Internet является наиболее популярной глобальной сетью. В ее состав входит множество свободно соединенных сетей. Внутри каждой сети, входящей в Internet, существуют

конкретная структура связи и определенная дисциплина управления. Внутри Internet структура и методы соединений между различными сетями для конкретного пользователя не имеют никакого значения.

Персональные компьютеры, ставшие в настоящее время непременным элементом любой системы управления, привели к буму в области создания локальных вычислительных сетей. Это, в свою очередь, вызвало необходимость в разработке новых информационных технологий.

Практика применения персональных компьютеров в различных отраслях науки, техники и производства показала, что наибольшую эффективность от внедрения вычислительной техники обеспечивают не отдельные автономные ПК, а локальные вычислительные сети.

Сетевые операционные системы – это комплекс программ, которые обеспечивают одновременную работу группы пользователей.

Структура Internet

Internet представляет собой глобальную компьютерную сеть. Само ее название означает "между сетей".

Это сеть, соединяющая отдельные сети.

Логическая структура Internet представляет собой некое виртуальное объединение, имеющее свое собственное информационное пространство.

Internet обеспечивает обмен информацией между всеми компьютерами, которые входят в сети, подключенные к ней. Тип компьютера и используемая им операционная система значения не имеют. Соединение сетей обладает громадными возможностями. С собственного компьютера любой абонент Internet может передавать сообщения в другой город, просматривать каталог библиотеки Конгресса в Вашингтоне, знакомиться с картинами на последней выставке в музее Метрополитен в Нью-Йорке, участвовать в конференции IEEE и даже в играх с абонентами сети из разных стран. Internet предоставляет в распоряжение своим пользователям множество всевозможных ресурсов.

Основные ячейки Internet — локальные вычислительные сети. Это значит, что Internet не просто устанавливает связь между отдельными компьютерами, а создает пути соединения для более крупных единиц

— групп компьютеров. Если некоторая локальная сеть непосредственно подключена к Internet, то каждая рабочая станция этой сети также может подключаться к Internet. Существуют также компьютеры, самостоятельно подключенные к Internet. Они называются хост-компьютерами (host — хозяин). Каждый подключенный к сети компьютер имеет свой адрес, по которому его может найти абонент из любой точки света.

Важной особенностью Internet является то, что она, объединяя различные сети, не создает при этом никакой иерархии — все компьютеры, подключенные к сети, равноправны. Для иллюстрации возможной структуры некоторого участка сети Internet приведена схема соединения различных сетей (рис. 3.1).

Мост – это устройство, соединяющее две сети, использующие одинаковые методы передачи данных. Устройство, обеспечивающее соединение административно независимых коммуникационных сетей, – это роутер.

Шлюз – это устройство, которое позволяет организовать обмен данными между двумя сетями, использующими различные протоколы взаимодействия.

Прокси-сервер сети Интернет обеспечивает анонимизацию доступа к различным ресурсам.

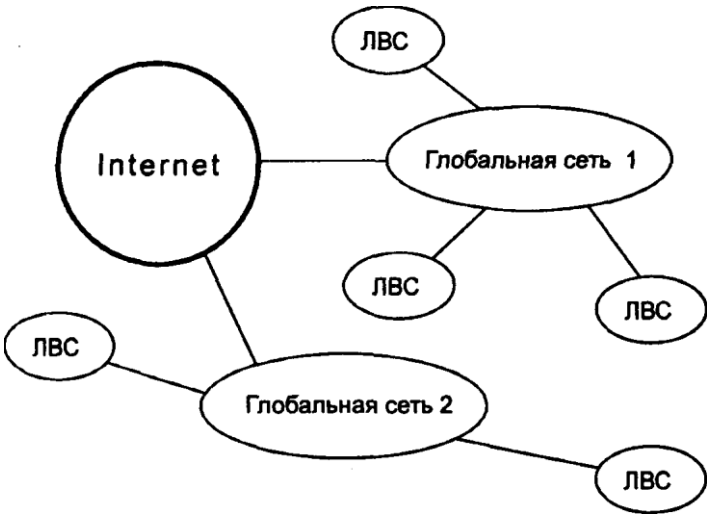


Рис. 3.1. Подключение различных сетей к Internet

Система адресации в Internet

Internet самостоятельно осуществляет передачу данных. К адресам станций предъявляются специальные требования. Адрес должен иметь формат, позволяющий вести его обработку автоматически, и должен нести некоторую информацию о своем владельце.

С этой целью для каждого компьютера устанавливаются два адреса: цифровой IP-адрес (IP — Internetwork Protocol — межсетевой протокол) и доменный адрес.

Оба эти адреса могут применяться равноценно. Цифровой адрес удобен для обработки на компьютере, а доменный адрес — для восприятия пользователем.

Для пользователей числовой IP-адрес все же неудобен, поэтому была придумана доменная система обозначения компьютеров. Компьютеры теперь можно обозначать не трудными для запоминания цифрами, а словами (именами), при этом сеть оказалась поделенной на части, называемые *доменами* (лат. dominium — владение). Домены даются во "владение" различным организациям, которые отвечают за их поддержку. Домены могут быть вложены друг в друга, т.е. организация, отвечающая за более крупный домен, имеет право назначать более мелкие в пределах этого домена.

Цифровой адрес имеет длину 32 бита. Для удобства он разделяется на четыре блока по 8 бит, которые можно записать в десятичном виде. Адрес содержит полную информацию, необходимую для идентификации компьютера.

Два блока определяют адрес сети, а два другие — адрес компьютера внутри этой сети. Существует определенное правило для установления границы между этими адресами. Поэтому IP-адрес включает в себя три компонента: адрес сети, адрес подсети, адрес компьютера в подсети.

Пример. В двоичном коде цифровой адрес записывается следующим образом: 10000000001011010000100110001000. В

десятичном коде он имеет вид: 192.45.9.200. Адрес сети —192.45; адрес подсети — 9; адрес компьютера — 200.

Доменный адрес определяет область, представляющую ряд хост-компьютеров. В отличие от цифрового адреса он читается в обратном порядке. Вначале идет имя компьютера, затем имя сети, в которой он находится. Надо отметить, что компьютеры, к которым подключаются пользователи, часто называют *хост-компьютерами,* и они имеют один (или несколько) постоянных адресов в Интернет, а компьютеры пользователей обычно при каждом сеансе связи получают новые адреса, хотя могут иметь и постоянные.

Чтобы абонентам Internet можно было достаточно просто связаться друг с другом, все пространство ее адресов разделяется на области — домены. Возможно также разделение по определенным признакам и внутри доменов.

В системе адресов Internet приняты домены, представленные географическими регионами. Они имеют имя, состоящее из двух букв.

Пример. Географические домены некоторых стран: Франция — fr; Канада — ca; США — us; Россия — ru.

Существуют и домены, разделенные по тематическим признакам. Такие домены имеют трехбуквенное

сокращенное название.

Пример. Учебные заведения — edu. Правительственные учреждения — gov. Коммерческие организации — corn.

Компьютерное имя включает, как минимум, два уровня доменов. Каждый уровень отделяется от другого точкой. Слева от домена верхнего уровня располагаются другие имена. Все имена, находящиеся слева, — поддомены для общего домена.

Пример. Существует имя medic.pnzgu.ru. Здесь ru — географический домен Российской Федерации. pnzgu — домен Пензенского государственного университета, medic — поддомен кафедры «Медицинские информационные системы и технологии».

Для пользователей Internet адресами могут быть просто их регистрационные имена на компьютере, подключенном к сети. За именем следует знак @. Все это слева присоединяется к имени компьютера.

В Internet могут использоваться не только имена отдельных людей, но и имена групп. Для обработки пути поиска в доменах имеются специальные серверы имен. Они преобразовывают доменное имя в соответствующий цифровой адрес.

Локальный сервер передает запрос на глобальный сервер, имеющий связь с другими локальными серверами имен. Поэтому пользователю просто нет никакой необходимости знать цифровые адреса.

Для выхода в Internet вы должны знать адрес домена, с которым хотите установить связь.

Пользователи узлов (компьютеров сети Интернет), входящих в состав WWW, общаются между собой на основе протокола HTTP (Hyper Text Transfer Protocol). Этот протокол задает правила общения между программой просмотра Web-страниц и WWW-сервером, которые укладываются в схему "запрос — ответ".

Указывая доменный адрес сервера и вид протокола (HTTP), мы тем самым запрашиваем определенную услугу: найти на сервере в нужном месте нужный нам HTML-документ. В простейшем случае программа просмотра Web-страниц требует некий документ, и сервер его выдает. Таким образом, чтобы просмотреть нужную вам Web-страницу, вы должны в адресном поле программы просмотра Web-страниц написать требуемый адрес (например, **http://www.rambler.ru)** и нажать на клавиатуре клавишу <Enter>.

Способы организации передачи информации

TCP/IP позволяет только передавать информацию, а использованием ее занимаются сервисы, которые можно условно разделить на интерактивные, прямые и отложенные.

Интерактивные сервисы Internet требуют быстрого реагирования. Например, сервис IRC — Internet Relay Chat — разговоры через Internet посредством специальных серверов. Пользователи присоединяются к одному из каналов тематических групп и участвуют в разговоре, который ведется путем набора текста. Синхронизация узлов IRC позволяет, подключившись к одному из них, участвовать во всей сети IRC.

Прямые сервисы характеризуются тем, что информация к клиенту возвращается немедленно, но может

быть отложена на неопределенный срок для ознакомления. Например, документы WWW (World Wide Web). WWW — это самый популярный сервис Internet, является системой представления и обмена информацией, дает возможность визуального восприятия информации в Сети. Основа WWW — гипермедийный документ, в ко- тором каждый элемент может являться ссылкой на другой документ или его часть.

Гипермедийные документы, из которых в основном состоит Internet, называются Web-страницами, а их тематические совокупности — Web-сайтами. Сайтом называют некую совокупность страниц, объединенных по смыслу и/или по оформлению. Ссылки организованы таким образом, что любой информационный ресурс в Internet адресуется однозначно.

Цифровая подпись используется для того, чтобы получатель сообщения знал, что это то самое письмо, а не какое либо иное. Для того чтобы наладить обмен электронными сообщениями, имеющими цифровую подпись, необходимо передать получателю сообщений открытый ключ шифрования.

В Интернете используются различные сервисы: электронная почта, телеконференции, Интернет- пейджер, Интернет-магазин и т.д. Сервисная система, при помощи которой можно общаться через сеть Интернет с другими людьми в режиме реального времени, имеет наименование IRC.

Отложенные сервисы характеризуются тем, что запрос и получение информации могут быть разделены по времени на неопределенный срок. Например, электронная почта.

Электронная почта

Электронная почта (e-mail — electronic mail) выполняет функции обычной почты. Она обеспечивает передачу сообщений из одного пункта в другой. Главным ее преимуществом является независимость от времени. Электронное письмо приходит сразу же после его отправления и хранится в почтовом ящике до получения адресатом. Кроме текста оно может содержать графические и звуковые файлы, а также двоичные файлы — программы.

Электронные письма могут отправляться сразу по нескольким адресам. Пользователь Internet с помощью электронной почты получает доступ к различным услугам сети, так как основные сервисные программы Internet имеют интерфейс с ней. Суть такого подхода заключается в том, что на хост-компьютер отправляется запрос в виде электронного письма. Текст письма содержит набор стандартных формулировок, которые и обеспечивают доступ к нужным функциям. Такое сообщение воспринимается компьютером как команда и выполняется им.

Для работы с электронной почтой создано большое количество программ. Их можно объединить под обобщающим названием mail. Так, для работы пользователей в MS DOS применяется программа bml, наиболее распространенной программой для Unix-систем является программа elm. Пожалуй, одна из наиболее удобных и несложных в использовании программ — Eudora для Microsoft Windows. В операционной системе Windows 95 работу с электронной почтой обеспечивает приложение Microsoft Exchange. Эти программы выполняют следующие функции:

- подготовку текста;
- чтение и сохранение корреспонденции;
- удаление корреспонденции;
- ввод адреса;
- комментирование и пересылку корреспонденции;
- импорт (прием и преобразование в нужный формат) других файлов.

Сообщения можно обрабатывать собственным текстовым редактором программы электронной почты. Из-за ограниченности его возможностей обработку текстов большого размера лучше выполнять внешним редактором. При отправке такого текста программа электронной почты дает возможность его обработать.

Обычно программы электронной почты пересылают тексты в коде ASCII и в двоичном формате. Код ASCII позволяет записывать только текст и не дает возможности передавать информацию об особенностях национальных шрифтов.

В двоичных файлах сохраняется любая информация. Поэтому для передачи комбинированных сообщений (графика и текст), а также для передачи программ используются двоичные файлы.

При участии в дискуссиях или в составлении рассылочных списков необходимо оформлять сообщения в коде ASCII. Сообщения, записанные другими программами, можно отправлять, точно зная, что у абонента есть такая же программа.

При отправлении сообщений по электронной почте необходимо указывать в адресе не только имя хост-компьютера, но и имя абонента, которому сообщение предназначено.

Формат адреса электронной почты должен иметь вид:

имя пользователя@адрес хост-компьютера

Для каждого пользователя на одном хост-компьютере может быть заведен свой каталог для получения сообщений по электронной почте.

Специальный стандарт MIME (Multipurpose Internet Mail Extension) — многоцелевое расширение почты Internet — позволяет вкладывать в символьные сообщения любые двоичные файлы, включая графику, аудио- и видеофайлы.

World-Wide-Web (Всемирная информационная сеть)

WWW является одной из самых популярных информационных служб Internet. Две основные особенности отличают WWW: использование

гипертекста и возможность клиентов взаимодействовать с другими приложениями Internet.

Гипертекст — текст, содержащий в себе связи с другими текстами, графической, видео- или звуковой информацией.

Внутри гипертекстового документа некоторые фрагменты текста четко выделены. Указание на них с помощью, например, мыши позволяет перейти на другую часть этого же документа, на другой документ в этом же компьютере или даже на документы на любом другом компьютере, подключенном к Internet.

Все серверы WWW используют специальный язык HTML (Hypertext Markup Language — язык разметки гипертекста). HTML-документы представляют собой текстовые файлы, в которые встроены специальные команды.

WWW обеспечивает доступ к сети как клиентам, требующим только текстовый режим, так и клиентам, предпочитающим работу в режиме графики. В первом случае используется программа Lynx, во втором — Mosaic. Отображенный на экране гипертекст представляет собой сочетание алфавитно-цифровой информации в различных форматах и стилях и некоторые графические изображения — картинки.

Связь между гипертекстовыми документами осуществляется с помощью ключевых слов. Найдя ключевое слово, пользователь может перейти в другой документ, чтобы получить дополнительную информацию. Новый документ также будет иметь гипертекстовые ссылки.

Работать с гипертекстами предпочтительнее на рабочей станции клиента, подключенной к одному из Web-серверов, чем на

страницах учебника, поэтому изложенный материал можно считать первым шагом к познанию службы WWW.

Работая с Web-сервером, можно выполнить удаленное подключение Telnet, послать абонентам сети электронную почту, получить файлы с помощью FTP-анонима и выполнить ряд других приложений (прикладных программ) Internet. Это дает возможность считать WWW интегральной службой Internet.

Создание страниц WWW. Так как создание собственного сервера WWW является сложным и дорогостоящим, то многие пользователи сети Internet могут размещать свою информацию на уже существующих серверах. Собственные страницы WWW можно создавать с помощью таких средств, как Microsoft Internet Assistant for Word и Netscape Navigator Gold. Редактор страниц Microsoft Internet Assistant представляет собой набор макрокоманд, на базе которого создаются документы HTML.

В диалоговом режиме пользователь может создать свой документ. Редактор при этом обеспечивает:

- ☑ ввод заголовка документа;
- ☑ вставку графического изображения или видеофрагмента;
- ☑ вставку гипертекстовой ссылки;
- ☑ вставку закладки;
- ☑ просмотр страниц WWW.

Редактор, встроенный в навигатор Netscape Navigator Gold, содержит средства для работы с языком JAVA. Этот язык позволяет интерпретировать программы, полученные из сети, на локальном компьютере пользователя. JAVA — язык объектно-ориентированного программирования. Он используется для

передового способа создания приложений для Internet — программирования аплетов (аплет — небольшое приложение). С помощью аплетов можно создавать динамичные Web-страницы. Для создания web-приложений используются языки PERL, JAVA SCRIPT, PHP.

Браузеры — программы просмотра Web-страниц

Основная задача программы-браузера (англ. browse [brauz] — пролистать, проглядеть, просмотреть) — открыть по указанному адресу Web-страницу. Но современные браузеры располагают значительно более широкими возможностями и позволяют работать не только со службой WWW, но и с электронной почтой, телеконференциями и другими службами Интернет. Таких служб достаточно много — это и удаленный доступ (Telnet), и передача файлов (FTP), и многое другое.

В настоящее время программы-браузеры выпускают многие фирмы. Но фирма Microsoft к каждой новой версии программы *Internet Explorer* (IE) практически сразу выпускает локализованную (русскоязычную) версию. Кроме того, на многих компьютерах установлена операционная система Windows, а это означает, что система будет содержать встроенные браузер *IE* и почтовую программу *Outlook Express.*

Наиболее популярными на данный момент браузерами являются Mozilla Firefox, Google Chrome, Opera,

Safari.

Настройка браузера

Программа-браузер *IE* имеет стандартный для Windows-приложений вид: в верхней части экрана расположено Главное меню, ниже — панель инструментов, под ней — адресная строка, ниже — информационное окно браузера, под ним — информационная строка браузера, показывающая состояние загрузки Web-страницы, в правом верхнем углу — три кнопки управления состоянием и размерами окна программы.

С помощью этой программы можно настраивать размеры окна, вид панели инструментов, тип, цвета, размер шрифтов и другие характеристики представляемой в информационном окне информации. Настроек очень много, ниже рассматриваются только некоторые из них. Вызвать окно настроек можно, выполнив команду **Вид, Свойства.**

Открытие Web-страниц и работа с поисковыми системами

В адресное поле программы-браузера (далее — браузера) можно вводить не полный адрес компьютера (URL), а только его часть, начинающуюся с букв www. Например, можно вводить не http://www.rambler.ru, а www.rambler.ru, остальное браузер допишет сам. Существует два варианта сохранить понравившийся адрес:

- выполнить команду **Избранное, Добавить в;**
- щелкнуть по кнопке <Избранное> на панели инструментов.

Если Web-страница долго не открывается (более 3 — 4 мин.), можно перезагрузить адрес. Для этого надо щелкнуть по кнопке <Стоп> (прервать загрузку), затем — по кнопке <Обновить>. Иногда это приводит к ускорению загрузки страницы.

Указатель мыши в области гиперссылки приобретает вид ладони с указательным пальцем.

Открыть документ по адресу, указанному в гиперссылке, можно, нажав один раз левую кнопку мыши на гиперссылке. В результате в текущее окно браузера будет загружен этот документ.

Для открытия документа в новом окне, не закрывая текущее окно, надо нажать пра вую кнопку мыши (указатель мыши — на гиперссылке) и выполнить команду **Открыть в новое окно.** Не рекомендуется открывать много окон, так как это может привести к замедлению работы программы.

Вернуться на предыдущую страницу можно, щелкнув по кнопке <Назад> на панели инструментов.

Изменить кодировку символов (если на экране появились нечитаемые выражения) можно, выполнив команду **Вид, Шрифты** и выбрав другую (по сравнению с установленной) кодировку. Обычно используется либо кодировка Cyrillic KOI8-R, либо Cyrillic Windows-1251.

Работа браузера с Web-страницами в режиме off-line

Если вы при просмотре Web-страниц в режиме on-line открывали по гиперссылкам другие Web- страницы, то и в режиме off-line это будет выполняться.

Некоторые Web-страницы могут не открываться. Это значит, что объем Web-страниц, хранящихся в журнале, больше, чем размер дискового пространства, отведенного вами под временные файлы Интернета. Открываться будут только последние страницы, которые вы

просматривали и суммарный объем которых не превышает размер временных файлов Интернета.

Стандартные возможности Windows-приложений в браузере

Для сохранения Web-страниц надо выполнить команду **Файл, Сохранить как,** затем в соответствующем поле ввести имя сохраняемого файла, выбрать папку, в которой хотите сохранить этот файл, и тип файла, в котором хотите сохранить информацию, а затем щелкнуть по кнопке <Сохранить>. Сохранять файл можно в двух форматах — в HTML или в текстовом. Для выбора типа файла надо нажать на значок черного треугольника в правой части поля «Тип файла» и щелкнуть курсором по нужному формату.

Для сохранения рисунков с Web-страниц надо навести указатель мыши на рисунок, щелкнуть правой кнопкой и выполнить команду **Сохранить рисунок как,** а далее выполнить действия, аналогичные указанным в предыдущем абзаце, т.е. задать имя, задать тип файла и указать, в какой папке следует сохранить рисунок. Рисунки можно сохранять в двух форматах — в BMP (стандартный формат Windows для рисунков) и в JPG. Лучше сохранять в формате JPG, так как в этом случае файл рисунка намного меньше по размеру, чем файл этого же рисунка в формате BMP.

Поиск информации в Интернет

Глобальная сеть Интернет объединяет миллионы компьютеров и локальных сетей, к ее услугам прибегают сотни миллионов человек. Но сеть Интернет — это лишь средство связи компьютеров и локальных сетей между собой. Для хранения и передачи информации по сети

Интернет созданы специальные информационные службы, иногда называемые сервисами Интернет. Этих служб несколько, наиболее часто используемыми являются электронная почта, электронные библиотеки, телеконференции. Но самой популярной службой является World Wide Web (WWW) — всемирная паутина.

Служба WWW имеет свои особенности, благодаря которым она и стала такой популярной. Вся информация в этой службе хранится на *WWW-серверах* в виде гипертекстовых документов, называемых *Web-страницами.* Эти документы пишутся на языке HTML (Hyper Text Markup Language) и могут содержать информацию различного вида: текст, рисунки, аудио и видео, что делает эту информацию чрезвычайно привлекательной для пользователей. Гиперссылки в HTML-документах могут указывать как на другую часть этого документа, так и на другой документ, расположенный на любом сервере сети Интернет. Это позволяет легко отыскивать требуемую информацию, переходя посредством гиперссылок от документа к документу. А вообще-то для поиска информации в сети Интернет используются специальные поисковые серверы. Но прежде чем что-то искать, надо знать, где информация находится, поэтому рассмотрим способы адресации в сети Интернет.

Текстовые процессоры — инструменты для создания HTML-документов

В данной работе рассмотрим, как создавать несложные Web-страницы, а точнее, HTML-документы.

HTML-документ становится Web-страницей, когда он определенным образом зарегистрирован в Интернет, т.е. его можно будет открыть по определенному адресу. Существует несколько групп программ, в которых можно создавать HTML-документы, но

самыми простыми и доступными для начинающего пользователя являются текстовые процессоры.

В настоящее время в состав современных текстовых процессоров входят инструменты для создания Web-страниц.

Текстовые процессоры имеют определенные преимущества по сравнению со специализированными авторскими инструментами HTML. Например, пользователям удобно работать с текстовыми процессорами. Кроме того, документы, подготовленные текстовыми программами, можно распространять в разнообразных форматах, отличных от формата HTML, по обычной или по электронной почте. Текстовый процессор представляет собой единый инструмент для выполнения всех этих задач. Текстовые процессоры оснащены множеством средств для редактирования текста, в частности для проверки орфографии и синтаксиса, автоматического исправления грамматических ошибок и форматирования.

Есть и недостатки. Некоторые характерные для Интернет понятия и функции остаются за пределами возможностей текстовых процессоров, например ни одна из этих программ не работает с кадрами. А поскольку HTML — не "родной" язык текстовых процессоров, все элементы документа должны подвергаться процедуре преобразования. Обычно такие детали, как рамки таблиц и некоторые текстовые расширения, не удается преобразовать должным образом. Кроме того, ни одна из программ текстовых процессоров не обеспечивает возможности разбиения длинного документа на несколько HTML-страниц на основе указанных пользователем признаков, таких, как границы глав и разделов или стили заголовков. Вместо этого документ экспортируется как одна

длинная HTML-страница. С помощью любого из текстовых процессоров можно преобразовать документ, подготовленный в его среде, в одну-единственную HTML-страницу.

Создание шаблона HTML-документа и заполнение его информацией

Для создания HTML-документов в текстовом процессоре Word должны быть соответствующие инструменты. Для проверки этого выполните команду **Файл, Создать.** Если в появившемся окне есть вкладка *Web-страницы,* то эти инструменты у вас есть. Если этой вкладки нет, то надо переустановить Microsoft Office в режиме *Выборочно (Custom),* добавив "галочку" в строку *Создание HTML.*

При заполнении шаблона информацией не забывайте стирать слова шаблона, такие, как *Вставьте заголовок* или *Введите текст.*

Слова, выделенные синим цветом, являются гиперссылками, они позволяют переходить сразу к указанным подразделам документа.

Вставка в документ "бегущей строки", графического объекта и гиперссылок

Размеры бегущей строки можно менять, как и размеры любого объекта Windows. Вставку в документрисунка из файла можно выполнять тремя способами:

- выполнив команду **Вставка, Рисунок, Из файла,** выбирать файл с подходящим рисунком из каталогаClipart;
- нажав правую кнопку мыши и открыв пункт **Рисунок,** выбирать файл с подходящим рисунком изкаталога Clipart;
- нажав на значок рисунка в левой нижней части окна, после чего выбирать файл с подходящимрисунком из каталога Clipart.

Вставить рисунок с его предварительным просмотром можно командой **Вставка, Рисунок, Картинки.**

Гиперссылку на текст, находящийся на разрабатываемой вами странице, можно сделать следующим образом:

- поставьте курсор в ту часть текста, куда надо перейти по гиперссылке;
- выполните команду **Вставка, Закладка;**
- в строке *Имя закладки* введите сочетание символов, например *Закл1;*
- переведите курсор в ту часть текста, где будет гиперссылка;
- напишите название гиперссылки;
- выделите это название;
- выполните команду **Вставка, Гиперссылка;**
- щелкните по кнопке <Обзор> напротив поля «Имя объекта в документе»;
- выберите имя закладки *Закл1,* щелкните по кнопке <ОК>, затем снова щелкните
- <ОК> — гиперссылка готова.

Контрольные вопросы:

1. Перечислите и опишите основные информационные службы глобальной сети Интернет.
2. Расскажите о способах адресации в сети Интернет.
3. Какие функции выполняют программы-браузеры?
4. Опишите технологию просмотра web-страниц с использованием программ-браузеров.
5. Чем отличаются режимы работы браузеров on-line и off-line?
6. Опишите стандартные возможности Windows-приложений в браузере.
7. Каковы преимущества и недостатки текстовых процессоров при создании HTML-документов по сравнению со специализированными авторскими инструментами HTML.
8. Как создать HTML-страницу с использованием шаблонов текстового

процессора?

9. Дайте определение понятиям: роутер, мост, шлюз. Для чего необходим прокси-сервер сети Интернет?
10. Назовите аппаратное обеспечение и топологии локальных вычислительных сетей.
11. Для чего необходима цифровая подпись?
12. Расскажите про историю развития глобальных компьютерных сетей.

4. Технология работы в глобальной сети Интернет

Задание 1. Настройка браузера

1. Ознакомьтесь с содержимым пунктов меню браузера.
2. Научитесь раскрывать окно браузера на весь экран и сворачивать его до прежнего размера.
3. Научитесь производить настройку домашней страницы браузера.
4. Научитесь производить настройку временных файлов Интернет.

Порядок выполнения задания 1

1. Для ознакомления с пунктами меню браузера:

- запустите браузер *IE*, щелкнув по соответствующему значку на Рабочем столе;
- просмотрите названия содержания пунктов и подпунктов меню, а также назначение кнопок на панели управления (удерживая на них курсор более 1 секунды) для лучшей ориентации в функциях, выполняемых браузером. Часть функций стандартна для Windows-приложений, часть специфична для браузера.

2. Для изменения размеров окна браузера:

- раскройте окно браузера на весь экран. Для этого выполните команду **Просмотр, На весь экран;**
- вернитесь к прежнему размеру экрана. Для этого щелкните по кнопке <На весь экран> на панелиинструментов в верхней части окна.

3. Для настройки домашней страницы браузера:

- выполните команду Вид, Свойства обозревателя;
- откройте вкладку *Общие;*
- в окне «Домашняя страница» в адресномполе установите начальную страницу обзора **http://medic.pnzgu.ru**.

4. Для настройки элемента Временные файлы Интернета:

- на вкладке *Общие* щелкните по кнопке <Настройка>. В появившемся окне просмотрите объем дискового пространства, выделяемого под временные файлы. Конечно, чем больше этого пространства, тем лучше для пользователя, но это зависит от свободного места на вашем диске. Обычно размер этих файлов устанавливают в пределах 1 - 2 % от объема диска. Если вы затрудняетесь выбрать нужный объем самостоятельно, то лучше оставить настройки по умолчанию;
- в окне «История» установите число 20, т.е. адрес любой открываемой вами Web-страницы будет храниться в журнале 20 дней;
- закройте окно «Свойства обозревателя».

Задание 2. Открытие Web-страниц и работа с поисковыми системами

1. Откройте в браузере Web-страницу поисковой системы Rambler.
2. Сохраните адрес открытой Web-страницы в папке с именем "Русскоязычные поисковые системы".
3. С помощью тематического поиска в поисковой системе Rambler найдите информацию о ВУЗах страны, готовящих по специальности «Медицинская кибернетика».
4. Составьте сложный запрос для поиска информации о ВУЗах страны, готовящих по специальности

«Медицинская кибернетика» среди найденных информационных ресурсов.

Порядок выполнения задания 2

1. Для открытия Web-страницы поисковой системы Rambler:

- откройте программу *IE;*
- в адресное поле браузера введите **www.rambler.ru;**
- нажмите клавишу <Enter>. Через некоторое время на экране появится Web-страница этой поисковой системы.

2. Для сохранения адреса поисковой системы Rambler в папке с именем Русскоязычные поисковые системы:

- выполните команду **Избранное, Добавить в;**
- <Создать папку>;
- введите имя папки *Русскоязычная поисковая система* и щелкните по кнопке <ОК>;
- закройте окно «Добавление в избранное», щелкнув по кнопке <ОК>.

3. Чтобы найти информацию о ВУЗах страны, осуществляющих подготовку врачей по специальности

«Медицинская кибернетика», необходимо выполнить следующие действия:

- на стартовой странице поисковой системы Rambler в строке «Найти» ввести следующие ключевые слова «ВУЗ специальность «Медицинская кибернетика»»,
- щелкните по кнопке «Поиск»;
- ознакомьтесь с результатами поиска по ключевым словам.

4. Для составления и выполнения сложного запроса в поисковой системе Rambler необходимо:

- В строке «Найти» ввести дополнительные ключевые слова, например «ПГУ»;
- установить переключатель режимов поиска в положение «Искать в найденном»;

- щелкните по кнопке «Поиск»;
- откройте одну из появившихся в результате поиска ссылку и просмотрите ее содержание;
- закройте браузер.

Задание 3. Работа браузера с Web-страницами в режиме off-line

1. Откройте программу IE в режиме off-line (в автономном режиме, т.е. без установления связи с провайдером).
2. Откройте и просмотрите Web-страницы, на которые вы заходили сегодня.

Порядок выполнения задания 3

1. Для открытия программы IE в режиме off-line:
- откройте программу *IE;*
- откройте пункт меню **Файл;**
- щелкните по пункту **Автономная работа.**
2. Для открытия и просмотра Web-страниц, на которые вы заходили сегодня, выполните следующие действия:
- на панели инструментов щелкните по кнопке <Журнал>;
- в открывшемся окне щелкните по папке Сегодня;
- в открывшемся перечне папок откройте одну из папок;
- откройте одну из ссылок и просмотрите ее, при этом можно переходить по тем ссылкам, которые вы использовали;
- закройте журнал;
- для отмены режима автономной работы браузера выполните команду Файл, Автономная работа.

Задание 4. Стандартные возможности Windows-приложений в браузере

1. Сохраните информацию с Web-страницы в виде текстового файла в личной папке на рабочем диске.

2. Сохраните выделенную часть информации с Web-страницы в виде файла Word в личной папке на рабочем диске.
3. Сохраните рисунок с Web-страницы в виде jpg-файла в личной папке на рабочем диске.
4. Просмотрите сохраненные вами текстовые файлы.
5. Просмотрите сохраненный вами рисунок.
6. Найдите заданную информацию на Web-странице.

Порядок выполнения задания 4

1. Сохраните информацию с Web-страницы о поисковом языке Rambler в виде текстового файла. Для этого:

- откройте программу *IE;*
- в адресное поле браузера введите
- нажмите клавишу <Enter>. Через некоторое время на экране появится Web-страница;
- откройте пункт меню **Файл;**
- откройте пункт **Сохранить как;**
- в поле «Имя файла» введите имя Пример-1;
- в поле «Тип файла» выберите *Файл текста;*
- выберите личную папку на рабочем диске, где будет храниться файл;
- щелкните по кнопке <Сохранить>.

2. Выделите часть текстовой информации на Web-странице и сохраните ее в виде файла в текстовом процессоре Word. Для этого:

- выделите произвольный абзац текста на Web-странице;
- скопируйте его в буфер обмена;
- откройте программу *Word,* выполнив команду **Пуск, Программы, Word;**
- откройте новый документ;
- скопируйте туда информацию из буфера обмена;
- сохраните эту информацию в личной папке на рабочем диске как файл *Word,* задав ему имя Пример-2;

- закройте программу *Word.*

3. Сохраните рисунок с Web-страницы в виде JPG-файла в личной папке на рабочем диске. Для этого:

- в адресное поле браузера введите имя **medic.pnzgu.ru**;
- нажмите клавишу <Enter>;
- выберите любую фотографию и щелкните по ней правой кнопкой мыши;
- выберите пункт **Сохранить рисунок как;**
- задайте имя рисунку, например МИ ПГУ*;*
- тип файла выберите JPG;
- выберите личную папку на рабочем диске, куда поместите рисунок;
- щелкните по кнопке <Сохранить>;
- закройте браузер.

4. Просмотрите созданные вами текстовые файлы. Для этого:

- откройте личную папку на рабочем диске;
- щелкните по файлу Пример-1. В окне программы Блокнот (по умолчанию настроенной на просмотр и редактирование текстовых файлов) просмотрите сохраненную вами текстовую информацию с Web-страницы;
- закройте программу Блокнот;
- щелкните по файлу Пример-2. Этот файл откроется в окне программы Word; просмотрите этот файл;
- закройте программу Word.

5. Просмотрите созданный вами графический файл. Для этого:

- в личной папке на рабочем диске щелкните по файлу МИ ПГУ;
- просмотрите рисунок. По умолчанию в качестве программы просмотра рисунков, как правило, установлена программа Paint. Если эта программа не установлена на вашем компьютере, то рисунок можно просмотреть из любого графического редактора;
- закройте графический редактор.

6. Найдите слово Новости на стартовой странице сайта Медицинские

информационные ресурсы Пензенской области. Для этого:

- откройте программу *IE;*
- в адресное поле браузера введите имя **medic.pnzgu.ru**;
- нажмите клавишу <Enter>. Через некоторое время на экране появится Web-страница;
- в пункте *Правка* выберите подпункт *Найти на этой странице;*
- в поле для ввода введите слово *Новости;*
- щелкните по кнопке <Найти и далее>. Слово *Обновления* на странице будет выделено, заданная информация на Web-странице найдена;
- закройте браузер.

Задание 5. Создание HTML-документов

1. Создайте личную основную страницу.
2. Замените данные шаблона нужной вам информацией.
3. Вставьте в документ "бегущую строку".
4. Вставьте в документ графический объект.
5. Вставьте в Документ гиперссылку на текстовый файл, находящийся на рабочем диске.
6. Вставьте в документ гиперссылку Дата создания.

Порядок выполнения задания 5

1. Создайте личную основную страницу. Для этого:

- откройте программу *Microsoft Word*;
- откройте пункт меню **Файл;**
- откройте пункт меню **Создать;**
- откройте вкладку *Web-страницы;*
- выделите значок **Личная основная страница** и щелкните по кнопке <ОК>.

2. Просмотрите полученную страницу и введите в нее необходимую информацию, заменив данные шаблона. Для этого:

- вместо *Вставьте заголовок* напишите *Моя первая Web-страница,*
- вместо подзаголовка вставьте свою фамилию, имя, отчество;
- в разделе *Сведения о работе* сотрите строки *Введите текст* и вместо них введите информативные данные;
- замените весь раздел *Сведения о работе* информацией об учебном заведении. В этом случае выделите название гиперссылки *Сведения о работе* в оглавлении и напишите *Сведения об учебе;*
- аналогично удалив ненужные, введите новые пункты в разделе *Мои контакты.*

3. Вставьте в документ "бегущую строку". Для этого:

- вставьте пустую строку между заголовком и подзаголовком страницы (подведя курсор к концузаголовка и нажав клавишу <Enter>);
- откройте пункт меню **Вставка** выберите пункт **Бегущая строка** или нажмите на кнопку **Бегущая строка** панели инструментов **Веб-компоненты**;

- настройте параметры "бегущей строки" и щелкните по кнопке <ОК>.

4. Для того чтобы вставить на страницу графический объект, выполните следующие действия:

- вставьте пустую строку после подзаголовка страницы;
- откройте пункт меню **Вставка;**
- выберите пункт **Рисунок** и далее либо *Картинки,* либо *Из файла* (в зависимости от того, что вы хотите вставлять — рисунок из коллекции программы Word или имеющиеся у вас графические файлы);
- вставьте на место пустой строки выбранный вами графический объект.

5. Для того чтобы вставить на страницу гиперссылку на файл:

- установите курсор на тексте *Вставьте гиперссылку* в подразделе *Список гиперссылок;*
- сотрите текст *Вставьте гиперссылку,* оставив курсор в этой строке;
- выполните команду **Вставка, Гиперссылка;**
- для выбора имени файла, на который можно переходить по гиперссылке, щелкните по кнопке <Обзор> рядом с полем «Связать с файлом/URL»;
- выберите созданный ранее вами текстовый файл и щелкните по кнопке <ОК>;
- проверьте работу гиперссылки, щелкнув по ней, — на экране должен открыться текст вашего файла;
- закройте этот файл.

6. Используя материалы Краткой справки, создайте гиперссылку Дата создания, указывающую на слова Дата создания в конце страницы.

Просмотрите созданный вами HTML-документ, выполнив команду **Файл, Просмотр Web-страницы.** Далее вы можете уже самостоятельно изменять свою страничку и поместить ее на один из web-серверов, где под такие страницы выделяют место.

Задание 6. Работа с электронной почтой.

1. Зарегистрируйтесь на любом почтовом сервере или войдите в свой аккаунт, если у Вас уже имеется электронный почтовый ящик.
2. Ознакомьтесь с возможностями электронной почты.
3. Отправьте на адрес cyborg.penza@mail.ru письмо с прикрепленным файлом следующего содержания:

   Сохранение оптимальной жизнедеятельности человека при взаимодействии с окружающей средой определяется тем, что для его организма существует определенный физиологический предел выносливости по отношению к любому фактору среды и за границей предела этот фактор неизбежно будет оказывать угнетающее влияние на здоровье человека.

4. Выйдите из почты и закройте браузер.

Порядок выполнения задания 6

1. Если у Вас уже имеется электронный почтовый ящик, то зарегистрируйтесь в нем под своим аккаунтом.

   В противном случае, зарегистрируйте почтовый ящик на бесплатном почтовом сервере **mail.ru**. Для

   этого:

- в адресной строке браузера введите адрес сайта **mail.ru** и нажмите Enter;
- нажмите на ссылку **Регистрация почты**;
- далее заполните регистрационную форму. Пример заполнения приведен на рис.6.1. Пароль от почтового ящика должен быть надежным (информация о том, как можно выбрать пароль, размещена в разделе Помощь).

- После заполнения формы нажмите кнопку **Зарегистрироваться**. В случае возникновения ошибок при регистрации следуйте указаниям службы поддержки почтового сервера.

2. Для ознакомления с возможностями электронной почты, последовательно нажмите на пиктограммы следующих разделов (рис. 6.2):

- входящие и отправленные письма, черновики, спам и корзину;
- написать, письма, адреса;
- поиск по почте, настройки почты, свой электронный адрес и т.д.

3. Для того чтобы написать письмо, необходимо выполнить следующие действия:

- нажать на кнопку **Написать** на панели инструментов почты;
- затем введите адрес того, кому вы собираетесь отправить письмо: cyborg.penza@mail.ru;
- в поле **Тема** введите вашу фамилию, имя и номер группы (рис. 6.3);
- введите текст, представленный в п. 3 задания 6;
- затем прикрепите любой файл к этому письму (например, графический файл);
- нажмите на кнопку **Отправить**.

4. Выйдите из почты при помощи команды **Выход**. Закройте браузер.

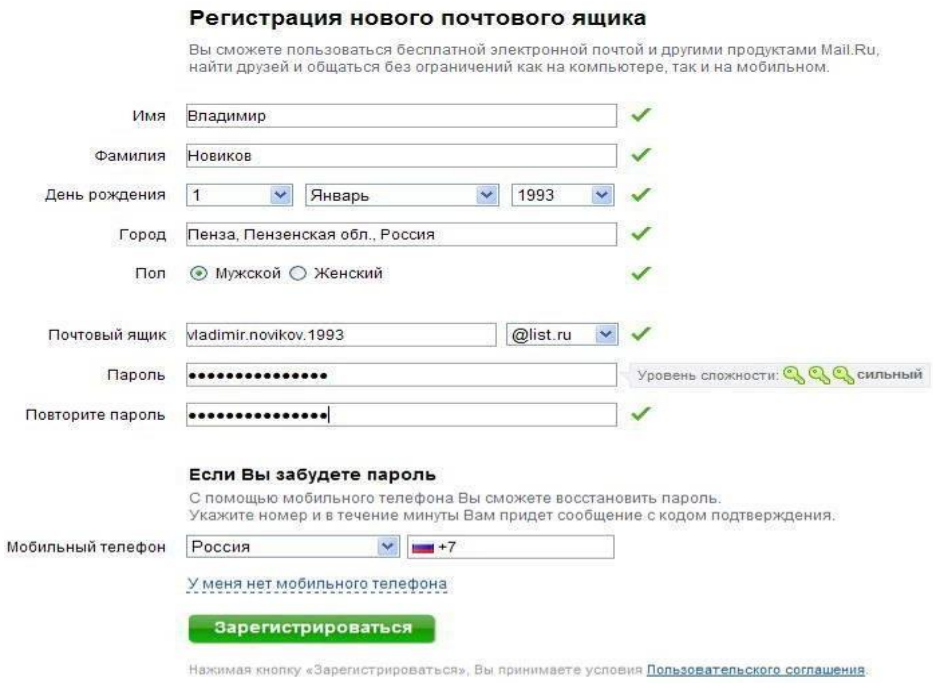


Рис 6.1. Форма регистрации

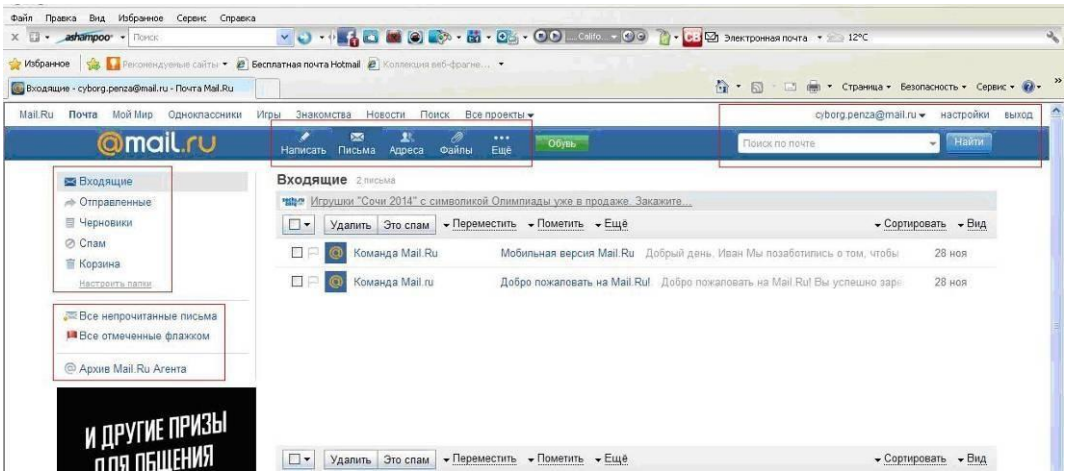


Рис 6.2. Основные возможности электронной почты

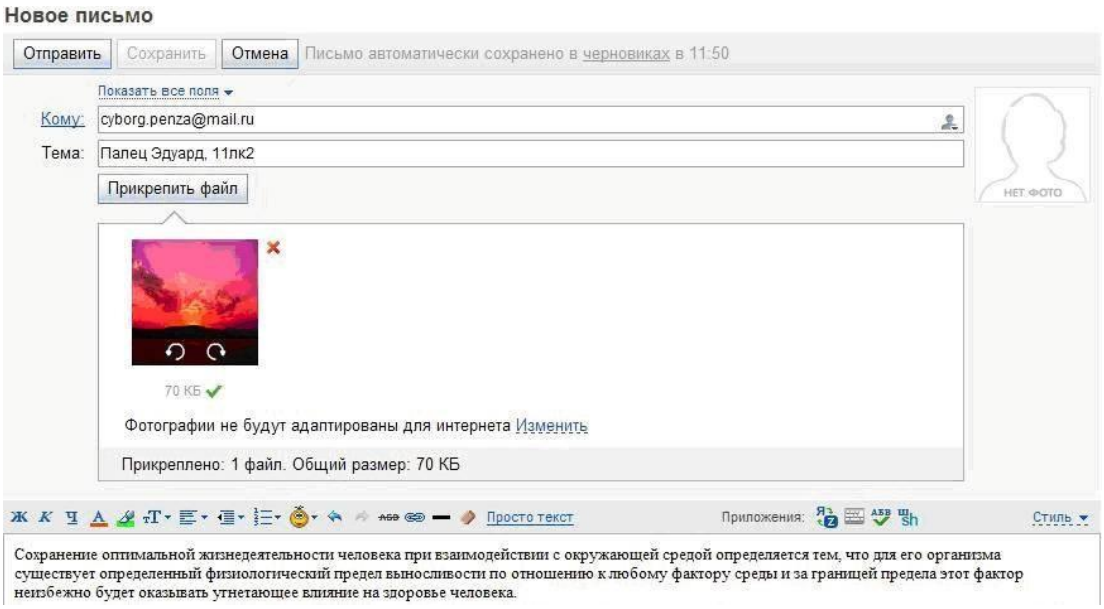


Рис. 6.3. Отправка электронного письма

Практическая работа 5

Тема: Отладка базового PPP с аутентификацией

Цели: Произвести отладку базового PPP с аутентификацией

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задачи

Часть 1. Построение сети и загрузка настроек устройств

Часть 2. Поиск и устранение неполадок канального уровня Часть 3. Поиск и устранение неполадок сетевого уровня

Исходные данные/сценарий

Маршрутизаторы в сети вашей компании были настроены неопытным сетевым инженером.

В результате нескольких ошибок в настройках возникли проблемы со связью. Начальник попросил вас найти и устранить неполадки в настройке и задокументировать работу. Найдите и исправьте ошибки, используя свои знания PPP и стандартные методы тестирования. Убедитесь, что на всех

последовательных каналах используется аутентификация CHAP PPP и что все сети доступны.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы Cisco Catalyst серии 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены и они не имеют загрузочных настроек. Если вы не уверены в этом, обратитесь к инструктору.

Топология

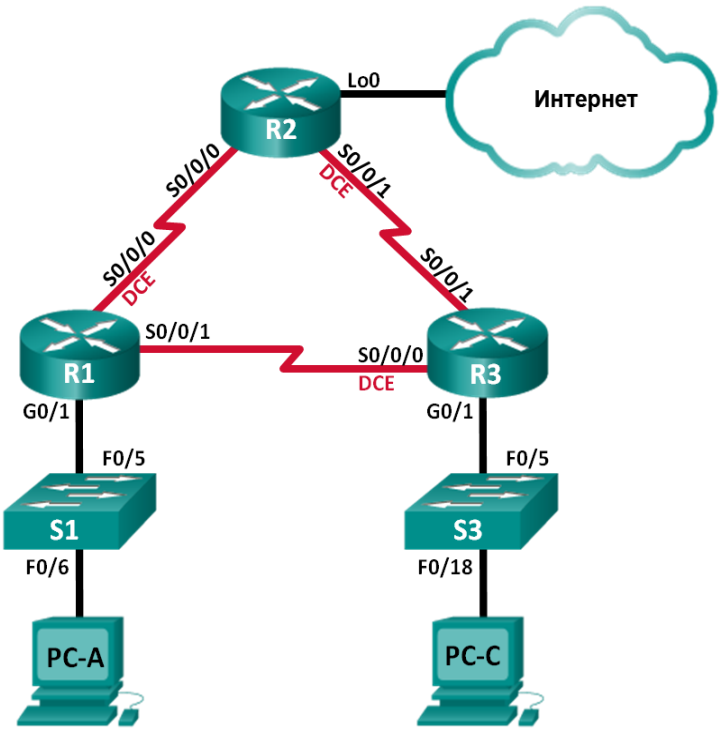


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252	Недоступно
	S0/0/1	192.168.13.1	255.255.255.252	Недоступно
R2	Lo0	209.165.200.225	255.255.255.252	Недоступно
	S0/0/0	192.168.12.2	255.255.255.252	Недоступно
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	Недоступно
R3	G0/1	192.168.3.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	Недоступно
	S0/0/1	192.168.23.2	255.255.255.252	Недоступно
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);
- 2 ПК (Windows 7, Vista и XP с программой эмуляции терминала, например, Tera Term)
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и загрузка настроек устройств

В части 1 вам предстоит создать топологию сети, настроить базовые параметры для узлов ПК и загрузить настройки маршрутизаторов.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Настройте узлы ПК.

Шаг 3: Загрузите настройки маршрутизатора.

Загрузите в соответствующий маршрутизатор следующие настройки. На всех маршрутизаторах настроены одинаковые пароли. Пароль привилегированного режима — class. Пароль для консоли и доступа vty — cisco. Все последовательные интерфейсы должны быть настроены с инкапсуляцией PPP и аутентификацией по протоколу CHAP с паролем chap123.

Настройка маршрутизатора R1:

hostname R1 enable secret class no ip domain lookup banner motd #Unauthorized Access is Prohibited!# username R2 password chap123 username R3 password chap123 interface g0/1 ip address 192.168.1.1 255.255.255.0 no shutdown interface s0/0/0 ip address 192.168.12.1 255.255.255.252 clock rate 128000 encapsulation ppp ppp authentication chap interface s0/0/1 ip address 192.168.31.1 255.255.255.252 encapsulation ppp ppp authentication pap exit router ospf 1 router-id 1.1.1.1

network 192.168.1.0 0.0.0.255 area 0 network 192.168.12.0 0.0.0.3 area 0 network 192.168.13.0 0.0.0.3 area 0 passive-interface g0/1 exit

line con 0 password cisco logging synchronous login line vty 0 4 password cisco login

Настройка маршрутизатора R2:

hostname R2 enable secret class no ip domain lookup banner motd #Unauthorized Access is Prohibited!# username R1 password chap123 username r3 password chap123 interface lo0 ip address 209.165.200.225 255.255.255.252 interface s0/0/0 ip address 192.168.12.2 255.255.255.252 encapsulation ppp ppp authentication chap no shutdown interface s0/0/1 ip address 192.168.23.1 255.255.255.252 clock rate 128000 no shutdown exit router ospf 1 router-id 2.2.2.2 network 192.168.12.0 0.0.0.3 area 0 network 192.168.23.0 0.0.0.3 area 0 default-information originate exit ip route 0.0.0.0 0.0.0.0 loopback0 line con 0 password cisco logging synchronous login line vty 0 4

password cisco login

Настройка маршрутизатора R3:

hostname R3 enable secret class no ip domain lookup banner motd #Unauthorized Access is Prohibited!# username R2 password chap123 username R3 password chap123

interface g0/1 ip address 192.168.3.1 255.255.255.0 no shutdown interface s0/0/0 ip address 192.168.13.2 255.255.255.252 clock rate 128000 encapsulation ppp ppp authentication chap no shutdown interface s0/0/1 ip address 192.168.23.2 255.255.255.252 encapsulation ppp ppp authentication chap no shutdown exit router ospf 1 router-id 3.3.3.3 network 192.168.13.0 0.0.0.3 area 0 network 192.168.23.0 0.0.0.3 area 0 passive-interface g0/1 line con 0 password cisco logging synchronous login line vty 0 4

password cisco login

Шаг 4: Сохраните текущую конфигурацию.

Часть 2: Поиск и устранение неполадок канального уровня

В части 2 следует использовать команды show для устранения неполадок канального уровня. Не забудьте проверить такие параметры, как тактовая частота, инкапсуляция, CHAP и имена и пароли пользователей.

Шаг 1: Изучите настройку маршрутизатора R1.

a. Используйте команду show interfaces, чтобы определить, установлен ли PPP на обоих последовательных каналах.

Основываясь на результатах работы команды show interfaces для S0/0/0 и S0/0/1, укажите возможные неполадки в каналах PPP.

_____

_____

b. В процессе поиска и устранения неполадок используйте команду debug ppp authentication для просмотра результатов аутентификации PPP в реальном времени.

R1# debug ppp authentication

PPP authentication debugging is on

c. Для исследования настроек на S0/0/0 используйте команду show run interface s0/0/0 .

Устраните все неполадки, связанные с S0/0/0. Запишите команды, использованные для исправления настройки.

Укажите выходные данные команды debug, выполненной после устранения неполадки.

_____

_____

d. Для исследования параметров на S0/0/1 используйте команду show run interface s0/0/1 .

Устраните все неполадки, связанные с S0/0/1. Запишите команды, использованные для исправления настройки.

_____

_____

Укажите выходные данные команды debug, выполненной после устранения неполадки.

_____

_____

e. Для отключения вывода данных команды debug PPP используйте команду no debug ppp authentication или undebug all.

f. Для проверки правильности настроек имени и пароля пользователя используйте команду show running-config | include username .

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления настройки.

_____

_____

Шаг 2: Исследуйте настройку маршрутизатора R2.

a. Используйте команду show interfaces, чтобы определить, установлен ли PPP на обоих последовательных каналах.

Все ли каналы установлены? _____

Если ответ отрицательный, то какие каналы следует проверить? В чем заключаются возможные причины неполадок?

_____

_____

b. Для исследования связей, которые не были установлены, используйте команду show run interface.

Устраните все обнаруженные неполадки, относящиеся к интерфейсам. Запишите команды, использованные для исправления настройки.

_____

_____

c. Для проверки правильности настроек имени и пароля пользователя используйте команду show running-config | include username .

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления настройки.

_____

_____

d. Используйте команду show ppp interface serial для того последовательного интерфейса, который вы отлаживаете.

Связь установлена? ___

Шаг 3: Исследуйте настройку маршрутизатора R3.

a. Используйте команду show interfaces, чтобы определить, установлен ли PPP на обоих последовательных каналах.

Все ли каналы установлены? _____

Если ответ отрицательный, то какие каналы следует проверить? В чем заключаются возможные причины неполадок?

_____

_____

b. Для исследования всех последовательных связей, которые не были установлены, используйте команду show run interface.

Устраните все неполадки, обнаруженные на интерфейсах. Запишите команды, использованные для исправления настройки.

_____

_____

c. Для проверки правильности настроек имени и пароля пользователя используйте команду show running-config | include username .

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления настройки.

_____

_____

d. Используйте команду show, чтобы убедиться, что последовательные связи установлены.

e. Связь по протоколу PPP установлена во всех каналах? _____

f. Эхо-запрос от узла ПК А к Lo0 выполняется успешно? _____

g. Успешно ли выполняется эхо-запрос от узла ПК А на узел ПК С? _____

Примечание. Для успешной передачи эхо-запросов между компьютерами может потребоваться отключение межсетевого экрана.

Часть 3: Поиск и устранение неполадок сетевого уровня

В части 3 вам предстоит убедиться, что подключения уровня 3 установлены на всех интерфейсах, исследуя для этого настройки IPv4 и OSPF.

Шаг 1: Убедитесь, что интерфейсы, указанные в таблице адресации, активны и настроены с правильными IP-адресами.

Выполните команду show ip interface brief на всех маршрутизаторах, чтобы убедиться, что все интерфейсы находятся в рабочем состоянии (up/up).

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления настройки.

_____

_____

Шаг 2: Проверка маршрутизации OSPF

Введите команду show ip protocols, чтобы убедиться, что OSPF запущен и что все сети объявляются.

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления настройки.

_____

_____

Успешно ли выполняется эхо-запрос от узла ПК A на узел ПК C? _____

Если между некоторыми узлами нет связи, продолжите поиск и устранение неполадок, чтобы устранить все имеющиеся неполадки.

Примечание. Для успешной передачи эхо-запросов между компьютерами может потребоваться отключение межсетевого экрана**.**

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet № 1**	**Интерфейс Ethernet № 2**	**Последовательный интерфейс № 1**	**Последовательный интерфейс № 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Практическая работа 6

Тема: Проверка PPP

Цели: Произвести проверку протокола PPP

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задачи

Часть 1. Построение сети и загрузка конфигурации устройств

Часть 2. Поиск и устранение неполадок канального уровня Часть 3. Поиск и устранение неполадок сетевого уровня

Общие сведения/сценарий

Маршрутизаторы в сети вашей компании были настроены неопытным сетевым инженером. В результате нескольких ошибок в настройках возникли проблемы с подключением. Ваш начальник поручил вам найти и устранить неполадки конфигурации и задокументировать работу. Найдите и исправьте ошибки, используя свои знания PPP и стандартные методы тестирования. Убедитесь, что на всех последовательных каналах используется аутентификация CHAP PPP и что все сети доступны.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии 15.2(4)M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Точные идентификаторы интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что у всех маршрутизаторов и коммутаторов была удалена начальная конфигурация. Если вы не уверены, обратитесь к инструктору.

Топология

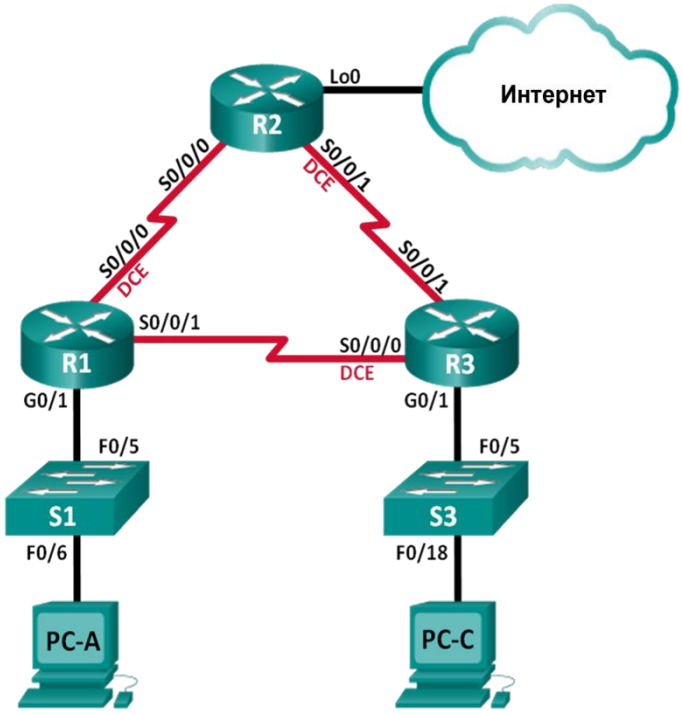


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Н/Д (недоступно)

	S0/0/0 (DCE)	192.168.12.1	255.255.255.252	Н/Д (недоступно)
	S0/0/1	192.168.13.1	255.255.255.252	Н/Д (недоступно)
R2	Lo0	209.165.200.225	255.255.255.252	Н/Д (недоступно)
	S0/0/0	192.168.12.2	255.255.255.252	Н/Д (недоступно)
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	Н/Д (недоступно)
R3	G0/1	192.168.3.1	255.255.255.0	Н/Д (недоступно)
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	Н/Д (недоступно)
	S0/0/1	192.168.23.2	255.255.255.252	Н/Д (недоступно)
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3
(универсальный образ) или аналогичная модель)
- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- 2 ПК (ОС Windows с программой эмуляции терминалов, такой как Tera Term)
- Консольные кабели для настройки устройств на базе Cisco IOS через консольные порты
- Кабели Ethernet и последовательные кабели в соответствии с топологией

Часть 1: Построение сети и загрузка настроек устройств

В части 1 вам предстоит создать топологию сети, настроить базовые параметры для хостов ПК и загрузить настройки маршрутизаторов.

Шаг 1: Подключите кабели сети согласно приведенной топологии.

Шаг 2: Настройте узлы ПК.

Шаг 3: Загрузите настройки маршрутизатора.

Загрузите в соответствующий маршрутизатор следующие настройки. На всех маршрутизаторах настроены одинаковые пароли. Пароль привилегированного режима — **class**. Пароль для консоли и доступа vty — **cisco**. Все последовательные интерфейсы должны быть настроены с инкапсуляцией PPP и аутентификацией по протоколу CHAP с паролем **chap123**.

Конфигурация маршрутизатора R1:

hostname R1 enable secret class no ip domain lookup banner motd #Unauthorized Access is Prohibited!# username R2 password chap123 username R3 password chap123 interface g0/1 ip address 192.168.1.1 255.255.255.0 no shutdown interface s0/0/0 ip address 192.168.12.1 255.255.255.252 clock rate 128000 encapsulation ppp ppp authentication chap interface s0/0/1 ip address 192.168.31.1 255.255.255.252 encapsulation ppp ppp authentication pap exit router ospf 1 router-id 1.1.1.1 network 192.168.1.0 0.0.0.255 area 0 network 192.168.12.0 0.0.0.3 area 0 network 192.168.13.0 0.0.0.3 area 0 passive-interface g0/1 exit line con 0 password cisco logging synchronous login line vty 0 4 password cisco login

Конфигурация маршрутизатора R2:

hostname R2 enable secret class no ip domain lookup banner motd #Unauthorized

Access is Prohibited!# username R1 password chap123 username r3 password chap123 interface lo0 ip address 209.165.200.225 255.255.255.252 interface s0/0/0 ip address 192.168.12.2 255.255.255.252 encapsulation ppp ppp authentication chap no shutdown interface s0/0/1 ip address 192.168.23.1 255.255.255.252 clock rate 128000 no shutdown exit router ospf 1 router-id 2.2.2.2 network 192.168.12.0 0.0.0.3 area 0 network 192.168.23.0 0.0.0.3 area 0 default-information originate exit

ip route 0.0.0.0 0.0.0.0 loopback0 line con 0 password cisco logging synchronous login line vty 0 4

password cisco login

Конфигурация маршрутизатора R3:

hostname R3 enable secret class no ip domain lookup banner motd #Unauthorized Access is Prohibited!# username R2 password chap123 username R3 password chap123 interface g0/1 ip address 192.168.3.1 255.255.255.0 no shutdown interface s0/0/0 ip address 192.168.13.2 255.255.255.252 clock rate 128000 encapsulation ppp ppp authentication chap no shutdown interface s0/0/1 ip address

192.168.23.2 255.255.255.252 encapsulation ppp ppp authentication chap no shutdown exit router ospf 1 router-id 3.3.3.3 network 192.168.13.0 0.0.0.3 area 0 network 192.168.23.0 0.0.0.3 area 0 passive-interface g0/1 line con 0 password cisco logging synchronous login line vty 0 4 password cisco login

Шаг 4: Сохраните текущую конфигурацию.

Часть 2: Поиск и устранение неполадок на канальном уровне

В части 2 вы будете использовать команды **show** для поиска и устранения неполадок на канальном уровне. Не забудьте проверить такие параметры, как тактовая частота, инкапсуляция, CHAP и имена и пароли пользователей.

Шаг 1: Проверьте конфигурацию маршрутизатора R1.

g. Используйте команду **show interfaces**, чтобы определить, установлен ли PPP на обоих последовательных каналах.

Основываясь на результатах работы команды **show interfaces** для S0/0/0 и S0/0/1, укажите возможные неполадки в каналах PPP.

_____

_____

h. В ходе поиска и устранения неполадок используйте команду **debug ppp authentication** для просмотра сведений об аутентификации PPP в режиме реального времени.

R1# **debug ppp authentication**

PPP authentication debugging is on

i. Для исследования параметров на S0/0/0 используйте команду **show run interface s0/0/0**.

Устраните все неполадки, связанные с S0/0/0. Запишите команды, использованные для исправления конфигурации.

_____

_____

Укажите выходные данные команды debug, выполненной после устранения неполадки.

_____

_____

j. Для исследования параметров на S0/0/1 используйте команду **show run interface s0/0/1**.

Устраните все неполадки, связанные с S0/0/1. Запишите команды, использованные для исправления конфигурации.

_____

Укажите выходные данные команды debug, выполненной после устранения неполадки.

_____

_____

k. Для отключения вывода данных команды debug PPP используйте команду **no debug ppp authentication** или **undebug all**.

l. Для проверки правильности настроек имени и пароля пользователя используйте команду **show running-config | include username**.

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления конфигурации.

_____

_____

Шаг 2: Проверьте конфигурацию маршрутизатора R2.

e. Используя команду **show interfaces**, определите, установлен ли PPP на обоих последовательных каналах.

Все ли каналы установлены? _____

Если ответ отрицательный, то какие каналы следует проверить? В чем заключаются возможные причины неполадок?

_____

_____

f. Для исследования связей, которые не были установлены, используйте команду **show run interface**.

Устраните все обнаруженные неполадки, относящиеся к интерфейсам. Запишите команды, использованные для исправления конфигурации.

_____

_____

g. Для проверки правильности настроек имени и пароля пользователя используйте команду **show running-config | include username**.

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления конфигурации.

_____

_____

h. Используйте команду **show ppp interface serial** для того последовательного интерфейса, который вы отлаживаете.

Связь установлена? _____

Шаг 3: Проверьте конфигурацию маршрутизатора R3.

h. Используйте команду **show interfaces**, чтобы определить, установлен ли PPP на обоих последовательных каналах.

Все ли каналы установлены? _____

Если ответ отрицательный, то какие каналы следует проверить? В чем заключаются возможные причины неполадок?

_____

_____

i. Используйте команду **show run interface** для проверки всех последовательных каналов, соединение для которых не было установлено.

Устраните все неполадки, обнаруженные на интерфейсах. Запишите команды, использованные для исправления конфигурации.

_____

_____

j. Для проверки правильности настроек имени и пароля пользователя используйте команду **show running-config | include username**.

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления конфигурации.

_____

_____

k. Используйте команду **show interface**, чтобы убедиться, что последовательные связи установлены.

l. По всем ли каналам PPP установлены соединения? _____

m. Эхо-запрос от узла ПК A к Lo0 выполняется успешно? _____

n. Успешно ли выполняется эхо-запрос от узла ПК A на узел ПК C?

_____

Примечание. Чтобы успешно получать ответы на ping-запросы между ПК, может потребоваться отключить межсетевой экран.

Часть 3: Поиск и устранение неполадок сетевого уровня

В части 3 вам предстоит убедиться, что подключения уровня 3 установлены на всех интерфейсах, исследуя для этого настройки IPv4 и OSPF.

Шаг 1: Убедитесь, что интерфейсы, указанные в таблице адресации, активны и настроены с правильными IP-адресами.

Выполните команду **show ip interface brief** на всех маршрутизаторах, чтобы убедиться, что все интерфейсы находятся в рабочем состоянии (up/up).

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления конфигурации.

_____

_____

Шаг 2: Проверка маршрутизации OSPF

Выполните команду **show ip protocols** и убедитесь, что протокол OSPF работает и все сети анонсированы.

Устраните все обнаруженные неполадки. Запишите команды, использованные для исправления конфигурации.

_____

_____

Успешно ли выполняется эхо-запрос от узла ПК A на узел ПК C? _____

Если между некоторыми хостами нет связи, продолжите поиск и устранение неполадок, чтобы устранить все имеющиеся неполадки.

Примечание. Чтобы успешно получать ответы на ping-запросы между ПК, может потребоваться отключить межсетевой экран.

Сводная таблица по интерфейсам маршрутизаторов

Сводка по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet № 1**	**Интерфейс Ethernet № 2**	**Последовательный интерфейс № 1**	**Последовательный интерфейс № 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах Cisco IOS для обозначения интерфейса.

Практическая работа 7

Тема: Настройка маршрутизатора в качестве клиента PPPoE для подключения DSL

Цели: Произвести настройку маршрутизатора в качестве клиента PPPoE для подключение DSL

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задачи

Часть 1. Развёртывание сети

Часть 2. Настройка маршрутизатора ISP

Часть 3. Настройка маршрутизатора Cust1

Исходные данные/сценарий

Интернет-провайдеры часто используют протокол PPPoE для передачи данных по каналам DSL своим заказчикам. PPP поддерживает назначение IP-адреса устройству на удаленном конце канала PPP. Что ещё более важно, PPP поддерживает аутентификацию CHAP. Интернет-провайдеры могут проверять учётные записи, чтобы определить, оплатил ли заказчик свой счёт, прежде чем позволить ему подключиться к Интернету

В этой лабораторной работе выполняется настройка подключения на стороне клиента и интернетпровайдера для настройки PPPoE. В большинстве случаев достаточно выполнить настройку на стороне клиента.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы Cisco Catalyst серии 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь в том, что маршрутизаторы и коммутаторы очищены от данных и на них нет стартовых конфигураций. Если вы не уверены в этом, обратитесь к инструктору.

Топология

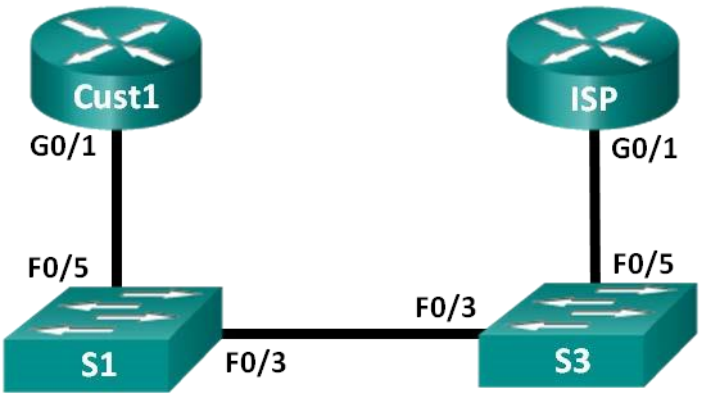


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Cust1	G0/1	Получен с помощью PPP	Получен с помощью PPP	Получен с помощью PPP
ISP	G0/1	Недоступно	Недоступно	Недоступно

Необходимые ресурсы:

- 2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Построение сети

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

i. Отключите поиск DNS.

j. Настройте имя устройств в соответствии с топологией.

k. Зашифруйте незашифрованные пароли.

l. Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.

m. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

n. Назначьте **cisco** в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.

o. Настройте ведение журнала состояния консоли на синхронный режим.

p. Сохраните настройку.

Часть 2: Настройка маршрутизатора интернет-провайдера ISP

В части 2 необходимо настроить маршрутизатор ISP с использованием параметров PPPoE для приёма подключений от маршрутизатора Cust1.

Примечание. Многие из команд настройки PPPoE для маршрутизатора интернет-провайдера выходят за рамки курса; однако они необходимы для выполнения лабораторной работы. Их можно скопировать и вставить в Маршрутизатор ISP в командной строке режима глобальной конфигурации.

f. Создайте в локальной базе учётных записей имя пользователя **Cust1** с паролем **ciscopppoe**.

ISP(config)# **username Cust1 password ciscopppoe**

g. Создайте пул адресов, которые будут назначены пользователям.

ISP(config)# **ip local pool PPPoEPOOL 10.0.0.1 10.0.0.10**

h. Создайте виртуальный шаблон Virtual Template и свяжите с ним IP-адрес G0/1. Свяжите виртуальный шаблон с пулом адресов. Настройте CHAP для аутентификации пользователей.

ISP(config)# **interface virtual-template 1**

ISP(config-if)# **ip address 10.0.0.254 255.255.255.0**

ISP(config-if)# **mtu 1492**

ISP(config-if)# **peer default ip address pool PPPoEPOOL**

ISP(config-if)# **ppp authentication chap callin**

ISP(config-if)# **exit**

i. Назначьте шаблон группе PPPoE.

ISP(config)# **bba-group pppoe global**

ISP(config-bba-group)# **virtual-template 1**

ISP(config-bba-group)# **exit**

j. Свяжите группу bba-group с физическим интерфейсом G0/1.

ISP(config)# **interface g0/1**

ISP(config-if# **pppoe enable group global**

ISP(config-if)# **no shutdown**

Часть 3: Настройка маршрутизатора Cust1

В части 3 необходимо настроить маршрутизатор Cust1 с использованием параметров PPPoE.

f. Настройте интерфейс G0/1 для подключения PPPoE.

Cust1(config)# **interface g0/1**

Cust1(config-if)# **pppoe enable**

Cust1(config-if)# **pppoe-client dial-pool-number 1**

Cust1(config-if)# **exit**

g. Свяжите интерфейс G0/1 с интерфейсом номеронабирателя Dialer. Используйте имя пользователя **Cust1** и пароль **ciscopppoe**, настроенные в части 2.

Cust1(config)# **interface dialer 1**

Cust1(config-if)# **mtu 1492**

Cust1(config-if)# **ip address negotiated**

Cust1(config-if)# **encapsulation ppp**

Cust1(config-if)# **dialer pool 1**

Cust1(config-if)# **ppp authentication chap callin**

Cust1(config-if)# **ppp chap hostname Cust1**

Cust1(config-if)# **ppp chap password ciscopppoe**

Cust1(config-if)# **exit**

h. Настройте статический маршрут по умолчанию через интерфейс номеронабирателя.

Cust1(config)# **ip route 0.0.0.0 0.0.0.0 dialer 1**

i. Настройте отладку на маршрутизаторе Cust1 для отображения согласования PPP и PPPoE.

Cust1# **debug ppp authentication**

Cust1# **debug pppoe events**

j. Включите интерфейс G0/1 на маршрутизаторе Cust1 и проверьте выходные данные отладки при установлении сеанса номеронабирателя PPPoE и во время аутентификации CHAP.

*Jul 30 19:28:42.427: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down

*Jul 30 19:28:46.175: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up

*Jul 30 19:28:47.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

*Jul 30 19:29:03.839: padi timer expired

*Jul 30 19:29:03.839: Sending PADI: Interface = GigabitEthernet0/1

*Jul 30 19:29:03.839: PPPoE 0: I PADO R:30f7.0da3.0b01 L:30f7.0da3.0bc1 Gi0/1

*Jul 30 19:29:05.887: PPPOE: we've got our pado and the pado timer went off

*Jul 30 19:29:05.887: OUT PADR from PPPoE Session

*Jul 30 19:29:05.895: PPPoE 1: I PADS R:30f7.0da3.0b01 L:30f7.0da3.0bc1 Gi0/1

*Jul 30 19:29:05.895: IN PADS from PPPoE Session

*Jul 30 19:29:05.899: %DIALER-6-BIND: Interface Vi2 bound to profile Di1 *Jul 30 19:29:05.899: PPPoE: Virtual Access interface obtained.

*Jul 30 19:29:05.899: PPPoE : encap string prepared

*Jul 30 19:29:05.899: [0]PPPoE 1: data path set to PPPoE Client

*Jul 30 19:29:05.903: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up

*Jul 30 19:29:05.911: Vi2 PPP: Using dialer call direction

*Jul 30 19:29:05.911: Vi2 PPP: Treating connection as a callout

*Jul 30 19:29:05.911: Vi2 PPP: Session handle[C6000001] Session id[1]

*Jul 30 19:29:05.919: Vi2 PPP: No authorization without authentication

*Jul 30 19:29:05.939: Vi2 CHAP: I CHALLENGE id 1 len 24 from "ISP"

*Jul 30 19:29:05.939: Vi2 PPP: Sent CHAP SENDAUTH Request

*Jul 30 19:29:05.939: Vi2 PPP: Received SENDAUTH Response FAIL

*Jul 30 19:29:05.939: Vi2 CHAP: Using hostname from interface CHAP

*Jul 30 19:29:05.939: Vi2 CHAP: Using password from interface CHAP

*Jul 30 19:29:05.939: Vi2 CHAP: O RESPONSE id 1 len 26 from "Cust1"

*Jul 30 19:29:05.955: Vi2 CHAP: I SUCCESS id 1 len 4

*Jul 30 19:29:05.955: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state to up *Jul 30 19:29:05.983: PPPoE : ipfib_encapstr prepared

*Jul 30 19:29:05.983: PPPoE : ipfib_encapstr prepared

j. Введите команду **show ip interface brief** на маршрутизаторе Cust1, чтобы отобразить IP-адрес, назначенный маршрутизатором ISP. Выходные данные приведены ниже. Каким способом был получен этот IP-адрес? _____

Cust1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Embedded-Service-Engine0/0 unassigned YES unset administratively down down

GigabitEthernet0/0 unassigned YES unset administratively down down

GigabitEthernet0/1 unassigned YES unset up up

Serial0/0/0 unassigned YES unset administratively down down

Serial0/0/1 unassigned YES unset administratively down down

Dialer1 10.0.0.1 YES IPCP up up

Virtual-Access1 unassigned YES unset up up

Virtual-Access2 unassigned YES unset up up

k. Введите команду **show ip route** на маршрутизаторе Cust1. Выходные данные приведены ниже.

Cust1# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, Dialer1

10.0.0.0/32 is subnetted, 2 subnets

C 10.0.0.1 is directly connected, Dialer1

C 10.0.0.254 is directly connected, Dialer1

l. Введите команду **show pppoe session** на маршрутизаторе Cust1. Выходные данные приведены ниже.

Cust1# **show pppoe session**

1 client session

Uniq ID PPPoE RemMAC Port VT VA State
SID LocMAC VA-st Type
N/A 1 30f7.0da3.0b01 Gi0/1 Di1 Vi2 UP
30f7.0da3.0bc1 UP

m. Отправьте эхо-запрос на адрес 10.0.0.254 с маршрутизатора Cust1. Эхо-запрос должен быть успешным. В противном случае устраните неполадки, пока не будет установлено подключение.

Cust1# **ping 10.0.0.254**

Type escape sequence to abort. Sending 5, 100-byte ICMP
Echos to 10.0.0.254, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

Вопросы на закрепление

Почему интернет-провайдеры, использующие технологию DSL, главным образом используют протокол PPPoE?

_____

_____

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet № 1**	**Интерфейс Ethernet № 2**	**Последовательный интерфейс № 1**	**Последовательный интерфейс № 2**

1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Практическая работа 8

Тема: Настройка туннеля VPN GRE по схеме «точка-точка»

Цели: Произвести настройку тунеля VPN GRE по схеме «точка-точка»

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Задачи

Часть 1. Базовая настройка устройств

Часть 2. Настройка туннеля GRE

Часть 3. Включение маршрутизации через туннель GRE

Исходные данные/сценарий

Универсальная инкапсуляция при маршрутизации (GRE) — это протокол туннелирования, способный инкапсулировать различные протоколы сетевого уровня между двумя объектами по общедоступной сети, например, в Интернете.

GRE можно использовать с:

- подключением сети IPv6 по сетям IPv4
- пакетами групповой рассылки, например, OSPF, EIGRP и приложениями потоковой передачи данных

В этой лабораторной работе необходимо настроить незашифрованный туннель GRE VPN «точкаточка» и убедиться, что сетевой трафик использует туннель. Также будет нужно настроить протокол маршрутизации OSPF внутри туннеля GRE VPN. Туннель GRE существует между маршрутизаторами WEST и EAST в области 0 OSPF. Интернет-провайдер не знает о туннеле GRE. Для связи между маршрутизаторами WEST и EAST и интернет-провайдером применяются статические маршруты по умолчанию.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интеграцией сервисов Cisco 1941 (ISR) под управлением ОС Cisco IOS версии 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы Cisco Catalyst серии 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейсов указаны в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены и они не имеют загрузочных настроек. Если вы не уверены в этом, обратитесь к инструктору.

Топология

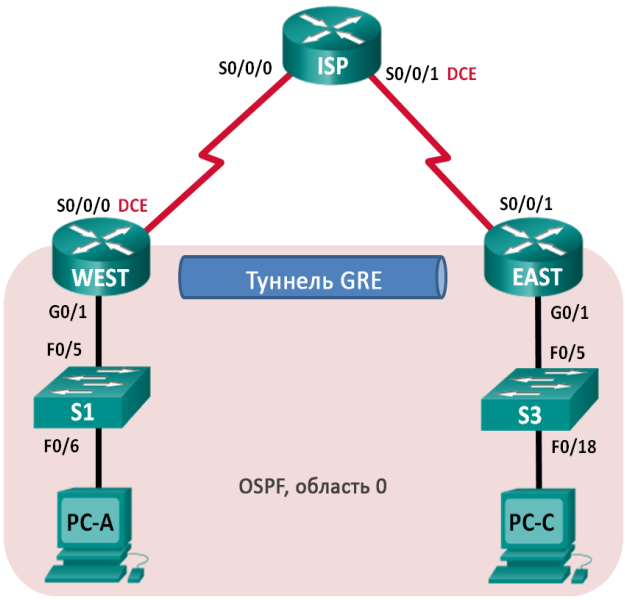


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
WEST	G0/1	172.16.1.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Недоступно
	Tunnel0	172.16.12.1	255.255.255.252	Недоступно
ISP	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Недоступно
EAST	G0/1	172.16.2.1	255.255.255.0	Недоступно
	S0/0/1	10.2.2.1	255.255.255.252	Недоступно
	Tunnel0	172.16.12.2	255.255.255.252	Недоступно
PC-A	NIC	172.16.1.3	255.255.255.0	172.16.1.1
PC-C	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Базовая настройка устройств

В части 1 вам предстоит настроить топологию сети и базовые параметры маршрутизатора, например, IP-адреса интерфейсов, маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

k. Отключите поиск DNS.

l. Назначьте имена устройств.

m. Зашифруйте незашифрованные пароли.

n. Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.

o. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

p. Назначьте cisco в качестве пароля для консоли и виртуального терминала VTY и активируйте учётную запись.

q. Настройте ведение журнала состояния консоли на синхронный режим.

r. Примените IP-адреса к интерфейсам Serial и Gigabit Ethernet в соответствии с таблицей адресации и активируйте физические интерфейсы. На данном этапе не настраивайте интерфейсы Tunnel0.

s. Настройте тактовую частоту на **128000** для всех последовательных интерфейсов DCE.

Шаг 4: Настройте маршруты по умолчанию к маршрутизатору интернет-провайдера.

WEST(config)# **ip route 0.0.0.0 0.0.0.0 10.1.1.2**

EAST(config)# **ip route 0.0.0.0 0.0.0.0 10.2.2.2**

Шаг 5: Настройте компьютеры.

Настройте IP-адреса и шлюзы по умолчанию на всех ПК в соответствии с таблицей адресации.

Шаг 6: Проверьте соединение.

На данный момент компьютеры не могут отправлять друг другу эхо-запросы. Каждый ПК должен получать ответ на эхо-запрос от своего шлюза по умолчанию. Маршрутизаторы могут отправлять эхозапросы на последовательные интерфейсы других маршрутизаторов в топологии. Если это не так, устраните неполадки и убедитесь в наличии связи.

Шаг 7: Сохраните текущую конфигурацию.

Часть 2: Настройка туннеля GRE

В части 2 необходимо настроить туннель GRE между маршрутизаторами WEST и EAST.

Шаг 1: Настройка интерфейса туннеля GRE.

c. Настройте интерфейс туннеля на маршрутизаторе WEST. Используйте S0/0/0 на маршрутизаторе WEST в качестве интерфейс источника туннеля и 10.2.2.1 как назначение туннеля на маршрутизаторе EAST.

WEST(config)# **interface tunnel 0**

WEST(config-if)# **ip address 172.16.12.1 255.255.255.252**

WEST(config-if)# **tunnel source s0/0/0**

WEST(config-if)# **tunnel destination 10.2.2.1**

d. Настройте интерфейс туннеля на маршрутизаторе EAST. Используйте S0/0/1 на маршрутизаторе EAST в качестве интерфейс источника туннеля и 10.1.1.1 как назначение туннеля на маршрутизаторе WEST.

EAST(config)# **interface tunnel 0**

EAST(config-if)# **ip address 172.16.12.2 255.255.255.252**

EAST(config-if)# **tunnel source 10.2.2.1**

EAST(config-if)# **tunnel destination 10.1.1.1**

Примечание. Для команды **tunnel source** в качестве источника можно использовать имя интерфейса или IP-адрес.

Шаг 2: Убедитесь, что туннель GRE работает.

a. Проверьте состояние интерфейса туннеля на маршрутизаторах WEST и EAST.

WEST# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Embedded-Service-Engine0/0 unassigned YES unset administratively down down

GigabitEthernet0/0 unassigned YES unset administratively down down

GigabitEthernet0/1 172.16.1.1 YES manual up up

Serial0/0/0 10.1.1.1 YES manual up up

Serial0/0/1 unassigned YES unset administratively down down

Tunnel0 172.16.12.1 YES manual up up

EAST# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Embedded-Service-Engine0/0 unassigned YES unset administratively down down

GigabitEthernet0/0 unassigned YES unset administratively down down

GigabitEthernet0/1 172.16.2.1 YES manual up up

Serial0/0/0 unassigned YES unset administratively down down

Serial0/0/1 10.2.2.1 YES manual up up

Tunnel0 172.16.12.2 YES manual up up

b. С помощью команды **show interfaces tunnel 0** проверьте протокол туннелирования, источник туннеля и назначение туннеля, используемые в этом туннеле.

Какой протокол туннелирования используется? Какие IP-адреса источника и назначения туннеля связаны с туннелем GRE на каждом маршрутизаторе?

_____

e. Отправьте эхо-запрос по туннелю из маршрутизатора WEST на маршрутизатор EAST с использованием IP-адреса интерфейса туннеля.

WEST# **ping 172.16.12.2**

Type escape sequence to abort. Sending 5, 100-byte ICMP

Echos to 172.16.12.2, timeout is 2 seconds: !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/36 ms

f. С помощью команды **traceroute** на маршрутизаторе WEST определите тракт к интерфейсу туннеля на маршрутизаторе EAST. Укажите путь до маршрутизатора EAST.

_____

e. Отправьте эхо-запрос и сделайте трассировку маршрута через туннель от маршрутизатора EAST к маршрутизатору WEST с использованием IP-адреса интерфейса туннеля.

Укажите путь от маршрутизатора EAST до маршрутизатора WEST?

_____

_____

С какими интерфейсами связаны эти IP-адреса? Почему?

_____

f. Команды **ping** и **traceroute** должны успешно выполняться. Если это не так, устраните неполадки и перейдите к следующей части.

Часть 3: Включение маршрутизации через туннель GRE

В части 3 необходимо настроить протокол маршрутизации OSPF таким образом, чтобы локальные сети (LAN) на маршрутизаторах WEST и EAST могли обмениваться данными с помощью туннеля GRE.

После установления туннеля GRE можно реализовать протокол маршрутизации. Для туннелирования GRE команда network будет включать сеть IP туннеля, а не сеть, связанную с последовательным интерфейсом. точно так же, как и с другими интерфейсами, например, Serial и Ethernet. Следует помнить, что маршрутизатор ISP в этом процессе маршрутизации не участвует.

Шаг 1: Настройка маршрутизации по протоколу OSPF для области 0 по туннелю.

c. Настройте идентификатор процесса OSPF 1, используя область 0 на маршрутизаторе WEST для сетей 172.16.1.0/24 и 172.16.12.0/24.

WEST(config)# **router ospf 1**

WEST(config-router)# **network 172.16.1.0 0.0.0.255 area 0**

WEST(config-router)# **network 172.16.12.0 0.0.0.3 area 0**

d. Настройте идентификатор процесса OSPF 1, используя область 0 на маршрутизаторе EAST для сетей 172.16.2.0/24 и 172.16.12.0/24.

EAST(config)# **router ospf 1**

EAST(config-router)# **network 172.16.2.0 0.0.0.255 area 0** EAST(config-router)# **network 172.16.12.0 0.0.0.3 area 0**

Шаг 2: Проверка маршрутизации OSPF.

a. Отправьте с маршрутизатора WEST команду **show ip route** для проверки маршрута к локальной сети 172.16.2.0/24 на маршрутизаторе EAST.

WEST# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP + - replicated route, % - next hop override

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 10.1.1.2
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.1.1.0/30 is directly connected, Serial0/0/0
L 10.1.1.1/32 is directly connected, Serial0/0/0
172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C 172.16.1.0/24 is directly connected, GigabitEthernet0/1
L 172.16.1.1/32 is directly connected, GigabitEthernet0/1
O 172.16.2.0/24 [110/1001] via 172.16.12.2, 00:00:07, Tunnel0
C 172.16.12.0/30 is directly connected, Tunnel0
L 172.16.12.1/32 is directly connected, Tunnel0

Какой выходной интерфейс и IP-адрес используются для связи с сетью 172.16.2.0/24?

_____

b. Отправьте с маршрутизатора EAST команду для проверки маршрута к локальной сети 172.16.1.0/24 на маршрутизаторе WEST.

Какой выходной интерфейс и IP-адрес используются для связи с сетью 172.16.1.0/24?

_____

Шаг 3: Проверьте связь между конечными устройствами.

c. Отправьте эхо-запрос с ПК A на ПК C. Эхо-запрос должен пройти успешно. Если это не так, устраните неполадки и убедитесь в наличии связи между конечными узлами.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение межсетевого экрана.

d. Запустите трассировку от ПК A к ПК C. Каков путь от ПК A до ПК C?

_____

_____

Вопросы на закрепление

1. Какие еще настройки необходимы для создания защищенного туннеля GRE?

_____

____

2. Если вы добавили дополнительные локальные сети к маршрутизатору WEST или EAST, то что нужно сделать, чтобы сеть использовала туннель GRE для трафика?

_____

_____

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet № 1**	**Интерфейс Ethernet № 2**	**Последовательный интерфейс № 1**	**Последовательный интерфейс № 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех сочетаний настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Виды работ практики и проверяемые результаты обучения по профессиональному модулю

Учебная практика

Виды работ	**Проверяемые результаты: требования к практическому опыту и коды формируемых ПК, ОК, умений (ПО, ПК, ОК, У)**	**Документ, подтверждающий качество выполнения работ**
Охране труда для системного администратора. Изучить инструктаж по технике безопасности при работе с компьютером и его периферией. Организовывать рабочее место. Подключить ПК. «*Общие требования охраны труда. Требования охраны труда перед началом работы. Требования охраны труда во время работы. Требования охраны труда в аварийных ситуациях. Требования охраны труда по окончании работы*». *Настройка прав доступа. Оформление технической документации, правила оформления документов.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	Аттестационный лист по учебной практике
Настройка аппаратного и программного обеспечения сети. Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain.	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Программная диагностика неисправностей. Аппаратная	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК	

диагностика неисправностей. Устранение паразитирующей нагрузки в сети. *Поиск неисправностей технических средств. Выполнение действий по устранению неисправностей. Использование активного, пассивного оборудования сети.*	2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7.. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Построение физической карты локальной сети. Установка WEB-сервера. Диагностика и обслуживание Web сервера. *Диагностика и обслуживание файлового сервера. Диагностика и обслуживание почтового сервера. Диагностика и обслуживание SQL – сервера. Конфигурирование web-сервера. Запуск, перезапуск и останов сервера.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7.ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Взаимодействие с базами данных. Установка брандмауэра. *Сохранение и восстановление больших наборов правил. Обеспечение безопасности.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Администрирование серверов и рабочих станций. *Организация доступа к локальным сетям и Интернету. Установка и сопровождение сетевых сервисов.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Подключение к оборудованию CISCO. Настройка подключения по Telnet и SSH. *Создание одноранговой и клиент-серверной сети. Знакомство PDU и BPDU пакетами на различных уровнях модели OSI в сетевом симуляторе CISCO Packet tracer. Агрегация каналов. Изучение STP и RSTP протоколов OSI в сетевом симуляторе CISCO Packet tracer. Расчёт стоимости сетевого оборудования и программного.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
IPv4 адресация, маска подсети. Решение задач на разбиение сети на подсети. IPv6 адресация, маска подсети. Решение задач на разбиение сети на подсети. *Маршрутизация в IPv4 пространстве адресов. Маршрутизация в IPv6 пространстве адресов.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5 ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Изучение демилитаризованная зоны - реализация на маршрутизаторе с использованием zone based firewall.	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	

Разработка алгоритма и интерфейса программы анализа информационных рисков и её тестирование. *Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации. *Организация защищенных каналов передачи данных для объединения территориально распределенных офисов в одну сеть*.	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Разработка политик безопасности и внедрение их в операционные системы. *Обеспечение безопасности Wi-Fi-сетей.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Настройка ipsec и VPN. Настройка межсетевых экранов. *Реализация мер по обеспечению безопасности электронной почты в корпоративной сети*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств. *Защита от атак типа "фишинг".*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Настройка защиты беспроводных сетей с помощью систем шифрования.	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Архивация и восстановление ключей в windowsserver (PKI).	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5 ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Установка и настройка системы обнаружения атак Snort. Работа со встроенными сканерами диагностики и управления. Обеспечение сетевой безопасности.	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	

Производственная практика

Виды работ	**Проверяемые результаты: требования к практическому**	**Документ, подтверждающий качество**

	опыту и коды формируемых профессиональных, общих компетенций, умений (ПО, ПК, ОК,У)	**выполнения работ**
1. Вводный инструктаж по ТБ и ПБ. Знакомство с предприятием. *Общие требования охраны труда. Требования охраны труда перед началом работы. Требования охраны труда во время работы. Требования охраны труда в аварийных ситуациях. Требования охраны труда по окончании работы. Основные правила гигиены труда и внутреннего распорядка. Рациональные приемы работы и способы организации труда и рабочего места. Составление структуры предприятия. Определение функций специалистов предприятия. Определение перспективы развития производства. Составление плана освоения новых технологий. Организационная структура предприятия / организации, базового подразделения. Круг решаемых задач. Используемое программное обеспечение. Функции и назначения подразделений предприятия / организации. Производственные связи между структурными подразделениями объекта практики. Перечень и конфигурация технических средств вычислительной техники виды вычислительной техники, их характеристики, средства коммуникаций, оснащение техническими средствами работников предприятия.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	Аттестационный лист по производственной практике
2. Ознакомление с проводимыми на ЛВС предприятия регламентные технические осмотры объектов сетевой инфраструктуры. *Определение проведения на предприятии мониторинга и анализа работы локальной сети и регулярное резервирование. Перечень и назначение программных средств, установленных на ПК предприятия*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
3. Знакомство с архитектурой системы управления сетью предприятия. *Структуры системы управления сетью. Архитектура сети.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК	

Использование удалённого администрирования в управлении сетью предприятия. Управление отказами. Выявление, определение и устранение последствий сбоев и отказов в работе сети. Настройка активного и пассивного сетевого оборудования. Построение физической топологии сети Проведение профилактического обслуживания оборудования компьютерных сетей.	4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
4. Используемые программные или аппаратно-программные системы в сетях предприятия. *Функции мониторинга, анализ трафика в сетях предприятия. Выявление причин аномальной работы сети предприятия.* *Приведения сети в работоспособное состояние. Локализации неисправностей сети. Контрольно-измерительная аппаратура предприятия.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
5. Применение хранилищ данных и резервного копирования данных на предприятии.	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
6. Применение и методы аутентификации, авторизации и администрирования действий пользователей в локальной сети. *Применение и используемые методы криптографической защиты информации и электронной цифровой подписи. Управление подсистемой контроля входа в ЛВС предприятия.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
7. Использование виртуальных защищённых сетей VPN. *Управление подсистемой управления доступом к БД предприятия. Технологии анализа защищённости и обнаружения атак. Администрирование баз данных, создание, редактирование, заполнение таблиц.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Установка на серверы и рабочие станции: операционные системы и необходимое для работы программное обеспечение. *Анализ журналов операционной системы, контроль доступа, обеспечение целостности и сохранности данных.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	

Осуществление конфигурирования программного обеспечения на серверах и рабочих станциях.	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Поддержка в работоспособном состоянии программное обеспечение серверов и рабочих станций.	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Регистрация пользователей локальной сети и почтового сервера, назначает идентификаторы и пароли. *Настройка и применение протоколов управления сетью. Мониторинг и анализ сетевого трафика и сетевых узлов.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Установка прав доступа и контроль использования сетевых ресурсов. *Участие в настройке и управлении доступом, производительностью, безопасностью, ошибками. Настройка беспроводных локальных сетей. Управление учетными записями в доменной сети. Удаленное управление рабочими станциями и серверным оборудованием.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Обеспечение своевременного копирования, архивирования и резервирования данных.	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования. *Применение диагностического оборудования. Участие в планировании восстановительных работ после сбоя.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Выявление ошибок пользователей и программного обеспечения и принятие мер по их исправлению. *Разработка функциональных схем элементов автоматизированной системы защиты информации.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Проведение мониторинга сети, разрабатывать предложения по развитию инфраструктуры сети. *Анализ входящего и исходящего трафика.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6.	

	ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Работа с кабельными сканерами и тестерами	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия. *Участие в разработке регламентов профилактических осмотров. Мониторинг и анализ сети с применением программных и аппаратных средств. Контроль утечки конфиденциальной информации, участие в разработке политик безопасности. Настройка систем обнаружения атак.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Осуществление антивирусной защиты локальной вычислительной сети, серверов и рабочих станций. *Установка и настройка средств обеспечения антивирусной защиты для Веб и почтового трафика.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
Документирование всех произведенных действий. *Заполнение технической документации.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	
8. Подготовка отчетной документации по практике. *Оформление отчетной документации по итогам производственной практики в соответствии с требованиями. Сдача отчетной документации по практике.*	ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ПК 1.6 ПК 1.7 ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ПО. У1. У2. З1. З2. З3. З4. З5. З6. З7.	

3.2. КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Промежуточная аттестация является основной формой контроля в период обучения студентов. Периодичность, формы и сроки проведения

промежуточной аттестации определяются учебным планом по специальности.

Перечень форм промежуточной аттестации по элементам профессионального модуля

Элемент модуля	**Формы промежуточной аттестации**
МДК 01.01	*Экзамен*
МДК 01.02	*Экзамен*
УП 01.01	*Дифференцированный зачет*
ПП 01.01	*Дифференцированный зачет*
ПМ 01(в целом)	*Экзамен квалификационный*

3.2.1.Материалы для проведения промежуточной аттестации

Материально-техническое обеспечение контрольно-оценочных мероприятий № «Информатика»

Оборудование учебного кабинета:

- рабочее место преподавателя;
- посадочные места по количеству студентов;

Технические средства обучения:

- компьютер с программным обеспечением
- мультимедийный проектор
- мультимедийное оборудование;

– принтер лазерный;

– сканер;

– аудиосистема;

– локальная сеть;

– подключение к глобальной сети Интернет;

Итоговый контроль освоения вида профессиональной деятельности **Эксплуатация объектов сетевой инфраструктуры** осуществляется на экзамене (квалификационном). Условием допуска к экзамену

(квалификационному) является положительная аттестация по МДК, учебной практике и производственной практике.

Экзамен (квалификационный) проводится в виде выполнения теоретических и практических заданий.

Промежуточный контроль освоения профессионального модуля осуществляется при проведении дифференцированного зачета по МДК, учебной и производственной практике. Предметом оценки освоения МДК являются умения и знания.

Условием положительной аттестации (вид профессиональной деятельности освоен) на экзамене квалификационном является положительная оценка освоения всех профессиональных компетенций по всем контролируемым показателям. При отрицательном заключении хотя бы по одной из профессиональных компетенций принимается решение «вид профессиональной деятельности не освоен».

Промежуточный контроль освоения профессионального модуля осуществляется при проведении дифференцированного зачета по МДК и дифференцированного зачета по учебной и производственной практике. Предметом оценки освоения МДК являются умения и знания.

Предметом оценки по учебной и (*или*) производственной практике является приобретение практического опыта *(может быть также освоение общих и профессиональных компетенций, умений, в зависимости от этого далее надо использовать различные формы)*.

Контроль и оценка по учебной и (или) производственной практике проводится на основе характеристики обучающегося с места прохождения практики, составленной и завизированной представителем образовательного учреждения и ответственным лицом организации (базы практики).

Задания для оценки освоения учебной дисциплины (промежуточная аттестация)

МДК 01.01. Компьютерные сети

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Билет №1.

1. Эволюция вычислительных систем. Системы пакетной обработки. Многотерминальные системы. Появление глобальных сетей.

2. Система выделенных серверов организации. Функции выделенного сервера.

3. Перевести в двоичную систему и записать в восьмиразрядной сетке IP-адрес 192.168.1.1

Билет №2.

1. Эволюция вычислительных систем. Первые локальные сети. Создание стандартных технологий локальных сетей. Стр.

2. Система выделенных серверов организации. Аппаратная реализация выделенного сервера. Размещение выделенных серверов организации.

3. Построить в эмуляторе Cisco Packet Tracer сегмент сети из 2-х компьютеров на основе концентратора. Выставить на компьютерах произвольные адреса и маски из одного сетевого сегмента.

Билет №3.

1. Вычислительные сети как распределённые системы. Мультипроцессорные компьютеры. Многомашинные вычислительные комплексы. Вычислительные сети.

2. Логическое структурирование локальной сети организации. Виртуальные сети VLAN. Управляемые коммутаторы с поддержкой VLAN.

3. Записать в двоичной форме маску сети, соответствующую IP-адресу 192.100.100.100

Билет №4.

1. Классификация компьютерных сетей. Классификация по территориальному признаку. Классификация по масштабам подразделения.

2. Логическое структурирование локальной сети организации. Типовая физическая структура сети предприятия. Логическая структура локальной сети.

3. Записать в тетради базовые настройки сетевого интерфейса для произвольного статического IP-адреса класса С.

Билет №5.

1. Преимущества использования компьютерных сетей.

2. Технология PoE. Использование коммутаторов PoE. Использование инжекторов для питания устройств PoE. Пассивный PoE.

3. Разбить доменный адрес fttp://ftp-arch.ucl.ac.uk на смысловые элементы. Дать каждому элементу соответствующее пояснение.

Билет №6.

1. Основные программные и аппаратные компоненты сети. Топология физических и логических связей. Полносвязная топология.

2. Исполнение структурированных кабельных систем. Назначение и состав СКС. Реализация линий передачи данных в составе СКС.

3. Начертить в тетради локальную сеть организации на основе корневого коммутатора и коммутаторов трёх отделов. В первом отделе работает три сотрудника, а во втором и третьем по два. Выставить на компьютерах IP-адреса из одного сетевого сегмента.

Билет №7.

1. Основные программные и аппаратные компоненты сети. Ячеистая топология. Топология «общая шина». Топология «звезда». Топология «кольцо». Составные топологии.

2. Исполнение структурированных кабельных систем. Использование составных линий в составе СКС. Выбор патч-корда.

3. Полоса пропускания канала составляет 1 кГц. Мощность сигнала превышает мощность шума в линии в 15 раз. Определить пропускную способность канала.

Билет №8.

1. Линии связи. Физическая среда передачи данных. Проводные и кабельные линии связи. Радиоканалы наземной и спутниковой связи.

2. Группа стандартов 802.11. Частотные полосы и каналы в стандартах 2,4 ГГц. Сети Wi-Fi.

3. Закодируйте цифровые данные одного байта 0101 1000, используя потенциальный код без возвращения к нулю (NRZ). Начертите импульсную схему кодирования.

Билет №9.

1. Линии связи. Коаксиальный кабель. Витая пара. Волоконно-оптический кабель.

2. Группа стандартов 802.11. Структура сети Wi-Fi. Безопасность сети Wi-Fi. Преимущества и недостатки сети Wi-Fi.

3. Запишите в двоичном и в десятичном виде стандартные маски сетевых классов A, B и C.

Билет №10.

1. Кодирование цифровых данных. Различные подходы к кодированию цифровых данных. Аналоговое кодирование (модуляция) цифровых данных. Цифровое кодирование данных.

2. Разделка UTP и монтаж коннектора RJ-45. Порядок разделки и монтажа.

3. Для класса сетевых IP-адресов C запишите две возможные маски, позволяющие разделить сеть на две независимые подсети. Для каждой маски напишите пример адреса, удовлетворяющего этой маске.

Билет №11.

1. Кодирование цифровых данных. Потенциальный код без возвращения к нулю NRZ. Биполярный код AMI (NRZI).

2. Разделка UTP и монтаж коннектора RJ-45. Тестирование коннектора RJ-45. Проблема кроссирования кабелей, прямой и кроссированный кабель.

3. Начертить в тетради схему локальной сети организации на основе корневого коммутатора и двух коммутаторов отделов. В каждом отделе должно быть по два рабочих места сотрудника. Выставить на конечных сетевых устройствах IP-адреса и маски из одного сетевого сегмента.

Билет №12.

1. Проблемы передачи данных. Искажение сигнала. Проблемы синхронизации передатчика и приёмника.

2. Эволюция вычислительных систем. Современные тенденции развития сетевых технологий.

3. Построить таблицу соответствия стека протоколов TCP/IP и OSI.

Билет №13.

1. Проблемы передачи данных. Контроль достоверности данных. Организация совместного использования линий связи.

2. Локальная сеть организации на основе Fast Ethernet.

3. Начертить схему взаимодействия интерфейсов и протоколов двух узлов A и B для сетевого стека, состоящего из 4-х уровней (физический, канальный, сетевой, транспортный).

Билет №14.

1. Характеристики линий связи.

2. Спецификации Ethernet по физической среде передачи. Спецификация 10Base-5 (IEEE 802.3). Спецификация 10Base-2 (802.3a).

3. Начертить схему прямого обжима для раскладки T568B. Указать на схеме цвета жил.

Билет №15.

1. Режимы передачи данных. Симплекс, полудуплекс и полный дуплекс.

2. Спецификации Ethernet по физической среде передачи. Спецификация 10Base-T (802.3i). Спецификация 100Base-T (Fast Ethernet, 802.3u).

3. Начертить схему кроссированного кабеля. Указать на схеме цвета жил.

Билет №16.

1. Система отношений «клиент-сервер». Понятия «клиент» и «сервер». Сетевая операционная система.

2. Общая идеология технологии Ethernet.

3. Построить таблицу соответствия стека протоколов IPX/SPX (Novell) и OSI.

Билет №17.

1. Система отношений «клиент-сервер». Одноранговые сети и сети с выделенным сервером. Сетевые приложения.

2. Стандартизация протоколов локальных сетей.

3. Построить в эмуляторе Cisco Packet Tracer сегмент на основе коммутатора по топологии «звезда», подключённый к внешней сети Интернет. В сегменте должно быть три ПК.

Билет №18.

1. Взаимодействие открытых систем. Протоколы и интерфейсы. Модель OSI.

2. Служба DNS. Ключевые понятия DNS. Основные принципы организации и функционирования DNS.

3. Запишите первые байты адресов каждого сетевого класса A, B, C, D, E. Таблица на

Билет №19.

1. Взаимодействие открытых систем. Уровни модели OSI. Соответствие популярных стеков протоколов модели OSI.

2. Распределения IP-адресов. Ручная настройка IP-адреса.

3. Закодируйте цифровые данные одного байта 0101 1000, используя манчестерский код. Начертите импульсную схему кодирования.

Билет №20.

1. Адресация узлов в компьютерных сетях. Требования к схеме назначения адресов (имён).

2. Распределения IP-адресов. Распределение IP-адресов службой DHCP.

3. Найти ширину полосы пропускания канала связи, если известно, что пропускная способность канала составляет 10 000 бит/с, а мощность сигнала превосходит мощность шума в линии в 31 раз.

Билет №21.

1. Адресация узлов в компьютерных сетях. Схемы адресации. Аппаратные, символьные и числовые адреса.

2. Адресация IPv4. Использование масок при администрировании локальных сетей.

3. Записать в двоичной форме маску сети, соответствующую IP-адресу 128.250.64.32 128_{10} = 1000 0000_2 начало байта – 10. Следовательно класс адресов В. У класса В маска 255.255.0.0 или 1111 1111.1111 1111.0000 0000.0000 0000

Билет. №22.

1. Стек протоколов TCP/IP. Состав стека протоколов TCP/IP. Прикладные протоколы TCP/IP.

2. Адресация IPv4. Классы адресов IPv4.

3. Начертить в тетради схему сети по топологии общая шина, содержащую 4 компьютера. Выставить на компьютерах произвольные адреса из класса В.

Билет №23.

1. Стек протоколов TCP/IP. Порты TCP и UDP.

2. Адресация IPv4. Запрещённые адреса.

3. Построить в эмуляторе Cisco Packet Tracer сегмент сети на основе коммутатора для двух компьютеров. Выставить на компьютерах адреса из одного сетевого сегмента.

Билет №24.

1. Исполнение структурированных кабельных систем. Прокладка силовых кабелей в составе СКС. Требования пожарной безопасности.

2. Адресация IPv4. Схемы адресации узлов в сетях TCP/IP.

3. Записать в двоичной форме маску сети, соответствующую IP-адресу 126.1.2.3

Билет №25.

1. Кодирование цифровых данных. Биполярный импульсный код. Манчестерский код.
2. Адресация IPv4. Физическая структура IP-адреса IPv4.
3. Построить в эмуляторе Cisco Packet Tracer сеть, состоящую из двух компьютеров, соединённых патч-кордом. Выставить на компьютерах IP-адреса из класса C.

МДК.01.02. Организация, принципы построения и функционирования компьютерных сетей

ПК, ОК, формируемые в процессе выполнения практических работ ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Билет №1

1. Компьютерные сети. Типы сетей передачи данных.

2. Трансляция сетевых адресов NAT. Назначение и основные виды NAT. Перегруженный NAT.

3. Построить сеть на основе коммутатора и четырёх ПК. Используя различные маски переменной длины, изолировать трафик ПК1 и ПК2 от ПК3 и ПК4.

Билет №2

1. Понятие сетевого протокола. Основные типы сетевых протоколов.

2. Настройка протокола динамической маршрутизации OSPFv2.

3. Имеется сеть на основе двух L2-коммутаторов. К каждому коммутатору подключены по три ПК. Создать три сетевых сегмента на основе VLAN, по одному сегменту на каждом коммутаторе и третий сегмент сделать распределённый по двум коммутаторам.

Билет №3

1. Модель OSI. Уровни передачи данных. Основные функции уровня.

2. Протокол динамической маршрутизации EIGRP. Особенности, преимущества и недостатки.

3. Построить сеть на основе двух L2-коммутаторов с конфигурационной петлёй, т.е. коммутаторы соединены двумя линками. К каждом коммутатору подключены по два ПК. Настроить работу EtherChannel между коммутаторами.

Билет №4

1. Адресация в сетях передачи данных. Сетевые IP-адреса.

2. Диагностика неисправностей в работе протокола динамической маршрутизации EIGRP.

3. Построить сеть на основе двух L2-коммутаторов и четырёх подключенных к ним ПК, по два к каждому. Задать на каждом коммутационном сегменте разные маски и адреса. Подключить L2-коммутаторы к маршрутизатору и настроить получить на нём связь двух сегментов коммутации.

Билет №5

1. Основы коммутации. Коллизии, домен коллизий. Широковещательный домен. Симметричное и асимметричное коммутирование.

2. Соединение «точка-точка». Протокол PPPoE.

3. Построить сеть на основе двух L3-коммутаторов и двух подключенных к ним ПК, по одному к каждому. Выставить на каждом ПК IP-адреса из разных классов. Прописать на каждом маршрутизаторе дефолтные маршруты так, чтобы ПК могли пинговать друг друга.

Билет №6

1. Виртуальные локальные сети VLAN. Порты доступа и транковые порты.

2. Мониторинг сети. Мониторинг web-сервера. Утилита tcpdump.

3. Построить сеть на основе двух маршрутизаторов и двух подключенных к ним ПК, по одному к каждому. Выставить на каждом ПК IP-адреса из разных классов. Прописать на каждом маршрутизаторе дефолтные маршруты так, чтобы ПК могли пинговать друг друга.

Билет №7

1. Основы маршрутизации. Метрика, домен маршрутизации, конвергенции в сетях.

2. Поиск и устранение неполадок в сети. Отладка сети.

3. Построить сеть на основе L2-коммутатора, двух подключенных к нему ПК и одного сервера. Настроить на сервере протокол динамической адресации DHCP. Получить на каждом ПК IP-адреса от DHCP-сервера.

Билет №8

1. Статическая маршрутизации. Её достоинства и недостатки. Особенности настройки и диагностики.

2. Основы сетевой безопасности. Назначение и основные функции протокола AAA.

3. Построить сеть на основе двух маршрутизаторов. К первому маршрутизатору подключен ПК, имитирующий ЛВС, ко второму маршрутизатору подключен сервер, имитирующий сервер провайдера. Между маршрутизаторами имеет кроссовый линк. Настроить на маршрутизаторе ЛВС NAT типа PAT.

Билет №9

1. Протоколы динамической маршрутизации RIP и RIPv2. Особенности, преимущества и недостатки.

2. Виртуальные частные сети VPN. Основные понятия и виды.

3. Построит сеть на основе трёх последовательно соединённых маршрутизаторов. К двум крайним маршрутизаторам цепочки подключены по одному ПК. Настроить на маршрутизаторах работу протокола OSPF так, чтобы ПК могли пинговать друг друга.

Билет №10

1. Динамическая конфигурация и адресация сетевых узлов, протокол DHCP.

2. Виртуальные сети. Функция Anti-Replay, туннелирование. Динамические многоточечные виртуальные частные сети DMVPN.

3. Построить сеть на основе двух L2-коммутаторов, подключенных маршрутизатору. К каждому коммутатору подключены по два ПК, имеющие IP-адреса разных классов. Настроить маршрутизатор так, чтобы все ПК могли пинговать друг друга.

Билет №11

1. Основные понятия протокола STP. Корневой и назначенный коммутатор. Расчёт стоимости маршрута. Состояния портов в STP.

2. Технология IPSec. Транспортный и туннельный режимы. Протокол управления ключами ISARMP.

3. Построить сеть на основе L2-коммутатора и четырёх подключенных к нему ПК. Настроить на ПК1 и ПК2 маски из класса B, а на ПК3 и ПК4 маски из класса C. Подключить L2-коммутатор к маршрутизатору и создать на нём стандартные списки доступа, позволяющие ПК1 «видеть» ПК3, но запрещающие связи: ПК1-ПК4 и ПК2-ПК3.

Билет №12

1. Беспроводные локальные сети WLAN. Зона покрытия, пропускная способность, помехи, потребляемая мощность, стоимость. WAP, микросота.

2. Сетевые системы обнаружения вторжений.

3. Построить сеть на основе L2-коммутатора и четырёх подключенных к нему ПК. Выделить ПК1 и ПК2 в VLAN2, а ПК3 и ПК4 в VLAN3. Подключить L2-коммутатора к маршрутизатору. Настроить на маршрутизаторе расширенный список доступа разрешающий http-протокол между VLAN.

Билет №13

1. Поиск и устранение неисправностей в беспроводных локальных сетях.

2. Сетевые эмуляторы. Назначение и основные функции Cisco Packet Tracer. (см. практические работы)

3. Построить сеть на основе L2-коммутатора, двух подключенных к нему ПК и одного публичного DMZ-сервера. Подключить L2-коммутатор к межсетевому экрану Sisco ASA. Межсетевой экран подключить к

маршрутизатору провайдера, к которому также подключить сервер. Настроить на Cisco ASA инспектирование трафика таким образом, чтобы сервер, находящийся в локальной сети, был доступен из сети провайдера, но с данного сервера ЛВС была недоступна.

Билет №14

1. Протоколы WLAN. Их классификация, различия, преимущества и недостатки. WiFi.

2. Сетевые системы предотвращения вторжений.

3. Построить сеть на основе L2-коммутатора и шести подключенных к нему ПК. Разделить все ПК на три VLAN (2, 3 и 4) по два ПК в каждой. Подключить L2-коммутатор к маршрутизатору. Настроить на маршрутизаторе списки доступа, разрешающие связь между VLAN2 и VLAN4.

Билет №15

1. Агрегирование каналов на основе EtherChannel.

2. Протокол сетевого времени NTP. Назначение и алгоритм работы.

3. Построить сеть на основе L2-коммутатора и четырёх подключенных к нему ПК. Выделить ПК1 и ПК2 в VLAN2, а ПК3 и ПК4 в VLAN3. Подключить L2-коммутатора к маршрутизатору. Настроить на маршрутизаторе расширенный список доступа позволяющий выполнять пинг между VLAN.

Билет №16

1. Масштабирование сетей. Принцип работы протокола STP, протокол RSTP.

2. Технология IPSec, её место в модели OSI. Протоколы AH и ESP.

3. Построить сеть на основе двух маршрутизаторов, к каждому из которых подключен ПК. Настроить на маршрутизаторах работу протокола динамической маршрутизации EIGRP.

Билет №17

1. Протокол динамической маршрутизации OSPF и OSPFv2. Особенности, преимущества и недостатки.

2. Виртуальные частные сети VPN. Удалённый доступ (Remote Access) и создание распределённых виртуальных локальных сетей (Site-to-Site).

3. Построить сеть на основе L2-коммутатора, к которому подключены три ПК. Выделить каждый ПК в отдельную VLAN. Подключить L2-коммутатора транковым линком к L3-коммутатору. Настроить на L3-коммутаторе маршрутизацию между VLAN-сегментами на основе VLAN-интерфейсов.

Билет №18

1. Динамическая маршрутизации. Её достоинства и недостатки. Особенности настройки и диагностики.

2. Технология IPSec, основные понятия. Протоколы PAP и CHAP. OTP и цифровые сертификаты. Биометрия, контекстуальные проверки

3. Построить сеть на основе двух маршрутизаторов, к каждому из которых подключен ПК. Настроить на маршрутизаторах работу протокола динамической маршрутизации OSPF.

Билет №19

1. Основы маршрутизации. Типы протоколов маршрутизации. Автономная система.

2. Протокол сетевого управления SNMP. Назначение, алгоритм работы.

3. Построить сеть на основе L2-коммутатора. Подключить L2-коммутатор к маршрутизатору. Настроить на маршрутизаторе работу DHCP-протокола. Получить на каждом ПК IP-адреса от DHCP-сервера.

Билет №20

1. Принцип маршрутизации. Типы маршрутов. Административное расстояние.

2. Широкополосный доступ, DSL. Типы широкополосного доступа, преимущества и недостатки.

3. Построить сеть на основе двух маршрутизаторов и двух подключенных к ним ПК, по одному к каждому. Выставить на каждом ПК IP-адреса из разных классов. Прописать на каждом маршрутизаторе статические, но не дефолтные, маршруты так, чтобы ПК могли пинговать друг друга.

Билет №21

1. Виртуальные локальные сети VLAN. Назначение, основные функции. VLAN по умолчанию.

2. Соединение «точка-точка». Протокол PPP. Протоколы LCP и NCP.

3. Построить сеть на основе двух L3-коммутаторов и двух подключенных к ним ПК, по одному к каждому. Выставить на каждом ПК IP-адреса из разных классов. Прописать на каждом маршрутизаторе статические, но не дефолтные, маршруты так, чтобы ПК могли пинговать друг друга.

Билет №22

1. Принцип коммутации. Симплексный, полудуплексный и дуплексный режимы. Одноадресная, многоадресная и широковещательная связь.

2. Диагностика неисправностей в работе протокола динамической маршрутизации OSPF.

3. Построить сеть на основе одного L2-коммутатора, к которому подключены четыре ПК. Выделить ПК1 и ПК2 в VLAN2, а ПК3 и ПК4 в VLAN3. Подключить коммутатор к маршрутизатору и настроить на нём связь между сегментами коммутации на основе sub-интерфейсов.

Билет №23

1. Адресация в сетях передачи данных. Физические адреса.

2. Настройка протокола динамической маршрутизации OSPFv6.

3. Построить сеть на основе L2-коммутатора и четырёх подключенных к нему ПК. Выделить ПК1 и ПК2 в VLAN2, а ПК3 и ПК4 в VLAN3. Подключить L2-коммутатор к L3-коммутатору. Настроить на L3-коммутаторе маршрутизацию между VLAN-интерфейсами.

Билет №24

1. Уровни сетевой модели стека протоколов TCP/IP.

2. Основные средства диагностики сети с использованием командной строки. Команды ipconfig, ping, tracert, net. (см. лекции)

3. Построить сеть на основе двух L2-коммутаторов с конфигурационной петлёй, т.е. коммутаторы соединены двумя линками. К каждом коммутатору подключены по два ПК. Продемонстрировать работу протокола STP.

Билет №25

1. Сетевые устройства. Их типы и различия.
2. Адресное пространство сетевого протокола. Сетевой протокол нового поколения IPv6. Назначение и основные особенности.
3. Построить сеть на основе L2-коммутатора и четырёх ПК. Изолировать трафик ПК1 и ПК2 в VLAN2, а трафик ПК3 и ПК4 в VLAN3.

3.2.2 Оценка приобретения практического опыта. по учебной и производственной практике профессионального модуля

Целью оценки по учебной и производственной практике является оценка профессиональных и общих компетенций, практического опыта и умений. Оценка по учебной и производственной практике выставляется на основании результатов выполнения комплексной практической работы и данных аттестационного листа (характеристики профессиональной деятельности студента на практике) с указанием видов работ, выполненных студентами во время практики, их объема, качества выполнения в соответствии с технологией и требованиями организации, в которой проходила практика

Задания для промежуточной аттестации по учебной практике, для оценки сформированности общих и профессиональных компетенций.

Дифференцированный зачёт.
По УП.01.01. Учебная практика "Настройка сетевой инфраструктуры»

Вариант-I

1. ***Доступом к сети называют:***
   а. взаимодействие станции (узла сети) со средой передачи данных для обмена информацией с другими станциями;
   б. взаимодействие станции со средой передачи данных для обмена информацией с друг с другом;
   в. это установление последовательности, в которой станции получают доступ к среде передачи данных;
   г. это установление последовательности, в которой серверы получают доступ к среде передачи данных.

2. Конфликтом называется:

а. ситуация, при которой две или более станции "одновременно" бездействуют;

б. ситуация, при которой две или более станции "одновременно" пытаются захватить линию;

в. ситуация, при которой два или более сервера "одновременно" пытаются захватить линию;

г. ситуация, при которой сервер и рабочая станция "одновременно" пытаются захватить линию.

3. Дискретная модуляция это…

а. процесс представления цифровой информации в дискретной форме;

б. процесс представления синусоидального несущего сигнала;

в. процесс представления на основе последовательности прямоугольных импульсов;

г. процесс представления аналоговой информации в дискретной форме.

4. Коммуникационный протокол описывающий формат пакета данных называется:

а. TCP|IP

б. TCP

в. UPD

г. IP

5. Метод потенциального кодирования NRZ это…

д. метод биполярного кодирования с альтернативной инверсией;

е. метод без возвращения к нулю;

ж. метод с потенциальным кодом с инверсией при единице;

з. биполярный импульсный код.

6. Маршрутизация это…

а. это правило назначения выходной линии связи данного узла связи ТКС для передачи пакета, базирующегося на информации, содержащейся в заголовке пакета (адреса отправителя и получателя), и информации о загрузке этого узла (длина очередей пакетов) и, возможно, ТКС в целом;

б. это процесс передачи данных с одного ПК на другой ПК, когда эти ПК находятся в разных сетях;

в. это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до пункта назначения;

г. специализированный сетевой компьютер, имеющий как минимум один сетевой интерфейс и пересылающий пакеты данных между различными сегментами сети, связывающий разнородные сети различных архитектур, принимающий решения о пересылке на основании информации о топологии сети и определённых правил, заданных администратором.

7. Какие способы маршрутизации существуют:

а. централизованная, распределенная, смешанная;

б. адаптивная, децентрализованная, смешанная;

в. прямая, косвенная, смешанная;

г. прямая, децентрализованная, центральная.

8. Компьютерная сеть это …

а. группа компьютеров связанных между собой с помощью витой пары;

б. группа компьютеров связанных между собой;

в. система связи компьютеров или вычислительного оборудования (серверы, маршрутизаторы и другое оборудование);

г. группа компьютеров обменивающихся информацией.

9. Узел сети, с помощью которого соединяются две сети построенные по одинаковой технологии:

а. мультиплексор;

б. хаб;

в. шлюз;

г. мост.

10. Сервер-это?

а. сетевая программа, которая ведёт диалог одного пользователя с другим;

б. мощный компьютер, к которому подключаются остальные компьютеры;

в. компьютер отдельного пользователя, подключённый в общую сеть;

г. стандарт, определяющий форму представления и способ пересылки сообщения.

11. В компьютерной сети Интернет транспортный протокол TCP обеспечивает:

а. передачу информации по заданному адресу

б. способ передачи информации по заданному адресу

в. получение почтовых сообщений

г. передачу почтовых сообщений

12. Компьютер, подключённый к Интернету, обязательно должен иметь:

а. Web – сайт**;**

б. установленный Web – сервер;

в. IP – адрес;

г. брандмауэр.

13. Как по-другому называют корпоративную сеть:

а. глобальная

б. региональная

в. локальная

г. отраслевая

14. Домен-это...

а. часть адреса, определяющая адрес компьютера пользователя в сети

б. название программы, для осуществления связи между компьютерами

в. название устройства, осуществляющего связь между компьютерами

г. единица скорости информационного обмена

15. Провайдер – это:

а. владелец узла сети, с которым заключается договор на подключение к его узлу;

б. специальная программа для подключения к узлу сети;

в. владелец компьютера с которым заключается договор на подключение его компьютера к узлу сети;

г. аппаратное устройство для подключения к узлу сети.

16. Сетевой шлюз это:

а. встроенный межсетевой экран;

б. устройство подключения компьютера к телефонной сети

в. устройство внешней памяти

г. аппаратный маршрутизатор или программное обеспечение для сопряжения компьютерных сетей, использующих разные протоколы.

17. Коммутация – это:

а. это процесс передачи данных с одного ПК на другой ПК, когда эти ПК находятся в разных сетях;

б. процесс соединения абонентов коммуникационной сети через транзитные узлы.

в. это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до пункта назначения;

г. специализированный сетевой компьютер, имеющий как минимум один сетевой интерфейс и пересылающий пакеты данных между различными сегментами сети, связывающий разнородные сети различных архитектур, принимающий решения о пересылке на основании информации о топологии сети и определённых правил, заданных администратором.

18. В зависимости от направления возможной передачи данных способы передачи данных по линии связи делятся на следующие типы:

а. полусимплексный, полудуплексный, симплексный;
б. полусимплексный, полудуплексный, дуплексный;
в. дуплексный, полудуплексный, симплексный;
г. симплексный, дуплексный.

19. При частотном методе уплотнении происходит:

а. передача информации в цифровом виде;
б. процесс распространения оптического излучения в многомодовом оптическом волокне;
в. увеличения пропускной способности систем передачи информации;
г. передача информационного потока по физическому каналу на соответствующей частоте – поднесущей.

20. В функции канального уровня входит:

а. формирование кадра, контроль ошибок и повышение достоверности, обеспечение кодонезависимой передачи, восстановление исходной последовательности блоков на приемной стороне, управление потоком данных на уровне звена, устранение последствий потерь или дублирования кадров;
б. формирование кадра, контроль ошибок и повышение достоверности, обеспечение кодозависимой передачи, восстановление исходной

последовательности блоков на приемной стороне, управление потоком данных на уровне звена, устранение последствий потерь или дублирования кадров;

в. контроль ошибок и повышение достоверности, обеспечение кодозависимой передачи, восстановление исходной последовательности блоков на передающей стороне, управление потоком данных на уровне звена, устранение последствий потерь или дублирования кадров;

г. контроль ошибок и повышение достоверности, обеспечение кодозависимости передачи, восстановление исходной последовательности блоков на передающей стороне, управление потоком данных на уровне звена.

Вариант-II

1. Управлением доступа к среде называют:

а. взаимодействие станции (узла сети) со средой передачи данных для обмена информацией с другими станциями;

б. взаимодействие станции со средой передачи данных для обмена информацией с друг с другом;

в. это установление последовательности, в которой станции получают доступ к среде передачи данных;

г. это установление последовательности, в которой серверы получают доступ к среде передачи данных.

2. Типичная среда передачи данных в ЛВС это…

а. отрезок (сегмент) коаксиального кабеля;

б. сетевой адаптер подключенный к витой паре;

в. маршрутизатор связанный с контроллером;

г. среда распространения Wi Fi.

3. Аналоговая модуляция это…

а. процесс представления цифровой информации в дискретной форме;
б. передача дискретных данных по каналам связи
на основе последовательности прямоугольных импульсов;
в. передача дискретных данных по каналам связи
на основе синусоидального несущего сигнала;
г. процесс представления аналоговой информации в дискретной форме.

4. Программа, взаимодействующая с сетевым адаптером называется:

а. сетевой драйвер
б. передающая среда
в. мультиплексор
г. сетевой адаптер

5. Метод потенциального кодирования AMI это…

а. метод биполярного кодирования с альтернативной инверсией;
б. метод без возвращения к нулю;
в. метод с потенциальным кодом с инверсией при единице;
г. биполярный импульсный код.

6. Алгоритм маршрутизации это…

а. это правило назначения выходной линии связи данного узла связи ТКС для передачи пакета, базирующегося на информации, содержащейся в заголовке пакета (адреса отправителя и получателя), и информации о загрузке этого узла (длина очередей пакетов) и, возможно, ТКС в целом;
б. это процесс передачи данных с одного ПК на другой ПК, когда эти ПК находятся в разных сетях;
в. это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до пункта назначения;
г. специализированный сетевой компьютер, имеющий как минимум один сетевой интерфейс и пересылающий пакеты данных между различными

сегментами сети, связывающий разнородные сети различных архитектур, принимающий решения о пересылке на основании информации о топологии сети и определённых правил, заданных администратором.

7. Какие методы маршрутизации существуют:

а. прямая, децентрализованная, адаптивная;
б. адаптивная, децентрализованная, смешанная;
в. прямая, фиксированная, смешанная;
г. простая, фиксированная, адаптивная.

8. Сервер, служащий для хранения файлов, которые используются всеми рабочими станциями называется:

а. сервер телекоммуникаций;
б. дисковый сервер;
в. файловый сервер;
г. почтовый сервер.

9. Информация в компьютерных сетях передается по каналам связи в виде отдельных:

а. сообщений;
б. данных;
в. посланий;
г. пакетов.

10. Основными требованиями, предъявляемыми к алгоритму маршрутизации являются:

а. оптимальность выбора маршрута, простота реализации, устойчивость, быстрая сходимость, гибкость реализации;
б. прямой маршрут, помехоустойчивость;

в. передача пакета в узел связи, передача пакета в направлении, не приводящем к минимальному времени его доставки;

г. время доставки пакетов адресату, нагрузка на сеть, затраты ресурса в узлах связи.

11. Для соединения компьютеров в сетях используются кабели различных типов. По какому из них передаётся информация, закодированная в пучке света.

а. витая пара;

б. телефонный;

в. коаксиальный;

г. оптико – волоконный.

12. Задан адрес электронной почты в сети Интернет: user_name@mtu-net.ru***. Каково имя домена верхнего уровня?***

а. ru ;

б. mtu-net.ru;

в. mtu-net;

г. user-name.

13. Как называется узловой компьютер в сети:

а. терминал

б. модем

в. хост-компьютер

г. браузер.

14. Модем это…

а. устройство передачи информации от одного компьютера к другому посредством использования телефонных линий;
б. устройство передачи информации от сервера к рабочей станции;
в. устройство передачи информации только в нутрии локальной сети;
г. устройство передачи аналоговых сигналов от рабочей станции к серверу.

15. Брандмауэр – это:

д. встроенный межсетевой экран;
е. устройство подключения компьютера к телефонной сети;
ж. устройство внешней памяти;
з. компьютер-сервер.

16. Сетевой шлюз это:

а. встроенный межсетевой экран;
б. устройство подключения компьютера к телефонной сети;
в. устройство внешней памяти;
г. аппаратный маршрутизатор или программное обеспечение для сопряжения компьютерных сетей, использующих разные протоколы.

17. Какие схемы коммутации абонентов в сетях существуют:

а. коммутация каналов, сообщений, серверов;
б. коммутация каналов, ячеек, сообщений, пакетов;
в. коммутация каналов, ячеек, рабочих станций, пакетов;
г. коммутация каналов, ячеек, рабочих станций, серверов, пакетов.

18. Коммутация пакетов это:

а. образование непрерывного составного физического канала из последовательно соединенных отдельных канальных участков для прямой передачи данных между узлами;

б. передача единого блока данных между транзитными компьютерами сети с временной буферизацией этого блока на диске каждого компьютера;
в. техника коммутации абонентов, которая была специально разработана для эффективной передачи компьютерного трафика;
г. сетевая программа, которая ведёт диалог одного пользователя с другим.

19. При уплотнении по поляризации происходит:

а. передача информации в цифровом виде;
б. процесс распространения оптического излучения в многомодовом оптическом волокне;
в. увеличения пропускной способности систем передачи информации;
г. уплотнение потоков информации с помощью оптических несущих, имеющих линейную поляризацию.

20. Байт-ориентированные протоколы обеспечивают:

а. передачу пакетов данных, поступающих от протоколов верхних уровней, узлу назначения, адрес которого также указывает протокол верхнего уровня;
б. возможность представления информации 8-битным расширенным двоичным кодом EBCDIC;
в. управление передачей данных, представляемых байтами;
г. уплотнение потоков информации с помощью оптических несущих, имеющих линейную поляризацию.

Эталон ответа

Вариант-I

Вопрос	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***	***13***	***14***	***15***	***16***	***17***	***18***	***19***	***20***
Ответ	***а***	***б***	***г***	***г***	***б***	***б***	***а***	***в***	***г***	***б***	***б***	***в***	***г***	***а***	***а***	***г***	***б***	***в***	***г***	***а***

Вариант-II

Вопрос	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***	***13***	***14***	***15***	***16***	***17***	***18***	***19***	***20***
Ответ	***в***	***а***	***б***	***а***	***а***	***а***	***г***	***в***	***г***	***а***	***г***	***а***	***в***	***а***	***а***	***г***	***б***	***в***	***г***	***в***

Задания для промежуточной аттестации по производственной практике, для оценки сформированности общих и профессиональных компетенций

Дифференцированный зачёт.

По ПП.01.01. Учебная практика "Настройка сетевой инфраструктуры»

1. Что такое фишинг?

a) Техника безопасности, используемая для защиты сетевых ресурсов.

b) Незаконные действия для получения личной информации пользователей.

c) Программа для выявления компьютерных вирусов.

2. Какую роль играет пароль в кибербезопасности?

a) Защищает от вирусов и вредоносных программ.

b) Позволяет пользователям получать доступ к защищенным ресурсам.

c) Обеспечивает шифрование информации.

3. Что такое двухфакторная аутентификация?

a) Метод защиты, использующий два разных пароля.

b) Метод проверки личности, который требует двух независимых подтверждений.

c) Метод защиты, использующий шифрование данных.

4. Что такое межсетевой экран (firewall)?

a) Программа для защиты от вредоносных программ.

b) Оборудование или программное обеспечение, контролирующее потоки данных между

сетями.

c) Технология шифрования информации.

5. Что такое DDoS-атака?

a) Попытка получить несанкционированный доступ к системе.

b) Атака на сервер, ограничивающая его доступность.

c) Защитная система, предотвращающая атаки на сеть.

6. Что такое сетевая угроза "мальварь" (malware)?

a) Приложение, разработанное для защиты данных пользователя.

b) Вредоносное программное обеспечение, созданное с целью нанесения вреда системе или

укравшие данные пользователя.

c) Слово, применяемое для описания сигналов или шума в сетях передачи данных.

7. Что такое "фаерфокс" (Firefox)?

a) Один из наиболее популярных интернет-браузеров.

b) Протокол безопасной передачи данных.

c) Система защиты, используемая в криптографии.

8. Что такое "пинг" (ping)?

a) Программа для проверки доступности сетевых узлов.

b) Сетевая угроза, направленная на взлом платежных систем.

c) Метод шифрования информации.

9. Что такое "фильтр спама" (spamfilter)?

a) Программа или устройство, фильтрующее нежелательные электронные сообщения.

b) Шифрование данных для их защиты от несанкционированного доступа.

c) Комплексная система защиты информации в сети.

10. Что такое "вирус" в контексте компьютерной безопасности?

a) Программа для проверки системы на наличие уязвимостей.

b) Программа, распространяющаяся и внедряющаяся в систему без разрешения пользователя,

вызывая различные проблемы.

c) Система, обеспечивающая шифрование данных и их безопасность.

11. Очень сложные пароли гарантируют 100% защиту?

А. Нет

Б. Да, если после работы полностью очищать куки и не хранить пароль на компьютере

В. Да, если пароль не сохранен на компьютере

12. Какие вирусы активизируются после включения ОС?

А. Снифферы

Б. Загрузочные

В. Трояны

Г.Черви

13 .Представляют ли угрозу вирусы для крупных компаний?

А. Нет

Б.Да, представляют

В. Скорее нет. В крупных компаниях развита система безопасности

Г.Если компания обладает сотрудниками занимающимися безопасностью сети, вирусы не

могут нанести такому предприятию вреда

14. С чем связана атака введением произвольных запросов в базу данных?

А. Уязвимость SQL Injection

Б.Сбой Denial of Service

В. Ошибка Denial of Service

Г.Неполадка PHP Include

15. Фильтрация контента, для чего она служит?

А. Защищает от скрытой загрузки вредоносного программного обеспечения

Б.Помогает быстро находить в сети требуемый контент сохраняя при этом много

драгоценного времени

В. Отключает назойливую рекламу

Г.Отсеивает поисковый спам

16. Какой уровень безопасности трафика обеспечивает WPA2?

А. Высокий

Б.Низкий

В. Достаточный для домашней сети

Г.Средний

17. Сколько минимально символов должен содержать безопасный пароль, состоящий из латинских строчных букв?

А. 15

Б.8

В . 10

Г.6

18. Какую угрозу можно назвать преднамеренной? Сотрудник:

А. Открыл письмо содержащее вредоносное ПО

Б.Ввел неправильные данные

В. Совершил не авторизованный доступ

Г.Включил компьютер без разрешения

19. Безопасно ли вводить пароли простым копированием?

А. Безопасно если это мой компьютер

Б.Да

В. Безопасно если после работы очистить куки

Г.Нет

20. Какую защиту необходимо использовать против программы iris или ее аналогов?

А. Шифровать трафик

Б.Использовать очень сложные пароли

В. Устанавливать только лицензионные антивирусы

Г.Не пользоваться Wi-fi

21. Что может привести к заражению компьютера?

А. Получение сообщения по электронной почте

Б.Загрузка пиратского ПО

В. Создание нового файла

Г.Отправка сообщения по электронной почте

22. Что такое Brute Force?

А. Взлом методом заражения системы через вредоносный файл

Б.Метод заставляющий пользователя самому раскрыть конфиденциальную информацию

В. Получение конфиденциальной информации с компьютера методом электронной рассылки

Г.Взлом методом перебора паролей

23. В каком блок файле autorun.inf чаще всего прописывается вредоносная программа?

А. Ореп

Б. Setup

В. Downloade

r.D ll

24Как называется преднамеренно внесенный в программное обеспечение объект, приводящий к действиям программного обеспечения не предусмотренным производителем, приводящим к нарушению конфиденциальности и целостности информации?

А. Троян

Б.Бэкдор

В. Закладка

Г.Вирус

25Безопасно ли сохранять пароли в автозаполнении браузера?

А. Да, если пароль к входу в систему знаю только я один

Б. Нет

В. Да, если этим компьютером пользуюсь только я один

Г Да

26. Для чего служит DLP? Система выполняет функцию:

А. Защита компьютера от вирусов

Б.Выполняет функцию безопасного ввода паролей

В. Пред отвращает утечку информации с компьютера

Г.Предупреждает пользователя о попытках взлома и хакерских атаках

27. Антивирус полностью защищает компьютер от вирусов и атак при работе в сети. Вы согласны с этим?

А. Нет

Б.Да, если это лицензионный антивирус известного производителя

В. Защищает совместно с включенным бродмауэром

Г Да

28. Самый лучший способ хранения паролей в информационной системе?

А. Хеширование

Б.Вообще не сохранять

В. Архивирование

Г.Хранить только с включенным брандмауэром

29. Какое минимальное количество символов должен содержать пароль входа субъектов в систему АС, при классе защищенности 1 А?

А.12

Б.8

В .10

Г .15

30. На каких системах более динамично распространяются вирусы?

AL.inux

E.MacOS

B. Android

r.W indows

3.2.3.Контрольно-оценочные средства по ПМ.01 Настройка сетевой инфраструктуры, для проведения экзамена квалификационного

В состав комплекта входит задание для экзаменующихся, пакет экзаменатора.

Задания для экзаменующегося

Коды проверяемых профессиональных и общих компетенций:

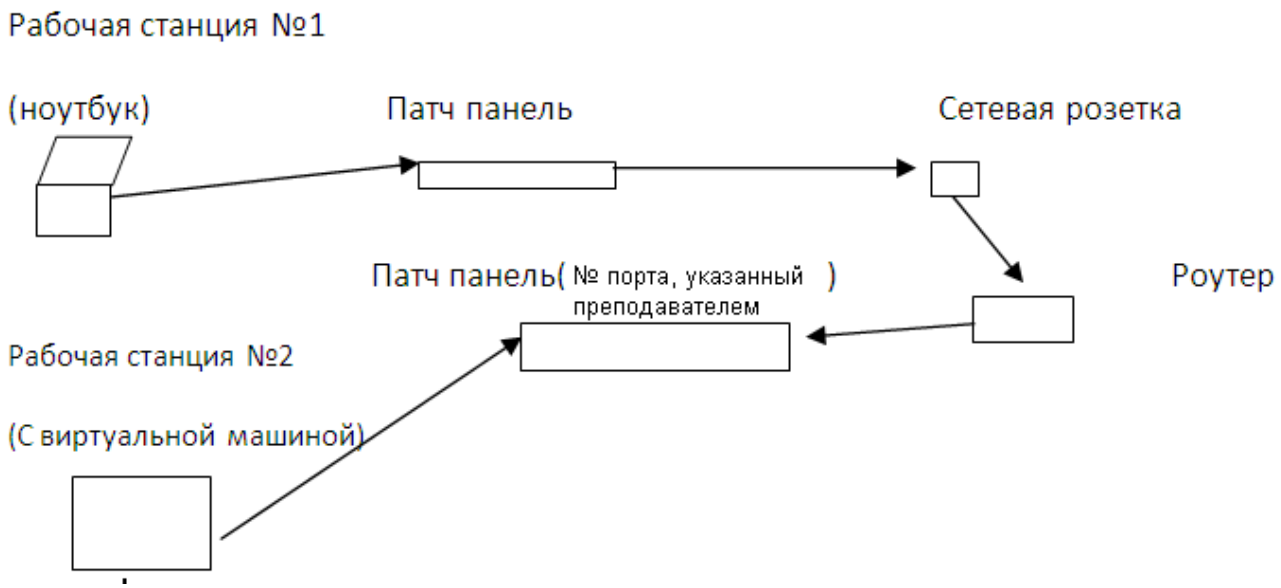
ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4. ПК 1.5. ОК 1. ОК 2. ОК 3. ОК 4. ОК 5. ОК 6. ОК 7. ОК 8. ОК 9.

Экзаменационный материал:

Экзаменационный билет №1

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

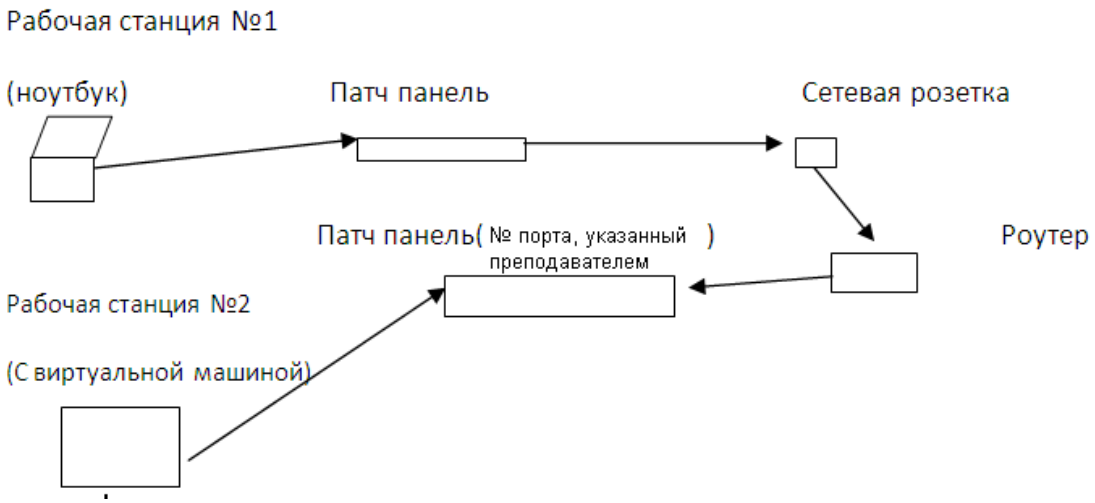
Схема. Подключение временного ПК.



Экзаменационный билет №2

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

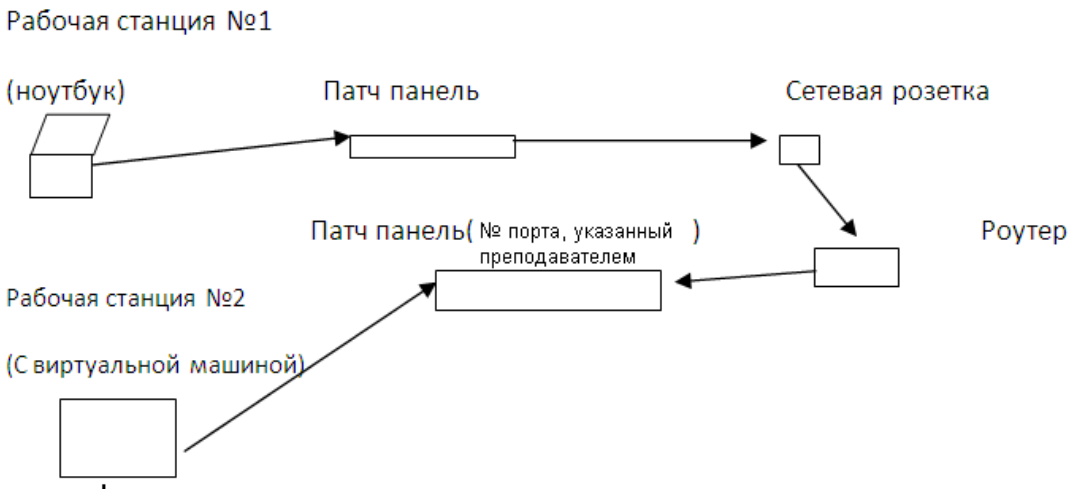
Схема. Подключение временного ПК.



Экзаменационный билет №3

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

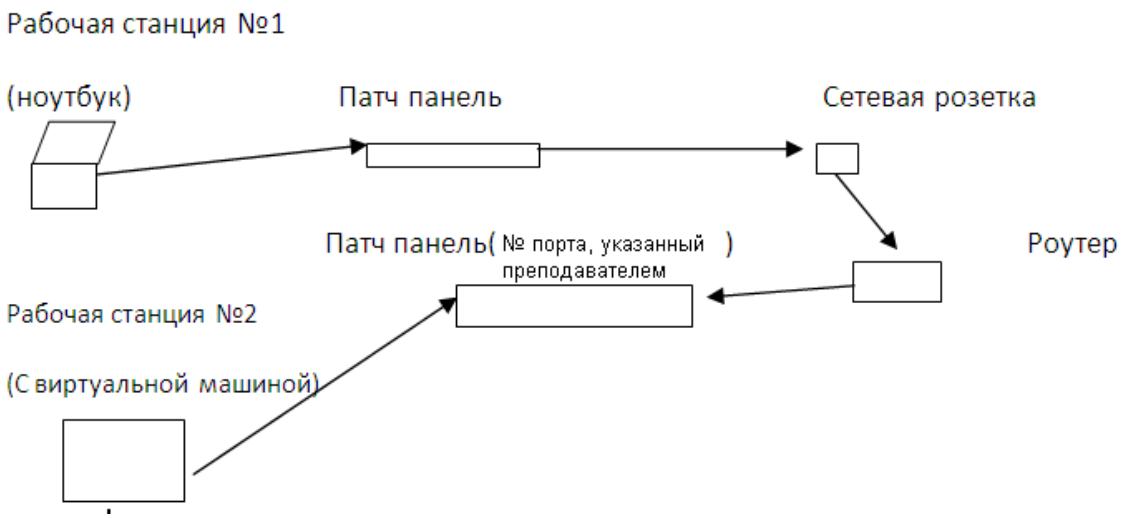
Схема. Подключение временного ПК.



Экзаменационный билет №4

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

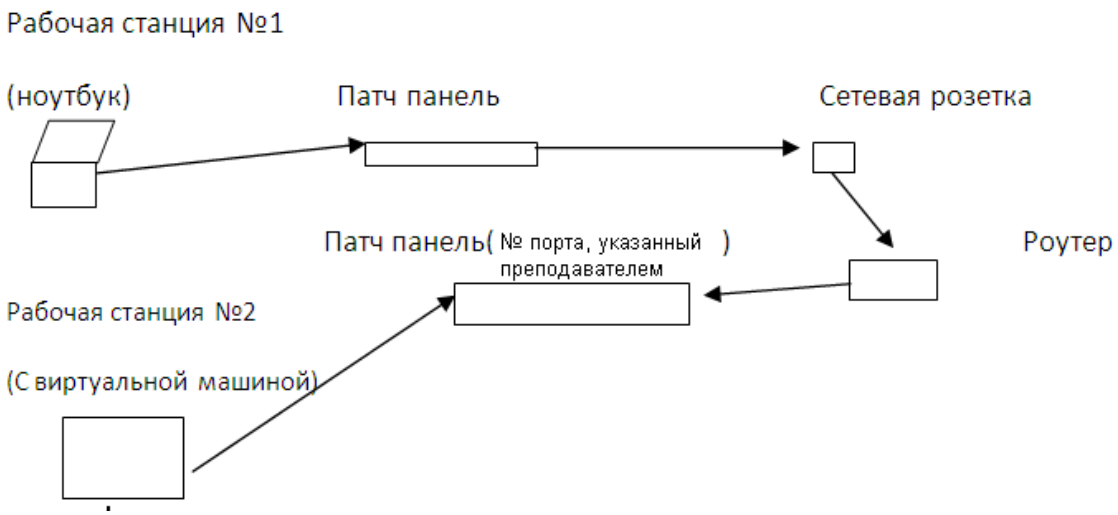
Схема. Подключение временного ПК.



Экзаменационный билет №5

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

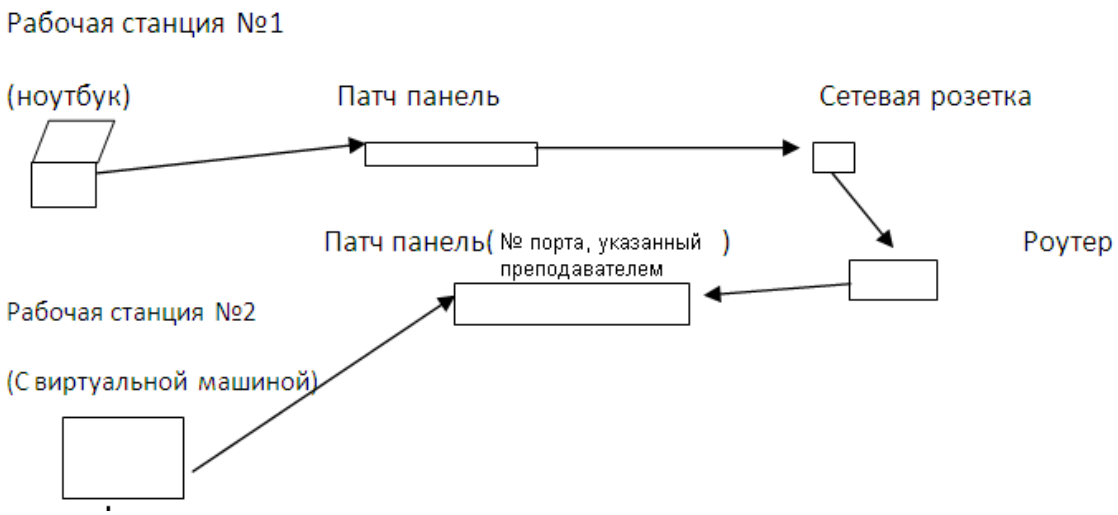
Схема. Подключение временного ПК.



Экзаменационный билет №6

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

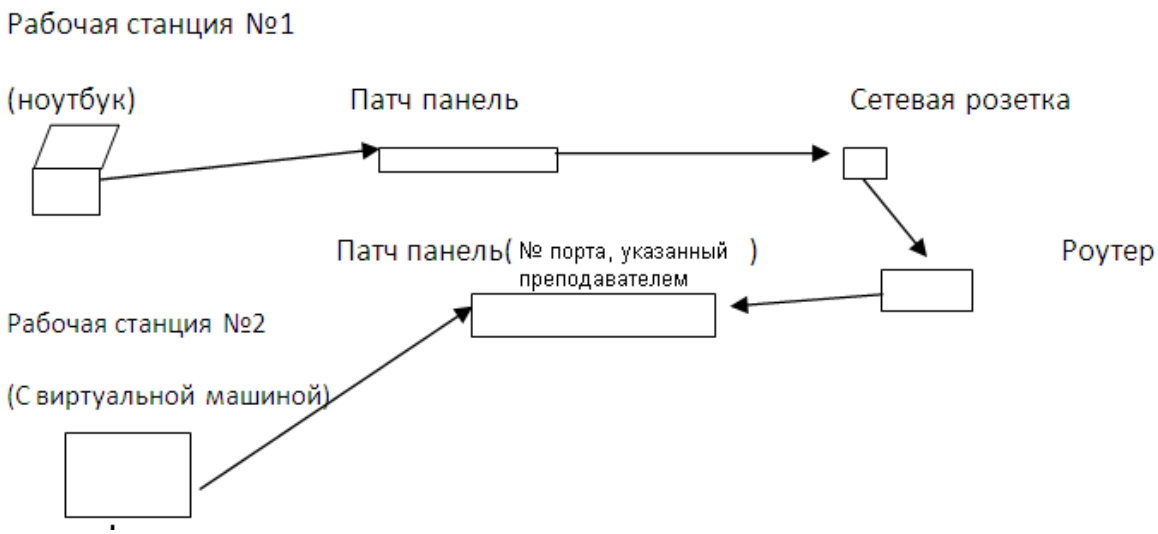
Схема. Подключение временного ПК.



Экзаменационный билет №7

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

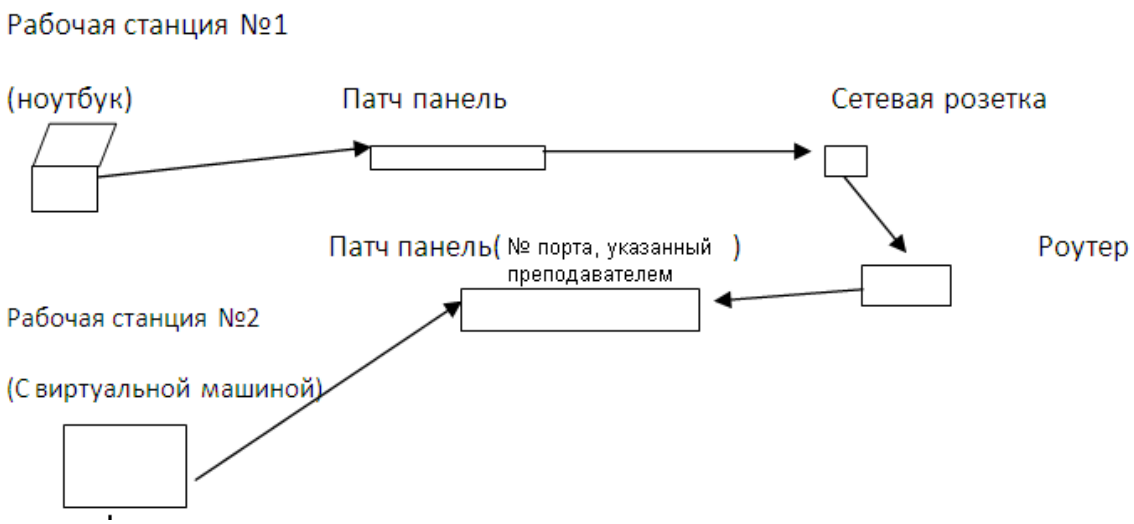
Схема. Подключение временного ПК.



Экзаменационный билет №8

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

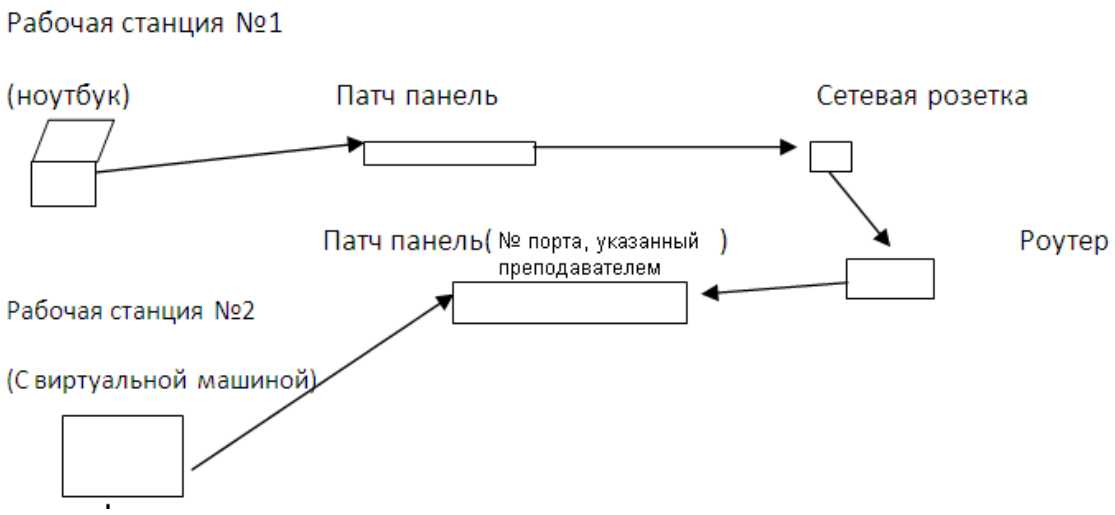
Схема. Подключение временного ПК.



Экзаменационный билет №9

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

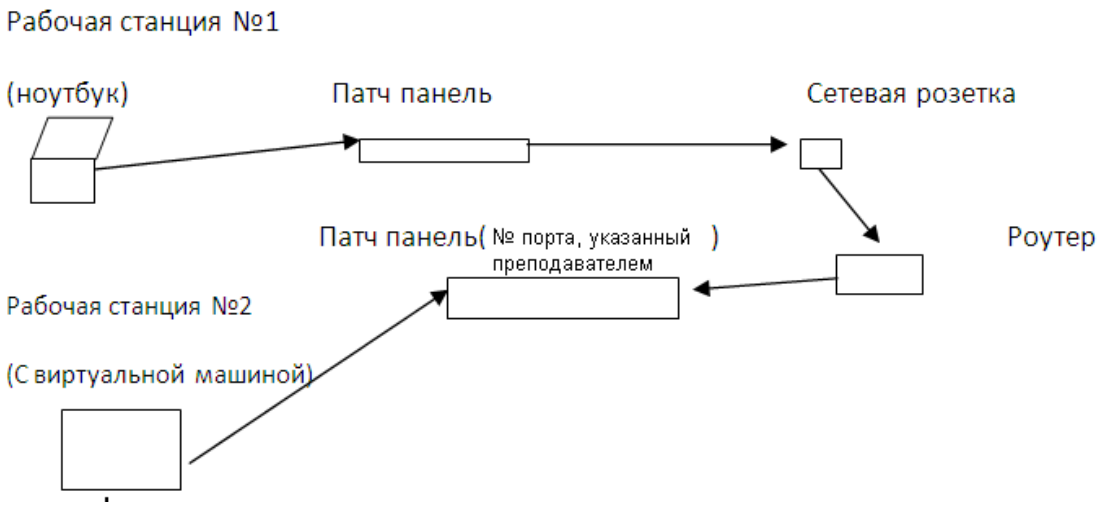
Схема. Подключение временного ПК.



Экзаменационный билет №10

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

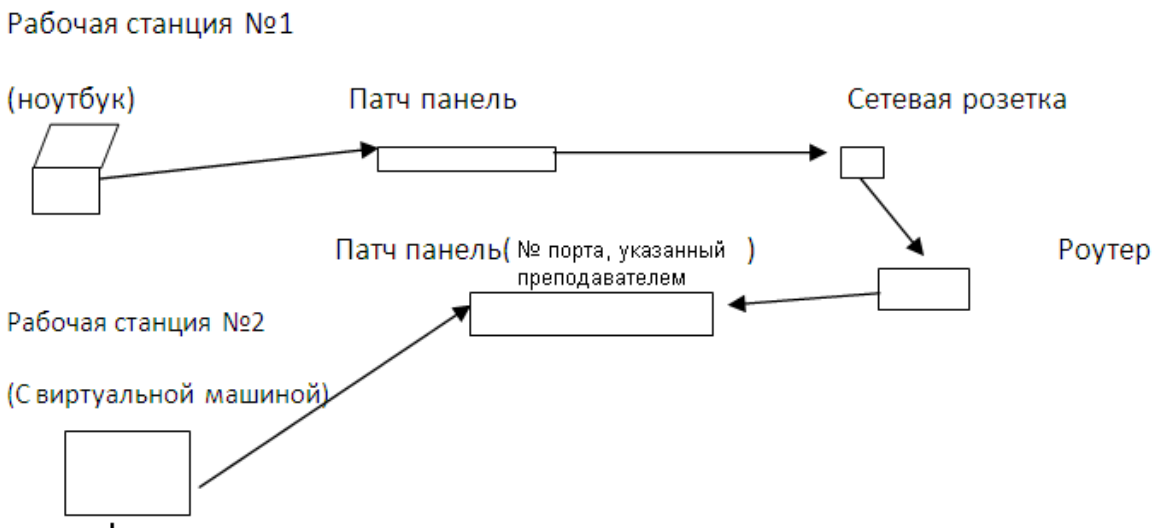
Схема. Подключение временного ПК.



Экзаменационный билет №11

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

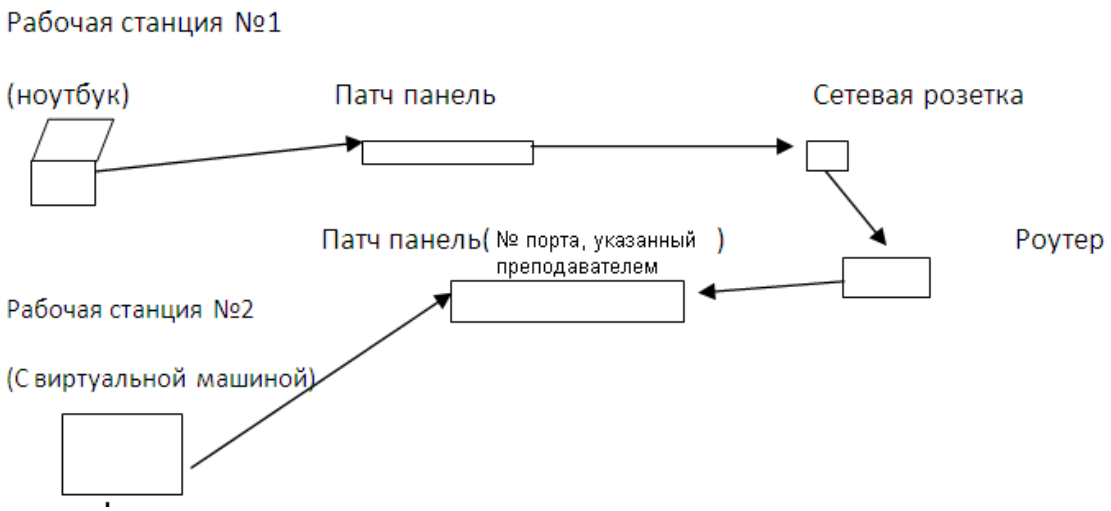
Схема. Подключение временного ПК.



Экзаменационный билет №12

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

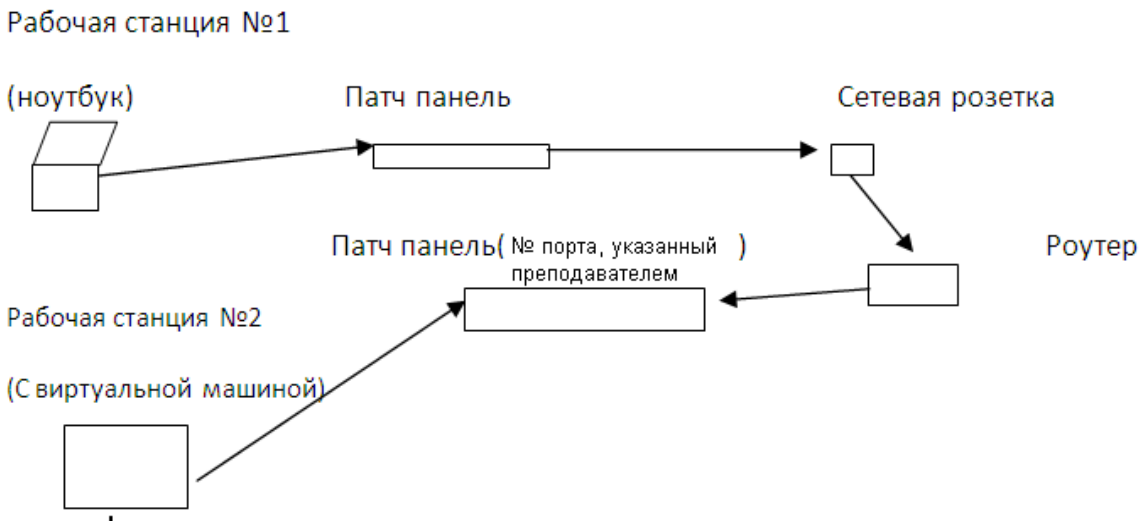
Схема. Подключение временного ПК.



Экзаменационный билет №13

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

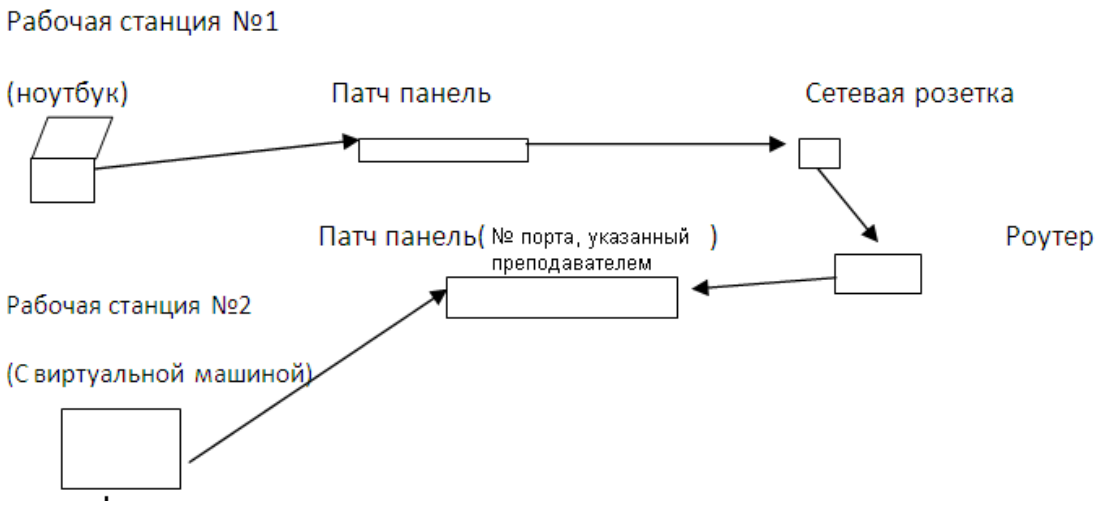
Схема. Подключение временного ПК.



Экзаменационный билет №14

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

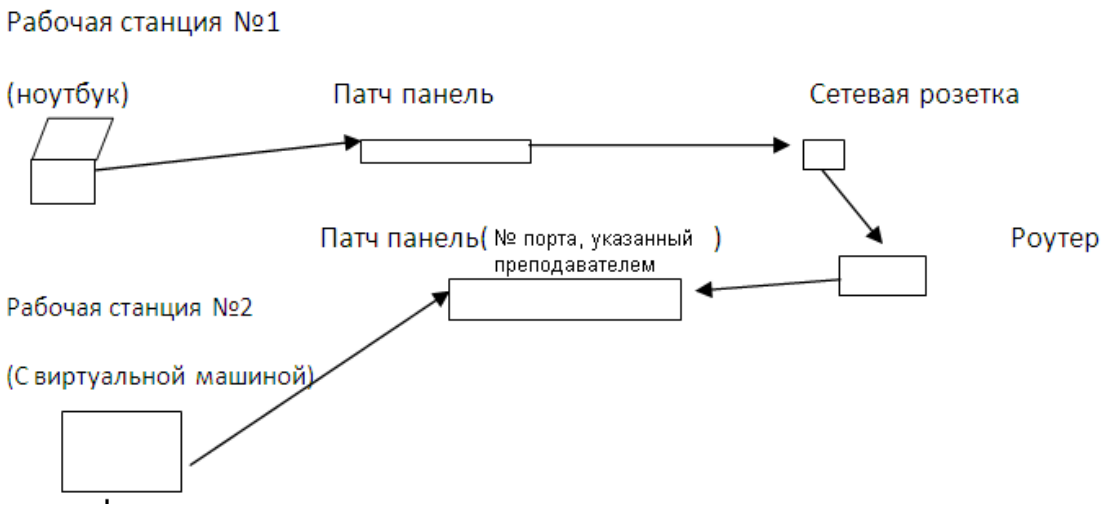
Схема. Подключение временного ПК.



Экзаменационный билет №15

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

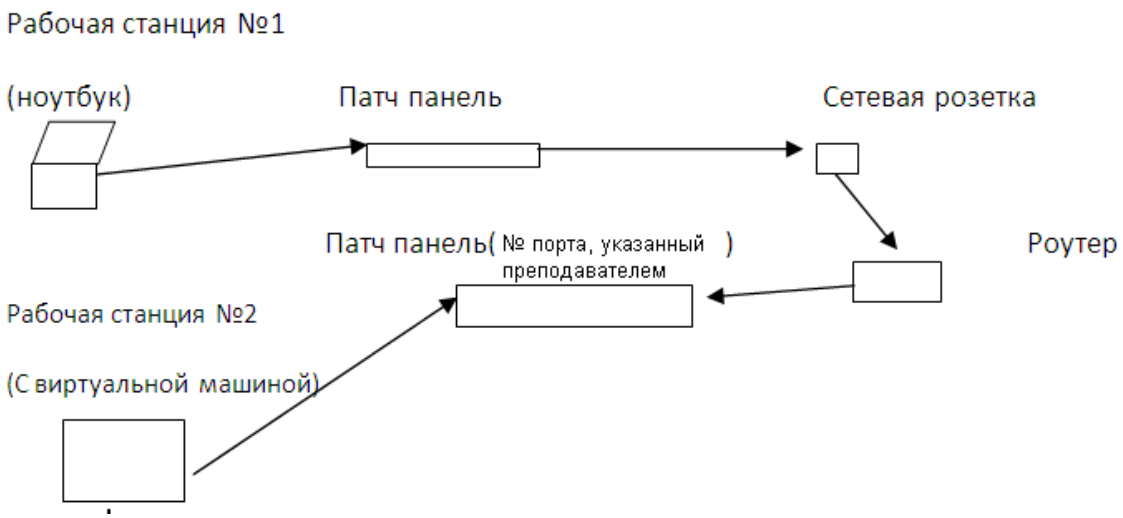
Схема. Подключение временного ПК.



Экзаменационный билет №16

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

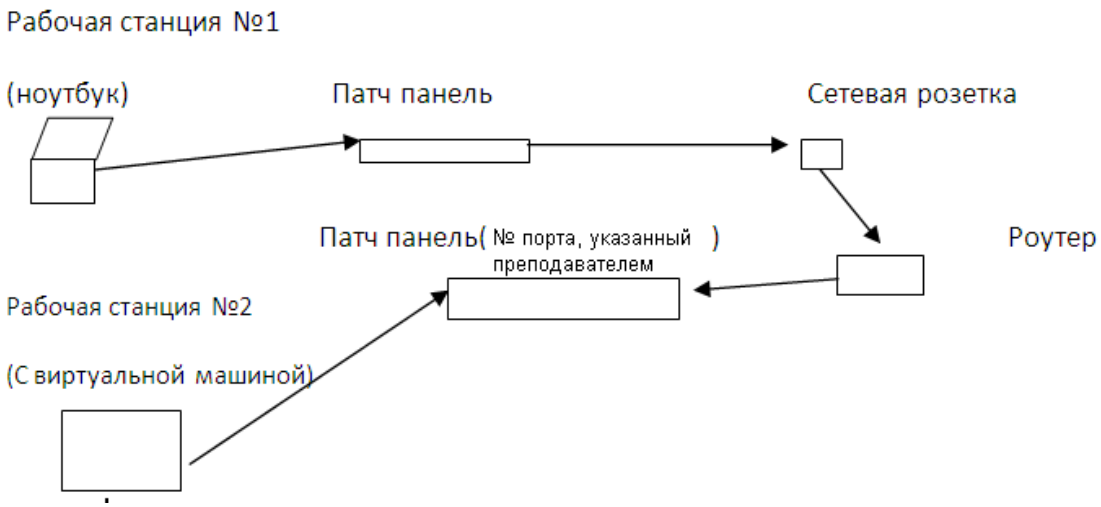
Схема. Подключение временного ПК.



Экзаменационный билет №17

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

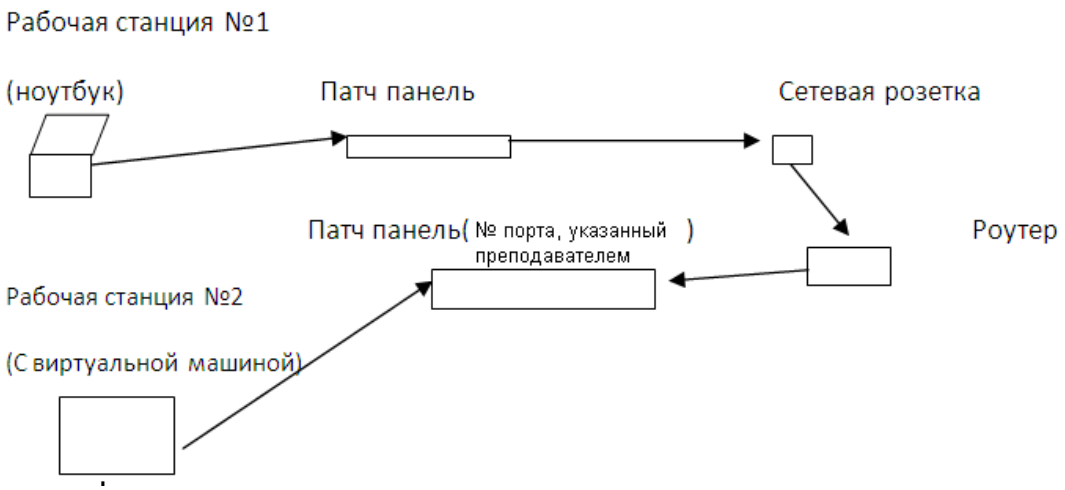
Схема. Подключение временного ПК.



Экзаменационный билет №18

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

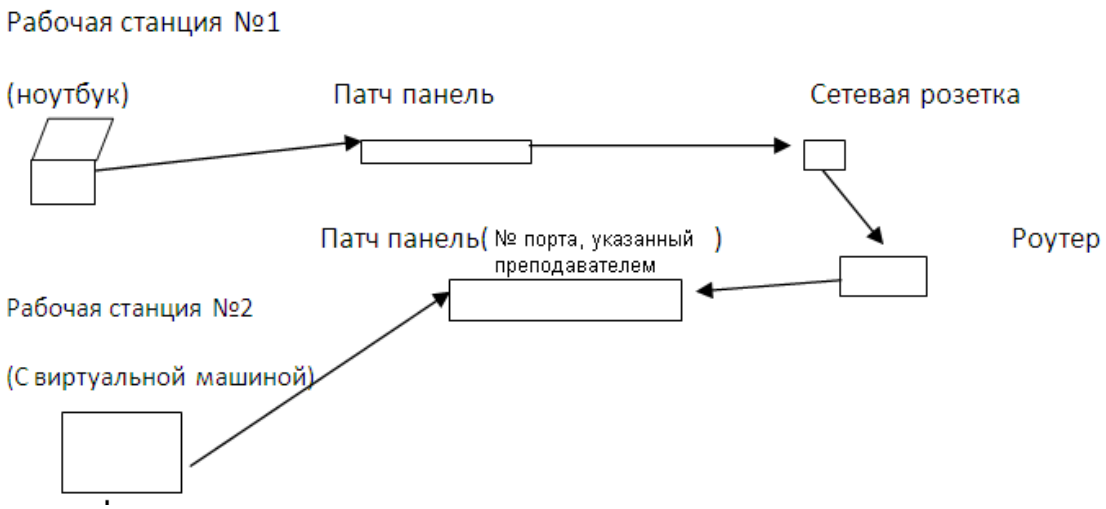
Схема. Подключение временного ПК.



Экзаменационный билет №19

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

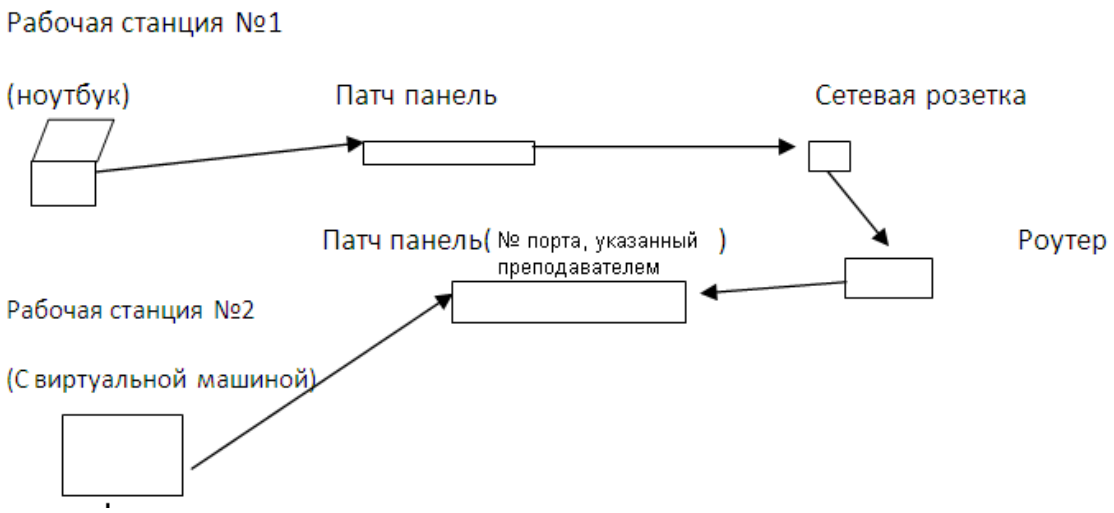
Схема. Подключение временного ПК.



Экзаменационный билет №20

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

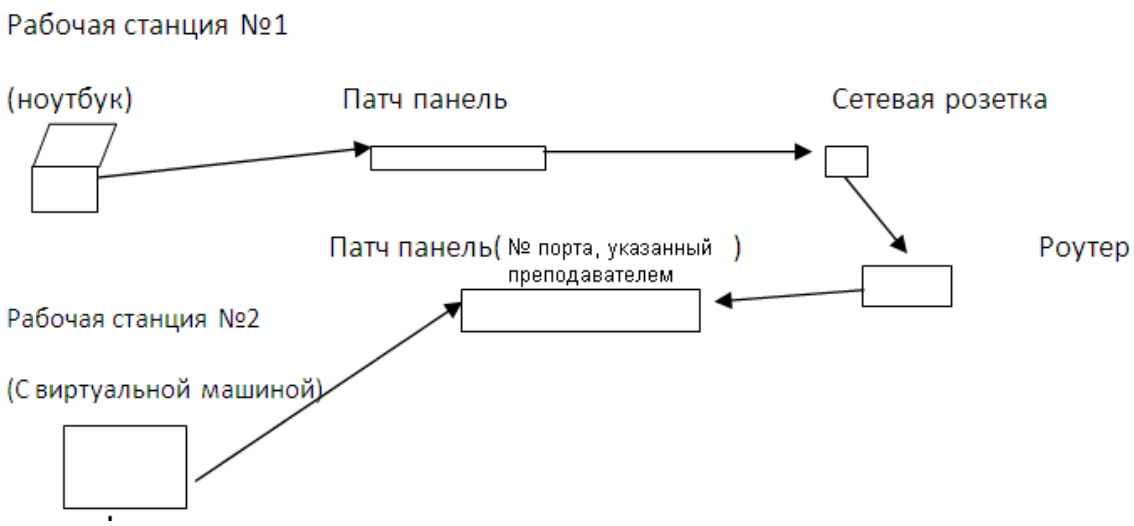
Схема. Подключение временного ПК.



Экзаменационный билет №21

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

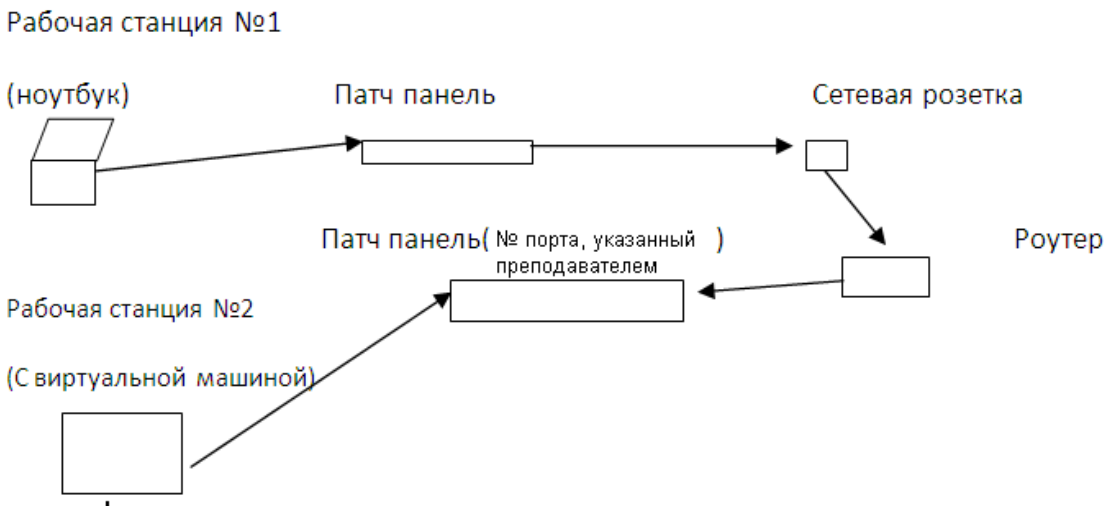
Схема. Подключение временного ПК.



Экзаменационный билет №22

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

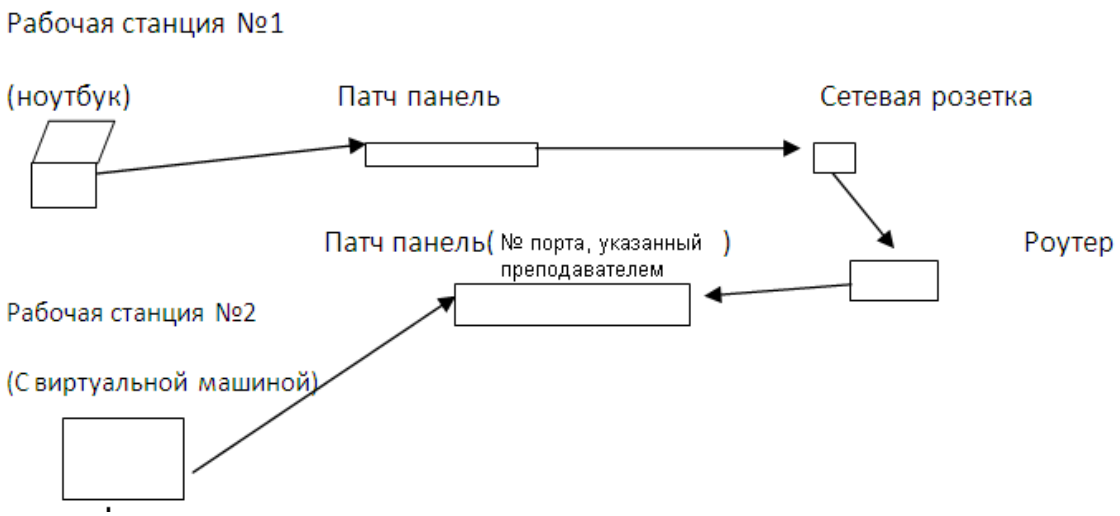
Схема. Подключение временного ПК.



Экзаменационный билет №23

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

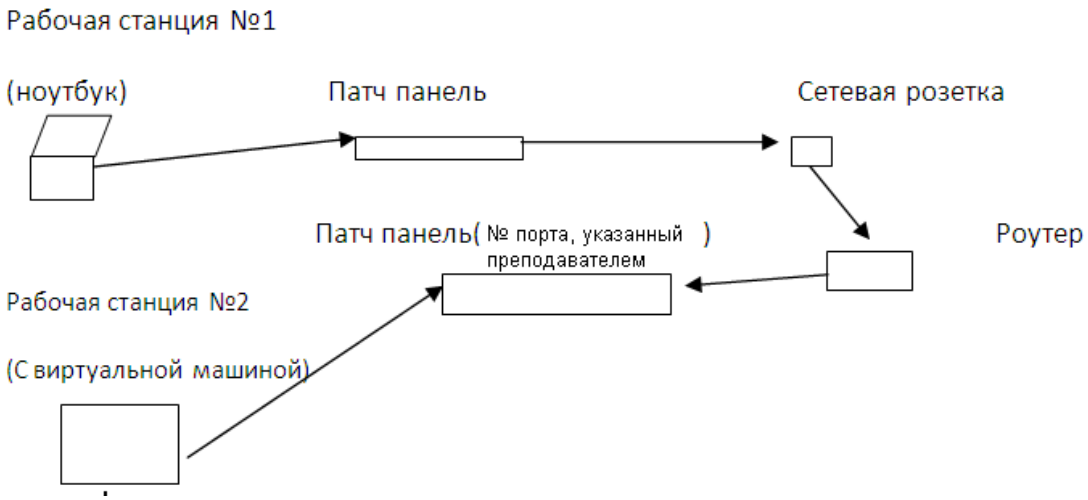
Схема. Подключение временного ПК.



Экзаменационный билет №24

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

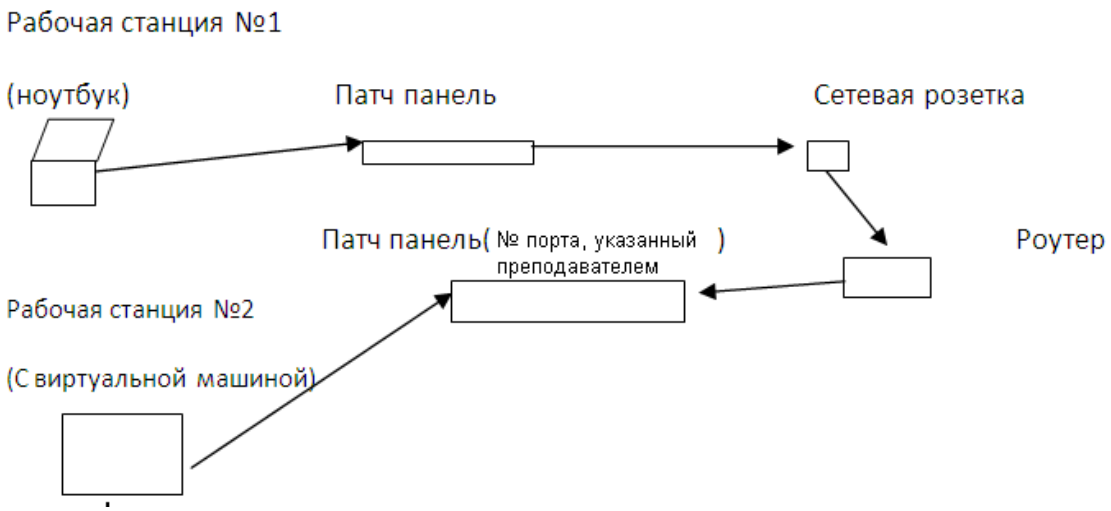
Схема. Подключение временного ПК.



Экзаменационный билет №25

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

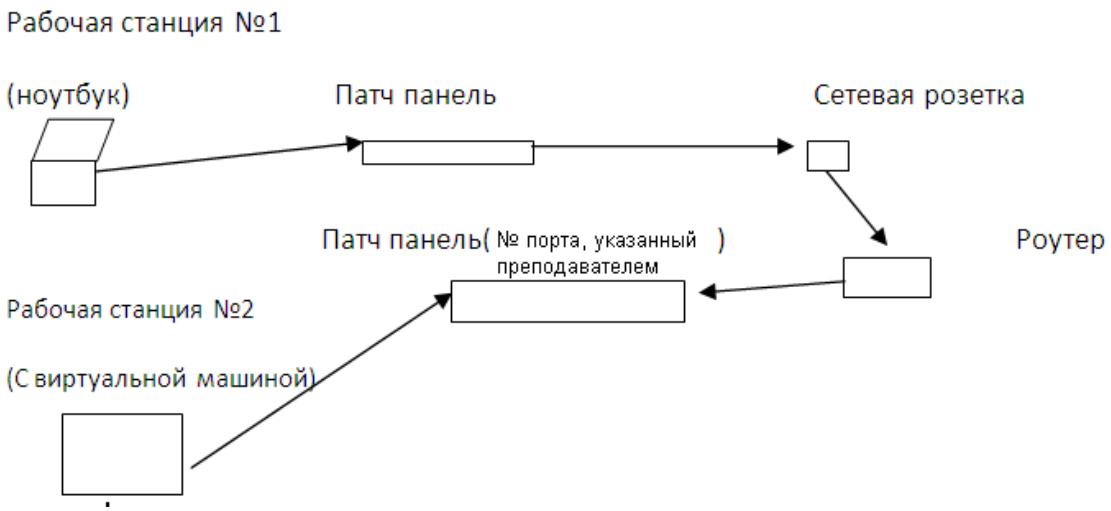
Схема. Подключение временного ПК.



Экзаменационный билет №26

Вы системный администратор небольшой компании, у вас есть ЛВС одну из машин которой(№1) необходимо объединить с временной дополнительной рабочей станцией не нарушая общей схемы существующей ЛВС, обеспечив при этом Антивирусную безопасность и безопасность пользователей данной ЛВС. Для этого согласно приложенной схеме, объедените в сегмент ЛВС, одну из рабочих станций(виртуальная машина) защитите антвирусом 360 Total Security(опишите основные компоненты),на основе второй рассмотрите возможности антивируса Kaspersky Workstation и используя имеющиеся возможности запретите доступ к сайту www.wikipedia.ru.

Схема. Подключение временного ПК.



4.ХАРАКТЕРИСТИКА И КРИТЕРИИ ОЦЕНОК ФОРМ И ВИДОВ КОНТРОЛЯ

4.1.Контроль успеваемости

Текущий контроль - это непрерывно осуществляемый в ходе аудиторных и самостоятельных занятий по учебному курсу контроль уровня знаний, умений, и практического опыта деятельности обучающегося в течение семестра.

- Текущий контроль знаний проводится для всех обучающихся лицея, обучающихся по основным профессиональным образовательным программам.

- Текущий контроль проводится в пределах учебного времени, отведенного на соответствующий ОП (раздел ОП) или практику.

Текущий контроль освоения обучающимися программного материала ОП может иметь следующие виды: входной, оперативный и рубежный контроль.

Входной контроль проводится с целью выявления степени реальной готовности обучающихся к освоению учебного материала ОП.

Форму проведения входного контроля выбирает преподаватель, он же готовит контролирующие материалы на основе типовых заданий для входного контроля. Результаты входного контроля могут явиться основой для корректировки рабочих программ профессиональных модулей, а также для выстраивания индивидуальной траектории обучения с каждым обучающимся или учебной группой.

Оперативный контроль проводится с целью объективной оценки качества освоения программ профессиональных модулей, а также стимулирования учебной работы обучающихся, мониторинга результатов образовательной деятельности, подготовки обучающихся к промежуточной аттестации и обеспечения максимальной эффективности учебного процесса.

Рубежный контроль - это форма текущего контроля, направленная на проверку освоения тематически завершенной части рабочей программы модуля или промежуточные срезы знаний. Формируется на основе типовых заданий для оценки освоения ОП.

В течение семестра по ОП (разделу ОП) проводится не менее 1 рубежного контроля.

В качестве форм рубежного контроля ОП (раздела ОП) или практики можно использовать:

- тестирование (в том числе компьютерное);
- прием отчетной документации по практике;
- проверка индивидуальных домашних заданий, самостоятельных работ

4.2.Практические занятия

Правила выполнения лабораторно-практических заданий.

Подготовка к лабораторно-практическим работам заключается в самостоятельном изучении теории по рекомендуемой литературе, предусмотренной рабочей программой. Выполнение заданий производится индивидуально в часы, предусмотренные расписанием занятий в соответствии с методическими указаниями к лабораторно-практическим работам. Отчет по практической работе каждый студент выполняет индивидуально с учетом рекомендаций по оформлению.

Отчет выполняется в рабочей тетради, сдается преподавателю по окончанию занятия или в начале следующего занятия. Отчет должен включать пункты:

- название лабораторной или практической работы
- цель работы
- оснащение
- задание
- порядок работы
- решение, развернутый ответ, таблица, ответы на контрольные вопросы (в зависимости от задания)
- вывод по работе.

Лабораторная или практическая работа считается выполненной, если она соответствует критериям, указанным в лабораторно-практической работе. Если студент имеет пропуски лабораторно-практических занятий по уважительной или неуважительной причине, то выполняет работу во время консультаций, отведенных группе по данной дисциплине.

Практические занятия.

Практические занятия как виды учебных занятий направлены на экспериментальное подтверждение теоретических положений и формирование общих и профессиональных компетенций, учебных и профессиональных практических умений и составляют важную часть теоретической и профессиональной практической подготовки.

Выполнение обучающимися практических занятий проводится с целью:

- формирования практических умений в соответствии с требованиями к уровню подготовки, установленными рабочей программой профессионального модуля по конкретным разделам и темам междисциплинарных курсов;
- обобщения, систематизации, углубления, закрепления полученных теоретических знаний;
- совершенствования умений применять полученные знания на практике, реализации единства интеллектуальной и практической деятельности;
- развития интеллектуальных умений у будущих специалистов: аналитических, проектировочных, конструкторских и др.;
- выработки таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива при решении поставленных задач при освоении общих компетенций.

Практические занятия могут носить репродуктивный, частично-поисковый и поисковый характер.

Работы, носящие *репродуктивный характер,* отличаются тем, что при их проведении обучающиеся пользуются подробными инструкциями, в которых указаны: цель работы, пояснения (теория, основные характеристики),

оборудование, аппаратура, материалы и их характеристики, порядок выполнения работы, таблицы, выводы (без формулировки), контрольные вопросы, учебная и специальная литература.

Работы, носящие *частично-поисковый характер*, отличаются тем, что при их проведении обучающиеся не пользуются подробными инструкциями, им не дан порядок выполнения необходимых действий, и они требуют от обучающихся самостоятельного подбора оборудования, выбора способов выполнения работы в инструктивной и справочной литературе и др.

Работы, носящие *поисковый характер*, характеризуются тем, что обучающиеся, опираясь на имеющиеся у них теоретические знания, должны решить новую для них проблему.

Оценка «5» ставится в том случае, если обучающийся:

а) выполнил задание в полном объеме с соблюдением необходимой последовательности действий, расчетов и измерений;

б) самостоятельно и рационально выбрал и подготовил для выполнения задания все необходимое оборудование, все расчеты, измерения и построения провел в условиях, обеспечивающих получение результатов и выводов с наибольшей точностью;

в) в представленном отчете правильно и аккуратно выполнил все записи, таблицы, рисунки, чертежи, графики, вычисления и сделал выводы;

г) соблюдал требования охраны труда.

Оценка «4» ставится в том случае, если выполнены требования к оценке 5, но:

а) расчеты, измерения и построения проводились в условиях, не обеспечивающих достаточной точности;

б) было допущено два-три недочета, или не более одной негрубой ошибки и одного недочета.

Оценка «3» ставится, если задание выполнено не полностью, но объем выполненной части таков, что можно сделать выводы, или если в ходе выполнения задания были допущены следующие ошибки:

а) действия проводились в нерациональных условиях, что привело к получению результатов с большой погрешностью;

б) в отчете были допущены в общей сложности не более двух ошибок (в записях единиц, измерениях, в вычислениях, графиках, таблицах, схемах, анализе алгоритма работы и т.д.), не принципиальных для данного вида работы, не повлиявших на результат выполнения;

в) задание выполнено не полностью, однако объем выполненной части таков, что позволяет получить правильные результаты и сделать выводы по основным, принципиально важным задачам занятия.

Оценка «2» ставится в том случае, если:

а) задание выполнено не полностью, и объем выполненной части не позволяет сделать правильные выводы;

б) расчеты, измерения, вычисления, наблюдения или другие действия производились неправильно;

в) в ходе работы и в отчете обнаружились в совокупности все недостатки, отмеченные в требованиях к оценке «3».

В тех случаях, когда обучающийся показал оригинальный и/или наиболее рациональный подход к выполнению задания и в процессе выполнения здания, но не избежал тех или иных недостатков, оценка за выполнение работы по усмотрению преподавателя может быть повышена по сравнению с указанными выше критериями.

Тестирование.

Критерии оценки результатов тестирования могут быть различными. На практике чаще всего применяют два критерия:

- соотношение между количеством правильных ответов на вопросы с общим числом вопросов теста
- время, затраченное для ответа на вопросы.

Первый критерий является основным, поэтому при оценке ответов учитываются либо только он один (чаще всего) либо оба одновременно.

Первый критерий - выбор преподавателем верного соотношения между числом правильных ответов на вопросы с общим числом вопросов теста для определения оценки зависит от важности проверяемого материала и актуальности поставленных вопросов.

При этом контроль должен быть объективным и отвечать тем целям, которые перед ним поставлены.

Чаще всего число вопросов в блоках применяется 10, 5 или, в тесте может быть и другое число вопросов. Если проверяют знания по обычному материалу, т. е. не требующему высокой ответственности принимаемых решении, когда неточности в его знании не влекут за собой особо тяжелых последствий, то на практике часто принимают такие значения первого критерия:

При числе вопросов в тесте равном 10 оценки будут следующие:

Отлично - при 9-10 правильных ответах,

Хорошо - при 7- 8 правильных ответах,

Удовлетворительно - при 5- 6 правильных ответах,

Неудовлетворительно - при правильных ответов менее 5.

Из изложенного видно, что каждой оценки соответствует определенный числовой диапазон правильных ответов, который в свою очередь, зависит от числа вопросов в тесте.

При большом количестве вопросов в тесте, целесообразно числовой диапазон правильных ответов заменять на процент правильных ответов, тогда оценка может соответствовать, например,

Отлично - при 90% правильных ответах,

Хорошо - при 70% правильных ответах,

Удовлетворительно - при 50% правильных ответах,

Неудовлетворительно - при правильных ответов менее 50%.

При решении вопроса о том, каким выбрать первый критерий знаний, целесообразно учитывать возможную неравнозначность вопросов в тестах. В тесте один или несколько вопросов могут быть основными, т. е. более

сложными для ответа, или включающими наиболее важный материал, а остальные вопросы - дополнительными.

В этом случае удельный "вес" основных вопросов будет выше, чем дополнительных, и может в большей степени влиять на принятие преподавателем решения о выставлении оценки.

Второй критерий - время, затраченное для ответов на вопросы, применяется в тех случаях, когда требуется оценивать не только правильность ответа на вопросы, но и время, необходимое для того чтобы ответить.

Чаще всего этот критерий применяется, когда основными вопросами тестов являются вопросы с результативным методом ввода ответов и когда для ответов предусмотрено решение задач в ограниченное время.

Ответы проверяемых, которые не успели ответить, оцениваются как неудовлетворительные, либо оценка по первому критерию соответствующим образом снижается.

Числовые значения и первого и второго критериев, разработанные преподавателем для различных разделов (тем) данной дисциплины, должны быть согласованы между собой. Необходимо также провести согласование числовых значений критериев, применяемых разными преподавателями.

В рамках компетентностного подхода ФГОС используется модель оценки результатов обучения, об уровнях усвоения знаний и постепенном восхождении обучающихся по образовательным траекториям.

Выделены следующие *уровни* результатов обучения обучающихся.

Первый уровень. Результаты обучения свидетельствуют об усвоении ими некоторых элементарных знаний основных вопросов по дисциплине. Допущенные ошибки и неточности показывают, что обучающиеся не овладели необходимой системой знаний по дисциплине.

Второй уровень. Достигнутый уровень оценки результатов обучения показывает, что обучающиеся обладают необходимой системой знаний и владеют некоторыми умениями по дисциплине. Обучающиеся способны понимать и интерпретировать освоенную информацию, что является основой

успешного формирования умений и навыков для решения практико-ориентированных задач.

Третий уровень. Обучающиеся продемонстрировали результаты на уровне осознанного владения учебным материалом и учебными умениями, навыками и способами деятельности по дисциплине. Обучающиеся способны анализировать, проводить сравнение и обоснование выбора методов решения заданий в практико-ориентированных ситуациях.

Четвертый уровень. Обучающиеся способны использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных практико-ориентированных ситуациях. Достигнутый уровень оценки результатов обучения по дисциплине является основой для формирования общекультурных и профессиональных компетенций, соответствующих требованиям ФГОС.

В тестах данная модель реализована в трех взаимосвязанных блоках заданий.

Первый блок – задания на уровне «знать», в которых очевиден способ решения, усвоенный обучающимся при изучении дисциплины. Задания этого блока оцениваются по шкале «правильно-неправильно».

Второй блок – задания на уровне «знать» и «уметь», в которых нет явного указания на способ выполнения, и обучающийся для их решения самостоятельно выбирает один из изученных способов. Задания данного блока оцениваются с учетом частично правильно выполненных заданий.

Третий блок – задания на уровне «знать», «уметь», «владеть». Он представлен case-заданиями, содержание которых предполагает использование комплекса умений и навыков, для того чтобы обучающийся мог самостоятельно сконструировать способ решения, комбинируя известные ему способы и привлекая знания из разных дисциплин. Задания данного блока также оцениваются с учетом частично правильно выполненных заданий.

Промежуточная аттестация.

Промежуточная аттестация обеспечивает оперативное управление учебной деятельностью обучающегося и ее корректировку и проводится с целью определения:

- соответствия уровня и качества подготовки специалиста Федеральным государственным образовательным стандартам СПО в части государственных требований;
- полноты и прочности теоретических знаний по ОП в целом;
- сформированности умений применять полученные теоретические знания при решении практических задач;
- сформированности у студентов общих и профессиональных компетенций, соответствующих видам профессиональной деятельности:
- сформированности умений самостоятельно работать с учебной и справочной литературой.

4.3. Дифференцированный зачет/экзамен

Дифференцированный зачет как форма промежуточной аттестации проводится за счет объема времени, отводимого на изучение ОП. Задания для дифференцированного зачета включают задания, вопросы по учебному материалу, направленному на освоение компетенций и вида деятельности согласно требованиям федерального государственного образовательного стандарта.

При проведении дифференцированного зачета уровень подготовки обучающегося оценивается в баллах: «5» (отлично), «4» (хорошо), «3» (удовлетворительно), «2» (неудовлетворительно). Неудовлетворительная оценка «2» в зачетную книжку не ставится.

Критерии оценки ответов обучающихся при проведении дифференцированных зачетов

Оценка «5» - изложение полученных знаний в устной, письменной или графической форме полное, в соответствии с требованиями учебной программы; выделение существенных признаков изученного с помощью операций анализа и синтеза; выявление существенных признаков причинно

следственных связей, формулировка выводов и обобщений; самостоятельное применение знаний в практической деятельности, выполнение заданий как воспроизводящего, так и творческого характера;

Оценка «4» - изложение полученных знаний в устной, письменной или графической форме полное, в соответствии с требованиями учебной программы; допускаются отдельные незначительные ошибки; при выделении существенных признаков изученного также допускаются отдельные незначительные ошибки; в практической, самостоятельной деятельности возможна небольшая помощь преподавателя;

Оценка «3» - изложение полученных знаний неполное, однако это не препятствует освоению последующего программного материала; допускаются отдельные существенные ошибки, исправляемые с помощью преподавателя; имеются затруднения при выделении существенных признаков изученного и формулировке выводов. Недостаточная самостоятельность в практической деятельности и выполнении заданий воспроизводящего характера;

Оценка «2» - изложение учебного материала неполное, бессистемное; имеются существенные ошибки, которые учащийся не в состоянии исправить даже с помощью преподавателя; неумение производить простейшие операции синтеза и анализа, делать обобщения и выводы.

Зачет проводится в устной форме по билетам: студент должен выполнить два задания (на подготовку ответа на каждое из них отводится 15 минут).

На зачете не разрешается пользоваться литературой, нормативно-правовыми актами, конспектами и иными вспомогательными средствами. В случае использования студентов подобной литературы преподаватель оставляет за собой право удалить студента с зачета, выставив ему неудовлетворительную оценку.

Оценивание ответа на зачете осуществляется следующим образом:

Оценка **зачтено** выставляется, если ответ логически и лексически грамотно изложенный, содержательный и аргументированный ответ, подкрепленный знанием литературы и источников по теме задания, умение отвечать на

дополнительно заданные вопросы; незначительное нарушение логики изложения материала, периодическое использование разговорной лексики, допущение не более одной ошибки в содержании задания, а также не более одной неточности при аргументации своей позиции, неполные или неточные ответы на дополнительно заданные вопросы; незначительное нарушение логики изложения материала, периодическое использование разговорной лексики при допущении не более двух ошибок в содержании задания, а также не более двух неточностей при аргументации своей позиции, неполные или неточные ответы на дополнительно заданные вопросы.

Оценка **не зачтено** выставляется, если в ответе допущено существенное нарушение логики изложения материала, систематическое использование разговорной лексики, допущение не более двух ошибок в содержании задания, а также не более двух неточностей при аргументации своей позиции, неправильные ответы на дополнительно заданные вопросы; существенное нарушение логики изложения материала, постоянное использование разговорной лексики, допущение не более трех ошибок в содержании задания, а также не более трех неточностей при аргументации своей позиции, неправильные ответы на дополнительно заданные вопросы; полное отсутствие логики изложения материала, постоянное использование разговорной лексики, допущение более трех ошибок в содержании задания, а также более трех неточностей при аргументации своей позиции, полное незнание литературы и источников по теме вопроса, отсутствие ответов на дополнительно заданные вопросы.

Оценка зачтено может выставляться по результатам текущего контроля, осуществляемого в ходе семинарских/практических занятий на основе оценки активности работы студентов, их участия в дискуссиях и выступлений с докладами, а также по результатам оценки посещаемости студентами лекций и семинаров.

Примерные критерии оценки: оценки «отлично» заслуживает студент, обнаруживший всестороннее, систематическое и глубокое знание учебно-

программного материала, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка «отлично» выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала;

оценки «хорошо» заслуживает студент, обнаруживший полные знания учебно-программного материала, успешно выполняющий предусмотренные в программе задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка «хорошо» выставляется студентам, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности;

оценки «удовлетворительно» заслуживает студент, обнаруживший знание учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющийся с выполнением заданий, предусмотренных программой, знакомый с основной литературой, рекомендованной программой. Как правило, оценка «удовлетворительно» выставляется студентам, допустившим погрешность в ответе на экзамене и при выполнении экзаменационных заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя;

оценка «неудовлетворительно» выставляется студенту, обнаружившему пробелы в знаниях основного учебно-программного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине».

Преподавателем может быть разработана самостоятельная методика формирования результирующей оценки.

Критерии оценок знаний студентов на экзаменах

Отметка «отлично» ставится, если:

знания отличаются глубиной и содержательностью, дается полный исчерпывающий ответ, как на основные вопросы билета, так и на дополнительные:

- студент свободно владеет научными понятиями;
- студент способен к интеграции знаний по определенной теме, структурированию ответа, к анализу положений существующих теорий, научных школ, направлений по вопросу билета;
- логично и доказательно раскрывает проблему, предложенную в билете;
- ответ не содержит фактических ошибок и характеризуется глубиной, полнотой, уверенностью студента;
- ответ иллюстрируется примерами, в том числе из собственной практики;
- студент демонстрирует умение вести диалог и вступать в научную дискуссию.

Отметка «хорошо» ставится, если:

знания имеют достаточный содержательный уровень, однако отличаются слабой структурированностью; раскрыто содержание билета, имеются неточности при ответе на дополнительные вопросы:

- в ответе имеют место несущественные фактические ошибки, которые студент способен исправить самостоятельно, благодаря наводящему вопросу;
- недостаточно раскрыта проблема по одному из вопросов билета;
- недостаточно логично построено изложение вопроса;
- ответ прозвучал недостаточно уверенно;
- студент не смог показать способность к интеграции и адаптации знаний или теории и практики.

Отметка «удовлетворительно» ставится, если:

знания имеют фрагментарный характер, отличаются поверхностностью и малой содержательностью содержание билета раскрыто слабо, имеются неточности при ответе на основные вопросы билета:

- программные материал в основном излагается, но допущены фактические ошибки;
- ответ носит репродуктивный характер;
- студент не может обосновать закономерности и принципы, объяснить факты;
- нарушена логика изложения, отсутствует осмысленность представляемого материала;
- у студента отсутствуют представления о межпредметных связях.
- Отметка «неудовлетворительно» ставится, если:
- обнаружено незнание или непонимание студентом сущностной части социальной психологии;
- допускаются существенные фактические ошибки, которые студент не может исправить самостоятельно;

На большую часть дополнительных вопросов по содержанию экзамена студент затрудняется дать ответ или не дает верных ответов.

Литература:

Основной источник:

1. Максимов, Н. В. Компьютерные сети: учебное пособие / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2021. — 464 с.

Дополнительные источники:

1. Сергеев А.Н. Основы локальных компьютерных сетей: учебное пособие. СПО. – Москва:Лань, 2020. – 184 с.
2. Новожилов Е.О. Компьютерные сети. – М.: ОИЦ «Академия, 2021.

Информационные справочно-правовые системы:

«Консультант-Плюс», «Гарант» и другие.

Интернет – ресурсы:

1. https://urait.ru/bcode/437357
2. https://znanium.com/catalog/product/1189333

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ПРЕДДИПЛОМНОЙ ПРАКТИКЕ

СПЕЦИАЛЬНОСТЬ 09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

2024

СОДЕРЖАНИЕ

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств предназначен для контроля и оценки результатов освоения производственной преддипломной практики по специальности 09.02.06 Сетевое и системное администрирование, и соответствующих профессиональных компетенций (ПК) и общих компетенций (ОК):

ПК 1.1. Документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации

ПК 1.2. Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем.

ПК 1.3. Устранять неисправности в работе инфокоммуникационных систем.

ПК 1.4. Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности.

ПК 1.5. Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем.

ПК 1.6. Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта.

ПК 1.7. Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем.

ПК 2.1. Принимать меры по устранению сбоев в операционных системах.

ПК 2.2. Администрировать сетевые ресурсы в операционных системах.

ПК 2.3. Осуществлять сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.

ПК 2.4. Осуществлять проведение обновления программного обеспечения операционных систем и прикладного программного обеспечения.

ПК 2.5. Осуществлять выявление и устранение инцидентов в процессе функционирования операционных систем.

ПК 3.1. Осуществлять проектирование сетевой инфраструктуры.

ПК 3.2. Обслуживать сетевые конфигурации программно-аппаратных средств.

ПК 3.3. Осуществлять защиту информации в сети с использованием программно-аппаратных средств.

ПК 3.4. Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры.

ПК 3.5. Модернизировать сетевые устройства информационно-коммуникационных систем.

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде;

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и

поддержания необходимого уровня физической подготовленности;
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

При реализации производственной преддипломной практики у обучающихся должны быть сформированы:

Настройка сетевой инфраструктуры.

практический опыт:

- проектирования архитектуры локальной сети в соответствии с поставленной задачей;
- установки и настройки сетевых протоколов и сетевого оборудования в соответствии с конкретной задачей;
- выбора технологии, инструментальных средств при организации процесса исследования объектов сетевой инфраструктуры;
- обеспечения безопасного хранения и передачи информации в локальной сети;
- использования специального программного обеспечения для моделирования, проектирования и тестирования компьютерных сетей.

умения:

- проектировать локальную сеть, выбирать сетевые топологии;
- использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети.

знания:

- общие принципы построения сетей, сетевых топологий, многослойной модели OSI, требований к компьютерным сетям;
- архитектуру протоколов, стандартизации сетей, этапов проектирования сетевой инфраструктуры;
- базовые протоколы и технологии локальных сетей;
- принципы построения высокоскоростных локальных сетей;
- стандарты кабелей, основные виды коммуникационных устройств, терминов, понятий, стандартов и типовых элементов

структурированной кабельной системы.

Организация сетевого администрирования операционных систем.

практический опыт:

- восстановления параметров при помощи серверов архивирования и средств управления специализированных операционных систем сетевого оборудования;
- запуска, мониторинга и контроля процедуры установки прикладного программного обеспечения на конечных устройствах пользователей и/или серверном оборудовании;
- выполнения резервного копирования программного обеспечения технических средств, попадающих в область потенциального домена возникновения сбоя;
- выполнения обновления программного обеспечения технических средств согласно инструкции;
- сопоставление аварийной информации от различных устройств информационно-коммуникационной системы;

локализация отказов в сетевых устройствах и операционных системах;

- выявления и определения сбоев и отказов сетевых устройств, и операционных систем;
- устранения последствий сбоев и отказов сетевых устройств и операционных систем

умения:

- идентифицировать и оценивать степень критичности инцидентов, возникающих при установке и работе программного обеспечения, и принимать решение по изменению процедуры установки;
- использовать современные методы контроля производительности информационно-коммуникационной систем;
- локализовать отказ и инициировать корректирующие действия;
- работать с серверами архивирования и средствами управления операционных систем;

- пользоваться нормативно-технической документацией в области инфокоммуникационных технологий;
- использовать различные средства и режимы установки и обновления программного обеспечения информационно-коммуникационной системы, в том числе автоматические;
- выполнять плановое архивирование программного обеспечения пользовательских устройств согласно графику

знания:

- принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети;
- архитектуры аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы;
- лицензионные требования по настройке устанавливаемого программного обеспечения;
- типовые причины инцидентов, возникающих при установке программного обеспечения;
- типовые процедуры и стандарты обновления программного обеспечения технических средств;
- лицензионные требования по настройке обновляемого программного обеспечения;
- регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе;
- требования охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системы

Эксплуатация объектов сетевой инфраструктуры

практический опыт:

− Проектировать архитектуру локальной сети в соответствии с поставленной задачей.

− Использовать специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей.

- Настраивать протоколы динамической маршрутизации.
- Определять влияния приложений на проект сети.
- Анализировать, проектировать и настраивать схемы потоков трафика в компьютерной сети.
- Устанавливать и настраивать сетевые протоколы и сетевое оборудование в соответствии с конкретной задачей.
- Выбирать технологии, инструментальные средства при организации процесса исследования объектов сетевой инфраструктуры.
- Создавать и настраивать одноранговую сеть, компьютерную сеть с помощью маршрутизатора, беспроводную сеть.
- Выполнять поиск и устранение проблем в компьютерных сетях.
- Отслеживать пакеты в сети и настраивать программно-аппаратные межсетевые экраны.
- Настраивать коммутацию в корпоративной сети.
- Обеспечивать целостность резервирования информации.
- Обеспечивать безопасное хранение и передачу информации в глобальных и локальных сетях.
- Создавать и настраивать одноранговую сеть, компьютерную сеть с помощью маршрутизатора, беспроводную сеть.
- Выполнять поиск и устранение проблем в компьютерных сетях.
- Отслеживать пакеты в сети и настраивать программно-аппаратные межсетевые экраны.
- Фильтровать, контролировать и обеспечивать безопасность сетевого трафика.
- Определять влияние приложений на проект сети.
- Мониторинг производительности сервера и протоколирования системных и сетевых событий.
- Использовать специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей.

- Создавать и настраивать одноранговую сеть, компьютерную сеть с помощью маршрутизатора, беспроводную сеть.
- Создавать подсети и настраивать обмен данными;
- Выполнять поиск и устранение проблем в компьютерных сетях.
- Анализировать схемы потоков трафика в компьютерной сети.
- Оценивать качество и соответствие требованиям проекта сети.
- Оформлять техническую документацию.
- Определять влияние приложений на проект сети.
- Анализировать схемы потоков трафика в компьютерной сети.
- Оценивать качество и соответствие требованиям проекта сети.

умения:

- Проектировать локальную сеть.
- Выбирать сетевые топологии.
- Рассчитывать основные параметры локальной сети.
- Применять алгоритмы поиска кратчайшего пути.
- Планировать структуру сети с помощью графа с оптимальным расположением узлов.
- Использовать математический аппарат теории графов.
- Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.
- Выбирать сетевые топологии.
- Рассчитывать основные параметры локальной сети.
- Применять алгоритмы поиска кратчайшего пути.
- Планировать структуру сети с помощью графа с оптимальным расположением узлов.
- Использовать математический аппарат теории графов.
- Использовать многофункциональные приборы и программные средства мониторинга.
- Использовать программно-аппаратные средства технического контроля
- Использовать программно-аппаратные средства технического контроля.

- Читать техническую и проектную документацию по организации сегментов сети.
- Контролировать соответствие разрабатываемого проекта нормативно-технической документации.
- Использовать программно-аппаратные средства технического контроля.
- Использовать техническую литературу и информационно-справочные системы для замены (поиска аналогов) устаревшего оборудования.
- Читать техническую и проектную документацию по организации сегментов сети.
- Контролировать соответствие разрабатываемого проекта нормативно-технической документации.
- Использовать техническую литературу и информационно-справочные системы для замены (поиска аналогов) устаревшего оборудования.

знания:

- Общие принципы построения сетей.
- Сетевые топологии.
- Многослойную модель OSI.
- Требования к компьютерным сетям.
- Архитектуру протоколов.
- Стандартизацию сетей.
- Этапы проектирования сетевой инфраструктуры.
- Элементы теории массового обслуживания.
- Основные понятия теории графов.
- Алгоритмы поиска кратчайшего пути.
- Основные проблемы синтеза графов атак.
- Системы топологического анализа защищенности компьютерной сети.
- Основы проектирования локальных сетей, беспроводные локальные сети.

- Стандарты кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование.
- Средства тестирования и анализа.
- Базовые протоколы и технологии локальных сетей.
- Общие принципы построения сетей.
- Сетевые топологии.
- Стандартизацию сетей.
- Этапы проектирования сетевой инфраструктуры.
- Элементы теории массового обслуживания.
- Основные понятия теории графов.
- Основные проблемы синтеза графов атак.
- Системы топологического анализа защищенности компьютерной сети.
- Архитектуру сканера безопасности.
- Принципы построения высокоскоростных локальных сетей.
- Требования к компьютерным сетям.
- Требования к сетевой безопасности.
- Элементы теории массового обслуживания.
- Основные понятия теории графов.
- Основные проблемы синтеза графов атак.
- Системы топологического анализа защищенности компьютерной сети.
- Архитектуру сканера безопасности.
- Требования к компьютерным сетям.
- Архитектуру протоколов.
- Стандартизацию сетей.
- Этапы проектирования сетевой инфраструктуры.
- Организацию работ по вводу в эксплуатацию объектов и сегментов компьютерных сетей.

- Стандарты кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование.
- Средства тестирования и анализа.
- Программно-аппаратные средства технического контроля.
- Принципы и стандарты оформления технической документации.
- Принципы создания и оформления топологии сети.
- Информационно-справочные системы для замены (поиска) технического оборудования.

2. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Для оценивания сформированности соответствующих компетенций по производственной преддипломной практике применяется аналитическая шкала оценивания.

Критерии оценивания	**Шкала оценивания**			
	неудовлетворительно	**удовлетворительно**	**хорошо**	**отлично**
	показатели			
Соответствие	содержание работы не	содержание работы	содержание	содержание
Содержания теме работы и полнота ее раскрытия	соответствует теме, полностью не соответствует	соответствует не в полной мере теме, тема не полностью раскрыта, требования выполнены со значительными замечаниями	соответствует теме работы, тема раскрыта не полном объеме, несоответствие носит незначительный характер	соответствует теме работы, тема раскрыта в полном объеме, полностью соответствует требованиям
Требования к оформлению работы	Требования не выполнены; имеются грубые стилистические, орфографические, пунктуационные и грамматические ошибки	требования выполнены с незначительными замечаниями, имеются небольшие стилистические, орфографические, пунктуационные и грамматические ошибки	требования выполнены с незначительными замечаниями, имеются небольшие стилистические, орфографические, пунктуационные и грамматические ошибки	требования выполнены полностью, отсутствуют стилистические, орфографические, пунктуационные и грамматические ошибки
Качество выполнения работы	имеются значительные логические нарушения в изложении материала; выводы не соответствуют фактическому материалу, либо носят необоснованный характер	имеются незначительные логические нарушения в изложении материала; выводы не в полной мере соответствуют фактическому материалу	материал изложен логично; сделаны самостоятельные выводы, отвечающие фактическому материалу	материал изложен логично и доказательно; выводы самостоятельные, полные, соответствуют фактическому материалу

Качество защиты	Обучающийся не владеет материалом, показывает неудовлетворительные знания, умения и навыки по применению показателей, методик; на поставленные вопросы дает неправильные ответы	Обучающийся не в полной мере владеет материалом, показывает удовлетворительные знания, умения и навыки по применению показателей, методик; на большинство вопросов дает неправильные ответы	обучающийся владеет материалом, показывает хорошие знания, умения и навыки по применению показателей, методик; на большинство вопросов дает правильные ответы	обучающийся свободно владеет материалом, показывает отличные знания, умения и навыки по применению показателей, методик; правильно отвечает на вопросы по теме работы

3. ТИПОВЫЕ КОНТРОЛЬНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ УМЕНИЙ И (ИЛИ) ПРАКТИЧЕСКОГО ОПЫТА В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Типовые контрольные вопросы
по производственной преддипломной практике
для промежуточной аттестации в форме дифференцированного зачета

Тема 1 Задачи и цели сетевого администрирования, понятие о сетевых протоколах и службах

1. Перечисление задач сетевого администрирования.
2. Перечисление обязанностей сетевого (и системного) администратора.
3. Перечисление основных сетевых служб, функционирующих в корпоративной сети.
4. Изучение моделей межсетевого взаимодействия (модель OSI, модель DARPA).

Тема 2 Протокол TCP/IP, служба DNS

1. Стек протокола TCP/IP (протоколы, входящие в стек TCP/IP; IP-адресация, классы адресов, публичные и приватные IP-адреса; маска подсети).
2. Введение в IP-маршрутизацию.
3. Разрешение имен узлов в IP-адреса (локальный файл hosts; система доменных имен DNS).
4. Служба DNS (пространство имен, домены, зоны, зоны прямого и обратного просмотра, основные и дополнительные зоны, репликация зон).
5. Разрешение имен службой DNS (итеративные и рекурсивные запросы DNS).

Тема 3 Служба каталогов Active Directory

1. Основные понятия служб каталогов системы Windows Server — лес, дерево, домен, организационное подразделение.
2. Планирование пространства имён Active Directory (AD).
3. Установка контроллеров доменов.
4. Логическая и физическая структуры AD, управление репликацией AD.

5. Серверы Глобального каталога и Хозяева операций.

6. Управление пользователями и группами. Управление организационными подразделениями (ОП), делегирование полномочий.

7. Групповые политики.

8. Система безопасности Windows Server (протокол Kerberos, настройка параметров системы безопасности).

Тема 4 Служба файлов и печати (на примере Windows Server)

1. Управление дисками в системе Windows Server (основные и динамические диски).

2. Управление разделами и томами.

3. Виды томов — простой, составной, зеркальный, том с чередованием, том RAID-5.

4. Файловые системы FAT, NTFS.

5. Права доступа к файловым ресурсам, сетевые и локальные права доступа, наследование прав доступа, взятие во владение, аудит доступа к ресурсам

6. Сжатие и шифрование информации, квоты, дефрагментация.

7. Термины и понятия сетевой печати.

8. Установка драйверов, настройка принтеров.

9. Протокол IPP (Internet Printing Protocol).

10. Изложите сущность перспективных технических новшеств в компьютерных сетях, применяемых на практике.

11. Обоснуйте выбор расходного материала (вид кабеля, розетки, коннекторы, патч-панели и т.д.) при проектировании компьютерной сети.

12. Обоснуйте выбор варианта прокладки кабеля при проектировании компьютерной сети.

13. Обоснуйте подбор инструмента и его необходимое количество при проектировании компьютерной сети.

14. Примите решение в случае обрыва кабеля при его прокладке.

15. Назовите факторы, отрицательно влияющие на качество выполнения работ.

16. Озвучьте Ваши предложения по улучшению организации труда на участке компьютерной сети.

17. Озвучьте Ваши предложения по размещению коммутационной комнаты в административном здании.

18. Продемонстрируйте ваши навыки в работе с кабельным тестером.

19. Продемонстрируйте ваши навыки в работе набором для трассировки кабелей.

20. Возникают ли у Вас трудности при работе в команде?

21. Опишите порядок Ваших действий, как руководителя работ при прокладке сетей в административном здании.

22. Какие Вы предпримите действия при нарушении техники безопасности Вашими товарищами во время выполнения работ.

23. Является ли для значимым повышение разряда по итогам производственной практики?

24. Какие инновации встречались на производственной практике в месте ее прохождения.

25.Дайте определения понятиям: Оконечный, промежуточный, смежный узлы.

26. Опишите Принцип работы сети Ethernet.

27. Опишите конструкцию коаксиального кабеля, и назначение его частей.

28. Опишите конструкцию оптоволоконного кабеля, и назначение его частей.

29. Типы антивирусных программ.

30. Классы вирусных программ.

31. Принципы работы файл-сервера, клиент-сервера.

32. Принцип работы коммутатора.

33. Классы ip-адресов.

34. Расчет количества хостов и максимальный и минимальный ip-адрес.

35. Назовите классы подсетей.

36. Перечислите основные сетевые протоколы.

37. Процесс установки Active Directory.

38. Перечислите основные виды антивирусного программного обеспечения.

39. Какие сведения можно просмотреть в журнале мониторинга.

40. Перечислите средства удаленного доступа.

41. Требования к проектированию аппаратных (серверных) комнат.

42. В каких случаях применяется кольцевая топология сети.

43. Что такое DHCP сервер.

44. Для чего используется служба NAT.

45. Чем отличаются сети LAN от сетей WAN.

46. Типы резервного копирования используемые в операционных системах семейства Windows.

47. Назовите основные утилиты для диагностики сети в операционных системах семейства Windows.

48. Назовите команду которая позволяет отслеживать маршрут в Cisco.

49. Назовите диапазон ip-адресов сети класса С.

50. Сколько ip-адресов можно использовать в сети 192.168.10.90 \25.

51. Установите операционную систему на сервер.

52. Опишите порядок регистрации пользователей в локальной сети.

53. Какие права доступа существуют.

54. Опишите порядок настройки архивации и резервного копирования.

55. Разработайте предложения по развитию инфраструктуры сети.

56. Какие меры стоит принять при восстановлении сети после сбоя.

57. Назовите порядок действий при монтаже витой пары на стороне коммутационного шкафа.

58. Перечислите неисправности витой пары.

59. Назовите порядок действий при диагностике неисправностей в пассивном оборудовании.

60. Назовите порядок действий при диагностике неисправностей в активном оборудовании.

61. Назовите программные средства для диагностики компьютера.

62. Приведите порядок действий при замене расходных материалов.

63. Назовите порядок действий при диагностике мелких неисправностей в электронных схемах.

64. Установите операционную систему.

65. Для чего нужны обновления.

66. Порядок настройки сервера автоматических обновлений Windows.

67. Создайте точку восстановления в ручном и автоматическом режимах.

68. Действия при мониторинге сетевой активности.

69. Смоделируйте схему сети в Cisco packet tracer.

70. Сконфигурируйте компьютер для работы в одноранговой сети.

71. Перечислите основные модули службы FTP.

72. Перечислите протоколы электронной почты.

73. Назовите неисправности беспроводной сети.

74. Порядок действий при настройке общих папок.

75. Назовите порядок действий при монтаже витой пары на стороне коммутационного шкафа.

76. Перечислите неисправности витой пары.

77. Назовите порядок действий при диагностике неисправностей в пассивном оборудовании.

78. Назовите порядок действий при диагностике неисправностей в активном оборудовании.

79. Назовите программные средства для диагностики компьютера.

80. Приведите порядок действий при замене расходных материалов.

81.Последовательность выполнения приемов по подготовке электропаяльника к работе.

82.Меры предосторожности при работе с паяльником.

83.Последовательность действий при соединении деталей параллельной пайкой.

84.Классификация назначения флюсов и припоев.

85.Классификация и маркировка различных радиоэлементов.

86. Установка пассивного телекоммуникационного оборудования

87. Постройте физическую карту локальной сети.

88. Перечислите регламенты технических осмотров.

89. Порядок действий при восстановлении сети после сбоя.

90. Назовите порядок настройки межсетевых экранов.

91. Назовите порядок настройки беспроводной сети.

92. Порядок внедрения политик безопасности в операционные системы.

93. Заполните дефектную ведомость.

94. Перечислите действия при проверке состояния трущихся поверхностей в оргтехнике .

95. Что подразумевается под пробной эксплуатацией после ремонта.

96. Перечислите недоделки после ремонта, которые можно выявить визуально.

97. Перечислите возможные нарушения в работе сетевого оборудования, оргтехники.

98. Опишите назначение должности, на которой вы проходили практику.

99. Перечислите основные ваши должностные обязанности на практике.

100. Перечислите техническую документацию по планированию и учету выполнения работ.

101. Перечислите информационные технологии, использованные в ходе прохождения практики.

102. Перечислите основные должностные обязанности системного администратора.

103. Какие основные неисправности возникают на участке компьютерной сети на месте прохождения практики.

104. Назовите основные причины возникновения неисправностей компьютерной сети.

105. Перечислите мероприятия по охране труда при производстве монтажных работ.

106. Перечислите основные пункты Положения по оплате труда на Вашем предприятии.

107. От чего зависит стоимость материалов, необходимых для текущего ремонта компьютерной сети?

108. Перечислите меры предосторожности при монтаже КС.

109. Опишите основные проблемные участки сети на Вашем предприятии.

110. Перечислите основные должностные обязанности техника по обслуживанию ВТ.

111. Какая топология сети используется на вашем предприятии.

112. Перечислите основные виды коммутационного оборудования использующиеся на вашем предприятии.

4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ И ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ.

Процедура оценивания знаний, умений и опыта деятельности при проведении промежуточной аттестации по практике производственной преддипломной практике проводится в форме дифференцированного зачета.

Порядок организации и проведения промежуточной аттестации обучающегося, форма проведения, процедура сдачи зачета, сроки и иные вопросы определены Положением о порядке организации и проведения текущего контроля успеваемости и промежуточной аттестации; Положением о практической подготовке обучающихся.

Процедура оценивания знаний, умений и навыков при проведении промежуточной аттестации по производственной преддипломной практике осуществляется путем подготовки обучающимся отчета по практике с его последующей защитой.

Процесс подготовки и защиты отчета состоит из ряда последовательных этапов:

- получение задания на практику;

- выполнение работ в соответствии с заданием практики;

- подготовка отчета по практике в соответствии с требованиями программы производственной преддипломной практики;

- защита отчета по практике.

По результатам проверки и защиты отчета по практике выставляется отметка в соответствии со шкалой оценивания.

Приложение 1 к
макету по ПДП

Задание
на производственную преддипломную практику

Ф.И.О. обучающегося _____
Специальность 09.02.06 Сетевое и системное администрирование
Сроки практики _____
Наименование организации _____

№ п/п	Содержание практики	Кол-во часов
1	Согласование с руководителем практики от профильной организации индивидуального задания, содержания и планируемых результатов практики; проведение инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка; знакомство с местом прохождения практики	
2	Теоретическая работа (ознакомление с нормативными документами, научной литературой, периодическими изданиями по теме дипломной работы с целью обоснованного выбора теоретической базы предстоящей работы, методического и практического инструментария исследования, постановке целей и задач работы, формулирования гипотез, разработки плана сбора необходимого фактического материала)	
3	Сбор фактических данных о деятельности изучаемого объекта практики в соответствии с выбранной темой дипломной работы; работа с эмпирической базой исследования; анализ данных характеризующих деятельность хозяйствующего субъекта Практическая работа на предприятии, в соответствии с выбранной тематикой дипломной работы	
4	Обобщение полученных результатов (сбор и систематизация накопленной информации, оформление отчета о прохождении практики)	
	Общее количество часов	

Руководитель практики от лицея _____(_____)
(подпись) (Ф.И.О.)

Задание, содержание и планируемые результаты практики согласованы Руководитель практики от организации
_____(_____)
(подпись) (Ф.И.О.)

Приложение 2 к
макету по ПДП

Аттестационный лист
на производственную преддипломную практику

Обучающегося: _____
Специальность 09.02.06 Сетевое и системное администрирование
Место практики: _____
Сроки практики: _____

Уровень освоения компетенций обучающегося по результатам практики

№ п.п.	Код контролируемой компетенции (или ее части)	Формулировка компетенции	Уровень освоения компетенции							
			высокий		средний		достаточный		низкий	
1	ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.								
2	ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.								
3	ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.								
4	ОК 04	Эффективно взаимодействовать и работать в коллективе и								

		команде.								
5	ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.								
6	ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.								
7	ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.								
8	ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.								
9	ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках.								

10	ПК 1.1.	Документировать состояния инфокоммуникационн ых систем и их составляющих в процессе наладки и эксплуатации.								
11	ПК 1.2.	Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационны х систем.								
12	ПК 1.3.	Устранять неисправности в работе инфокоммуникационны х систем.								
13	ПК 1.4.	Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности.								
14	ПК 1.5.	Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем.								
15	ПК 1.6.	Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта.								
16	ПК 1.7.	Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационны х систем.								
17	ПК 2.1.	Принимать меры по устранению сбоев в								

		операционных системах.								
18	ПК 2.2.	Администрировать сетевые ресурсы в операционных системах.								
19	ПК 2.3.	Осуществлять сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.								
20	ПК 2.4.	Осуществлять проведение обновления программного обеспечения операционных систем и прикладного программного обеспечения.								
21	ПК 2.5.	Осуществлять выявление и устранение инцидентов в процессе функционирования операционных систем.								
22	ПК 3.1.	Осуществлять проектирование сетевой инфраструктуры.								
23	ПК 3.2.	Обслуживать сетевые конфигурации программно-аппаратных средств.								
24	ПК 3.3.	Осуществлять защиту информации в сети с использованием программно-аппаратных средств.								
25	ПК 3.4.	Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры.								
26	ПК 3.5.	Модернизировать сетевые устройства информационно-коммуникационных систем.								

Мнение об уровне подготовленности обучающегося к решению профессиональных задач *(отметить нужное)*		высокий		достаточный	
		средний		низкий	

Характеристика на обучающегося по освоению профессиональных компетенций в период практики:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Заключение об уровне сформированности профессиональных компетенций:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Оценка после защиты (с учетом характеристики с места практики):_____

Руководитель практики от организации_____(_____)

Руководитель практики от образовательной организации_____(_____)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ
СПЕЦИАЛЬНОСТЬ

СПЕЦИАЛЬНОСТЬ 09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ
АДМИНИСТРИРОВАНИЕ

2024

СОДЕРЖАНИЕ

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

1.1. Область применения

Фонд оценочных средств предназначен для контроля и оценки результатов освоения профессионального модуля Эксплуатация объектов сетевой инфраструктуры по специальности 09.02.06 Сетевое и системное администрирование в части освоения основного вида профессиональной деятельности (ВПД) «Эксплуатация объектов сетевой инфраструктуры», и соответствующих профессиональных компетенций (ПК) и общих компетенций (ОК):

ПК 3.1. Осуществлять проектирование сетевой инфраструктуры.

ПК 3.2. Обслуживать сетевые конфигурации программно-аппаратных средств.

ПК 3.3. Осуществлять защиту информации в сети с использованием программно-аппаратных средств.

ПК 3.4. Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры.

ПК 3.5. Модернизировать сетевые устройства информационно-коммуникационных систем.

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

При реализации программы ПМ.03 Эксплуатация объектов сетевой инфраструктуры», МДК.03.01 «Эксплуатация объектов сетевой инфраструктуры», МДК.03.02 «Безопасность компьютерных сетей» УП И ПП у обучающихся должны быть сформированы:

практический опыт:

Проектировать архитектуру локальной сети в соответствии с поставленной задачей.

Использовать специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей.

Настраивать протоколы динамической маршрутизации.

Определять влияния приложений на проект сети.

Анализировать, проектировать и настраивать схемы потоков трафика в компьютерной сети.

Устанавливать и настраивать сетевые протоколы и сетевое оборудование в соответствии с конкретной задачей.

Выбирать технологии, инструментальные средства при организации процесса исследования объектов сетевой инфраструктуры.

Создавать и настраивать одноранговую сеть, компьютерную сеть с помощью маршрутизатора, беспроводную сеть.

Выполнять поиск и устранение проблем в компьютерных сетях.

Отслеживать пакеты в сети и настраивать программно-аппаратные межсетевые экраны.

Настраивать коммутацию в корпоративной сети.

Обеспечивать целостность резервирования информации.

Обеспечивать безопасное хранение и передачу информации в глобальных и локальных сетях.

Создавать и настраивать одноранговую сеть, компьютерную сеть с помощью маршрутизатора, беспроводную сеть.

Выполнять поиск и устранение проблем в компьютерных сетях.

Отслеживать пакеты в сети и настраивать программно-аппаратные межсетевые экраны.

Фильтровать, контролировать и обеспечивать безопасность сетевого трафика.

Определять влияние приложений на проект сети.

Мониторинг производительности сервера и протоколирования системных и сетевых событий.

Использовать специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей.

Создавать и настраивать одноранговую сеть, компьютерную сеть с помощью маршрутизатора, беспроводную сеть.

Создавать подсети и настраивать обмен данными;

Выполнять поиск и устранение проблем в компьютерных сетях.

Анализировать схемы потоков трафика в компьютерной сети.

Оценивать качество и соответствие требованиям проекта сети.

Оформлять техническую документацию.

Определять влияние приложений на проект сети.

Анализировать схемы потоков трафика в компьютерной сети.

Оценивать качество и соответствие требованиям проекта сети.

умения:

У1. Проектировать локальную сеть.

У2. Выбирать сетевые топологии.

У3. Рассчитывать основные параметры локальной сети.

У4. Применять алгоритмы поиска кратчайшего пути.

У5. Планировать структуру сети с помощью графа с оптимальным расположением узлов.

У6. Использовать математический аппарат теории графов.

У7. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.

У8. Выбирать сетевые топологии.

У9. Рассчитывать основные параметры локальной сети.

У10. Применять алгоритмы поиска кратчайшего пути.

У11. Планировать структуру сети с помощью графа с оптимальным расположением узлов.

У12. Использовать математический аппарат теории графов.

У13. Использовать многофункциональные приборы и программные средства мониторинга.

У14. Использовать программно-аппаратные средства технического контроля

У15. Читать техническую и проектную документацию по организации сегментов сети.

У16. Контролировать соответствие разрабатываемого проекта нормативно-технической документации.

У17. Использовать техническую литературу и информационно-справочные системы для замены (поиска аналогов) устаревшего оборудования.

знания:

З1. Общие принципы построения сетей.

З2. Сетевые топологии.

З3. Многослойную модель OSI.

З4. Требования к компьютерным сетям.

35. Архитектуру протоколов.

36. Стандартизацию сетей.

37. Этапы проектирования сетевой инфраструктуры.

38. Элементы теории массового обслуживания.

39. Основные понятия теории графов.

310. Алгоритмы поиска кратчайшего пути.

311. Основные проблемы синтеза графов атак.

312. Системы топологического анализа защищенности компьютерной сети.

313. Основы проектирования локальных сетей, беспроводные локальные сети.

314. Стандарты кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование.

315. Средства тестирования и анализа.

316. Базовые протоколы и технологии локальных сетей.

317. Общие принципы построения сетей.

318. Сетевые топологии.

319. Стандартизацию сетей.

320. Этапы проектирования сетевой инфраструктуры.

321. Элементы теории массового обслуживания.

322. Основные понятия теории графов.

323. Основные проблемы синтеза графов атак.

324. Системы топологического анализа защищенности компьютерной сети.

325. Архитектуру сканера безопасности.

326. Принципы построения высокоскоростных локальных сетей.

327. Требования к компьютерным сетям.

328. Требования к сетевой безопасности.

329. Элементы теории массового обслуживания.

330. Основные понятия теории графов.

331. Основные проблемы синтеза графов атак.

332. Системы топологического анализа защищенности компьютерной сети.

333. Архитектуру сканера безопасности.

334. Требования к компьютерным сетям.

335. Архитектуру протоколов.

336. Стандартизацию сетей.

337. Этапы проектирования сетевой инфраструктуры.

338. Организацию работ по вводу в эксплуатацию объектов и сегментов компьютерных сетей.

339. Стандарты кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование.

340. Средства тестирования и анализа.

341. Программно-аппаратные средства технического контроля.

342. Принципы и стандарты оформления технической документации

343. Принципы создания и оформления топологии сети.

344. Информационно-справочные системы для замены (поиска) технического оборудования.

1.2. Формы контроля и оценивания элементов профессионального модуля/дисциплины

Элементы модуля, профессиональный модуль	**Формы контроля и оценивания**	
	Промежуточная аттестация	**Текущий контроль**
МДК.03.01 Эксплуатация объектов сетевой инфраструктуры	Экзамен	Устный и письменный опрос; Тестирование; Оценка результатов выполнения практических работ; Контроль выполнения домашних и самостоятельных работ; Разбор ситуационных заданий.
МДК.03.02 Безопасность компьютерных сетей	Экзамен	
УП.03.01 Учебная практика «Эксплуатация объектов сетевой инфраструктуры»	Дифференцированный зачет	Оценка выполнения проверочных заданий по учебной практике; Наблюдение и оценка выполнения работ при прохождении учебной практики.
ПП. 03.01 Производственная практика «Эксплуатация объектов сетевой инфраструктуры»	Дифференцированный зачет	Наблюдение и оценка выполнения работ при прохождении производственной практики.

ПМ.03 Эксплуатация объектов сетевой инфраструктуры	Экзамен квалификационный

1.3. Перечень оценочных средств и их характеристика

Формы контроля	Виды контроля	Краткая характеристика	Формы контрольно-оценочного средства в фонде
Текущий контроль успеваемости	Устный опрос	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемым МДК, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.	Вопросы для обсуждения
	Защита практических работ	Учебные занятия, которые направлены на экспериментальное подтверждение теоретических положений и формирование учебных и профессиональных практических умений и составляют важную часть теоретической и профессиональной практической подготовки.	Вопросы по практическим работам
	Ситуационные задания	Проблемное задание, в котором обучающемуся предлагают осмыслить реальную профессионально-ориентированную ситуацию, необходимую для решения данной проблемы. Сущность данного метода состоит в том, что учебный материал подается обучающемуся в виде реальных профессиональных проблем конкретного предприятия или характерных для определенного вида профессиональной деятельности. Работая над решением кейса, обучающийся приобретает профессиональные знания, умения, навыки в результате активной творческой работы. Он самостоятельно формулирует цели, находит и собирает различную информацию, анализирует ее, выдвигает гипотезы, ищет варианты решения проблемы, формулирует выводы, обосновывает оптимальное решение ситуации.	Варианты ситуационных заданий составляются на основе типовых заданий.
	Домашняя и самостоятельная работа	Самостоятельная работа, домашняя работа - планируемая учебная, учебно-исследовательская, научно-исследовательская работа обучающихся, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.	Задания для самостоятельной работы выдается преподавателем дифференцированно

			согласно рабочей программе
	Тестирование	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Банк тестовых заданий, составляется на основе типовых заданий
Промежуточная аттестация	Дифференцированный зачет экзамен, квалификационный экзамен	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Задания, вопросы по учебному материалу, направленному на освоение компетенций и вида деятельности согласно требованиям федерального государственного образовательного стандарта.	Банк заданий, составляется на основе типовых заданий

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ МОДУЛЯ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

В результате контроля и оценки по профессиональному модулю осуществляется комплексная проверка следующих профессиональных и общих компетенций:

Показатели оценки результата освоения профессиональных компетенций

В результате оценки осуществляется проверка следующих объектов:

Предмет оценивания (*ПК,ОК,У,З,ПО)*	**Объекты оценивания**	**Показатели**
ПК 3.1. Осуществлять проектирование сетевой инфраструктуры.	Осуществление проектирования сетевой инфраструктуры.	Правильное проектирование сетевой инфраструктуры.
ПК 3.2. Обслуживать сетевые конфигурации программно-аппаратных средств.	Обслуживание сетевой конфигурации программно-аппаратных средств.	Правильное обслуживание сетевой конфигурации программно-аппаратных средств.
ПК 3.3. Осуществлять защиту информации в сети с использованием программно-аппаратных средств.	Осуществление защиты информации в сети с использованием программно-аппаратных средств.	Правильно осуществлять защиту информации в сети с использованием программно-аппаратных средств.
ПК 3.4. Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры.	Осуществление устранения нетипичных неисправностей в работе сетевой инфраструктуры.	Грамотное устранять нетипичные неисправности в работе сетевой инфраструктуры.
ПК 3.5. Модернизировать сетевые устройства информационно-коммуникационных систем.	Модернизация сетевых устройств информационно-коммуникационных систем.	Грамотная модернизация сетевых устройств информационно-коммуникационных систем.
ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Выбор способа решения задач профессиональной деятельности, применительно к различным контекстам.	Грамотный выбор способа решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач	Использование современных средств поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.	Грамотное использование современных средств поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.

профессиональной деятельности.		
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.	Планирование и реализация собственного профессионального и личностного развития, предпринимательской деятельности в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.	Грамотное планирование и реализация собственного профессионального и личностного развития, предпринимательской деятельности в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде.	Эффективное взаимодействие и работа в коллективе и команде.	Грамотная взаимодействие и работа в коллективе и команде.
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.	Осуществление устной и письменной коммуникации на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.	Правильное осуществление устной и письменной коммуникации на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.	Проявление гражданско-патриотической позиции, демонстрация осознанного поведения на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.	Правильное проявление гражданско-патриотической позиции, демонстрация осознанного поведения на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.
ОК 7. Содействовать сохранению окружающей среды,	Содействие сохранению окружающей среды, ресурсосбережению,	Грамотное содействие сохранению окружающей среды, ресурсосбережению, применять

ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.	применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.	знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.
ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	Использование средств физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	Правильное использование средств физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 9. Пользоваться профессиональной документацией на государственном и иностранном языках.	Использование профессиональной документацией на государственном и иностранном языках.	Правильное использование профессиональной документацией на государственном и иностранном языках.
У1. Проектировать локальную сеть.	Умение проектирования локальных сетей.	Использование умения проектирование локальных сетей.
У2. Выбирать сетевые топологии.	Умение выбира сетевых топологий.	Использование умения выбира сетевых топологий.
У3. Рассчитывать основные параметры локальной сети.	Умение рассчитывания основных параметров локальной сети.	Грамотное умение рассчитывания основных параметров локальной сети.
У4. Применять алгоритмы поиска кратчайшего пути.	Умение применять алгоритмы поиска кратчайшего пути.	Грамотное умение применять алгоритмы поиска кратчайшего пути.
У5. Планировать структуру сети с помощью графа с оптимальным расположением узлов.	Умение планирования структуры сети с помощью графа с оптимальным расположением узлов.	Использование умения планирования структуры сети с помощью графа с оптимальным расположением узлов.
У6. Использовать математический аппарат теории графов.	Умение использования математического аппарата теории графов.	Грамотное умение использования математического аппарата теории графов.
У7. Настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для	Умение настраивание стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.	Грамотное умение настраивание стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети.

диагностики работоспособности сети.		
У8. Выбирать сетевые топологии.	Умение выбора сетевых топологий.	Грамотное умение выбора сетевых топологий.
У9. Рассчитывать основные параметры локальной сети.	Умение рассчитывание основных параметров локальной сети.	Использование умения рассчитывание основных параметров локальной сети.
У10. Применять алгоритмы поиска кратчайшего пути.	Умение применение алгоритмов поиска кратчайшего пути.	Использование умения применения алгоритмов поиска кратчайшего пути.
У11. Планировать структуру сети с помощью графа с оптимальным расположением узлов.	Умение планирования структуры сети с помощью графа с оптимальным расположением узлов.	Использование умения планирования структуры сети с помощью графа с оптимальным расположением узлов.
У12. Использовать математический аппарат теории графов.	Умение использования математического аппарата теории графов.	Грамотное умение использования математического аппарата теории графов.
У13. Использовать многофункциональные приборы и программные средства мониторинга.	Умение использования многофункционального прибора и программного средства мониторинга.	Грамотное умение использования многофункционального прибора и программного средства мониторинга.
У14. Использовать программно-аппаратные средства технического контроля.	Умение использования программно-аппаратных средств технического контроля.	Грамотное умение использования программно-аппаратных средств технического контроля.
У15. Читать техническую и проектную документацию по организации сегментов сети.	Умение читать техническую и проектную документацию по организации сегментов сети.	Грамотное умение читать техническую и проектную документацию по организации сегментов сети.
У16. Контролировать соответствие разрабатываемого проекта нормативно-технической документации.	Умение контролирования соответствие разрабатываемого проекта нормативно-технической документации.	Использовать умение контролирования соответствие разрабатываемого проекта нормативно-технической документации.
У17. Использовать техническую литературу и информационно-справочные системы для замены (поиска аналогов) устаревшего оборудования.	Умение использования технической литературы и информационно-справочные системы для замены (поиска аналогов) устаревшего оборудования.	Грамотное умение использования технической литературы и информационно-справочные системы для замены (поиска аналогов) устаревшего оборудования.
У18. Контролировать соответствие	Умение контролирования соответствие	Использование умения контролирования соответствие

разрабатываемого проекта нормативно-технической документации.	разрабатываемого проекта нормативно-технической документации.	разрабатываемого проекта нормативно-технической документации.
31. Общие принципы построения сетей.	Знание общих принципов построения сетей.	Использование знаний общих принципов построения сетей.
32. Сетевые топологии.	Знание сетевой топологии.	Использовать знания сетевой топологии.
33. Многослойную модель OSI.	Знание многослойной модели OSI.	Использовать знания многослойной модели OSI.
34. Требования к компьютерным сетям.	Знание требований к компьютерным сетям.	Использовать знания требований к компьютерным сетям.
35. Архитектуру протоколов.	Знание архитектуры протоколов.	Использование знаний архитектуры протоколов.
36. Стандартизацию сетей.	Знание стандартизации сетей.	Использование знаний стандартизации сетей.
37. Этапы проектирования сетевой инфраструктуры.	Знание этапов проектирования сетевой инфраструктуры.	Использование знаний этапов проектирования сетевой инфраструктуры.
38. Элементы теории массового обслуживания.	Знание элементов теории массового обслуживания.	Использование знаний элементов теории массового обслуживания.
39. Основные понятия теории графов.	Знание основных понятий теории графов.	Использование знаний основных понятий теории графов.
310. Алгоритмы поиска кратчайшего пути.	Знание алгоритмов поиска кратчайшего пути.	Использование знаний алгоритмов поиска кратчайшего пути.
311. Основные проблемы синтеза графов атак.	Знание основных проблем синтеза графов атак.	Использование знаний основных проблем синтеза графов атак.
312. Системы топологического анализа защищенности компьютерной сети.	Знание систем топологического анализа защищенности компьютерной сети.	Использование знаний систем топологического анализа защищенности компьютерной сети.
313. Основы проектирования локальных сетей, беспроводные локальные сети.	Знание основ проектирования локальных сетей, беспроводные локальные сети.	Использование знаний основ проектирования локальных сетей, беспроводные локальные сети.
314. Стандарты кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование.	Знание стандартов кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование.	Использование знаний стандартов кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование.

315. Средства тестирования и анализа.	Знание средств тестирования и анализа.	Использование знаний средств тестирования и анализа.
316. Базовые протоколы и технологии локальных сетей.	Знание базовых протоколов и технологии локальных сетей.	Использование знаний базовых протоколов и технологии локальных сетей.
317. Общие принципы построения сетей.	Знание общих принципов построения сетей.	Использование знаний общих принципов построения сетей.
318. Сетевые топологии.	Знание сетевых топологий.	Использование знаний сетевых топологий.
319. Стандартизацию сетей.	Знание стандартизации сетей.	Использование знаний стандартизации сетей.
320. Этапы проектирования сетевой инфраструктуры.	Знание этапов проектирования сетевой инфраструктуры.	Использование знаний этапов проектирования сетевой инфраструктуры.
321. Элементы теории массового обслуживания.	Знание элементов теории массового обслуживания.	Использование знаний элементов теории массового обслуживания.
322. Основные понятия теории графов.	Знание основных понятий теории графов.	Использование знаний основных понятий теории графов.
323. Основные проблемы синтеза графов атак.	Знание основных проблем синтеза графов атак.	Использование знаний основных проблем синтеза графов атак.
324. Системы топологического анализа защищенности компьютерной сети.	Знание системы топологического анализа защищенности компьютерной сети.	Использование знаний системы топологического анализа защищенности компьютерной сети.
325. Архитектуру сканера безопасности.	Знание архитектуры сканера безопасности.	Использование знаний архитектуры сканера безопасности.
326. Принципы построения высокоскоростных локальных сетей.	Знание принципов построения высокоскоростных локальных сетей.	Использование знания принципов построения высокоскоростных локальных сетей.
327. Требования к компьютерным сетям.	Знание требований к компьютерным сетям.	Использование знания требований к компьютерным сетям.
328. Требования к сетевой безопасности.	Знание требований к сетевой безопасности.	Использование знания требований к сетевой безопасности.
329. Элементы теории массового обслуживания.	Знание элементов теории массового обслуживания.	Использование знаний элементов теории массового обслуживания.
330. Основные понятия теории графов.	Знание основных понятия теории графов.	Использование знания основных понятия теории графов.
331. Основные проблемы синтеза графов атак.	Знание основных проблем синтеза графов атак.	Использование знания основных проблем синтеза графов атак.

332. Системы топологического анализа защищенности компьютерной сети.	Знание системы топологического анализа защищенности компьютерной сети.	Использование знания системы топологического анализа защищенности компьютерной сети.
333. Организацию работ по вводу в эксплуатацию объектов и сегментов компьютерных сетей.	Знание организации работ по вводу в эксплуатацию объектов и сегментов компьютерных сетей.	Использование знания организации работ по вводу в эксплуатацию объектов и сегментов компьютерных сетей.
334. Программно-аппаратные средства технического контроля.	Знание программно-аппаратных средств технического контроля.	Использование знания программно-аппаратных средств технического контроля.
335. Принципы и стандарты оформления технической документации.	Знание принципов и стандартов оформления технической документации.	Использование знания принципов и стандартов оформления технической документации.
336. Принципы создания и оформления топологии сети.	Знание принципов создания и оформления топологии сети.	Использование знания принципов создания и оформления топологии сети.
337. Информационно-справочные системы для замены (поиска) технического оборудования.	Знание информационно-справочных систем для замены (поиска) технического оборудования.	Использование знаний информационно-справочных систем для замены (поиска) технического оборудования.

3. ОЦЕНКА ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Основной целью оценки профессионального модуля является оценка умений и знаний, ПК и ОК.

Оценка профессионального модуля осуществляется с использованием следующих форм и методов контроля:

- практические занятия;
- тестирование;
- дифференцированный зачет;
- экзамен.

3.1 ТЕКУЩИЙ И РУБЕЖНЫЙ КОНТРОЛЬ

Материалы для проведения текущей и рубежной аттестации.

Материально-техническое обеспечение фонда оценочных мероприятий

Контрольно-оценочные мероприятия проводятся в учебном кабинете №2 «Информационных технологий в профессиональной деятельности».

- Оборудование учебного кабинета:
- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- учебная доска.

Технические средства обучения:

- компьютер с программным обеспечением
- мультимедийный проектор
- мультимедийное оборудование;

– принтер лазерный;

– сканер;

– аудиосистема;

– локальная сеть;

– подключение к глобальной сети Интернет.

Комплект оценочных средств.

Комплект материалов для оценки сформированности общих и профессиональных компетенций по МДК.03.01 «Эксплуатация объектов

сетевой инфраструктуры», МДК.03.02 «Безопасность компьютерных сетей», УП.03.01 Учебная практика " Эксплуатация объектов сетевой инфраструктур", ПП.03.01 Производственная практика" Эксплуатация объектов сетевой инфраструктуры", ПМ.03 «Эксплуатация объектов сетевой инфраструктуры».
http://testdoc.ru
http://oltest.ru

Задания рубежного контроля

Тестирование.

МДК 03.01 «Эксплуатация объектов сетевой инфраструктуры»

Вариант 1

Количество вопросов – 30. Возможны несколько правильных ответов

1) Что такое «BACKUP-СЕРВЕР»?

1. Сервер, на который копируется контент с продакшн-сервера;
2. Файловый сервер;
3. Сервер печати;
4. Web-сервер;

2) Укажите количество основных этапов восстановления работоспособности сети:

1. 3;
2. 4;
3. 5;
4. 6;
5. 7.

3) Это неполадки, которые проявляются нерегулярно. Они имеют особенность проявляться в самые неподходящие моменты *(выберите несколько вариантов ответов).*

1. Перемежающийся отказ;
2. Сбой;
3. Систематический сбой;
4. Отказ;

5. Скрытые дефекты.

4) Информация, которая загружается в хранилище, должна *(вставьте недостающее слово)* **в целостную структуру, отвечающую целям анализа данных:**

1. загружаться;
2. интегрироваться;
3. преобразовываться;
4. переформатироваться.

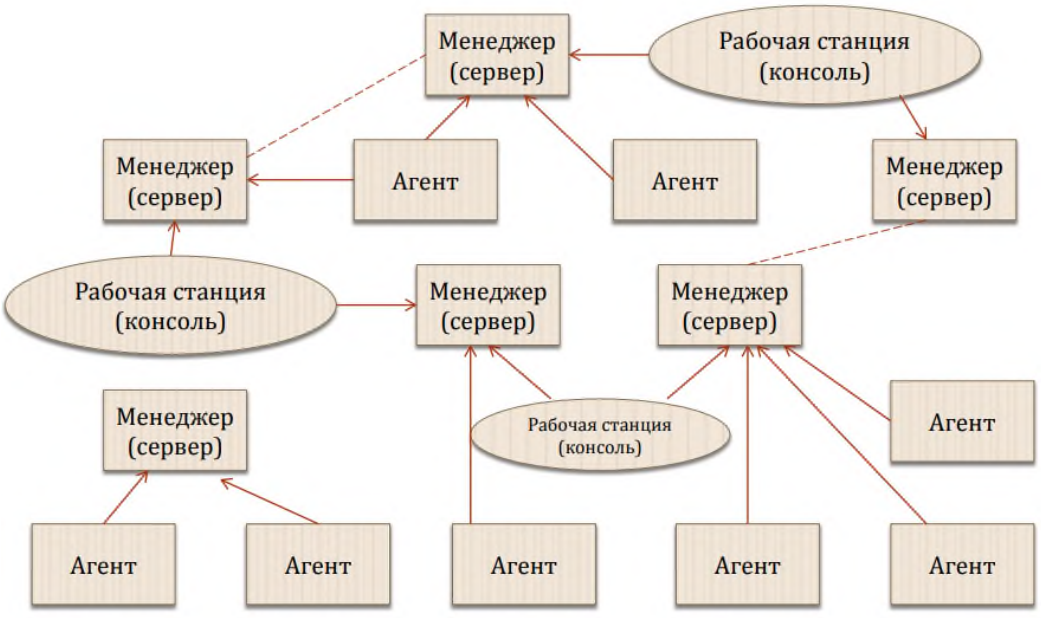
5) Активное сетевое оборудование предназначено для:

1. передачи сигнала без усиления;
2. передачи сигнала с усилением;
3. выполнения всех необходимых действий, связанных с передачей данных.

6) Хранилища данных являются:

1. одноуровневыми;
2. многозадачными;
3. линейными;
4. структурированными.

7) На рисунке изображена схема взаимодействия.



(выберите один вариант ответа):

1. Взаимодействие агента, менеджера и управляемого ресурса;

2. Распределенная система управления на основе нескольких менеджеров и рабочих станций;

3. Иерархические связи между менеджерами;

4. Одноранговые связи между менеджерами.

8) Что такое стример?

1. тип дискового накопителя;

2. накопитель на магнитной ленте;

3. тип гибкого диска;

4. тип флэш - памяти.

9) Резервная копия, которая создается при включенном сервере БД, называется:

1. оптимальный бекап базы данных;

2. горячий бекап базы данных;

3. холодный бекап базы данных;

4. бекап базы данных.

10) Позволяют оценить готовность сети организации к внедрению тех или иных продуктов или комплексных решений, предлагаемых производителями*:*

1. методики аудита;

2. способы аудита;

3. все варианты ответовверны;

4. средства аудита.

11) Процесс приведения данных к некоторому виду, который могут понимать только отправитель и получатель:

1. Модуляция;

2. Шифрование;

3. Синхронизация;

4. Сравнение.

12) Масштабируемость (scalability) означает:

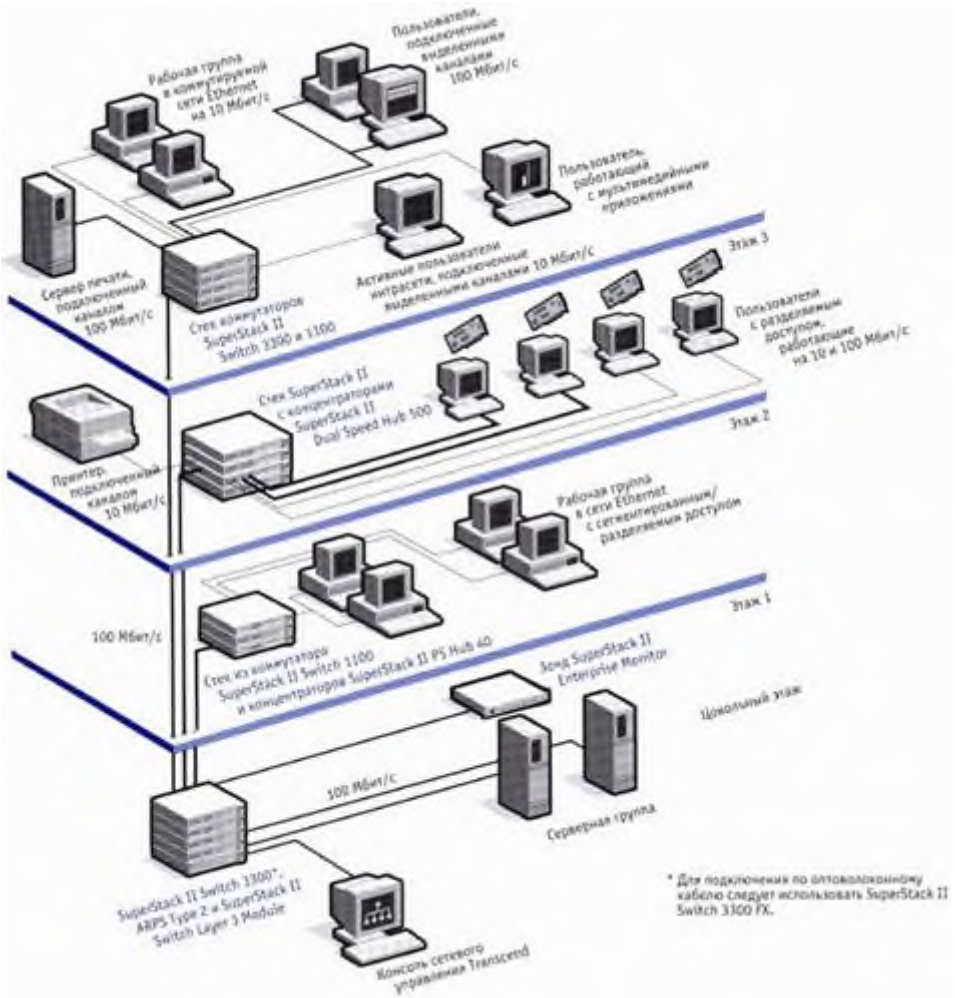
1. возможность сравнительно легкого добавления отдельных элементов сети,

наращивания длины сегментов сети и замены существующей аппаратуры более мощной;

2. что сеть позволяет наращивать количество узлов и протяженность связей в очень широких пределах, при этом производительность сети не ухудшается;

3. что сеть представляется пользователям не как множество отдельных компьютеров, связанных между собой сложной системой кабелей, а как единая традиционная вычислительная машина с системой разделения времени.

13) На рисунке изображена:



1. логическая карта сети;

2. физическая карта сети;

3. схема здания с расположением ПК,

14) Информация в хранилище данных структурируется по разным уровням детализации *(выберите правильные варианты ответов)*:

1. низкая степень суммаризации;

2. высокая степень суммаризации;

3. текущая детальная информация;

4. одноуровневой суммаризации;

5. многоуровневой суммаризации.

15) Выберите основные средства, применяемые для анализа и диагностики вычислительных сетей *(выберите несколько вариантов).*

1. Агенты систем управления;

2. Анализаторы протоколов;

3. Экспертные системы;

4. Встроенные системы диагностики и управления;

5. Антивирусы.

16) Обслуживание ЛВС сводится к текущему поддержанию работоспособности сети, которое включает в себя следующие основные работы *(выберите несколько вариантов)*:

1. Обеспечение взломстойкости сети;

2. Настройка и поддержка работоспособности компьютеров и периферии;

3. Своевременное протирание от пыли серверов и сетевого оборудования;

4. Установка и удаление программ пользователей;

5. Плановая диагностика серверов и другого сетевого оборудования.

17) Укажите порядок проведения аудита

1. Постановка задачи и уточнение границ работ;

2. Сбор данных;

3. Анализ данных и оформление результатов

4. Встроенные системы диагностики и управления;

5. Антивирусы.

18) Расширяемость (extensibility) означает…

1. Что сеть позволяет наращивать количество узлов и протяженность связей в очень широких пределах, при этом производительность

сети не ухудшается;

2. что сеть представляется пользователям не как множество отдельных компьютеров, связанных между собой сложной

системой кабелей, а как единая традиционная вычислительная машина с системой разделения времени;

3. что сеть позволяет наращивать количество узлов и протяженность связей

в очень широких пределах, при этом производительность сети не ухудшается.

19) Укажите виды резервного копирования *(выберите несколько вариантов).*

1. Резервное копирование в режиме реального времени;
2. Дифференциальное резервирование;
3. Резервирование клонированием;
4. Инкрементное резервирование;
5. Резервирование в виде образа;
6. Полное резервирование

20) Резервирование, при котором происходит копирование только тех файлов, которые были изменены с тех пор, как в последний раз выполнялось полное или добавочное резервное копирование.

1. Резервное копирование в режиме реального времени;
2. Дифференциальное резервирование;
3. Резервирование клонированием;
4. Инкрементное резервирование;
5. Резервирование в виде образа;
6. Полное резервирование.

21) Как называется копирование, которое администратор делает вручную?

1. резервное копирование в режиме реального времени;
2. ручное копирование;
3. одноразовое копирование;
4. администраторское копирование.

22) Процесс создания копии данных на носителе, предназначенном для восстановления данных…

1. Резервное копирование в режиме реального времени;

2. Дифференциальное резервирование;

3. Резервирование клонированием;

4. Инкрементное резервирование;

5. Резервирование в виде образа;

6. Полное резервирование.

23) Это комплекс организационно – технических мероприятий и работ, производимых на объекте и направленных на поддержание в рабочем или исправном состоянии оборудования (программного обеспечения) систем в процессе их использования по назначению с целью повышения надежности и эффективности их работы.

1. Техническое обслуживание;

2. Резервное копирование;

3. Инвентаризация;

4. Модернизация.

24) Подразумевается, что некий набор носителей используется циклически.

1. Простая ротация;

2. Циклическое использование;

3. Сложная ротация;

4. Циклическая ротация;

25) Сопоставьте определение мониторинга компьютерных сетей *(расположите их в хронологическом порядке):*

1. мониторинг осуществляется в процессе обслуживания оборудования;

2. мониторинг парольной защиты и контроль надежности пользовательских паролей;

3. предупреждение и своевременное выявление попыток несанкционированного доступа;

4. мониторинг производительности КС производится по обращениям пользователей в ходе обслуживания систем и при проведении профилактических работ

_____Мониторинг производительности;

_____Мониторинг аппаратного обеспечения;

_____Мониторинг попыток несанкционированного доступа;

_____Мониторинг парольной защиты

26) Как минимизировать паразитный трафик? *(выберите несколько вариантов).*

1. Установка антивирусных программ;
2. Отключение «лишних» служб Windows;
3. Использование межсетевого экрана (брандмауэры);
4. Верных вариантов ответа нет;
5. Установка критических обновлений для ОС Windows.

27) Резервирование, при котором каждый файл, который был изменен с момента последнего полного резервирования, копируется каждый раз заново…

1. Резервное копирование в режиме реального времени;
2. Дифференциальное резервирование;
3. Резервирование клонированием;
4. Инкрементное резервирование;
5. Резервирование в виде образа;
6. Полное резервирование.

28) Выберите основные требования к хранилищам данных *(выберите несколько вариантов)*.

1. верных ответов нет;
2. поддержка внутренней непротиворечивости данных;
3. поддержка высокой скорости;
4. полнота и достоверность хранимых данных;
5. возможность получения и сравнения данных.

29) Способ отслеживания событий и действий пользователей, отслеживание состояния сетевой инфраструктуры

1. аудит;

2. мониторинг;

3. анализ;

4. диагностика..

30) Технология, которая позволяет гибко распределять ресурсы между приложениями, каждое из которых при этом "видит" только предназначенные ему ресурсы и "считает", что ему выделен отдельный сервер

1. ротация;

2. виртуализация;

3. инвентаризация;

4. авторизация;

5. инициализация

Ключи к тестам:

1-1	11-2	21-3
2-6	12-2	22-1
3-1,3,5	13-2	23-1
4-2	14-1,2,3	24-1
5-3	15-1,2,3,4	25-4,**1**,3,2
6-4	16-1,2,5	26-1,2,3,5
7-2	17-1,2,3	27-1
8-2	18-3	28-2,3,4,5
9-2	19-1,2,3,4,5,6	29-1
10-1	20-4	30-2

Вариант 2

Количество вопросов – 30. Возможны несколько правильных ответов

1) Данная группа действий используется для постоянного получения информации о составе технических средств сети

1. Техническое обслуживание;

2. Резервное копирование;

3. Инвентаризация;

4. Модернизация.

2) Это рабочий сервер, который выполняет, какие либо сервисы для пользователей (собирательное название)

1. Продакшн-сервер;

2. Почтовый сервер;

3. Файловый сервер;

4. Сервер баз данных.

3) Расставьте соответствие видам коллизий

1. это коллизия, фиксируемая в домене, где подключено измерительное устройство, в пределах передачи преамбулы или первых 64 байт кадра, когда источник передачи находится в домене;

2. это коллизия, которая возникает в другом физическом сегменте сети (т. е. за повторителем);

3. это местная коллизия, которая фиксируется уже после того, как станция передала в канал связи

_____Удаленная коллизия (remote collision);

_____Поздняя коллизия (late collision)

_____Местная коллизия (local collision)

4) Смена рабочего набора носителей в процессе копирования

1. Резервирование;

2. Ротация;

3. Арбитраж (arbitration);

4. Восстановление после ошибок (errorrecovery).

5) Какая схема изображена на рисунке?

1. физическая карта сети;

2. логическая карта сети;

3. схема здания с расположением ПК

6) Укажите основные характеристики производительности сети

(выберите несколько вариантов ответов).

1. Количество байт, полученных с рабочей станции;

2. Количество ошибок системы безопасности;

3. Количество команд в очереди на исполнение;

4. Сеансы соединений с сервером;

5. Количество коллизий в секунду.

7) Делегирование внешней специализированной компании решение вопросов, связанных с разработкой, внедрением и сопровождением информационных систем как целиком на уровне инфраструктуры предприятия, так и объемов работ, связанных с развитием и/или поддержкой функционирования отдельных участков системы, логической структуры;

1. контракт;

2. договор;

3. шефство;

4. аутсорсинг.

8) Утилизация канала связи сети – это…

1. наложение двух и более кадров (пакетов) от станций, пытающихся передать кадр в один и тот же момент времени из-за наличия задержки распространения сигнала по сети или наличия неисправной сетевой платы;

2. доля пропускной способности канала связи, занимаемой кадрами, коллизиями и помехами;

3. нежелательное физическое явление или воздействие электрических, магнитных или электромагнитных полей, электрических токов или напряжений внешнего или внутреннего источника, которое нарушает нормальную работу технических средств.

9) Полное резервирование – это…*(выберите несколько вариантов ответов)*

1. ежедневное;

2. еженедельное;

3. ежемесячное;

4. квартальное.

10) Выберите минимальный комплект эксплуатационной документации на сетевую инфраструктуру … *(выберите несколько вариантов ответов)*

1. таблицу конфигурации сетевых устройств;

2. профили приложений;

3. инструкции обслуживающему персоналу;

4. таблицу конфигурации устройств, подключаемых к сети;

5. схему топологии сети.

11) Сопоставьте устройства для тестирования сетевой инфраструктуры

1. предназначены для тестирования кабелей различных категорий. Также они собирают данные о статистических показателях трафика;

2. выполняют сертификацию в соответствии с требованиями одного из международных стандартов на кабельные системы;

3. используются для диагностики медных кабельных систем;

4. предназначены для проверки кабелей на отсутствие физического разрыва;

5. совмещают функции нескольких устройств анализаторов протоколов

_____Устройства для сертификации кабельных систем;

_____Тестеры;

_____Сетевые мониторы;

_____Кабельные сканеры

_____Многофункциональные портативные устройства анализа и диагностики.

12) Что обозначает изображенная на рисунке схема взаимодействия?

1. Взаимодействие агента, менеджера и управляемого ресурса.

2. Одноранговые связи между менеджерами.

3. Иерархические связи между менеджерами.

4. Распределенная система управления на основе нескольких менеджеров и рабочих станций.

13) Прозрачность (transparency) означает...:

1. что сеть представляется пользователям не как множество отдельных компьютеров, связанных между собой сложной системой кабелей, а как единая традиционная вычислительная машина с системой разделения времени;

2. что сеть позволяет наращивать количество узлов и протяженность связей в очень широких пре- делах, при этом производительность сети не ухудшается;

3. возможность сравнительно легкого добавления отдельных элементов сети, наращивания длины сегментов сети и замены существующей аппаратуры более мощной.

14) Выберите основные этапы отслеживания состояния компьютерных сетей *(Выберите несколько вариантов ответа)*.

1. Сканирование;

2. Анализ;

3. Мониторинг;

4. Контроль;

5. Тестирование

15) Сопоставьте схемы ротации бекапов

1. это политика, по которой делается резервное копирование;

2. администратор делает копирование вручную. Обычно делается
полный бекап данных

3. подразумевается, что некий набор носителей используется циклически.

_____Одноразовое копирование.

_____Простая ротация

_____Ротация

16) Паразитный трафик - это...

1. трафик, возникающий в результате работы «паразитных» программ-вирусов;

2. исходящий трафик, отправка которого не было явно инициировано самим пользователем или

3. входящий трафик, получение которого не было явно инициировано самим пользователем илиустановленным на компьютере программным обеспечением

17) Данные о структуре, размещении, трансформации данных, которые используются любыми процессами хранилища...

1. оперативные источники данных;

2. метаданные;

3. средства доступа и анализа данных;

4. верных вариантов ответа нет;

5. средства переноса и трансформации данных.

18) Единственное предназначение такого сервера – хранить данные с других серверов. Обычно сам он никаких сервисов не выполняет

1. Файл-сервер;

2. Почтовый сервер;

3. Web-сервер;

4. Продакшн-сервер;

5. backup-сервер.

19) Основные компоненты хранилища данных *(Выберите несколько вариантов ответа)*.

1. оперативные источники данных;

2. метаданные;

3. средства доступа и анализа данных;

4. верных вариантов ответа нет;

5. средства переноса и трансформации данных.

20) Укажите два принципиальных подхода к организации управления сложными сетями *(Выберите несколько вариантов ответа).*

1. децентрализованное управление;

2. удаленное управление;

3. комплексное управление;

4. централизованное управление.

21) Как называется процесс, когда два или более продакшн серверов копируют друг на друга свои данные

1. сложное копирование данных;

2. выборочное копирование данных;

3. перекрестное копирование данных;

4. продакшн-копирование данных;

5. backup-копирование данных.

22) Расставьте соответствия

1. гетерогенной;

2. интегрируемой

3. одноранговая

4. клиент-серверная

_____Сеть, которая может включать в себя разнообразное программное и аппаратное обеспечение называется, работающее без проблем

_____Сеть, состоящая из разнотипных элементов, называется

_____Сеть, основанная на равноправии участников

_____Сеть, в которой задания или сетевая нагрузка распределены между поставщиками услуг, называемыми серверами, и заказчиками услуг, называемыми клиентами

23) Выберите правильное определение терминов

1. представляет собой систему, осуществляющую наблюдение, контроль и управление каждым элементом сети;

2. означает, что сеть может включать в себя разнообразное программное и аппаратное обеспечение, то есть в ней могут сосуществовать различные операционные системы

3. определяет количественные оценки вероятности того, что сеть будет передавать определенный поток данных между двумя узлами в соответствии с потребностями приложения или пользователя

_____Качество обслуживания

_____Управляемость

_____Совместимость

24) Это процесс сбора, отсеивания и предварительной обработки данных с целью представления результирующей информации пользователям для статистического анализа и аналитических отчетов

1. СУБД;

2. HDD;

3. хранилища данных;

4. raid-массив.

25) В сетях Ethernet наиболее распространенными являются следующие типы ошибок *(Выберите несколько вариантов ответа)*.

1. Длинный кадр;

2. Блики;

3. Ошибка выравнивания;

4. Ошибки контрольной последовательности;

5. Короткий кадр.

26) Для реализации хранилищ данных используют:

1. средства записи данных, средства удаления данных, средства хранения данных;

2. средства поиска данных, средства форматирования данных, средства

редактирования данных;

3. средства хранения данных, средства извлечения и просмотра данных, средства пополнения хранилищ данных.

27) Логические (информационные) аспекты работы ЛВС включают в себя……..*(Выберите несколько вариантов ответа).*

1. недопустимо использование несанкционированного ПО;

2. не допускается осуществление попыток несанкционированного доступа к ресурсам Сети;

3. не допускается использование общих ресурсов ЛВС;

4. пользователи не должны использовать ЛВС для передачи другим компьютерам или оборудованию сети бессмысленной или бесполезной информации;

5. не допускается передача большого объема информации по сети.

28) Процесс создания копии данных на носителе, предназначенном для восстановления данных…

1. Резервное копирование в режиме реального времени;

2. Дифференциальное резервирование;

3. Резервирование клонированием;

4. Инкрементное резервирование;

5. Резервирование в виде образа;

6. Полное резервирование.

29) Способ отслеживания событий и действий пользователей, отслеживание состояния сетевой инфраструктуры

1. аудит;

2. мониторинг;

3. анализ;

4. диагностика..

30) Как минимизировать паразитный трафик? (выберите несколько вариантов).

1. Установка антивирусных программ;

2. Отключение «лишних» служб Windows;

3. Использование межсетевого экрана (брандмауэры);

4. Верных вариантов ответа нет;

5. Установка критических обновлений для ОС Windows.

Ключи к тестам:

1-3	11-2,4,1,3,5	21-3
2-1	12-1	22-2,1,3,4
3-2,3,1	13-1	23-3,1,2
4-2	14-2,3,4	24-3
5-2	15-2,3,1	25-1,2,3,4,5
6-2,3,4,5	16-3	26-3
7-4	17-2	27-1,2,4
8-2	18-5	28-1
9-2,3,4	19-1,2,3,5	29-1
10-1,4,5	20-1,4	30-1,2,3,5

Итоговый тест МДК.03.02 «Безопасность компьютерных сетей»

(1 вариант)

Вариант 1

Количество вопросов – 30. Возможны несколько правильных ответов

1) Компьютерные вирусы, которые внедряются в программы и обычно активируются при их загрузке, называются …

1. макровирусами;

2. сетевыми;

3. загрузочными;

4. файловыми;

2) Какая угроза возникает в результате технологической неисправности за пределами информационной системы?

1. техническая;

2. внешняя;

3. технологическая;

4. информационная;

5. логическая.

3) К аспектам информационной безопасности относятся *(выберите несколько вариантов ответов).*

1. доступность;

2. дискретность;

3. конфиденциальность;

4. актуальность;

5. целостность.

4) Во время выполнения резервного копирования задается степень сжатия архивации. При этом степень сжатия при архивации определяется …

1. в зависимости от количества обрабатываемых файлов;

2. размером упакованного файла;

3. размером исходного файла;

4. отношением размера упакованного файла к размеру исходного.

5) Системный администратор обнаружил, что компьютер генерального директора компании заражен вирусами, скрывающими свое присутствие, подставляя вместо своего тела незараженные участки программного кода. Какой вирус обнаружил системный администратор?

1. сетевые черви;

2. вирусы-мутанты;

3. стелс-вирусы;

4. паразитические вирусы.

6) Пользователь установил на компьютер ПО, по его мнению, относящееся к антивирусным средствам. Проводящий профилактику ПК системный администратор заметил, что на компьютере не установлен антивирус. Какая программа, установлена на ПК пользователя?

1. Kaspersky Internet Security;

2. 37vast! Home Edition;

3. FineReader Home Edition;

4. Dr.Web Security Suite.

7) В организацию закупили физические средства защиты информации (см. рис). Это ....

(выберите один вариант ответа):

1. средства, которые реализуются в виде автономных устройств и систем;

2. устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по
стандартному интерфейсу;

3. средства, которые реализуются в виде электрических, электромеханических и электронных устройств;

4. это программы, предназначенные для выполнения функций, связанных с защитой информации.

8) Метод пароля и его модификация, метод вопрос-ответ, метод секретного алгоритма – это методы

1. паролизации;

2. идентификации;

3. аутентификации;

4. авторизации.

**9) В компьютерную сеть организации проник злоумышленник (хакер) и уничтожил основные данные отдела закупок. Какую последовательность действий должен предпринять системный администратор для дальнейшей защиты информации и
предотвращения убытков оптимальный бекап базы данных** *(укажите порядок*

следования действий)?

1. Восстановить данные отдела закупок из резервных копий;

2. Определить «место» проникновения злоумышленника;

3. Устранить уязвимость системы.

10) Системный администратор обнаружил, что в системе выполняются действия одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями. Это действие называется ....

1. подстава;

2. замена;

3. обман;

4. маскарад;

5. аналогия.

11) Виды технической разведки (по месту размещения аппаратуры) *(Выберите несколько вариантов ответа)*

1. космическая;

2. магнитометрическая;

3. воздушная;

4. наземная;

5. фотографическая;

6. морская;

7. оптическая.

12) Под изоляцией и разделением (требование к обеспечению ИБ) понимают:

1. разделение объектов защиты на группы так, чтобы нарушение защиты одной группы не влияло на безопасность других групп;

2. разделение информации на группы так, чтобы нарушение одной группы информации не влияло на безопасность других групп информации (документов);

13) Что такое аутентификация?

1. Определение файлов, из которых удалена служебная информация;

2. Нахождение файлов, которые изменены в информационной системе несанкционированно;

3. Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно
осуществляется перед разрешением доступа);

4. Определение файлов, из которых удалена служебная информация;

5. Проверка количества переданной и принятой информации.

14) Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности, называется

1. организацией безопасности;

2. политикой безопасности;

3. политикой информации;

4. защитой информации;

15) Кодирование информации –

1. метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом;

2. представление информации в виде условных сигналов с целью автоматизации ее хранения, об работки, передачи и т.д.

16) В классификации компьютерных вирусов по среде обитания условно выделяют …

1. простейшие, черви, стелс-вирусы, полиморфные, троянские;

2. неопасные, опасные, очень опасные;

3. резидентные, нерезидентные;

4. файловые, загрузочные, сетевые;

17) Доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации, называется

1. утечкой;

2. несанкционированным доступом;

3. разглашением;

4. нарушением конфиденциальности;

18) Системный администратор, работающий по аутсосрсингу, обнаружил, что в обслуживаемой компании защита не разнесена по уровням. Он выделил эти уровни и сообщил администрации об ошибках. Какие основные уровни обеспечения защиты информации указал системный администратор? *(Выберите несколько вариантов ответа).*

1. процедурный;

2. программно-технический;

3. вероятностный:

4. административный;

5. физический;

6. распределительный;

7. законодательный.

19) Вы, как системный администратор обнаружили, что на сервер компании осуществлен доступ к объекту в нарушение установленных в системе правил разграничения доступа. Как называется такой доступ?

1. преступный;

2. несанкционированный;

3. запрещенный;

4. конфиденциальный;

5. криминальный;

20) Компьютерные сети, объединяющие территориально рассредоточенные компьютеры, возможно находящиеся в различных странах, называются …

1. локальными;

2. глобальными;

3. региональными;

4. персональными;

21) На компьютере бухгалтера компании, системный администратор

обнаружил вирус, скрывающий себя за счет шифрования основного тела вируса и существенной модификации от копии к копии модуля-расшифровщика, Данный вирус называется …

1. полиморфным;
2. троянским;
3. вирусом-спутником;
4. макровирусом.

22) Что является основой для формирования государственной политики в сфере информации?

1. закон;
2. доктрина;
3. конституция;
4. постановление;
5. указ;
6. нормативы.

23) Установите соответствие

1. наука о скрытой передаче информации путем сохранения в тайне самого факта передачи;
2. наука, скрывающая содержимое секретного сообщения;

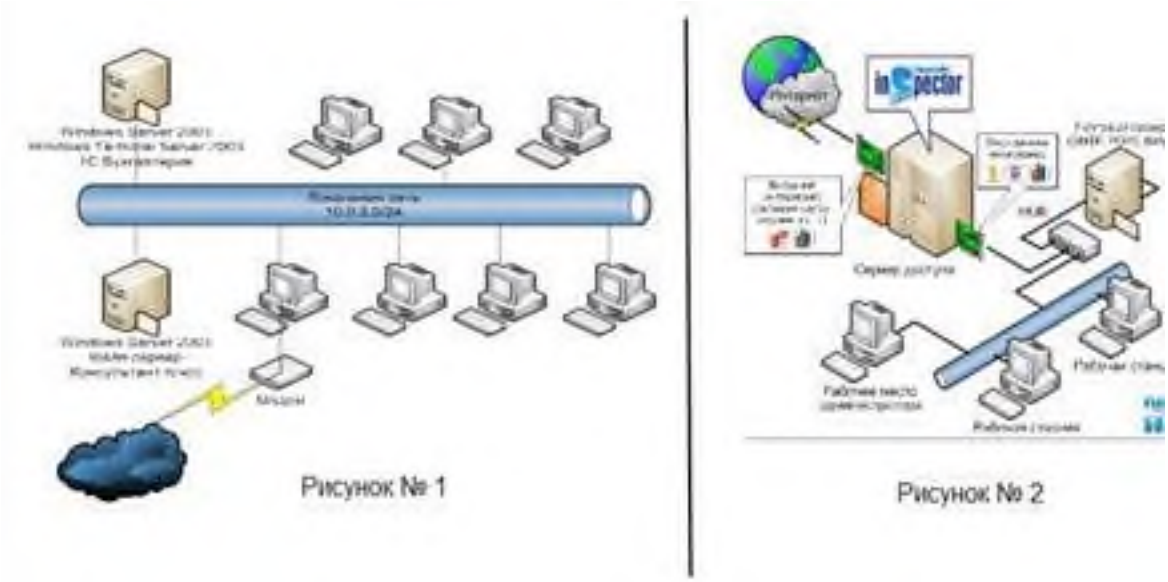
_____криптография;

_____стеганография.

24) Нежелательная цепочка носителей информации, один или несколько из которых являются правонарушителем или его специальной аппаратурой называется

1. каналом утечки информации;
2. каналом разглашения информации;
3. каналом нарушения конфиденциальности;
4. каналом нарушения секретности;

25) На рисунке изображены две схемы локальных сетей с выходом в Интернет. Какая из сетей является наиболее защищенной?



1. Рисунок № 2;

2. Рисунок № 1;

26) В организацию закупили технические средства защиты информации (см. рис.). Это…

1. это программы, предназначенные для выполнения функций, связанных с защитой информации;

2. устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по
стандартному интерфейсу;

3. средства, которые реализуются в виде электрических, электромеханических

и электронных устройств;

4. Верных вариантов ответа нет;

5. средства, которые реализуются в виде автономных устройств и систем.

27) В организации, в которой вы работаете, есть человек- криптограф. Что входит в его задачу?

1. взломать систему защиты;

2. обеспечить конфиденциальность и аутентификацию передаваемых сообщений.

28) К видам защиты информации относятся: *(выберите несколько вариантов)*.

1. юридические;

2. административно-организационные;

3. правовые и законодательные;

4. морально-этические;

29) Что такое целостность информации?

1. Свойство информации, заключающееся в возможности изменения только единственным пользователем;

2. Свойство информации, заключающееся в возможности ее изменения любым субъектом;

3. Свойство информации, заключающееся в ее существовании в виде единого набора файлов;

4. Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменнompo отношению к некоторому фиксированному ее состоянию).

30) Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации называется

1. кодируемой;

2. защищаемой;

3. шифруемой;

4. недостоверной;

5. собственной.

Ключи к тестам:

1-4	11-1,3,4,6	21-1
2-1	12-1	22-2
3-1,3,5	13-3	23-2,1
4-4	14-2	24-1
5-3	15-2	25-1
6-3	16-4	26-3
7-1	17-2	27-2
8-3	18-1,2,4,7	28-2,3,4
9-3	19-2	29-4
10-4	20-2	30-2

Критерии оценок:

Оценка «5» - ошибок нет (100% правильных ответов)

«4» - 1-4 ошибки (80-90% правильных ответов)

«3» - 5-9 ошибок (70% правильных ответов)

«2» - 10 ошибок (60% правильных ответов)

Практические задания для оценки степени усвоения дисциплины

(текущий контроль)

МДК.03.01 Эксплуатация объектов сетевой инфраструктуры»

Раздел 01. Эксплуатация объектов сетевой инфраструктуры

Тема 1.1. Эксплуатация технических средств сетевой инфраструктуры

50 часов.

Правила выполнения практических работ

При подготовке к выполнению практической работы обучающимся следует:

- изучить теоретические вопросы, изложенные в методических указаниях;

-ознакомиться с техникой безопасности при работе в кабинете №2 «Информатики и информационных технологий»;

-получить у преподавателя задание на выполнение практической работы, которое выдается после проверки теоретической подготовки обучающегося.

-внимательно слушать инструктаж на деловых играх и тренингах

-активно участвовать в обсуждениях, работать в группах

Результаты выполнения практической работы проверяются преподавателем.

Безопасность труда

Инструкция по охране труда для системного администратора

1. Общие требования охраны труда

1.1. К самостоятельной работе системным администратором допускаются лица, прошедшие при поступлении на работу вводный инструктаж по охране труда, инструктаж по электробезопасности на рабочем месте (с присвоением соответствующей группы по электробезопасности), обучение и проверку знаний по охране труда.

1.2. Системный администратор должен:

знать действие на человека опасных и вредных производственных факторов, возникающих во время работы;

соблюдать требования производственной санитарии, электробезопасности и пожарной безопасности;

знать место расположения огнетушителей и аптечек;

знать правила внутреннего трудового распорядка, установленные на предприятии;

знать назначение средств индивидуальной защиты (СИЗ);

уметь оказывать первую помощь пострадавшим, пользоваться средствами пожаротушения.

1.3. Во время работы на системного администратора могут воздействовать следующие опасные факторы:

повышенный уровень электромагнитных излучений;

повышенный уровень ионизирующих излучений (у мониторов на электронно-лучевых трубках);

повышенный уровень статического электричества;

повышенная напряженность электростатического поля; – повышенная или пониженная ионизация воздуха;

повышенная яркость света;

прямая и отраженная блесткость;

повышенное напряжение в электрической цепи, замыкание которой может произойти через тело человека;

статические перегрузки костно-мышечного аппарата и динамические локальные перегрузки мышц кистей рук;

повышенный уровень загазованности и запыленности воздуха (в первую очередь по углекислому газу и аммиаку, которые образуются при выдыхании), особенно в плохо вентилируемых помещениях;

перенапряжение органов зрения;

повышенный уровень шума от работающих вентилятора охлаждения ПК и принтера, от неотрегулированных источников люминесцентного освещения и др.;

умственное перенапряжение, эмоциональные перегрузки и монотонность труда.

1.4. Нормы и сроки выдачи СИЗ определяются согласно Типовым отраслевым нормам бесплатной выдачи рабочим и служащим специальной одежды, специальной обуви и других СИЗ.

1.5. Площадь на одно рабочее место с персональным компьютеров на базе электронно-лучевой трубки, должна составлять не менее 6 м, на базе плоских дискретных экранов (жидкокристаллические, плазменные) – не менее 4,5 м.

1.6. Оснащение светопроницаемых конструкций и оконных проёмов должно позволять регулировать параметры световой среды в помещении.

2. Требования охраны труда перед началом работы

2.1. Перед началом работы системный администратор обязан:

осмотреть и привести в порядок рабочее место;

отрегулировать освещенность на рабочем месте, убедиться в достаточности освещенности, отсутствии отражений на экране, отсутствии встречного светового потока;

проверить правильность подключения оборудования в электросеть;

проверить правильность установки стола, стула, подставки для ног, положения оборудования, угла наклона экрана, положение клавиатуры и, при необходимости, произвести регулировку рабочего стола и кресла, а также расположение элементов компьютера в соответствии с требованиями эргономики и в целях исключения неудобных поз и длительных напряжений тела.

2.2. При включении компьютера соблюдать правила электробезопасности.

2.3. Системному администратору запрещается приступать к работе при:

отсутствии информации о соответствии параметров данного оборудования требованиям санитарных норм;

обнаружении неисправности оборудования;

отсутствии защитного заземления электрооборудования;

отсутствии огнетушителя и аптечки первой помощи.

3. Требования охраны труда во время работы

3.1. Системный администратор во время работы обязан:

выполнять только ту работу, которая ему была поручена, и по которой он был проинструктирован;

в течение всего рабочего дня содержать в порядке и чистоте рабочее место;

соблюдать санитарные нормы и режимы работы и отдыха;

соблюдать правила эксплуатации вычислительной техники в соответствии с инструкциями по эксплуатации;

соблюдать установленные режимом рабочего времени регламентированные перерывы в работе и выполнять упражнения для глаз, шеи, рук, туловища, ног.

3.2. Системному администратору во время работы запрещается:

прикасаться к задней панели системного блока (процессора) при включенном питании;

переключать разъемы интерфейсных кабелей периферийных устройств при включенном питании;

загромождать верхние панели устройств бумагами и посторонними предметами;

допускать захламленность рабочего места;

производить отключение питания во время выполнения активной задачи;

допускать попадание влаги на поверхность системного блока (процессора), монитора, рабочую поверхность клавиатуры, дисководов, принтеров и др. устройств;

включать сильноохлажденное (например, принесенное с улицы в зимнее время) оборудование;

производить самостоятельно вскрытие и ремонт оборудования (если это не входит в рабочие обязанности).

4. Требования охраны труда в аварийных ситуациях

4.1. Системный администратор обязан:

во всех случаях обнаружения обрыва проводов питания, неисправности заземления и других повреждений электрооборудования, появления запаха гари немедленно отключить питание и сообщить об аварийной ситуации своему непосредственному руководителю и дежурному электрику;

при обнаружении человека, попавшего под напряжение, немедленно освободить его от действия тока путем отключения электропитания и до прибытия врача оказать потерпевшему первую медицинскую помощь;

при обнаружении пострадавшего немедленно вызвать медицинских работников, до их прибытия оказать пострадавшему первую помощь и, по возможности, сохранить текущую обстановку на месте происшествия для возможности дальнейшего расследования несчастного случая;

при любых случаях сбоя в работе технического оборудования или программного обеспечения немедленно вызвать представителя инженерно-технической службы эксплуатации вычислительной техники;

в случае появления недомогания (рези в глазах, резком ухудшении видимости, невозможности сфокусировать взгляд или навести его на резкость, появлении

боли в пальцах и кистях рук, усилении сердцебиения и пр.) немедленно покинуть рабочее место, сообщить о происшедшем своему непосредственному руководителю и обратиться к врачу;

при возгорании оборудования отключить питание и принять меры к тушению очага пожара при помощи огнетушителя, если это не угрожает собственной жизни и здоровью, вызвать пожарную команду и сообщить о происшествии своему непосредственному руководителю.

5. Требования охраны труда по окончании работы

5.1. По окончании работ системный администратор обязан соблюдать следующую последовательность выключения техники:

произвести закрытие всех активных задач;

выключить питание системного блока (процессора);

выключить питание всех периферийных устройств;

привести в порядок свое рабочее место;

снять и убрать в предназначенное для этого место спецодежду, спецобувь и СИЗ.

5.2. По окончании работ системный администратор обязан осмотреть и привести в порядок рабочее место, вымыть с мылом руки и лицо.

Практическая работа №1.

Тема: «Оконцовка кабеля витая пара».

Цель работы. 1. Изучение обжима коннекторов 8P8C методом прямого соединения;

2. Изучение обжим коннекторов 8P8C методом кроссового соединения;

3. Развитие и закрепление интереса обучаемых к преподаваемому предмету.

Оборудование, инструмент и наглядные пособия. коннекторы 8P8C; кабель витая пара; кримпер; кабель-тестер.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Ход работы:

1. Изучить методические указания к работе;

2. Осуществить обжим коннектора прямым методом;

3. Осуществить обжим коннектора кроссовым методом;

4. Проверить правильность соединения с помощью кабель-тестера.

Содержание отчета

1. Название работы.
2. Цель работы.
3. Выполнение заданий.
4. Проверка. Ответ.

Контрольные вопросы и задания.

1. Активное сетевое оборудование
2. Пассивное сетевое оборудование.
3. Перечислите виды сред передачи данных.
4. Как с помощью стандартных сетевых утилит проверить работоспособность сетевого адаптера.
5. Почему концентратор и повторитель относят к пассивному сетевому оборудованию?

Практическая работа №2.

Тема: «Заделка кабеля витая пара в розетку».

Цель работы. Изучение методов соединения компьютеров (рабочих станций) в локальных сетях. Ознакомление с понятием структурированной кабельной системы и ее компонентами. Получение практических навыков создания горизонтальной подсистемы, включающей розетку с гнездом RJ-45. Получение практических навыков тестирования кабельных систем.

Оборудование, инструмент и наглядные пособия. 1. Кабель горизонтальной системы, заделанный с одного конца. 2. Патч-панель RJ-45 (смонтирована в настенный 19" навесной монтажный шкаф). 3. Гнездо (jack) типа UTP cat 5 или 5e. 4. Два тестовых патч-корда типа RJ-45. 5. Стриппер для витой пары (специальный инструмент для разделки кабеля). 6. Ккримп-тул

(crimp-tool) – специальный инструмент для заделки кабеля витая пара в разъемы RJ-45. 7. Тестер для проверки наличия контактов заделанного кабеля.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Ход работы.

Задача 1. Заделка проводников в розетку.

Отчет о работе.

Предъявите преподавателю протестированную розетку.

Контрольные вопросы и задания.

1. Каким образом рабочая станция подсоединяется к горизонтальной подсистеме здания?

2. Каково назначение патч-панели RJ-45 и ее конструкция?

3. Что такое раскладка кабеля 568 А и 568 В?

Практическая работа №3.

Тема: «Кроссирование и монтаж патч-панели в коммутационный шкаф, на стену».

ЦЕЛЬ РАБОТЫ: «Изучить кроссирование и монтаж патч-панели в коммутационный шкаф, на стену».

Оборудование, инструмент и наглядные пособия: патч-панели, коммутационный шкаф.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Ход работы.

Задание 1. Сделайте кроссировку кабеля.

Задание 2. Устройство патч-панели. Монтаж патч-панели коммутационный шкаф, на стену.

Контрольные вопросы.

1. Опишите процесс кроссирования патч-панели.

2. Опишите процесс монтажа патч-панели в коммутационный шкаф, на стену.

3. Опишите процесс кроссирования кабеля?

4. Как устроена патч-панель?

5. Выполните обжим кабеля UTP.

Практическая работа №4

Тема: «Тестирование кабеля».

Цель работы. Изучить подключение и тестирование сетевого оборудования на основе коаксиального кабеля с помощью устройства LANcat V.

Оборудование, инструмент и наглядные пособия. LANcat V - ручное устройство для тестирования кабелей.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Ход работы.

Задание. 1 Сделайте общее описание устройства LANcat V.

Задание 2. Подключение коаксиального модуля к LANcat V.

Задание 3. Калибровка NVP (Nominal Velocity of Propagation).

Задание 4. Проверка сопротивлений терминаторов.

Задание 5. Проверка кабелей на импеданс.

Задание 6. Нахождение ошибок.

Задание 7. Соединение кабелей и подключение к сети.

Задание 8. Проверка уровня помех (шумов).

Задание 9. Поиск неисправностей в сети аппаратными средствами.

Задание 10. Тестирование и диагностика сети.

Задание 11. Основные правила прокладки кабеля.

Правила создания отчета

1. Составить спецификацию типа сети. Выписать диапазоны допустимых значений для импеданса, сопротивления терминаторов, уровня помех.

2. Заполнить таблицы по всем протестированным кабелям.

N кабеля	Тип кабеля	Длина	Импеданс	Ошибки	Причины

1	Arcnet	10.5	100	Short	Плохо обжат коннектор

3. Записать правила прокладки и тестирования сети 10Base2.

4. Записать последовательность поиска и устранения ошибок.

Контрольные вопросы и задания.

1. Какие типы коаксиальных сетей можно тестировать с помощью устройства LANcat V?

2. Что такое импеданс? Какие значения импеданса и для каких сетей используются?

3. Можно ли соединять кабели различного типа? Дать пояснения.

4. Что такое терминатор? Зачем он нужен?

5. Какие виды ошибок может обнаружить LANcat V?

6. Что такое NVP? От чего оно зависит?

7. Что такое предельный порог шумов?

8. Что измеряет тест NOISE?

9. Что измеряет тест LENGTH?

10. Как соединить между собой два компьютера?

Практическая работа №5.

Тема: «Поддержка пользователей сети».

Цель работы. Познакомиться с основными компонентами сетевого оборудования, их назначением и характеристиками. Ознакомление с аппаратным обеспечение локальной компьютерной сети; Получение навыков работы в локальной компьютерной сети; Научиться устанавливать права доступа к сетевым ресурсам, работать с информацией, расположенной на компьютерах локальной сети.

Оборудование, инструмент и наглядные пособия. ПК, ОС Windows.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. Получить навыки по подключению отдельного ПК к ЛВС.

Задание 2. Изучить простейшие приемы работы в сетевой среде и команды ОС.

Задание 3. Развить компьютерную грамотность.

Задание 4. Изучить состав и назначение основных компонентов сетевого оборудования.

Задание 5. Определить состав и основные характеристики оборудования и системного программного обеспечения, установленного в Вашем компьютере.

Задание 6. Определить сетевое имя компьютера и рабочую группу, в которую он входит.

Задание 7. Определить состав установленных в компьютере сетевых адаптеров и познакомиться с их основными свойствами.

Задание 8. Проверить текущее состояние сетевых подключений Вашего компьютера.

Задание 9. Подготовить отчет, ответить на контрольные вопросы.

Контрольные вопросы и задания.

1. Что такое неэкранированная витая пара?
2. На какие два больших класса подразделяют все сетевое оборудование, и чем они отличаются друг от друга.
4. Укажите основные отличия в работе концентраторов и коммутаторов.
5. Какие существуют группы кабелей?
6. Что такое структурированная кабельная система, и каково ее назначение.
7. Какие элементы относятся к классу пассивного сетевого оборудования.
8. Какие основные ограничения следует учитывать при прокладке кабелей ЛВС.

9. Что такое компьютерная сети и её назначение?

10. Классификация сетей по территориальному признаку.

11. Основные понятия локальной компьютерной сети.

12. Что такое IP адрес и для чего он предназначен? Как просмотреть свой IP адрес?

13. Как назначить папке общий доступ? Как отключить общий доступ?

14. Что такое сетевой диск и как его подключить. В чём отличие сетевого диска от папки с общим доступом?

Практическая работа №6

Тема: «Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы)».

Цель работы. Изучить правила технической эксплуатации ПК, серверов, периферийного и активного сетевого оборудования.

Оборудование, инструмент и наглядные пособия. ПК, сервер, принтеры разных типов, коммуникационное оборудование.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. Изучить правила технической эксплуатации ПК

Задание 2. Изучить правила технической эксплуатации серверов

Задание 3. Изучить правила технической эксплуатации принтеров

Задание 4. Изучить правила технической эксплуатации коммутационного оборудования

Задание 5. Научиться определять по внешнему виду типы разъемов, подключаемое к ним оборудование;

Задание 6. Знать основные устройства персонального компьютера, их назначение и основные характеристики;

Задание 7. Научиться определять компоненты системного блока по внешнему виду, уяснить порядок и способы их соединения.

Задание 8. Изучите способ подключения мыши.

Задание 9. Заполните таблицу:

Разъем	Тип разъема	Количество контактов	Примечания

Задание 10. Определить наличие основных устройств персонального

компьютера.

Задание 11. Установите местоположение блока питания, выясните мощность блока питания (указана на ярлыке).

Задание 12. Установите местоположение материнской платы.

Задание 13. Установите характер подключения материнской платы к блоку питания.

Задание 14. Установите местоположение жесткого диска. Установите местоположение его разъема питания.

Задание 15. Установите местоположения привода CD-ROM (DVD-ROM).

Задание 16.Установите местоположение платы видеоадаптера. Определите тип интерфейса платы видеоадаптера.

Задание 17.При наличии прочих дополнительных устройств выявите их назначение, опишите характерные особенности данных устройств (типы разъемов, тип интерфейса и др.).

Задание 18. Заполните таблицу:

Устройство	**Характерные особенности**	**Куда и при помощи чего подключается**

Задание 19. Ответить на контрольные вопросы

Задание 20. Оформить отчет

Отчет о работе.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Контрольные вопросы и задания.

1. Как часто нужно проводить чистку системного блока?
2. Как правильно нужно присоединять кабель к порту ПК? Почему?
3. Функции ИБП.
4. Зачем нужно знать, где находится аварийный рубильник выключения питания?
5. Правила подключения принтеров к сети.
6. Особенности эксплуатации струйных принтеров.
7. Особенности эксплуатации лазерных принтеров.

8. Какой тип кабеля должен использоваться для горизонтальной подсистемы?

9. Какие меры нужно принять для повышения надежности ЛВС?

10. Какое коммутационное оборудование вы знаете?

11. Какие правила технической эксплуатации коммутационного оборудования?

12. Архитектура вычислительных систем.

13. Состав системного блока.

14. Назначение, основные характеристики, интерфейс устройств персонального компьютера (по каждому устройству), входящих в состав системного блока.

15. Устройство жесткого диска.

16. Базовая аппаратная конфигурация.

17. Основные характеристики монитора.

18. Характеристики (тип разъема, количество контактов, скорость передачи данных) разъемов: видеоадаптера; последовательных портов; параллельного порта; шины USB; сетевой карты; питания системного блока; питания монитора.

19. Типы периферийных устройств.

Практическая работа №7

Тема: «Выполнение действий по устранению неисправностей».

Цель работы. Научиться выявлять и устранения возможных неисправностей сетевого оборудования. Освоить технологию определения неисправностей технических средств.

Оборудование, инструмент и наглядные пособия. ПК, сетевые анализаторы; кабельные сканеры.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Ход работы.

Задание 1. Основные правила прокладки кабеля.

Задание 2. Протестируйте и продиагностируйте сети.

Задание 3. Поиск неисправностей в сети аппаратными средствами.

Задание 4. Перечислите приборы для сертификации кабельных систем.

Задание 5. Поиск неисправностей в сети. Утилиты TCP/IP.

Задание 6. Перечислите наиболее вероятные причины проблем в работе сети, с которыми столкнулись сотрудники компании.

_____

_____

_____

_____

Задание 7. Опишите ниже проблемы, обнаруженные вами в ходе поиска и устранения неполадок, а также укажите, какие изменения вы внесли в конфигурации сетевых устройств, чтобы устранить эти проблемы.

_____

_____

_____

_____

Задание 8. В ходе этой лабораторной работы вы выполняли поиск и устранение неполадок на всех устройствах, прежде чем вносить какие-либо изменения. Можно ли найти и устранить неполадки другим способом**?**

_____

_____

_____

Отчет о работе.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Контрольные вопросы и задания.

1. Ошибки канального уровня
2. Ошибки сетевого уровня
3. Ошибки физического уровня
4. Ошибки администрирования

5. Укажите аппаратные средства диагностики и тестирования сети. Опишите принцип работы каждого из них.

6. Опишите работу утилит ping и ipconfig.

7. Назначение и компоненты системной платы.

8. Что такое северный мост? Его назначение.

9. Что такое южный мост? Его назначение.

10. Что такое форм-фактор материнской платы?

11. Назначение центрального процессора.

12. Что такое многоядерный процессор?

13. Что такое кэширование?

14. Оперативное запоминающее устройство. Его назначение.

15. Что такое энергозависимые и энергонезависимые запоминающие устройства?

16. Универсальная последовательная шина USB.

17. Шина ввода-вывода PCI и PCI-Express.

18. Шина AGP.

19. Видеокарта. Назначение и устройство.

20. Сетевой адаптер. Назначение, типы, параметры и функции. Назначение и типы оптических приводов.

21. Жёсткий диск. Назначение и устройство.

Практическая работа №8

Тема: «Выполнение мониторинга и анализа работы локальной сети с помощью программных средств».

Цель работы: «Изучить мониторинг и анализ работы локальной сети с помощью программных средств».

Оборудование, инструмент и наглядные пособия: Windows 7,10,11, программные средства.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. Зайти в интерпретатор командной строки. С помощью утилиты ***ipconfig*** определить и записать в отчёт следующую информацию:

– Название сетевого подключения.

– Тип используемого адаптера.

– MAC-адрес адаптера.

– IP-адрес сетевого подключения.

– Сетевую маску.

– Основной шлюз.

– IP-адрес DNS сервера.

– IP-адрес DHCP сервера.

Задание 2. Работа с анализатором протоколов tcpdump

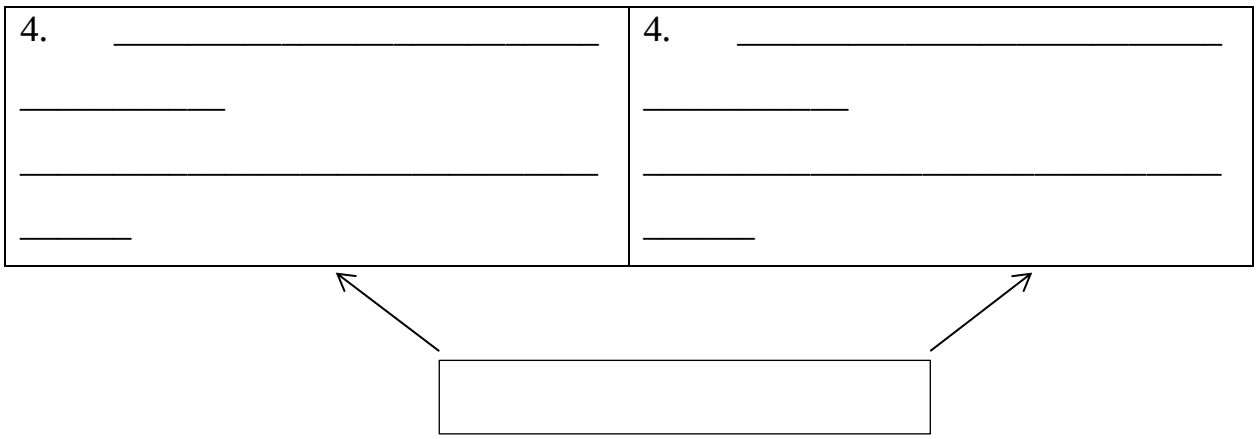
Задание 3. Работа с анализатором протоколов wireshark

Индивидуальная карточка

1. Назовите виды средств мониторинга сети?

Виды средств мониторинга сети

1. _____ _____ _____ _____ 2. _____ _____ _____ _____ 3. _____ _____ _____ _____	1. _____ _____ _____ _____ 2. _____ _____ _____ _____ 3. _____ _____ _____ _____



2. Для чего предназначены следующие утилиты:

Ping -

_____

_____

Traceroute -

_____

_____

Arp -

_____

_____

3. Назовите и охарактеризуйте наиболее часто используемые ключи команд ipconfig, nslookup, arp.

ipconfig –

_____

nslookup –

_____

arp

_____

Отчет о работе.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Контрольные вопросы и задания.

1) Для чего предназначена утилита ipconfig?

(После ответа одному студенту предлагается показать использование команды).

2) Назовите причину не получения Ip-адреса от службы DHCP.

3) Назовите и охарактеризуйте список наиболее часто употребляемых ключей при вызове утилиты ping.

4) Назовите причины отсутствия эхо-ответа в результате выполнения команды ping.

5) Назовите и охарактеризуйте список наиболее часто употребляемых ключей при вызове утилиты tracert?

(После ответа одному студенту предлагается показать возможности использование ключей в команде tracert).

6) Найдите ошибки в командах.

(На слайде демонстрируются команды, в которых требуется найти ошибку. После нахождения ошибки студенту предлагается её исправить, введя правильно команду).

Практическая работа №9.

Тема: «Оформление технической документации, правила оформления документов».

Цель работы: изучить оформление технической документации, правила оформления документов».

Оборудование и наглядные пособия: техническая документация.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1.Используя теоретический материал изучить особенности оформления технической документации.

Задание 2. Написать основные виды и определение технической документации.

Задание 3. Раскрыть понятие и виды конструкторской документации.

Задание 4. Раскрыть понятие и виды проектно-сметной документации.

Задание 5. Раскрыть понятие и виды технологической документации.

Задание 6. Раскрыть понятие и виды научно-исследовательской документации.

Задание 7. Подготовить отчет, ответить на контрольные вопросы.

Вопросы для контроля.

1. Для чего необходимо руководство пользователя?
2. Чем руководство оператора отличается от руководства пользователя?
3. Что включает в себя руководство программиста?
4. Каким цветом оформляют текстовую документацию?
5. Номеруют ли страницу титульного листа?
6. Раскройте особенности изготовления и оформления технической документации
7. Как оформить лист «содержание»?
8. Указывается ли на листе «содержание» название документа?
9. Перечислите основные текстовые редакторы
10. Особенности технической документации по изобретательству и стандартизации
11. Можно ли интегрировать разнообразные документы в текстовый формат?

Практическая работа №10

Тема: «Протокол управления SNMP».

Цель работы: Ознакомление с протоколом SNMP и программными утилитами (net-snmp) для работы с ним.

Оборудование и наглядные пособия: персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. Создание сети и настройка базовых параметров устройств.

Задание 2. Настройка диспетчера и агентов SNMP.

Задание 3. Преобразование кодов OID с использованием Cisco SNMP Object Navigator.

Контрольные вопросы.

1. На каком уровне модели OSI функционирует протокол SNMP?
2. Что представляет собой SNMP?
3. Какие функции и назначение SNMP?
4. Какие протокольные уровни различаются в модели передачи данных TCP/IP?
5. Какие примитивы реализуются в SNMP?
6. Что входит в структуру информационных баз управления MIB компьютерных сетей?
7. Какие разновидности протоколов SNMP применяются для управления в сетях телекоммуникаций?
8. Какие принципиальные отличия имеют место между SNMPV1 и SNMPV3?
9. Перечислите несколько потенциальных преимуществ наблюдения за сетью протокола SNMP
10. Почему при работе SNMPv2 предпочтительно использовать исключительно доступ с правами для чтения?

Практическая работа №11

Тема: «Основные характеристики протокола SNMP».

Цель работы: Изучите теоретическую информацию о протоколе SNMP. На практике приведите пример использования этого протокола там или иным спомобом.

Оборудование и наглядные пособия: персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. База данных управляемых элементов.

Задание 2. Язык описания информации.

Задание 3. Безопасность и администрирование.

Задание 4. Протокол управления SNMP.

Контрольные вопросы.

1. Какие функции выполняет протокол SNMP?
2. Какие программы используют протокол SNMP и для чего?

Практическая работа №12

Тема: «Набор услуг (PDU) протокола SNMP».

Цель работы Изучите теоретическую информацию описывающую работу протокола SNMP и ответьте на контрольные вопросы. Выделите основные элементы SNMP и вынесете их в табличный вид в отчете о работе.

Оборудование и наглядные пособия: персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. Опишите информацию SNMP PDU (или сообщения SNMP протокола).

Задание 2. Опишите специализированный тип Trap.

Задание 3. Опишите логика работы протокола SNMP.

Контрольные вопросы

1. Что такое PDU?
2. Опишите архитектуру SNMP протокола.
3. Без каких элементов не будет работать SNMP протокол?

Практическая работа №13.

Тема: «Формат сообщений SNMP».

Цель работы: Изучите теоретическую информацию и опишите формат сообщений SNMP в отчете о работе.

Оборудование и наглядные пособия: персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Ход работы.

Задание 1. Опишите теоретическую информацию и формат сообщений SNMP в отчете о работе.

Контрольные вопросы.

1. Какие примитивы реализуются в SNMP?
2. Что входит в структуру информационных баз управления MIB компьютерных сетей?
3. Какие разновидности протоколов SNMP применяются для управления в сетях телекоммуникаций?

Практическая работа №14.

Тема: «Задачи управления: анализ производительности сети».

Цель работы: Изучить задачи управления: анализ производительности сети.

Оборудование и наглядные пособия: персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Ход работы.

Задание 1. Опишите задачи управления: анализ производительности сети и для чего она предназначена.

Контрольные вопросы

1) Как осуществляется анализ сети?
2) Какие возможности управления предоставляет ПО?

Практическая работа №15

Тема: «Задачи управления: анализ надежности сети».

Цель работы: Изучить работу программы анализа безопасности компьютерной сети.

Оборудование и наглядные пособия: персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. Задачи управления: проанализировать надежности сети.

Задание 2. Плусы и минусы задачи управления надежности сети.

Контрольные вопросы

1) Как организуется анализ параметров безопасности сети?
2) Какие параметры безопасности учитываются в процессе анализа?

Практическая работа№16

Тема: «Управление безопасностью в сети».

Цель: Изучить теоретический материал, выполнить задание и ответить на контрольные вопросы.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. Устранение возникающих неисправностей.

Задание 2. Управление производительностью сети.

Задание 3. Охарактеризовать производительности сети.

Задание 4. Инструменты отслеживания характеристик производительности сети.

Задание 5. Общесистемное управление.

Задание 6. Управление безопасностью сети.

Задание 7. Разработка и внедрение политики защиты компьютерной сети.

Задание 8. Разработка и реализация политики защиты.

Задание 9. Реализация политики физической защиты.

Задание 10. Управление учетными записями.

Задание 11. Управление учетными записями пользователей.

Контрольные вопросы

1) Что такое общесистемное управление?
2) Что такое управление безопасностью сети?
3) Что такое схемы сетевого наименования?
4) Что такое учетная запись пользователя в серверной операционной системе?
5) Как осуществляется управление учетными записями?
6) Какие дополнительные средства защиты чаще всего применяются?
7) Как выполняется выяснение потребностей компании?

Практическая работа№17

Тема: «Учет трафика в сети».

Цель: Изучение сетевого трафика, генерируемого сетевым устройством в сетях передачи данных при работе с различными сетевыми сервисами; анализ служебных заголовок часто используемых сетевых протоколов.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. Запустить анализатор трафика Wireshark и проанализирова трафик.

Задание 2. Настроить фильтр на широковещательный трафик.

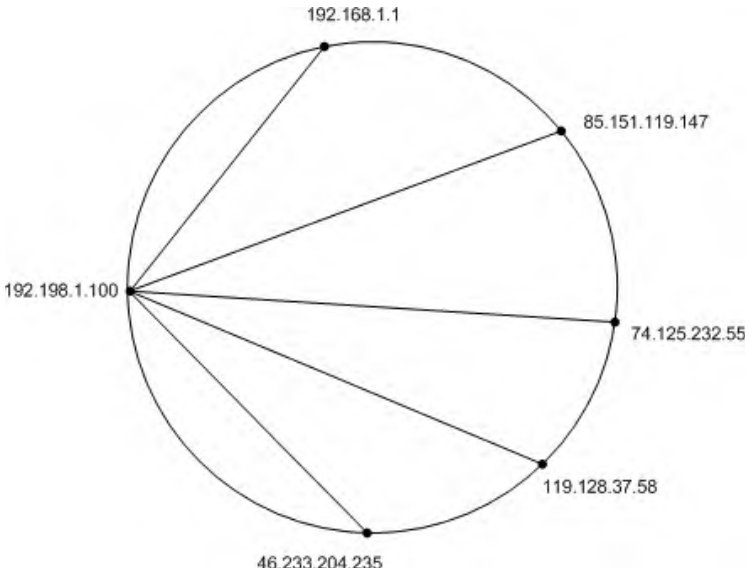
Задание 3. Разобрать пакет ARP: запрос и ответ. Снять скриншоты экранов с таблицами анализа протокола ARP.

Задание 4. Убрать настройку фильтров. Запустить браузер, набрать URL

какого- либо веб-ресурса (по желанию студента или заданию преподавателя). Отследить и разобрать пакеты DNS (запрос и ответ).

Задание 5. Разобрать пакеты http двух типов: запрос (GET) и ответ сервера. Снять скриншоты экранов: таблицы анализа, график интенсивности трафика HTTP в общем трафике, диаграмму соединений.

Задание 6. На основании данных об IP-адресах в полученном трэйсе и инструмента GraphAnalysis, построить карту сети (см. рис. 1), указав с помощью соединительных линий логические связи (т.е. наличие соединений)



между хостами.

Рис. 1 – Пример карты сети

К защите:

1. Знать принципы формирования пакетов в локальных сетях (технологии IP и Ethernet).
2. Иметь представление о функциях и процессе формирования пакетов протоколов ARP и HTTP, запросов/ответов DNS, понимать особенности широковещательного трафика.
3. Представить отчет, содержащий скриншоты для всех исследуемых протоколов: таблицы с анализом трафика, графики, диаграммы.

Контрольные вопросы

1. Сколько каналов у протокола ARP и за что отвечают они?
2. К какому сетевому уровню относится протокол ICMP и за что он отвечает?

Ответы на контрольные вопросы.

1. Протокол ARP относится к 2 – канальному уровню модели OSI т.к. этот уровень отвечает за физическую адресацию, а ARP – это протокол предназначенный для определения MAC адреса по известному IP

2. Протокол ICMP относится к 3 – сетевому уровню модели OSI т.к. этот уровень отвечает за определение маршрута и логическую адресацию. ICMP – это сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных, например, запрашиваемая услуга недоступна или хост, или маршрутизатор не отвечают.

3. TTL (Time To Live) — поле в заголовке IPv4 пакета. Оно задает «время жизни» пакета. Каждый маршрутизатор должен уменьшать значение поля TTL при прохождении пакета на единицу. Это приведет к изменению заголовка пакета, следовательно, маршрутизатор должен пересчитать контрольную сумму IP-заголовка.

Изначально поле TTL должно было дополнительно уменьшаться на единицу каждую секунду, пока пакет обрабатывается маршрутизатором. Но в последствии от ежесекундного уменьшения отказались и не всегда упоминают этот факт (факт присутствия в протоколе данного правила). Причина отказа проста — большинство маршрутизаторов, как правило, обрабатывают поток пакетов настолько быстро, что они не задерживаются на секунду.

Когда значение поля TTL достигает 0, маршрутизатор должен отбросить такой пакет. Следовательно имеет место правило: маршрутизатор не пропускает пакеты с нулевым значением поля TTL. В этом действии кроется основное предназначение этого поля — избежание петель маршрутизации. В случае ошибочной маршрутизации, пакет не будет ходить бесконечно по сети, а отбросится через некоторое время. TTL до основного шлюза и до 8.8.8.8 (64 и 52)

4. Сокет (англ. socket — разъём) — название программного интерфейса для обеспечения обмена данными между процессами. Процессы при таком обмене

могут исполняться как на одной ЭВМ, так и на различных ЭВМ, связанных между собой сетью. Сокет — абстрактный объект, представляющий конечную точку соединения.

Следует различать клиентские и серверные сокеты. Клиентские сокеты грубо можно сравнить с конечными аппаратами телефонной сети, а серверные — с коммутаторами. Клиентское приложение (например, браузер) использует только клиентские сокеты, а серверное (например, веб-сервер, которому браузер посылает запросы) — как клиентские, так и серверные сокеты.

Интерфейс сокетов впервые появился в BSD Unix. Программный интерфейс сокетов описан в стандарте POSIX.1 и в той или иной мере поддерживается всеми современными операционными системами.

Принципы сокетов

Для взаимодействия между машинами с помощью стека протоколов TCP/IP используются адреса и порты. Адрес представляет собой 32-битную структуру для протокола IPv4, 128-битную для IPv6. Номер порта — целое число в диапазоне от 0 до 65535 (для протокола TCP).

Эта пара определяет сокет («гнездо», соответствующее адресу и порту).

В процессе обмена, как правило, используется два сокета — сокет отправителя и сокет получателя. Например, при обращении к серверу на HTTP-порт сокет будет выглядеть так: 194.106.118.30:80, а ответ будет поступать на mmm.nnn.ppp.qqq:xxxxx.

Каждый процесс может создать «слушающий» сокет (серверный сокет) и привязать его к какому-нибудь порту операционной системы (в UNIX непривилегированные процессы не могут использовать порты меньше 1024).

Слушающий процесс обычно находится в цикле ожидания, то есть просыпается при появлении нового соединения. При этом сохраняется возможность проверить наличие соединений на данный момент, установить тайм-аут для операции и т. д.

Каждый сокет имеет свой адрес. ОС семейства UNIX могут поддерживать много типов адресов, но обязательными являются INET-адрес и UNIX-адрес.

Если привязать сокет к UNIX-адресу, то будет создан специальный файл (файл сокета) по заданному пути, через который смогут сообщаться любые локальные процессы путём чтения/записи из него (см. сокет домена Unix). Сокеты типа INET доступны из сети и требуют выделения номера порта.
Обычно клиент явно «подсоединяется» к слушателю, после чего любое чтение или запись через его файловый дескриптор будут передавать данные между ним и сервером.

5. 53 - порт, идентифицирующий протокол DNS
6. 80 – порт, идентифицирующий протокол HTTP

Практическая работа№18

Тема: «Средства мониторинга компьютерных сетей».

Цель: На практике изучить средства мониторинга компьютерных сетей.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. На практике покажите использование одного средства из каждого класса средств мониторинга и анализа компьютерной сети.

Задание 2. Отразите результаты в отчете о работе

Задание 3. Ответьте на контрольные вопросы.

Контрольные вопросы

1) Что такое агенты систем управления?
2) Опишите принцип работы анализатора протоколов.
3) Что такое экспертные системы?
4) Что такое системы диагностики и за счет каких протоколов такие системы функционируют?

Практическая работа№19

Тема: «Средства анализа сети с помощью команд сетевой операционной системы».

Цель: Получить навыки использования стандартных сетевых утилит ОС Windows

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. Проанализируйте средства анализа сети с помощью команд сетевой операционной системы и сделайте вывод.

Задание 2. Ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

Задание 3. Выведите список доступных сетевых ресурсов своего компьютера;

Задание 4. Спросив у соседа слева имя компьютера, просмотрите его общие ресурсы;

Задание 5. Получив свой IP адрес, «опросите» его. Сначала с минимальным размером пакета, затем с максимально возможным;

Задание 6. Используя ранее полученное от соседа слева имя компьютера, определите его IP адрес;

Задание 7. Используя IP адрес полученный в предыдущем пункте, проверьте подключение к нему, используя число ретрансляций на маршруте, где делается отметка времени, равное количеству его общих сетевых ресурсов;

Задание 8. Просмотрите список всех сетевых портов на вашем компьютере и сосчитайте количество открытых (прослушиваемых);

Задание 9. Определите маршрут до сайта yandex.ru, с максимальным числом прыжков, равным значению полученному в предыдущем пункте;

Задание 10. Очистите текущую конфигурацию DHCP, затем обновите её;

Задание 11. Изучив утилиту **netsh**, измените с ее помощью свой IP адрес на статический – 192.168.1., маска подсети – 255.255.255.0;

Задание 12. Проверьте подключение к IP адресу из п.2.5;

Задание 13. Используя **netsh**, верните свой IP адрес на получение по DHCP;

Задание 14. Сделайте диск C:\ общим сетевым ресурсом, используя в качестве имени Фамилию, а в качестве комментария строку «Моя первая Шара»;

Задание 15. Выведите список общих сетевых ресурсов соседа слева;

Задание 16. Подключите созданный соседом ресурс в качестве сетевого диска «Z:»;

Задание 17. Выведите список подключений вашего компьютера;

Задание 18. Отключите сетевой диск «Z:» ;

Задание 19. Сделайте выводы;

Контрольные вопросы

1. Какой протокол необходим для работы с утилитой ***ping***? Найти описание и характеристики протокола.
2. Можно ли утилитой ***tracert*** задать максимальное число ретрансляций?
3. Какой результат выдаст утилита ***netstat*** с параметрами ***-a -s -r?*** Поясните полученный результат.
4. Что такое localhost?
5. Найти самостоятельно любую стандартную сетевую утилиту Windows

Практическая работа№20

Тема: «Финальная комплексная практическая работа по эксплуатации объектов сетевой инфраструктуры».

Цель: Применить на практике получение навыки и знания при выполнении итоговой работы.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Ход работы.

Задание:

Выберете тематику разработки сетевой инфраструктуры из нижеперечисленных:

1) ЛВС организации
2) СКС Организации

Далее выполните следующие работы для описания сетевой инфраструктуры

1) Создайте проектную документацию

1. Создайте логическую схему сети.
2. Создайте физическую схему сети.
3. Отразите административную подсистему.

2) Создайте техническую документацию:

1. Отразите схему обжима кабеля (выполните тестирование кабеля).
2. Отразите процесс кроссирования кабеля в информационную розетку и патч-панель.

3) Организуйте работу средств мониторинга и анализа сетевой инфраструктуры.
4) Организуйте работу средств управления сетью.

Контрольные вопросы

1) Что такое проектная документация
2) Что такое техническая документация
3) Что такое административная подсистема
4) Что такое локально вычислительная сеть и чем отличаются понятия СКС и ЛВС?
5) Опишите схему обжима витой пары
6) Что такое кроссирование?
7) Какие средства требуются для управления сетью (какие основные команды)?
8) Для чего выполняется мониторинг и анализ компьютерной сети, и какую информацию он может предоставить?

Критерии оценки:

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если не выполнена одна часть задания, выводы сделаны правильно

3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

Тема 1.2. Эксплуатация систем IP- телефонии. Автоматизированные системы управления технологическими процессами (АСУ ТП). Промышленные сетевые технологии и протоколы в АСУ ТП

Практическая работа№1

Тема: «Настройка аппаратных IP-телефонов. Настройка программных IP-телефонов, факсов. Развертывание сети с использованием VLAN для IP-телефонии».

Цель: Научится подключать и настраивать аппаратные IP-телефоны для работы в сети. Изучить настройку программных IP-телефонов, факсов. Изучить развертывание сети с использованием VLAN для IP-телефонии.

Оборудование и наглядные пособия: IP-телефон DHP-150S, учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Ход работы.

Задание 1. Установите и настройте аппаратный IP-телефон DHP-150S.

Задание 2. Подключите IP-телефон.

Задание 3. Настройте параметры SIP.

Задание 4. Настройте IP-телефон с использованием Web-интерфейса.

Задание 5. Установте и настройте аппаратный IP-телефон DHP-400S.

Задание 6. Статусы индикаторов.

Задание 7. Настройте телефон с установочного меню.

Задание 8. Установите статический IP-адрес.

Задание 9. Установите динамический IP-адрес.

Задание 10. Настройте телефон через web-браузер.

Задание 11. Подключите и настройте IP-телефонию. Выборите провайдера VOIP-связи.

Задание 12. Используйте программы и устройства для связи. Установите и настройте VOIP-оборудования.

Задание 13. Сравните виртуальный и аналоговый АТС плюсы и минусы. Примените программные и аппаратные IP-АТС.

Задание 14. Особенности настройки программных и аппаратных IP-АТС. Возможные проблемы при работе с IP-телефонией.

Задание 15. Варианты организации ip-телефонии в офисе.

Задание 16. Настройте работу VOIP-телефонии за NAT.

Задание 17. Настройка факса для ip телефонии. Программное подключение при наличии гарнитуры. Максимальное число одновременных подключений**.** Способ передачи DTMF-сигналов**.**

Задание 18. Закрепить навыки работы с сетевым оборудованием 2+ и 3 уровня.

Задание 19. Ознакомиться с оборудованием VoIP;

Задание 20. Научиться основам настройки VLAN.

Содержание отчета

1. Цель работы, исходные данные в соответствии с заданным вариантом из таблиц 7.1 и 7.2.

2. Результаты произведенных настроек (заполненная таблица 7.3,результаты выполнения команд из пунктов 4, 5, 9 подраздела 7.2), изображение смоделированной сети (см. пример на рисунке 7.3).

3. Вывод по работе.

4. Ответы на контрольные вопросы.

Контрольные вопросы.

1. Перечислите операции установки и настройки аппаратного IP-телефона DHP-150S.

2. Перечислите названия клавиш аппаратного IP-телефона DHP-150S и их функции.

3. Перечислите операции установки и настройки программного IP-телефона.

4. Перечислите операции установки и настройки факса для ip телефонии.

5. Что такое VLAN?

6. Какие решения существуют для настройки VLAN?

7. Что такое VTP?

8. Что такое trunk?

9. Терминология портов Cisco (касательно VLAN)

10. Что такое DTP?

11. Что такое VoIP?

12. Виды IP-телефонии

13. Основные данные по коммутатору 2960

14. Основные данные по маршрутизатору 2811

15. Что такое TFTP?

16. Порядок настройки маршрутизатора для IP-телефонии

17. Использование telephony-service

18. Настройка VLAN на коммутаторе

19. Действия при добавлении IP-телефона в имеющуюся сеть IP-телефонии

Практическая работа№2

Тема: «Настройка шлюза».

Цель: Усвоить навыки настройки шлюза.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. Подключите кабели в сети в соответствии с топологией. Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Настройте базовые параметры для маршрутизатора R1. Настройте базовые параметры на коммутаторах S1 и S2. Настройте базовые параметры на компьютерах PC-A и PC-B.

Задание 2. Настройте коммутаторы для работы с сетями VLAN и создания транковых каналов. Настройте сети VLAN на коммутаторе S1. Настройте сети VLAN на коммутаторе S2.

Задание 3. Проверка транковой связи, сетей VLAN, маршрутизации и подключения. Узнать шлюз в Windows.

Контрольные вопросы:

1. Опишите поэтапно настройку шлюза.
2. В чём заключается преимущество использования устаревшего метода маршрутизации между VLAN?
3. На кого ориентированы современные маршрутизаторы?

Практическая работа№3

Тема: «Установка, подключение и первоначальные настройки голосового маршрутизатора. Настройка таблицы пользователей в голосовом маршрутизаторе. Настройка групп в голосовом маршрутизаторе. Настройка таблицы маршрутизации вызовов в голосовом маршрутизаторе. Настройка голосовых сообщений в маршрутизаторе».

Цель: Изучить установку, подключение и первоначальную настройку голосового маршрутизатора. Изучить настройки таблиц пользователей в голосовом маршрутизаторе. Изучить настройки групп в голосовом маршрутизаторе. Изучить настройку таблицы маршрутизации вызовов в голосовом маршрутизаторе. Изучить настройки голосовых сообщений в маршрутизаторе.

Оборудование и наглядные пособия: маршрутизатор голосовой, маршрутизатор вызовов DVX-7090, учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Ход работы.

Задание 1. Настройте сетевые параметры.

Задание 2. Настройте таблицы пользователей.

Задание 3. Пропишите основные настройки пользователя.

Задание 4. Настройте регитрацию пользователя.

Задание 5. Настройте группы в голосовом маршрутизаторе.

Задание 6. Настройте таблицы маршрутизации вызовов в голосовом маршрутизаторе.

Задание 7. Настройте голосовые сообщения в маршрутизаторе.

Контрольные вопросы.

1. Опишите поэтапно установку и подключение голосового маршрутизатора.
2. Как производиться первоначальная настройка голосового маршрутизатора?
3. Перечислите основные операции настройки таблиц пользователей в голосовом маршрутизаторе».
4. Перечислите основные операции по настройке групп в голосовом маршрутизаторе.
5. Перечислите основные настройки таблицы маршрутизации вызовов в голосовом маршрутизаторе.
6. Перечислите основные настройки голосовых сообщений в маршрутизаторе.

Практическая работа№4

Тема: «Настройка программно-аппаратной IP-АТС. Установка и настройка программной IP-АТС (например, Asterisk)».

Цель: Изучить настройку программно-аппаратной IP-АТС. Изучить установку и настройку программной IP-АТС (например, Asterisk).

Оборудование и наглядные пособия: маршрутизатор, учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Ход работы.

Задание 1. Настройте программно-аппаратную IP-АТС.

Задание 2. Изучите руководство по настройке IP-АТС Asterisk.

Задание 3. Изучите особенности настройки IP-АТС в соответствии с рекомендациями, указанными в Методическом пособии «Приемы и методы работы с аппаратурой и программным обеспечением».

Задание 4. Соберите сеть с топологией, представленной на рис. 1

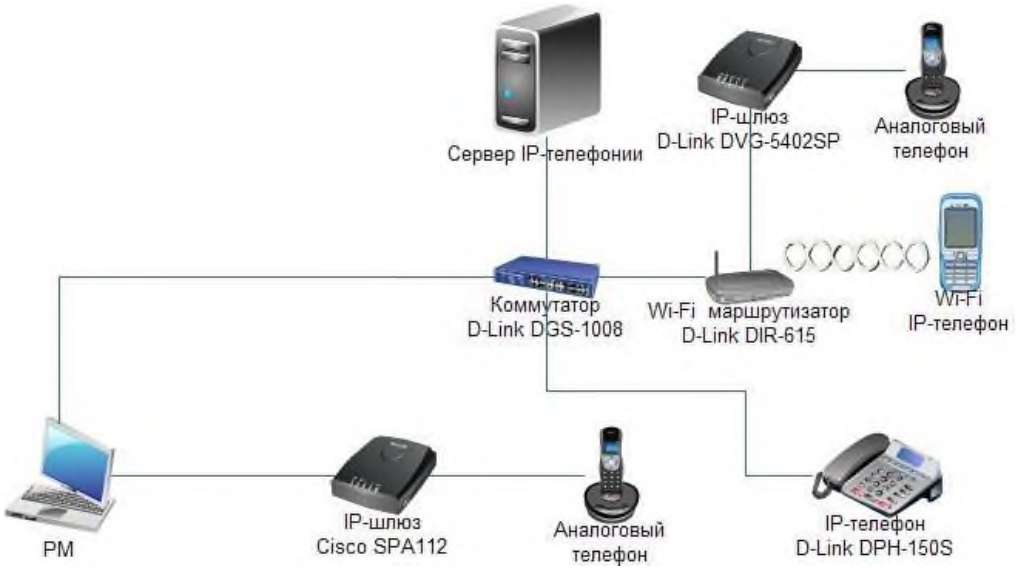


Рис. 1. Топология сети

Контрольные вопросы.

1. Перечислите основные настройки программно-аппаратной IP-АТС.

2. Перечислите основные операции установки и настройки программной IP-АТС (например, Asterisk).

Практическая работа№5

Тема: «Тестирование кодеков. Исследование параметров качества обслуживания».

Цель: Изучить тестирование кодеков. Исследование параметров качества обслуживания. Провести тестирование существующих кодеков, сравнить различные реализации кодеков. Получить экспериментальные

данные загрузки кодеками сетевого канала, объем потребляемого трафика и подверженности кодеков негативным влияниям задержек и потерь пакетов в сети передачи данных.

Оборудование и наглядные пособия: комутатор, учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Ход работы.

Задание 1. Протестируйте кодеки. Исследуйте параметры качества обслуживания.

Содержимое отчета

1. Название работы
2. Цель работы
3. Теоретические сведения
4. Значимые фрагменты настроек sip.conf для каждого эксперимента
5. Скриншоты окна статистики trafshow
6. Скриншоты окна статистики wireshark
7. Результаты выполнения тестирования в виде таблицы

Кодек	Требуемая полоса пропускания	Количество пакетов за минуту	Пропускание тишины	Влияние потерь пакетов	Влияние задержек

8. Анализ полученных результатов
9. Выводы.

Контрольные вопросы

1. Как задать приоритет использования кодеков для сервера Asterisk?
2. Как задать использование кодека G711 по А закону?
3. Какие кодеки относятся к стандарту ITU-T?
4. Назовите этапы кодирования голосовых данных.
5. В чем суть процесса компандирования?
6. Какие кодеки наиболее восприимчивы к проблемам в сетевом канале?
7. Какие кодеки имеют наименьшую полосу пропускания, и почему?

8. Приведите пример фильтра, для отлова голосовых пакетов
9. Где в сетевом пакете указывается используемый кодек?
10. Как изменить используемый кодек в настройках UA?

Практическая работа№6

Тема: «Мониторинг и анализ соединений по различным протоколам. Мониторинг вызовов в программном коммутаторе».

Цель: Изучить мониторинг и анализ соединений по различным протоколам. Изучить мониторинг вызовов в программном коммутаторе.

Оборудование и наглядные пособия: программый коммутатор, учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. Проведите мониторинг и анализ соединений по различным протоколам.

Задание 2. Проанализировать и изучить мониторинг вызовов в программном коммутаторе.

Контрольные вопросы.

1. Перечислите операции мониторинга и анализа соединений по различным протоколам.
2. Что такое программный коммутатор дайте ему определение?
3. Как происходит мониторинг вызовов в программном коммутаторе?

Практическая работа№7

Тема: «Создание резервных копий баз данных».

Цель: Применить на практике получение навыки и знания при выполнении итоговой работы.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ПК 3.6. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ОК10. ОК11.

Ход работы.

Задание 1. Просмотреть и изучить структуры базы данных.

Задание 2. Создайте резервную копию базы данных.

Задание 3. Восстановите базы данных из резервных копий.

Задание 4. Необходимо создать резервные копии базы данных «МММ» с использованием полного резервного копирования, разностного резервного копирования и резервного копирования журнала транзакций.

Контрольные вопросы.

1. Какие причины резервирования данных?
2. Какие существуют типы резервного копирования?
3. Какие преимущества дает механизм теневых копий?
4. Какие типы резервного копирования Вы знаете? В чем их особенности?
5. Кто планирует какие данные нужно резервировать?
6. Какие недостатки имеет архивирование, проделанное в данной лабораторной работе?
7. Какие данные необходимо резервировать?
8. Что такое резервное копирование?
9. Какие условия нужно соблюдать для сохранения плановых резервных копий на внешний диск?
10. Что нужно сделать, чтобы восстановить целый том?
11. Какие нужно проделать шаги для полного восстановления сервера?
12. Из за чего размер резервной копии на DVD диске может быть меньше чем том на сервере?

Практическая работа№8

Тема: «Практическое применение специализированных сетевых интерфейсов для умного дома».

Цель: Изучить практическое применение специализированных сетевых интерфейсов для умного дома.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, программное обеспечение для умного дома, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание №1 На практике примените специализированные сетевые интерфейсы для умного дома.

Контрольные вопросы

1. Перечислите сетевые интерфейсы для умного дома.
2. Охарактеризуем кратко модули умного дома.

Практическая работа№9

Тема: «Определение свойств объектов управления на практике. Классификация технологических объектов управления на примере производственного предприятия. Анализ и сравнение систем управления технологическими объектами на примере различных отраслей промышленности».

Цель: Изучить определение свойств объектов управления на практике. Изучить классификация технологических объектов управления на примере производственного предприятия. Изучить анализ и сравнение систем управления технологическими объектами на примере различных отраслей промышленности.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание №1. Изучить теоретические сведения по теме.

Задание №2. Найдите информацию об АСУ по вашей специальности. Ответ представить в виде таблицы.

Название АСУ	Назначение	Цели

Задание №3 Определите свойств объектов управления на практике.

Задание №4 Про классифицируете технологические объекты управления на примере производственного предприятия.

Задание №5 Про анализируете и сравните системы управления технологическими объектами на примере различных отраслей промышленности.

Задание №6. Сделать вывод о проделанной работе:

Отчет прислать преподавателю на электронную почту sergei888xxxxx@yandex.ru

Контрольные вопросы

№ п/п	***Вопрос***	***Ответ***
1.	Что называется управлением?	
2.	Что называется системой управления?	
3.	Какие виды систем управления существуют?	
4.	Что называется автоматизированной системой управления?	
5.	Какую задачу решают автоматизированные системы управления?	
6.	Какие цели преследуют АСУ?	
7.	Какие функции осуществляют АСУ?	
8.	Приведите примеры автоматизированных систем управления.	

Практическая работа№10

Тема: «Изучение принципов работы АСУТП и САУ на примере реальных систем управления. Создание простой модели технологического процесса. Ознакомление с современными технологиями АСУТП на примере существующих проектов и исследований».

Цель: Изучить принцип работы АСУТП и САУ на примере реальных систем управления. Изучить создание простой модели технологического процесса. Ознакомиться с современными технологиями АСУТП на примере существующих проектов и исследований.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание №1 Принципы работы АСУТП и САУ на примере реальных систем управления.

Задание №2 Создать простую модель технологического процесса.

Задание №3 Ознакомиться с современными технологиями АСУТП на примере существующих проектов и исследований.

Контрольные вопросы

1. Какие различия при работе АСУТП и САУ?
2. Что такое технологический процесс?
3. Какие существуют современные технологии АСУТП?

Практическая работа№11

Тема: «Программирование элементов АСУТП на языках программирования на практике. Настройка и проверка работоспособности элементов АСУТП на примере конкретной системы управления. Интеграция АСУТП с другими системами и оборудованием в производственном процессе. Оценка эффективности и экономическая оценка внедрения АСУТП».

Цель: Изучить программирование элементов АСУТП на языках программирования на практике. Изучить настройку и проверку работоспособности элементов АСУТП на примере конкретной системы управления. Изучить интеграцыю АСУТП с другими системами и оборудованием в производственном процессе. Изучить оценку эффективности и экономическую оценку внедрения АСУТП.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Ход работы.

Задание №1 С программировать элемент АСУТП на языках программирования.

Задание №2 Настроить и проверить работоспособности элементов АСУТП на примере конкретной системы управления.

Задание №3 Интегрировать АСУТП с другими системами и оборудованием в производственном процессе.

Задание №4 Оценить эффективность и экономическую оценку внедрения АСУТП.

Контрольные вопросы

1. На каком языке програмирования вы будете програмировать элементы АСУТП?
2. Как настроивается и проверяется работоспособность элементов АСУТП?
3. Как можно интегрировать АСУТП с другими системами и оборудованием.
4. Как вы оцениваете эффективность и экономическую оценку внедрения АСУТП?
5. Где используется SCADA?

Практическая работа№12

Тема: «Разработка системы управления производственными процессами в условиях неопределенности и переменных условий работы. Применение нейронных сетей в системах управления технологическими процессами. Применение экспертных систем в системах управления технологическими процессами. Создание проекта автоматизации управления технологическим процессом на основе АСУТП».

Цель: Изучить разработку системы управления производственными процессами в условиях неопределенности и переменных условий работы. Изучить применение нейронных сетей в системах управления технологическими процессами. Изучить применение экспертных систем в системах управления технологическими процессами. Изучить создание проекта автоматизации управления технологическим процессом на основе АСУТП.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание №1 Разработайте систему управления производственными процессами в условиях неопределенности и переменных условий работы.

Задание №2 Применить нейронные сети в системах управления технологическими процессами.

Задание №3 Применить экспертные системы в системах управления технологическими процессами.

Задание №4 Создайте проект автоматизации управления технологическим процессом на основе АСУТП.

Контрольные вопросы

1. Объясните, как разрабатывается система управления производственными процессами?

2. Как применяются нейронные сети в системах управления технологическими процессами?

3. Как применяются экспертные системы в системах управления технологическими процессами?

4. Как создать проект автоматизации управления технологическим процессом на основе АСУТП?

Практическая работа№13

Тема: «Работа с основными сетевыми технологиями в промышленной автоматизации. Разработка схемы промышленной сети и выбор средств ее реализации».

Цель: Изучить работку с основными сетевыми технологиями в промышленной автоматизации. Изучить разработку схемы промышленной сети и выбор средств ее реализации.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание №1 Работать с основными сетевыми технологиями в промышленной автоматизации.

Задание №2 Разработать схемы промышленной сети и выбор средств ее реализации.

Контрольные вопросы

1. Дайте краткую характеристику работы с основными сетевыми технологиями в промышленной автоматизации.
2. Как разработатывается схема промышленной сети и выбор средств ее реализации дайте подробную характеристику.

Практическая работа№14

Тема: «Практическое применение протокола MODBUS для обмена данными между устройствами. Создание конфигурации сети с использованием протокола MODBUS. Организация работы контроллера (slave) и операторной панели (master) по протоколу MODBUS. Выравнивание адресов переменных в поле памяти протокола MODBUS. Настройка работы контроллера (master) с модулями ввода/вывода (slave) по протоколу MODBUS RTU. Практическая работа с различными устройствами по протоколу MODBUS RTU. Работа с протоколом MODBUS TCP».

Цель: Изучить практическое применение протокола MODBUS для обмена данными между устройствами. Изучить создание конфигурации сети с использованием протокола MODBUS. Изучить организацию работы контроллера (slave) и операторной панели (master) по протоколу MODBUS. Изучить выравнивание адресов переменных в поле памяти протокола MODBUS. Изучить настройку работы контроллера (master) с модулями ввода/вывода (slave) по протоколу MODBUS RTU. Изучить практическую работу с различными устройствами по протоколу MODBUS RTU. Изучить работу с протоколом MODBUS TCP.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание №1 На практике примените протокол MODBUS для обмена данными между устройствами.

Задание №2 Создайте конфигурацию сети с использованием протокола MODBUS.

Задание №3 Организуйте работу контроллера (slave) и операторной панели (master) по протоколу MODBUS

Задание №4 Выравните адреса переменных в поле памяти протокола MODBUS.

Задание №5 Настроить работу контроллера (master) с модулями ввода/вывода (slave) по протоколу MODBUS RTU.

Задание №6 На практическе проработать с различными устройствами по протоколу MODBUS RTU.

Задание №7 Работать с протоколом MODBUS TCP.

Контрольные вопросы

1. Как на практике применяется протокол MODBUS для обмена данными

между устройствами?

2. Как создать конфигурацию сети с использованием протокола MODBUS?

3. Опишите организацию работы контроллера (slave) и операторной панели (master) по протоколу MODBUS.

4. Как выравниваются адреса переменных в поле памяти протокола MODBUS?

5. Как происходит процесс настройки работы контроллера (master) с модулями ввода/вывода (slave) по протоколу MODBUS RTU?

6. Объясните, как на практике прорабатывается с различными устройствами по протоколу MODBUS RTU?

7. Объясните, как происходит работа с протоколом MODBUS TCP?

Практическая работа№15

Тема: «Работа с типовыми проводными и кабельными протоколами в промышленности. Изучение беспроводных локальных сетей для промышленного применения. Работа с преобразователями интерфейсов в промышленной сети. Ознакомление с современными тенденциями в развитии сетевых технологий в АСУ ТП, включая web-серверы и облачные решения. Особенности применения промышленных сетевых протоколов в условиях высоких нагрузок и плохой связи».

Цель: Изучить работу с типовыми проводными и кабельными протоколами в промышленности. Изучить беспроводные локальные сети для промышленного применения. Изучить работу с преобразователями интерфейсов в промышленной сети. Изучить современные тенденции в развитии сетевых технологий в АСУ ТП, включая web-серверы и облачные решения. Изучить особенности применения промышленных сетевых протоколов в условиях высоких нагрузок и плохой связи.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание №1 Работать с типовыми проводными и кабельными протоколами в промышленности.

Задание №2 Изучите беспроводные локальные сети для промышленного применения.

Задание №3 Работать с преобразователями интерфейсов в промышленной сети.

Задание №4 Ознакомиться с современными тенденциями в развитии сетевых технологий в АСУ ТП, включая web-серверы и облачные решения.

Задание №5 Ознакомиться с особенностями применения промышленных сетевых протоколов в условиях высоких нагрузок и плохой связи.

Контрольные вопросы

1. Как работают с типовыми проводными и кабельными протоколами в промышленности?
2. Какие вы знаете беспроводные локальные сети для промышленного применения?
3. Как преобразовывается интерфейсы в промышленной сети?
4. Какие существуют современные тенденции в развитии сетевых технологий в АСУ ТП, включая web-серверы и облачные решения?
5. Какие особенностями применения промышленных сетевых протоколов в условиях высоких нагрузок и плохой связи?

Практическая работа№16

Тема: «Сравнительный анализ промышленных Ethernet-технологий: EtherNet/IP, PROFINET, Modbus TCP. Применение промышленных маршрутизаторов для обеспечения безопасности и надежности работы сетевой инфраструктуры. Практическое использование промышленных маршрутизаторов. Организация удаленного доступа к сетевым устройствам в промышленной сети. Разработка и тестирование собственного промышленного протокола для обмена данными между устройствами в сети.

Организация кластера промышленных компьютеров для выполнения высокопроизводительных вычислений в АСУ ТП».

Цель: Изучить сравнительный анализ промышленных Ethernet-технологий: EtherNet/IP, PROFINET, Modbus TCP. Изучить применение промышленных маршрутизаторов для обеспечения безопасности и надежности работы сетевой инфраструктуры. Изучить практическое использование промышленных маршрутизаторов. Изучить организацию удаленного доступа к сетевым устройствам в промышленной сети. Изучить разработку и тестирование собственного промышленного протокола для обмена данными между устройствами в сети. Изучить организацию кластера промышленных компьютеров для выполнения высокопроизводительных вычислений в АСУ ТП.

Оборудование и наглядные пособия: промышленный маршрутизатор, учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание №1Сравните анализ промышленных Ethernet-технологий: EtherNet/IP, PROFINET, Modbus TCP.

Задание №2 Примените промышленные маршрутизаторы для обеспечения безопасности и надежности работы сетевой инфраструктуры.

Задание №3 Используйте практически промышленные маршрутизаторы.

Задание №4 Организуйте удаленный доступ к сетевым устройствам в промышленной сети.

Задание №5 Разработайте и протестируйте собственный промышленный протокол для обмена данными между устройствами в сети.

Задание №6 Организуйте кластер промышленных компьютеров для выполнения высокопроизводительных вычислений в АСУ ТП.

Контрольные вопросы

1. Охарактеризуйте сравнительный анализ промышленных Ethernet-технологий: EtherNet/IP, PROFINET, Modbus TCP.

2. Назовите марки промышленных маршрутизаторов для обеспечения безопасности и надежности работы сетевой инфраструктуры.

3. Какие особенности использования промышленных маршрутизаторов?

4. Как орзанизовываетсяудаленный доступ к сетевым устройствам в промышленной сети опишите весь процесс.

5. Как разрабатывается и протестируестя собственный промышленный протокол для обмена данными между устройствами в сети?

6. Как организовывается кластер промышленных компьютеров для выполнения высокопроизводительных вычислений в АСУ ТП?

Практическая работа№17

Тема: «Диагностика и устранение неисправностей в системах IP-телефонии. Финальная комплексная практическая работа по эксплуатации систем IP-телефонии».

Цель: Изучить диагностику и устранение неисправностей в системах IP-телефонии. Применить на практике получение навыки и знания при выполнении итоговой работы.

Оборудование и наглядные пособия: IP-телефон, учебные пособия, литература, персональный компьютер, операционная система Windows 10.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание:

Задание 1. Продиагностируйте и устраните неисправности в системах IP-телефонии.

Выберете тематику разработки систем IP-телефонии из нижеперечисленных:

1) Настройте аппаратный IP-телефон.

2) Настройте шлюза.

Далее выполните следующие работы для описания систем IP-телефонии:

3) Работа с голосовым маршрутизатором: установка, подключение и первоначальные настройки голосового маршрутизатора:

1. Настройте таблицы пользователей в голосовом маршрутизаторе.

2. Настройте группы в голосовом маршрутизаторе.

3. Настройте таблицы маршрутизации вызовов в голосовом

Маршрутизаторе.

4). Настройте голосовые сообщения в маршрутизаторе.

5) Настройте программно-аппаратной IP-АТС:

1. Установите и настройте программной IP-АТС (например, Asterisk).

6) Тестирование кодеков. Исследуйте параметры качества обслуживания.

7). Мониторинг и анализ соединений по различным протоколам.

8) Мониторинг вызовов в программном коммутаторе.

Контрольные вопросы

1. Как провидится диагностика и устранение неисправностей в системах IP-телефонии.

2. Перечислите операции установки и настройки аппаратного IP-телефона DHP-150S.

3. Опишите поэтапно настройку шлюза.

4. Опишите поэтапно установку и подключение голосового маршрутизатора.

5. Как производиться первоначальная настройка голосового маршрутизатора?

6. Опишите какие производятся настройки таблиц пользователей в голосовом маршрутизаторе.

7. Назовите какие производятся настройки групп в голосовом маршрутизаторе.

8. Опишите как производистя настройка таблиц маршрутизации вызовов в голосовом Маршрутизаторе.

9. Какие производятся настройки в голосовом сообщении маршрутизатора.

10. Для чего проводятся настройки программно-аппаратной IP-АТС:

11. Как установить и настроить программный IP-АТС (например, Asterisk).

12. Для чего проводится тестирование кодеков. Дайте анализ как проводтся исследование параметров качества обслуживания.

13. Промониторьте и проанализируету соединение по различным протоколам.

14. Для чего проводится мониторинг вызовов в программном коммутаторе.

15. Перечислите основные опреции диагностики и устранение неисправностей в системах IP-телефонии и их настройка.

Критерии оценки:

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если не выполнена одна часть задания, выводы сделаны правильно

3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

МДК.03.02. Безопасность компьютерных сетей

Раздел 2. Безопасность компьютерных сетей

Тема 2.1. Безопасность компьютерных сетей. Обеспечение сетевой безопасности.

Практическая работа №1

Тема: «Социальная инженерия. Исследование сетевых атак и инструментов проверки защиты сети».

Цель работы. Изучить социальную инженерию. Изучить исследование сетевых атак и инструментов проверки защиты сети.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10, компьютер с доступом к Интернету.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание:

1. Сделать презентацию терминов, указанных в задании

2. Выполнить анализ объекта защиты информации по предложенным выше пунктам: А) Описать автоматизированную информационную систему для предложенного преподавателем виртуального предприятия (указать составляющие автоматизированной системы, их основные характеристики и т.д.) Б) Предположить угрозы и уязвимости для этой системы В) Указать технологии, средства и инструменты, которые можно применить для защиты информации в автоматизированной системе указанного объекта. Г) Предположить возможные действия нарушителей при условии выполнения защиты информации в соответствии с п. В)

3. Разработать документ «Политика безопасности», указать СПИСОК документов, которые необходимо разработать для реализации политики безопасности на предприятии.

4. Составить тест (или кроссворд), включающий не менее 10 терминов (или основных понятий) курса (тест должен содержать не менее 3-х вариантов ответа).

5. Результаты работы оформить в виде отчета (текстовый файл, файл - презентация). Отчет должен содержать ФИО студента, номер группы, ответы на поставленные вопросы. Название папки должно содержать фамилию и группу студента.

Задача

В этой лабораторной работе вы изучите методы социальной инженерии, а также способы, которые помогут распознать и предотвратить ее.

Инструкции

Примеры исследования Социальной инженерии

Социальная инженерия связана с информационной безопасностью, она используется для описания методов, используемых человеком (или лицами), которые манипулируют людьми, чтобы получить доступ или поставить под угрозу информацию об организации или ее компьютерных системах.

Социального инженера обычно трудно идентифицировать, и он может претендовать на звание нового сотрудника, ремонтника или исследователя. Социальный инженер может даже предоставить учетные данные для подтверждения этой личности. Завоевывая доверие и задавая вопросы, он или она могут собрать воедино достаточно информации, чтобы проникнуть в сеть организации.

Вопрос:

Используйте любой интернет-браузер для исследования случаев социальной инженерии. Обобщите три примера, найденные в вашем исследовании.ведите ваш ответ здесь.

Распознание признаков социальной инженерии

Социальные инженеры - не более чем воры и шпионы. Вместо того, чтобы проникнуть в вашу сеть через Интернет, они пытаются получить доступ, полагаясь на желание человека быть любезным. Хотя сценарий, приведенный ниже и описанный в книге Кристофера Хаднаги «Искусство взлома человека», не является специфическим для сетевой безопасности, он иллюстрирует, как ничего не подозревающий человек может непреднамеренно выдавать конфиденциальную информацию.

«В кафе было относительно тихо, когда я, одетый в костюм, сидел за пустым столом. Я положил свой портфель на стол и стал ждать подходящей жертвы. Вскоре именно такая жертва прибыла с другом и села за стол рядом с моим. Она положила свою сумку на сиденье рядом с собой, притянула сиденье ближе и постоянно держала руку на сумке.

Через несколько минут ее подруга ушла в туалет. Жертва [цель] была одина, поэтому я подал сигнал Алексу и Джесс. Играя в паре, Алекс и Джесс спросили жертву, сфотографирует ли она их обоих. Она с радостью согласилась это сделать. Она убрала руку от своей сумки, чтобы взять камеру и сфотографировать «счастливую пару», и, пока она отвлеклась, я протянул руку, взял ее сумку и запер ее в моем портфеле. Моя жертва еще не заметила,

что ее сумка пропала, когда Алекс и Джесс покинули кафе. Алекс тогда пошел в соседний гараж.

Ей не потребовалось много времени, чтобы понять, что ее сумка пропала. Она начала паниковать, отчаянно оглядываясь по сторонам. Именно на это мы и надеялись, поэтому я спросил ее, нужна ли ей помощь.

Она спросила меня, видел ли я что-нибудь. Я сказал ей, что нет. Потом убедил ее сесть и подумать о том, что было в сумке. По телефону. Косметика Немного денег. И ее кредитные карты. Бинго!

Я спросил, с кем она работала, а затем сказал, что я работаю в этом банке. Какая удача! Я заверил ее, что все будет хорошо, но ей нужно будет немедленно заблокировать свою кредитную карту. Я позвонил по номеру «справочной службы», которым на самом деле был Алекс, и передал ей свой телефон.

Алекс был в фургоне в гараже. На приборной панели проигрыватель компакт-дисков воспроизводил служебные шумы. Он заверил, что ее карта может быть легко аннулирована, но для подтверждения ее личности ей нужно было ввести свой PIN-код на клавиатуре телефона, который она использовала. На моем телефоне и моей клавиатуре.

Когда у нас был ее PIN-код, я ушел. Если бы мы были настоящими ворами, у нас был бы доступ к ее счету через банкомат и покупки с помощью PIN-кода. К счастью для нее, это было просто телешоу».

Помните: «Те, кто строит стены, думают иначе, чем те, кто стремится пройти над, под, вокруг или через них». Пол Уилсон - "Настоящие аферисты"

Задание №6. Исследуйте сетевые атаки и инструменты проверки защиты сети.

Контрольные вопросы.

Вопрос:

1. Исследуйте способы распознавания социальной инженерии. Опишите три примера, найденные в вашем исследовании.

Исследуйте способы распознавания социальной инженерии.

Вопросы:

2. Есть ли в вашей образовательном учреждении процедуры, помогающие предотвратить социальную инженерию?

Введите ваш ответ здесь.

3. Если да, то каковы некоторые из этих процедур?

Введи **ваш ответ здесь.**

4. Используйте Интернет для изучения процедур, которые используют другие организации, чтобы помешать социальным инженерам получить доступ к конфиденциальной информации.

5. Дайте полный анализ по исследованию сетевых атак.

6. Какие существуют инструменты для проверки защиты сети. Дать полную характеристику одному из них.

Перечислите свои выводы.

Практическая работа №2

Тема: «Настройка безопасного доступа к маршрутизатору».

Цель работы. Освоить настройку безопасного доступа к маршрутизатору.

Оборудование и наглядные пособия: маршрутизатор, учебные пособия, литература, персональный компьютер, операционная система Windows 10, компьютер с доступом к Интернету.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Ход работы.

Задание 1. Изучение методики настройки настройка безопасного доступа к маршрутизатору.

Задание 2. Выполнение настройки.

Задание 3. Отчет о проделанной работе.

Контрольные вопросы.

1) С какой целью производятся настройки ограничения доступа к сетевым устройствам?

2) Какие возможности дает рабочий режим?

3) Конфигурационный терминал?

4) Какие уровни шифрования применяются к стандартным паролям на маршрутизаторах CISCO?

5) Сколько существует уровней привилегий?

6) Какие общепринятые меры безопасности вы применяли в лабораторной работе?

7) Опишите порядок команд для настройки telnet-доступа.

8) Опишите порядок команд для настройки ssh-доступа.

Практическая работа №3

Тема: «Обеспечение административного доступа AAA и сервера Radius».

Цель работы. Изучить обеспечение административного доступа AAA и сервера Radius.

Оборудование и наглядные пособия:, учебные пособия, литература, персональный компьютер, операционная система Windows 10, компьютер с доступом к Интернету.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. Обеспечить административный доступ AAA и сервера Radius

Задачи 2. Настройка основных параметров устройства. Настройте основные параметры, такие как имена хостов, IP-адреса интерфейсов и пароли для доступа. Настройте статическую маршрутизацию.

Задание 3. Настройка локальной аутентификации. Настройте локального пользователя базы данных и локальный доступ для линий консоли, vty и aux. Проверьте конфигурацию.

Задание 4. Настройка локальной аутентификации с помощью AAA. Настройте локальную базу данных пользователей с помощью Cisco IOS. Настройте локальную аутентификацию AAA с помощью Cisco IOS. Проверьте конфигурацию.

Задание 5. Настройка централизованной аутентификации с помощью AAA и RADIUS. Установите на компьютер сервер RADIUS. Настройте пользователей на сервере RADIUS. На маршрутизаторе настройте сервисы AAA с помощью Cisco IOS, чтобы получить доступ к серверу RADIUS для аутентификации. Проверьте конфигурацию AAA и RADIUS.

Контрольные вопросы.

1. Зачем организации может понадобиться использование централизованного сервера аутентификации вместо того, чтобы настраивать пользователей и пароли на каждом маршрутизаторе по отдельности?

_____
_____
_____
_____
_____
_____
_____
_____

2. Сравните локальную аутентификацию и локальную аутентификацию с использованием AAA.

_____
_____
_____
_____
_____
_____
_____
_____

3. На основе содержания онлайн-курса Академии, результатов поиска в Интернете, а также использования RADIUS в данной лабораторной работе сравните RADIUS и TACACS+.

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet 1**	**Интерфейс Ethernet 2**	**Последовательный интерфейс 1**	**Последовательный интерфейс 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать конфигурацию маршрутизатора, определите его тип по интерфейсам, а также по количеству имеющихся интерфейсов. Эффективно перечислить все комбинации настроек для маршрутизатора каждого класса невозможно. В данной таблице приведены идентификаторы возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов в устройстве. В эту таблицу не включены какие-либо иные типы интерфейсов, даже если в определенном маршрутизаторе они могут присутствовать. В качестве примера можно привести интерфейс ISDN BRI. В строке в скобках приведены официальные аббревиатуры, которые могут использоваться в командах Cisco IOS для представления интерфейсов.				

Практическая работа №4

Тема: «Настройка политики безопасности брандмауэров. Настройка системы предотвращения вторжений (IPS)».

Цель работы. Изучить настройку политики безопасности брандмауэров. Провести настройку системы предотвращения вторжений (IPS).

Включите IOS IPS. Настроить ведение журнала.·Изменить подпись IPS.·Проверить IPS. Предпосылки / Сценарий.

Оборудование и наглядные пособия:, учебные пособия, литература, персональный компьютер, операционная система Windows 7, 10, компьютер с доступом к Интернету.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. Изучение методики настройки политики безопасности брандмауэров. Выполнение настройки. Отчет о проделанной работе.

Устранение/Скрытие уязвимостей сетевых портов. Настройка программного брандмауэра.

Задание 2. Изучить и освоить работу брандма́уэра. Agnitum Outpost Firewall Pro версии 4.0

Задание 3. Для выполнения данной работы необходимо иметь следующее установленное программное обеспечение: VMware Workstation версии 5.0 или выше, Agnitum Outpost Firewall Pro версии 4.0 или выше, Xspider версии 7.0 или выше.

Задание 4. Защитить машину брандмауэром и произвести сканирование.

Задание 5. По варианту выданному преподавателем произвести настройку брандмауэра для устранения или скрытия найденных путем сканирования портов уязвимостей

Задание 6. Запретить доступ на виртуальной машине для HOST-компьютера и осуществить новое сканирование на уязвимости.

Задание 7. По завершении сканирования создайте отчет и сравните с сохраненными ранее.

Задание 8. Настройте глобальные правила для оставшихся портов. Полученные результаты необходимо предоставить в отчете.

Задание 9. Настройте базовые параметры маршрутизатора. Настройте имена хостов, IP-адреса интерфейсов и пароли для доступа. Настройте статическую маршрутизацию.

Задание 10. Настройте IOS IPS с помощью CLI. Настройте IOS IPS с помощью CLI. Измените сигнатуры IPS. Рассмотрите итоговую конфигурацию IPS. Проверьте работоспособность IPS. Запишите сообщения журнала IPS на сервер syslog.

Задание 11. Имитация атаки. Используйте инструмент сканирования для моделирования атаки.

Задача 12. Проверка доступа к сети LAN маршрутизатора R1 из R2.

Задача 13. Подготовка маршрутизатора и сервера TFTP.

Задача 14. Настройка криптографического ключа IPS.

Задача 15. Настройка IPS.

Задача 16. Загрузка пакета сигнатур IOS IPS на маршрутизатор.

Задача 17. Проверка правила IPS и изменение сигнатуры.

Задача 18. Проверка IPS с помощью Zenmap.

Задача 19. Проверка сообщений Syslog на маршрутизаторе R1.

Контрольные вопросы.

1 Каково назначение NetBIOS?. Объяснить важность протокола NetBIOS и взаимодействующих с ним портов.

2 Назовите основные пять режимов или политик системы Agnitum Outpost Firewall Pro работы с сетью.

3 . В каком режиме функционирует система Agnitum Outpost Firewall Pro сразу после запуска по умолчанию? Приведите характеристики этого режима.

4. На каком уровне стека протокола TCP/IP функционирует система Agnitum Outpost Firewall Pro?

5. Если при использовании файлов сигнатур версии 5.x в сигнатуру вносятся изменения, будут ли они видны на маршрутизаторе в конфигурации?

_____
_____
_____
_____
_____
_____
_____
_____

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet 1**	**Интерфейс Ethernet 2**	**Последовательный интерфейс 1**	**Последовательный интерфейс 2**
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать конфигурацию маршрутизатора, определите его тип по интерфейсам, а также по количеству имеющихся интерфейсов. Эффективно перечислить все комбинации настроек для маршрутизатора каждого класса невозможно. В данной таблице приведены идентификаторы возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов в устройстве. В эту таблицу не включены какие-либо иные типы интерфейсов, даже если в определенном маршрутизаторе они могут присутствовать. В качестве примера можно привести интерфейс ISDN BRI. В строке в скобках приведены официальные аббревиатуры, которые могут использоваться в командах Cisco IOS для представления интерфейсов.				

Практическая работа №5

Тема: «Настройка безопасности на втором уровне на коммутаторах».

Цель работы. Провести настройка безопасности на втором уровне на коммутаторах.

Оборудование и наглядные пособия:, коммутатор, учебные пособия, литература, персональный компьютер, операционная система Windows 10, компьютер с доступом к Интернету.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Ход работы.

Задание 1. Изучение методики настройки настройки безопасности на втором уровне на коммутаторах. Выполнение настройки. Отчет о проделанной работе.

Задание 2. Настройте базовые параметры коммутатора. Создайте топологию. Настройте имя хоста, IP-адрес и пароли для доступа.

Задание 3. Настройте IP DHCP Snooping. Настройте DHCP на маршрутизаторе R1. Настройте связь между сетями VLAN на маршрутизаторе R1. Настройте интерфейс F0/5 коммутатора S1 как магистральный канал. Проверьте работу DHCP на компьютерах PC-A и PC-B. Включите DHCP Snooping. Проверьте DHCP Snooping.

Задание 4. Настройте базовые параметры коммутатора.

Задание 5. Настройка DHCP.

Задание 6. Настройка связи между сетями VLAN.

Задание 7. Настройка DHCP Snooping.

Контрольные вопросы.

1. Перечислите основные настройки безопасности на втором уровне на коммутаторах.
2. Для чего проводятся настройки безопасности на втором уровне на коммутаторах.

Практическая работа №6.

Тема: «Исследование методов шифрования».

Цель работы. Научится шифровать слова и предложения различными способами.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10, компьютер с доступом к Интернету.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Ход работы.

Задание 1. Исследуйте методы шифрования.

Контрольные вопросы.

1. Какие методов шифрования вы знаете?

2. В каких случаях шифрование вырождается в кодирование. Покажите это на примерах из лабораторной работы.

Ответ: Шифрование вырождается в кодирование, когда гамма состоит из одинаковых значений байт. В таком случае каждый символ однозначно переводится в другой по одному и тому же правилу. Например, при шифровании открытого текста единичной гаммой или гаммой y = {56797 56797 56797 56797 56797 56797 56797}

$56797_{10} = 1101\ 1101\ 1101\ 1101_2$

Практическая работа №7

Тема: «Настройка Site-to-SiteVPN используя интерфейс командной строки».

Цель работы. Изучить технологию настройки Site-to-SiteVPN используя интерфейс командной строки

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10, компьютер с доступом к Интернету.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Ход работы.

Задание 1. Изучите методики настройки Site-to-SiteVPN используя интерфейс командной строки. Выполните настройки. Отчет о проделанной работе.

Задание 2. Подготовка к настройке VPN. Настройка маршрутизации между dyn1 и dyn2. Настройка маршрута по умолчанию на dyn4 и dyn5. Проверить доступность внешних интерфейсов

Задание 3. Настроить политику IKE (ISAKMP). Настроить pre-shared ключ, который будет использоваться для аутентификации. Указать какой трафик между сетями необходимо шифровать. Шифроваться должен трафик между сетями 10.0.10.0/24 и 10.0.20.0/24. Настроить политику для защиты передаваемых данных (transform-set). Настроить crypto-map и применить её на внешнем интерфейсе. Проверка работы VPN

Контрольные вопросы.

1. Назовите основные настройки Site-to-SiteVPN используя интерфейс командной строки.

Практическая работа №8.

Тема: «Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM».

Цель работы. Провести изучение базовой настройки шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки. Изучить базовую настройку шлюза безопасности ASA и настройку брандмауэров используя ASDM.

Оборудование и наглядные пособия: маршрутизатор, учебные пособия, литература, персональный компьютер, операционная система Windows 10, компьютер с доступом к Интернету.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. Изучите методики базовой настройки шлюза безопасности ASA и настройки брандмауэров используя интерфейс командной строки. Выполните настройки. Отчет о проделанной работе.

Задание 2. Настройте параметры ASA и безопасности интерфейса с помощью командной строки. Настройте политику маршрутизации, трансляции адресов и проверки с помощью командной строки.

Задание 3. Настройка DHCP, AAA и SSH. Настройте DMZ, статический NAT и ACL. Настройте основных параметров устройства. Организация доступа к консоли ASA и ASDM.

Задание 4. Настройте ASA и межсетевого экрана с использованием мастера запуска ASDM. Настройте параметры ASA в меню настройки ASDM.

Задание 5. Настройте DMZ, статического преобразования NAT и ACL-списков. Настройте параметры ASA и безопасности интерфейса с помощью командной строки.

Задание 6. Настройте политику маршрутизации, трансляции адресов и проверки с помощью командной строки. Настройте DHCP, AAA и SSH. Настройте DMZ, статический NAT и ACL.

Задание 7. Изучите методику базовой настройки шлюза безопасности ASA и настройки брандмауэров используя ASDM. Выполните настройки. Отчет о проделанной работе.

Контрольные вопросы.

1. Опишите базовые настройки шлюза безопасности ASA.
2. Опишите настройки брандмауэров используя интерфейс командной строки.
3. Опишите базовые настройки шлюза безопасности ASA и настройку брандмауэров используя ASDM.

Практическая работа №9

Тема: «Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM».

Цель работы. Провести настройку Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM.

Оборудование и наглядные пособия: машрутизотор, учебные пособия, литература, персональный компьютер, операционная система Windows 10, компьютер с доступом к Интернету.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. Настройте Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM.

Контрольные вопросы.

1. Опишите настройку Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM.

Практическая работа №10.

Тема: «Настройка Clientless Remote Access SSL VPNs используя ASDM. Настройка AnyConnect Remote Access SSL VPN используя ASDM».

Цель работы. Провести настройку Clientless Remote Access SSL VPNs используя ASDM. Провести настройку AnyConnect Remote Access SSL VPN используя ASDM.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10, компьютер с доступом к Интернету.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. Изучите методику настройки Clientless Remote Access SSL VPNs используя ASDM. Выполните настройки. Отчет о проделанной работе.

Задание 2. Изучите методику настройки AnyConnect Remote Access SSL VPN используя ASDM. Выполните настройки. Отчет о проделанной работе.

Контрольные вопросы.

1. В чем преимущества бесклиентских и клиентских VPN?

_____

_____

_____

_____

_____

_____

Их проще настроить, потому что требуется только браузер и не нужно устанавливать клиентское программное обеспечение. Их можно использовать для ограничения доступа к очень конкретным ресурсам на основе URL-адресов, определенных администрацией сети.

2. В чем разница между использованием SSL и IPsec для шифрования туннеля удаленного доступа?

_____

_____

_____

_____

_____

_____

Клиентские виртуальные частные сети могут предложить более безопасный туннель при использовании IPsec, но их несколько сложнее настроить.

3. Как происходит настройка Clientless Remote Access SSL VPNs используя ASDM.

4. Опишите как минимум два преимущества клиентских и бесклиентских VPN?

_____

_____

_____

_____

_____

Пользователи имеют доступ к тем же внутренним сетевым ресурсам, как если бы они находились в локальной сети. Клиентские VPN-решения, такие как AnyConnect, можно настроить на автоматическую загрузку соответствующего клиентского программного обеспечения в зависимости от характеристик клиентской платформы.

5. Опишите хотя бы одно различие между использованием SSL и IPsec для шифрования туннеля удаленного доступа?

_____

_____

_____

_____

Клиентские VPN могут предложить более безопасный туннель при использовании IPsec, но их несколько сложнее настроить.

6. Опишите настройку AnyConnect Remote Access SSL VPN используя ASDM.

Практическая работа №11

Тема: «Настройка VPN-туннелей для организации защищенных каналов передачи данных между территориально распределенными офисами. Работа с механизмами шифрования и аутентификации для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам. Настройка и использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет. Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети с использованием программного обеспечения для мониторинга и обнаружения угроз. Разработка и внедрение мер по минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях. Настройка и работа с системами

обнаружения и предотвращения сетевых вторжений для раннего обнаружения и предотвращения угроз безопасности».

Цель: Изучить настройку VPN-туннелей для организации защищенных каналов передачи данных между территориально распределенными офисами. Изучить работу с механизмами шифрования и аутентификации для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам. Изучить настройку и использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет. Изучить анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети с использованием программного обеспечения для мониторинга и обнаружения угроз. Изучить разработку и внедрение мер по минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях. Изучить настройку и работу с системами обнаружения и предотвращения сетевых вторжений для раннего обнаружения и предотвращения угроз безопасности.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10, компьютер с доступом к Интернету, Oracle VM Virtual Box, виртуальная машина под управлением Windows 2008 Server, имя сервера DC2 и виртуальная машина под управлением Windows 7, объединенные в локальную сеть.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание 1. Установка VPN-PPTP сервера на Windows 2008 Server.

Задание 2. Настройка VPN-PPTP клиента на операционной системе Windows 7.

Задание №3 Провести работу с механизмами шифрования и аутентификации для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам.

Задание №4 Настроить и использовать фаерволов и межсетевые экраны для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.

Задание №5 Проанализировать содержимое трафика и контролировать приложения и пользователей в системах безопасности сети с использованием программного обеспечения для мониторинга и обнаружения угроз.

Задание №6 Разработать и внедрить меру по минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях.

Задание №7 Настроить и работать с системами обнаружения и предотвращения сетевых вторжений для раннего обнаружения и предотвращения угроз безопасности.

Контрольные вопросы

1. Система обнаружения вторжений - это …
2. Типы технологий IDS: …
3. Основные режимы работы программы Snort: …
4. Принцип работы программы WinPatrol: …
5. MJ Registry Watcher – это …
6. Какие протоколы поддерживает VPN сервер Windows 2008 Server?

Перечислите основные шаги, необходимые для установки VPN сервера?

7. Перечислите основные шаги, необходимые для создания VPN подключения на Windows 7?
8. Возможно ли использование сертификатов для шифрования трафика VPN?
9. В каком из протоколов VPN используется алгоритм Диффи –Хеллмана?
10. Может ли Windows 7 выступать в роли VPN сервера?
11. Что такое фаерволов и для чего он нужен?
12. Какое вы знаете программные обеспечения для мониторинга и обнаружения угроз?

Практическая работа №12

Тема: «Настройка и использование виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам. Настройка и работа с системами управления доступом для контроля доступа к корпоративной сети. Обеспечение безопасности Wi-Fi-сетей: настройка безопасных точек доступа, использование сетевой аутентификации, шифрования трафика и других методов. Разработка и внедрение мер по обеспечению безопасности электронной почты в корпоративной сети: настройка антивирусного программного обеспечения, проверка на наличие вредоносных вложений, обучение пользователей основам безопасности электронной почты. Обучение пользователям основам защиты от атак типа "фишинг". Работа с антивирусным программным обеспечением для защиты от вирусов и других вредоносных программ: установка, настройка, обновление базы данных, сканирование и удаление вредоносных программ».

Цель: Изучить настройку и использование виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам. Изучить настройку и работу с системами управления доступом для контроля доступа к корпоративной сети. Изучить обеспечение безопасности Wi-Fi-сетей: настройка безопасных точек доступа, использование сетевой аутентификации, шифрования трафика и других методов. Изучить разработку и внедрение мер по обеспечению безопасности электронной почты в корпоративной сети: настройка антивирусного программного обеспечения, проверка на наличие вредоносных вложений, обучение пользователей основам безопасности электронной почты. Изучить обучение пользователям основам защиты от атак типа "фишинг". Изучить работу с антивирусным программным обеспечением для защиты от вирусов и других вредоносных программ: установка, настройка, обновление базы данных, сканирование и удаление вредоносных программ.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10, компьютер с доступом к Интернету, антивирусная программа.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание №1 Настроить и использовать виртуальные части сетей (VPN) для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам.

Задание №2 Настроить и работать с системами управления доступом для контроля доступа к корпоративной сети.

Задание №3 Обеспечить безопасность Wi-Fi-сетей: настроить безопасные точеки доступа, использование сетевой аутентификации, шифрования трафика и других методов.

Задание №4 Разработать и внедрение мер по обеспечению безопасности электронной почты в корпоративной сети: настройка антивирусного программного обеспечения, проверка на наличие вредоносных вложений, обучение пользователей основам безопасности электронной почты.

Задание №5 Обучить пользователя основам защиты от атак типа "фишинг".

Задание №6 Работать с антивирусными програмнами обеспечениями для защиты от вирусов и других вредоносных программ: установка, настройка, обновление базы данных, сканирование и удаление вредоносных программ.

Контрольные вопросы.

1. Как настраивается виртуальные части сетей (VPN) для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам?
2. Как настроить работу с системами управления доступом для контроля доступа к корпоративной сети?
3. Как обеспечивается безопасность Wi-Fi-сетей?

4. Как разрабоываются и внедряются меры по обеспечению безопасности электронной почты в корпоративной сети?

5. Что такое атака типа "фишинг"?

6. Как устанавливаются, настраиваются, обновляются базы данных, сканируются и удаляются вредоносные программы антивирусных программ?

Практическая работа №13

Тема: «Настройка и использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности. Настройка и использование межсетевых экранов и фаерволов для обеспечения комплексной защиты корпоративной сети от несанкционированного доступа через Интернет. Внедрение системы управления доступом для контроля доступа к корпоративной сети: настройка правил доступа, аутентификация пользователей, управление привилегиями. Использование технологий виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа: настройка и управление VPN-туннелями, защита данных, маршрутизация трафика».

Цель: Изучить настройку и использование систем обнаружения вторжений для раннего обнаружения, и предотвращения угроз безопасности. Изучить настройку и использование межсетевых экранов и фаерволов для обеспечения комплексной защиты корпоративной сети от несанкционированного доступа через Интернет. Изучить внедрение системы управления доступом для контроля доступа к корпоративной сети: настройка правил доступа, аутентификация пользователей, управление привилегиями. Изучить использование технологий виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа: настройка и управление VPN-туннелями, защита данных, маршрутизация трафика.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10, компьютер с доступом к Интернету.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Ход работы.

Задание №1 Настроить и использовать системы обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.

Задание №2 Настроить и использовать межсетевые экраны и фаервол для обеспечения комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.

Задание №3 Внедрить системы управления доступом для контроля доступа к корпоративной сети: настройка правил доступа, аутентификация пользователей, управление привилегиями.

Задание №4 Использовать технологии виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа: настройка и управление VPN-туннелями, защита данных, маршрутизация трафика.

Контрольные вопросы.

1. Как работает система обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности?
2. Перечислите основные этапы настроики и использование межсетевых экранов и фаервол для обеспечения комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.
3. Что такое аутентификация пользователей?
4. Что такое виртуальные частные сети? Зачем нужен удаленный доступ и принцип его работы?

Практическая работа №14

Тема: «Обеспечение безопасности Wi-Fi-сетей: настройка и управление беспроводными точками доступа, защита сетевого трафика, аутентификация пользователей. Защита от DDoS-атак: использование специализированных средств защиты от DDoS-атак, настройка маршрутизации трафика, мониторинг сетевой активности. Реализация мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети:

настройка политик безопасности для мобильных устройств, управление устройствами и приложениями, защита данных на устройствах. Обеспечение безопасности облачных сервисов: выбор надежных провайдеров облачных сервисов, настройка правил доступа и аутентификации, шифрование данных, мониторинг активности в облачных сервисах».

Цель: Изучить обеспечение безопасности Wi-Fi-сетей: настройка и управление беспроводными точками доступа, защита сетевого трафика, аутентификация пользователей. Изучить защиту от DDoS-атак: использование специализированных средств защиты от DDoS-атак, настройка маршрутизации трафика, мониторинг сетевой активности. Изучить реализацию мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети: настройка политик безопасности для мобильных устройств, управление устройствами и приложениями, защита данных на устройствах. Изучить обеспечение безопасности облачных сервисов: выбор надежных провайдеров облачных сервисов, настройка правил доступа и аутентификации, шифрование данных, мониторинг активности в облачных сервисах.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10, компьютер с доступом к Интернету.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание №1 Обеспечить безопасность Wi-Fi-сетей: настройка и управление беспроводными точками доступа, защита сетевого трафика, аутентификация пользователей.

Задание №2 Защитить от DDoS-атак: использование специализированных средств защиты от DDoS-атак, настройка маршрутизации трафика, мониторинг сетевой активности.

Задание №3 Реализовать меру по обеспечению безопасности мобильных устройств, используемых в корпоративной сети: настройка политики безопасности для мобильных устройств, управление устройствами и приложениями, защита данных на устройствах.

Задание №4 Обеспечить безопасность облачных сервисов: выбор надежных провайдеров облачных сервисов, настройка правил доступа и аутентификации, шифрование данных, мониторинг активности в облачных сервисах.

Контрольные вопросы.

1. Как настраивается Wi-Fi-сеть?
2. Что такое DDoS-атака?
3. Назавите все настройки политики безопасности для мобильных устройств?
4. Что такое облачный сервис и как настраиваются правила доступа?

Практическая работа №15

Тема: «Финальная комплексная лабораторная работа по безопасности».

Цель: Применить на практике получение навыки и знания при выполнении итоговой работы.

Оборудование и наглядные пособия: учебные пособия, литература, персональный компьютер, операционная система Windows 10, компьютер с доступом к Интернету.

Формируемые компетенции: ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. **ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.**

Ход работы.

Задание:

Выберете тематику по безопасность компьютерных сетей из нижеперечисленных:

1) Изучение методики комплексной оценки безопасности;
2) Комплексная оценка безопасности;
3) Что изучетс социальная инженерия.
4) Настройте безопасный доступ к маршрутизатору.

5) Настройте систему предотвращения вторжений (IPS).

6) Настройте Site-to-SiteVPN используя интерфейс командной строки

7) Проведите базовую настройку шлюза безопасности ASA и настройте брандмауэров используя ASDM.

8). Настройте Clientless Remote Access SSL VPNs используя ASDM.

9) Отчет о проделанной работе.

Контрольные вопросы

1. Дайте определение социальной инженерии.

2. Опишите как происходит настройка безопасного доступа к маршрутизатору.

3. Опишите поэтапно настройку системы предотвращения вторжений (IPS).

4. Как производиться проверка базовой настройки шлюза безопасности ASA и настройка брандмауэров используя ASDM.

5. Опишите какие производятся настройка Site-to-SiteVPN используя интерфейс командной строки.

6. Как проводится настройка Clientless Remote Access SSL VPNs используя ASDM.

Критерии оценки:

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если не выполнена одна часть задания, выводы сделаны правильно

3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

Виды работ практики и проверяемые результаты обучения по профессиональному модулю

Учебная практика

Виды работ	**Проверяемые результаты: требования к практическому опыту и коды формируемых ПК,**	**Документ, подтверждающий качество выполнения работ**

	ОК, умений (ПО, ПК, ОК,У)	
Охрана труда для системного администратора. Изучить инструктаж по технике безопасности при работе с компьютером и его периферией. Организовывать рабочее место. Подключить ПК. «*Общие требования охраны труда. Требования охраны труда перед началом работы. Требования охраны труда во время работы. Требования охраны труда в аварийных ситуациях. Требования охраны труда по окончании работы*». *Настройка прав доступа. Оформление технической документации, правила оформления документов.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	Аттестационный лист по учебной практике
Настройка аппаратного и программного обеспечения сети. Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain.	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
Программная диагностика неисправностей. Аппаратная диагностика неисправностей. Устранение паразитирующей нагрузки в сети. *Поиск неисправностей технических средств. Выполнение действий по устранению неисправностей. Использование активного, пассивного оборудования сети.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
Построение физической карты локальной сети. Установка WEB-сервера. Диагностика и обслуживание Web сервера. *Диагностика и обслуживание файлового сервера. Диагностика и обслуживание почтового сервера. Диагностика и обслуживание SQL – сервера. Конфигурирование web-сервера. Запуск, перезапуск и останов сервера.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
Взаимодействие с базами данных. Установка брандмауэра. *Сохранение и восстановление больших наборов правил. Обеспечение безопасности.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	

Администрирование серверов и рабочих станций. *Организация доступа к локальным сетям и Интернету. Установка и сопровождение сетевых сервисов.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
Подключение к оборудованию CISCO. Настройка подключения по Telnet и SSH. *Создание одноранговой и клиент-серверной сети. Знакомство PDU и BPDU пакетами на различных уровнях модели OSI в сетевом симуляторе CISCO Packet tracer. Агрегация каналов. Изучение STP и RSTP протоколов OSI в сетевом симуляторе CISCO Packet tracer. Расчёт стоимости сетевого оборудования и программного.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
IPv4 адресация, маска подсети. Решение задач на разбиение сети на подсети. IPv6 адресация, маска подсети. Решение задач на разбиение сети на подсети. *Маршрутизация в IPv4 пространстве адресов. Маршрутизация в IPv6 пространстве адресов.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
Изучение демилитаризованная зоны - реализация на маршрутизаторе с использованием zone based firewall.	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
Разработка алгоритма и интерфейса программы анализа информационных рисков и её тестирование. *Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации. *Организация защищенных каналов передачи данных для объединения территориально распределенных офисов в одну сеть*.	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
Разработка политик безопасности и внедрение их в операционные системы.	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7.	

Обеспечение безопасности Wi-Fi-сетей.	ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
Настройка ipsec и VPN. Настройка межсетевых экранов. *Реализация мер по обеспечению безопасности электронной почты в корпоративной сети*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств. *Защита от атак типа "фишинг".*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
Настройка защиты беспроводных сетей с помощью систем шифрования.	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
Архивация и восстановление ключей в windowsserver (PKI).	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
Установка и настройка системы обнаружения атак Snort. Работа со встроенными сканерами диагностики и управления. Обеспечение сетевой безопасности.	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	

Производственная практика

Виды работ	**Проверяемые результаты: требования к практическому опыту и коды формируемых профессиональных, общих компетенций, умений(ПО, ПК, ОК,У)**	**Документ, подтверждающий качество выполнения работ**
1. Вводный инструктаж по ТБ и ПБ. Знакомство с предприятием. *Общие требования охраны труда. Требования охраны труда перед*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5.	Аттестационный лист по производственной практике

началом работы. Требования охраны труда во время работы. Требования охраны труда в аварийных ситуациях. Требования охраны труда по окончании работы. Основные правила гигиены труда и внутреннего распорядка. Рациональные приемы работы и способы организации труда и рабочего места. Составление структуры предприятия. Определение функций специалистов предприятия. Определение перспективы развития производства. Составление плана освоения новых технологий. Организационная структура предприятия / организации, базового подразделения. Круг решаемых задач. Используемое программное обеспечение. Функции и назначения подразделений предприятия / организации. Производственные связи между структурными подразделениями объекта практики. Перечень и конфигурация технических средств вычислительной техники виды вычислительной техники, их характеристики, средства коммуникаций, оснащение техническими средствами работников предприятия.	У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
2. Ознакомление с проводимыми на ЛВС предприятия регламентные технические осмотры объектов сетевой инфраструктуры. *Определение проведения на предприятии мониторинга и анализа работы локальной сети и регулярное резервирование. Перечень и назначение программных средств, установленных на ПК предприятия*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
3. Знакомство с архитектурой системы управления сетью предприятия. *Структуры системы управления сетью. Архитектура сети.* *Использование удалённого администрирования в управлении сетью предприятия. Управление отказами. Выявление, определение и*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	

устранение последствий сбоев и отказов в работе сети. Настройка активного и пассивного сетевого оборудования. Построение физической топологии сети Проведение профилактического обслуживания оборудования компьютерных сетей.		
4. Используемые программные или аппаратно-программные системы в сетях предприятия. *Функции мониторинга, анализ трафика в сетях предприятия. Выявление причин аномальной работы сети предприятия.* *Приведения сети в работоспособное состояние. Локализации неисправностей сети. Контрольно-измерительная аппаратура предприятия.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
5. Применение хранилищ данных и резервного копирования данных на предприятии.	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
6. Применение и методы аутентификации, авторизации и администрирования действий пользователей в локальной сети. *Применение и используемые методы криптографической защиты информации и электронной цифровой подписи. Управление подсистемой контроля входа в ЛВС предприятия.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
7. Использование виртуальных защищённых сетей VPN. *Управление подсистемой управления доступом к БД предприятия. Технологии анализа защищённости и обнаружения атак. Администрирование баз данных, создание, редактирование, заполнение таблиц.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
8. Установка на серверы и рабочие станции: операционные системы и необходимое для работы программное обеспечение. *Анализ журналов операционной системы, контроль доступа, обеспечение целостности и сохранности данных.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	

9. Осуществление конфигурирования программного обеспечения на серверах и рабочих станциях.	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
10. Поддержка в работоспособном состоянии программное обеспечение серверов и рабочих станций.	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
11. Регистрация пользователей локальной сети и почтового сервера, назначает идентификаторы и пароли. *Настройка и применение протоколов управления сетью. Мониторинг и анализ сетевого трафика и сетевых узлов.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
12. Установка прав доступа и контроль использования сетевых ресурсов. *Участие в настройке и управлении доступом, производительностью, безопасностью, ошибками. Настройка беспроводных локальных сетей. Управление учетными записями в доменной сети. Удаленное управление рабочими станциями и серверным оборудованием.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
13. Обеспечение своевременного копирования, архивирования и резервирования данных.	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
14. Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования. *Применение диагностического оборудования. Участие в планировании восстановительных работ после сбоя.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
15. Выявление ошибок пользователей и программного обеспечения и принятие мер по их исправлению. *Разработка функциональных схем элементов автоматизированной системы защиты информации.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	

16. Проведение мониторинга сети, разрабатывать предложения по развитию инфраструктуры сети. *Анализ входящего и исходящего трафика.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
17. Работа с кабельными сканерами и тестерами	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
18. Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия. *Участие в разработке регламентов профилактических осмотров. Мониторинг и анализ сети с применением программных и аппаратных средств. Контроль утечки конфиденциальной информации, участие в разработке политик безопасности. Настройка систем обнаружения атак.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
19. Осуществление антивирусной защиты локальной вычислительной сети, серверов и рабочих станций. *Установка и настройка средств обеспечения антивирусной защиты для Веб и почтового трафика.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
20. Документирование всех произведенных действий. *Заполнение технической документации.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	
21. Подготовка отчетной документации по практике. *Оформление отчетной документации по итогам производственной практики в соответствии с требованиями. Сдача отчетной документации по практике.*	ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9. ПО. У1. У2. У3. У4. У5. У6. У7. У8. У9. У10. У11. У12. У13. У14. У15. У16. У17. У18.	

3.2. КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРЕМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Промежуточная аттестация является основной формой контроля в период обучения обучающихся. Периодичность, формы и сроки проведения промежуточной аттестации определяются учебным планом по специальности.

Перечень форм промежуточной аттестации по элементам профессионального модуля

Элемент модуля	**Формы промежуточной аттестации**
МДК.03.01	Экзамен
МДК.03.02	Экзамен
УП.03.01	Дифференцированный зачет
ПП.03.01	Дифференцированный зачет
ПМ.03(в целом)	Экзамен квалификационный

3.2.1. Материалы для проведения промежуточной аттестации

Материально-техническое обеспечение контрольно-оценочных мероприятий Эксплуатации объектов сетевой инфраструктуры

Оборудование учебного кабинета:

- рабочее место преподавателя;
- посадочные места по количеству студентов;

Технические средства обучения:

- компьютер с программным обеспечением
- мультимедийный проектор
- мультимедийное оборудование;

– принтер лазерный;

– сканер;

– аудиосистема;

– локальная сеть;

– подключение к глобальной сети Интернет;

Итоговый контроль освоения вида профессиональной деятельности **Эксплуатация объектов сетевой инфраструктуры** осуществляется на экзамене (квалификационном). Условием допуска к экзамену

(квалификационному) является положительная аттестация по МДК, учебной практике и производственной практике.

Экзамен (квалификационный) проводится в виде выполнения теоретических и практических заданий.

Промежуточный контроль освоения профессионального модуля осуществляется при проведении экзамена по МДК, дифференцированного зачета учебной и производственной практике. Предметом оценки освоения МДК являются умения и знания.

Условием положительной аттестации (вид профессиональной деятельности освоен) на экзамене квалификационном является положительная оценка освоения всех профессиональных компетенций по всем контролируемым показателям. При отрицательном заключении хотя бы по одной из профессиональных компетенций принимается решение «вид профессиональной деятельности не освоен».

Промежуточный контроль освоения профессионального модуля осуществляется при проведении дифференцированного зачета по МДК и дифференцированного зачета по учебной и производственной практике. Предметом оценки освоения МДК являются умения и знания.

Предметом оценки по учебной и (*или*) производственной практике является приобретение практического опыта *(может быть также освоение общих и профессиональных компетенций, умений, в зависимости от этого далее надо использовать различные формы)*.

Контроль и оценка по учебной и (или) производственной практике проводится на основе характеристики обучающегося с места прохождения практики, составленной и завизированной представителем образовательного учреждения и ответственным лицом организации (базы практики).

Здания для оценки освоения учебной дисциплины (промежуточная аттестация)

МДК 03.01. Эксплуатация объектов сетевой инфраструктуры

ПК, ОК, формируемые в процессе выполнения практических работ ПК

3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Билет №1.

1. Физические аспекты эксплуатации.

2. Настройка H.323. Описание H.323 и общие рекомендации.

3. Оконцовка кабеля витая пара

Билет №2.

1. Полоса пропускания, паразитная нагрузка.

2. Настройка SIP. Описание и общие рекомендации.

3. Заделка кабеля витая пара в розетку

Билет №3.

1. Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.

2. Функциональные компоненты H.323.Установка и поддержка соединения H.323.

3. Настройка аппаратных IP-телефонов.

Билет №4.

1. Физическое вмешательство в инфраструктуру сети.

2. Технология SIP и связанные с ней стандарты.

3. Кроссирование и монтаж патч-панели в коммутационный шкаф, на стену

Билет №5.

1. Расширяемость сети.

2. Соединения без и с использованием GateKeeper. Соединения с использованием нескольких GateKeeper.

3. Настройка программных IP-телефонов, факсов.

Билет №6.

1. Масштабируемость сети.

2.. Организация эксплуатации систем IP-телефонии.

3. Тестирование кабеля.

Билет №7.

1. Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб).

2. Многопользовательские конференции. Обеспечение отказоустойчивости.

3. Развертывание сети с использованием VLAN для IP-телефонии.

Билет №8.

1. Наращивание длины сегментов сети; замена существующей аппаратуры.

2. Функциональные компоненты SIP.

3. Настройка шлюза.

Билет №9.

1. Техническая и проектная документация.

2. Управление программным коммутатором.

3. Поддержка пользователей сети.

Билет №10.

1. Увеличение количества узлов сети; увеличение протяженности связей между объектами сети.

2. Сообщения SIP. Адресация SIP. Модель установления соединения. Планирование отказоустойчивости.

3. Установка, подключение и первоначальные настройки голосового маршрутизатора.

Билет №11.

1. Паспорт технических устройств.

2. Установка и инсталляция программного коммутатора.

3. Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы).

Билет №12.

1. Физическая карта всей сети; логическая топология компьютерной сети.

2. Монтажные процедуры коммутатора. Процедуры инсталляции. Управление аппаратными средствами и портами.

3. Настройка таблицы пользователей в голосовом маршрутизаторе.

Билет №13.

1. Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры.

2. Протоколы управления MGCP, H.248.

3. Настройка групп в голосовом маршрутизаторе.

Билет №14.

1. Проверка объектов сетевой инфраструктуры и профилактические работы

2. Создание аналоговых абонентов. Внутристанционная маршрутизация.

3. Настройка таблицы маршрутизации вызовов в голосовом Маршрутизаторе.

Билет №15.

1. Проведение регулярного резервирования.

2. Маршрутизация. Группы соединительных линий.

3. Выполнение действий по устранению неисправностей технических средств сетевой инфраструктуры.

Билет №16.

1. Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения о неполадках.

2. Подключение станций с TDM (абонентский доступ TDM).

3. Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.

Билет №17.

1. Программное обеспечение мониторинга компьютерных сетей и сетевых устройств.

2. Сигнализация SIP, SIP-T, H.323 и SIGTRAN.

3. Настройка голосовых сообщений в маршрутизаторе.

Билет №18.

1. IP-абоненты. Группы абонентов. Дополнительные абонентские услуги.

2. Протокол SNMP, его характеристики, формат сообщений, набор услуг.

3. Протокол управления SNMP.

Билет №19.

1. Задачи управления: анализ производительности и надежности сети.

2. Техническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт систем IP-телефонии.

3. Настройка программно-аппаратной IP-АТС.

Билет №20.

1. Оборудование для диагностики и сертификации кабельных систем.

2. Восстановление работы сети после аварии.

3. Основные характеристики протокола SNMP.

Билет №21.

1. Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.

2. Схемы послеаварийного восстановления работоспособности сети, техническая и проектная документация, способы резервного копирования данных, принципы работы хранилищ данных.

3. Установка и настройка программной IP-АТС (например, Asterisk).

Билет. №22.

1. Оформление технической документации, правила оформления документов.

2. Установка Active Directory в сети Windows.

3. Тестирование кодеков. Исследование параметров качества обслуживания.

Билет №23.

1. Проверка объектов сетевой инфраструктуры и профилактические работы.

2. Выявление, определение и устранение последствий сбоев и отказов в работе сети.

3. Набор услуг (PDU) протокола SNMP.

Билет №24.

1. Программные или аппаратно-программные системы, функции мониторинга, анализ трафика в сетях.

2. Встроенные системы диагностики и управления.

3. Мониторинг и анализ соединений по различным протоколам.

Билет №25.

1. Оборудование для диагностики и сертификации кабельных систем

2. Маркировка кабельных жгутов.

3. Формат сообщений SNMP.

Билет №26.

1. Маркирующие элементы, процессе эксплуатации объектов сетевой инфраструктуры.

2. Работа с объектами администрируемой СКС.

3. Мониторинг вызовов в программном коммутаторе.

Билет №27.

1. Базовые функции сканеров PVMax.

2. Классы и уровни администрирования.

3. Задачи управления: анализ производительности сети.

Билет №28.

1. Маркировка коммутационных панелей и розеток.

2. Сервера и рабочие станции системы управления iTracs.

3. Создание резервных копий баз данных.

Билет №29.

1. Проведение регламентных и ремонтных работ.

2. Аппаратная часть решения FuturePatch.

3. Задачи управления: анализ надежности сети.

Билет №30.

1. Типы волоконно-оптических (ВО) линий связи. Состав оборудования типового ВО-канала связи.

2. Специализированное программное обеспечение типа - МС решения FuturePatch.

3. Диагностика и устранение неисправностей в системах IP-телефонии.

МДК.03.02. Безопасность компьютерных сетей.

ПК, ОК, формируемые в процессе выполнения практических работ ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Билет №1

1. Фундаментальные принципы безопасной сети.

2. Реализация технологий брандмауэра.

3. Социальная инженерия.

Билет №2

1. Современные угрозы сетевой безопасности.

2. Безопасный доступ к устройствам.

3. Исследование сетевых атак и инструментов проверки защиты сети.

Билет №3

1. Криптографические системы.

2. Обеспечение безопасности пользовательских компьютеров.

3. Настройка безопасного доступа к маршрутизатору.

Билет №4

1. Вирусы, черви и троянские кони. Методы атак.

2. Реализация технологий предотвращения вторжения.

3. Обеспечение административного доступа AAA и сервера Radius.

Билет №5

1. Безопасность Сетевых устройств OSI.

2. Криптографические сервисы.

3. Настройка политики безопасности брандмауэров.

Билет №6

1. Безопасность локальной сети.

2. Базовая целостность и аутентичность.

3. Настройка системы предотвращения вторжений (IPS).

Билет №7

1. Назначение административных ролей.

2. Реализация технологий VPN.

3. Настройка безопасности на втором уровне на коммутаторах.

Билет №8

1. VPN. GRE VPN. Компоненты и функционирование IPSec VPN.

2. Соображения по безопасности второго уровня (Layer-2).

3. Исследование методов шифрования.

Билет №9

1. Управление безопасной сетью.

2. Конфиденциальность в криптографии.

3. Настройка Site-to-SiteVPN используя интерфейс командной строки.

Билет №10

1. Принципы безопасности сетевого дизайна.

2. Конфигурация безопасности второго уровня.

3. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки.

Билет №11

1. Введение в Адаптивное устройство безопасности ASA.

2. Безопасная архитектура.

3. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM.

Билет №12

1. Реализация Site-to-site IPSec VPN с использованием CLI.

2. Криптография открытых ключей.

3. Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM.

Билет №13

1. Управление процессами и безопасность.

2. Безопасность беспроводных сетей, VoIP и SAN.

3. Настройка Clientless Remote Access SSL VPNs используя ASDM.

Билет №14

1. Конфигурация фаирвола на базе ASA с использованием графического интерфейса ASDM.

2. Тестирование сети на уязвимости.

3. Настройка AnyConnect Remote Access SSL VPN используя ASDM.

Билет №15

1. Непрерывность бизнеса, планирование восстановления аварийных ситуаций.

2. Реализация Site-to-site IPSec VPN с использованием CCP.

3. Расчёт стоимости сетевого оборудования и программного.

Билет №16

1. IPS технологии.

2. ACL. Технология брандмауэра.

3. Установка и сопровождение сетевых сервисов.

Билет №17

1. Жизненный цикл сети и планирование.

2. Конфигурация VPN на базе ASA с использованием графического интерфейса ASDM.

3. Диагностика и обслуживание SQL – сервера.

Билет №18

1. Реализация Remote-access VPN.

2. Авторизация, аутентификация и учет доступа (AAA).

3. Диагностика и обслуживание файлового сервера.

Билет №19

1. Мониторинг и управление устройствами.

2. IPS сигнатуры.

3. Диагностика и обслуживание почтового сервера.

Билет №20

1. Использование функция автоматизированной настройки безопасности.

2. Свойства AAA.

3. Настройка прав доступа.

Билет №21

1. Реализация IPS.

2. Разработка регламентов компании и политик безопасности.

3. Поиск неисправностей технических средств.

Билет №22

1. Проверка и мониторинг IPS.

2. Локальная AAA аутентификация.

3. Решение задач на разбиение сети на подсети.

Билет №23

1. Контекстный контроль доступа (CBAC).

2. Server-based AAA.

3. Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain.

Билет №24

1. Политики брандмауэра основанные на зонах.

2. Охране труда для системного администратора.

3. Настройка ipsec и VPN.

Билет №25

1. Изучить инструктаж по технике безопасности при работе с компьютером и его периферией.

2. Взаимодействие с базами данных.

3. Настройка аппаратного и программного обеспечения сети.

Билет №26

1. Организовывать рабочее место.

2. Оформление технической документации, правила оформления документов.

3. Программная диагностика неисправностей

Билет №27

1. Требования охраны труда перед началом работы.

2. Использование активного, пассивного оборудования сети.

3. Аппаратная диагностика неисправностей.

Билет №28

1. Требования охраны труда во время работы.

2. Администрирование серверов и рабочих станций.

3. Настройка защиты беспроводных сетей с помощью систем шифрования.

Билет №29

1. Настройка межсетевых экранов.

2. IPv4 адресация, маска подсети.

3. Анализ входящего и исходящего трафика

Билет №30

1. Подключение к оборудованию CISCO.

2. Организация доступа к локальным сетям и Интернету.

3. Разработка политик безопасности и внедрение их в операционные системы.

3.2.2 Оценка приобретения практического опыта по учебной и производственной практике профессионального модуля.

Целью оценки по учебной и производственной практике является оценка профессиональных и общих компетенций, практического опыта и умений. Оценка по учебной и производственной практике выставляется на основании результатов выполнения комплексной практической работы и данных аттестационного листа (характеристики профессиональной деятельности обучающегося на практике) с указанием видов работ, выполненных обучающимся во время практики, их объема, качества выполнения в соответствии с технологией и требованиями организации, в которой проходила практика

Задания для промежуточной аттестации по учебной практике, для оценки сформированности общих и профессиональных компетенций

Дифференцированный зачёт.

Тестирование.

Тестовое задание.

По УП.03.01 Учебная практика «Эксплуатация объектов сетевой инфраструктуры»

<u>Вариант 1</u>

Количество вопросов – 30. Возможны несколько правильных ответов

1) Протокол SIP в стеке протоколов TCP/IP находится на

1. транспортном уровне;
2. прикладном уровне;
3. сетевом уровне;
4. уровне звена данных.

2) Провайдер расширил функционал своих услуг за счет введения нового но еще незарегистрированного в IANA функционала. Смогут ли внешние пользователи обращаясь к внутренним пользователям провайдера воспользоваться этим дополнительным функционалом? *(Ответ считается верным, если отмечены все правильные варианты ответов.)*

1. нет;
2. да, после регистрации в IANA;
3. да;

3) Протокол описания сеансов связи используется для

1. обмена между сторонами данными о функциональных возможностях сторон;
2. описания принимающей стороной ее функциональных возможностях;
3. описания передающей стороной ее функциональных возможностях;

4) С помощью какого протокола реализуется возможность превращения телефонного разговора в видео-звонок не прерывая сеанс связи?

1. SIP;
2. SDP;
3. H.323;

5) База данных адресной информации хранится в

1. сервере определения местоположения пользователей;
2. прокси-сервере;
3. сервере переадресации

6) Выберите верное утверждение. Прокси-сервера типа stateful

1. применяются для обслуживания большого количества клиентов;
2. предоставляют большее количество услуг чем сервер типа stateless;

3. работают быстрее чем сервер типа stateless;

7) Сервер переадресации предназначен для определения

1. общего адреса;

2. текущего адреса;

3. глобального адреса;

8) Сколько видов сигнальных сообщений определены в протоколе SIP?

1. 8;

2. 2;

3. 4;

4. 6.

5. 12

9) Обработка пользователей на сервере SIP телефонии может осуществляться

1. по разным правилам;

2. с помощью одних и тех-же правил определенных на этапе конфигурирования сервера;

10) Чем отличается соединение SIP с сервером переадресации от соединения SIP с прокси-сервером

1. сервер переадресации не выдает INVITE;

2. сервер переадресации опрашивает шлюзы ТфОп;

3. сервер переадресации не выдает ACK;

11) Принцип декомпозиции шлюза подразумевает:

1. разбиение функционала шлюза на блоки;

2. дополнение функционала шлюза отдельными функциональными блоками;

12) Контроллер сигнализации обеспечивает

(Ответ считается верным, если отмечены все правильные варианты ответов.)

1. функции управления шлюзами;

2. согласование между традиционной телефонной сетью и сетью IP;

3. обмен сигнальной информацией;

13) Устройство управления вызовами (CallAgent) выполняет следующие функции

1. доставку сигнальной информации;
2. преобразование речевой информации, поступающей со стороны ТфОП;
3. управление шлюзом;
4. кодирование и упаковку речевой информации в пакеты RTP/UDP/IP

14) Специализированные шлюзы получаются путем

1. объединения набора определенных команд;
2. назначения со стороны контроллеров;
3. адаптирования программ;

15) Контроллер сигнализаций CA управляет элементами с помощью

1. ASCII сообщений;
2. протокола UDP;
3. протокола SDP;

16) В классификации транспортных шлюзов (MediaGateways) – AccessGateway представляет из себя

1. шлюз, подключающий к IP-сети аналоговые, кабельные модемы, линии xDSL и широкополосные устройства беспроводного доступа;
2. шлюз для подключения к сети IP-телефонии небольшой учрежденческой АТС через аналоговый или цифровой интерфейс;
3. сервер доступа к IP-сети для передачи данных;
4. шлюз с цифровым интерфейсом для подключения к сети с маршрутизацией IP-пакетов учрежденческой АТС

17) Примером виртуального порта является

(Ответ считается верным, если отмечены все правильные варианты ответов.)

1. порт на удаленном сетевом оборудовании;
2. источник речевой информации в интерактивном речевом сервере;
3. программа-бот, синтезирующая голосовые сообщения

18) Connection означает

1. подключение порта к порту-инициатору соединения, которое создается между ним и другим портом;

2. подключение порта к одному из двух концов соединения,

которое создается между ним и другим портом;

3. подключение порта к порту-реципиенту соединения, которое создается между ним и другим портом.

19) При помощи протокола MGCP устройство управления и шлюз обмениваются командами представляющими из себя

1. набор текстовых строк;

2. последовательность спец-символов;

20) С помощью CallAgent можно определить

(Ответ считается верным, если отмечены все правильные варианты ответов.)

1. протокол абонента;

2. DMTF;

3. поднятие трубки абонента;

21) Объективными, измеряемыми или рассматриваемыми показателями качества являются *(Ответ считается верным, если отмечены все правильные варианты ответов.)*

1. время соединения;

2. пропускная способности сети;

3. время отклика;

4. изменение задержки в сети

22) Уменьшить задержку, вносимую сетью, можно за счет *(Ответ считается верным, если отмечены все правильные варианты ответов.)*

1. улучшения дизайна инфраструктуры;

2. выделения пакетов содержащих информацию реального времени;

3. увеличения количества провайдеров;

23) К достоинствам модели Diff-Serv можно отнести *(Ответ считается верным, если отмечены все правильные варианты ответов.)*

1. единое понимание метода обработки определенного трафика;

2. возможность анализа информационных потоков;

3. отсутствие необходимости резервирования ресурсов;

24) Отметьте обязательные элементы узла поддерживающего IntServ *(Ответ считается верным, если отмечены все правильные варианты ответов.)*

1. классификатор;

2. диспетчер пакетов;

3. протокол резервирования ресурсов;

4. блок управления доступом;

25) В случае модели IntServ объем ресурсов, которые необходимы маршрутизатору для обработки и хранения информации RSVP

1. увеличивается пропорционально количеству потоков QoS;

2. увеличивается логарифмически относительно количества потоков QoS;

3. уменьшается пропорционально количеству потоков QoS;

4. уменьшается экспоненциально относительно количества потоков QoS

26) Использование RSVP сеансов связи позволяет

(Ответ считается верным, если отмечены все правильные варианты ответов.).

1. автоматически освобождать ресурсы канала при завершении сеансов;

2. динамически распределять загрузку канала;

3. в случае невозможности вызова отмены освобождения средства протокола автоматически отменяют запрос на ресурсы;

27) MPLS позиционируется как

1. способ построения IP-магистралей с гарантированной доставкой;

2. способ построения высокоскоростных IP-магистралей;

3. способ построения надежных IP-магистралей;

4. способ построения емких IP-магистралей;

28) Укажите корректную последовательность методов обеспечения QoS в технологиях соответственно IntServ, DiffServ, MPLS

1. резервирование, приоретизация, перемаршрутизация;

2. перемаршрутизация, резервирование, приоретизация;

3. приоретизация, резервирование, перемаршрутизация;

29) Алгоритм LLQ служит для

1. обеспечения гарантированной доставки;

2. обеспечения малой задержки;

3. обеспечения полосы пропускания;

30) MPLS (многопротокольная коммутация по меткам) предназначена для

1. создания гомогенного трафика в транспортных сетях;

2. ускорения коммутации пакетов в транспортных сетях;

3. использования протокола RSVP-TE;

Ключи к тестам:

1-2	11-1	21-2,4
2-1,2	12-1,2,3	22-1,2
3-1	13-3	23-1,3
4-2	14-1	24-1,2,3,4
5-1	15-1	25-1
6-2	16-1	26-1,3
7-2	17-2,3	27-2
8-2	18-2	28-1
9-1	19-1	29-2
10-1	20-2,3	30-2

Критерии оценок:

Оценка «5» - ошибок нет (100% правильных ответов)

«4» - 1-4 ошибки (80-90% правильных ответов)

«3» - 5-9 ошибок (70% правильных ответов)

«2» - 10 ошибок (60% правильных ответов)

Безопасность компьютерных сетей

Вариант 1

Количество вопросов – 30. Возможны несколько правильных ответов

1) Работник отдела кадров небольшой компании отправил данные персонала генеральному директору по сети Интернет в другой город. Через час эти данные были известны ("выложены") большинству

пользователей Интернета. Что забыл установить системный администратор на сервере локальной сети организации? (Передача данных директором в сеть исключается). (*Выберите несколько вариантов ответа).*

1. Средства архивирования данных;
2. Защиту от несанкционированного доступа;
3. Средства криптографической защиты;
4. Средства антивирусной защиты;
5. VPN.

2) Основные группы технических средств ведения разведки (*Выберите несколько вариантов ответа).*

1. радиомикрофоны;
2. электронные «уши»;
3. фотоаппараты;
4. системы определения местоположения контролируемого объекта;
5. дистанционное прослушивание разговоров.

3) Уровень секретности - это

1. административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов;
2. ответственность за модификацию и НСД информации;
3. гриф конфиденциальности на документе;

4) Злоумышленник не смог преодолеть защиту ИС за установленный промежуток времени. Это параметр ИС называется....

1. Группа показателей защиты, соответствующая определенному классу защиты;
2. Прочность защиты в ИС;
3. Способность системы защиты информации обеспечить достаточный

уровень своей безопасности;

4. Время защиты информации.

5) Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется

1. системой защиты;

2. системой безопасности;

3. системой уничтожения;

4. системой угроз.

6) Разновидности угроз безопасности. (*Выберите несколько вариантов ответа).*

1. техническая разведка;

2. технические;

3. программно-математические;

4. физические;

5. программные;

6. организационные.

7) Информация может быть защищена без аппаратных и программных средств защиты с помощью

1. двоичных преобразований;

2. криптографических преобразований;

3. трансляционных преобразований;

4. специальных преобразований..

8) Что такое компьютерный вирус?

1. Разновидность программ, которые не работают;

2. Разновидность программ, которые не работают;

3. Разновидность программ, которые способны к размножению;

4. Разновидность программ, которые способны к размножению.

9) В организации имеется локальная сеть с выходом в Интернет. Что будет использовать системный администратор для обеспечения защиты передаваемой по сети информации?

1. средства резервного копирования;

2. средства идентификации и аутентификации;

3. средства антивирусной защиты;

4. средства криптографической защиты.

10) Абстрактное содержание какого-либо высказывания, описание, указание, сообщение либо известие - это

1. пароль;

2. данные;

3. текст;

4. информация;

11) При приеме на работу специалиста по информационной защите работодатель попросил указать законы России в области компьютерного права? *(Выберите несколько вариантов ответа)*

1. о гражданском долге;

2. о правовой ответственности;

3. О государственной тайне;

4. о правовой охране программ для ЭВМ и БД;

5. об информации, информатизации, защищенности информации;

6. об авторском праве и смежных правах;

7. оптическая.

12) Выделите группы, на которые делятся средства защиты информации:

1. химические, аппаратные, программные, криптографические, комбинированные;

2. физические, аппаратные, программные, этнографические, комбинированные;

3. физические, аппаратные, программные, криптографические, комбинированные.

13) Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?

1. операционной системы, сетевого программного обеспечения;

2. операционной системы, системы управления базами данных;

3. сетевого программного обеспечения и системы управления базами данных;

4. операционной системы, сетевого программного обеспечения и системы управления базами данных.

14) К угрозам какого характера относятся действия, направленные на сотрудников компании или осуществляемые сотрудниками компании с целью получения конфиденциальной информации или нарушения функции бизнес-процессов?

1. организационного;
2. кадрового;
3. административного;
4. бизнес-процессного.

15) С компьютеров компании периодически пропадает информация. В чем заключается основная причина потерь информации, связанной с ПК?

1. с глобальным хищением информации;
2. с недостаточной образованностью в области безопасности;
3. с появлением интернета.

16) Организационные угрозы подразделяются на: *(Выберите несколько вариантов ответа)*

1. физические угрозы;
2. угрозы воздействия на персонал;
3. несанкционированный доступ;
4. действия персонала;

17) Сжатие папки, файла или группы файлов без потери данных называется …

1. архивированием;
2. архивированием;
3. формализацией;
4. шифрованием;

18) К методам защиты от НСД относятся *(Выберите несколько вариантов ответа).*

1. разделение доступа;

2. разграничение доступа;

3. ограничение доступа;

4. ограничение доступа;

5. увеличение доступа;

19) Верификация -

1. это проверка принадлежности субъекту доступа предъявленного им идентификатора;

2. это присвоение имени субъекту или объекту;

3. это присвоение имени субъекту или объекту.

20) Линейное шифрование -

1. криптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому;

2. криптографическое преобразование информации в целях ее
защиты от ознакомления и модификации посторонними лицами;

3. несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу.

21) Системный администратор обнаружил, что в защите ИС возможны события, действия, процессы или явления, которые могут привести к ущербу интересов компании. Это называется ...

1. риском;

2. угрозой;

3. уязвимостью;

22) В крупной организации посторонний человек ознакомился (неизвестным нам способом) с секрет ной информацией. Это привело к крупной финансовой потере. Данная потеря информации называется

1. Утечка информации;

2. Потеря, хищение, разрушение или неполучение переданных данных;

3. Угроза.

23) Как подразделяются вирусы в зависимости от деструктивных возможностей?

1. Безвредные, неопасные, опасные, очень опасные;

2. Сетевые, файловые, загрузочные, комбинированные;

3. Резидентные, нерезидентные;

4. Полиморфные, макровирусы, вирусы-невидимки, "паразитические", "студенческие", "черви", компаньон-вирусы.

24) Административная и законодательная мера, соответствующая мере ответственности лица за потерю конкретной секретной информации, регламентированная специальным документом с учетом государственных и военно-стратегических, коммерческих или частных интересов - это...

1. Уровень секретности;

2. Уровень конфиденциальности;

3. Уровень защиты информации;

4. Уровень безопасности информации.

25) Служба (комплекс программ) в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам

1. Сервер комплексных запросов;

2. Сервер безопасности;

3. Прокси-сервер;

4. Сервер сетевых служб.

26) Под информационной безопасностью понимают

1. защиту от несанкционированного доступа;

2. защиту информации от компьютерных вирусов;

3. защиту информации от случайных и преднамеренных воздействий естественного и искусственного характера.

27) Вы пришли работать в крупную компанию. В компании был уволен системный администратор за передачу служебной информации в сеть Интернет. Что вы должны предпринять в первую очередь, для того чтобы оградить организацию от проникновения бывшего работника на сервер?

1. Сменить логин и пароль администратора сервера (предприятия, домена);

2. Удалить учетную запись администратора сервера;

3. Сменить логины и пароли всех учетных записей пользователей;

4. Переустановить ОС на сервере и создать новые учетные записи пользователей.

28) Сопоставьте определения

1. присвоение субъектам и объектам идентификатора и / или сравнение идентификатора с перечнем присвоенных идентификаторов;

2. процедура проверки подлинности, например: проверка подлинности пользователя путем сравнения введенного им пароля с паролем в базе данных пользователей;

_____Идентификация;

_____Аутентификация.

29) Установите соответствие

1. это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок;

2. это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной
информации за пределы контролируемой зоны в виде производственных или промышленных отходов;

3. это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей;

4. это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии.

_____Защита информации от утечки по электромагнитным каналам:

_____Защита информации от утечки по визуально-оптическому каналу;

_____защита информации от утечки по акустическому каналу;

_____Защита информации от утечки по материально-вещественному каналу.

30) Для отражения хакерских атак используется *(выберите несколько вариантов ответа)*

1. архиваторы (backup);

2. антивирусные программы;

3. VPN;

4. proxy;

5. межсетевые экраны.

Ключи к тестам:

1-2,3,5	11-3,4,5,6	21-2
2-1,2,4	12-3	22-2
3-1	13-4	23-1
4-2	14-1	24-1
5-1	15-2	25-3
6-1,3,6	16-2,4	26-3
7-2	17-1	27-1
8-3	18-1,2,3,4	28-1,2
9-4	19-3	29-1,4,3,2
10-4	20-1	30-2,5

Критерии оценок:

Оценка «5» - ошибок нет (100% правильных ответов)

«4» - 1-4 ошибки (80-90% правильных ответов)

«3» - 5-9 ошибок (70% правильных ответов)

«2» - 10 ошибок (60% правильных ответов)

Задания для промежуточной аттестации по производственной практики, для оценки сформированности общих и профессиональных компетенций

Дифференцированный зачёт.

Тестирование.

Тестовое задание.

По ПП.03.01 «Эксплуатация объектов сетевой инфраструктуры»

Вариант 1

Количество вопросов – 30. Возможны несколько правильных ответов

1) Какой тип коммутации используют ТфОП для функционирования?

1. коммутацию связей;

2. коммутацию каналов;

3. коммутацию пакетов;

4. коммутацию сообщений.

2) В случае установки модемного соединения со скоростью 56Кб, при передаче речи в режиме VoIP какое теоретическое количество одновременных разговоров можно провести, если использовать кодек G729?

1. 5 и более;

2. 6 и более;

3. 2 и более;

4. 7 и более;

3) Имея в наличии интернет соединение мы можем одновременно посылать или принимать *(Ответ считается верным, если отмечены все правильные варианты ответов.)*

1. данные в аналоговом формате;

2. обычные данные;

3. голосовые данные;

4. видеоданные;

4) Архитектура VoIP является:

1. проприетарной;

2. закрытой;

3. открытой;

4. полуоткрытой.

5) Протоколами IP-телефонии являются

(Ответ считается верным, если отмечены все правильные варианты ответов.):

1. MGCP;

2. H.323;

3. SIP

4. MPEG

6) В оцифровке голосового сообщения участвуют:

1. программные средства;

2. аппаратные и программные средства;

3. аппаратные средства;

4. информационные средства.

7) Качество упаковки голосового сообщения (используемого кодека)...

1. прямо пропорционально качеству передаваемого голосового сообщения;

2. не влияет на качество передаваемого голосового сообщения;

3. обратно пропорционально качеству передаваемого голосового сообщения;

4. равно качеству передаваемого голосового сообщения.

8) При осуществлении телефонного звонка посредством IP- телефона с голосовым сообщением происходит

1. оба преобразования и аналого-цифровое, и цифро- аналоговое;

2. только аналого-цифровое преобразование;

3. только цифро-аналоговое преобразование;

4. никаких преобразований.

9) IP-телефоном можно назвать

(Ответ считается верным, если отмечены все правильные варианты ответов.)

1. компьютер с микрофоном и колонками и запущенным программным обеспечением IP-телефонии;

2. связку стандартный телефон подключенный к IP-шлюзу;

3. специализированный терминал, имеющий вид обычного телефона с записанным в память программным обеспечением IP-телефонии;

10) Используя IP-телефонию, вы можете осуществлять телефонные звонки:

(Ответ считается верным, если отмечены все правильные варианты ответов.):

1. телефон-компьютер;

2. компьютер-компьютер;

3. телефон-телефон;

11) На сетевом уровне стека протоколов VoIP в качестве способа передачи голоса используется протокол:

1. IP;

2. MLPPP;

3. Ethernet;

4. FrameRelay.

12) На транспортном уровне стека протоколов VoIP добавляется *(Ответ считается верным, если отмечены все правильные варианты ответов.)*

1. определение транспорта передачи;

2. механизм установки очередности пакетов;

3. тип транспортируемого кодека;

4. механизм расстановки временных меток

13) Отметьте протоколы используемые на пятом уровне стека протоколов VoIP

(Ответ считается верным, если отмечены все правильные варианты ответов.)

1. H.323;

2. SDP;

3. UDP;

4. SIP

14) При осуществлении звонка с помощью IP-телефонии разговор считается приемлемым, в случае если задержка в одном направлении

1. не превышает 415мс;

2. не превышает 400мс;

3. не превышает 500мс;

4. Не превышает 700 мс;

15) Задержка кодирования или обработки зависит от

(Ответ считается верным, если отмечены все правильные варианты

ответов.).

1. используемого протокола;

2. типа операционной системы;

3. типа алгоритма обработки;

4. скорости работы процессора;

16) Является ли выбор операционной системы фактором, влияющим на общую величину задержки?

1. да;

2. нет;

17) Зачем производители оборудования используют в нём ОС реального времени?

1. для осуществления мониторинга в реальном режиме времени;

2. для снижения влияния ОС на возникающие задержки;

3. для возможности осуществления звонков в реальном времени

18) С помощью чего определяются пакеты пришедшие не в порядке очередности?

1. с помощью номера и сетевого адреса пакета;

2. с помощью номера пакета;

3. с помощью значений временных меток RTP-пакетов.

19) Временные задержки характерны для

(Ответ считается верным, если отмечены все правильные варианты ответов.).

1. телефонии использующей коммутацию пакетов;

2. IP-телефонии;

3. телефонии использующей коммутацию каналов;

20) Квантование это.

1. разбиение диапазона значений на конечное число интервалов;

2. разбитие сигнала по временной составляющей;

3. передача коротких пакетов (квантов) информации;

21) При переходе от цифрового вида к аналоговому сигнал преобразуется с помощью

1. АЦП;
2. АПК;
3. ЦАП;

22) H.323 предусматривает рекомендации

(Ответ считается верным, если отмечены все правильные варианты ответов.)

1. управление полосой пропускания;
2. поддержку групповой адресации;
3. поддержку многоточечных конференций;
4. стандарты для кодеков;

23) H.323 поддерживает многоадресную передачу. При многоадресной передаче

1. один пакет информации отправляется всем необходимым адресатам с дублированием;
2. один пакет информации отправляется всем необходимым адресатам без дублирования;
3. все пакеты информации отправляются методом каскадирования всем необходимым адресатам;

24) Какие протоколы используются терминалами для управления аутентификацией?

(Ответ считается верным, если отмечены все правильные варианты ответов.)

1. RTCP;
2. H.225;
3. H.245;
4. RAS;

25) Терминал H.323 в статическом режиме

1. обменивается с контроллерами сообщениями типа mGRQ;

2. запрашивает адрес контроллера;

3. адрес контроллера прописан в памяти терминала;

26) RAS-канал используется для реализации таких механизмов управления как

(Ответ считается верным, если отмечены все правильные варианты ответов.).

1. управление шириной полосы пропускания;

2. контроль аутентификации;

3. определение доменных имен;

4. обработка видеосигналов;

27) При отсутствии в сети шлюза

1. обязательно нужно реализовать функцию авторизации абонента;

2. обязательно нужно реализовать функцию гарантированной доставки пакетов;

3. обязательно нужно реализовать функцию преобразования номера ТфОП в транспортный адрес IP-сети;

4. обязательно нужно реализовать функцию АЦП преобразования;

28) MultipointProcessors (MP) отвечают за___потоков *(выберите несколько вариантов)*.

1. обработку;

2. согласование;

3. микширование;

29) Маршрутизация сигналов вызова является

(Ответ считается верным, если отмечены все правильные варианты ответов.)

1. обязательной возможностью контроллера зоны;

2. факультативной возможностью контроллера зоны;

3. возможностью реализуемой в шлюзе или в контроллере зоны;

30) Факультативные функции контроллера зоны

(Ответ считается верным, если варианты ответов.)

1. трансляция адреса;

2. управление полосой пропускания;

3. управление вызовами;

4. авторизация вызова;

Ключи к тестам:

1-2	11-1	21-3
2-4	12-2,4	22-1,2,3,4
3-2,3,4	13-1,2,4	23-2
4-3	14-2	24-2,4
5-1,2,3	15-3,4	25-3
6-2	16-1	26-1,2
7-3	17-2	27-3
8-1	18-3	28-1,3
9-1,2,3	19-1,2	29-2,3
10-1,2,3	20-1	30-3,4

Безопасность компьютерных сетей

Список вопросов теста 40.

Вопрос 1

Контроль целостности передаваемых по сетям данных осуществляется посредством ..

Варианты ответов

1. электронной цифровой подписи

2. аутентификации данных

3. аудита событий

4. межсетевого экранирования

Вопрос 2

Преобразовательный процесс, в ходе которого исходный текст (или открытый текст) заменяется изменённым текстом, называется

Варианты ответов

1. шифрование

2. дешифрование

3. преобразование

4. искажение

Вопрос 3

Процесс, в ходе которого шифрованный текст преобразуется в исходный, называется

Варианты ответов

1. шифрование
2. дешифрование
3. преобразование
4. искажение

Вопрос 4

Информация, необходимая для беспрепятственного шифрования и дешифрования текстов, называется (*напишите правильный ответ*):

_____

Вопрос 5

При симметричном шифровании для шифрования и расшифровки используются

Варианты ответов

1. два ключа разной длины
2. два разных по значению ключа
3. один и тот же ключ
4. два открытых ключа
5. два закрытых ключа
6. один открытый ключ и один закрытый ключ

Вопрос 6

Относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом, называется

Варианты ответов

1. закрытый ключ шифрования
2. электронная цифровая подпись
3. вирусная маска
4. открытый ключ шифрования

Вопрос 7

Криптосистема включает (*выбирите несколько вырианов ответа*):

Варианты ответов

1. алгоритм шифрования
2. набор ключей, используемых для шифрования
3. систему управления ключами
4. антивирусное ПО
5. межсетевой экран

Вопрос 8

Механизм безопасности, который является сильным психологическим средством, напоминающим потенциальным нарушителям о неотвратимости наказания за несанкционированные действия, а пользователям - за возможные критические ошибки

Варианты ответов

1. регистрация и аудит
2. аутентификация
3. идентификация
4. VPN
5. межсетевой экран

Вопрос 9

Главное свойство компьютерных вирусов заключается в возможности ...

Варианты ответов

1. их самопроизвольного внедрения в различные объекты операционной системы
2. нарушения информационной безопасности
3. заражения окружающих
4. уничтожения данных и компьютера

Вопрос 10

Вирусы, которые заражают файлы - документы и электронные таблицы офисных приложений, называются вирусы

Варианты ответов

1. файловые
2. сетевые
3. макро-
4. загрузочные

Вопрос 11

Вирусы, которые заражают файлы - документы и электронные таблицы офисных приложений, называются … вирусы (*напишите правильный ответ*):

_____

Вопрос 12

Самошифрование и полиморфичность используются для ...

Варианты ответов

1. саморазмножения вируса
2. максимального усложнения процедуры обнаружения вируса
3. расшифровки тел вируса
4. для скрытия действий антивирусной программы

Вопрос 13

Одним из наиболее эффективных способов борьбы с вирусами является ...

Варианты ответов

1. использование антивирусного программного обеспечения
2. использования операционной системы UNIX
3. ограничение доступа пользователей к ЭВМ
4. шифрование данных

Вопрос 14

Антивирусная программа, основанная на подсчёте контрольных сумм для присутствующих на диске файлов/системных секторов называется ...

Варианты ответов

1. иммунизатор
2. блокировщик
3. сканер

4. CRC-сканер

Вопрос 15

Антивирусная программа, перехватывающая «вирусоопасные» ситуации и сообщающая об этом пользователю, называется .

Варианты ответов

1. иммунизатор
2. блокировщик
3. сканер
4. CRC-сканер

Вопрос 16

Компьютерным вирусом является ...

Варианты ответов

1. полиморфик-генератор
2. утилита скрытого администрирования
3. макро-вирус
4. логическая бомба

Вопрос 17

Идентификация и аутентификации применяются для ...

Варианты ответов

1. регистрации событий безопасности
2. выявления попыток несанкционированного доступа
3. обеспечения целостности данных
4. для ограничения доступа случайных и незаконных субъектов информационной системы к её объектам

Вопрос 18

Анализ накопленной информации, проводимый оперативно, в реальном времени или периодически называется.

Варианты ответов

1. аудит
2. идентификация

3. аутентификации

4. шифрование

Вопрос 19

Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется.

Варианты ответов

1. активным

2. оперативным

3. неотложным

4. автоматическим

Вопрос 20

Аутентификация, которая использует динамические данные аутентификации, меняющиеся с каждым сеансом работы, называется

Варианты ответов

1. устойчивой

2. статической

3. постоянной

4. переменной

Вопрос 21

Программная или программно-аппаратная система, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации

Варианты ответов

1. межсетевой экран

2. иммунизатор

3. антивирусная программа

4. CRC-сканер

Вопрос 22

4 типа межсетевых экранов: ... (*выбирите несколько выриантов ответа*):

Варианты ответов

1. межсетевые экраны с фильтрацией пакетов
2. шлюзы сеансового уровня
3. шлюзы прикладного уровня
4. межсетевые экраны экспертного уровня
5. шлюзы физического уровня
6. межсетевые экраны канального уровня

Вопрос 23

Межсетевые экраны ... уровня сочетают в себе элементы всех трёх остальных категорий (*напишите правильный ответ*):

_____

Вопрос 24

Виртуальные частные сети включают следующие сервисы безопасности: ... (*выбирите несколько вырианов ответа*):

Варианты ответов

1. экранирование
2. шифрование
3. туннелирование
4. аудит
5. регистрацию и контроль доступа
6. электронную цифровую подпись

Вопрос 25

Для реализации технологии VPN на все компьютеры, имеющие выход в Интернет, устанавливаются VPN-…, которые обрабатывают IP-пакеты, передаваемые по вычислительным сетям (*напишите правильный ответ*):

_____

Вопрос 26

Межсетевой протокол, отвечающий за адресацию в сети Интернет -

Варианты ответов

1. IP
2. ICMP
3. ARP
4. RARP
5. UDP
6. TCP

Вопрос 27

Межсетевой протокол управления сообщениями

Варианты ответов

1. IP
2. ICMP
3. ARP
4. RARP
5. UDP
6. TCP

Вопрос 28

Протокол разрешения адресов, выполняющий преобразование логических сетевых адресов в аппаратные.

Варианты ответов

1. IP
2. ICMP
3. ARP
4. RARP
5. UDP
6. TCP

Вопрос 29

Протокол разрешения адресов, выполняющий преобразование аппаратных сетевых адресов в логические - …

Варианты ответов

1. IP

2. ICMP

3. ARP

4. RARP

5. UDP

6. TCP

Вопрос 30

Протокол управления передачей данных, использующий автоматическую повторную передачу пакетов, содержащих ошибки.

Варианты ответов

1. IP

2. ICMP

3. ARP

4. RARP

5. UDP

6. TCP

Вопрос 31

Для реализации технологии VPN на все компьютеры, имеющие выход в Интернет, устанавливаются VPN-…, которые обрабатывают IP-пакеты, передаваемые по вычислительным сетям (*напишите правильный ответ*):

_____

Вопрос 32

Уровень модели TCP/IP, определяющий способ общения пользовательских приложений, - … (*напишите правильный ответ*):

_____

Вопрос 33

Уровень модели TCP/IP, позволяющий сетевым приложениям получать сообщения по строго определённым каналам с конкретными параметрами, - … (*напишите правильный ответ*):

_____

Вопрос 34

На ... уровне модели TCP/IP определяются адреса включённых в сеть компьютеров, выделяются логические сети и подсети, реализуется маршрутизация между ними (*напишите правильный ответ*):

_____

Вопрос 35

На . уровне модели TCP/IP определяется адресация физических интерфейсов сетевых устройств, например, сетевых плат (*напишите правильный ответ*):

_____

Вопрос 36

К ... уровню модели TCP/IP относятся программы управления физическими сетевыми устройствами, так называемые драйверы (*напишите правильный ответ*):

_____

Вопрос 37

Межсетевой протокол, обеспечивающий адресацию в сетях (аббревиатура латинскими буквами), - ... (*напишите правильный ответ*):

_____

Вопрос 38

Протокол разрешения адресов, выполняющий преобразование логических сетевых адресов в аппаратные (аббревиатура латинскими буквами) (*напишите правильный ответ*):

_____

Вопрос 39

Протокол разрешения адресов, выполняющий преобразование аппаратных сетевых адресов в логические (аббревиатура латинскими буквами) (*напишите правильный ответ*):

_____

Вопрос 40

Протокол пользовательских датаграмм (аббревиатура латинскими буквами) (*напишите правильный ответ*):

_____

Ключи к тестам:

1-1	11- макро	21-1	31- агенты, агент
2-1	12-2	22-1,2,3,4	32-прикладное
3-2	13-1	23- экспертного	33- транспортный
4- ключ	14-4	24-1,2,3	34- сетевым, сетевой
5-3	15-2	25- агенты	35- канальном
6-2	16-3	26-1	36- канальному
7-1,2,3	17-4	27-2	37- IP
8-1	18-1	28-3	38- ARP
9-1	19-1	29-4	39- RARP
10-3	20-1	30-6	40- UDP

3.2.3.Контрольно-оценочные средства по ПМ.03 «Эксплуатация объектов сетевой инфраструктуры», для проведения экзамена (квалификационного)

В состав комплекта входит задание для экзаменующихся, пакет экзаменатора.

Задания для экзаменующегося.

Коды проверяемых профессиональных и общих компетенций:

ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ОК 1. ОК2. ОК 3. ОК.4. ОК 5. ОК 6. ОК7. ОК8. ОК9.

Инструкция

Внимательно прочитайте задание.

Для выполнения практической части, Вы можете воспользоваться нормативно-технической документацией и методической литературой, учебно-методической литературой, имеющейся на специальном столе.

Экзаменационный материал:

Билет №1

1. Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети.

2. Настройка H.323. Описание H.323 и общие рекомендации.

3. Оконцовка кабеля витая пара.

Билет №2

1. Современные угрозы сетевой безопасности.

2. Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.

3. Исследование сетевых атак и инструментов проверки защиты сети.

Билет №3

1. Вирусы, черви и троянские кони. Методы атак.

2. Полоса пропускания, паразитная нагрузка.

3. Заделка кабеля витая пара в розетку.

Билет №4

1. Функциональные компоненты H.323.Установка и поддержка соединения H.323.

2. Наращивание длины сегментов сети; замена существующей аппаратуры.

3. Настройка аппаратных IP-телефонов

Билет №5

1. Безопасный доступ к устройствам.

2. Расширяемость сети. Масштабируемость сети.

3. Настройка безопасного доступа к маршрутизатору.

Билет №6

1. Назначение административных ролей. Мониторинг и управление устройствами.

2. Настройка SIP. Описание и общие рекомендации.

3. Тестирование кабеля.

Билет №7

1. Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб).

2. Соединения без и с использованием GateKeeper.

3. Протокол управления SNMP.

Билет №8

1. Протокол SNMP, его характеристики, формат сообщений, набор услуг.

2. Обеспечение безопасности пользовательских компьютеров.

3. Настройка шлюза.

Билет №9

1. Соединения с использованием нескольких GateKeeper.

2. Проверка объектов сетевой инфраструктуры и профилактические работы.

3. Задачи управления: анализ производительности сети.

Билет №10

1. Многопользовательские конференции. Обеспечение отказоустойчивости.

2. Использование функции автоматизированной настройки безопасности.

3. Обеспечение административного доступа AAA и сервера Radius.

Билет №11

1. Технология SIP и связанные с ней стандарты.

2. Программное обеспечение мониторинга компьютерных сетей и сетевых устройств.

3. Настройка политики безопасности брандмауэров.

Билет №12

1. Криптографические сервисы. Базовая целостность и аутентичность.

2. Процедуры инсталляции коммутатора. Управление аппаратными средствами и портами.

3. Учет трафика в сети.

Билет №13

1. Увеличение количества узлов сети; увеличение протяженности связей между объектами сети.

2. Функциональные компоненты SIP. Сообщения SIP.

3. Настройка программных IP-телефонов, факсов.

Билет №14

1. Свойства AAA. Локальная AAA аутентификация. Server-based AAA.

2. Физическая карта всей сети; логическая топология компьютерной сети.

3. Развертывание сети с использованием VLAN для IP-телефонии.

Билет №15

1. Адресация SIP. Модель установления соединения. Планирование отказоустойчивости.

2. Соображения по безопасности второго уровня (Layer-2).

3. Настройка групп в голосовом маршрутизаторе.

Билет №16

1. Техническая и проектная документация. Паспорт технических устройств.

2. IPS технологии. IPS сигнатуры.

3. Настройка программно-аппаратной IP-АТС.

Билет №17

1. Протоколы управления MGCP, H.248.

2. Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры.

3. Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.

Билет №18

1. Создание аналоговых абонентов. Внутристанционная маршрутизация.

2. Конфиденциальность. Криптография открытых ключей.

3. Диагностика и устранение неисправностей в системах IP-телефонии.

Билет №19

1. Управление программным коммутатором. Маршрутизация. Группы соединительных линий.

2. Задачи управления: анализ производительности и надежности сети.

3. Настройка голосовых сообщений в маршрутизаторе.

Билет №20

1. ACL. Технология брандмауэра.

2. Подключение станций с TDM (абонентский доступ TDM).

3. Настройка таблицы пользователей в голосовом маршрутизаторе.

Билет №21

1. Проведение регулярного резервирования.

2. Сигнализация SIP, SIP-T, H.323 и SIGTRAN. IP-абоненты.

3. Настройка таблицы маршрутизации вызовов в голосовом маршрутизаторе.

Билет №22

1. Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения о неполадках.

2. Контекстный контроль доступа (CBAC).

3. Настройка политики безопасности брандмауэров.

Билет №23

1. Реализация IPS. Проверка и мониторинг IPS.

2. Группы абонентов. Дополнительные абонентские услуги.

3. Установка и настройка программной IP-АТС (например, Asterisk).

Билет №24

1. Оборудование для диагностики и сертификации кабельных систем.

2. Организация эксплуатации систем IP-телефонии.

3. Установка, подключение и первоначальные настройки голосового маршрутизатора.

Билет №25

1. Техническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт систем IP-телефонии.

2. Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.

3. Кроссирование и монтаж патч-панели в коммутационный шкаф, на стену.

Билет №26

1. Восстановление работы сети после аварии.

2. Конфигурация безопасности второго уровня локальной сети. Безопасность беспроводных сетей, VoIP и SAN.

3. Тестирование кодеков. Исследование параметров качества обслуживания.

Билет №27

1. Безопасная архитектура. Управление процессами и безопасность управление сетью.

2. Схемы послеаварийного восстановления работоспособности сети, техническая и проектная документация, способы резервного копирования данных, принципы работы хранилищ данных.

3. Настройка системы предотвращения вторжений (IPS).

Билет №28

1. Политики брандмауэра основанные на зонах.

2. Тестирование сети на уязвимости.

3. Настройка Clientless Remote Access SSL VPNs используя ASDM.

Билет №29

1. VPN. GRE VPN. Компоненты и функционирование IPSec VPN.

2. Конфигурация фаирвола на базе ASA с использованием графического интерфейса ASDM.

3. Мониторинг вызовов в программном коммутаторе.

Билет №30

1. Жизненный цикл сети и планирование. Разработка регламентов компании и политик безопасности.

2. Конфигурация VPN на базе ASA с использованием графического интерфейса ASDM.

3. Создание резервных копий баз данных.

Пакет экзаменатора при оценивании задания.

Пакет экзаменатора
Билет №1 **ЗАДАНИЕ № 1** Текст задания: Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети.

Исходные данные для задания: Комплекты и ксерокопии задания. На этих копиях, кроме изображения стандартов физического компонента сети и примеры сетевой инфраструктуры придприятия, сформулированы вопросы, на которые требуется дать ответы.
Вопросы к заданию:

1. Что такое компьютерная сеть?
2. Виды вычеслительных сетей.
3. Что входит в сетевое оборудование?

ЗАДАНИЕ № 2
Текст задания: Настройка H.323. Описание H.323 и общие рекомендации.
Исходные данные для задания: Комплекты и ксерокопии задания. На этих копиях, кроме изображения архитектуры сети H.323, зона сети H.323, виды конференции сети H.323, сетевых компонентов H.323, сформулированы вопросы, на которые требуется дать ответы.
Вопросы к заданию:

4. Зачем нужна настройка H.323. Два главных стандарта видеосвязи
5. Этапы вызова H.323? Преимущества H.323.
6. Какие преимущества работы IP-телефонии?

ЗАДАНИЕ № 3
Текст задания: Оконцовка кабеля витая пара.
Исходные данные для задания: Комплекты и ксерокопии задания. На этих копиях, кроме изображения коннектора 8P8C; кабеля витая пара; кримпер; кабель-тестер, сформулированы вопросы, на которые требуется дать ответы.
Вопросы к заданию:

6. Активное сетевое оборудование это- …? Пассивное сетевое оборудование – это …?
7. Перечислите виды сред передачи данных. Как с помощью стандартных сетевых утилит проверить работоспособность сетевого адаптера
8. Почему концентратор и повторитель относят к пассивному сетевому оборудованию?

Объекты оценки	Критерий результата оценки	Отметка о выполнении	
		да	нет
ПК 3.1. Осуществлять проектирование сетевой инфраструктуры.	Осуществление проектирования сетевой инфраструктуры.		
ПК 3.2. Обслуживать сетевые конфигурации программно-аппаратных средств.	Обслуживание сетевой конфигурации программно-аппаратных средств.		
ПК 3.3. Осуществлять защиту информации в сети с использованием программно-аппаратных средств.	Осуществление защиты информации в сети с использованием программно-аппаратных средств.		
ПК 3.4. Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры.	Осуществление устранения нетипичных неисправностей в работе сетевой инфраструктуры.		
ПК 3.5. Модернизировать сетевые устройства информационно-коммуникационных систем.	Модернизация сетевых устройств информационно-коммуникационных систем.		

Условия выполнения задания
1. Место выполнения задания: учебный кабинет №2 «Информатики и информационных технологий»; мастерские и лаборатории не предусмотрены.
2. Для выполнения задания используется
рабочее место, оборудованное персональным компьютером, програмное обеспечение.

Пакет прикладных программ Microsoft Office Инструкции по технике безопасности Нормативно-правовая литература

УСЛОВИЯ

1 Внимательно изучите информационный блок пакета экзаменатора

2.Ознакомьтесь с заданиями для экзаменующихся

Количество вариантов задания для экзаменующегося – 30

Условия выполнения задания:

Время выполнения задания - 20 минут.

Всего на экзамен 6 часов

– **Критерии оценки выполнения задания:**

– 1. Соответствие ГОСТ Р 6.30-2003

– 2. Соответствие образцам документов

– 3. Обращение к информационным источникам

– **Оборудование и материально-техническое оснащение:**

– Сетевое и системное администрирование: рабочий стол (парта), компьютерный стол, компьютер с программным обеспечением и выходом в сеть Интернет, чисты листы бумаги формата А4, ручка, линейка, карандаш, ластик, авторучка, бумага, принтер, клей, справочная литература и методические рекомендации, плакаты, макеты деталей двигателя, сеялки, жатки, доильного аппарата.

Подготовка и защита портфолио.

Тип портфолио: использован портфолио смешанного типа.

Проверяемые компетенции **ПК 1.1-ПК 1.5 ОК 1.-ОК 9.**

Перечень документов, входящих в портфолио.

Состав портфолио:(видео-презентация)

Дополнительные материалы:

Грамоты, дипломы за и общественные и спортивные достижения,

Сертификаты за участие в мероприятиях колледжа, города, района и округа.

Приказы о поощрениях и др.

Перечень документов, входящих в портфолио:
1.Письменные отзывы и характеристики педагогов колледжа, куратора – мастера производственного обучения, представителей администрации колледжа, подтверждающие высокий уровень познавательной активности, мотивации обучающегося на учебно-профессиональную деятельность, академических способностей и учебных достижений;
2.Письменные отзывы и характеристики руководителей различных видов производственной практики, представителей администрации учреждения, в котором обучающийся проходил производственную практику, аргументировано подтверждающие соответствующий уровень освоения профессиональных компетенций, принятие ценностей выбранной профессии, уровень развития профессионально-значимых личностных качеств, письменных самоанализ;
3.Отзывы и характеристики куратора – мастера производственного обучения, заместителя директора по учебной и учебно-производственной работе, объединения по интересам, педагогов и руководителей учреждений дополнительного образования, подтверждающие высокую социальную активность обучающегося, позитивное отношение к различным видам деятельности;
4.Копии грамот, дипломов, сертификатов, свидетельств, фото, подтверждающие участие в мероприятиях различного уровня и др.
Основные требования к оформлению портфолио:
1.Титульный лист.
1.1.Оформляется на отдельном листе
1.2.Содержит следующую информацию:
1.2.1.ФИО, обучающегося
1.2.2.год рождения
1.2.3.профессия
1.2.4.период формирования (дата начала и окончания формирования портфолио)
1.3.В правом верхнем углу титульного листа рекомендуется поместить фотографию обучающегося.
2.При оформлении портфолио должны соблюдаться следующие требования:
2.1.Систематичность и регулярность ведения портфолио
2.2.Достоверность сведений, представленных в портфолио
2.3.Аккуратность и эстетичность оформления
2.4.Разборчивость при ведении записей.
3.Обязательно наличие в портфолио четко сформулированного содержания/оглавления (с названиями разделов, наименованиями материалов и т.п.)

Портфолио оформляется обучающимся самостоятельно в электронном виде и/или на бумажных носителях. Документы должны быть заверены подписями и печатью.

Требования к презентации и защите портфолио:

1. Защита (доклад) сопровождается мультимедийной презентацией (не более 10- 12 слайдов). Продолжительность доклада-3-5 минут.

Требования к презентации:

Презентация состоит из:

- титульного слайда, на нем указываются:
  тема работы
  фамилия, имя и отчество автора, номер группы, курс, наименование учебного заведения
- информационных слайдов (до 12 слайдов)
- завершающего слайда.

Информационные слайды могут содержать диаграммы и графики, также текстовые, табличные и графические материалы, видео-ролики, предназначенные для более чёткого восприятия аудиторией информации, излагаемой в докладе.

Формат слайдов Параметры страницы:

- Размер слайдов - экран
- Ориентация - альбомная
- Ширина - 24 см
- Высота - 18 см
- Графический и текстовый материалы размещаются на слайдах, так, чтобы слева и справа от края слайда оставалось использованное поле шириной не менее 0,5.см.

Критерии оценивания:

1.Свободное владение специальной терминологией.
2.Правильные ответы на вопросы комиссии.
3.Эстетика, оригинальность оформления портфолио.
4.Полнота портфолио.
Соответствие требованиям.

Пакет экзаменатора при оценивании портфолио.

ПАКЕТ ЭКЗАМЕНАТОРА			
Представление портфолио обучающегося			
Объекты оценки	Критерии оценки результата	Отметка о выполнении	
		да	нет
ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Выбор способа решения задач профессиональной деятельности, применительно к различным контекстам.		
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.	Использование современных средств поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.		
ОК 03. Планировать и реализовывать собственное	Планирование и реализация собственного		

профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.	профессионального и личностного развития, предпринимательской деятельности в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.		
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде.	Эффективное взаимодействие и работа в коллективе и команде.		
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.	Осуществление устной и письменной коммуникации на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.		
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.	Проявление гражданско-патриотической позиции, демонстрация осознанного поведения на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.		
ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.	Содействие сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.		
ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня	Использование средств физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.		

физической подготовленности.			
ОК 9. Пользоваться профессиональной документацией на государственном и иностранном языках.	Использование профессиональной документацией на государственном и иностранном языках.		
Условия выполнения заданий: Дополнительная литература: Положение о портфолио обучающегося в ГБПОУ СО «ИТАТиУ»			

4.ХАРАКТЕРИСТИКА И КРИТЕРИИ ОЦЕНОК ФОРМ И ВИДОВ КОНТРОЛЯ

4.1.Контроль успеваемости.

Текущий контроль - это непрерывно осуществляемый в ходе аудиторных и самостоятельных занятий по учебному курсу контроль уровня знаний, умений, и практического опыта деятельности обучающегося в течение семестра.

- Текущий контроль знаний проводится для всех обучающихся лицея, обучающихся по основным профессиональным образовательным программам.
- Текущий контроль проводится в пределах учебного времени, отведенного на соответствующий ОП (раздел ОП) или практику.

Текущий контроль освоения обучающимися программного материала ОП может иметь следующие виды: входной, оперативный и рубежный контроль.

Входной контроль проводится с целью выявления степени реальной готовности обучающихся к освоению учебного материала ОП.

Форму проведения входного контроля выбирает преподаватель, он же готовит контролирующие материалы на основе типовых заданий для входного контроля. Результаты входного контроля могут явиться основой для корректировки рабочих программ профессиональных модулей, а также для выстраивания индивидуальной траектории обучения с каждым обучающимся или учебной группой.

Оперативный контроль проводится с целью объективной оценки качества освоения программ профессиональных модулей, а также стимулирования учебной работы обучающихся, мониторинга результатов образовательной деятельности, подготовки обучающихся к промежуточной аттестации и обеспечения максимальной эффективности учебного процесса.

Рубежный контроль - это форма текущего контроля, направленная на проверку освоения тематически завершенной части рабочей программы модуля или промежуточные срезы знаний. Формируется на основе типовых заданий для оценки освоения ОП.

В течение семестра по ОП (разделу ОП) проводится не менее 1 рубежного контроля.

В качестве форм рубежного контроля ОП (раздела ОП) или практики можно использовать:

- тестирование (в том числе компьютерное);
- прием отчетной документации по практике;
- проверка индивидуальных домашних заданий, самостоятельных работ

4.2.Практические занятия

Правила выполнения лабораторно-практических заданий.

Подготовка к лабораторно-практическим работам заключается в самостоятельном изучении теории по рекомендуемой литературе, предусмотренной рабочей программой. Выполнение заданий производится индивидуально в часы, предусмотренные расписанием занятий в соответствии с методическими указаниями к лабораторно-практическим работам. Отчет по практической работе каждый студент выполняет индивидуально с учетом рекомендаций по оформлению.

Отчет выполняется в рабочей тетради, сдается преподавателю по окончанию занятия или в начале следующего занятия. Отчет должен включать пункты:

- название лабораторной или практической работы
- цель работы
- оснащение
- задание
- порядок работы
- решение, развернутый ответ, таблица, ответы на контрольные вопросы (в зависимости от задания)
- вывод по работе.

Лабораторная или практическая работа считается выполненной, если она соответствует критериям, указанным в лабораторно-практической работе. Если студент имеет пропуски лабораторно-практических занятий по

уважительной или неуважительной причине, то выполняет работу во время консультаций, отведенных группе по данной дисциплине.

Практические занятия.

Практические занятия как виды учебных занятий направлены на экспериментальное подтверждение теоретических положений и формирование общих и профессиональных компетенций, учебных и профессиональных практических умений и составляют важную часть теоретической и профессиональной практической подготовки.

Выполнение обучающимися практических занятий проводится с целью:

- формирования практических умений в соответствии с требованиями к уровню подготовки, установленными рабочей программой профессионального модуля по конкретным разделам и темам междисциплинарных курсов;
- обобщения, систематизации, углубления, закрепления полученных теоретических знаний;
- совершенствования умений применять полученные знания на практике, реализации единства интеллектуальной и практической деятельности;
- развития интеллектуальных умений у будущих специалистов: аналитических, проектировочных, конструкторских и др.;
- выработки таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива при решении поставленных задач при освоении общих компетенций.

Практические занятия могут носить репродуктивный, частично-поисковый и поисковый характер.

Работы, носящие *репродуктивный характер,* отличаются тем, что при их проведении обучающиеся пользуются подробными инструкциями, в которых указаны: цель работы, пояснения (теория, основные характеристики), оборудование, аппаратура, материалы и их характеристики, порядок выполнения работы, таблицы, выводы (без формулировки), контрольные вопросы, учебная и специальная литература.

Работы, носящие *частично-поисковый характер*, отличаются тем, что при их проведении обучающиеся не пользуются подробными инструкциями, им не дан порядок выполнения необходимых действий, и они требуют от обучающихся самостоятельного подбора оборудования, выбора способов выполнения работы в инструктивной и справочной литературе и др.

Работы, носящие *поисковый характер*, характеризуются тем, что обучающиеся, опираясь на имеющиеся у них теоретические знания, должны решить новую для них проблему.

Оценка «5» ставится в том случае, если обучающийся:

а) выполнил задание в полном объеме с соблюдением необходимой последовательности действий, расчетов и измерений;

б) самостоятельно и рационально выбрал и подготовил для выполнения задания все необходимое оборудование, все расчеты, измерения и построения провел в условиях, обеспечивающих получение результатов и выводов с наибольшей точностью;

в) в представленном отчете правильно и аккуратно выполнил все записи, таблицы, рисунки, чертежи, графики, вычисления и сделал выводы;

г) соблюдал требования охраны труда.

Оценка «4» ставится в том случае, если выполнены требования к оценке 5, но:

а) расчеты, измерения и построения проводились в условиях, не обеспечивающих достаточной точности;

б) было допущено два-три недочета, или не более одной негрубой ошибки и одного недочета.

Оценка «3» ставится, если задание выполнено не полностью, но объем выполненной части таков, что можно сделать выводы, или если в ходе выполнения задания были допущены следующие ошибки:

а) действия проводились в нерациональных условиях, что привело к получению результатов с большой погрешностью;

б) в отчете были допущены в общей сложности не более двух ошибок (в записях единиц, измерениях, в вычислениях, графиках, таблицах, схемах,

анализе алгоритма работы и т.д.), не принципиальных для данного вида работы, не повлиявших на результат выполнения;

в) задание выполнено не полностью, однако объем выполненной части таков, что позволяет получить правильные результаты и сделать выводы по основным, принципиально важным задачам занятия.

Оценка «2» ставится в том случае, если:

а) задание выполнено не полностью, и объем выполненной части не позволяет сделать правильные выводы;

б) расчеты, измерения, вычисления, наблюдения или другие действия производились неправильно;

в) в ходе работы и в отчете обнаружились в совокупности все недостатки, отмеченные в требованиях к оценке «3».

В тех случаях, когда обучающийся показал оригинальный и/или наиболее рациональный подход к выполнению задания и в процессе выполнения здания, но не избежал тех или иных недостатков, оценка за выполнение работы по усмотрению преподавателя может быть повышена по сравнению с указанными выше критериями.

Тестирование.

Критерии оценки результатов тестирования могут быть различными. На практике чаще всего применяют два критерия:

- соотношение между количеством правильных ответов на вопросы с общим числом вопросов теста
- время, затраченное для ответа на вопросы.

Первый критерий является основным, поэтому при оценке ответов учитываются либо только он один (чаще всего) либо оба одновременно.

Первый критерий - выбор преподавателем верного соотношения между числом правильных ответов на вопросы с общим числом вопросов теста для определения оценки зависит от важности проверяемого материала и актуальности поставленных вопросов.

При этом контроль должен быть объективным и отвечать тем целям, которые перед ним поставлены.

Чаще всего число вопросов в блоках применяется 10, 5 или, в тесте может быть и другое число вопросов. Если проверяют знания по обычному материалу, т. е. не требующему высокой ответственности принимаемых решении, когда неточности в его знании не влекут за собой особо тяжелых последствий, то на практике часто принимают такие значения первого критерия:

При числе вопросов в тесте равном 10 оценки будут следующие:

Отлично - при 9-10 правильных ответах,

Хорошо - при 7- 8 правильных ответах,

Удовлетворительно - при 5- 6 правильных ответах,

Неудовлетворительно - при правильных ответов менее 5.

Из изложенного видно, что каждой оценки соответствует определенный числовой диапазон правильных ответов, который в свою очередь, зависит от числа вопросов в тесте.

При большом количестве вопросов в тесте, целесообразно числовой диапазон правильных ответов заменять на процент правильных ответов, тогда оценка может соответствовать, например,

Отлично - при 90% правильных ответах,

Хорошо - при 70% правильных ответах,

Удовлетворительно - при 50% правильных ответах,

Неудовлетворительно - при правильных ответов менее 50%.

При решении вопроса о том, каким выбрать первый критерий знаний, целесообразно учитывать возможную неравнозначность вопросов в тестах. В тесте один или несколько вопросов могут быть основными, т. е. более сложными для ответа, или включающими наиболее важный материал, а остальные вопросы - дополнительными.

В этом случае удельный "вес" основных вопросов будет выше, чем дополнительных, и может в большей степени влиять на принятие преподавателем решения о выставлении оценки.

Второй критерий - время, затраченное для ответов на вопросы, применяется в тех случаях, когда требуется оценивать не только правильность ответа на вопросы, но и время, необходимое для того чтобы ответить.

Чаще всего этот критерий применяется, когда основными вопросами тестов являются вопросы с результативным методом ввода ответов и когда для ответов предусмотрено решение задач в ограниченное время.

Ответы проверяемых, которые не успели ответить, оцениваются как неудовлетворительные, либо оценка по первому критерию соответствующим образом снижается.

Числовые значения и первого и второго критериев, разработанные преподавателем для различных разделов (тем) данной дисциплины, должны быть согласованы между собой. Необходимо также провести согласование числовых значений критериев, применяемых разными преподавателями.

В рамках компетентностного подхода ФГОС используется модель оценки результатов обучения, об уровнях усвоения знаний и постепенном восхождении обучающихся по образовательным траекториям.

Выделены следующие *уровни* результатов обучения обучающихся.

Первый уровень. Результаты обучения свидетельствуют об усвоении ими некоторых элементарных знаний основных вопросов по дисциплине. Допущенные ошибки и неточности показывают, что обучающиеся не овладели необходимой системой знаний по дисциплине.

Второй уровень. Достигнутый уровень оценки результатов обучения показывает, что обучающиеся обладают необходимой системой знаний и владеют некоторыми умениями по дисциплине. Обучающиеся способны понимать и интерпретировать освоенную информацию, что является основой успешного формирования умений и навыков для решения практико-ориентированных задач.

Третий уровень. Обучающиеся продемонстрировали результаты на уровне осознанного владения учебным материалом и учебными умениями, навыками и способами деятельности по дисциплине. Обучающиеся способны

анализировать, проводить сравнение и обоснование выбора методов решения заданий в практико-ориентированных ситуациях.

Четвертый уровень. Обучающиеся способны использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных практико-ориентированных ситуациях. Достигнутый уровень оценки результатов обучения по дисциплине является основой для формирования общекультурных и профессиональных компетенций, соответствующих требованиям ФГОС.

В тестах данная модель реализована в трех взаимосвязанных блоках заданий.

Первый блок – задания на уровне «знать», в которых очевиден способ решения, усвоенный обучающимся при изучении дисциплины. Задания этого блока оцениваются по шкале «правильно-неправильно».

Второй блок – задания на уровне «знать» и «уметь», в которых нет явного указания на способ выполнения, и обучающийся для их решения самостоятельно выбирает один из изученных способов. Задания данного блока оцениваются с учетом частично правильно выполненных заданий.

Третий блок – задания на уровне «знать», «уметь», «владеть». Он представлен case-заданиями, содержание которых предполагает использование комплекса умений и навыков, для того чтобы обучающийся мог самостоятельно сконструировать способ решения, комбинируя известные ему способы и привлекая знания из разных дисциплин. Задания данного блока также оцениваются с учетом частично правильно выполненных заданий.

Промежуточная аттестация.

Промежуточная аттестация обеспечивает оперативное управление учебной деятельностью обучающегося и ее корректировку и проводится с целью определения:

- соответствия уровня и качества подготовки специалиста Федеральным государственным образовательным стандартам СПО в части государственных требований;
- полноты и прочности теоретических знаний по ОП в целом;

- сформированности умений применять полученные теоретические знания при решении практических задач;

- сформированности у студентов общих и профессиональных компетенций, соответствующих видам профессиональной деятельности:

- сформированности умений самостоятельно работать с учебной и справочной литературой.

4.3. Дифференцированный зачет/экзамен

Дифференцированный зачет как форма промежуточной аттестации проводится за счет объема времени, отводимого на изучение ОП. Задания для дифференцированного зачета включают задания, вопросы по учебному материалу, направленному на освоение компетенций и вида деятельности согласно требованиям федерального государственного образовательного стандарта.

При проведении дифференцированного зачета уровень подготовки обучающегося оценивается в баллах: «5» (отлично), «4» (хорошо), «3» (удовлетворительно), «2» (неудовлетворительно). Неудовлетворительная оценка «2» в зачетную книжку не ставится.

Критерии оценки ответов обучающихся при проведении дифференцированных зачетов

Оценка «5» - изложение полученных знаний в устной, письменной или графической форме полное, в соответствии с требованиями учебной программы; выделение существенных признаков изученного с помощью операций анализа и синтеза; выявление существенных признаков причинно следственных связей, формулировка выводов и обобщений; самостоятельное применение знаний в практической деятельности, выполнение заданий как воспроизводящего, так и творческого характера;

Оценка «4» - изложение полученных знаний в устной, письменной или графической форме полное, в соответствии с требованиями учебной программы; допускаются отдельные незначительные ошибки; при выделении существенных признаков изученного также допускаются отдельные

незначительные ошибки; в практической, самостоятельной деятельности возможна небольшая помощь преподавателя;

Оценка «3» - изложение полученных знаний неполное, однако это не препятствует освоению последующего программного материала; допускаются отдельные существенные ошибки, исправляемые с помощью преподавателя; имеются затруднения при выделении существенных признаков изученного и формулировке выводов. Недостаточная самостоятельность в практической деятельности и выполнении заданий воспроизводящего характера;

Оценка «2» - изложение учебного материала неполное, бессистемное; имеются существенные ошибки, которые учащийся не в состоянии исправить даже с помощью преподавателя; неумение производить простейшие операции синтеза и анализа, делать обобщения и выводы.

Зачет проводится в устной форме по билетам: студент должен выполнить два задания (на подготовку ответа на каждое из них отводится 15 минут).

На зачете не разрешается пользоваться литературой, нормативно-правовыми актами, конспектами и иными вспомогательными средствами. В случае использования студентов подобной литературы преподаватель оставляет за собой право удалить студента с зачета, выставив ему неудовлетворительную оценку.

Оценивание ответа на зачете осуществляется следующим образом:

Оценка **зачтено** выставляется, если ответ логически и лексически грамотно изложенный, содержательный и аргументированный ответ, подкрепленный знанием литературы и источников по теме задания, умение отвечать на дополнительно заданные вопросы; незначительное нарушение логики изложения материала, периодическое использование разговорной лексики, допущение не более одной ошибки в содержании задания, а также не более одной неточности при аргументации своей позиции, неполные или неточные ответы на дополнительно заданные вопросы; незначительное нарушение логики изложения материала, периодическое использование разговорной лексики при допущении не более двух ошибок в содержании задания, а также

не более двух неточностей при аргументации своей позиции, неполные или неточные ответы на дополнительно заданные вопросы.

Оценка **не зачтено** выставляется, если в ответе допущено существенное нарушение логики изложения материала, систематическое использование разговорной лексики, допущение не более двух ошибок в содержании задания, а также не более двух неточностей при аргументации своей позиции, неправильные ответы на дополнительно заданные вопросы; существенное нарушение логики изложения материала, постоянное использование разговорной лексики, допущение не более трех ошибок в содержании задания, а также не более трех неточностей при аргументации своей позиции, неправильные ответы на дополнительно заданные вопросы; полное отсутствие логики изложения материала, постоянное использование разговорной лексики, допущение более трех ошибок в содержании задания, а также более трех неточностей при аргументации своей позиции, полное незнание литературы и источников по теме вопроса, отсутствие ответов на дополнительно заданные вопросы.

Оценка зачтено может выставляться по результатам текущего контроля, осуществляемого в ходе семинарских/практических занятий на основе оценки активности работы студентов, их участия в дискуссиях и выступлений с докладами, а также по результатам оценки посещаемости студентами лекций и семинаров.

Примерные критерии оценки: оценки «отлично» заслуживает студент, обнаруживший всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка «отлично» выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала;

оценки «хорошо» заслуживает студент, обнаруживший полные знания учебно-программного материала, успешно выполняющий предусмотренные в программе задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка «хорошо» выставляется студентам, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности;

оценки «удовлетворительно» заслуживает студент, обнаруживший знание учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющийся с выполнением заданий, предусмотренных программой, знакомый с основной литературой, рекомендованной программой. Как правило, оценка «удовлетворительно» выставляется студентам, допустившим погрешность в ответе на экзамене и при выполнении экзаменационных заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя;

оценка «неудовлетворительно» выставляется студенту, обнаружившему пробелы в знаниях основного учебно-программного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине».

Преподавателем может быть разработана самостоятельная методика формирования результирующей оценки.

Критерии оценок знаний студентов на экзаменах

Отметка «отлично» ставится, если:

знания отличаются глубиной и содержательностью, дается полный исчерпывающий ответ, как на основные вопросы билета, так и на дополнительные:

- студент свободно владеет научными понятиями;

- студент способен к интеграции знаний по определенной теме, структурированию ответа, к анализу положений существующих теорий, научных школ, направлений по вопросу билета;
- логично и доказательно раскрывает проблему, предложенную в билете;
- ответ не содержит фактических ошибок и характеризуется глубиной, полнотой, уверенностью студента;
- ответ иллюстрируется примерами, в том числе из собственной практики;
- студент демонстрирует умение вести диалог и вступать в научную дискуссию.

Отметка «хорошо» ставится, если:

знания имеют достаточный содержательный уровень, однако отличаются слабой структурированностью; раскрыто содержание билета, имеются неточности при ответе на дополнительные вопросы:

- в ответе имеют место несущественные фактические ошибки, которые студент способен исправить самостоятельно, благодаря наводящему вопросу;
- недостаточно раскрыта проблема по одному из вопросов билета;
- недостаточно логично построено изложение вопроса;
- ответ прозвучал недостаточно уверенно;
- студент не смог показать способность к интеграции и адаптации знаний или теории и практики.

Отметка «удовлетворительно» ставится, если:

знания имеют фрагментарный характер, отличаются поверхностностью и малой содержательностью содержание билета раскрыто слабо, имеются неточности при ответе на основные вопросы билета:

- программные материал в основном излагается, но допущены фактические ошибки;
- ответ носит репродуктивный характер;
- студент не может обосновать закономерности и принципы, объяснить факты;

- нарушена логика изложения, отсутствует осмысленность представляемого материала;
- у студента отсутствуют представления о межпредметных связях.
- Отметка «неудовлетворительно» ставится, если:
- обнаружено незнание или непонимание студентом сущностной части социальной психологии;
- допускаются существенные фактические ошибки, которые студент не может исправить самостоятельно;

На большую часть дополнительных вопросов по содержанию экзамена студент затрудняется дать ответ или не дает верных ответов.

ЛИТЕРАТУРА.

Основные источники:

1. «Организация сетевого администрирования». Учебник. 4-е изд., стер | Громов Алексей Юрьевич, Баранчиков Алексей Иванович Москва. Академия 2021г.

Дополнительная литература:

1. Гагарина, Л. Г. Разработка и эксплуатация автоматизированных информационных систем : учеб. пособие / Л.Г. Гагарина. — М.: ИД «ФОРУМ» : ИНФРА-М, 2022. — 384 с. — Текст : электронный. - URL: https://new.znanium.com/catalog/product/1003025 (дата обращения: 05.03.2021)

2. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — М. :Юрайт, 2022. — 333 с. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452574 (дата обращения: 05.03.2021).

Информационные справочно-правовые системы:

«Консультант-Плюс», «Гарант» и другие.

Интернет-ресурсы:

1.http://www.proshkolu.ru/

2.http://school-collection.edu.ru

3.https://www.lants.ru/books/IT/%D0%A2.%D0%9B%D0%B8%D0%BC%D0%BE%D0%BD%D1%87%D0%B5%D0%BB%D0%BB%D0%B8,%20%D0%9A.%D0%A5%D0%BE%D0%B3%D0%B0%D0%BD,%20%D0%A1.%D0%A7%D0%B5%D0%B9%D0%BB%D0%B0%D0%BF%20-%20%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%BD%D0%BE%D0%B5%20%D0%B8%20%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B5%20%D0%B0%D0%B4%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5-2009.pdf

4. https://base.garant.ru/71577664/53f89421bbdaf741eb2d1ecc4ddb4c33/

5. https://www.garant.ru/products/ipo/prime/doc/71477664/