

Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Самарский государственный аэрокосмический университет
имени академика С.П. Королева
(национальный исследовательский университет)»

С.В. Суханов

**Компьютерные сети.
Лабораторный практикум**

Электронное учебное пособие

САМАРА
2011

Автор: СУХАНОВ Сергей Васильевич

Учебное пособие содержит сборник необходимых теоретических сведений и методических указаний к лабораторным работам, выполняемым в ходе изучения курса Компьютерные сети, а также образцы оформления отчетов по лабораторным работам, описание вариантов заданий к лабораторным работам, инструкции по использованию применяемого в ходе выполнения лабораторных работ программного обеспечения, инструкции по настройке сетевого оборудования.

Учебное пособие предназначено для бакалавров направлений 010400.62 «Прикладная математика и информатика» и 010900.62 «Прикладная математика и физика»

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Самарский государственный аэрокосмический университет
имени академика С.П. Королева
(национальный исследовательский университет)»

Факультет информатики
Кафедра технической кибернетики

Локальные сети на витой паре

**Методические указания к лабораторной работе
по курсу компьютерные телекоммуникации**

ОГЛАВЛЕНИЕ

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ	3
1. Базовые понятия компьютерных сетей	4
1.1. Классификация сетей.....	4
1.2. Модель OSI.....	4
1.3. Топологии сетей.....	6
2. Среды передачи данных в локальных сетях.....	8
2.1. Коаксиальный кабель	9
2.2. Витая пара.....	9
2.3. Спецификации Ethernet	10
2.4. Обжим витой пары.....	13
3. Структурированная кабельная система	15
Список контрольных вопросов	20
ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ОТЧЕТА	20

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Изучаемый материал: *Введение в компьютерные сети. Структурированные кабельные системы (СКС). Среда передачи данных. Кабели. Спецификации Ethernet. Обжим витой пары. Создание и настройка простейшей сети. Использование сетевых тестеров для диагностики сети.*

1. Изучить теоретическую часть.
2. Получить оборудование и материалы.
3. Обжать прямой кабель (в соответствии с указаниями преподавателя).
4. Проверить с помощью тестеров Fluke LinkRunner и/или Fluke CableIQ качество изготовленного кабеля.
5. Разбиться на группы по числу имеющихся в лаборатории коммутаторов (хабов/концентраторов).
6. Соединить прямым кабелем гнездо патч-панели (в коммутационном шкафу), соответствующее компьютеру студента, со свободным портом одного из коммутаторов (хабов/концентраторов).
7. После соединения настроить полученную простейшую сеть, т.е. задать на каждом компьютере IP-адреса из диапазона частных сетей (192.168.X.X), маски подсети (например, 255.255.255.0). Для этого использовать программу NetSetMan.
8. После настройки сети протестировать полученную сеть с помощью команды ping. Сначала пингуют loopback-адрес: **ping 127.0.0.1** для проверки стека протоколов TCP/IP. Затем пингуют свой собственный IP-адрес для проверки работоспособности сетевой карты. И в конце пингуют адрес соседнего компьютера. Во всех трех случаях все пинги должны пройти успешно. В случае неудачной проверки работоспособности сети студенты должны найти неисправность и исправить ее. Наконец проверить, видны ли все компьютеры сети в сетевом окружении Windows. Обменяться файлами.
9. Объединить две сети в единую сеть, соединив кабелем порты коммутаторов. Проверить связь между сетями, объяснить, почему она отсутствует.
10. Изменить сетевые настройки компьютеров так, чтобы они оказались в одной сети (два способа: или ввести одинаковый адрес сети, или изменить маску так, чтобы существующие адреса оказались в одной сети). Перекрестно пропинговать компьютеры объединенной сети, добиться полной связности. Убедиться, видны ли все компьютеры сети в сетевом окружении Windows. Обменяться файлами.
11. Протестировать с помощью тестеров Fluke LinkRunner и Fluke CableIQ качество сетевой разводки учебного класса (от сетевых розеток компьютеров и от патч-панели). Записать измеренные параметры линий для помещения в отчет.
12. Оформить отчет о лабораторной работе. Представить его преподавателю в электронной форме. Ответить, если необходимо, на вопросы. Получить зачет по лабораторной работе.

1. Базовые понятия компьютерных сетей

1.1. Классификация сетей

Сеть – набор устройств, соединенных между собой линиями связи и способных взаимодействовать между собой. Сети могут быть разными по своей величине, структуре и назначению. По размеру, сети можно разделить на LAN, MAN и WAN. LAN – локальная сеть размером от нескольких компьютеров до здания. Это наиболее распространенный вид сетей. MAN – так называемые кампусные сети, объединяют несколько зданий или даже районов города, как правило состоят из нескольких LAN, соединенных бекбонными линиями. WAN – глобальные сети, объединяют компьютеры на большом географическом пространстве, Internet – является глобальной сетью.

В любой сети присутствуют четыре физических компонента: компьютеры, линии связи, коммутаторы и маршрутизаторы.

Основными ресурсами, к которым предоставляет доступ сеть являются: данные и приложения, периферийные устройства (принтеры), хранилища данных и устройства резервного копирования.

Основными пользовательскими приложениями, используемыми в сетях являются: приложения для отправки и приема электронной почты, web-браузеры, мессенджеры (сетевые пейджеры), приложения для совместной работы и базы данных.

1.2. Модель OSI

Теоретической основой для описания сетей и взаимодействия устройств и приложений в сети является семиуровневая модель OSI. Эта модель была предложена в 1984 году организацией ISO (International Standard Organization). Для чего нужна модель OSI.

Во-первых, эта модель уменьшает сложность описания сетей в целом путем разбиения описания на небольшие части.

Во-вторых, модель стандартизирует компоненты сети, что позволяет использовать оборудование от различных производителей.

В-третьих, модель OSI позволяет разные типы сетевого оборудования и программ для осуществления коммуникаций.

В-четвертых, при использовании этой модели, изменения, производимые на одном ее уровне, не влияют на работу других уровней.

В-пятых, модель позволяет эффективно обновлять и исправлять отдельные компоненты сети, без необходимости обновлять другие компоненты и без необходимости исправления существующих протоколов.

В-шестых, модель OSI, упрощает изучение и понимание работы сетей.

Ниже, в таблице 1 приведены уровни модели OSI.

Таблица 1.

Уровни модели OSI.

Уровень	Название уровня на русском языке	Название уровня на английском языке
7	Уровень приложений	Application
6	Презентационный	Presentation
5	Сессионный	Session
4	Транспортный	Transport
3	Сетевой	Network
2	Канальный	Data Link
1	Физический	Physical

Физический уровень – определяет электрическую, механическую, процедурную и функциональную спецификацию для активации, поддержки и деактивации физических линий связи между системами. Такие характеристики, как уровень напряжения, синхронизация, физическая частота, дистанция передачи, Коннекторы и прочее определяются спецификациями физического уровня.

Канальный уровень – определяет формат данных для передачи и, как будет контролироваться доступ к физической среде передачи данных. Этот уровень также включает обнаружение ошибок и коррекцию для надежной доставки данных.

Сетевой уровень – обеспечивает соединение и выбор пути между двумя системами хостов, которые могут быть географически расположены в разных сетях. Развитие Интернет увеличило число пользователей получающих доступ к информации с сайтов по всему миру, и именно сетевой уровень управляет этими соединениями.

Транспортный уровень – обеспечивает пересылку данных, причем делает это так, чтобы скрыть детали транспортировки данных от верхних уровней модели OSI. Этот уровень обеспечивает так называемое виртуальное End-to-End соединение. То есть устанавливает виртуальный канал между двумя хостами для передачи данных и разрывает его, когда передача завершена. Так же этот уровень может обеспечивать надежную передачу данных путем обнаружения ошибок, восстановления информации и контроля потока.

Сессионный уровень устанавливает, управляет и разрывает сессию связи между двумя хостами. Сессионный уровень так же синхронизирует диалог презентационными уровнями на двух хостах и управляет передачей данных между ними.

Презентационный уровень проверяет, что информация, посланная уровня приложения одного хоста будет совместима и правильно прочитана уровнем приложений другого хоста. Так же этот уровень отвечает за формат и структуру данных, обеспечивает шифрование.

Уровень приложений – это ближайший к пользователю уровень модели OSI. Этот уровень предоставляет сетевые сервисы для пользовательских приложений, таких как электронная почта, передача файлов, эмуляция терминалов.

Этот уровень отличается от других тем, что не предоставляет доступ к службам других уровней модели, а только к приложениям за пределами модели OSI.

1.3. Топологии сетей

Топологию разделяют на физическую и логическую. Физическая топология описывает то как соединены устройства в сети физическими линиями связи, логическая – как происходит передача данных между устройствами.

1.3.1. Физические топологии

Общая шина – самая простая и дешевая топология. Широко применялась в сетях построенных с использованием коаксиального кабеля. Технологически представляет собой один общий магистральный (бекбонный) кабель к которому подключены все устройства сети.

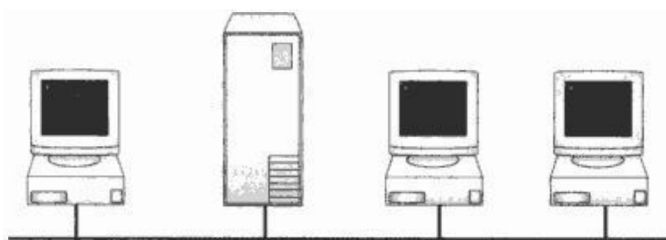


Рис. 1. Топология типа шина.

В настоящее время данная топология практически не используется, вследствие низкой скорости передачи данных.

Кольцо – тоже одна из старых топологий. Использовалась в сетях Token Ring. В свое время пользовалась большой популярностью, вследствие того что в сетях Token Ring скорость передачи данных была 16 Mbps, в отличие от Ethernet со скоростью 10 Mbps.

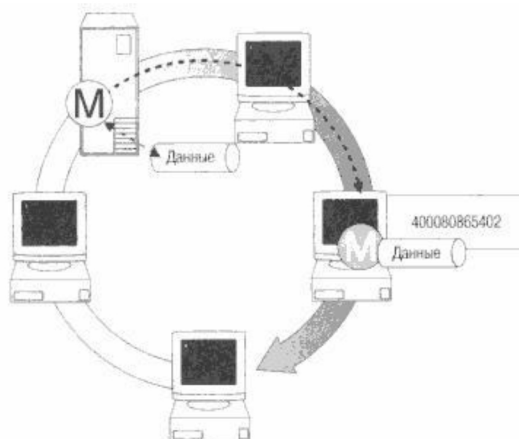


Рис. 2. Топология типа кольцо.

Кроме топологии кольцо так же есть топология **двойного кольца (Dual Ring)**. Двойное кольцо обеспечивало вдвое большую скорость передачи данных, поскольку данные могли передаваться одновременно в двух направлениях. В настоящее время топология двойного кольца также устарела и практически не используется.

Наиболее распространенной сейчас является физическая топология – **звезда (star)**.

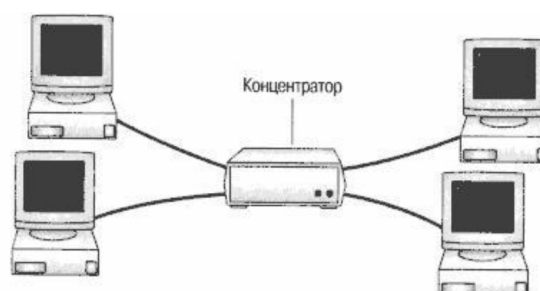


Рис.3. Топология звезда.

В данной топологии, отдельные хосты соединены посредством специального устройства. В качестве такого устройства может быть **концентратор (hub)** или **коммутатор (switch)**. Для повышения производительности сети рекомендуется использовать коммутаторы.

Три рассмотренные выше топологии являются топологиями для сегментов сети. Сегменты могут объединяться в более сложные сети, причем топология соединения сегментов так же применяются рассмотренные физические топологии.

1.3.2. Логические топологии

Несколько иначе обстоит дело с логическими топологиями, всего их существует 4 типа: общая шина, кольцо, звезда и полно связанная. Логические топологии общая шина, кольцо и звезда выглядят так же, как и физические, просто необходимо помнить, что в логической топологии нет понятия линии связи, а есть понятие виртуального канала. Полносвязанная логическая топология – это топология когда каждый хост имеет собственный виртуальный канал с любым другим хостом.

Часто логическая топология не совпадает с физической топологией. Ниже, в таблице 2, рассмотрим возможные соответствия между физическими и логическими топологиями.

Таблица 2.

Соответствие топологий.

Физическая топология	Логическая топология
Общая шина	Общая шина. Кольцо. При условии специальной настройки.
Кольцо	Только кольцо
Звезда	Общая шина, при условии, что связующее устройство – концентратор (hub). Звезда или полно связанная, при условии, что связующее устройство – коммутатор (switch)

Домен коллизий – логический участок компьютерной сети, в котором могут происходить коллизии пакетов данных, т. е. когда два устройства, подключенные к общей среде передачи, начинают одновременно передавать данные и, в результате наложения сигналов, данные теряются. Устройства вынуждены в этом

случае повторять передачу заново. Явление наиболее распространено в сетях Ethernet (а именно в сетях, использующих метод доступа CSMA/CD). Большое количество коллизий в сегменте значительно снижает производительность сети.

Домен коллизий может представлять некоторый участок коаксиального кабеля, к которому подключены несколько устройств, отдельный концентратор с подключенными к нему несколькими устройствами, или целые Ethernet-сети, построенные на основе концентраторов и повторителей.

Различные сетевые устройства работают на разных уровнях модели OSI и могут либо ограничивать, либо продлевать домен коллизий:

- устройства первого уровня OSI (концентраторы, повторители) воспроизводят любой сигнал, поступающий из среды передачи. Таким образом, эти устройства продлевают домен коллизий;
- устройства второго и третьего уровня OSI (коммутаторы, маршрутизаторы) ограничивают домен коллизий.

Задержка распространения – время с момента начала передачи фрейма, в течение которого может произойти коллизия. Определяется скоростью прохождения сигнала по проводу и скоростью передачи. Для 10Мб Ethernet задержка распространения составляет 51.2 мкс, для 100Мб – 5.12 мкс. Большая часть сетевого оборудования контролирует возникновение коллизий при передаче только в течение задержки распространения. Запоздавшая коллизия – коллизия, произошедшая после задержки распространения. Такие коллизии не обнаруживаются (большинством) сетевого оборудования и приводят к потерям фреймов.

Широковещательный домен – логический участок компьютерной сети, в котором каждое устройство может передавать данные непосредственно любому другому устройству, используя широковещательный адрес второго, канального уровня модели OSI.

В широком понимании смысла, широковещательный домен – участок сети, где устройства могут общаться напрямую, не обязательно используя широковещательный адрес канального уровня. Единственное условие – отсутствие необходимости передавать данные через промежуточное маршрутизирующее устройство.

Устройства, ограничивающие широковещательный домен – маршрутизаторы, работающие на третьем, сетевом уровне модели OSI, и коммутаторы на втором уровне модели OSI, поддерживающие технологию VLAN. Устройства первого уровня – концентраторы и повторители, а также коммутаторы без поддержки VLAN широковещательный домен не ограничивают.

2. Среда передачи данных в локальных сетях

В настоящее время используется три среды передачи данных в локальных и глобальных сетях: медный кабель (коаксиальный, витая пара), оптоволоконный кабель и эфир (для беспроводной связи).

Подробнее остановимся на рассмотрении медного кабеля, как самой распространенной среды передачи данных в локальных компьютерных сетях.

2.1. Коаксиальный кабель

Состоит из двух цилиндрических проводников, соосно вставленных один в другой. Чаще всего используется центральный медный проводник, покрытый пластиковым изолирующим материалом, поверх которого идёт второй проводник – медная сетка или алюминиевая фольга. Благодаря совпадению центров обоих проводов потери на излучение практически отсутствуют; одновременно обеспечивается хорошая защита от внешних электромагнитных помех. Поэтому такой кабель обеспечивает передачу данных на большие расстояния (до 500 метров) и используется при построении компьютерных сетей. Основной топологией для таких сетей является общая шина. Оконечные точки кабеля, являющегося общей шиной, должны быть замкнуты специальными терминаторами.

Основные категории коаксиального кабеля для построения локальных сетей: RG-8, RG-11 (толстый Ethernet) и RG-58 (тонкий Ethernet).

Сеть типа «тонкий ethernet» – это сеть, построенная на базе коаксиального кабеля категории RG-58. Максимальная длина сегмента сети – 200 метров. Кабель присоединяется к компьютеру с помощью BNC (British Naval Connector) коннектора.

Сеть типа «толстый ethernet» – это сеть, построенная на базе коаксиального кабеля категории RG-8, RG-11. Этот кабель толще (примерно 12 мм в диаметре против 6 мм у тонкого) и из-за этого плохо гнется, занимает больше места и имеет значительную стоимость. Однако, за счет более толстого проводника, позволяет передавать данные на расстояние до 500 метров без использования дополнительных усилителей.

2.2. Витая пара

Витая пара (UTP) – вид кабеля связи, представляет собой одну или несколько пар изолированных проводников, скрученных между собой (с небольшим числом витков на единицу длины), для уменьшения взаимных наводок при передаче сигнала, и покрытых пластиковой оболочкой. Один из компонентов современных структурированных кабельных систем. Используется в телекоммуникациях и в компьютерных сетях в качестве сетевого носителя для многих технологиях, таких как Ethernet, ARCNet и Token ring. В настоящее время, благодаря своей дешевизне и лёгкости в установке, является самым распространённым для построения локальных сетей.

В зависимости от наличия защиты – электрически заземлённой медной оплетки или алюминиевой фольги вокруг скрученных пар, определяют разновидности данной технологии:

- неэкранированная витая пара (UTP – Unshielded twisted pair);
- экранированная витая пара (STP – Shielded twisted pair);
- фольгированная витая пара (FTP – Foiled twisted pair);
- фольгированная экранированная витая пара (SFTP – Shielded Foiled twisted pair).

В некоторых типах экранированного кабеля, защита может использоваться ещё и вокруг каждой пары – это индивидуальное экранирование. Экранирование

обеспечивает лучшую защиту от электромагнитных наводок как внешних, так и внутренних и т. д.

Для подключения к компьютеру (или другому устройству) используется коннектор RJ-45.

Существуют следующие категории витой пары:

- CAT1 – (полоса частот 0.1 МГц) телефонный кабель, всего одна пара, известный в России, как «лапша». В США использовался ранее, и проводники были скручены между собой. Используется только для передачи голоса или данных при помощи модема.
- CAT2 – (полоса частот 1 МГц) старый тип кабеля, 2-е пары проводников, поддерживал передачу данных на скоростях до 4 Мбит/с, использовался в сетях token ring и ARCNet. Сейчас иногда встречается в телефонных сетях.
- CAT3 – (полоса частот 16 МГц) 2-х парный кабель, использовался при построении локальных сетей 10BASE-T и token ring, поддерживает скорость передачи данных только до 10 Мбит/с. В отличие от предыдущих двух, отвечает требованиям стандарта IEEE 802.3. Также до сих пор встречается в телефонных сетях.
- CAT4 – (полоса частот 20 МГц) кабель состоит из 4-х скрученных пар, использовался в сетях token ring, 10BASE-T, 10BASE-T4, скорость передачи данных не превышает 16 Мбит/с, сейчас не используется.
- CAT5 – (полоса частот 100 МГц) 4-х парный кабель, это и есть, то, что обычно называют кабель «витая пара», благодаря высокой скорости передачи, до 100 Мбит/с при использовании 2-х пар и до 1000 Мбит/с, при использовании 4-х пар, является самым распространённым сетевым носителем, использующимся в компьютерных сетях до сих пор. При прокладке новых сетей пользуются несколько усовершенствованным кабелем CAT5e – (полоса частот 125 МГц), который лучше пропускает высокочастотные сигналы.
- CAT6 – (полоса частот 250 МГц) применяется в сетях Fast Ethernet и Gigabit Ethernet, состоит из 4-х пар проводников и способен передавать данные на скорости до 10 Гбит/с. Добавлен в стандарт в июне 2002 года.
- CAT7 – Скорость передачи данных до 10 Гбит/с, частота пропускаемого сигнала до 600-700 МГц. Кабель этой категории экранирован. Кроме того, для подключения к компьютеру и другим устройствам используется не привычный коннектор RJ-45, а новый, специально разработанный коннектор GG-45, который обратно совместим с коннектором RJ-45.

2.3. Спецификации Ethernet

2.3.1. 10 Мбит/с Ethernet

- 10BASE5, IEEE 802.3 (называемый также «Толстый Ethernet») – первоначальная разработка технологии со скоростью передачи данных 10 Мбит/с. Следуя раннему стандарту IEEE использует коаксиальный кабель, с волновым сопротивлением 50 Ом (RG-8), с максимальной длиной сегмента 500 метров.

- 10BASE2, IEEE 802.3a (называемый «Тонкий Ethernet») – используется кабель RG-58, с максимальной длиной сегмента 200 метров, компьютеры присоединялись один к другому, для подключения кабеля к сетевой карте нужен T-коннектор, а на кабеле должен быть BNC-коннектор. Требуется наличие терминаторов на каждом конце. Многие годы этот стандарт был основным для технологии Ethernet.
- StarLAN 10 – Первая разработка, использующая витую пару для передачи данных на скорости 10 Мбит/с. В дальнейшем, эволюционировал в стандарт 10BASE-T.
- 10BASE-T, IEEE 802.3i – для передачи данных используется 4 провода кабеля витой пары (две скрученные пары) категории-3 или категории-5. Максимальная длина сегмента 100 метров.
- FOIRL – (акроним от англ. Fiber-optic inter-repeater link). Базовый стандарт для технологии Ethernet, использующий для передачи данных оптический кабель. Максимальное расстояние передачи данных без повторителя 1 км.
- 10BASE-F, IEEE 802.3j – Основной термин для обозначения семейства 10 Мбит/с ethernet-стандартов использующих оптоволоконный кабель на расстоянии до 2 километров: 10BASE-FL, 10BASE-FB и 10BASE-FP. Из перечисленного только 10BASE-FL получил широкое распространение.
- 10BASE-FL (Fiber Link) – Улучшенная версия стандарта FOIRL. Улучшение коснулось увеличения длины сегмента до 2 км.
- 10BASE-FB (Fiber Backbone) – Сейчас неиспользуемый стандарт, предназначался для объединения повторителей в магистраль.
- 10BASE-FP (Fiber Passive)- Топология «пассивная звезда», в которой не нужны повторители – никогда не применялся.

2.3.2. Быстрый Ethernet (100 Мбит/с) (Fast Ethernet)

- 100BASE-T – Основной термин для обозначения одного из трёх стандартов 100 Мбит/с ethernet, использующий в качестве среды передачи данных витую пару. Длина сегмента до 100 метров. Включает в себя 100BASE-TX, 100BASE-T4 и 100BASE-T2.
- 100BASE-TX, IEEE 802.3u – Развитие технологии 10BASE-T, используется топология звезда, задействован кабель витая пара категории-5, в котором фактически используются 2 пары проводников, максимальная скорость передачи данных 100 Мбит/с.
- 100BASE-T4 – 100 Мбит/с ethernet по кабелю категории-3. Задействованы все 4 пары. Сейчас практически не используется. Передача данных идёт в полудуплексном режиме.
- 100BASE-T2 – Не используется. 100 Мбит/с ethernet через кабель категории-3. Используется только 2 пары. Поддерживается полнодуплексный режим передачи, когда сигналы распространяются в противоположных направлениях по каждой паре. Скорость передачи в одном направлении – 50 Мбит/с.

- 100BASE-FX – 100 Мбит/с ethernet с помощью оптоволоконного кабеля. Максимальная длина сегмента 400 метров в полудуплексном режиме (для гарантированного обнаружения коллизий) или 2 километра в полнодуплексном режиме по многомодовому оптическому волокну и до 32 километров по одномодовому.

2.3.3. Гигабит Ethernet

- 1000BASE-T, IEEE 802.3ab – Стандарт Ethernet 1 Гбит/с. Используется витая пара категории 5е или категории 6. В передаче данных участвуют все 4 пары. Скорость передачи данных – 250 Мбит/с по одной паре.
- 1000BASE-TX, – Стандарт Ethernet 1 Гбит/с, использующий только витую пару категории 6. Передающие и принимающие пары разделены физически по две пары в каждом направлении, что существенно упрощает конструкцию приемопередающих устройств. Скорость передачи данных – 500 Мбит/с по одной паре. Практически не используется.
- 1000Base-X – общий термин для обозначения технологии Гигабит Ethernet, использующей в качестве среды передачи данных оптоволоконный кабель, включает в себя 1000BASE-SX, 1000BASE-LX и 1000BASE-CX.
- 1000BASE-SX, IEEE 802.3z – 1 Гбит/с Ethernet технология, использует многомодовое волокно дальность прохождения сигнала без повторителя до 550 метров.
- 1000BASE-LX, IEEE 802.3z – 1 Гбит/с Ethernet технология, использует многомодовое волокно дальность прохождения сигнала без повторителя до 550 метров. Оптимизирована для дальних расстояний, при использовании одномодового волокна (до 10 километров).
- 1000BASE-CX – Технология Гигабит Ethernet для коротких расстояний (до 25 метров), используется специальный медный кабель (Экранированная витая пара (STP)) с волновым сопротивлением 150 Ом. Заменён стандартом 1000BASE-T, и сейчас не используется.
- 1000BASE-LH (Long Haul) – 1 Гбит/с Ethernet технология, использует одномодовый оптический кабель, дальность прохождения сигнала без повторителя до 100 километров.

2.3.4. 10 Гигабит Ethernet

- Новый стандарт 10 Гигабит Ethernet включает в себя семь стандартов физической среды для LAN, MAN и WAN. В настоящее время он описывается поправкой IEEE 802.3ae и должен войти в следующую ревизию стандарта IEEE 802.3.
- 10GBASE-CX4 – Технология 10 Гигабит Ethernet для коротких расстояний (до 15 метров), используется медный кабель CX4 и коннекторы InfiniBand.
- 10GBASE-SR – Технология 10 Гигабит Ethernet для коротких расстояний (до 26 или 82 метров, в зависимости от типа кабеля), используется многомодовое оптоволокно. Он также поддерживает расстояния до 300 метров с использованием нового многомодового оптоволокна (2000 МГц/км).

- 10GBASE-LX4 – использует уплотнение по длине волны для поддержки расстояний от 240 до 300 метров по многомодовому оптоволокну. Также поддерживает расстояния до 10 километров при использовании одномодового оптоволокну.
- 10GBASE-LR и 10GBASE-ER – эти стандарты поддерживают расстояния до 10 и 40 километров соответственно.
- 10GBASE-SW, 10GBASE-LW и 10GBASE-EW – Эти стандарты используют физический интерфейс, совместимый по скорости и формату данных с интерфейсом OC-192 / STM-64 SONET/SDH. Они подобны стандартам 10GBASE-SR, 10GBASE-LR и 10GBASE-ER соответственно, так как используют те же самые типы кабелей и расстояния передачи.
- 10GBASE-T, IEEE 802.3an-2006 – принят в июне 2006 года после 4 лет разработки. Использует экранированную витую пару. Расстояния – до 100 метров.

Стандарт 10 Гигабит Ethernet ещё слишком молод, поэтому потребуется время, чтобы понять, какие из вышеперечисленных стандартов передающих сред будут реально востребованы на рынке.

2.4. Обжим витой пары

При передаче данных на скорости до 100 Мбит\с включительно используются только 2 пары из 4, при этом задействованы контакты 1,2,3,6. Поэтому важно соблюсти именно порядок подключения контактов. Существует 2 стандарта организации EIA/TIA описывающий порядок подключения проводников витой пары.

Таблица 3. Обжим витой пары, стандарт T568A.

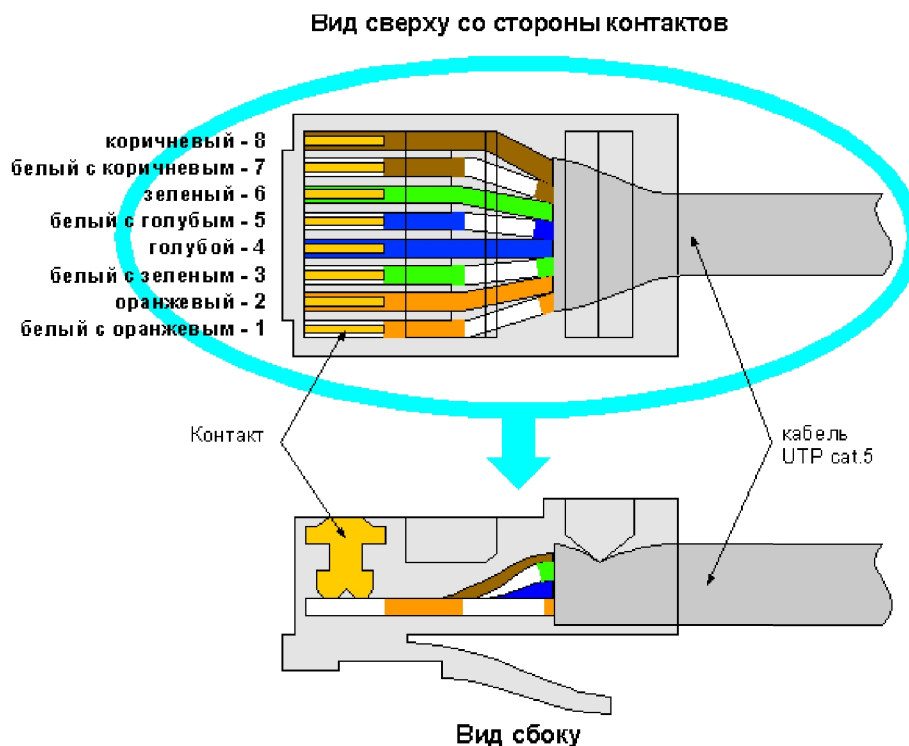
1	2	3	4	5	6	7	8
							
Бело-зеленый	Зеленый	Бело-оранжевый	Синий	Бело-синий	Оранжевый	Бело-коричневый	Коричневый

Таблица 4. Обжим витой пары, стандарт T568B.

1	2	3	4	5	6	7	8
							
Бело-оранжевый	Оранжевый	Бело-зеленый	Синий	Бело-синий	Зеленый	Бело-коричневый	Коричневый

Для того, чтобы получить так называемый прямой кабель, необходимо оба конца кабеля обжимать по одному и тому же стандарту (например T568B – такой вариант наиболее часто используется на практике). Если необходим, так называемый кроссовый кабель, то один конец обжимается по стандарту T568A, а другой по стандарту T568B, т.е. в кроссовом кабеле пары 1-2 и 3-6, меняются местами, перекрещиваются.

Прямой кабель используется для соединений: хост – коммутатор, коммутатор – роутер. Кроссоверный кабель используется для соединений: хост – хост, коммутатор – коммутатор, роутер – роутер, хост – роутер.



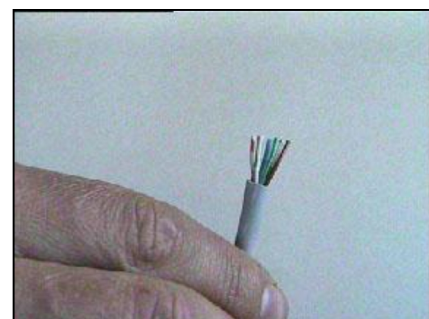
Последовательность действий при обжиме витой пары



1. Зачистка наружной изоляции круглого кабеля витой пары



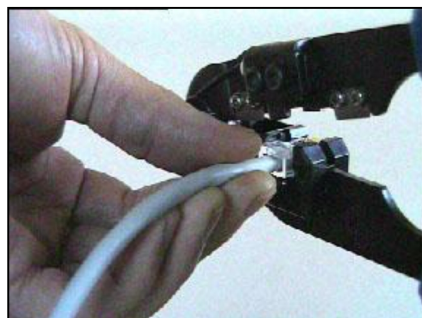
2. Удаление наружной изоляции по кольцевому надрезу



3. Все подготовлено для заправки в разъем



4. Заправка проводников витой пары в разъем RG-45



5. Установка разъема RJ-45 в гнездо обжимного устройства



6. Опрессовка разъема

3. Структурированная кабельная система

Структурированная кабельная система (СКС) представляет собой иерархическую кабельную среду передачи электрических или оптических сигналов в здании, разделённую на структурные подсистемы и состоящую из элементов — кабелей и разъёмов. По сути СКС состоит из набора медных и оптических кабелей, коммутационных панелей, соединительных шнуров, кабельных разъёмов, модульных гнёзд информационных розеток и вспомогательного оборудования. СКС обеспечивает подключение локальной АТС, одновременную работу компьютерной и телефонной сетей и предоставляет возможность гибкого изменения конфигурации кабельной системы. Кабели, оснащенные разъемами и проложенные по определенным правилам, образуют линии и магистрали. Линии, магистрали, точки подключения и коммутации являются функциональными элементами СКС.

СКС проектируется с учетом избыточности, как по числу абонентов, так и по пропускной способности. Таким образом, закладывается возможность для дальнейшего её расширения без реструктуризации. Наличие СКС существенно упрощает обслуживание и эксплуатацию компьютерных сетей и других подсистем.

Территориально СКС может покрывать один или несколько этажей здания или несколько зданий. Для кроссирования кабелей отводятся специальные помещения, называемые этажными кроссовыми (ЭК), и кроссовые здания (КЗ). В кроссовых поддерживается температурный режим, режим кондиционирования и электропитания. Этажные кроссовые соединяются вертикальной кабельной магистралью. Рабочие места и точки подключения соединяются с этажными кроссовыми горизонтальной кабельной магистралью. Вертикальная кабельная магистраль рассчитывается на большую пропускную способность, чем горизонтальная.

Каждый элемент СКС маркируется. В зависимости от типа элемента маркировка может наноситься несколько раз (в случае кабелей — как минимум на двух концах). Маркировки составляют информационную базу элементов СКС, по которой осуществляется коммутация и планирование мощностей.

Структурированная кабельная система - это универсальная кабельная система здания, группы зданий, предназначенная для использования достаточно длительный период времени без реструктуризации.

Универсальность СКС подразумевает использование ее для различных систем:

- компьютерная сеть;
- телефонная сеть;
- охранная система;
- пожарная сигнализация.

Такая кабельная система независима от оконечного оборудования, что позволяет создать гибкую коммуникационную инфраструктуру предприятия.

Структурированная кабельная система - это совокупность пассивного коммуникационного оборудования:



Кабель - этот компонент используется как среда передачи данных СКС. Кабель различают на экранированный и неэкранированный.

Розетки - этот компонент используют как точки входа в кабельную сеть здания.

Коммутационные панели (патч-панели) - используются для администрирования кабельных систем в коммутационных центрах этажей и здания в целом.

Коммутационные шнуры (патч-корды) - используются для подключения офисного оборудования в кабельную сеть здания, организации структуры кабельной системы в центрах коммутации.

СКС - охватывает все пространство здания, соединяет все точки средств передачи информации, такие как компьютеры, телефоны, датчики пожарной и охранной сигнализации, системы видеонаблюдения и контроля доступа. Все эти средства обеспечиваются индивидуальной точкой входа в общую систему здания. Линии, отдельные для каждой информационной розетки, связывают точки входа с коммутационным центром этажа, образуя горизонтальную кабельную подсистему. Все этажные коммутационные узлы специальными магистралями объединяются в коммутационном центре здания. Сюда же подводятся внешние кабельные магистрали для подключения здания к глобальным информационным ресурсам, таким как телефония, интернет и т.п. Такая топология позволяет надежно управлять всей системой здания, обеспечивает гибкость и простоту системы.

Составные части СКС на плане этажа:

- 1 - Рабочее место, рабочая зона.
- 2 - Горизонтальная кабельная проводка.
- 3 - Коммутационный узел этажа.
- 4 - Вертикальная кабельная проводка.
- 5 - Служебные технические средства.

Рабочее место - область, где установлены технические средства пользователя, подключенные к кабельной сети здания. Рабочее место оснащается не менее чем двумя информационными розетками, так как типичное офисное рабочее место содержит как минимум компьютер пользователя и его телефон. Для их подключения к СКС используются розетки со стандартизированным разъемом RJ-45 и коммутационные шнуры длиной от 1 до 5 метров.

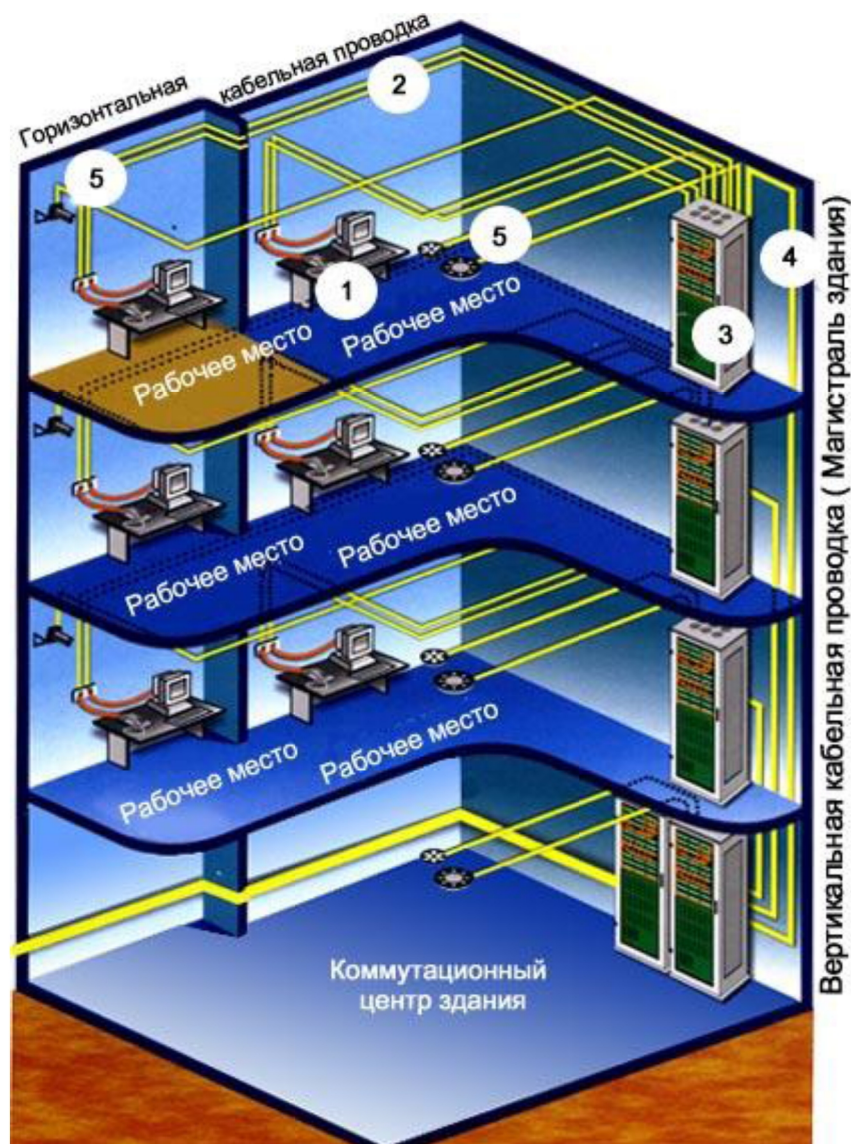
Горизонтальная кабельная проводка - кабельные линии, соединяющие рабочее место с коммутационным узлом этажа. Горизонтальная кабельная проводка, на основе медных проводников, использует четырехпарный одножильный кабель в различном исполнении. В обычных условиях применяются неэкранированный, а при повышенных требованиях к электромагнитному излучению, совместимости или конфиденциальности - экранированный кабель.

Коммутационный узел этажа - область, в которой сходятся линии горизонтальной кабельной проводки, размещается коммутационное оборудование и осуществляется администрирование кабельной системы этажа. Под администрированием понимается внесение изменений и дополнений в существующие конфигурации. Основой таких центров являются патч и кросс-панели. Для простоты монтажа и удобства работы, коммутационное оборудование размещают в специальных шкафах и стойках, к которым подводятся все кабельные линии. Шкафы также выполняют функцию ограничения доступа к коммутационному оборудованию.

Вертикальная кабельная проводка - кабельные линии, соединяющие коммутационный узел этажа с коммутационным центром здания.

Магистральная подсистема - подсистема комплекса зданий, которая может строиться из медного и/или оптоволоконного типов кабеля, и которая объединяет кабельные системы зданий.

В каждом конкретном здании в общем случае присутствуют три подсистемы СКС: вертикальная кабельная подсистема, горизонтальная кабельная подсистема и подсистема рабочих мест. Для достаточно крупных зданий, с большим количеством рабочих мест на этажах, все эти три подсистемы присутствуют в явном виде. Для относительно небольших зданий с ограниченным количеством рабочих мест рекомендуется организовывать один узел коммутации СКС, куда сходится вся горизонтальная кабельная разводка. В этом случае вертикальная кабельная подсистема может отсутствовать либо носить вырожденный характер, при котором вертикальная кабельная подсистема представляется совокупностью коммутационных шнуров, соединяющих порты "этажных" коммутаторов ЛВС (коммутаторов для подключений рабочих мест) с портами центрального (магистрального) коммутатора.



- **Оргтехника**- компьютер, телефон, факс и другое периферийное оборудование



- **Датчик пожарной сигнализации**- использует СКС как среду передачи данных пожарной телеметрии безопасности здания



- **Система видеонаблюдения**- использует СКС как среду передачи видеосигнала



- **Коммутационный шнур**- использует для перенаправления кабельных линий в центре ком-



- **Информационная розетка**- служит точкой входа в кабельную сеть здания



- **Датчик охранной сигнализации**- использует СКС как среду передачи данных телеметрии безопасности здания



- Кабельная проводка прокладывается по закладным каналам внутри стен, по декоративным кабельным коробам внутри помещений, по лоткам за фальш-потолками или под фальш-полами



- **Коммутационная панель**- объединяет входы кабельных линий, и используется для администрирова-

мутации и для подключения
оборудования к информацион-
ным розеткам

ния кабельной системы в центре
коммутации



- **Коммутационный узел** - предназначен для монтажа и использования коммутационного оборудования кабельной системы, для централизации внешних и внутренних кабельных входов, для соединения кабельной системы с активным сетевым оборудованием

Литература по СКС

Смирнов И. Г. Структурированные кабельные системы - проектирование, монтаж и сертификация. Из-во: Экон-Информ, 2005 г. ISBN 5-9506-0144-0

Самарский П. А. Основы структурированных кабельных систем. Из-во: ДМК - АйТи, 2005 г. ISBN 5-98453-014-7

Семенов А.Б., Стрижаков С.К., Сунчелей И.Р. Структурированные кабельные системы. Из-во: ДМК Пресс. ISBN 5-98453-003-1

**Список контрольных вопросов
к лабораторной работе
Локальные сети на витой паре**

1. Дайте определение СКС.
2. Для каких систем используется СКС?
3. Перечислите составные части СКС.
4. Перечислите и нарисуйте основные топологии локальных сетей.
5. Опишите устройство и назначение коаксиального кабеля.
6. Опишите устройство и назначение витой пары.
7. Опишите стандарты EIA/TIA подключения проводников витой пары.
8. Перечислите назначение и основные функции сетевого тестера Fluke LinkRunner.
9. Перечислите назначение и основные функции квалифицирующего сетевого тестера Fluke CableIQ.
10. Дайте определений основных типов сетей по их масштабу: LAN, MAN, WAN.
11. Перечислите параметры кабеля (разделяемой среды) для 100BASE-TX.
12. Перечислите параметры кабеля (разделяемой среды) для 1000BASE-T.

**ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ОТЧЕТА
ПО ЛАБОРАТОРНОЙ РАБОТЕ**

Отчет по лабораторной работе должен содержать:

1. Титульный лист (см. образец).
2. Перечень выполненных заданий (с указанием результатов измерений, вариантов решения тестовых заданий, адресной информации, команд и их параметров – в зависимости от содержания пункта задания).
3. Письменный ответ на указанный преподавателем контрольный вопрос.

Отчет предоставляется преподавателю в электронной форме, в формате MS Word (шаблон названия файла: **ктк_ЛР_№_ группа_фамилия.doc**).

Образец титульного листа отчета

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Самарский государственный аэрокосмический университет
имени академика С.П. Королева
(национальный исследовательский университет)»

Факультет информатики
Кафедра технической кибернетики

ОТЧЕТ

по лабораторной работе по дисциплине
Компьютерные телекоммуникации
на тему
Локальные сети на витой паре

Выполнил студент 63Х группы Фамилия И.О.

Использование сетевых тестеров Fluke для диагностики локальных сетей

Использование сетевого тестера LinkRunner

Для успешного устранения любых проблем, связанных с сетью, важно применять правильную методологию:

1. Документируйте вашу сеть

Если у вас всегда есть под рукой актуальная сетевая документация (физические и логические схемы, базисные характеристики сети, результаты аудита или инвентаризации, настройки, таблицы адресов и привязок к хостам и т.п.), это существенно уменьшает время на устранение сбоя - время, которое, в противном случае, вы вынуждены тратить на работу в режиме обследования, чтобы всего лишь определить, в какой точке сети (общей схемы) подключен персональный компьютер, который, возможно, несет ответственность за возникновение проблемы.

2. Собирайте всю доступную информацию и анализируйте симптомы сбоя

Определите, изменялось ли что-либо в сети или в настройках самой рабочей станции непосредственно перед тем, как возникла проблема.

Прибор LinkRunner можно подключать в любой конечной точке сети; он позволяет сетевым инженерам без труда находить неисправности в среде передачи и исключать проблемы с физическим уровнем до того, как проводить диагностику на более высоком уровне.

Подключенный в той точке, где возникла проблема, прибор LinkRunner позволяет проверить ряд критически важных сетевых параметров, а также выдает информацию, на основе которой можно подготовиться к устранению сбоев, причины которых относятся к более высоким уровням модели взаимодействия OSI.

3. Локализуите сбой

Прежде всего, необходимо сузить зону поиска. Проблема затрагивает целый участок сети или только одного из пользователей? Даже если сбой касается только одного пользователя, причина может быть и в сети, и в физической среде передачи, и в самой рабочей станции. Зачастую процессы сбора информации и локализации проблемы проходят параллельно.

4. Устраните сбой и убедитесь, что проблема исчерпана

Если вы локализовали сбой, то определить его конкретный тип и необходимые меры по устранению будет несложно. Если причина в аппаратном обеспечении, то, скорее всего, придется физически заменить неисправный компонент, например, подключить новый патч-шнур, сменить порт на хабе или коммутаторе на другой или заменить сетевую карту в компьютере. Этот этап работы считается полностью завершенным, как только пользователь, вернувшись к своему компьютеру, убеждается, что проблема исчезла.

5. *Задокументируйте свои действия*

Вернитесь к пункту 1. Если по каждому возникшему сбою есть запись (о том, как он появился и как был устранен - такую функцию предлагает большинство соответствующих учетных приложений), то из них постепенно сформируется ваша внутренняя база данных. В будущем вы всегда сможете обратиться к ней, если похожая проблема возникнет снова.

Хотя операционные системы и программное обеспечение становятся с каждым годом все надежнее, все равно первым ответом системного администратора на жалобу пользователя будет: “Попробуйте перезагрузиться”. К сожалению, холодная перезагрузка устраняет так много разных проблем (часть из которых вообще необъяснима!), что этот шаг действительно необходим.

Большинство пользователей в состоянии запустить командную строку и сообщить администратору, что они получили в ответ на команду IPCONFIG. Это позволит убедиться, правильный ли адрес подсети установлен в компьютере.

Если персональный компьютер сконфигурирован по протоколу динамической конфигурации хоста (DHCP), но возвращает в ответ IP-адрес Windows по умолчанию (169.254.x.x), значит, у клиента нет связи с DHCP-сервером.

Портативные компьютеры обычно используют адрес той сети, к которой они подключаются в настоящий момент (динамический адрес), но иногда настройка DHCP предыдущей сети остается и после того, как компьютер уже перемещен. Попросите пользователя набрать две следующие команды в командной строке:

C:\>ipconfig /release

C:\>ipconfig /renew

Пусть пользователь попробует взять себе другой IP-адрес, который придет ему в ответ на вторую команду. Если команда IPCONFIG выдает в ответ сообщение о том, что DHCP-операцию выполнить невозможно, то, скорее всего, у пользователя установлен статический IP-адрес. Сверьте установленный IP-адрес с вашей документацией.

Если пользователь подтверждает правильность IP-адреса, попробуйте отправить на него со своего рабочего места запрос ping. Если рабочая станция откликается, то тогда надо попросить пользователя выполнить какое-либо другое действие с сетью, например, зайти на какую-нибудь веб-страницу или отправить запрос ping на локальный маршрутизатор, чтобы убедиться в том, что основное соединение с сетью есть.

Идентификация сбоя с рабочего места пользователя

Когда сетевой специалист приходит на рабочее место пользователя, очень важно серьезно отнестись к сбору информации о сбое. Расспросите пользователя обо всем, что он делал, когда с сетью возникла проблема. Иногда такой опрос провести нелегко, потому что зачастую пользователи даже не подозревают, как много самых обычных действий, выполненных на рабочей станции, влияет на параметры системы в целом. В худшем же случае пользователь отлично знает: то, что он натворил, делать было категорически нельзя. Тогда он ни за что не признается в этом. Как известно, все сомнения толкуются в пользу обвиняемого,

поэтому сначала надо расспросить пользователя обо всех недавних изменениях, включая даже перестановку мебели или скачку новой программки-хранителя экрана.

Повторите лично все те тесты, которые по телефону вы просили провести пользователя. Успешно прошедший запрос ping к сетевому серверу или к устройству за пределами сети немедленно говорит о том, что у рабочей станции проблемы с соединением с сетью на уровне 3 (сетевом) или выше. Тогда тесты всех более низких уровней уже не нужны, так что инженер может не принимать их во внимание.

Если же установку соединения на уровне 3 подтвердить не удастся, то вам придется начать с уровня 1.

Если проблема то появляется, то исчезает, или носит нерегулярный характер, то к целевому устройству необходимо отправлять непрерывный запрос ping с бесконечным потоком пакетов с запросами отклика. В ответ вы получите время отклика для каждого успешного запроса ping или время истечения для запросов, не получивших ответа.

C:\> ping -t x.x.x.x

Долгий отклик или пропущенные запросы можно затем проверить, отследив их до целевого устройства с помощью команд TRACERT или PATHPING. Трассировка покажет, в какой точке пути по сети возникает задержка или пропадают пакеты, и в этой точке надо будет проверить все, начиная с уровня 1.

C:\> tracert x.x.x.x

или

C:\> pathping x.x.x.x

Первые тесты при проведении диагностики на рабочем месте:

1. Тест на наличие соединения.
2. Проверка общей активности в сегменте сети.
3. Использование DHCP для диагностических целей.
4. Отправка запроса ping на локальные и удаленные адреса.

Тестирование соединения

Определить наличие подключения можно с помощью процесса автосогласования, в ходе которого два участника обмениваются информацией о своей скорости и настройках дуплекса. В результате такого обмена участники сравнивают свои возможности, а затем устанавливают соединение друг с другом на максимальной скорости, приемлемой для обоих устройств, и с соответствующими настройками дуплекса. Если у одного из участников не вполне корректные настройки или драйвера работают ненадлежащим образом, то процесс может дать сбой: приемлемые для обеих сторон настройки подобрать не удастся, поэтому связь будет неустойчивой, а может, даже будет полностью отсутствовать.

Как только вы подключили тестер LinkRunner к сегменту сети, он сразу же пытается установить связь с устройством на дальнем конце, каким бы оно ни было -хаб, коммутатор или сетевая карта персонального компьютера. Прибор LinkRunner в точности следует процедуре автосогласования, как она описана в

стандарте IEEE 802.3, при этом его светодиодный индикатор контролируется аппаратно, а не программным обеспечением. После того, как автосогласование успешно завершится, светодиод прибора LinkRunner будет гореть ярким зеленым светом, а результирующие скорость и дуплекс будут показаны в верхнем левом углу экрана.



На экране тестера LinkRunner показаны параметры успешно установленного соединения: скорость, дуплекс и процент использования.

Проверка общей активности в сегменте сети

Если в кабеле присутствует сетевой трафик, прибор LinkRunner показывает на экране степень использования в виде гистограммы.

Если вы тестируете совместно используемую среду Ethernet, где по-прежнему вместо коммутаторов используются хабы, то весьма вероятно, что сеть использует полудуплекс. Полудуплексный Ethernet ограничивает и количество станций, которые могут вести передачу одновременно, и размеры передаваемых пакетов. Если вести передачу одновременно пытается слишком много станций, то производительность Ethernet может значительно ухудшиться из-за коллизий. Если же вы тестируете сеть, в которой каждая станция подключена к отдельному порту коммутатора, риск чрезмерных коллизий уменьшается до пренебрежимо малого значения.

Хотя существование коллизий - нормальное явление для полудуплексных сетей Ethernet, тем не менее, существует очень неприятный эффект лавины: когда количество коллизий растет вместе с ростом трафика, сам трафик начинает увеличиваться за счет перепосылки пакетов. В результате производительность сети не просто снижается, а резко падает, при том, что количество отправленных пакетов, количество коллизий, а также пакетов, вынужденно отправленных повторно, растет как снежный ком. Как это всегда бывает, если производительность резко упала - ждите шквала жалоб от пользователей.

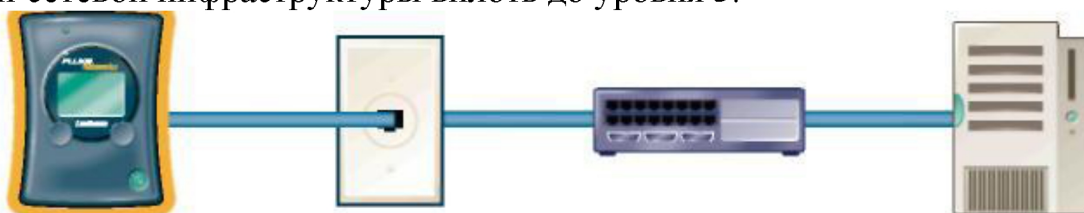
В большинстве сетей Ethernet обычный уровень трафика незначителен, и тогда проблему надо искать где-то в другом месте. Прибор LinkRunner может предоставить вам базовую статистику по уровням использования в сегменте, и это может стать ключом к пониманию проблем с низкой производительностью сети.

Использование DHCP для диагностических целей

Если удалось установить соединение, а уровень использования похож на правду, то теперь следует нажать кнопку, управляющую запросом ping. Прибор LinkRunner попытается получить от DHCP-сервера корректный IP-адрес. Поскольку нормальная работа DHCP основана на широковещательной технологии, то либо необходимо ставить по отдельному DHCP-серверу для каждой подсети (что дорого и сложно с точки зрения управления), либо использовать агенты-ретрансляторы DHCP, сортирующие и перенаправляющие

запросы и отклики между клиентами и серверами, физически находящимися в разных подсетях. Такие вспомогательные приложения на маршрутизаторах, регулирующие широковещательные рассылки - самый распространенный способ работы для корпоративных сетей, где предпочитают держать DHCP-сервера только в центре сети, в штаб-квартире. Невозможность автоматически получить от DHCP-сервера корректную настройку для клиента или прибора LinkRunner указывает на возможные проблемы системой ретрансляции DHCP.

Хотя в большинстве современных сетей используется протокол DHCP, тем не менее, прибор LinkRunner позволяет установить IP-адрес и вручную, статически. Успешное получение DHCP-адреса свидетельствует о том, что кабель, порт хаба или коммутатора и вся сетевая инфраструктура до DHCP-сервера работают корректно. Одна простая процедура позволяет проверить прилегающие участки сетевой инфраструктуры вплоть до уровня 3.



Успешное назначение DHCP-адреса подтверждает, что пользователь имеет работающее сетевое подключение и в состоянии получить правильный IP-адрес: это проверка с первого по третий сетевой уровень за один шаг.

Отправка запроса ping на локальные и удаленные адреса

Запрос ping - одно из самых популярных средств диагностики в истории компьютерных сетей. Эта функция включена во все распространенные операционные системы, которые предусматривают взаимодействие с Интернет, и когда нужно провести диагностику сбоя, чаще всего сетевые инженеры используют ее первой.

Утилита ping посылает сигнал (как правило, пакет ICMP с запросом отклика), который “отражается” устройством назначения (точнее, оно генерирует сигнал-отклик), что позволяет отправителю удостовериться, что устройство назначения находится в нужном месте, а заодно определить, сколько времени занимает путь сигнала туда и обратно.



Запрос ping можно отправлять и в локальные системы, и транзитом в удаленные, через Интернет.

Получив в самом начале адрес от DHCP-сервера и настроившись на него, прибор LinkRunner немедленно начинает отправку тестовых запросов ping к DNS-серверу (проверяя службу доменных имен) и к маршрутизатору, установленному по умолчанию. Адреса обоих были получены в ходе конфигурирования протокола DHCP.

Прибору LinkRunner можно дополнительно задать до четырех IP-адресов, один из которых можно отвести для функции автоматической отправки запросов ping. Успешное получение отклика на запрос ping при проверке веб-приложений, при идентификации пользователя и т.п. показывает, что эти сетевые сервисы принципиально доступны с рабочей станции клиента.

Сам факт прохождения запроса ping свидетельствует о том, что в сети вплоть до уровня 3 существует связь между двумя устройствами. Период кругового обращения (время путешествия сигнала туда и обратно) следует сравнить с известными значениями, и это уже дает вам представление о работе сети, достаточное для того, чтобы решить, нужно ли применить более глубокий анализ. Тем не менее, запросы ICMP сами по себе относятся к трафику с низким приоритетом, поэтому они могут оказаться отброшенными, если один из маршрутизаторов в сетевом пути или устройство назначения заняты. Вот почему следует отправлять запросы ping сериями -это даст устройству назначения больше возможностей ответить.

Сервера за пределами корпоративной сети тоже можно использовать в качестве точек назначения запросов ping, это позволяет проверить связь по глобальной сети между рабочей станцией клиента и локальным или удаленным узлом. Если сервера в пределах ответственности брандмауэра отвечают на запрос ping, а за пределами - нет, то сетевому инженеру стоит проверить маршрутизаторы или другие пограничные сетевые устройства -проблема может заключаться в них. Если часть серверов отвечает, а другая часть -нет, следует проанализировать отдельные сегменты сети и выяснить, почему они недоступны. Если запросы ping успешно получают отклик как от внутренних, так и от внешних серверов, включая приложения и сервисы, но клиент ими воспользоваться не может, значит, проблема возникает на каком-то другом уровне - она не связана с физической передачей сигналов. Успешное прохождение запросов ping говорит о том, что определенные типы трафика достигают сервера назначения; значит, невозможность получить доступ к каким-либо сервисам связана с учетной записью или настройками сервера.

Если проблему не удалось сходу идентифицировать и устранить с помощью описанных тестов “первой помощи”, то дальнейшие события могут развиваться по двум возможным направлениям.

- Если тесты показывают, что отсутствует связь, нет подключения к Ethernet, надо внимательно проверить сетевой кабель.

- Если первые тесты прошли успешно, связь есть, в сегменте присутствует некоторый трафик, похожий на обычный, от DHCP-сервера удастся получить адреса, и запросы ping к самым важным сетевым серверам проходят успешно, тогда проблема, скорее всего, возникает на более высоких сетевых уровнях.

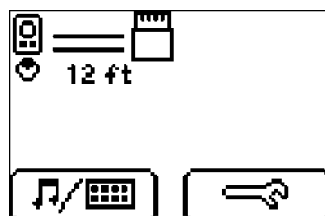
И разрешать их также следует на соответствующих сетевых уровнях: администратору надо будет проверять настройки учетной записи и конфигурацию рабочей станции.

Тестирование кабеля

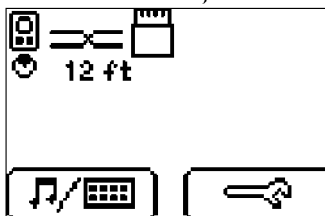
Первый кабель, который обязательно надо проверять - это патч-шнур, подключающий рабочую станцию или другое устройство к настенной розетке. Для такой проверки следует подключить один конец патч-шнура к сетевому гнезду прибора LinkRunner, а другой - ко второму гнезду, специально предназначенному для тестирования схемы разводки. Если с патч-шнуром все в порядке, его можно снова подключить к настенной или напольной розетке и использовать в следующих этапах тестирования.

Затем необходимо проверить, не кроется ли проблема со средой передачи в других участках кабеля - от стенной розетки до порта ближайшего коммутатора. Если в телекоммуникационном помещении очень много разных сетевых подключений, то найти нужный кабель в массе других, лежащих в трассе, не так-то легко - на это может потребоваться масса времени. Но прибор LinkRunner оснащен двумя функциями, которые существенно облегчают эту задачу и сводят затраты времени к минимуму. Тестер LinkRunner может работать как тон-генератор, подавая в кабель тональный сигнал, который можно обнаруживать специальным детектором. С помощью стандартного детектора кабели можно перебрать по порядку, пока тональный сигнал не укажет на нужный из них. Эта методика используется в тех случаях, когда точно не известно, подключен ли кабель к коммутатору, или в документации нет данных о том, какая настенная розетка к какому порту ведет.

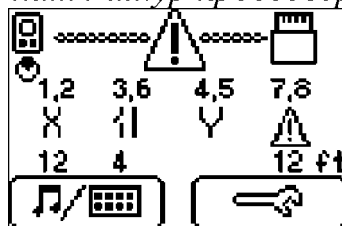
После того, как удаленный конец сегмента обнаружен, к нему следует подключить адаптер для тестирования схемы разводки: LinkRunner Wiremap Adapter или один из аксессуаров к прибору - например, идентификатор LinkRunner Cable ID, заказываемый дополнительно. При таком подключении схема разводки и наличие контакта проверяются во всем горизонтальном сегменте.



Так прибор LinkRunner показывает, что патч-шнур нормальный...



...что патч-шнур кроссоверный...



...и что патч-шнур неисправен.

Одновременно с тональным сигналом прибор Link Runner подает в кабель питание, чтобы светодиод над портом коммутатора мигал каждые три секунды. Эта функция очень облегчает поиск нужного порта. Когда порт установлен попробуйте переключить патч-шнур в другой (свободный) порт. Довольно часто порты, с которыми что-то не в порядке или которые уже совсем вышли из строя, все еще показывают светодиодами наличие подключения, и в таких случаях простая смена порта устраняет проблему.

Если же порт хаба или коммутатора в порядке, то проблему надо искать на рабочей станции. Сетевую карту на рабочей станции можно проверить, подключив к ней прибор LinkRunner напрямую. Так же, как и с портами хаба или коммутатора, тестер LinkRunner покажет наличие соединения, скорость и настройки дуплекса, предлагаемые сетевой картой. Если соединение есть, то следует перезагрузить компьютер или использовать утилиту командной строки для отправки запроса ping, чтобы сгенерировать трафик, который прибор LinkRunner сможет оценить. Если LinkRunner не показывает никакого трафика вообще (даже если персональный компьютер подтверждает, что ведет передачу), то необходимо проверить привязку драйверов и другие параметры конфигурации персонального компьютера. Если прибор LinkRunner сообщает о наличии и соединения, и трафика от персонального компьютера, то тогда следует детально проверять сетевые настройки персонального компьютера.

Диагностика на более высоких уровнях

Если рабочая станция устанавливает связь с сетью, то следующий этап проверки - убедиться, что адрес рабочей станции соответствует маске подсети, в которой она физически находится. Проверьте, чтобы рабочая станция оперировала правильным набором протоколов и чтобы они были правильно настроены. Наконец, сетевой инженер должен убедиться, что на компьютере установлены все необходимые программные компоненты и библиотеки. Обычно это проверяется путем удаления и последующей установки заново протокола или сетевой карты в конфигурации рабочей станции. Если все нужные компоненты на месте и правильно сконфигурированы, но при этом рабочая станция все еще не может корректно подключиться к сети и запустить соответствующие приложения, это говорит о том, что проблема имеет более высокий уровень и потребует проведения сетевого анализа другими техническими средствами.

Квалифицирующий сетевой тестер Fluke CableIQ

Тестер для проверки медного кабеля предназначен для устранения неисправностей в кабелях и определения возможности поддержки ими различных скоростей (10/100/1000/VoIP).

Основные возможности продукта:

- Квалификация - прибор проверяет, обеспечивают ли существующие кабели достаточную пропускную способность для поддержки передачи голоса, стандартов 10/100 Ethernet, VoIP или Gigabit Ethernet.
- Устранение неисправностей - отображение причин, по которым существующие кабели не поддерживают требуемую пропускную способность сети (например, перекрестные помехи при длине кабеля свыше 11 м).
- Обнаружение - прибор определяет, что находится на конце каждого кабеля, и отображает сведения о конфигурации устройства (скорость/дуплекс/пары).
- Определение неиспользованных портов коммутатора, доступных для перераспределения.
- Составление карт конфигурации проводки и отображение расстояния до мест возникновения неисправностей с помощью теста Intelligent Wiremap.
- Проверка всех типов кабелей с медными жилами: витая пара, коаксиальный кабель и аудиокабель.

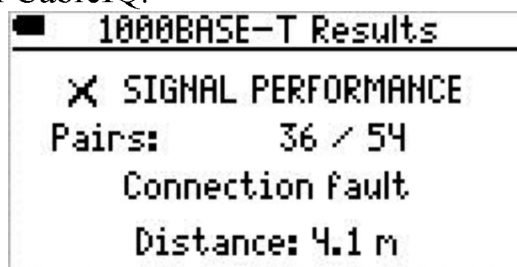
Термин "Квалификация" - это новая категория контрольно-измерительных приборов (тестеров), созданных для быстрого и эффективного решения задач, с которыми могут столкнуться ИТ специалисты при модернизации кабельных соединений и переходе на поддержку новых высокоскоростных сетевых технологий, а также для разрешения проблем с подключением пользователей к сети.

Квалифицирующий кабельный тестер, такой как новый CableIQ Qualification Tester (ciq-100, ciq-kit) от компании Fluke Networks, позволит определить сможет ли существующая кабельная система соответствовать новым требованиям, предъявляемым к ней новой сетевой технологией. Данная категория приборов отличается от сертифицирующих кабельных тестеров, таких как DTX CableAnalyzer (dtx-lt, dtx-1200, dtx-1800), которые оценивают соответствие кабельных систем на соответствие стандартов TIA/ISO и базовых тестеров кабеля, таких как MicroScanner Pro (mt-8200-32a, mt-8200-24a), которые проверяют только правильность проводников в кабеле и занимает промежуточное положение между ними.

Квалифицирующие кабельные тестеры позволяют выполнить серию тестов для более эффективного устранения проблем с подключением к сети и понять, к какой области относится проблема к кабелю или сетевому оборудованию. Например, первый шаг - проверка настроек порта активного оборудования и сетевой карты и определения возможного рассогласования по скорости или дуплексу. В случае если настройки соответствуют, то следующим шагом будет тест для квалификации соединения. Выполнение теста позволит понять -

достаточно ли полосы пропускания тестируемого кабеля для поддержания желаемой сетевой технологии для этого соединения.

С помощью режима Discover мы сможем быстро определить, что подключено к кабелю с другой стороны (ПК, порт активного оборудования) или он свободный. Используя функцию Hub Blink, прибор позволяет определить к какому порту коммутатора подключен кабель по мигающему индикатору порта. Возможно, Вы будете удивлены, как много незадействованных портов можно обнаружить при помощи CableIQ.



Подключите cableiq: ciq-100, ciq-kit к любому кабелю, коммутационной панели или розетке на стене - на экране мгновенно будет представлена детальная информация по данному кабелю (длина/схема соединения) и информация по устройству, которое может быть подключено на другом конце кабеля (скорость/дуплекс соединения). Полученная информация позволяет разрешить любые проблемы с подключением пользователей или оборудования к сети. Например, если режим Discover показывает что соединение согласовано по скорости и дуплексу, но проблема с соединением остается, следующим шагом будет запуск Autotest для проверки полосы пропускания. Если соединение не пройдет квалификацию, то в этом случае прибор предоставит информацию о причине сбоя, например высокий уровень переходного затухания в кабеле или большое изменение импеданса.



Для трассировки кабеля с помощью номерных идентификаторов вставьте идентификаторы в розетки на рабочих места, после этого протестируете кабельные соединения, подключая прибор к коммутационной панели в кроссовой. Для каждого соединения CableIQ отобразит схему разводки, длину по парам, расстояние до неисправностей (если они есть) и номер идентификатора, который находится на другом конце кабеля.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Самарский государственный аэрокосмический университет
имени академика С.П. Королева
(национальный исследовательский университет)»

Факультет информатики
Кафедра технической кибернетики

**Адресация в IP-сетях.
Практикум по IP-адресации**

**Методические указания к лабораторной работе
по курсу компьютерные телекоммуникации**

Составитель Суханов С.В., к.т.н., доцент

УДК 681.3

Адресация в IP-сетях. Практикум по IP-адресации:

Метод. указания / Самар. гос. аэрокосм. ун-т. Сост. Суханов С.В.
Самара, 2011. – 26 с.

Кратко изложены теоретические сведения о принципах адресации протокола IPv4, правилах использования масок переменной длины. Приведены краткие сведения о других протоколах, обеспечивающих согласованное использование IP-адресов, MAC-адресов, DNS-имен. Настоящие методические указания содержат задачи по IP-адресации, решение которых позволит студентам выработать навыки поиска и устранения проблем в компьютерных сетях, навыки планирования и разработки адресных схем.

Методические указания предназначены для студентов факультета информатики, обучающихся по специальности 01.05.01 Прикладная математика и информатика, направлений 01.05.00 Прикладная математика и информатика и 01.06.00 Прикладные математика и физика.

СОДЕРЖАНИЕ

1. АДРЕСАЦИЯ В IP-СЕТЯХ	4
1.1. Три уровня адресации	4
1.2. Формат IP-адреса (нотация)	5
1.3. Особые (зарезервированные) IP-адреса	6
1.4. Формат IP-адреса и маска подсети	8
1.5. Пример использования маски при IP-адресации	9
2. РАСПРЕДЕЛЕНИЕ IP-АДРЕСОВ В СЕТИ ИНТЕРНЕТ	10
2.1. Дефицит IP адресов и его преодоление	10
2.2. Адресация и технология CIDR.....	11
3. ОТОБРАЖЕНИЕ IP-АДРЕСОВ НА ЛОКАЛЬНЫЕ АДРЕСА	12
3.1. Протокол ARP.....	12
3.2. Алгоритм работы протокола ARP	13
3.3. Отображение IP-адресов на локальные адреса за пределами локальной сети.....	14
3.4. Отображение IP-адресов на локальные адреса в глобальных сетях	14
4. ОТОБРАЖЕНИЕ СИМВОЛЬНЫХ АДРЕСОВ НА IP-АДРЕСА: СЛУЖБА DNS	14
5. АВТОМАТИЗАЦИЯ ПРОЦЕССА НАЗНАЧЕНИЯ IP-АДРЕСОВ УЗЛАМ СЕТИ: ПРОТОКОЛ DHCP	15
5.1. Алгоритм работы протокола DHCP	16
6. ЗАДАЧИ НА IP-АДРЕСАЦИЮ	18

1. АДРЕСАЦИЯ В IP-СЕТЯХ

1.1. Три уровня адресации

Каждый **компьютер (узел, хост)**, а точнее, его сетевой интерфейс в сети TCP/IP может иметь адреса трех уровней:

1. Локальный (аппаратный) адрес узла (MAC-адрес).
2. Сетевой или IP-адрес, состоящий из 4 байт (протокол IPv4).
3. Символьное (доменное) имя.

Локальный (аппаратный) адрес узла - в большинстве технологий локальных сетей - это MAC-адрес сетевого адаптера или порта маршрутизатора (используется на втором, канальном уровне модели OSI), например:

11-A0-17-3D-BC-01.

Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизованно. MAC-адрес имеет формат 6 байтов: старшие 3 байта - идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем.

Сетевой или IP-адрес состоит из 4 байт (протокол IPv4), например:

109.26.17.100.

Этот адрес используется на сетевом уровне (третьем уровне модели OSI). Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов.

IP-адрес состоит из двух частей: **номера сети** и **номера узла**.

Номер сети может быть выбран администратором, либо назначен по рекомендации Network Information Center (NIC), если сеть должна работать как составная часть Internet. Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами. **Номер узла** в протоколе IPv4 назначается независимо от локального адреса узла.

Деление IP-адреса на поле номера сети и номера узла - гибкое, и граница между этими полями может изменяться в широких пределах (например, с помощью **масок**).

Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей (портов). Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение (интерфейс, порт).

Символьное (доменное) имя (идентификатор), например:

SERV1.IBM.COM

Адрес этого типа назначается администратором (не все узлы или порты имеют такой адрес) и состоит из нескольких частей, например, имени компьютера, имени организации, имени домена. Такой адрес, называемый также DNS-именем, используется на прикладном уровне модели OSI, например, в протоколах FTP или telnet.

Задачи адресации в стеке TCP/IP:

- Согласованное использование адресов различного типа (например, преобразование IP-адреса в MAC-адрес, доменного имени в IP-адрес, см. рис. 1).
- Обеспечение уникальности адресов (в пределах компьютера, подсети, корпоративной сети или Интернета).
- Конфигурирование сетевых интерфейсов и сетевых приложений.
- Обеспечение масштабируемости.

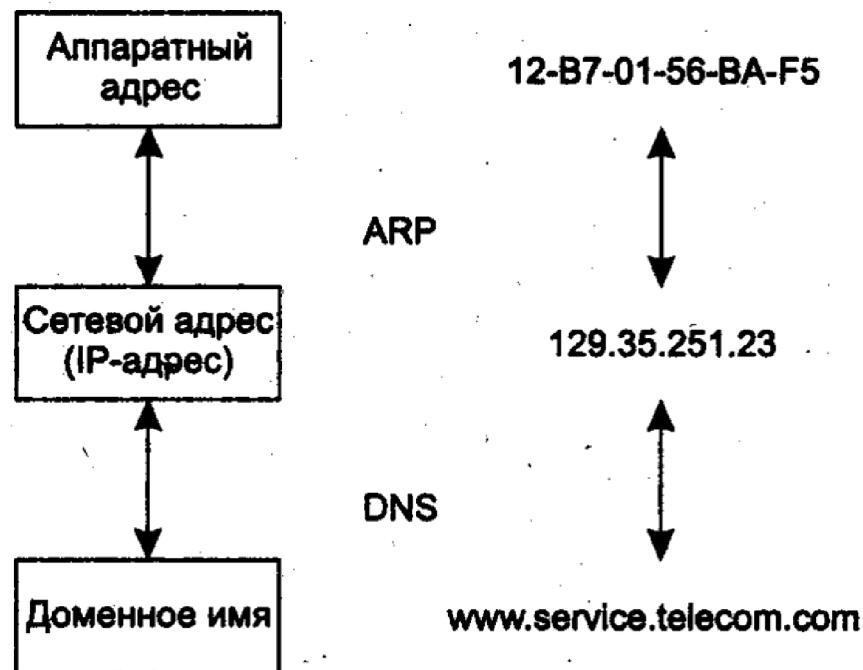


Рис. 1. Преобразование (отображение) адресов различных типов

1.2. Формат IP-адреса (нотация)

Наиболее распространенной формой представления IP-адреса является запись в виде четырех чисел, представляющих значения каждого байта в десятичной форме и разделенных точками:

128.10.2.30

Этот же адрес может быть представлен в двоичном формате, также разделенных точками (такая нотация используется редко, главным образом для пояснения способов преобразования адресов, выделения номеров сети и хоста с помощью масок):

1000 0000. 0000 1010. 0000 0010. 0001 1110

и в шестнадцатеричном формате (с точками):

80.0A.02.1D

В таблице 1 приведен более полный перечень различных форм представления IP-адреса и их связь между собой.

Формы представления IP-адреса

Нотация	Вид адреса	Преобразование из точечно-десятичной нотации
Точечно-десятичная Dot-decimal notation (DDN)	192.0.2.235	не требуется
Точечно-шестнадцатеричная Dotted Hexadecimal	0xC0.0x00.0x02.0xEB	Каждый октет независимо преобразуется шестнадцатеричную форму
Точечно-восьмеричная Dotted Octal	0300.0000.0002.0353	Каждый октет независимо преобразуется восьмеричную форму
Шестнадцатеричная Hexadecimal	0xC00002EB	Из точечно-шестнадцатеричной удаляют точки
Десятичная Decimal	3221226219	32-битное двоичное число выражают в десятичной форме
Восьмеричная Octal	030000001353	32-битное двоичное число выражают в восьмеричной форме

Структура адресного пространства протокола IPv4 с разбивкой на классы, признаки принадлежности адреса к соответствующему классу, соответствующие каждому классу диапазоны номеров сетей, диапазоны адресов, максимально возможное число узлов в сети, стандартная маска и диапазоны частных адресов даны в таблице 2.

1.3. Особые (зарезервированные) IP-адреса

В системе адресации протокола IPv4 существует множество соглашений об особой интерпретации IP-адресов (см. таблицу 3). Опишем подробнее наиболее важные из них:

1. Сеть с номером **0**, и, следовательно, адреса вида **0.x.x.x** – явно не используются, кроме следующего случая. Если IP-адрес состоит только из двоичных нулей (**неопределенный** адрес): **0.0.0.0**, или в двоичной форме: **0000 0000. 0000 0000. 0000 0000. 0000 0000**, то он обозначает адрес того узла, который сгенерировал этот пакет (этот режим используется только в некоторых сообщениях ICMP как адрес отправителя).
2. Если в поле **номера сети** стоят **нули**, например: **0.0.0.51** (для класса C), или в двоичной форме: **0000 0000. 0000 0000. 0000 0000. 0101 0001**, то по умолчанию считается, что этот узел принадлежит той же самой сети, что и узел, который отправил пакет (только как адрес отправителя).

Структура адресного пространства IPv4

Класс	Первые биты слева	Наименьший / наибольший номер сети	Диапазон адресов	Максимальное число узлов в сети	Стандартная маска	Диапазон частных (private) адресов
A	0	1.0.0.0 / 126.0.0.0	1.0.0.1 - 126.255.255.254	$2^{24}-2$, поле 3 байта	255.0.0.0	1 сеть: 10.0.0.0/8: 10.0.0.0: 10.0.0.1 - 10.255.255.254
B	10	128.0.0.0 / 191.255.0.0	128.0.0.1 - 191.255.255.254	$2^{16}-2$, поле 2 байта	255.255.0.0	16 сетей: 172.16.0.0/12 172.16.0.0 – 172.31.0.0: 172.16.0.1 - 172.31.255.254
C	110	192.0.0.0 / 223.255.255.0	192.0.0.1 - 223.255.255.254	2^8-2, поле 1 байт	255.255.255.0	256 сетей: 192.168.0.0/16: 192.168.0.0 - 192.168.255.0: 192.168.0.1 - 192.168.255.254
D	1110	224.0.0.0 / 239.255.255.255		Групповые адреса multicast	-	
E	11110	240.0.0.0 / 247.255.255.255		Зарезервировано	-	

3. Если все двоичные разряды IP-адреса равны 1, то есть: **255.255.255.255**, или в двоичной форме: **1111 1111. 1111 1111. 1111 1111. 1111 1111**, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такая рассылка называется **ограниченным широковещательным** сообщением (**limited broadcast**).

4. Если в поле адреса узла назначения (host) стоят сплошные 1, например: **72.255.255.255**, (для класса A),

или в двоичной форме: **0111 0010. 1111 1111. 1111 1111. 1111 1111**, то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером. Такая рассылка называется **широковещательным** сообщением (**broadcast**).

5. Адреса вида **127.x.x.x** зарезервированы для организации обратной связи при тестировании работы программного обеспечения узла без реальной отправки пакета по сети (например, когда клиентская и серверная часть программы работают на одном компьютере). Этот адрес имеет название **loopback**.

6. Групповой IP-адрес - **multicast** - обеспечивает доставку пакета сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса. Один и тот же узел может входить в несколько групп. Групповой адрес не делится на поля номера сети и узла и обрабатывается маршрутизатором особым образом. Обеспечивает распространение информации по схеме «один – ко многим» (например

Интернет теле- и радиовещание). В противоположность multicast (класс D) адреса классов A,B,C называют иногда **unicast** адресами.

Таблица 3

Зарезервированные IP-адреса

Блок адресов CIDR	Описание	Документ
0.0.0.0/8	Эта же сеть (только как адрес отправителя)	RFC 1700
10.0.0.0/8	Частная сеть (в диапазоне класса A)	RFC 1918
14.0.0.0/8	Общедоступные сети данных (доступны до 2008-02-10)	RFC 1700
127.0.0.0/8	Сеть адресов для Loopback - тестирования	RFC 3330
128.0.0.0/16	Зарезервировано (IANA)	RFC 3330
169.254.0.0/16	Link-Local (автоконфигурирование хостов в сетях Microsoft)	RFC 3927
172.16.0.0/12	Частные сети (в диапазоне класса B)	RFC 1918
191.255.0.0/16	Зарезервировано (IANA)	RFC 3330
192.0.0.0/24	Зарезервировано (IANA)	RFC 3330
192.0.2.0/24	Документирование и примеры кода	RFC 3330
192.88.99.0/24	Передача (преобразование) данных из IPv6 в IPv4	RFC 3068
192.168.0.0/16	Частные сети (в диапазоне класса B)	RFC 1918
198.18.0.0/15	Сеть тестирования (benchmark tests)	RFC 2544
223.255.255.0/24	Зарезервировано (IANA)	RFC 3330
224.0.0.0/4	Multicasts (бывший класс D)	RFC 3171
240.0.0.0/4	Зарезервировано (бывший класс E)	RFC 1700
255.255.255.255	Широковещательная рассылка (Broadcast)	

1.4. Формат IP-адреса и маска подсети

IP-адрес состоит из двух частей: номера сети и номера узла (без специального разграничителя).

Для выделения адреса сети (подсети) из IP-адреса могут использоваться (например, в маршрутизаторах):

- **Классы адресов** (RFC 791) с фиксированными границами номера сети и номера узла (информацию о маске не нужно передавать). Со второй половины 90-х годов XX века классовая адресация повсеместно вытеснена бесклассовой адресацией, при которой количество адресов в сети определяется только и исключительно маской подсети.
- **Маски подсети (subnet mask, subnetting)** (RFC 950, RFC 1518); обеспечивают гибкое изменение границы между номером сети и номером узла (**VLISM** – variable length subnet mask – **маски подсети переменной длины**). Это позволяет экономно использовать адресное пространство для создания множества сетей разного размера (однако, информацию о маске **нужно** передавать). Сведения о масках подсети переменной длины показаны в таблице 4.

Маски подсети переменной длины

Краткая запись (блок адресов CIDR)	Точечно-десятичная запись	Точечно-двоичная запись
IP-адрес/30	255.255.255.252	11111111.11111111.11111111.11111100
IP-адрес/29	255.255.255.248	11111111.11111111.11111111.11111000
IP-адрес/28	255.255.255.240	11111111.11111111.11111111.11110000
IP-адрес/27	255.255.255.224	11111111.11111111.11111111.11100000
IP-адрес/26	255.255.255.192	11111111.11111111.11111111.11000000
IP-адрес/25	255.255.255.128	11111111.11111111.11111111.10000000
IP-адрес/24	255.255.255.0	11111111.11111111.11111111.00000000
IP-адрес/23	255.255.254.0	11111111.11111111.11111110.00000000
IP-адрес/22	255.255.252.0	11111111.11111111.11111100.00000000
IP-адрес/21	255.255.248.0	11111111.11111111.11111000.00000000
IP-адрес/20	255.255.240.0	11111111.11111111.11110000.00000000
IP-адрес/19	255.255.224.0	11111111.11111111.11100000.00000000
IP-адрес/18	255.255.192.0	11111111.11111111.11000000.00000000
IP-адрес/17	255.255.128.0	11111111.11111111.10000000.00000000
IP-адрес/16	255.255.0.0	11111111.11111111.00000000.00000000
IP-адрес/15	255.254.0.0	11111111.11111110.00000000.00000000
IP-адрес/14	255.252.0.0	11111111.11111100.00000000.00000000
IP-адрес/13	255.248.0.0	11111111.11111000.00000000.00000000
IP-адрес/12	255.240.0.0	11111111.11110000.00000000.00000000
IP-адрес/11	255.224.0.0	11111111.11100000.00000000.00000000
IP-адрес/10	255.192.0.0	11111111.11000000.00000000.00000000
IP-адрес/9	255.128.0.0	11111111.10000000.00000000.00000000
IP-адрес/8	255.0.0.0	11111111.00000000.00000000.00000000

Маска подсети (subnet mask) – это число, применяемое в паре с IP-адресом, причем двоичная запись маски содержит слева непрерывную последовательность единиц в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети (подсети). Граница между последовательностями единиц и нулей в маске соответствует границе между номером сети (подсети) и номером узла в IP-адресе. Например:

255.255.128.0 ⇔ 1111 1111. 1111 1111. 1000 0000. 0000 0000

Иногда для пояснения использования масок переменной длины (VLSM, subnetting) в IP-адресе выделяют не 2, а 3 области:

- **Биты адреса сети.**
- **Биты подсети, заимствованные (borrowed) у адреса узла (host),** которые в сумме с предыдущим определяют реальный адрес сети (подсети).
- **Биты адрес узла.**

Например: **1000 0001. 0100 0000. 1000 0110. 0000 0101.**

Этот пример поясняет деление (условное) на сети и подсети: в «большой» сети класса В, образуется $32=2^5$ подсетей.

1.5. Пример использования маски при IP-адресации

Пусть заданы IP-адрес: **129.64.134.5** и маска подсети: **255.255.128.0**

Наложение маски для выделения адреса подсети реализуется логической операцией «и» (AND) над их двоичным представлением:

1000 0001. 0100 0000. 1000 0110. 0000 0101 ⇔ **129.64.134.5**

AND

1111 1111. 1111 1111. 1000 0000. 0000 0000 ⇔ **255.255.128.0**

=

(subnet; адрес подсети содержит нули в области номера узла)

1000 0001. 0100 0000. 1000 0000. 0000 0000 ⇔ **129.64.128.0**

(host)

0000 0000. 0000 0000. 0000 0110. 0000 0101 ⇔ **0.0.6.5**

В десятичной форме адреса подсети и узла, дополненные нулями до 32 бит, выглядят соответственно, как **129.64.128.0** и **0.0.6.5**.

Часто используют краткую запись: вместо IP-адрес: 129.64.134.5 и маска подсети: 255.255.128.0 записывают: **129.64.134.5/17**, то есть маска содержит 17 единиц, а значит в указанном IP-адресе: 129.64.134.5 под номер сети отведено 17 двоичных разрядов. В этом примере в «большой» сети класса В с помощью маски, содержащей 17 единиц, образуется $2^{32-17}=2^{15}$ подсети.

2. РАСПРЕДЕЛЕНИЕ IP-АДРЕСОВ В СЕТИ ИНТЕРНЕТ

В Интернете уникальность адресов гарантируется централизованной, иерархически организованной системой их распределения. Номер сети может быть назначен только по рекомендации специального подразделения Интернета.

Главным органом регистрации глобальных адресов в Интернете с 1998 г. является неправительственная некоммерческая организация ICANN (*Internet Corporation for Assigned Names and Numbers*), действующая через свой комитет IANA (*Internet Assigned Numbers Authority*). ICANN (IANA) координирует работу региональных отделов: ARIN - Америка; RIPE - Европа; APNIC - Азия и Тихоокеанский регион и т.п.

Региональные отделы выделяют блоки адресов крупным поставщикам услуг, а те, в свою очередь, распределяют их между своими клиентами, среди которых могут быть и более мелкие поставщики.

2.1. Дефицит IP адресов и его преодоление

Не смотря на усилия по увеличению размеров адресного пространства (см. рисунок 2), дефицит (public) адресов в Интернете ощущается (и нарастает) с начала 90-х годов 20-го века.

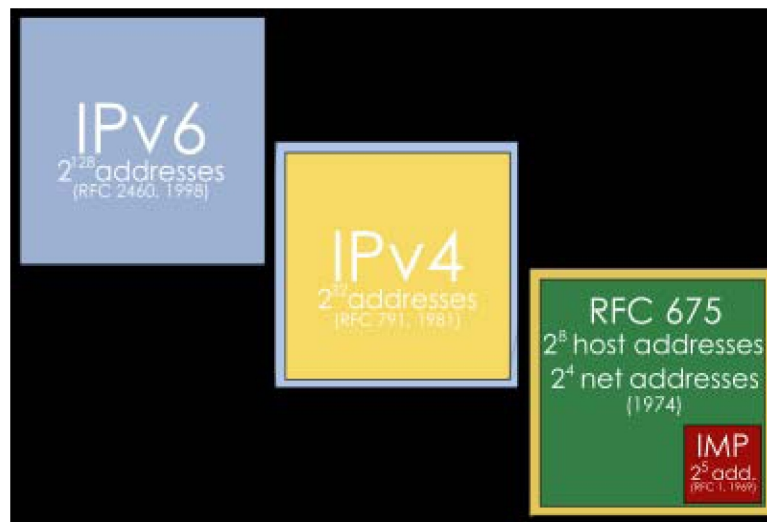


Рис. 2. Рост адресного пространства



Рис. 3. Пример нерационального использования пространства IP-адресов

Основные подходы для снятия проблемы дефицита адресов:

- Использование масок переменной длины VLSM.
- Использование протоколов CIDR (в определенном смысле, современный, усовершенствованный вариант VLSM) и NAT.
- Переход на IPv6 (наилучший вариант, но внедряется медленно).

2.2. Адресация и технология CIDR

Технология бесклассовой междоменной маршрутизации (**Classless Inter-Domain Routing, CIDR**), которая описана в документах RFC 1517 - 1520 (объявлена в 1993г.), позволяет центрам выдачи адресов гибко «нарезать» адреса на основе VLSM (главное условие - наличие непрерывных диапазонов адресов, такие адреса имеют одинаковый *префикс*, то есть одинаковые цифры в старших разрядах).

Внедрение технологии CIDR обеспечивает:

- Более экономное расходование адресного пространства.
- Уменьшение числа записей в таблицах маршрутизации за счет объединения маршрутов (**supernetting**) – одна запись в таблице маршрутизации может представлять большое количество сетей.

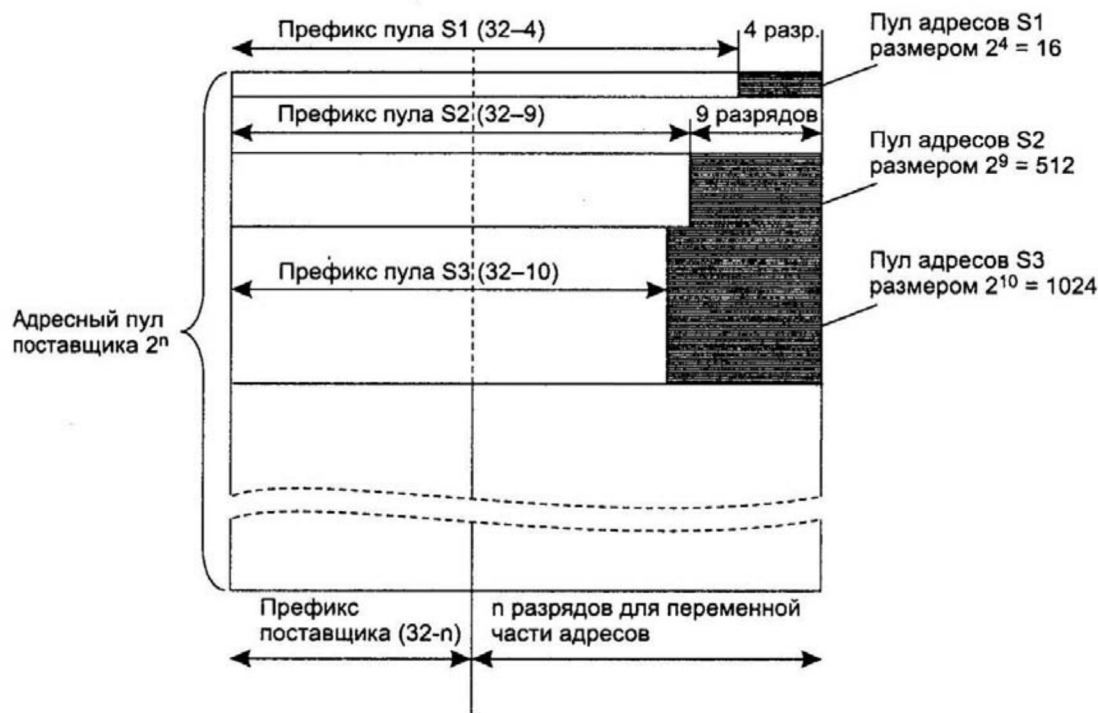


Рис. 4. Распределение IP-адресов в технологии CIDR

3. ОТОБРАЖЕНИЕ IP-АДРЕСОВ НА ЛОКАЛЬНЫЕ АДРЕСА

3.1. Протокол ARP

Одна из задач протокола IP – обеспечение совместной согласованной работы в сети, состоящей из подсетей, в общем случае использующих **разные** сетевые технологии.

Чтобы локальная технология сети смогла доставить пакет на следующий маршрутизатор, необходимо:

- Упаковать пакет в кадр нужного формата (например, Ethernet).
- Снабдить этот кадр локальным (MAC) адресом следующего маршрутизатора.

Для определения локального адреса по IP-адресу используется протокол разрешения адреса *Address Resolution Protocol, ARP*. Протокол ARP работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети - протокол локальной сети (Ethernet, Token Ring, FDDI) с возможностью широковещательного доступа одновременно ко всем узлам локальной сети, или же протокол глобальной сети (X.25, frame relay), как правило, не поддерживающий такой широковещательный доступ (ARP-сервер).

Протокол ReversARP. Существует также протокол, решающий обратную задачу - нахождение IP-адреса по известному локальному адресу. Он называется реверсивный ARP - *RARP (Reverse Address Resolution Protocol)* и используется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего сетевого адаптера.

3.2. Алгоритм работы протокола ARP

Если возникла необходимость послать пакет по адресу, например 194.85.135.65, то протокол IP сначала проверяет не содержится ли уже строка с таким IP-адресом в его ARP-таблице.

Если нет, то узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP-запрос (формат пакета протокола ARP показан на рисунке 5), вкладывает (инкапсулирует) его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широковещательно.

В локальных сетях протокол ARP использует широковещательные (broadcast) кадры протокола канального уровня для поиска в сети узла с заданным IP-адресом.

0	8	16	31
Тип сети (для Ethernet – 1 (0x1))		Тип протокола (для IP – 2048 (0x800))	
Длина локального адреса (для Ether- net – 6 (0x6))	Длина сетевого адреса (для IP – 4 (0x4))	Операция (для ARP - 1 (0x1)) (для RARP - 2 (0x2))	
Локальный адрес отправителя (source) (байты 0 - 3) 00 80 48 EB			
Локальный адрес отправителя (source) (байты 4 - 5) 7E 60		IP-адрес отправителя (source) (байты 0-1) 194.85.	
IP-адрес отправителя (source) (байты 2-3) 135.75		Искомый локальный адрес (получате- ля, target) (байты 0 - 1) 00 00	
Искомый локальный адрес (получателя, target) (байты 2-5) 00 00 00 00			
Искомый IP-адрес (получателя, target) (байты 0 - 3) 194.85.135.65			

Рис. 5. Формат пакета протокола ARP

Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP запросе отправитель указывает свой локальный адрес.

ARP-запросы и ответы используют один и тот же формат пакета. Так как локальные адреса могут в различных типах сетей иметь различную длину, то формат пакета протокола ARP зависит от типа сети.

Узел, отправляющий ARP-запрос, заполняет в пакете все поля, кроме поля искомого локального адреса, а в нем ставит нули (для RARP-запроса не указывается искомым IP-адрес). Значение этого поля заполняется узлом, опознавшим свой IP-адрес.

Для уменьшения числа ARP-запросов найденное соответствие между IP-адресом и MAC-адресом сохраняется автоматически в ARP-таблице соответствующего интерфейса в виде записи: 194.85.135.65 – 00 E0 F7 7F 19 20

Теперь, если вновь возникает необходимость послать пакет по адресу 194.85.135.65, то протокол IP прежде чем посылать широковещательный запрос

сначала проверяет, не содержится ли уже строка с таким IP-адресом в его ARP-таблице.

Если да, то адрес 00 E0 F7 7F 19 20 сразу ставится в поле MAC-адреса назначения посылаемого IP пакета. А широковещательный ARP-запрос не рассылается.

ARP-таблица пополняется не только за счет поступающих на данный интерфейс ARP-ответов, но и путем анализа и извлечения полезной адресной информации из широковещательных ARP-запросов.

В ARP-таблицах существует два типа записей: динамические и статические. Статические (они существуют пока устройство включено) создают вручную с помощью утилиты (команды) *arp*. Если динамическая запись не обновлялась в течение определенного времени, то она исключается из таблицы. Поэтому ARP-таблицу называют иногда *ARP-кэшем*.

3.3. Отображение IP-адресов на локальные адреса за пределами локальной сети

Протокол **ProxyARP** – разновидность протокола ARP, устанавливаемая на маршрутизаторах, позволяющая отображать IP-адреса на локальные в сетях с широковещанием даже в тех случаях, когда искомый узел находится за пределами данного широковещательного домена (домена коллизий).

3.4. Отображение IP-адресов на локальные адреса в глобальных сетях

В глобальных сетях, не поддерживающих широковещательную рассылку, администратору сети чаще всего приходится вручную формировать ARP-таблицы. В последнее время наметилась тенденция автоматизации работы протокола ARP и в глобальных сетях. Для этой цели среди всех маршрутизаторов, подключенных к какой-либо глобальной сети, выделяется специальный маршрутизатор (ARP-сервер), который ведет ARP-таблицу для всех остальных узлов и маршрутизаторов этой сети.

4. ОТОБРАЖЕНИЕ СИМВОЛЬНЫХ АДРЕСОВ НА IP-АДРЕСА: СЛУЖБА DNS

DNS (Domain Name System) - это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet. Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла. Спецификация DNS определяется стандартами RFC 1034 и 1035. DNS требует статической конфигурации своих таблиц, отображающих имена компьютеров в IP-адрес.

Протокол DNS является служебным протоколом прикладного уровня. Этот протокол несимметричен - в нем определены DNS-серверы и DNS-клиенты. DNS-серверы хранят часть распределенной базы данных о соответствии символьных имен и IP-адресов. Эта база данных распределена по административным доменам сети Internet. Клиенты сервера DNS знают IP-адрес сервера DNS своего админи-

стративного домена и по протоколу IP передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес.

Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он сразу посылает ответ клиенту, если же нет - то он посылает запрос DNS-серверу другого домена, который может сам обработать запрос, либо передать его другому DNS-серверу.

Все DNS-серверы соединены иерархически, в соответствии с иерархией доменов сети Internet. Клиент опрашивает эти серверы имен, пока не найдет нужные отображения. Этот процесс ускоряется из-за того, что серверы имен постоянно кэшируют информацию, предоставляемую по запросам.

Клиентские компьютеры могут использовать в своей работе IP-адреса нескольких DNS-серверов, для повышения надежности своей работы.

База данных DNS имеет структуру дерева, называемого доменным пространством имен, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены. Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена.

Корень базы данных DNS управляется IANA. Домены верхнего уровня назначаются для каждой страны, а также для различных организаций. Имена этих доменов должны следовать международному стандарту ISO 3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций используются следующие аббревиатуры:

- **com** - коммерческие организации (например, microsoft.com);
- **edu** - образовательные (например, mit.edu);
- **gov** - правительственные организации (например, nsf.gov);
- **org** - некоммерческие организации (например, fidonet.org);
- **net** - организации, поддерживающие сети (например, nsf.net).

Каждый домен DNS администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Каждый домен имеет уникальное имя, а каждый из поддоменов имеет уникальное имя внутри своего домена. Имя домена может содержать до 63 символов. Каждый хост в сети Internet однозначно определяется своим *полным доменным именем (fully qualified domain name, FQDN)*, которое включает имена всех доменов по направлению от хоста к корню. Пример полного DNS-имени: **citint.dol.ru**.

5. АВТОМАТИЗАЦИЯ ПРОЦЕССА НАЗНАЧЕНИЯ IP-АДРЕСОВ УЗЛАМ СЕТИ: ПРОТОКОЛ DHCP

При конфигурировании компьютеров и маршрутизаторов администратор должен задать: IP-адрес, маску, IP-адреса шлюза и серверов DNS, доменное имя и т.п.

Протокол динамического конфигурирования хостов (*Dynamic Host Configuration Protocol (DHCP)*) автоматизирует процесс конфигурирования сете-

вых интерфейсов, гарантируя от дублирования адресов, за счет централизованного управления их распределением.

DHCP является расширением протокола BOOTP, использовавшегося ранее для обеспечения бездисковых рабочих станций IP-адресами при их загрузке. DHCP сохраняет обратную совместимость с BOOTP.

Стандарт протокола DHCP был принят в октябре 1993 года. Последняя версия протокола (март 1997 года) описана в RFC 2131 и 2132.. Новая версия DHCP, предназначенная для использования в среде IPv6, носит название DHCPv6 и определена в RFC 3315 (июль 2003 года).

Протокол DHCP реализует модель **клиент-сервер**. Передача данных производится при помощи протокола UDP, при этом сервер принимает сообщения от клиентов на порт 67 и отправляет сообщения клиентам на порт 68. Сервер DHCP может работать в следующих режимах:

- ручное назначение статических адресов;
- автоматическое назначение статических адресов;
- автоматическое распределение динамических адресов.

5.1. Алгоритм работы протокола DHCP

Во время старта системы компьютер-клиент DHCP, находящийся в состоянии "инициализация", посылает сообщение **discover** (исследовать), которое широкоэпестательно распространяется по локальной сети и передается всем DHCP-серверам частной интeрсети. Каждый DHCP-сервер, получивший это сообщение, отвечает на него сообщением **offer** (предложение), которое содержит IP-адрес и конфигурационную информацию.

Компьютер-клиент DHCP переходит в состояние "выбор" и собирает конфигурационные предложения от DHCP-серверов. Затем он выбирает одно из этих предложений, переходит в состояние "запрос" и отправляет сообщение **request** (запрос) тому DHCP-серверу, чье предложение было выбрано.

Выбранный DHCP-сервер посылает сообщение **DHCP-acknowledgment** (подтверждение), содержащее тот же IP-адрес, который уже был послан ранее на стадии исследования, а также **срок аренды** для этого адреса. Кроме того, DHCP-сервер посылает параметры сетевой конфигурации.

Помимо IP-адреса, DHCP также может сообщать клиенту дополнительные параметры, необходимые для нормальной работы в сети. Эти параметры называются опциями DHCP. Список стандартных опций можно найти в RFC 2132.

Некоторыми из наиболее часто используемых опций являются:

- IP-адрес маршрутизатора по умолчанию;
- маска подсети;
- адреса серверов DNS;
- имя домена DNS.

Некоторые поставщики программного обеспечения могут определять собственные, дополнительные опции DHCP.

Некоторые реализации службы DHCP способны автоматически обновлять записи DNS, соответствующие клиентским компьютерам, при выделении им но-

вых адресов. Это производится при помощи протокола обновления DNS, описанного в RFC 2136.

После получения подтверждения, клиент переходит в состояние "**связь**", находясь в котором он может принимать участие в работе сети TCP/IP. Компьютеры-клиенты, которые имеют локальные диски, сохраняют полученный адрес для использования при последующих стартах системы. При приближении момента истечения срока аренды адреса компьютер пытается обновить параметры аренды у DHCP-сервера, а если этот IP-адрес не может быть выделен снова, то ему возвращается другой IP-адрес.

Реализация **протокола DHCP**. Компания Microsoft впервые включила сервер DHCP в поставку серверной версии Windows NT 3.5, выпущенной в 1994 году. Начиная с Windows 2000 Server реализация DHCP-сервера от Microsoft позволяет динамически обновлять записи DNS, что используется в Active Directory.

Internet Systems Consortium выпустил первую версию ISC DHCP Server (для Unix-подобных систем) 6 декабря 1997 года. 22 июня 1999 года вышла версия 2.0, более точно соответствующая стандарту.

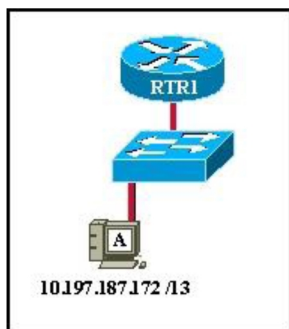
Компания Cisco включила сервер DHCP в Cisco IOS 12.0 в феврале 1999 года. Sun добавила DHCP-сервер в Solaris 8 в июле 2001 года.

6. ЗАДАЧИ НА IP-АДРЕСАЦИЮ

1. Какие адреса из приведенных ниже являются **частными (private)** адресами? (выбрать 3):
 1. 10.45.09.23;
 2. 15.87.234.87;
 3. 192.168.45.23;
 4. 172.17.78.98;
 5. 192.169.89.56;
 6. 172.32.45.90.
2. Преобразовать шестнадцатеричное число A2 в десятичную форму.
 1. 156.
 2. 158.
 3. 160.
 4. 162.
 5. 164.
 6. 166.
3. Какое утверждение точно описывает **public (внешний)** IP-адрес?
 1. Public IP-адрес не может использоваться в частной сети.
 2. Public IP-адрес должен быть уникальным в пределах всего Интернета.
 3. Public IP-адрес может дублироваться (т.е. использоваться более чем у одного порта/хоста) только в локальной сети.
 4. Public IP-адрес должен быть уникальным лишь в пределах локальной сети.
 5. Администраторы сети могут произвольно выбирать любые public IP-адреса для сетевых устройств, имеющих доступ в Интернет.
4. Какой класс IP-адресов (IPv4) позволяет обеспечить максимальное число **сетей**?
 1. Класс A.
 2. Класс B.
 3. Класс C.
 4. Класс D.
 5. Класс E.
5. Определить **широковещательный (broadcast)** адрес для сети класса C с адресом сети 192.168.32.0 и стандартной (default) маской?
 1. 192.168.0.0;
 2. 192.168.0.255;
 3. 192.168.32.0;
 4. 192.168.32.254;
 5. 192.168.32.255.

6. Компания использует адресную схему на основе адресов класса В, причем предполагается использовать не менее 100 подсетей. Какую маску следует выбрать для правильного формирования подсетей и конфигурирования хостов?

1. 255.255.0.0;
2. 255.255.240.0;
3. 255.255.254.0;
4. 255.255.255.0;
5. 255.255.255.128;
6. 255.255.255.192.



7.

В какой из указанных ниже подсетей находится хост А (см. рис.)?

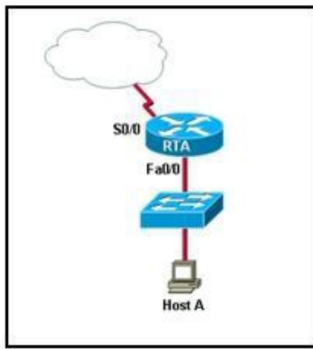
1. 10.197.0.0.
2. 10.192.0.0.
3. 10.197.184.0.
4. 10.197.187.0.
5. 10.197.187.168.

8. Имеется хост с IP-адресом 172.32.65.13 и стандартной маской подсети, к какой из сетей (подсетей) этот хост принадлежит?

1. 172.32.65.0;
2. 172.32.65.32;
3. 172.32.0.0;
4. 172.32.32.0.

9. Сеть надо разбить на подсети так, чтобы каждая подсеть обеспечивала 14 IP-адресов, пригодных для конфигурирования хостов. Какую маску подсети следует использовать для созданных таким образом новых подсетей.

1. 255.255.255.128;
2. 255.255.255.224;
3. 255.255.255.240;
4. 255.255.255.248;
5. 255.255.255.252.



10.

Хосту А (см. рис.) назначен IP-адрес 10.118.197.55/20. Сколько сетевых устройств может быть добавлено в эту же подсеть?

1. 253.
2. 509.
3. 1021.
4. 2045.
5. 4093.

11. Компания планирует разбить свою сеть на подсети, каждая из которых может содержать не более 27 хостов. Какая из приведенных ниже масок обеспечивает в каждой из образованных подсетей необходимое число хостов, оставляя при этом неиспользованными наименьшее число адресов?

1. 255.255.255.0.
2. 255.255.255.192.
3. 255.255.255.224.
4. 255.255.255.240.
5. 255.255.255.248.

12. Какое двоичное число соответствует десятичному числу 248?

1. 11101000.
2. 11110100.
3. 11111010.
4. 11111000.

13. Компания сформулировала следующие 4 требования к адресной схеме своей сети: имеется 25 подсетей; используется IP-адрес класса В; имеется максимум 300 компьютеров в каждой из подсетей; необходимо обеспечить минимальное число неиспользованных IP-адресов в каждой из подсетей. Какая из приведенных ниже масок обеспечивает выполнение выдвинутых требований?

1. 255.255.240.0.
2. 255.255.248.0.
3. 255.255.254.0.
4. 255.255.255.0.
5. 255.255.255.128.
6. 255.255.255.248.

14. Какие маски из приведенных ниже годятся для разбиения сети, использующей адреса класса В, на подсети? (Выбрать 2)

1. 255.0.0.0.
2. 255.254.0.0.
3. 255.224.0.0.
4. 255.255.255.192.
5. 255.255.252.0.
6. 255.255.0.0.

15. Компании, использующей адреса класса В, требуется создать не менее 1000 подсетей, в каждой из которых адресуется 50 хостов. Какая из приведенных ниже масок обеспечивает выполнение этих требований?

1. 255.255.0.0.
2. 255.255.240.0.
3. 255.255.255.0.
4. 255.255.255.192.
5. 255.255.255.224.

16. Адрес 223.168.17.167/29 – это:

1. адрес хоста;
2. адрес групповой рассылки (multicast);
3. широковещательный адрес;
4. адрес подсети.

17. Определить правильное соотношение числа подсетей и числа хостов, когда сеть с адресом 192.168.99.0 разбивается на подсети с помощью маски /29?

1. 6 сетей / 32 хоста.
2. 30 сетей / 6 хостов.
3. 14 сетей / 14 хостов.
4. 62 сети / 2 хоста.

18. Сетевой карте компьютера назначен IP-адрес 172.31.192.166 с маской 255.255.255.248. Какой подсети этот IP-адрес принадлежит?

1. 172.31.0.0.
2. 172.31.160.0.
3. 172.31.192.0.
4. 172.31.248.0.
5. 172.31.192.160.
6. 172.31.192.248.

19. Какая комбинация адреса сети и маски корректно идентифицирует IP-адреса из диапазона 172.16.128.0 - 172.16.159.255 (подсказка: это диапазон адресов ровно первых пяти подсетей)?

1. 172.16.128.0 255.255.255.224.
2. 172.16.128.0 255.255.0.0.
3. 172.16.128.0 255.255.192.0.
4. 172.16.128.0 255.255.224.0.
5. 172.16.128.0 255.255.255.192.

20. Какой из адресов является точно-десятичным эквивалентом IP-адреса, заданного в двоичной форме 10101101.00101011.11001001.00000011?

1. 169.35.200.2.
2. 169.43.201.3.
3. 173.35.201.2.
4. 173.43.201.3.
5. 175.13.193.2.
6. 175.43.193.3.

21. Для определения адреса подсети роутер производит логическое перемножение двоичного представления IP-адреса и маски. Каков будет результат для случая 172.16.115.73/20?

1. 172.16.0.0.
2. 172.16.96.0.
3. 172.16.112.0.
4. 172.16.115.0.

22. Выбрать **широковещательный (broadcast)** адрес для подсети, которой принадлежит адрес хоста 172.16.31.99/21.

1. 172.16.31.255.
2. 172.16.255.255.
3. 172.16.31.103.
4. 172.16.24.255.
5. 172.16.24.111.

23. Выбрать адрес подсети, которой принадлежит адрес хоста 192.168.32.52 с маской 255.255.255.240.

1. 192.168.32.0.
2. 192.168.32.32.
3. 192.168.32.48.
4. 192.168.32.63.
5. 192.168.32.255.

24. Сколько бит заимствуется для адреса подсети в адресе хоста 189.13.64.45 с маской 255.255.255.248?

1. 4.
2. 5.
3. 12.

4. 13.
5. 20.
6. 21.

25. Выбрать три адреса, разрешенных для использования в Интернете.

1. 14.31.6.12.
2. 220.225.225.23.
3. 172.16.13.91.
4. 182.16.44.5.
5. 192.168.100.35.
6. 127.13.64.2.

26. Укажите адрес подсети, которой принадлежит IP-адрес 150.3.123.18 с маской 255.255.224.0.

1. 150.3.0.0.
2. 150.3.123.0.
3. 150.3.64.0.
4. 150.3.96.0.



27.

Структура сети показана на рисунке. Четыре хоста нужно добавить в сеть 172.16.112.0. Какой из приведенных ниже адресов **нельзя** в этой подсети использовать для конфигурирования хостов?

1. 172.16.127.255.
2. 172.16.112.255.
3. 172.16.113.55.
4. 172.16.112.89.
5. 172.16.120.96.

28. Укажите **три** IP-адреса, которые являются public адресами.

1. 172.32.255.240.
2. 192.168.1.245.
3. 10.15.250.5.
4. 205.255.16.250.
5. 172.11.250.212.
6. 192.15.301.240.

29. Укажите **три** IP-адреса, которые совместно с маской 255.255.255.248 **можно** использовать для конфигурирования хостов.

1. 192.168.200.87.
2. 194.10.10.104.

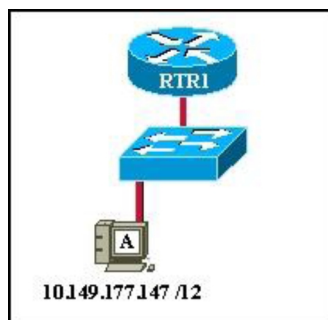
3. 223.168.210.100.
4. 220.100.100.154.
5. 200.152.2.160.
6. 196.123.142.190.

30. Хост имеет IP-адрес 192.168.65.54 и маску подсети 255.255.255.240. К какой из указанных ниже подсетей он принадлежит?

1. 192.168.65.16.
2. 192.168.65.32.
3. 192.168.65.48.
4. 192.168.65.64.

31. К какой из указанных ниже подсетей принадлежит хост, имеющий IP-адрес 160.16.240.69 /27?

1. 160.0.0.64.
2. 160.16.0.64.
3. 160.16.64.64.
4. 160.16.240.64.
5. 160.16.255.64.



32. Определить **широковещательный (broadcast)** адрес для подсети, в которой находится хост А (см. рис.)

1. 10.255.255.255.
2. 10.144.255.255.
3. 10.149.255.255.
4. 10.149.191.255.
5. 10.159.255.255.

33. Маршрутизатор (роутер) получил пакет с адресом получателя (destination) 172.16.30.79/22. В какую из указанных ниже подсетей этот пакет отправлен?

1. 172.16.30.0/22.
2. 172.16.28.0/22.
3. 172.16.30.76/22.
4. 172.16.30.64/22.
5. 172.16.28.56/22.
6. 172.16.0.0/22.

34. Указать **два** критерия, которые идентифицируют адрес класса В.

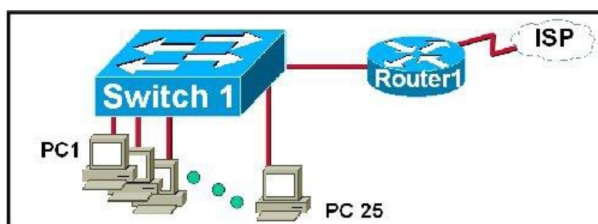
1. десятичное число в первом байте (старшем октете) принадлежит диапазону 127 – 191;
2. десятичное число в первом байте (старшем октете) принадлежит диапазону 128 – 192;
3. десятичное число в первом байте (старшем октете) принадлежит диапазону 128 – 191;
4. первый (старший) бит IP-адреса в двоичной форме – 0;
5. первые два (старших) бита IP-адреса в двоичной форме – 10;
6. первые три (старших) бита IP-адреса в двоичной форме – 110.

35. Сколько IP-адресов, разрешенных для назначения сетевым устройствам, доступно в каждой из подсетей, возникающих в результате применения маски 255.255.255.248 к адресу класса А?

1. 1022.
2. 510.
3. 254.
4. 126.
5. 30.
6. 6.

36. На сколько подсетей можно разделить сеть класса В, используя маску 255.255.252.0?

1. 4.
2. 6.
3. 64.
4. 252.
5. 255.
6. 1024.



37.

Структура сети показана на рисунке. Администратор планирует адресную схему для локальной сети, используя диапазон IP-адресов 172.25.14.0/26. Хостам должны быть назначены IP-адреса из диапазона 172.25.14.1 – 172.25.14.25. LAN-интерфейсу роутера должен быть назначен IP-адрес 172.25.14.63. Какое из приведенных ниже утверждений наилучшим образом описывает такую адресную схему?

1. Адреса в локальной сети – назначены корректно.
2. Используется неправильный адрес подсети.
3. LAN-интерфейсу роутера назначен широковещательный (broadcast) адрес.

4. Маска подсети не обеспечивает достаточное число адресов для адресации хостов в данной подсети.

38. Для создания подсетей, позаимствуем 4 бита у той части адреса класса C, которая отведена для адресации хостов. Для последней из образованных таким образом подсетей укажите диапазон адресов, пригодный для адресации хостов (приведен только 4-ый октет).

1. .224 - .239.
2. .225 - .239.
3. .225 - .254.
4. .241 - .254.
5. .241 - .255.
6. .240 - .255.

39. Компания XYZ использует адрес сети 192.168.4.0, а также маску 255.255.255.224 для создания подсетей внутри этой сети. Определить **максимальное число хостов**, которое можно адресовать в каждой из образуемых подсетей?

1. 6.
2. 14.
3. 30.
4. 62.

40. Какие **три** из указанных ниже IP-адресов являются адресами широковещательной рассылки (**широковещательными, broadcast**), если используется маска подсети 255.255.255.240?

1. 75.32.75.15.
2. 205.16.35.11.
3. 199.254.129.111.
4. 129.130.17.143.
5. 135.22.55.93.
6. 105.33.62.213.

Packet Tracer 4.11. Методическое пособие для начинающих

Система Packet Tracer 4.11 была разработана в фирме Cisco для того, чтобы помочь новичкам осваивать сетевые технологии. Настоящее методическое пособие поможет сформировать основные навыки работы в данной программе на примере создания небольшой сети.

1 Интерфейс

Панели:

1. Стандартная.
2. Правка.
3. Панель объектов. (3.1 – панель выбора объекта).
4. Панель тестирования.
5. Панель инструментов.
6. Панель навигации по рабочему пространству.
7. Рабочее пространство.

Рассмотрим окно программы (рисунок 1.1).

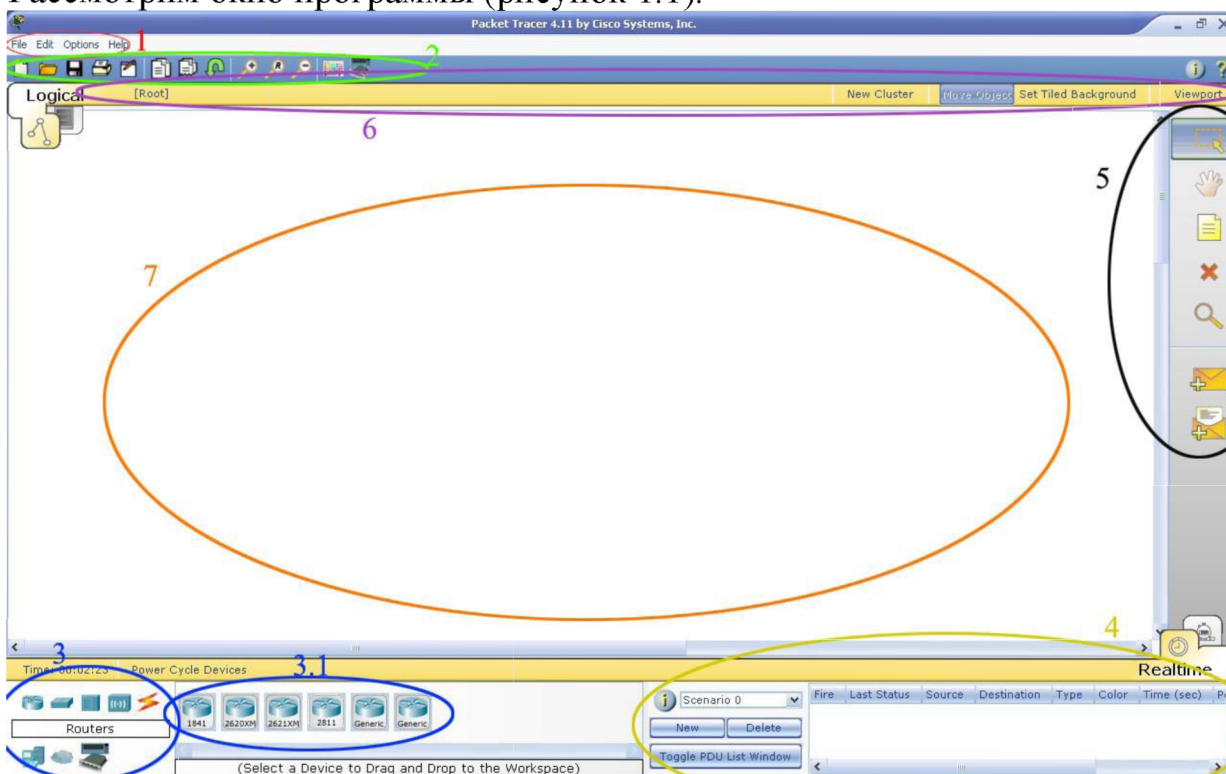


Рисунок 1.1

1. Стандартная. Особого пояснения не требует (рисунок 1.2).

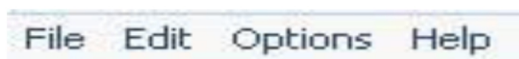


Рисунок 1.2

2. Правка. Сюда встроены основные функции стандартной панели, а так же добавлены инструменты масштабирования. Особое внимание следует уделить по-

следнему инструменту, который позволяет создать новый образец сетевого устройства (рисунок 1.3).

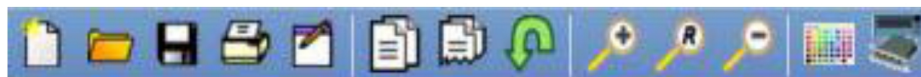


Рисунок 1.3

3. Панель объектов. Здесь мы выбираем определенный тип устройства, которое нам необходимо поместить на рабочее пространство. Далее рядышком раскрывается панель выбора объекта, где мы выбираем нужную нам модель устройства, и затем щелкаем по ней мышью, и потом щелчком мыши помещаем ее (или просто перетаскиваем - drag&drop) на рабочее пространство (рисунок 1.4).

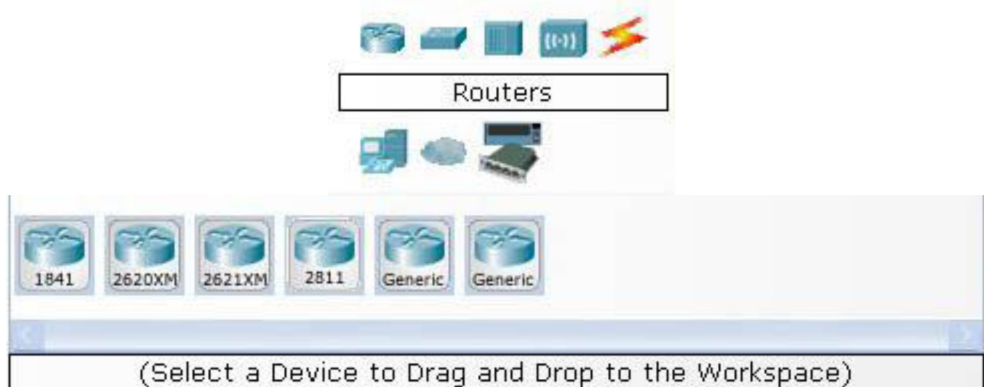


Рисунок 1.4

4. Панель тестирования. Здесь у нас в процессе тестирования в режиме реального времени показывается информация о пересылке пакетов, а так же статус о доставке. Так же тут присутствует режим симуляции пересылки пакетов, в процессе которого мы можем наблюдать транспортировку объектов и получать более детальную информацию (рисунок 1.5).

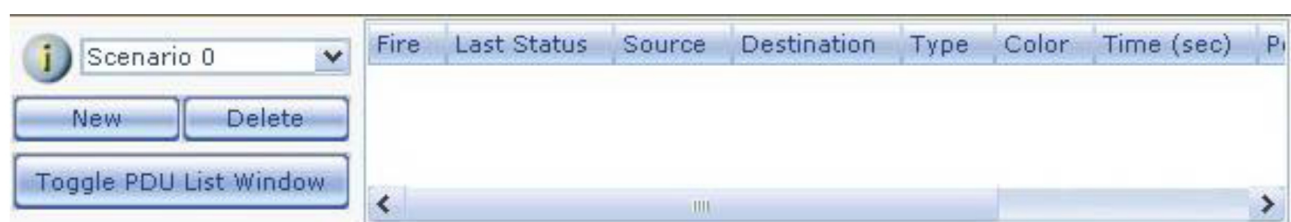


Рисунок 1.5

5. Панель инструментов. Данная панель содержит инструменты, которые наиболее часто используются: выделение, перемещение по рабочему пространству, заметка, удаление определенного устройства, инструмент для просмотра основных параметров, посылка пакетов стандартная и с выборочными настройками (рисунок 1.6).



Рисунок 1.6

6. Панель навигации. Имеет два режима логический и физический. В физическом режиме мы проектируем сеть, а непосредственно в логическом уже наносим на рабочее пространство необходимые устройства (рисунок 1.7).



Рисунок 1.7

2 Разработка компьютерной сети

Научимся пошагово создавать сеть и настраивать ее.

Итак, перед нами чистое рабочее пространство, и стоит задача установить сеть в каком-то офисе. Начнем с проектирования. Переходим на панели навигации в физический режим, далее переходим в корпоративный офис (рисунок 2.1). Если нам необходимо какое-то другое здание, то его можно тоже создать путем щелчка мыши по инструменту New Building на панели навигации.

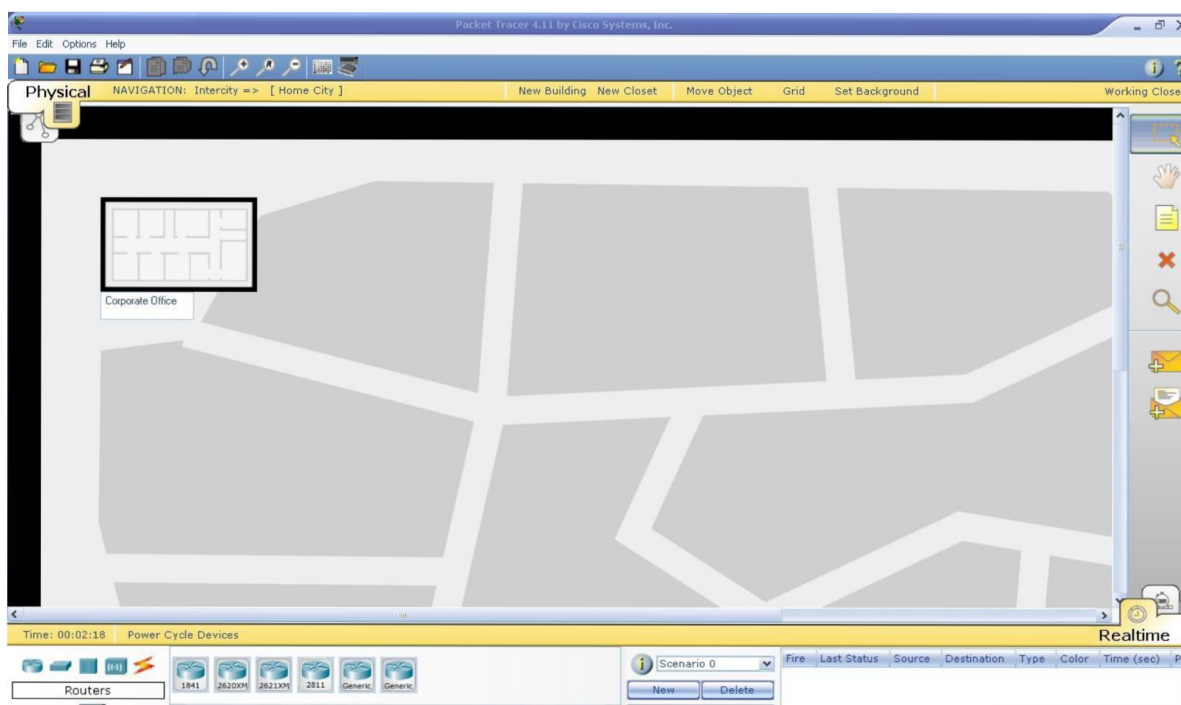


Рисунок 2.1

Перед нами рабочее пространство офиса, в котором нам необходимо установить сеть. В верхнем левом углу (рядом с панелью навигации) рабочего пространства уже висит новая область, которую необходимо перетащить с помощью мыши в нужное нам место (рисунок 2.2).

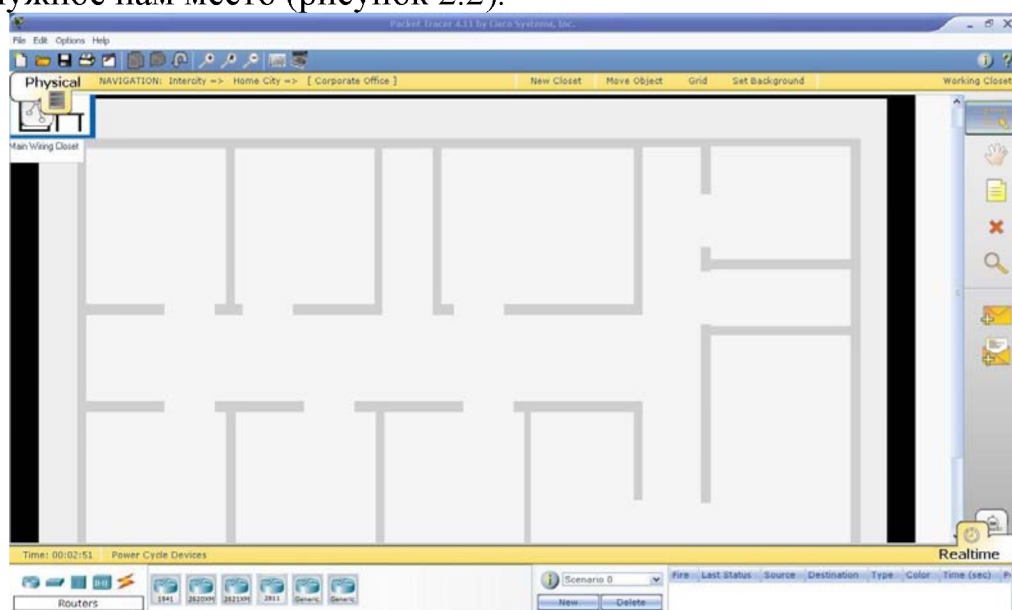


Рисунок 2.2

Далее, щелчком по этой области и выбором логического режима, мы переходим уже к непосредственной установке оборудования (рисунок 2.3).

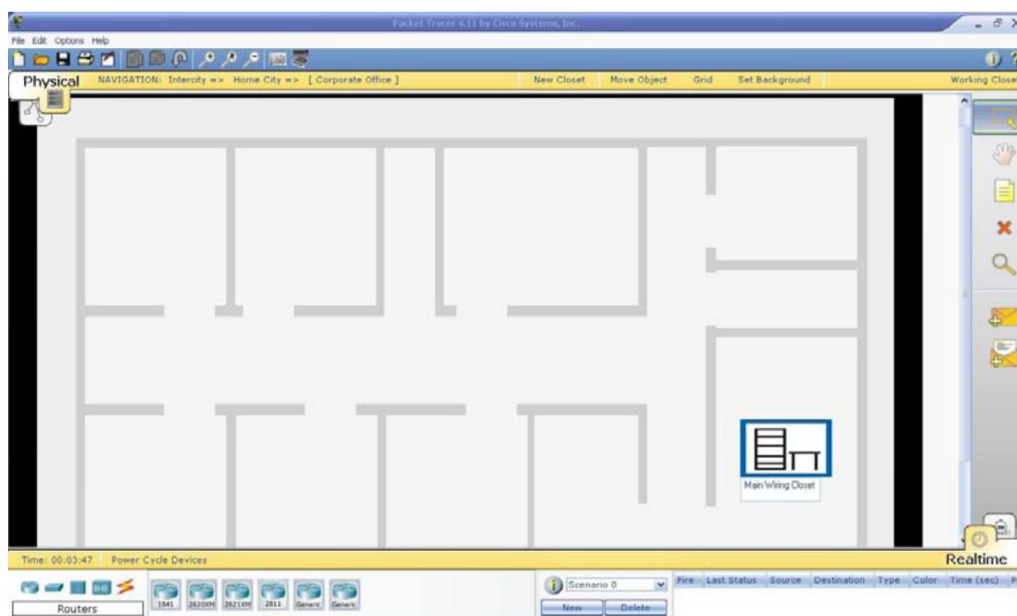


Рисунок 2.3

Теперь обратим наше внимание на панель объектов (рисунок 2.4). Здесь красным обведена панель объектов. Выбираем роутер Router pt Empty и переносим его на рабочее пространство. Так же в беспроводных устройствах Wireless devices выбираем беспроводной роутер и помещаем на рабочее пространство. Далее в Switches выбираем модель 2950-24 и так же переносим на рабочее пространство (рисунок 2.4).

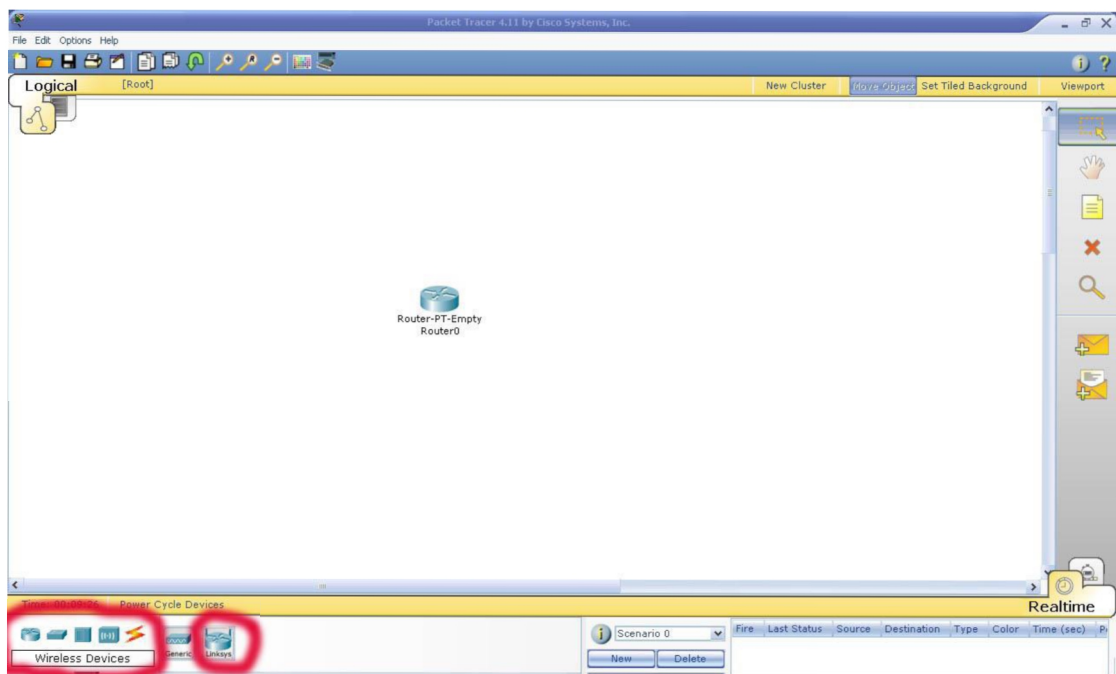


Рисунок 2.4

Далее щелчком мыши по роутеру мы входим в окно его настройки (рисунок 2.5). Здесь имеется его физическое представление, параметры и встроенная операционная система, благодаря которой процесс установки параметров можно проводить путем набора команд на клавиатуре (CLI).

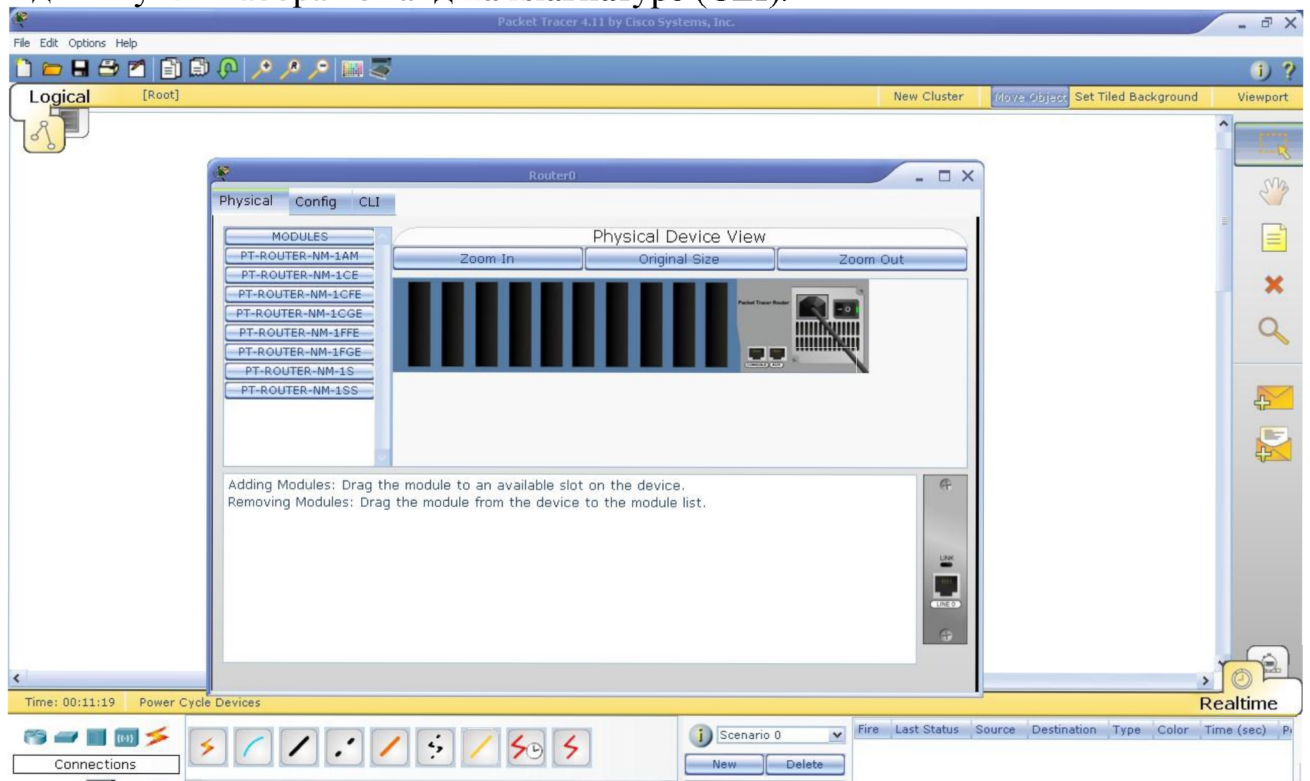


Рисунок 2.5

Переходим во вкладку физического представления, если она уже у вас не открыта. Теперь нам необходимо установить в роутер модули. Для этого всегда сначала отключают питание, затем переноской модулей в соответствующие слоты роутера, устанавливаем их (рисунок 2.6). Нам необходимы модули PT-Router-NM-

1CFE. Установим для начала 6 таких модулей. В конце не забудьте включить питание!!!

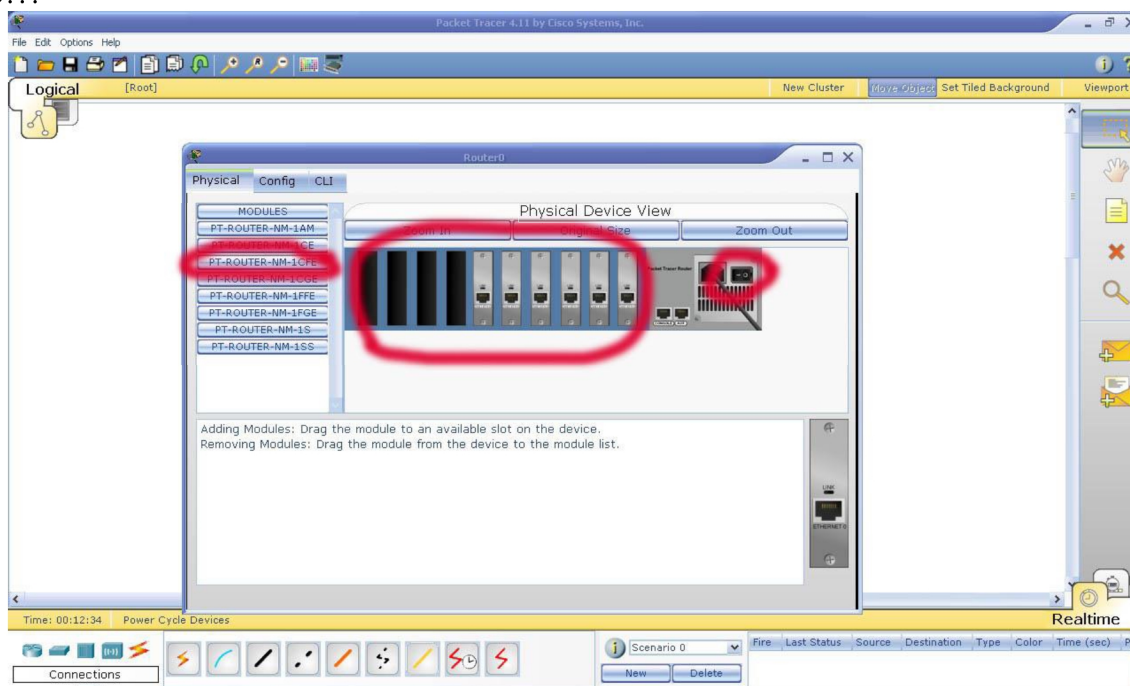


Рисунок 2.6

Теперь пока окно настройки можно закрыть. Выбираем на панели объектов «коммутация – connections» (провода), конкретнее провод Copper Straight-trough «витая пара (медь) – прямой» (рисунок 2.7). И путем щелчка сначала на одном роутере, потом на другом роутере соединяем их через **нужные нам (не перепутайте)!** порты. То же самое проделываем со свитчами. В результате рабочее пространство должно приобрести примерно такой вид (рисунок 2.7).

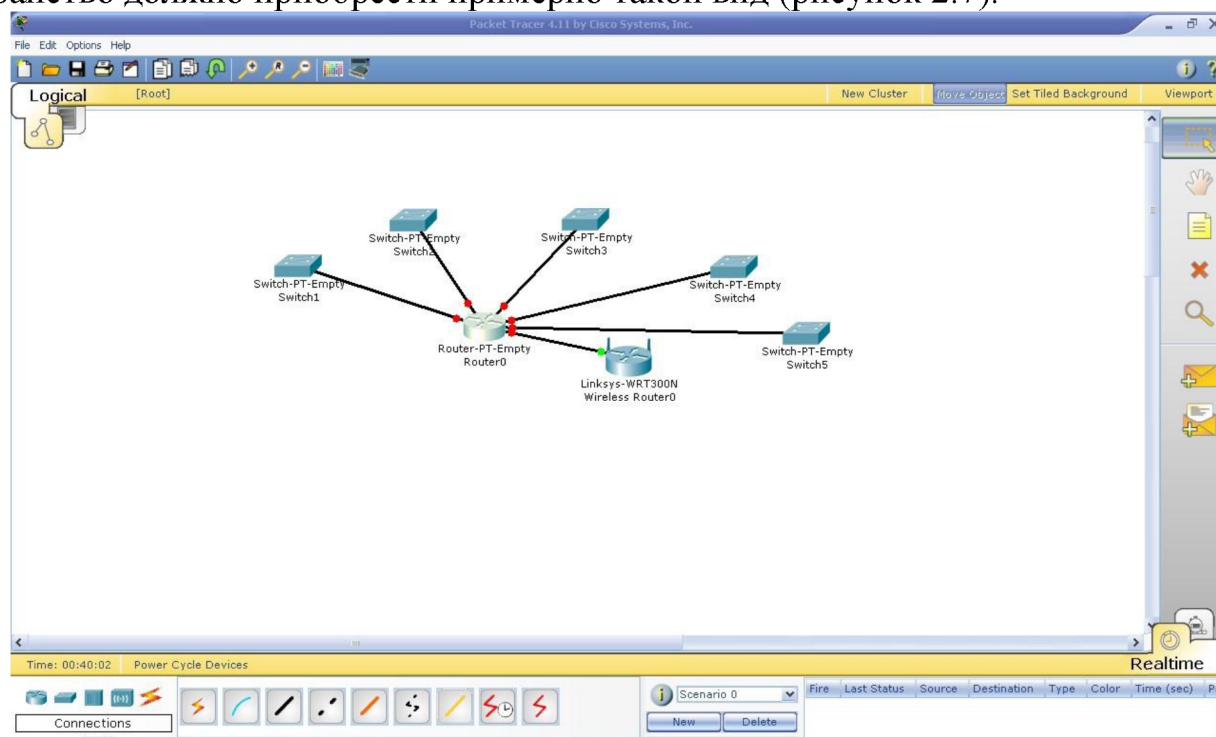


Рисунок 2.7

Перейдем в физический режим. Теперь создаем новую область для оборудования. Переходим в нее и переходим обратно в логический режим - продолжа-

ем установку оборудования. Для удобства, оборудование из главного офиса объединим в единый кластер. Это можно сделать путем выделения нужного нам оборудования на рабочем пространстве, затем щелчком мыши по инструменту, находящемуся на панели навигации New Cluster. Теперь добавим на рабочее пространство 4 компьютера и соединим их с первым свитчем из главного офиса (рисунок 2.8). Теперь перейдем в физический режим и перенесем новую область в необходимое нам место.

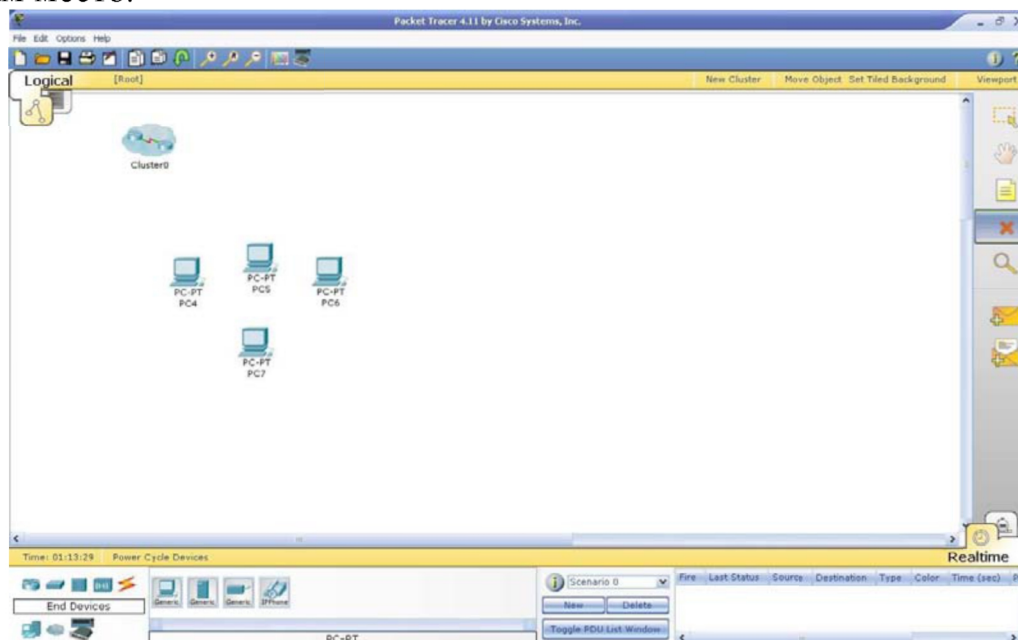


Рисунок 2.8

При установке оборудования, может возникнуть такая проблема: в одну область может попасть оборудование из другой. Такая проблема решается с помощью инструмента на панели навигации Move Object. При щелчке на ненужном в данной области оборудовании появляется раскрывающееся меню, где мы указываем, в какую область нам необходимо перенести устройство (рисунок 2.9).

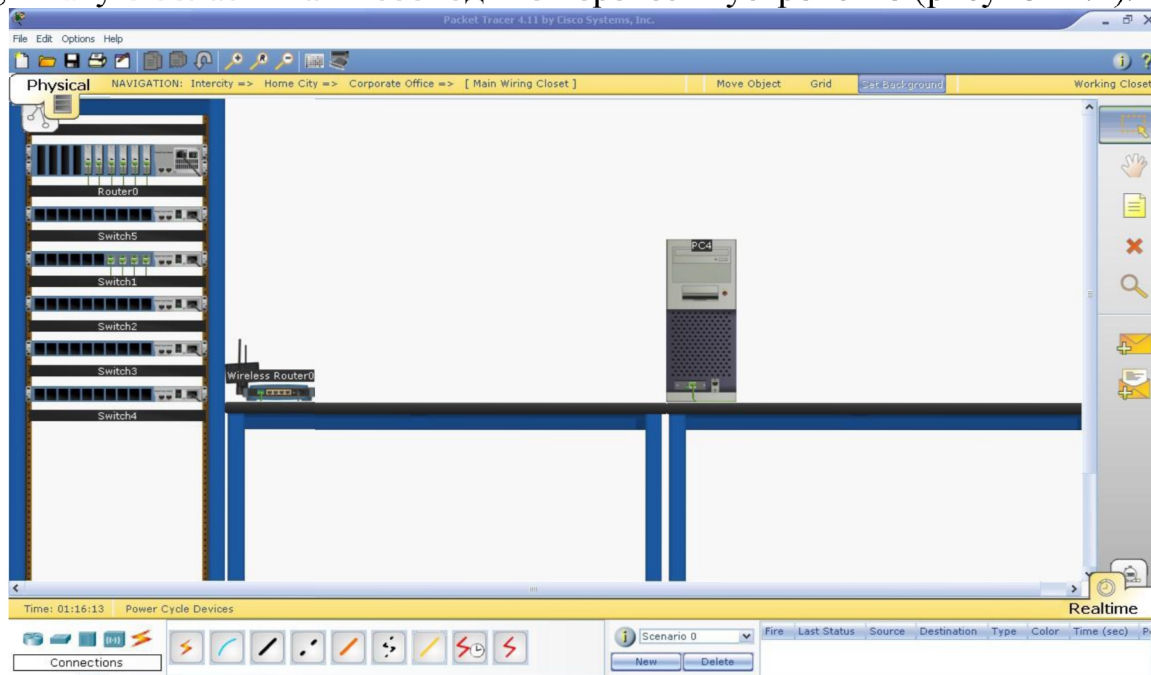


Рисунок 2.9

Создадим еще одну область с четырьмя компьютерами и объединим предыдущие компьютеры и новые в кластеры для удобства. Теперь создадим новую область, которая будет использоваться для беспроводного соединения. Перенесем на рабочее пространство точку доступа и соединим ее кабелем с беспроводным роутером.

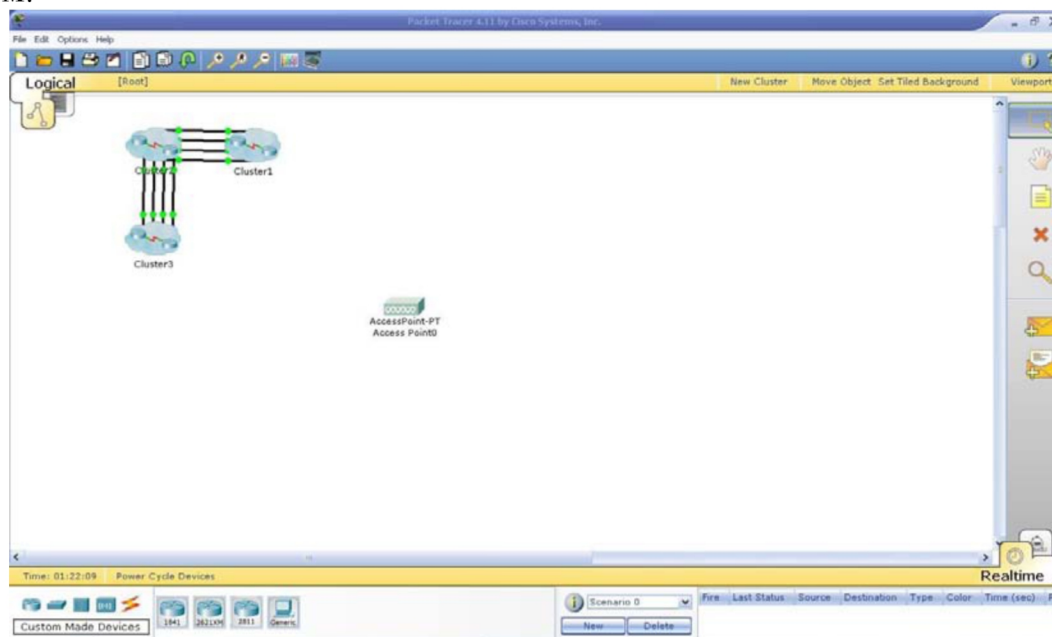


Рисунок 2.10

Теперь, что бы беспроводные устройства соединялись в нужном нам порядке, зададим ключи доступа. Для этого щелчком на беспроводном роутере переходим в его настройку. Открываем вкладку конфигурация. Слева в интерфейсе выбираем вкладку Wireless, переключаем на WEP и в окошке вводим ключ из 10 цифр. То же самое проделываем с точкой доступа, но в этом случае их ключи должны отличаться, так как точка доступа с роутером соединяется с помощью кабеля.

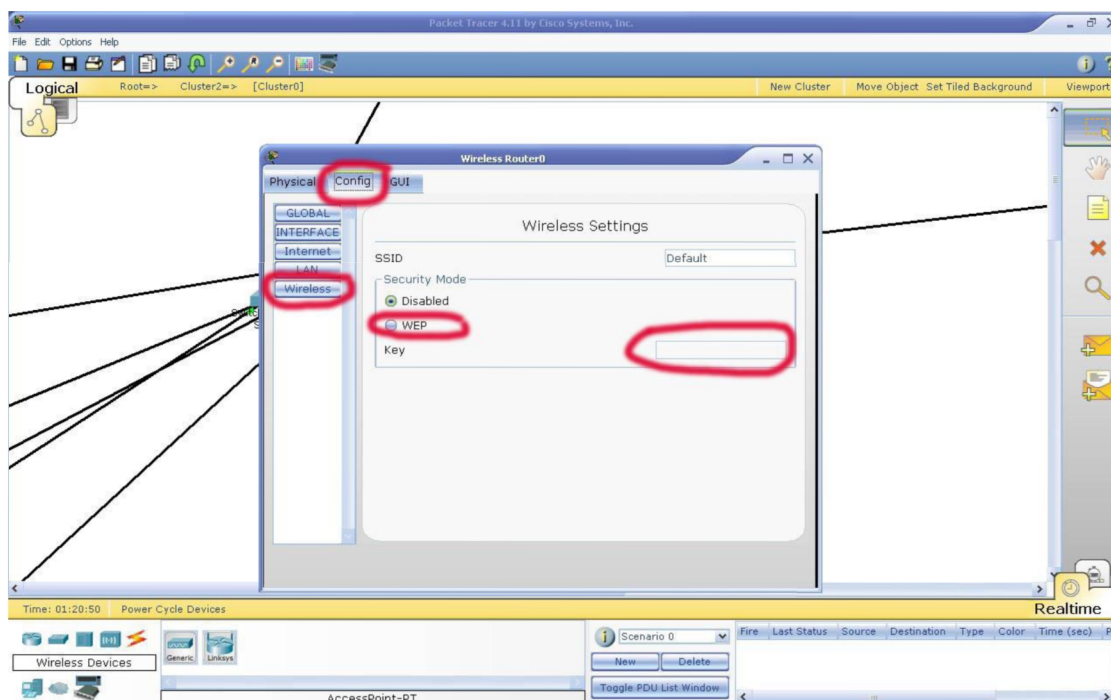


Рисунок 2.11

Так выглядит окно настройки точки доступа. Здесь в интерфейсе надо выбрать вкладку Port 1.

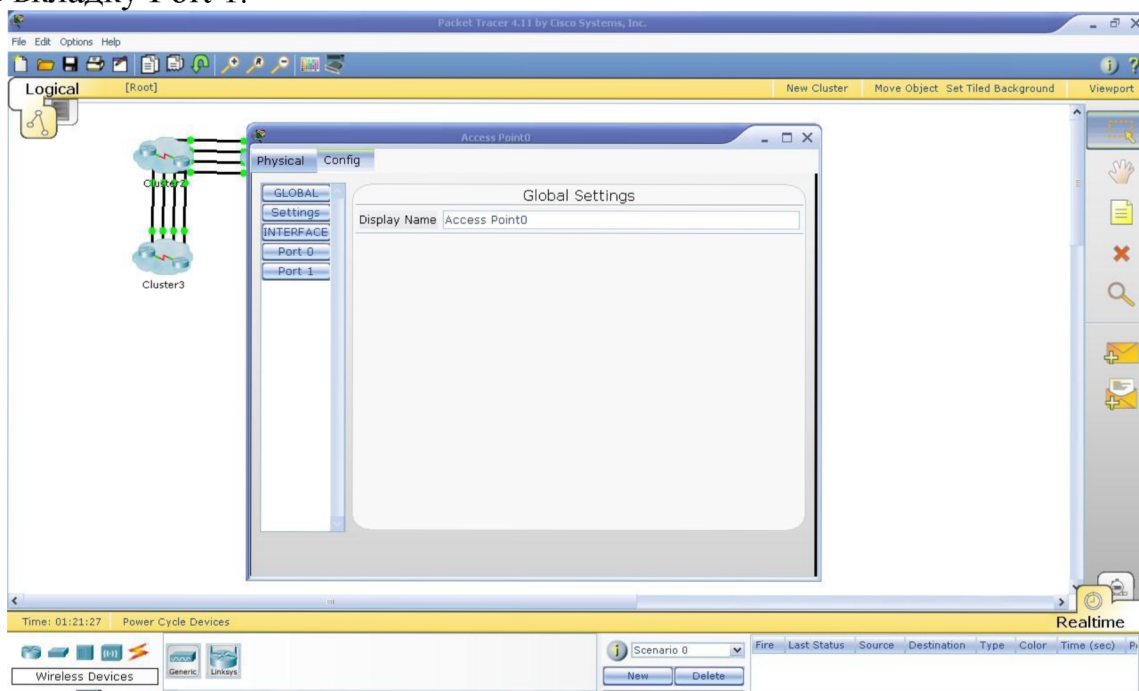


Рисунок 2.12

Перенесем на рабочее пространство компьютер с модулем для беспроводного подключения и в его настройке укажем ключ точки доступа. Через некоторое время, если все сделано правильно, то компьютер автоматически подключится к точке доступа. Итак, у нас есть сеть небольшого размера. Теперь необходимо раздать IP адреса и настроить маршрутизацию. Ее мы будем проводить автоматическим способом (rip). IP адреса выберем в диапазоне: 192.168.1-3.0-255.

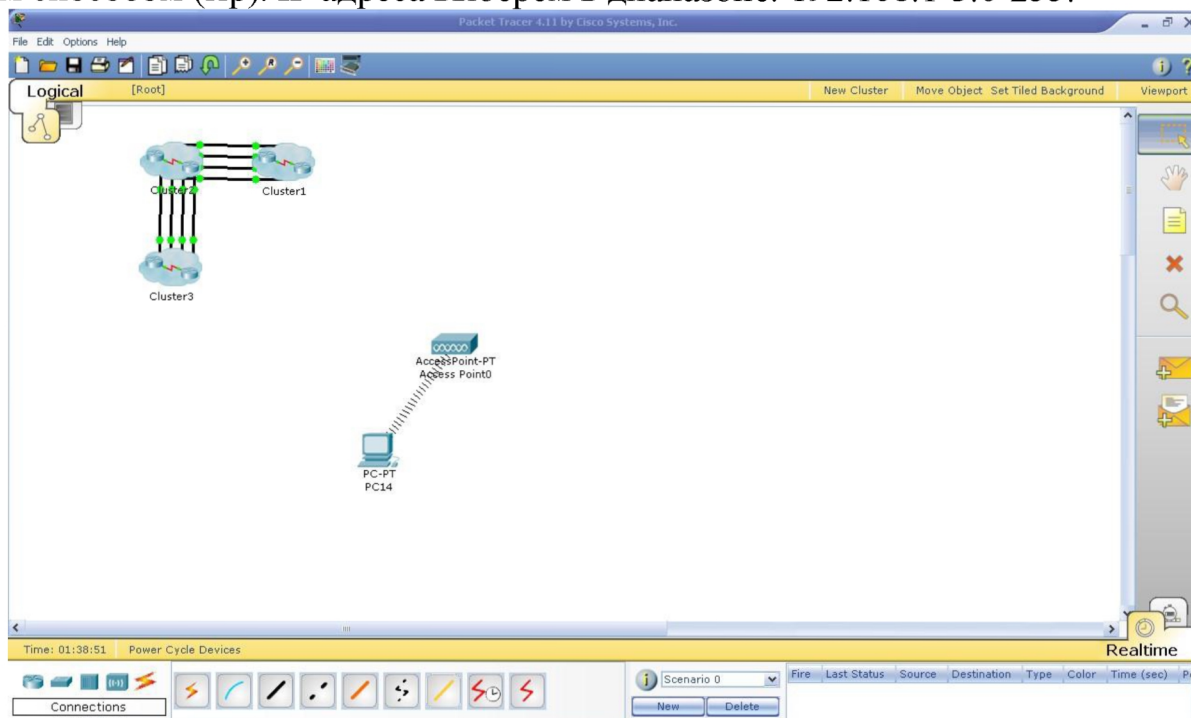


Рисунок 2.13

3 Раздача IP адресов и настройка маршрутизации

Обратимся сначала к окну настройки роутера, конкретнее к интерфейсу его модулей. FA0/0 даем IP адрес 192.168.1.1. Тут же появится ошибка, которая информирует нас о том, что устройство с таким адресом уже существует. Сейчас этот адрес автоматически был присвоен беспроводному роутеру. Обратимся к его настройке, конкретнее перейдем во вкладку CLI – операционная система, которая встроена в каждое устройство и используется для удобства настройки посредством команд, набираемых в командной строке.

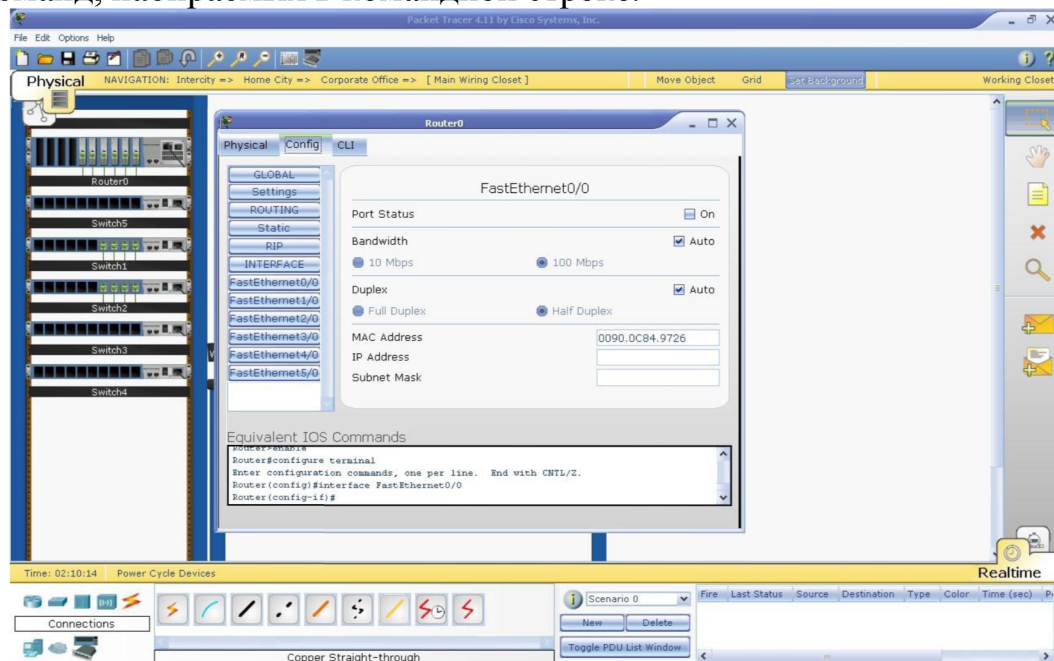


Рисунок 3.1

Во вкладке Network Setup указываем необходимый нам адрес. В данном случае, 192.168.1.2, и внизу этого окна щелкаем сохранить настройки. Теперь опять перейдем к главному роутеру, и начнем раздачу адресов.

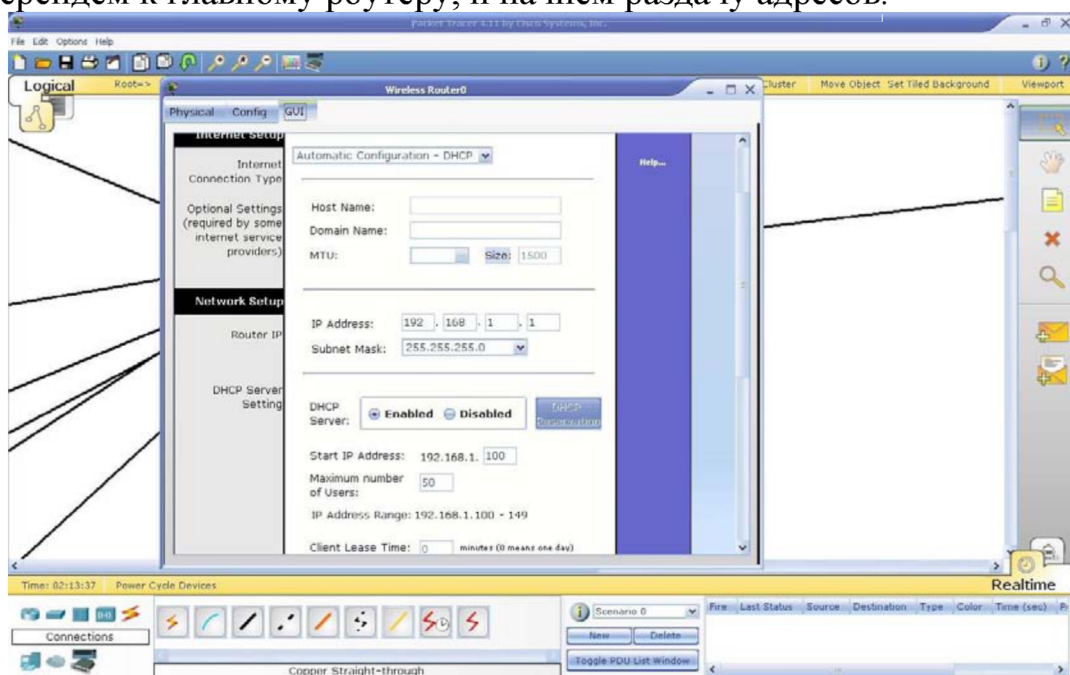


Рисунок 3.2

Для каждого модуля указываем адрес. Начнем с 0/0 – 192.168.1.1. Следующему модулю присвоим адрес: 192.168.2.1 и т.д. Главное не забывайте открыть порты, путем установки флажка в Port Status – On. Далее обратимся непосредственно к компьютерам.

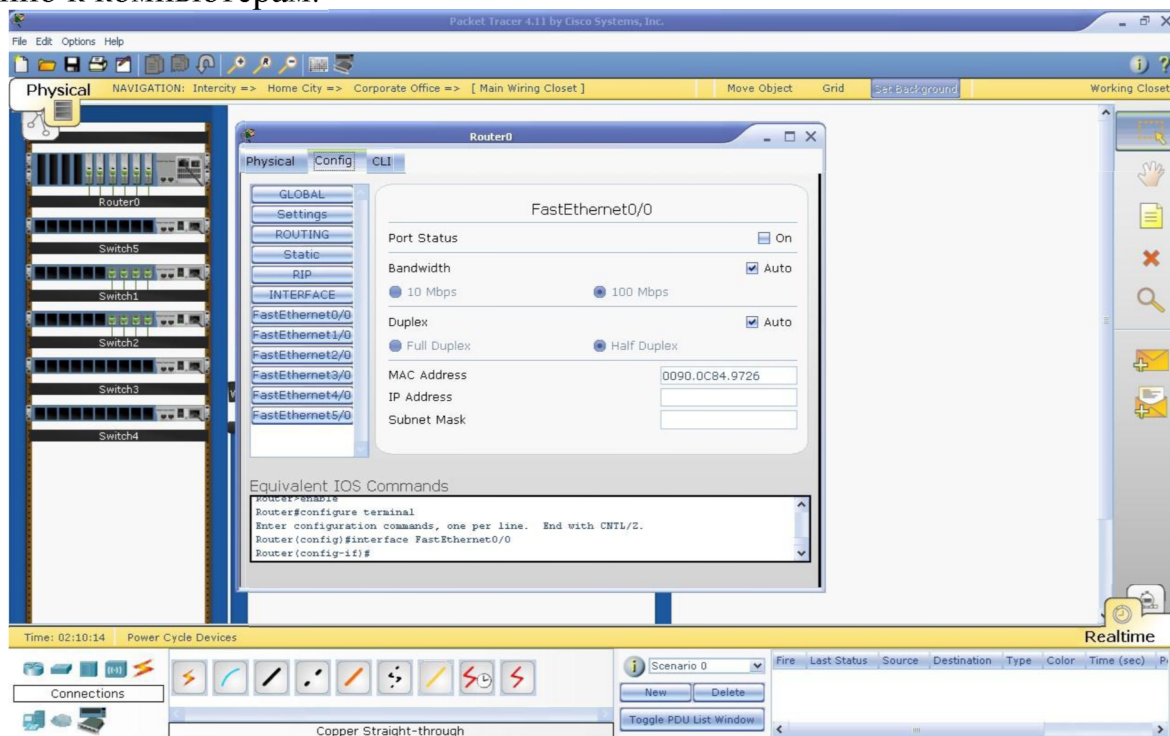


Рисунок 3.3

Компьютерам, относящимся к модулю 192.168.1.1 адреса, раздаем автоматически путем установки флажка на DHCP, к модулю 192.168.2.1 – соответственно 192.168.2.2 - 192.168.2.5 и т.д. Не забываем указывать обратный адрес во вкладке Settings – Gateway соответственно адресам модулей, к которым они подключены через свитч.

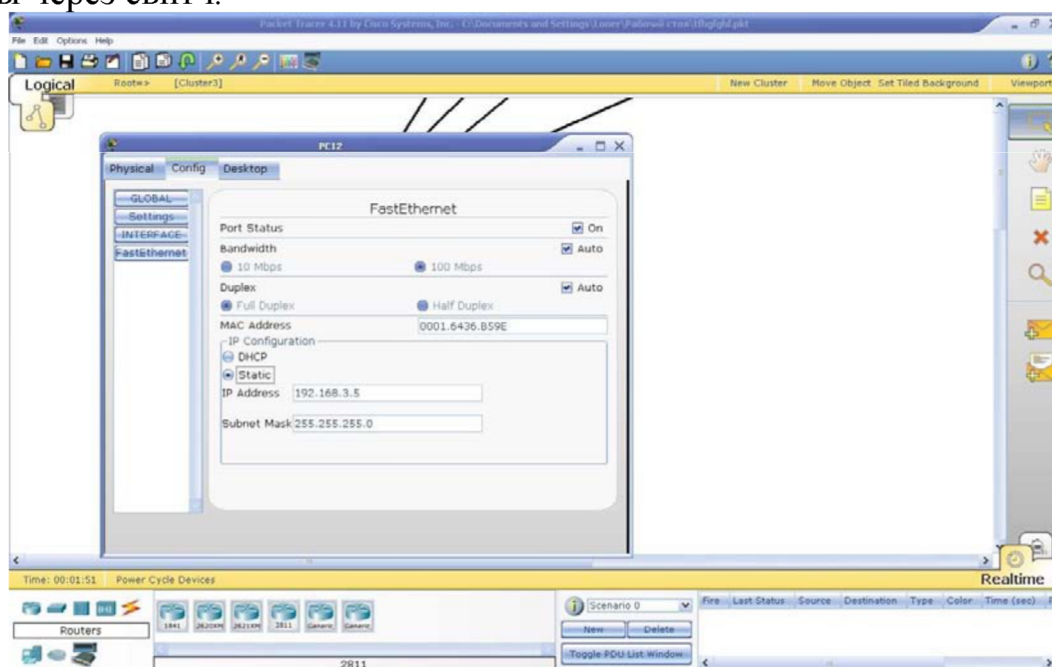


Рисунок 3.4

Обратимся к маршрутизации. Для этого опять перейдем к окну настройки роутера. Во вкладку Routing – Rip. В окошечке Network указываем адреса: 192.168.1.0, 192.168.2.0 и т.д. После указания адреса щелкаем на кнопку ADD. Если все было правильно выполнено, то у нас теперь есть рабочая сеть. Осталось ее только протестировать. Тестирование будем проводить в режиме реального времени.

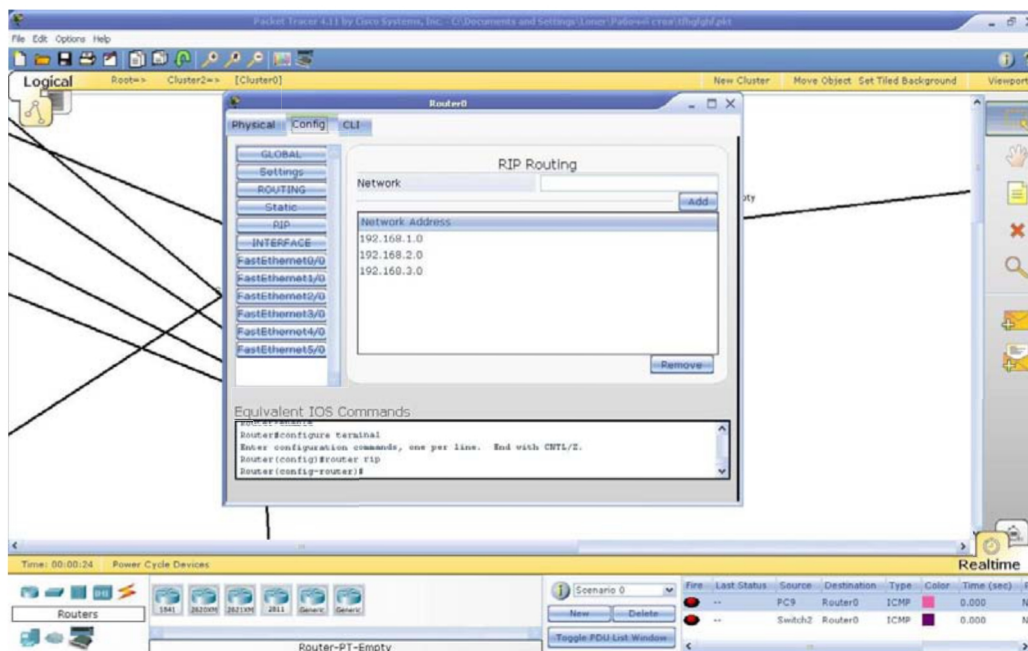


Рисунок 3.5

4 Тестирование

Для удобства мы удалили все кластеры (это делать не обязательно). Таким образом, рабочее пространство выглядит примерно так.

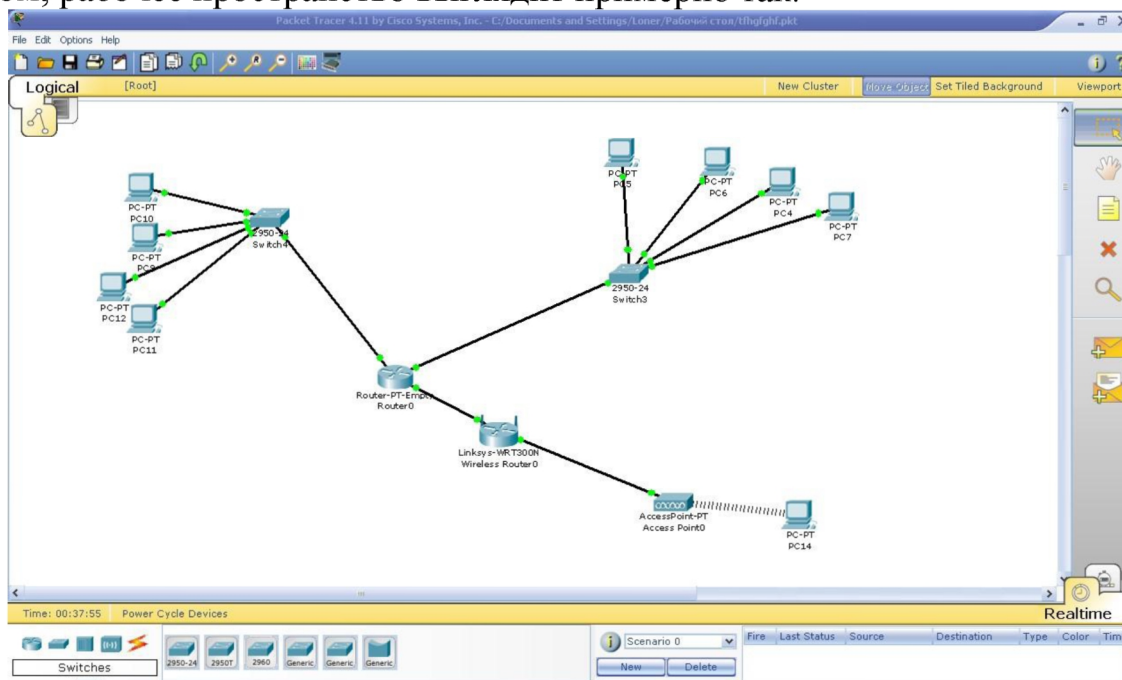


Рисунок 4.1

Выберем на панели отмеченный инструмент – PDU Simple. Затем щелкнем на компьютере одной сети, например, 10, затем на компьютере другой сети, например, 7. Внизу в панели тестирования отобразится статус – в нашем случае Successful. Значит, настроили мы правильно. Проверим беспроводную сеть – щелкнем на компьютере 14, затем на роутере. Внизу в панели тестирования отобразился статус Successful – настроили верно. Тестирование так же можно производить из командной строки любого компьютера путем отправки ping.

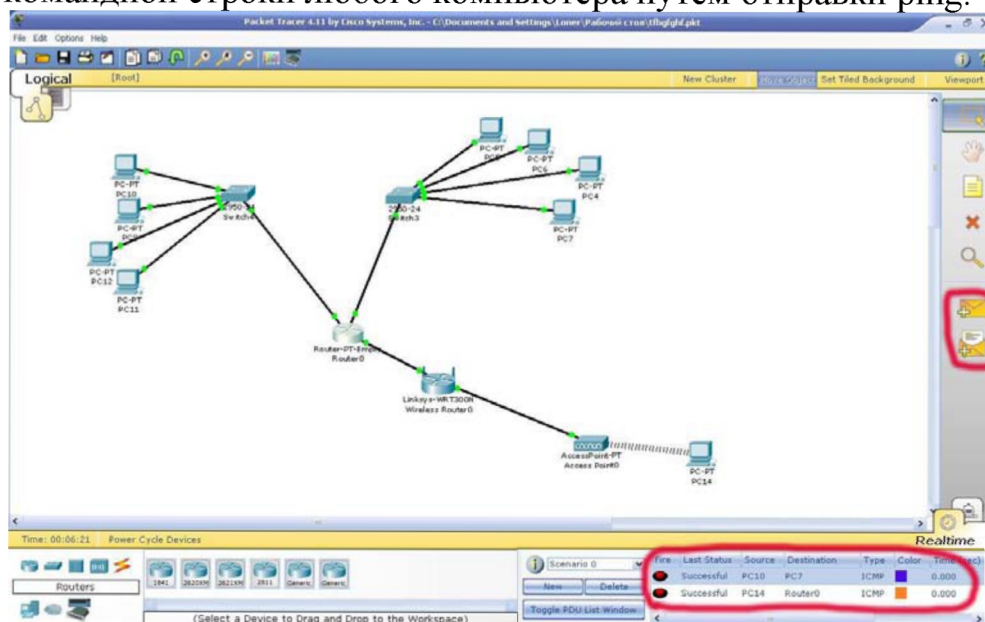


Рисунок 4.2

5 Добавим еще некоторые устройства

Поднимем сервер в одной из подсетей. Для этого в панели объектов выбираем End Devices, конкретнее Server-PT. Соединяем его со свитчем и настраиваем соответственно IP адрес и маршрутизацию.

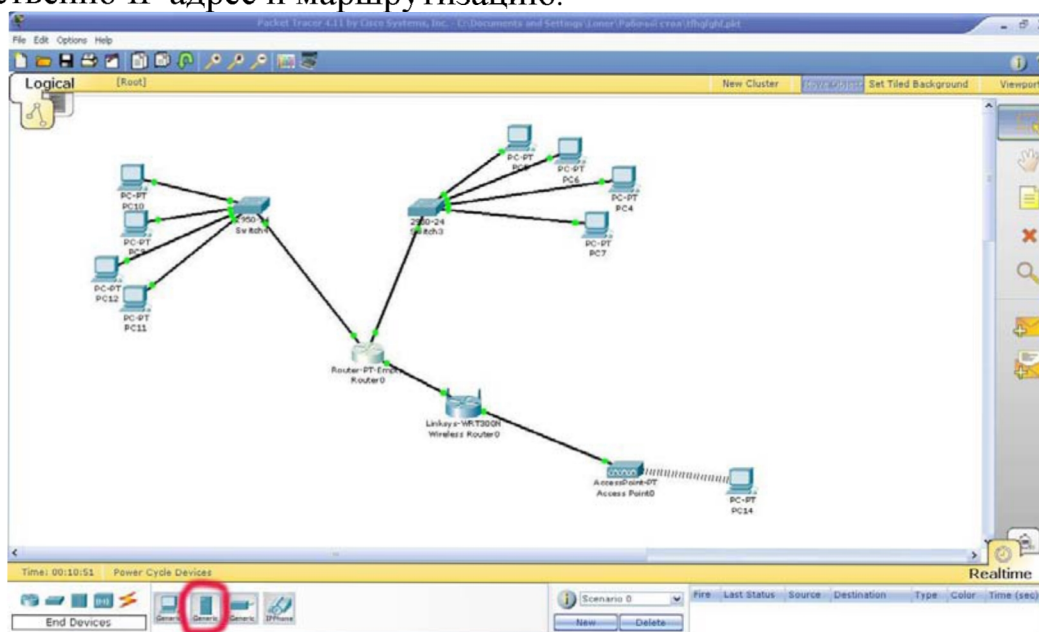


Рисунок 5.1

Тестировать будем, путем входа на сервер из другой подсети, через Web-браузер на одном из компьютеров. Если в браузере отобразится определенная страница, при указании в адресной строке IP адрес сервера, то настроили мы верно.

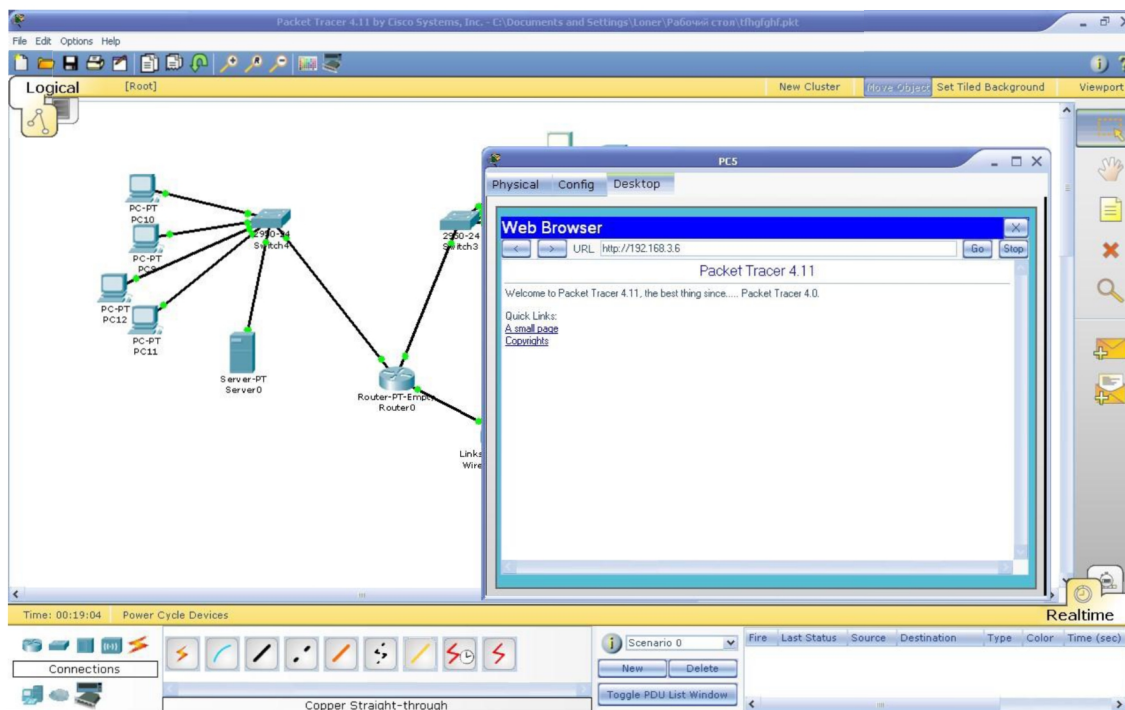


Рисунок 5.2

Добавим DSL модем. Он находится в WAN эмуляции, соединим его с беспроводным роутером и через кабель телефона с облаком (так же WAN эмуляция).

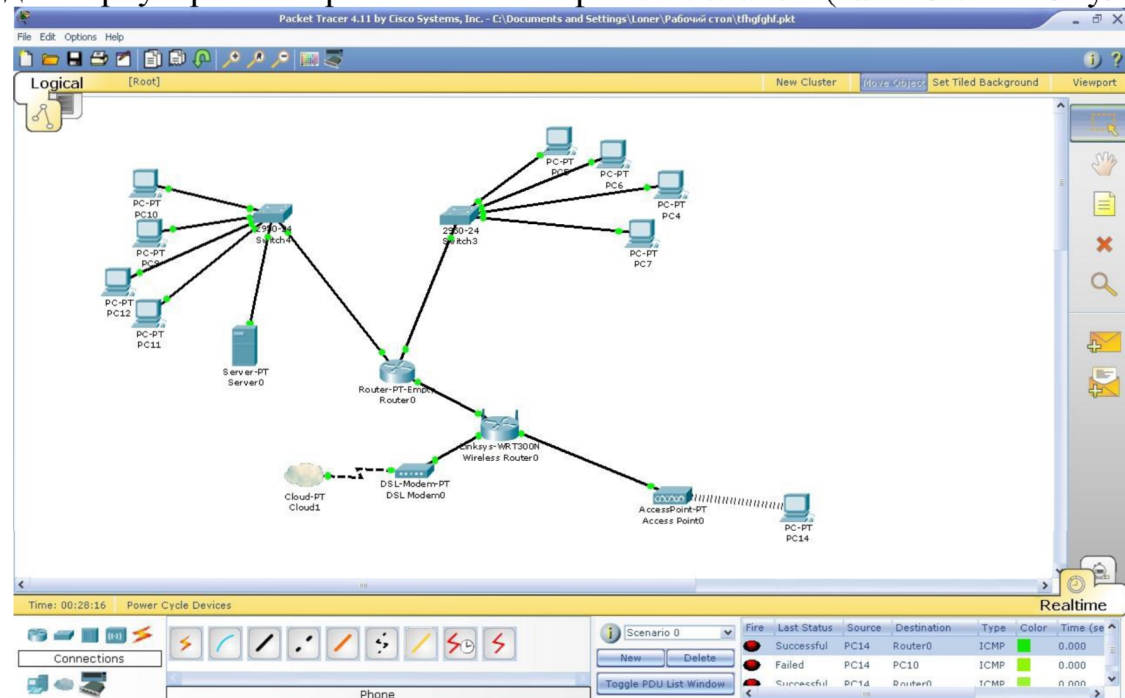


Рисунок 5.3

Итак, мы научились создавать сеть небольшого размера, с сервером и DSL модемом и настраивать ее. В основном все знания, полученные при выполнении предложенной работы достаточны для построения крупных сетей с большим количеством серверов и других устройств.

Packet Tracer 4.0 Skill Building Activity: Using Packet Tracer

Приобретение начальных навыков работы с Packet Tracer 4.11

Objective (Предстоит сделать): Use Packet Tracer to complete the following skills (использовать РТ для формирования следующих навыков):

- To learn to use Packet Tracer (изучить как пользоваться программой Packet Tracer, на примере версии 4.11)
- To examine Ping and MAC tables on various devices using various methods (проверять содержимое таблиц MAC-адресов, применять различными способами команду Ping для проверки различных сетевых устройств)

Scenario

These topologies represent two networks, one using a hub and the other using a switch. These topologies are ideal for studying ARP and ICMP behavior. (Эти топологии (схемы сети в файлах UsingHub.pkt и UsingSwitch.pkt) представляют две сети, одна - на основе хаба, другая – на основе свитча (коммутатора). Они идеально подходят для изучения работы протоколов ARP и ICMP)

Required Files (Необходимые для выполнения работы файлы)

To complete this lab, you will need the following Packet Tracer (.pkt) files.

- UsingHub.pkt
- UsingSwitch.pkt

Plan

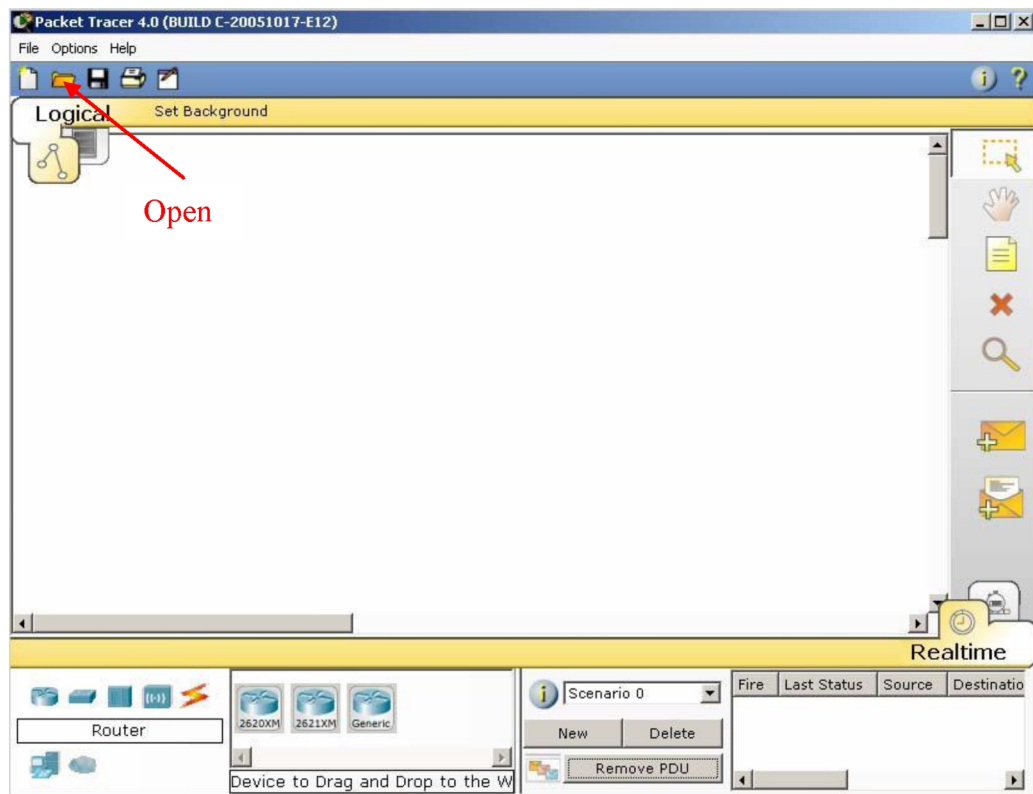
To learn to use Packet Tracer. (изучить как пользоваться программой Packet Tracer, на примере версии 4.11)

What is Packet Tracer? Packet Tracer is a protocol simulator developed by Cisco Systems. Packet Tracer (PT) is a powerful and dynamic tool that displays the various protocols used in networking, in either Real Time or Simulation mode. This includes layer 2 protocols such as Ethernet and PPP, layer 3 protocols such as IP, ICMP, and ARP, and layer 4 protocols such as TCP and UDP. Routing protocols can also be traced. (См. Метод указания)

Purpose (Цель работы): The purpose of this activity is to become familiar with the Packet Tracer interface. Learn how to use existing topologies and build your own. (Ознакомиться с интерфейсом программы. Изучить, как использовать существующие топологии (схемы сетей) и строить свои собственные).

Act (Часть) 1 Introduction to the Packet Tracer Interface using a Hub Topology (Знакомство с интерфейсом Packet Tracer (РТ) на примере сети на основе хаба)

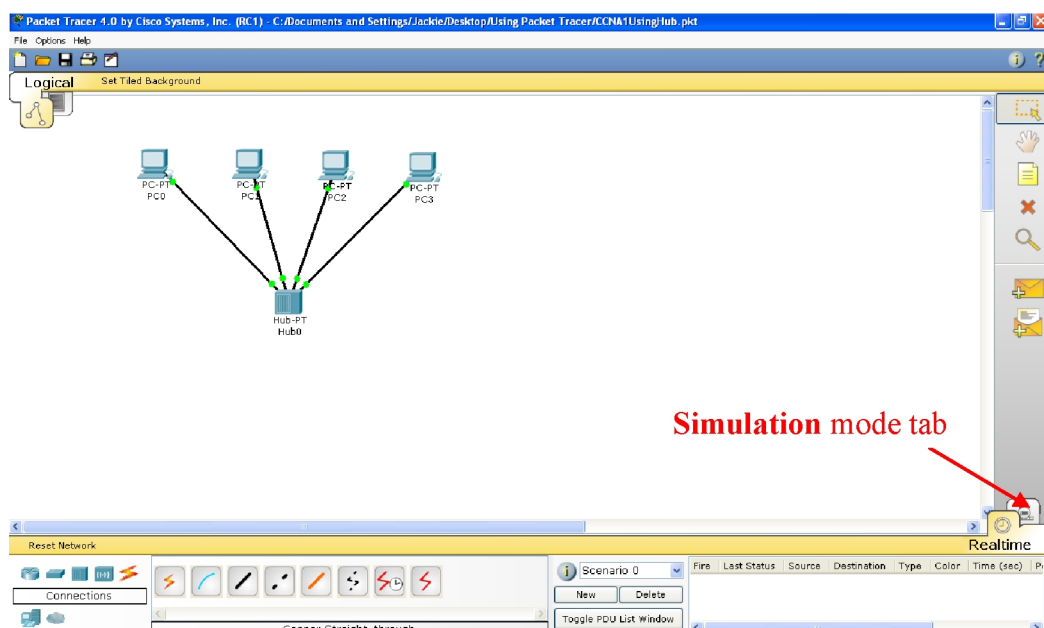
Step (шаг) 1 Start Packet Tracer and Entering Simulation Mode (Запуск РТ и включение Режимы Симуляции)



Step 2 Open an existing topology (Открытие существующей топологии)

Perform the following steps to open the **UsingHub.pkt** file. (Чтобы открыть **UsingHub.pkt**, сделайте следующее):

- Click the Open button on the toolbar. (Кликните кнопку Open)
- Open the CCNA1 folder. (Откройте папку CCNA3.x, затем папку CCNA1)
- Open the SkillBuilder_UsingPacketTracer folder. (Откройте папки ConceptBuilder_VariousProtocolLabs, затем папки SkillBuilder_UsingPacketTracer)
- Open the file UsingHub.pkt. (Двойным кликом запустите файл UsingHub.pkt)

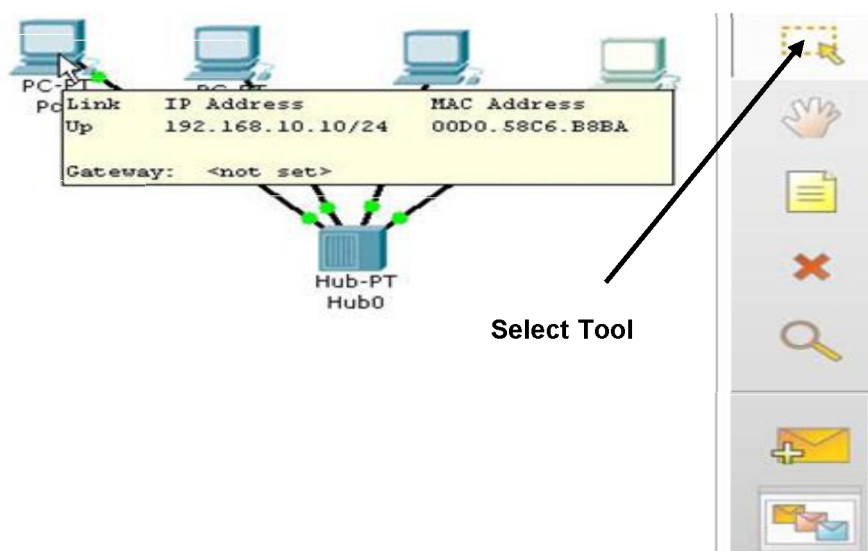


By default, the topology opens in **Realtime** mode. We will examine the difference between **Realtime** and **Simulation** modes in later steps. (По умолчанию топология открывается в **Realtime** mode (режим реального времени). Позже мы рассмотрим подробнее различия между режимами **Realtime** и **Simulation**). **Simulation** mode allows you to view a sequence of events associated with the communications be-

tween two or more devices. **Realtime** mode performs the operation with all of the sequence of events happening at “real time”. (Режим симуляции (т.е. моделирования, точнее программной имитации работы сетевых устройств, с возможностью изменения масштаба времени) позволяет видеть последовательность событий, из которых и складывается коммуникация между двумя или более устройствами. Режим реального времени выполняет (но тоже программно имитирует) ту же последовательность событий но в масштабе времени, характерном для работы реальных сетевых устройств в реальных «сетевых» обстоятельствах).

Help can be obtained by using the Help menu. Both online help and tutorials are available. Please take advantage of these facilities. (Через меню **Help**, доступна подробная справочная информация, плюс **tutorials** – обучающие флэш-анимации).

To view the IP address, subnet mask, default gateway, and MAC address of a host, move the cursor over that computer. Be sure the Select tool is selected. (Чтобы увидеть во всплывающем окне параметры, с которыми сконфигурирован хост (компьютер): IP-адрес, маску подсети, адрес шлюза по умолчанию и MAC-адрес, необходимо навести курсор на значок этого хоста, предварительно убедившись, что в вертикальной панели Common Tools (справа) выбрано средство **Select** (курсор изображается при этом в виде стрелки))



Step 3 Issue a ping from PC0 to PC1 (Выполнение на компьютере PC0 команды ping с IP-адресом компьютера PC1)

Pings and the ICMP protocol will be examined in much more detail in later steps. The ping program generates an IP packet with an encapsulated ICMP Echo Request message. It is a tool used to test basic layer 2 and layer 3 communications between two devices. When the user issues the ping command, most operating systems send multiple (four or five) ICMP Echo messages. When the destination device receives the ping, Echo Request, it issues an Echo Reply.

Command to be issued from PC0 is: **ping 192.168.10.37**

Packet Tracer allows you to either issue the command from the command prompt or to use the Add Simple PDU tool. Both methods will be used.

To enter Simulation Mode click the Simulation Mode tab in the lower right hand corner of the interface.

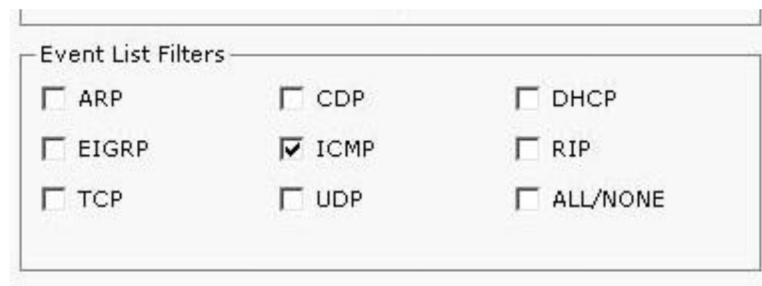
(Команда (программа) ping генерирует IP-пакет, в который инкапсулирован ICMP-эхо-запрос. Ping является инструментом, используемым для тестирования взаимодействия двух устройств на 2-м и 3-м уровнях модели OSI. Когда пользователь исполняет команду ping, большинство операционных систем по умолчанию посылают несколько (4 или 5) ICMP-эхо-запросов. Когда устройство, которому адресован ping, получает ICMP-эхо-запрос, оно генерирует ICMP-эхо-ответ и отправляет его обратно пославшему ping узлу).

В нашем примере хост PC0 должен выполнить команду: **ping 192.168.10.37**.

Packet Tracer позволяет посылать команду ping как обычно из командной строки или «графически», используя средство Add Simple PDU.

Чтобы войти в Simulation Mode надо кликнуть Simulation Mode tab в правом нижнем углу (непосредственно за Realtime Mode tab). После чего появится Simulation Panel).

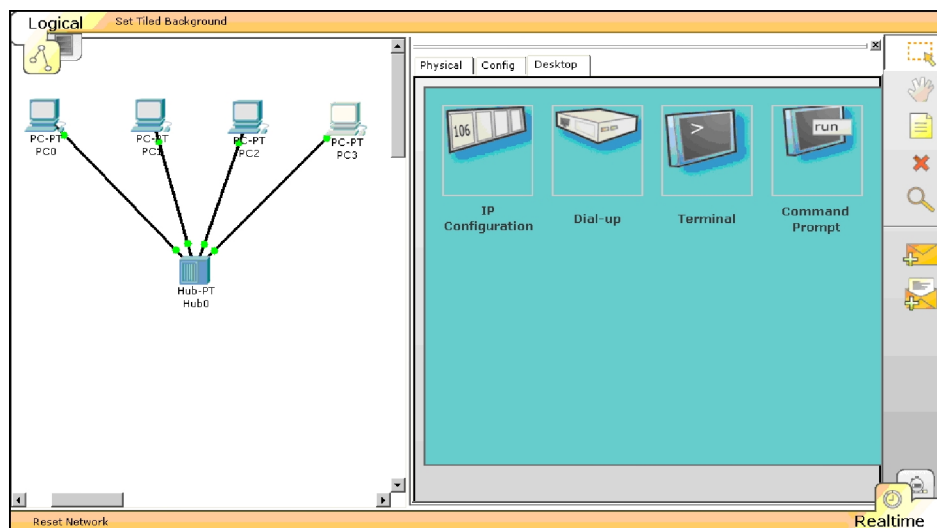
In order to view only the “pings”, in the **Event List**, click on **ALL/NONE** to clear all protocols, and then click on **ICMP** to select only that protocol. (Чтобы в списке событий **Event List** отражалось только то, что связано с командой ping, нужно отредактировать **Event List Filters**. Для этого нажмите кнопку **Edit Filters** в левом нижнем углу **Simulation panel**, затем кликнув на **Show All/None**, отключите события всех протоколов, а затем поставьте галку на протоколе **ICMP**)



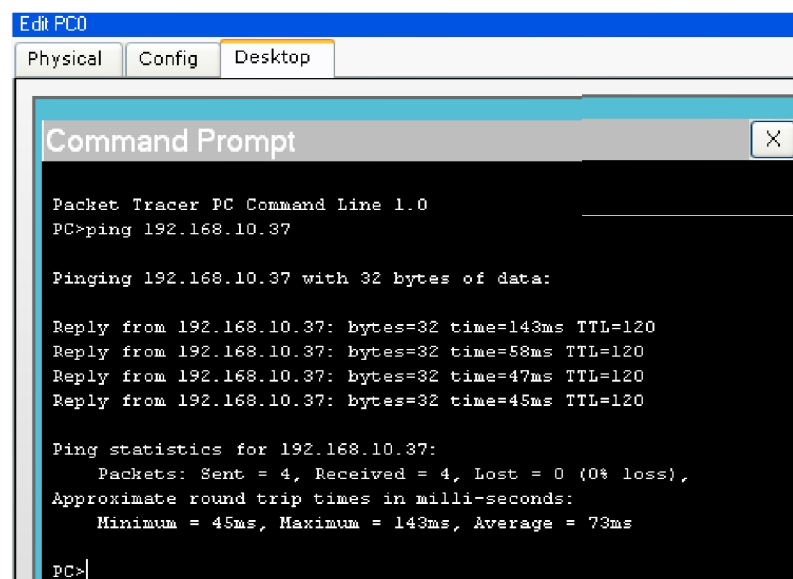
Ping: Using the Command Prompt in Realtime Mode (Выполнение ping из командной строки, находясь в Realtime Mode)

Return to Realtime mode by clicking the Realtime tab in the lower right hand corner of the screen. (Вернитесь в Realtime Mode, кликнув Realtime Mode tab (правый нижний угол основного окна))

1. Single click on **PC0** with the left mouse button. 2. Click on the **Desktop** tab. 3. Click on the **Command Prompt**. (Далее: 1. Кликните левой кнопкой мыши один раз на значок **PC0**. 2. В открывшемся окне управления хостом **PC0** выберите (клик) закладку **Desktop**. 3. В ней справа кликните на **Command Prompt**)



Click after **PC>** prompt and type the following ping command, **ping 192.168.10.37** and press the Enter key. (В открывшемся черном окне кликните после промта **PC>**, и наберите на клавиатуре следующую команду **ping 192.168.10.37**, а затем нажмите Enter).



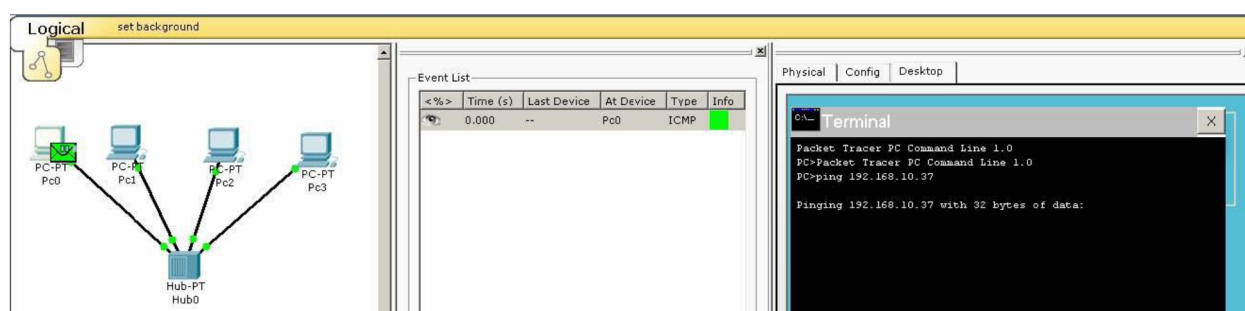
Ping: Using the Simulation mode (Ping в режиме Simulation mode:)

Click on the **Simulation** tab located on the bottom right side of the Packet Tracer screen. The tab is located behind the **Realtime** mode tab. (Перейдите в **Simulation mode**, кликнув на **Simulation** tab справа внизу основного окна (находится за **Realtime** mode tab.)

If you cannot see the topology close the Event List window. (Если окно **Simulation Panel** закрывает топологию (схему сети), его можно закрыть (чтобы потом открыть, кликнуть на кнопку **Event List** слева от **Simulation** tab))

Reissue the ping command in the **Terminal** screen (Use the Up Arrow key to repeat the last command). (Снова выполните ту же самую команду **ping** в уже открытом ранее окне **Command Prompt** (чтобы не пере-набирать команду заново, используйте стрелку вверх на клавиатуре, чтобы вызвать команду из кэша))

You will notice that an ICMP packet is now preparing to leave PC0 (left screen) and is also displayed in the **Event List** (middle screen). Заметьте, что ICMP пакет готовится покинуть PC0 (левая часть иллюстрации) и появилась первая строка в **Event List** (средняя часть иллюстрации)



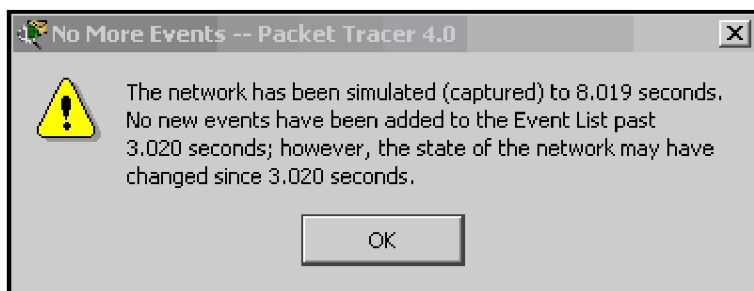
Click on the **Capture / Forward** button in **Play Controls** (the yellow bar below the windows) to view a step-by-step process of the ping command. Начинаяте кликать на кнопку **Capture / Forward** на вкладке **Simulation Panel** (или на желтой полосе под основным окном) что бы увидеть пошагово процесс выполнения команды ping.

As you click through the events, notice how the hub processes each frame (Ethernet frame, IP packet, and ICMP message). Notice that each event is listed in the Event List. Also, notice that the ping program displays the ICMP Echo Reply returned to PC0 from PC1. Продолжая кликать, обратите внимание, как хаб обрабатывает каждый кадр (Ethernet кадр, IP пакет, and ICMP сообщение) и в окне Event List появляются строки, описывающие события. Обратите также внимание, что команда ping показывает ICMP Echo Reply (эхо-ответ), возвращенный компьютеру PC0 от компьютера PC1.



Continue clicking the Capture / Forward button until all frames have been sent. **Notice that the hub floods all of the frames out all ports except the port in came in on.** Продолжайте кликать на кнопку **Capture / Forward** не будут посланы все кадры. Заметьте, что хаб рассылает поступающий на вход кадр на все свои порты (floods - затопливает), кроме того, на который пришел входящий кадр.

When the ping program is finished sending four pings (ICMP Echo Requests) you will receive the following message: Когда программа ping завершит посылать свои эхо запросы (ICMP Echo Requests), будет показано сообщение, вроде следующего:



Using the Simple PDU Tool Использование средства Simple PDU Tool

Another method for pinging a device is the use of the **Simple PDU tool**. This tool performs the ping without having to issue the ping command. Before proceeding with this step, close the Desktop for PC0, click the “X” in the right-hand corner. Другой метод проверки сети с помощью команды ping – это использование **средства Simple PDU Tool**. Закройте окно Desktop for PC0 (клик на крестик в правом верхнем углу этого окна).

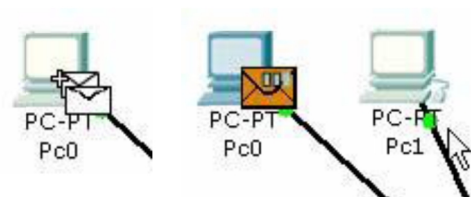


Restore the **Event List** if necessary by clicking Event List on the yellow bar to the left of Simulation and clicking the Reset Simulation button. Восстановите **Event List** (откройте заново, если окно не видно – кликните на кнопку **Event List** на желтой полосе), затем очистите окно, нажав кнопку **Reset Simulation**.

Choose the **Add Simple PDU** tool from the tool box Нажмите кнопку **Add Simple PDU** на правой вертикальной панели (tool box):



Click once on PC0, the device issuing the ping (ICMP Echo Request) and then click once on PC1 (the destination of the ICMP Echo Request). Кликните на иконку устройства, с которого выдается эхо-запрос (ICMP Echo Request), то есть на PC0, затем кликните на иконку устройства, которому направляется эхо-запрос, то есть на PC1.



Click the Capture / Forward button and watch the ICMP Echo Requests and ICMP Echo Replies. **Notice that the hub floods all of the frames out all ports except the incoming port.** Кликните на кнопку **Capture / Forward** и наблюдайте прохождение эхо-запросов и эхо-ответов. Заметьте, что **хаб рассылает поступающий на вход кадр на все свои порты, кроме того, на который пришел входящий кадр.**

Note: This tool only sends a single ICMP Echo Request instead of the four pings when using the command prompt. Средство **Simple PDU Tool** посылает единственный эхо-запрос, а не четыре как в том случае, когда команда ping выдается из командной строки.

Step 4 Viewing the frame using Protocol Analyzer Просмотр содержимого кадра с помощью анализатора протокола (Protocol Analyzer)

To examine the actual protocols being sent, click on the colored **Info** box in the **Event List**. Чтобы просмотреть информацию, посылаемую реально разными протоколами, следует кликнуть на цветной квадратик соответствующего события в колонке **Info** окна **Event List**.

PDU Info at Device: Pc0

OSI Model | Outbound PDU Details

At Device: Pc0
Source: Pc0
Destination: Pc1

In Layer

Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

Out Layer

Layer7
Layer6
Layer5
Layer4
Layer3: IP Header Src. IP: 192.168.10.10, Dest. IP: 192.168.10.37
Layer2:
Layer1

1. The Ping process starts next ping request.
2. The Ping process creates an ICMP echo request message and sends it to the lower process.
3. The source IP address is not specified. The device sets it to the port's IP address.
4. The destination IP address is in the same subnet. The device sets the next hop to destination.

Challenge Me << >>

Event List

<%>	Time (s)	Last Device	At Device	Type	Info
0.000	--	Pc0	Pc0	ICMP	
0.004	--	Pc0	Pc0	ICMP	
0.005	Pc0	Hub0	Pc0	ICMP	
0.006	Hub0	Pc1	Pc1	ICMP	
0.006	Hub0	Pc2	Pc2	ICMP	
0.006	Hub0	Pc3	Pc3	ICMP	
0.007	Pc1	Hub0	Pc1	ICMP	
0.008	Hub0	Pc0	Pc0	ICMP	
0.008	Hub0	Pc2	Pc2	ICMP	
0.008	Hub0	Pc3	Pc3	ICMP	

Reset Network ☒ Constant Delay



The default is a layer 3 **Outbound OSI Model** view with a brief description with what is occurring with this packet: По умолчанию открывается вкладка **OSI Model** с кратким описанием того, что происходит с пакетом на 3 уровне модели **OSI** на выходе из соответствующего устройства.

PDU Info at Device: Pc0

OSI Model | Outbound PDU Details

At Device: Pc0
Source: Pc0
Destination: Pc1

In Layer

Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

Out Layer

Layer7
Layer6
Layer5
Layer4
Layer3: IP Header Src. IP: 192.168.10.10, Dest. IP: 192.168.10.37
Layer2:
Layer1

1. The Ping process starts next ping request.
2. The Ping process creates an ICMP echo request message and sends it to the lower process.
3. The source IP address is not specified. The device sets it to the port's IP address.
4. The destination IP address is in the same subnet. The device sets the next hop to destination.

Challenge Me << >>

Click on the **Outbound PDU Details** tab to see the layer 2 Ethernet frame, and the layer 3 IP packet and ICMP message. Кликните на закладку **Outbound PDU Details**, чтобы увидеть структуру и содержимое соответственно: заголовков кадра Ethernet на 2-м уровне модели **OSI**, пакета IP и сообщения ICMP на 3-м уровне модели **OSI**.

PDU Info at Device: Pc0			
OSI Model		Outbound PDU Details	
PDU Formats			
Ethernet II			
0	4	8	14 19 Bytes
PREAMBLE: 1010 1010		DEST MAC: 0002.16AB.5C50	
		SRC MAC: 00D0.58C6.B8BA	
TYPE: 0x800		DATA (VARIABLE LENGTH)	
		FCS: 0x0	
IP			
0	4	8	16 19 31 Bits
4 IHL		TOS: 0x0	
ID: 0x0		TL: 0x0	
		FRAG OFFSET: 0x0	
TTL: 32		PRO: 0x1	
		CHKSUM: 0x0	
SRC IP: 192.168.10.10			
DST IP: 192.168.10.37			
OPT: 0x0		0x0	
DATA (VARIABLE LENGTH)			
ICMP			
0	8	16	31 Bits
TYPE: 0x8		CODE: 0x0	
		CHECKSUM: 0x0	

Click on layer 2 of the **Outbound OSI Model** view with a brief description with what is occurring at layer 2:
 Кликните на layer 2 правого окошка Out Layers, что бы увидеть краткое описание того, что происходит на 2-м уровне модели OSI.

PDU Info at Device: Pc0
OSI Model
Outbound PDU Details

At Device: Pc0
Source: Pc0
Destination: Pc1

In Layer
Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

Out Layer
Layer7
Layer6
Layer5
Layer4
Layer3: IP Header Src. IP: 192.168.10.10, Dest. IP: 192.168.10.37
Layer 2:
Layer1

1. The next hop IP address is unicast. The ARP process looks it up in the ARP table.
2. The next hop IP address is not in the ARP table. The ARP process tries to send an ARP request for that IP address and buffers this packet.

Challenge Me
<<
>>

Act 2 Looking at the Switch Algorithm and Switch MAC Address Tables Рассмотрение алгоритма работы коммутатора и таблицы MAC адресов коммутатора

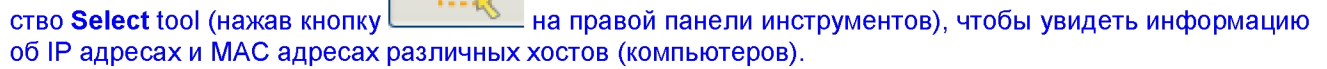
Step 1

Open the **UsingSwitch.pkt** file. Do not save the changes to the current network. Notice the similarity to the previous topology. The layer 1 hub has been replaced with a layer 2 switch. **Откройте файл UsingSwitch.pkt. Не сохраняйте!** изменения текущей работы. Заметим, что топология сети похожа на предыдущую (звезда).

Click on the **Simulation** icon to switch to simulation mode. **Кликните на кнопку Simulation**, чтобы переключиться в режим симуляции.

Step 2 Viewing the Switch MAC Address Table Просмотр таблицы MAC адресов коммутатора

Use the **Select** tool to view IP address and MAC address information for the various hosts. **Используйте сред-**



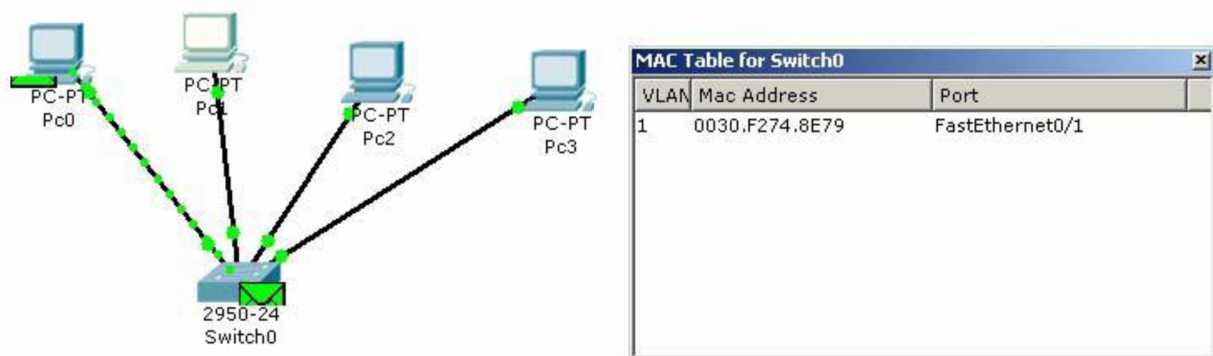
кнопку  на правой панели инструментов), чтобы увидеть **таблицу MAC адресов коммутатора**.

Diagram illustrating a switch configuration for VLAN 10. A central switch labeled "2950-24 Switch0" is connected to four PCs labeled "PC-PT PC0", "PC-PT PC1", "PC-PT PC2", and "PC-PT PC3". A window titled "MAC Table for Switch0" is open, showing a table with columns "VLAN", "Mac Addr", and "Port". The table is currently empty.

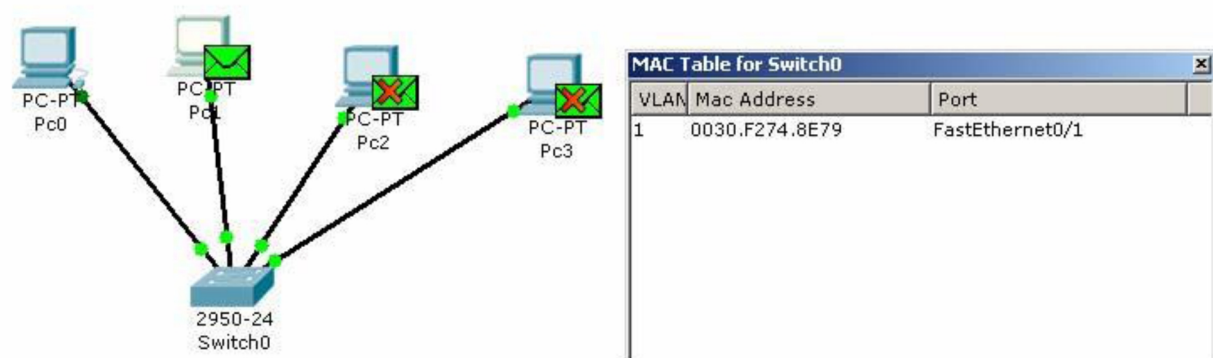
Note: Because of how Packet Tracer deals with the Spanning Tree Protocol, at times the switch may show amber lights on its interfaces. To correct this, click the **Realtime** mode icon, wait for the lights to turn green, and then click the **Simulation** mode icon, returning to where you left off. **Поскольку Packet Tracer реализует среди прочих и Spanning Tree Protocol, при включении коммутатора (или активизации отдельного его порта) сигнальные огни портов сначала становятся оранжевыми (пока отработывает алгоритм «покрывающего дерева», который ищет и отключает петли в топологии сети), и лишь затем становятся зелеными, когда коммутатор (порт) полностью готов к работе. Поэтому для ускорения описанного процесса рекомендуется временно переключиться в режим Realtime, а затем вернуться в режим Simulation, когда огни станут зелеными.**



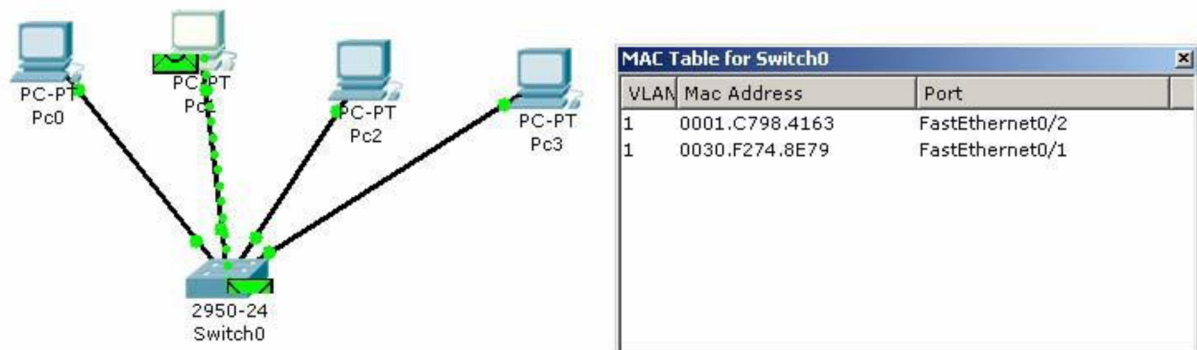
9



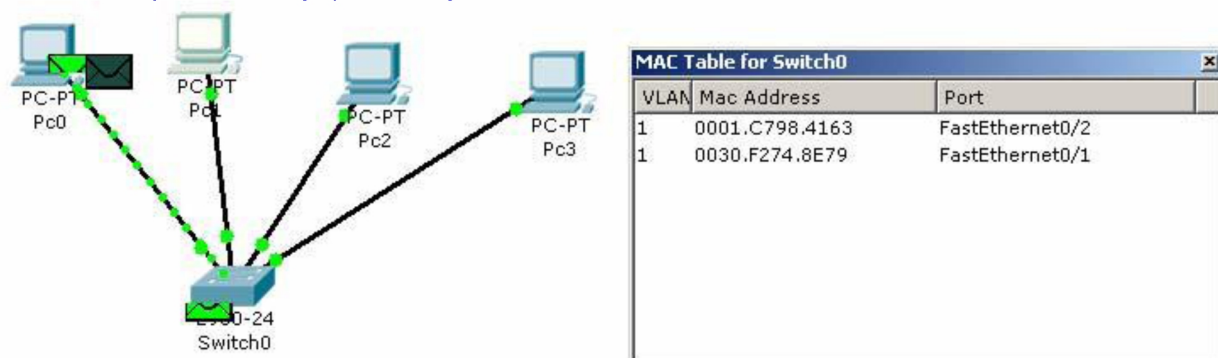
The packet is flooded out all ports because the Switch's MAC Address Table does not contain the Destination Address of the Ethernet frame. PC2 and PC3 disregard the frame: **Пакеты отправляются коммутатором на все его порты, поскольку таблица MAC адресов коммутатора не содержит MAC адрес получателя.**



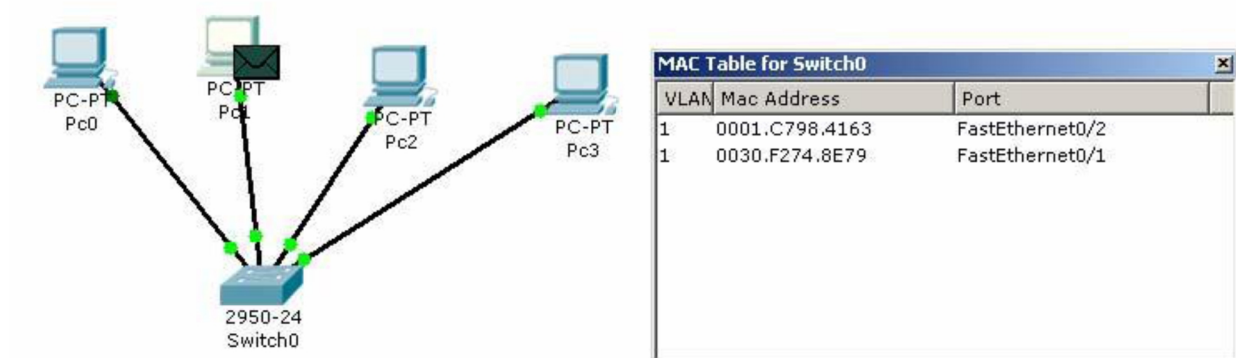
PC1 return the ARP reply. Switch0 learns the Source MAC Address of PC1: **PC1 возвращает ARP ответ. Коммутатор получает искомый MAC адрес хоста PC1 в качестве адреса отправителя.**



Because the Source MAC Address of PC0 was learned previously, when examining the Destination MAC Address of the frame, Switch0 filters the frame by only sending it out FastEthernet port 0/1. **Поскольку исходящий MAC адрес хоста PC0 только что был занесен в таблицу, коммутатор посылает кадр только на порт FastEthernet port 0/1, ведущий к хосту PC0.**



The rest of the pings, frames with IP packets containing ICMP Echo Requests from PC0 destined for PC1 and frames with IP packets containing ICMP Echo Replies from PC1 destined for PC0, are filtered by the switch and only sent out the appropriate interface (port). Далее собственно выполняется оставшаяся часть команды ping. Кадры с IP пакетами, содержащими ICMP эхо-запросы от PC0 идут напрямую к PC1, и, соответственно, кадры с IP пакетами, содержащими ICMP эхо-ответы от PC1 идут напрямую к PC0.



Step 4 Creating multiple scenarios

A technique used to learn new software is to experiment. Try different tools, look at various protocols using the Event List and the Info box, and use the Help and Tutorials. Have fun!

Act 3 Journaling

As you play with Packet Tracer, please record insights in your journal and answer the following questions

- How do you think network modeling will help your learning?
- Did your concepts of Ethernet, the hub algorithm, and the switch algorithm, change after using Packet Tracer?
- While using Packet Tracer, what questions about networking occurred to you?

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Самарский государственный аэрокосмический университет
имени академика С.П. Королева
(национальный исследовательский университет)»

Факультет информатики
Кафедра технической кибернетики

Динамическая маршрутизация и списки доступа

**Методические указания к лабораторной работе
по курсу компьютерные телекоммуникации**

ОГЛАВЛЕНИЕ

1. Настройка маршрутизаторов фирмы Cisco. Система команд IOS	3
1.1. Привилегированный режим	4
1.2. Режим глобальной конфигурации	5
1.3. Режим настройки интерфейсов	6
1.4. Настройка статической маршрутизации	7
2. Динамическая маршрутизация	8
2.1. Протокол маршрутизации RIP	8
2.2. Протокол маршрутизации EIGRP	11
2.3. Протокол маршрутизации OSPF	14
2.4. Замена одного протокола маршрутизации другим	16
3. Фильтрация пользовательского трафика	17
3.1. Списки доступа (Access Control List, ACL)	17
3.2. Списки доступа в маршрутизаторах Cisco	18
3.3. Создание стандартных списков доступа для протокола IP	19
3.4. Создание расширенных списков доступа для протокола IP	21
3.5. Назначение списков доступа на интерфейсы	22
Список контрольных вопросов	24
ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ОТЧЕТА	24

1. Настройка маршрутизаторов фирмы Cisco. Система команд IOS

Маршрутизаторы и коммутаторы фирмы Cisco управляются с помощью операционной системы IOS (Interconnection Operation System – межсетевая операционная система). Основным способом конфигурирования устройств фирмы Cisco является конфигурирование через интерфейс командной строки.

Режимы командной строки в IOS имеет несколько уровней. На рис. 1 приведена схема иерархии режимов.

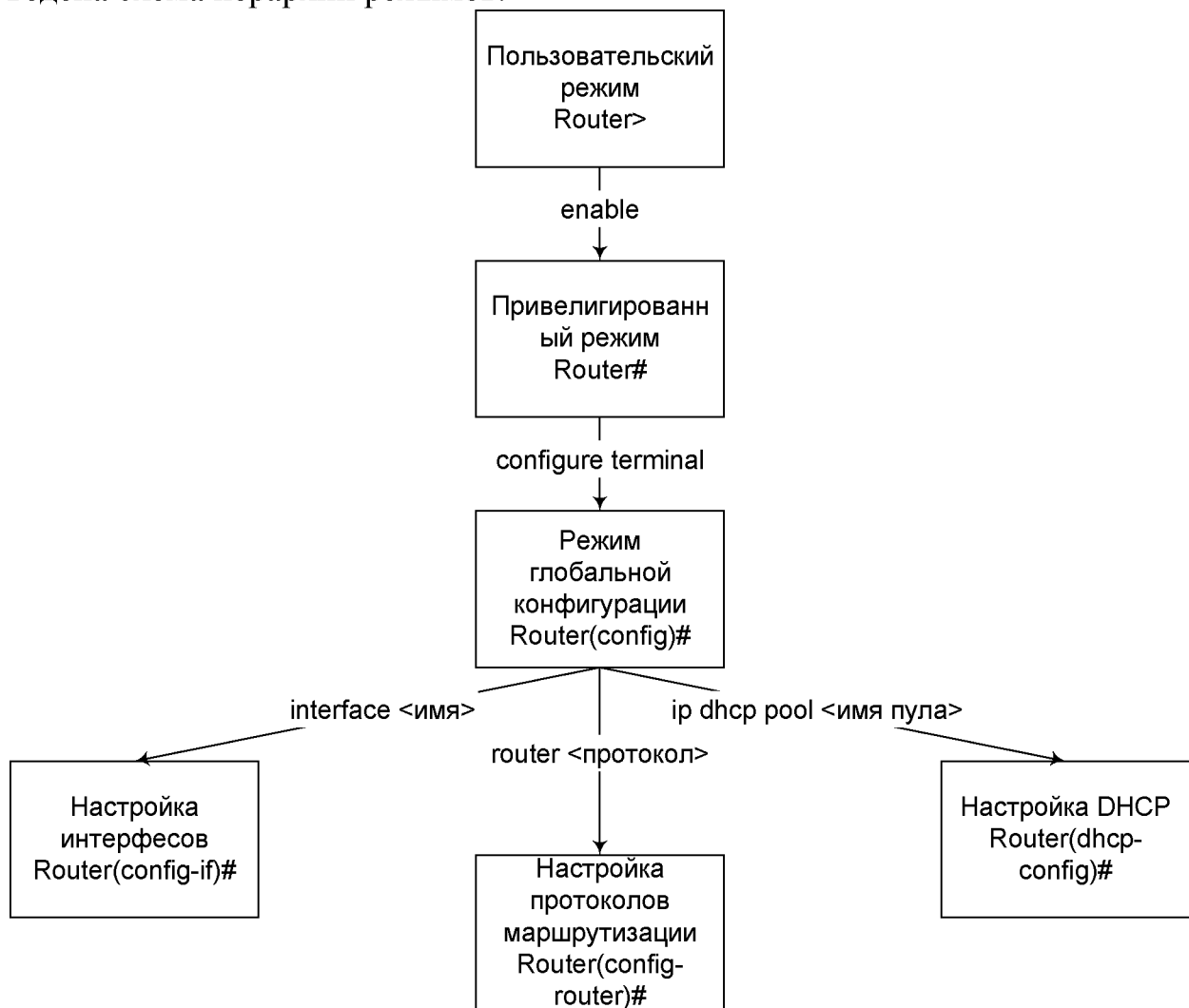


Рис.1. Иерархия режимов настройки Cisco IOS.

При подключении к роутеру, первоначально загружается пользовательский режим. Из этого режима невозможно производить настройку, можно лишь посмотреть некоторые текущие настройки. Приглашение командной строки имеет вид:

```
Router>
```

для перехода в привилегированный режим необходимо выполнить команду `enable`.

1.1. Привилегированный режим

Как правило, переход в привилегированный режим защищается паролем. После выполнения команды и ввода имени пользователя и пароля (если необходимо), IOS переходит в привилегированный режим. Приглашение командной строки сменит вид на:

```
Router#
```

Из данного режима можно посмотреть любые текущие настройки, запустить отладку. Основной командой для просмотра настроек является семейство команды `show`. Ниже приведены наиболее часто употребляемые команды.

```
show version
```

Выводит информацию об устройстве, версии IOS, текущее значение конфигурационного регистра.

```
show running-config
```

Выводит текущие настройки (хранящиеся в оперативной памяти).

```
show startup-config
```

Выводит настройки, хранящиеся в файле конфигураций (хранятся в NVRAM). Именно эти настройки будут использоваться при загрузке устройства (роутера или коммутатора).

```
show interfaces
```

Выводит информацию по всем интерфейсам устройства.

```
show interfaces <имя интерфейса>
```

Пример:

```
show interfaces serial0/0
```

Выводит информацию только по конкретному интерфейсу (например serial0/0).

```
show controllers serial <номер последовательного интерфейса>
```

Пример:

```
show controllers serial 0/0
```

Выводит информацию по контроллеру последовательного интерфейса. Позволяет определить, какой тип кабеля подсоединен (DCE или DTE), а так же частоту синхронизации (на стороне DCE).

```
show ip protocols
```

Показывает информацию о протоколах 3-го уровня модели OSI (ip-протоколы). В частности о запущенных протоколах маршрутизации и их настройках.

```
show ip route
```

Выводит таблицу маршрутизации для данного роутера.

```
show access-lists
```

Выводит информацию о всех списках доступа, настроенных на маршрутизаторе.

```
show access-lists <номер или имя списка>
```

Пример:

```
show access-lists 101
```

Выводит информацию о конкретном списке доступа (например, о списке номер 101).

```
show ip dhcp binding
```

Показывает информацию о выданных протоколом DHCP адресах.

Так же из привилегированного режима можно сохранить текущие настройки в энергонезависимую память (NVRAM), для того, чтобы после перезагрузки устройства сделанные настройки автоматически применились и не пришлось делать настройку заново. Это выполняется с помощью команды

```
copy running-config startup-config
```

1.2. Режим глобальной конфигурации

Для настройки роутера, необходимо перейти в режим глобальной конфигурации с помощью команды

```
configure terminal
```

После выполнения этой команды, приглашение командной строки сменится на

```
Router(config)#
```

Из режима глобальной конфигурации можно переходить к более детальным настройкам, например настройкам интерфейсов. Однако некоторые настройки выполняются непосредственно из этого режима.

Например, можно сменить имя устройства. Это делается с помощью команды

```
hostname <новое имя>
```

Пример:

```
hostname r1
```

После выполнения этой команды смениться приглашение командной строки, например было:

```
Router(config)#
```

станет

```
r1(config)#
```

1.3. Режим настройки интерфейсов

Все активные интерфейсы на маршрутизаторах должны быть специальным образом настроены. Как минимум, для нормальной работы необходимо настроить IP-адрес интерфейса и маску подсети (таким образом, обозначив его принадлежность к какой-то сети или подсети). Для последовательных интерфейсов, к которым подключен кабель DCE, так же необходимо указать частоту синхронизации.

Для перехода в режим настройки интерфейса необходимо выполнить команду

```
interface <имя интерфейса>
```

Пример:

```
interface fastEthernet 0/0
```

После выполнения данной команды мы перейдем в режим настройки интерфейса (например интерфейса fastEthernet 0/0). Так же смениться приглашение командной строки:

```
Router(config-if)#
```

В этом режиме доступны следующие команды:

```
ip address <IP-адрес> <маска>
```

Пример:

```
ip address 10.0.0.1 255.0.0.0
```

Эта команда задает IP-адрес и маску подсети на интерфейсе (в данном случае IP-адрес будет 10.0.0.1, а маска 255.0.0.0)

```
no shutdown
```

Эта команда включает интерфейс в работу. По умолчанию, на роутере все интерфейсы выключены, для того, чтобы включить интерфейс необходимо выполнить эту команду из режима настройки интерфейса. Для того чтобы выключить интерфейс существует команда

```
shutdown
```

```
clock rate <частота синхронизации>
```

Устанавливает частоту синхронизации (в битах в секунду). Данная команда актуальна только при настройке последовательного интерфейса к которому подключен DCE кабель. Без указания частоты синхронизации последовательный порт правильно работать не будет (будет физическое соединение на 1-м уровне модели OSI, но не будет логического соединения на 2-м уровне).

1.4. Настройка статической маршрутизации

Статические маршруты задаются непосредственно из режима глобальной конфигурации с помощью команды

```
ip route <адрес сети назначения> <маска сети назначения>  
<имя интерфейса> [метрика]
```

или

```
ip route <адрес сети назначения> <маска сети назначения>  
<адрес> [метрика]
```

Здесь адрес сети назначения – это адрес удаленной сети, до которой прописывается статический маршрут. Маска сети назначения – маска удаленной сети, до которой прописывается маршрут. Имя интерфейса – имя интерфейса, через который доступна удаленная сеть. Метрика – необязательный параметр, позволяющий указать метрику статического маршрута. По умолчанию, статические маршруты имеют метрику 1 (максимальная метрика 255). Чем меньше значение метрики, тем лучше маршрут.

Пример:

```
ip route 30.0.0.0 255.0.0.0 200.0.0.1 3
```

После выполнения этой команды в таблицу маршрутизации будет добавлен маршрут до сети 30.0.0.0 с маской 255.0.0.0, данная сеть доступна по адресу 200.0.0.1, метрика маршрута будет равна 3.

2. Динамическая маршрутизация

2.1. Протокол маршрутизации RIP

Протокол RIP является дистанционно-векторным протоколом внутренней маршрутизации. Процесс работы протокола состоит в рассылке, получении и обработке векторов расстояний до IP-сетей, находящихся в области действия протокола, то есть в данной RIP-системе. Результатом работы протокола на конкретном маршрутизаторе является таблица, где для каждой сети данной RIP-системы указано расстояние в хопах до этой сети и адрес следующего маршрутизатора. Информация о номере сети и адресе следующего маршрутизатора из этой таблицы вносится в таблицу маршрутов, информация о расстоянии до сети используется при обработке векторов расстояний.

2.1.1. Алгоритм построения таблицы маршрутов

Вектором расстояний называется набор пар ("Сеть", "Расстояние до этой сети"), извлеченный из таблицы маршрутов. Каждую такую пару мы назовем элементом вектора расстояний. Мы будем записывать вектор расстояний в виде (A=2, B=1): это означает, что расстояние от данного маршрутизатора до сети A равно 2, до сети B - 1.

Расстояние до сети, к которой маршрутизатор подключен непосредственно, примем равным 1.

Каждый маршрутизатор, на котором запущен модуль RIP, периодически широковещательно распространяет свой вектор расстояний. Вектор распространяется через все интерфейсы маршрутизатора, подключенные к сетям, входящим в RIP-систему.

Каждый маршрутизатор также периодически получает векторы расстояний от других маршрутизаторов. Расстояния в этих векторах увеличиваются на 1, после чего сравниваются с данными в таблице маршрутов, и, если расстояние до какой-то из сетей в полученном векторе оказывается меньше расстояния, указанного в таблице, значение из таблицы замещается новым (меньшим) значением, а адрес маршрутизатора, приславшего вектор с этим значением, записывается в поле "Следующий маршрутизатор" в этой строке таблицы. После этого вектор расстояний, рассылаемый данным маршрутизатором, соответственно изменится.

2.1.2. Реализация протокола RIP

Существуют две версии протокола RIP: RIP-1 и RIP-2. Версия 2 имеет некоторые усовершенствования, как то: возможность маршрутизации сетей по модели CIDR (кроме адреса сети передается и маска), поддержка мультикастинга, возможность использования аутентификации RIP-сообщений и др.

2.1.3. Работа протокола RIP

Для каждой записи в таблице маршрутов существует время жизни, контролируемое таймером. Если для любой конкретной сети, внесенной в таблицу маршрутов, в течение 180 с не получен вектор расстояний, подтверждающий или

устанавливающий новое расстояние до данной сети, то сеть будет отмечена как недостижимая (расстояние равно бесконечности). Через определенное время модуль RIP производит "сборку мусора" - удаляет из таблицы маршрутов все сети, расстояние до которых бесконечно.

При получении сообщения типа "ответ" для каждого содержащегося в нем элемента вектора расстояний модуль RIP выполняет следующие действия:

- проверяет корректность адреса сети и маски, указанных в сообщении;
- проверяет, не превышает ли метрика (расстояние до сети) бесконечности;
- некорректный элемент игнорируется;
- если метрика меньше бесконечности, она увеличивается на 1;
- производится поиск сети, указанной в рассматриваемом элементе вектора расстояний, в таблице маршрутов;
- если запись о такой сети в таблице маршрутов отсутствует и метрика в полученном элементе вектора меньше бесконечности, сеть вносится в таблицу маршрутов с указанной метрикой; в поле "Следующий маршрутизатор" заносится адрес маршрутизатора, приславшего сообщение; запускается таймер для этой записи в таблице;
- если искомая запись присутствует в таблице с метрикой больше, чем объявленная в полученном векторе, в таблицу вносятся новые метрика и, соответственно, адрес следующего маршрутизатора; таймер для этой записи перезапускается;
- если искомая запись присутствует в таблице и отправителем полученного вектора был маршрутизатор, указанный в поле "Следующий маршрутизатор" этой записи, то таймер для этой записи перезапускается; более того, если при этом метрика в таблице отличается от метрики в полученном векторе расстояний, в таблицу вносится значение метрики из полученного вектора;
- во всех прочих случаях рассматриваемый элемент вектора расстояний игнорируется.

Сообщения типа "ответ" рассылаются модулем RIP каждые 30 с по широковещательному или мультикастинговому (только RIP-2) адресу; рассылка "ответа" может происходить также вне графика, если маршрутная таблица была изменена (triggered response). Стандарт требует, чтобы triggered response рассылался не немедленно после изменения таблицы маршрутов, а через случайный интервал длительностью от 1 до 5 с. Эта мера позволяет несколько снизить нагрузку на сеть.

В каждую из сетей, подключенных к маршрутизатору, рассылается свой собственный вектор расстояний. Там, где это возможно, адреса сетей агрегируются (обобщаются), то есть несколько подсетей с соседними адресами объединяются под одним, более общим адресом с соответствующим изменением маски.

В случае triggered response посылается информация только о тех сетях, записи о которых были изменены.

Информация о сетях с бесконечной метрикой посылается только в том случае, если она была недавно изменена.

При получении сообщения типа "запрос" с адресом 0.0.0.0 маршрутизатор рассылает в соответствующую сеть обычное сообщение типа ответ. При получении запроса с любым другим значением в поле (полях) "IP Address" посылается ответ, содержащий информацию только о сетях, которые указаны. Такой ответ посылается на адрес запросившего маршрутизатора (не широковещательно).

2.1.4. Настройка протокола динамической маршрутизации RIP

Из режима глобальной конфигурации необходимо выполнить команду

```
router rip
```

после этого измениться приглашение командной строки:

```
Router(config-router)#
```

Таким образом мы перейдем в режим настройки протокола маршрутизации. Для настройки протокола RIP необходимо выполнить следующие команды:

```
version 2
```

Эта команда активизирует версию 2 протокола RIP (различия между первой и второй версией описаны выше).

Далее необходимо перечислить все непосредственно подключенные к маршрутизатору сети (т.е. сети, к которым относятся интерфейсы маршрутизатора). Для этого существует следующая команда:

```
network <адрес сети>
```

в данном случае маска подсети не указывается, при необходимости использовать маску, роутер автоматически узнает маску из настроек интерфейса.

Пример. Допустим к маршрутизатору непосредственно подключены 2 сети: 10.0.0.0/8 и 100.0.0.0/30. Из режима настройки протокола маршрутизации выполним следующие команды:

```
network 10.0.0.0
```

```
network 100.0.0.0
```

После этого, протокол RIP будет передавать в другим роутерам информацию о том, что к нему непосредственно подключены данные сети. Протоколы RIP запущенные на других роутерах будут использовать эту информацию для построения маршрутов.

Примечание 1. Записи /8 и /30 обозначают сокращенную запись маски. /8 соответствует маске 255.0.0.0, /30 маске 255.255.255.252. Вообще число указанное после символа «/» означает количество подряд идущих единиц в маске (/17 – 17 подряд идущих единиц в маске подсети, это будет соответствовать записи 255.255.128.0).

Примечание 2. Оборудование Cisco может отображать маску подсети в сокращенном виде, однако при настройке необходимо указывать маску в стандартном виде IP-адреса.

После выполнения всех вышеописанных команд на роутере будет настроен протокол динамической маршрутизации RIP.

2.2. Протокол маршрутизации EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol) – дистанционно-векторный протокол маршрутизации, разработанный фирмой Cisco на основе протокола IGRP той же фирмы. Протокол IGRP был создан как альтернатива протоколу RIP (до того, как был разработан OSPF). После появления OSPF Cisco представила EIGRP – переработанный и улучшенный вариант IGRP, свободный от основного недостатка дистанционно-векторных протоколов – особых ситуаций с заикливанием маршрутов – благодаря специальному алгоритму распространения информации об изменениях в топологии сети. Несмотря на то, что в общем случае протоколы состояния связей (OSPF) отрабатывают изменения в топологии сети быстрее, чем EIGRP, а также OSPF имеет ряд дополнительных возможностей, EIGRP более прост в реализации и менее требователен к вычислительным ресурсам маршрутизатора.

EIGRP-маршрутизатор обнаруживает своих соседей путем периодической рассылки сообщений "Hello". Эти же сообщения используются для мониторинга состояния связи с соседом (рассылаются каждые 5 секунд в сетях с большой пропускной способностью – например, Ethernet – и каждые 60 секунд в "медленных" сетях). Такой мониторинг позволяет рассылать в сети векторы расстояний не периодически, а только при изменении топологии сети.

EIGRP использует комплексное значение метрики, вычисляемое на основании показателей пропускной способности и задержки при передаче данных в сети. Также в расчет метрики могут быть включены показатели загрузки и надежности сети. В отличие от протокола RIP метрика в EIGRP не является фактором, ограничивающим размер системы.

При получении от соседей векторов расстояний, маршрутизатор для каждой сети назначения не только выбирает соседа, через которого лежит кратчайший путь в эту сеть, но также запоминает и вероятных заместителей (feasible successors). Вероятным заместителем становится маршрутизатор, объявивший метрику маршрута от себя до данной сети меньшую, чем полная метрика установленного маршрута. Рассмотрим пример на рис. 2 (для простоты метрики всех связей, кроме (4)-(5), считаем равными единице; метрика связи (4)-(5) равна 0,5).

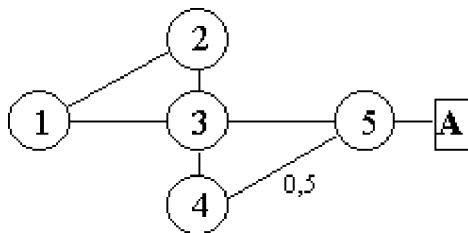


Рис 2. Пример EIGRP-системы

Кружками обозначены маршрутизаторы, прямоугольником – сеть назначения А. Маршрутизатор (3) получает от (5) элемент вектора расстояний ($A=1$), а от (4) – ($A=1,5$). В таблице маршрутизатора (3) узел (5) становится следующим

маршрутизатором на пути в сеть А, а узел (4) – вероятным заместителем, так как заявленное им расстояние до А (1,5) меньше полной метрики установленного маршрута (3)-(5)-А, которая равна 2.

Обратим внимание на маршрутизаторы (1) и (2). Они присылают узлу (3) элемент (А=3) и, следовательно, не являются вероятными заместителями маршрута из (3) в А, что, безусловно, разумно.

Если связь между узлами (3) и (5) обрывается, то (3) ищет в своей EIGRP-таблице вероятного заместителя ((4)) и немедленно устанавливает маршрут в сеть А через него. Таким образом время, в течение которого маршрут в сеть А отсутствовал, существенно сокращается по сравнению с протоколом RIP, где требуется ждать, когда соседи пришлют очередные векторы расстояний.

Если же ни одного вероятного заместителя не найдено (допустим, связь (3)-(4) тоже обрывается), то маршрутизатор переходит в активное состояние и начинает опрос всех своих соседей на предмет наличия маршрута в сеть А, сообщая при этом что его собственное расстояние до А равно бесконечности. Здесь вступает в работу алгоритм DUAL (Diffusing Update Algorithm). Следуя этому алгоритму, сосед отвечает на запрос только тогда, когда у него есть либо готовый маршрут в А, либо вероятный заместитель – в любом из этих случаев сосед присылает в узел (3) свое расстояние до А. Иначе сосед сам переходит в активное состояние и процесс повторяется (разумеется с той разницей, что к маршрутизатору (3) запрос не посылается; кроме того, маршрутизатор, находящийся в активном состоянии, сам может отвечать на запросы, посылая в ответ свое текущее значение расстояния до А). Таким образом область "активизированных" маршрутизаторов расширяется до тех пор, пока не будет обнаружен маршрут в сеть А или доказано его отсутствие, после чего волна сходится в обратном направлении к инициировавшему процесс узлу, при этом все маршрутизаторы вносят в свои таблицы надлежащие изменения.

В нашем простом примере, после того как (3) переходит в активное состояние, узлы (1) и (2) получают от него запрос о маршруте в сеть А с пометкой, что расстояние от (3) до А теперь равно бесконечности. Каждый из них, поскольку ранее он добирался в А через (3), помечает этот маршрут как недостижимый, и, не найдя вероятного заместителя, активизируется и опрашивает своего соседа. Получив эти запросы, (1) и (2) отвечают друг другу, что сеть А недостижима, переходят в пассивное состояние и возвращают узлу (3) информацию о недостижимости сети А.

Естественно, что подобная процедура (поиск вероятного заместителя, а при отсутствии такого – запуск алгоритма DUAL) происходит не только при обрыве связи, а также и в общем случае: если следующий маршрутизатор на пути в А прислал вектор, в котором расстояние до сети А увеличилось по сравнению с предыдущим сообщением от того же маршрутизатора.

В протоколе EIGRP также реализованы процедуры Split Horizon и Poison Reverse, которые выполняются не всегда, а в зависимости от состояния маршрутизатора и его соседей.

Из-за того, что EIGRP-маршрутизатор не просто принимает от соседей векторы расстояний, а строит на их основе некоторое представление от топологии

сети ("вероятные заместители"), контролирует состояние связи с соседями и использует алгоритм DUAL, что всё вместе напоминает протоколы состояния связей, Cisco классифицирует EIGRP как "гибридный" протокол.

2.2.1. Настройка протокола EIGRP

Настройка протокола EIGRP на роутерах Cisco производится аналогично настройке протокола RIP.

Из режима глобальной конфигурации необходимо выполнить команду

```
router eigrp <номер AC>
```

где номер AC – номер автономной системы.

Примечание. *Автономная система* - это система IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации с Интернет (RFC 1930).

Пример. Для настройки EIGRP в автономной системе 101 необходимо выполнить команду:

```
router eigrp 101
```

После выполнения данной команды роутер перейдет в режим настройки протокола маршрутизации и сменится приглашение командной строки:

```
Router(config-router)#
```

Из режима настройки протокола маршрутизации необходимо указать, как и при настройке RIP, непосредственно подключенные к роутеру сети. Делается это с помощью команды

```
network <адрес сети>
```

Пример. Если к роутеру подключена сеть 10.2.23.0, необходимо при настройке протокола eigrp выполнить следующую команду:

```
network 10.2.23.0
```

Как и при настройке RIP, маску подсети указывать не нужно. Роутер сам вычислит маску подсети, используя настройки интерфейса, к которому подключена данная сеть.

В случае если адреса указанных сетей можно выделить общую часть и просуммировать IP адреса (т.е. применить технологию CIDR), протокол EIGRP сделает это автоматически. Однако, в некоторых случаях, автосуммирование IP адресов не желательно, для отключения автосуммирования нужно выполнить команду

```
no auto-summary
```

После настройки протокола, на всех маршрутизаторах в AC, в таблице маршрутизации роутера появятся новые маршруты.

Для просмотра таблицы маршрутизации необходимо выполнить из привилегированного режима команду

```
show ip route
```

2.3. Протокол маршрутизации OSPF

Открытый протокол кратчайшего пути (Open Shortest Path First) предназначен для обмена информацией о маршрутизации в больших и очень больших объединенных сетях.

Основным преимуществом OSPF является его эффективность: даже в очень больших сетях OSPF мало загружает сеть своим трафиком. Самый существенный недостаток OSPF — его сложность: OSPF требует грамотного планирования и более сложен в настройке и администрировании.

Для вычисления маршрутов в таблице маршрутизации OSPF использует алгоритм выбора кратчайшего пути первым (SPF). Алгоритм SPF вычисляет кратчайший (имеющий наименьшую стоимость) путь между маршрутизатором и всеми сетями объединенной сети. Маршруты, вычисленные по алгоритму SPF, не могут быть циклическими.

Вместо того чтобы обмениваться записями таблиц маршрутизации, как это делают RIP-маршрутизаторы, OSPF-маршрутизаторы хранят схему объединенной сети, обновляя ее после каждого изменения топологии сети. Эта схема, называемая базой данных состояния связей, синхронизируется между всеми OSPF-маршрутизаторами и используется для вычисления маршрутов в таблице маршрутизации. Соседствующие OSPF-маршрутизаторы образуют соседство — логическую связь между маршрутизаторами для синхронизации базы данных состояния связей.

Изменения в топологии сети эффективно распространяются по всей объединенной сети, обеспечивая синхронизацию и соответствие действительности базы данных состояния связей на всех маршрутизаторах. При получении изменений базы данных состояния связей таблица маршрутизации пересчитывается.

По мере увеличения размера базы данных состояния связей увеличивается и требуемый объем памяти, а также время, необходимое для пересчета. Для решения этой проблемы масштабирования OSPF делит объединенную сеть на области (совокупности соединенных сетей), которые связаны друг с другом через магистральную область. Каждый маршрутизатор хранит базу данных состояния связей только для тех областей, которые к нему подключены. Маршрутизаторы на границах областей (ABR) связывают магистральную область с другими областями.

Для дальнейшего уменьшения количества перенаправляемых сведений в отдельных областях протокол OSPF предлагает использование изолированных областей. Изолированная область может содержать одну запись и точку выхода (один граничный маршрутизатор) или несколько граничных маршрутизаторов, когда любой граничный маршрутизатор может использоваться для достижения адреса назначения внешнего маршрута.

OSPF имеет следующие преимущества перед RIP:

- Маршруты, вычисленные OSPF, не могут быть циклическими.
- OSPF обеспечивает масштабируемость для больших и очень больших объединенных сетей.

- Более быстрая перенастройка при изменении топологии сети.

2.3.1. Настройка протокола OSPF

Для настройки протокола OSPF в бекбонной зоне или в зоне 0 необходимо выполнить следующие действия:

1. Из режима глобальной конфигурации выполнить команду

```
router ospf <ID процесса>
```

где ID процесса – номер процесса ospf, запущенного на роутере. При настройке протокола на маршрутизаторах в пределах одной зоны необходимо указывать одинаковый ID процесса.

Пример.

```
router ospf 1
```

2. В режиме настройки протокола маршрутизации необходимо перечислить все непосредственно подключенные к роутеру сети. Формат команды при этом отличается от формата, используемого при настройке протоколов RIP и EIGRP. Для указания подключенной сети необходимо выполнить команду:

```
network <адрес сети> <обратная маска> area <зона>
```

<обратная маска>, с точки зрения булевой алгебры является побитовым отрицанием обычной маски. В таблице 1 приведены примеры прямых масок и соответствующих им обратных. Так же как и прямая, обратная маска выделяет адрес сети и адрес хоста в IP адресе.

<зона> – это номер зоны в которой определяется протокол, бекбонная зона имеет номер 0.

Таблица 1.

Прямые и обратные маски

Прямая маска в десятичном виде	Прямая маска в двоичном виде	Обратная маска в двоичном виде	Обратная маска в десятичном виде
255.0.0.0 (8)	11111111.00000000.00000000.00000000	00000000.11111111.11111111.11111111	0.255.255.255
255.255.0.0 (16)	11111111.11111111.00000000.00000000	00000000.00000000.11111111.11111111	0.0.255.255
255.255.255.0 (24)	11111111.11111111.11111111.00000000	00000000.00000000.00000000.11111111	0.0.0.255
255.128.0.0 (9)	11111111.10000000.00000000.00000000	00000000.01111111.11111111.11111111	0.127.255.255
255.248.0.0 (13)	11111111.11111000.00000000.00000000	00000000.00000111.11111111.11111111	0.7.255.255
255.255.192.0 (18)	11111111.11111111.11000000.00000000	00000000.00000000.00111111.11111111	0.0.63.255
255.255.255.224 (27)	11111111.11111111.11111111.11100000	00000000.00000000.00000000.00011111	0.0.0.31
255.255.255.252 (30)	11111111.11111111.11111111.11111100	00000000.00000000.00000000.00000011	0.0.0.3

Пример. К роутеру непосредственно подключены сети 193.161.13.64/27 и 193.161.13.100/30, обе сети относятся к бекбонной зоне, то есть к зоне 0. Для

настройки протокола OSPF необходимо в режиме настройки протокола маршрутизации выполнить следующие две команды:

```
network 193.161.13.64 0.0.0.31 area 0
network 193.161.13.100 0.0.0.3 area 0
```

После настройки протокола OSPF на всех роутерах внутри одной зоны в таблице маршрутизации появятся новые маршруты, вычисленные протоколом.

2.4. Замена одного протокола маршрутизации другим

Зачастую возникает ситуация, когда требуется сменить протокол динамической маршрутизации, но при этом сеть должна работать. Конечно, можно прописать вручную временные статические маршруты, но это займет слишком много времени. Существует механизм замены одного протокола другим.

Рассмотрим это на примере. Допустим, в сети работает протокол RIP, нам надо заменить его протоколом EIGRP. Считая сеть единой автономной системой, на всех роутерах настраивается и запускается протокол EIGRP. При этом RIP продолжает работать. После того как в пределах автономной системы везде настроен и запущен EIGRP, отключаем протокол RIP с помощью команды

```
no router rip
```

Данную команду выполняем на всех маршрутизаторах, где запущен RIP.

После всех этих действий в сети будет работать протокол маршрутизации EIGRP. Таким же образом можно сменить RIP на OSPF, или EIGRP на OSPF.

Почему такое возможно? Дело в том, что каждый маршрут в таблице маршрутизации роутера имеет некоторые характеристики. Помимо метрики, которая определяет качество самого маршрута, есть характеристика, называемая административной дистанцией (АД). Именно с помощью АД роутер выбирает маршрут. АД это степень доверия роутера маршруту. Чем меньше значение АД – тем больше доверия. Естественно минимальную АД имеют маршруты к непосредственно подключенным сетям (АД = 0). Далее следуют статические маршруты, прописанные администратором (АД = 1). Протокол EIGRP имеет АД равное 90, OSPF – 110, RIP – 120.

Таким образом если в таблице маршрутизации находится несколько маршрутов до одной и той же сети, но с разными значениями АД, роутер выберет маршрут с минимальной АД.

Примечание 1. При необходимости административную дистанцию протокола динамической маршрутизации можно поменять вручную.

Примечание 2. Приведенные числовые данные административных дистанций являются значениями по умолчанию для маршрутизаторов фирмы Cisco.

3. Фильтрация пользовательского трафика

Маршрутизатор – пограничное устройство, соединяющее сеть с внешним миром. Поэтому на него возлагают **функции защиты сети от внешних атак с помощью фильтрации пользовательского трафика** в соответствии с различными признаками: адресами отправителя и получателя, типа протокола, типа приложения, генерирующего трафик и т.п.

Под **фильтрацией** понимается нестандартная обработка IP-пакетов, приводящая к отбрасыванию некоторых пакетов или изменению их маршрута.

Типичные условия фильтрации в маршрутизаторах:

- IP-адрес отправителя и получателя.
- MAC-адрес отправителя и получателя.
- Идентификатор интерфейса с которого поступил пакет.
- Тип протокола, сообщение которого несет IP-пакет (TCP, UDP, ICMP, HTTP, OSPF).

При наличии фильтра маршрутизатор сначала **сравнивает условия фильтрации с признаками пакета** и при их **совпадении** выполняет предписанные действия, например:

- **отбрасывает** пакет (drop),
- **изменяет** его маршрут,
- **помечает** как вероятного кандидата на удаление при возникновении перегрузки.

3.1. Списки доступа (Access Control List, ACL)

Access control lists (ACL) - списки доступа широко используются современными маршрутизаторами, не ограничивающимися простой проверкой адресов и продвижением пакетов. Сейчас они выполняют инкапсуляцию, туннелирование, преобразование протоколов, действия по обеспечению некоторой безопасности.

Разнообразие каналов связи, увеличивающееся использование сети Интернет и появление, наряду с данными, передачи голоса, видео - все это приводит к усложнению проходящего через маршрутизатор трафика.

Проблемы безопасности, балансировки нагрузки и распределения трафика по приоритетам поставили вопрос о необходимости фильтрации пакетов.

В итоге для этого стали применяться списки доступа различных типов. С их помощью маршрутизатор не становится полнофункциональным межсетевым экраном (для этого он должен уметь не только анализировать трафик, но и менять свои параметры в соответствии с накопленной статистикой трафика).

Список доступа - это упорядоченный набор операторов, каждый из которых разрешает или запрещает прохождение пакета через интерфейс.

Операторы списка доступа применяются к каждому пакету последовательно, начиная с первого, до тех пор, пока не будет найдено соответствие или достигнут конец списка. При первом же совпадении маршрутизатор определяет, сбросить пакет или принять его.

Поскольку после первого же совпадения прекращается проверка условий, то их порядок следования имеет важное значение. Поместив в начало списка наибо-

лее часто встречающиеся условия, можно **существенно снизить нагрузку на маршрутизатор**.

Кроме фильтрации пакетов, списки доступа применяются для выделения трафика определенных хостов при его передаче по защищенному туннелю через Интернет, для перенаправления трафика по другому маршруту, для фильтрации изменений в таблицах маршрутизации, для управления доступом к виртуальным терминалам.

Списки доступа могут применяться **на входе** в маршрутизатор и на его **выходе**.

В **первом** случае сначала выполняется проверка пакета, а затем, если он пропускается, - его маршрутизация. При сбросе пакета (drop) по адресу его отправителя посылается ICMP-сообщение "хост недоступен" (host unreachable).

Во **втором** случае пакет сначала маршрутизируется и только потом его параметры сравниваются с условиями списка.

3.2. Списки доступа в маршрутизаторах Cisco

В качестве типичного примера рассмотрим синтаксис списков доступа, разработанный компанией **Cisco Systems** для операционной системы **Cisco IOS**.

Списки доступа (access-list) позволяют управлять прохождением трафика через интерфейсы роутера, разрешая или запрещая передачу пакетов, удовлетворяющих указанным условиям. Списки доступа задают условия, которые роутер проверяет перед выполнением каких-либо действий.

Важнейшие области использования списков доступа:

- Управление передачей пакетов на интерфейсах.
- Управление доступом к виртуальным терминалам роутера и управлению через SNMP.
- Ограничение информации, передаваемой протоколами маршрутизации.

Cisco IOS поддерживает несколько видов списков доступа для протокола IP:

- **Стандартные** списки доступа (проверяют адрес отправителя пакета).
- **Расширенные** списки доступа (проверяют адрес отправителя, адрес получателя и еще ряд параметров пакета).
- **Динамические** расширенные списки доступа (имеют конечное «время жизни» и условия применения).

Списки доступа либо **нумеруются**, либо **именуются**. Использование нумерованных, либо именованных списков доступа определяется областью их применения (некоторые протоколы требуют использования только нумерованных списков, некоторые - допускают как именованные, так и нумерованные списки).

Если используются нумерованные списки, то номера их должны лежать в определенных диапазонах, в зависимости от области применения списка (см. таблицу 2).

Таблица 2.

**Диапазоны номеров, используемые при создании списков доступа
в маршрутизаторах Cisco Systems**

Протокол	Диапазон номеров
Стандартный IP	1-99 1300-1999 (с версии IOS 12.0)
Расширенный IP	100-199 2000-2699 (с версии IOS 12.0)
Коды Ethernet-type, алгоритм прозрачного моста (по типу протокола), алгоритм моста с маршрутизацией от источника (по типу протокола)*	200-299
DECnet и расширенный DECnet	300-399
XNS	400-499
Расширенный XNS	500-599
Apple Talk	600-699
Ethernet-адреса (MAC-адреса), алгоритм прозрачного моста (по коду производителя), алгоритм моста с маршрутизацией от источника (по коду производителя)*	700-799
IPX	800-899
Расширенный IPX	900-999
IPX SAP	1000-1099
Расширенный алгоритм прозрачного моста	1100-1199

* - В случае фильтрации пакетов на канальном уровне при назначении списка доступа интерфейсу вместо команды `access-group` используется команда `bridge-group`.

Задачи и правила построения списков доступа для различных протоколов различны, но, в общем, можно выделить **два этапа** работы с любыми списками доступа:

1. Сначала, необходимо **создать список доступа**.
2. Затем **применить** его к соответствующему **интерфейсу**, линии или логической операции, выполняемой роутером.

3.3. Создание стандартных списков доступа для протокола IP

Стандартный список доступа имеет ограниченные функциональные возможности: позволяет фильтровать пакеты только по адресу источника. Имеет следующий (базовый) формат (задается из режима глобальной конфигурации, то есть перед командой должен быть промпт: `Router(config)#`):

```
access-list access-list-number {deny | permit} {source-address [source-wildcard] | any} [log]
```

Жирным шрифтом выделены параметры оператора, которые вносятся в список в неизменном виде, а обычным шрифтом - которые заменяются символьными или числовыми значениями. В фигурных скобках находятся два параметра, один из которых обязательно должен присутствовать в операторе. Параметры, заключенные в квадратные скобки, необязательны.

Параметры стандартного списка доступа:

`Access-list-number` (номер списка) - это число от 1 до 99 (стандартный список доступа протокола IP). Начиная с версии IOS 12.0 для номера стандартного списка IP доступен интервал 1300-1999. Для фильтрации пакетов по 48-битным MAC-адресам используются числа из диапазона 700-799 (см. Таблицу 2).

Параметры `permit` или `deny` указывают, разрешается ли пакетам, удовлетворяющим условиям некоторого оператора списка, проходить через интерфейс. `Permit` - разрешить, `deny` - отказать.

`Source-address` (адрес источника) - это IP-адрес узла или группы узлов. Его задание осуществляется с использованием маски шаблона (`source-wildcard`). Действие этой маски противоположно по сравнению с маской подсети (`subnet mask`): двоичный нуль предполагает строгое совпадение в соответствующей позиции, а двоичная единица означает произвольное значение. Попросту: `source-wildcard` - это инвертированная маска подсети.

Ключевое слово `log` задает ведение журнала.

Примеры стандартных списков доступа (все команды вводятся в режиме глобальной конфигурации маршрутизатора `Router(config)#`):

1. Разрешение прохождения через маршрутизатор пакетов от всех хостов сети класса C - 140.12.11.0:

```
access-list 1 permit 140.12.11.0 0.0.0.255
```

2. Запрещение прохождения через маршрутизатор пакетов от всех хостов сети класса C - 140.12.11.0:

```
access-list 1 deny 140.12.11.0 0.0.0.255
```

3. Разрешение прохождения через маршрутизатор пакетов хоста с IP-адресом 140.12.11.5:

```
access-list 1 permit 140.12.11.5 0.0.0.0
```

или

```
access-list 1 permit host 140.12.11.5
```

4. Запрещение прохождения через маршрутизатор пакетов хоста с IP-адресом 140.12.11.5:

```
access-list 1 deny 140.12.11.5 0.0.0.0
```

5. Создадим стандартный список доступа с номером 1, который будет разрешать прохождение пакетов от конкретного хоста 193.161.13.14 и из сети 193.161.13.32/27, а все остальные пакеты будет отбрасывать. Выполним последовательно следующие команды:

```
access-list 1 permit host 193.161.13.14
```

```
access-list 1 permit 193.161.13.32 0.0.0.31
```

По умолчанию каждый список доступа в конце содержит неявный оператор `deny any`, который отсеивает весь трафик, кроме явно разрешенного, то есть:

```
access-list 1 deny any
```

3.4. Создание расширенных списков доступа для протокола IP

Расширенный список доступа обеспечивает более гибкую фильтрацию пакетов. Он позволяет отбирать пакеты по адресу источника и по адресу назначения, а также по протоколу, порту источника, порту назначения и даже по значению разрядов в некоторых полях внутри пакета.

Расширенный список доступа имеет следующий (базовый) формат (задается из режима глобальной конфигурации, то есть перед командой должен быть промпт: Router(config)#):

```
access-list access-list-number {deny | permit} {protocol |  
protocol-keyword}  
{source-address [source-wildcard] | any}  
[destination-address [destination-wildcard] | any]  
[precedence precedence] [tos tos] [established] [log]
```

Параметры расширенного списка доступа:

Access-list-number (номер списка) - число от 100 до 199, идентифицирующее операторы из расширенного списка доступа IP. Начиная с версии IOS 12.0 для номера списка доступен интервал 2000-2699.

Protocol-keyword задает протокол, подлежащий фильтрации, например, IP, TCP, UDP, ICMP и т.д.

Поддерживаются логические операции применительно к номерам портов (или другим параметрам): lt (less than - меньше), gt (greater than - больше), eq (equal - равно), neq (not equal - не равно).

Чтобы задать порт источника - source-port или порт назначения - destination-port, можно указать номер или мнемонический код порта, либо использовать логическую операцию для задания диапазона портов.

Примеры расширенных списков доступа:

1. Пример иллюстрирует использование логических операций:

```
access-list 101 permit TCP any host 140.12.11.10 eq WWW  
access-list 101 permit ICMP any host 140.12.11.10 eq 8
```

Первый оператор разрешает передачу пакетов TCP с любого узла по адресу 140.12.11.10, если эти пакеты принадлежат типу Web. Вместо мнемонического кода WWW можно задать число 80, так как трафик Web обычно использует порт 80. Второй оператор разрешает все адресованные указанному узлу сообщения ping (эхо запросы ICMP), которым назначен тип ICMP, равный 8. Синтаксис расширенных списков доступа позволяет задавать в конце оператора специфические для каждого протокола параметры; так, для протокола ICMP задаются не номера портов, как для протоколов UDP или TCP, а тип и если нужно - код сообщений ICMP. С учетом неявного оператора deny any в конце списка доступа весь остальной трафик (абсолютно весь) будет блокироваться.

2. В следующем примере создадим расширенный список доступа, который будет пропускать все пакеты, полученные от провайдера (адрес 112.24.11.109) по протоколу WWW (порт 80) независимо от их получателя, запрещать пакеты, идущие из сети 193.161.13.0/27 в сеть 193.161.13.64/27 с номерами портов большими, чем 1024, и запрещать пинговать хост 193.161.13.67 из сети 193.161.13.32. Все остальные пакеты должны беспрепятственно проходить. Для этого выполним последовательно следующие команды:

```
access-list 102 permit tcp host 112.24.11.109 any eq 80
access-list 102 deny tcp 193.161.13.0 0.0.0.31
193.161.13.64 0.0.0.31 gt 1024
access-list 102 deny icmp 193.161.13.32 0.0.0.31 host
193.161.13.67
access-list 102 permit ip any
```

Внимание! В конце каждого списка стоит неявное правило "deny any", поэтому нужно **явно разрешить** все виды необходимого трафика (см. последнюю строчку последнего примера), причем не только пользовательского, но и служебного, например, обмен информацией по протоколам динамической маршрутизации.

3.5. Назначение списков доступа на интерфейсы

Ошибкой многих начинающих (и не только) администраторов является то, что после создания списка доступа его просто "забывают" связать с каким-либо интерфейсом маршрутизатора. Список же начинает действовать только после связи его с интерфейсом.

К каждому интерфейсу можно «привязать» стандартный и/или расширенный списки доступа, которые могут быть или **inbound (in)** - проверяется когда пакет поступает на вход интерфейса снаружи, или **outbound (out)** - проверка происходит, когда пакет приходит изнутри маршрутизатора на интерфейс. Таким образом, всего можно назначить **4 списка доступа на каждый интерфейс**.

Для назначения списка доступа на интерфейс необходимо из режима настройки этого интерфейса выполнить команду:

```
ip access-group <номер списка> <направление>
```

где <номер списка> – номер применяемого на интерфейсе списка доступа;

<направление> – направление проверяемого трафика входящий (in) или исходящий (out).

То есть, для назначения стандартного списка доступа с номером 1 на интерфейс Ethernet 0/0, чтобы проверялся входящий трафик (in), нужно выполнить следующие команды:

```
Router# configure terminal
Router(config)# interface ethernet 0/0
```

```
Router(config-if)# ip access-group 1 in
```

Еще один пример. Назначим на интерфейс serial 0/0 для проверки выходного (out) трафика созданный ранее расширенный список доступа с номером 102. Для этого выполним команды:

```
Router# configure terminal
```

```
Router(config)# interface serial 0/0
```

```
Router(config-if)# ip access-group 102 out
```

Для удаления списка доступа из памяти маршрутизатора необходимо из режима глобальной конфигурации выполнить команду:

```
no access-list <номер списка>
```

Для удаления привязки списка доступа к интерфейсу нужно из режима настройки интерфейса, к которому привязан список, выполнить команду:

```
no ip access-group <номер списка> <направление>
```

Замечание. Cisco рекомендует:

Стандартные списки доступа следует размещать как можно ближе к пункту назначения.

Расширенные списки доступа следует размещать как можно ближе к источнику.

В заключение, другие рекомендации по конфигурированию и применению списков доступа:

1) использовать стандартный список доступа IP при фильтрации только по адресу источника;

2) в начало списка помещать наиболее часто встречающиеся условия для снижения нагрузки на роутер;

3) уделить внимание порядку следования операторов в списке доступа для исключения ошибок;

4) всегда применять список доступа к соответствующему интерфейсу и направлению фильтрации трафика;

5) список доступа отсеивает весь трафик, кроме явно разрешенного;

6) при составлении маски шаблона - двоичные нули означают совпадение, а двоичные единицы - произвольные символы;

7) операторы с более конкретными спецификациями всегда следует ставить перед операторами общего характера (для фильтрации по протоколу);

8) обращать внимание на правильность направления фильтрации трафика - "откуда-куда" местоположением оператора any.

**Список контрольных вопросов
к лабораторной работе
Динамическая маршрутизация и списки доступа**

1. Структура системы команд Cisco IOS.
2. Команды привилегированного режима системы команд Cisco IOS.
3. Команды режима глобальной конфигурации системы команд Cisco IOS.
4. Команды режима настройки интерфейсов системы команд Cisco IOS.
5. Настройка статической маршрутизации в Cisco IOS.
6. Протокол динамической маршрутизации Cisco RIP.
7. Настройка протокола RIP.
8. Протокол маршрутизации Cisco EIGRP.
9. Настройка протокола EIGRP.
10. Протокол маршрутизации OSPF.
11. Настройка протокола OSPF.
12. Как заменить один протокол маршрутизации другим?

**ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ОТЧЕТА
ПО ЛАБОРАТОРНОЙ РАБОТЕ**

Отчет по лабораторной работе должен содержать:

1. Титульный лист (см. образец).
2. Перечень выполненных заданий (с указанием адресной информации, команд и их параметров – в зависимости от содержания пункта задания).
3. Письменный ответ на указанный преподавателем контрольный вопрос.

Отчет предоставляется преподавателю в электронной форме, в формате MS Word (шаблон названия файла: **ктк_ЛР_№_группа_фамилия.doc**).

Образец титульного листа отчета

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Самарский государственный аэрокосмический университет
имени академика С.П. Королева
(национальный исследовательский университет)»

Факультет информатики
Кафедра технической кибернетики

ОТЧЕТ

по лабораторной работе по дисциплине
Компьютерные телекоммуникации
на тему

Динамическая маршрутизация и списки доступа

Выполнил студент 63Х группы Фамилия И.О.

ПОРЯДОК ВЫПОЛНЕНИЯ ЛАБОРАТОРНОЙ РАБОТЫ

Динамическая маршрутизация и списки доступа

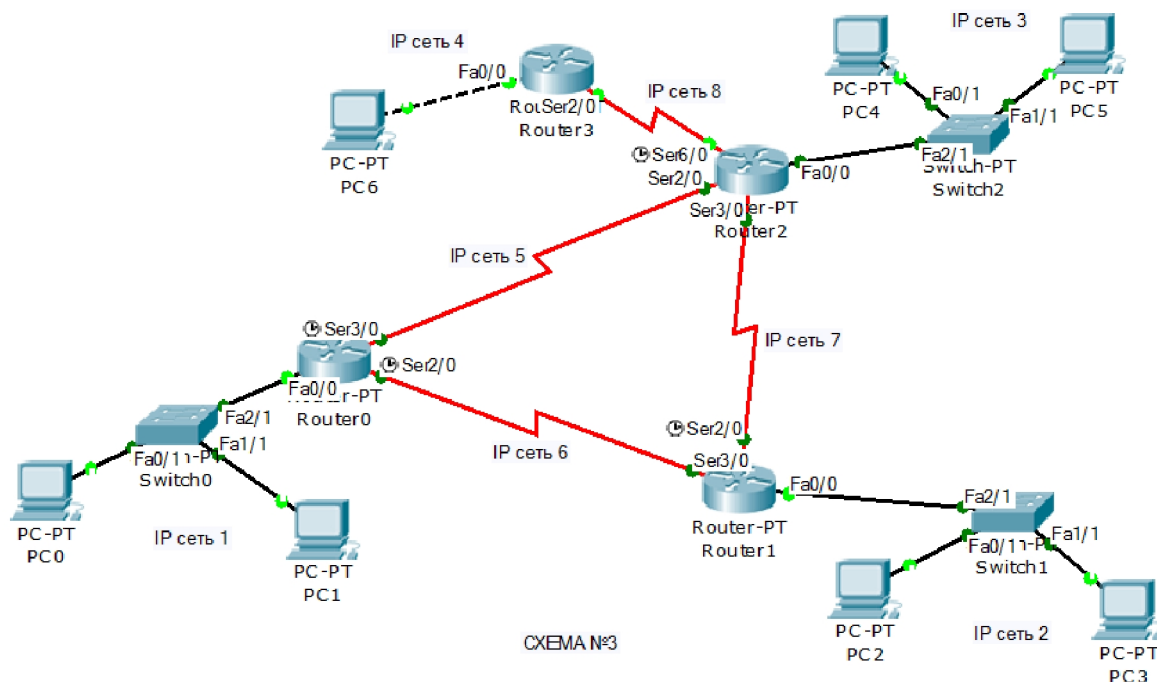
Изучаемый материал: *Настройка активного сетевого оборудования Cisco. Система команд Cisco IOS. Статическая и динамическая маршрутизация. Протоколы динамической маршрутизации RIP, EIGRP и OSPF. Списки доступа. Построение заданной сети в среде PacketTracer.*

1. В среде эмулятора PacketTracer создать сеть со структурой и настройками, показанными на рисунке, полученного варианта задания. Включить в PacketTracer-е режим отображения имен портов: Ctrl-R + галку “Port labels always shown”. Если не оговорено иное, при выборе хостов, коммутаторов и маршрутизаторов использовать Generic-устройства. **Не используйте** автоматический выбор типа кабеля («оранжевая молния» слева). Serial интерфейсы должны соединяться «красной молнией с часами» (Serial DCE), начиная со стороны, отмеченной на схеме DCE («часики»). В маршрутизаторе Router2 не хватает одного модуля с одним Serial интерфейсом, чтобы его добавить надо: «левый клик на маршрутизаторе», закладка Physical, выключить питание, добавить правильный модуль (PT-ROUTER-NM-1S), затем включить питание.
2. Настроить интерфейсы маршрутизаторов, т.е. для каждого задействованного Fast Ethernet и Serial интерфейса указать IP адрес, маску и включить его. Для Serial интерфейсов включить частоту синхронизации (clock rate = 64000) на стороне, отмеченной на схеме DCE («часики») (рис. 1).
3. Настроить оконечные устройства (хосты): в соответствии с номером сети, заданном на схеме, задать IP адрес, маску и адрес шлюза по умолчанию (default gateway).
4. Проверить работоспособность **отдельных** (периферийных) подсетей с помощью команды ping (быстрая проверка в RealTime mode). **Контрольная точка 1.**

5. Настроить статическую маршрутизацию между двумя указанными в соответствующем варианте IP сетями. Выполнить задание поэтапно: сначала прописать статический маршрут в одну сторону: от сети-отправителя к сети-получателю. Проверить наличие маршрута в таблице маршрутизации соответствующего роутера.
6. Протестировать маршрут до одного из хостов IP сети - получателя, выполнив команду `tracert` с одного из хостов IP сети - отправителя. Уметь пояснить, какую информацию и почему выводит на экран консоли команда `tracert`.
7. Перевести PacketTracer из режима RealTime в режим Simulation. В панели управления выбрать только ICMP пакеты. Проследить прохождение маршрута ICMP пакетами до одного из хостов IP сети - получателя, выполнив команду `ping` с одного из хостов IP сети - отправителя. Уметь пояснить, почему ICMP пакет перемещается именно так. Ответить на вопрос, почему нет связи с пингуемым хостом?
8. Затем добавить статический маршрут в обратную сторону: от сети-получателя к сети-отправителю. Проверить наличие маршрута в таблице маршрутизации соответствующего роутера.
9. Повторить действия пунктов 6 и 7. **Контрольная точка 2.**
10. Удалить статический маршрут.
11. На всех роутерах настроить и запустить протокол динамической маршрутизации RIPv2. Команда **version 2** выполняется только из командной строки («левый клик на маршрутизаторе», закладка CLI).
12. Проверить, что бы в таблицах маршрутизации появились маршруты, проложенные протоколом RIPv2.
13. Проверить (только после настройки RIPv2 на всех маршрутизаторах) работоспособность **всей сети в целом** с помощью команды `ping` (быстрая проверка в RealTime mode). Уметь читать таблицы маршрутизации и интерпретировать считанную информацию. **Контрольная точка 3.**

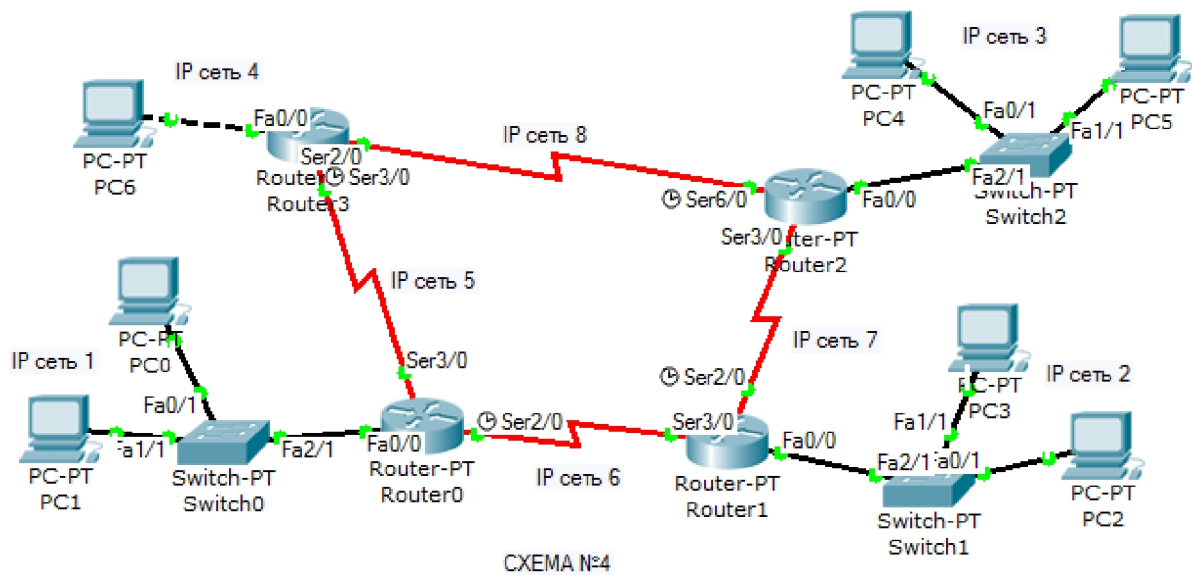
16. Настроить на всех маршрутизаторах один из протоколов динамической маршрутизации (EIGRP/OSPF – в зависимости от варианта задания).
17. Проверить, чтобы в таблицах маршрутизации появились маршруты, проложенные настроенным протоколом.
18. Отключить протокол маршрутизации RIP.
19. Проверить (только после настройки всех маршрутизаторов) работоспособность **всей сети в целом** с помощью команд ping (быстрая проверка в RealTime mode) и tracer. Уметь читать таблицы маршрутизации и интерпретировать считанную информацию. **Контрольная точка 4.**
20. Создать и применить на «правильные» интерфейсы один стандартный и один расширенный списки доступа.
21. Стандартный список доступа: запрещает прохождение пакетов, идущих от конкретного хоста IP сети 2 в IP сеть 1.
22. Расширенный список доступа: запрещает прохождение ICMP пакетов, идущих из IP сети 2 к конкретному хосту IP сети 3.
23. Назначить на правильные интерфейсы (см. рекомендации).
24. Проверить правильность работы списков доступа. **Контрольная точка 5.**
25. Оформить отчет о лабораторной работе. Представить его преподавателю в электронной форме. Ответить, если необходимо, на вопросы. Получить зачет по лабораторной работе.

Варианты 1 и 2



IP сеть №	Вариант 1	Вариант 2
IP сеть 1	132.201.5.0/27	205.13.10.0/28
IP сеть 2	132.201.5.32/27	205.13.10.16/28
IP сеть 3	132.201.5.64/27	205.13.10.32/28
IP сеть 4	5.118.15.0/26	153.67.9.0/27
IP сеть 5	132.201.5.96/30	205.13.10.48/30
IP сеть 6	132.201.5.100/30	205.13.10.52/30
IP сеть 7	132.201.5.104/30	205.13.10.56/30
IP сеть 8	5.118.15.64/30	153.67.9.32/30
Статические маршруты	IP сеть 1 ↔ IP сеть 3	IP сеть 2 ↔ IP сеть 4
Протокол динамической маршрутизации	EIGRP	OSPF

Варианты 3 и 4



IP сеть №	Вариант 3	Вариант 4
IP сеть 1	208.13.10.0/28	188.100.33.0/27
IP сеть 2	208.13.10.16/28	188.100.33.32/27
IP сеть 3	208.13.10.32/28	188.100.33.64/27
IP сеть 4	130.17.89.0/27	135.78.12.0/26
IP сеть 5	208.13.10.48/30	188.100.33.96/30
IP сеть 6	208.13.10.52/30	188.100.33.100/30
IP сеть 7	208.13.10.56/30	188.100.33.104/30
IP сеть 8	130.17.89.32/30	135.78.12.64/30
Статические маршруты	IP сеть 1 ↔ IP сеть 3	IP сеть 2 ↔ IP сеть 4
Протокол динамической маршрутизации	EIGRP	OSPF

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Самарский государственный аэрокосмический университет
имени академика С.П. Королева
(национальный исследовательский университет)»

Факультет информатики
Кафедра технической кибернетики

Беспроводные сети Wi-Fi

**Методические указания к лабораторной работе
по курсу компьютерные телекоммуникации**

САМАРА 2011

ОГЛАВЛЕНИЕ

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ	3
1. Общая характеристика беспроводных сетей.....	4
1.1. Основные элементы беспроводной сети	4
2. Стандарты IEEE 802.11	5
2.1. Стандарт IEEE 802.11g	7
3. Режимы работы устройств в беспроводной сети и особенности их организации	8
3.1. Режим Ad Hoc	8
3.2. Инфраструктурный режим	9
3.3. Режимы WDS и WDS with AP	13
3.4. Режим клиента	16
4. Организация и планирование беспроводных сетей	16
4.1. Офисная сеть.....	17
4.2. Сеть между несколькими офисами.....	20
5. Аутентификация в беспроводных сетях	21
5.1. Стандарт IEEE 802.11 сети с традиционной безопасностью	21
5.2. Спецификация WPA.....	24
5.3. Стандарт сети 802.11i с повышенной безопасностью (WPA2).....	25
5.4. Стандарт 802.1x/EAP (Enterprise-режим).....	27
Список контрольных вопросов	30
ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ОТЧЕТА.....	30

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Изучаемый материал: *основные виды беспроводного оборудования; физические и технические вопросы реализации протоколов беспроводных сетей 802.11; режимы работы беспроводной сети (Ad Hoc, инфраструктурный, мост, распределенный мост) и соответствующие топологии; настройка основных параметров беспроводного оборудования; безопасность беспроводных сетей: протоколы шифрования и аутентификации (IEEE 802.1, WEP, WPA, WPA2); настройка параметров протоколов шифрования и аутентификации для построения защищенной беспроводной сети.*

1. Изучить теоретическую часть.
2. Разбиться на 3 группы, получить у преподавателя набор сетевого оборудования (точки доступа, USB сетевые адаптеры) и описание конфигураций сетей, подлежащих построению и изучению.
3. Установить беспроводные USB-адаптеры, установить (если необходимо) драйверы устройств. Подключить точки доступа. Ввести основные настройки в соответствии с заданными конфигурациями сети.
4. **Изучение инфраструктурного режима работы точки доступа.**
 - a. Построить три изолированные беспроводные сети, точки доступа которых работают в режиме AP на непересекающихся частотных каналах. Проверить работоспособность этих сетей, исследовать их работу с помощью программы **InSSIDer**.
 - b. Объединить точки доступа изолированных сетей, используя проводное соединение (LAN) с коммутатором, создав единую локальную (и IP) сеть. Добавить проводные клиенты. Проверить работоспособность полученной смешанной (беспроводной – проводной) локальной сети, исследовать ее работу с помощью программы **InSSIDer**.
 - c. Настроить шифрование и аутентификацию (**WPA2-PSK**) на точках доступа и беспроводных клиентах.
5. **Изучение работы точки доступа в режимах распределенного моста / распределенного моста с точкой доступа (WDS / WDS with AP).**
 - a. Используя два проводных коммутатора Cisco Catalyst 2960 и один концентратор (хаб) построить три изолированные (проводные) сети. Используя три точки доступа, которые работают в режиме WDS на едином частотном канале, объединить локальные сети беспроводным (Wi-Fi) мостом. Проверить работоспособность полученной смешанной (беспроводной – проводной) локальной сети, исследовать ее работу с помощью программы **InSSIDer**.
 - b. Переключить две из трех точек доступа в режим **WDS with AP**. Добавить в полученную сеть беспроводные клиенты. Проверить работоспособность полученной смешанной (беспроводной – проводной) локальной сети, исследовать ее работу с помощью программы **InSSIDer**.
 - c. Настроить шифрование и аутентификацию (**WPA2-PSK**) на точках доступа и беспроводных клиентах.
6. Каждой подгруппе данные, собранные при выполнении пунктов задания 3, 4, 5, занести в отчет по форме выданной преподавателем (форма отчета - в файле `СТС_Lab_wifi_report.doc`). Начертить (с использованием обозначений, принятых в системе PacketTracer) схемы локальных сетей, реализованных подгруппой, отразить на схеме все сетевые настройки.

1. Общая характеристика беспроводных сетей

WI-FI - это современная беспроводная технология соединения компьютеров в локальную сеть и подключения их к Internet. Благодаря этой технологии Internet становится мобильным и дает пользователю свободу перемещения не то что в пределах комнаты, но и по всему миру.

Под аббревиатурой "Wi-Fi" (от английского словосочетания "Wireless Fidelity", которое можно дословно перевести как "высокая точность беспроводной передачи данных") в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам.

С увеличением числа мобильных пользователей возникает острая необходимость в оперативном создании коммуникаций между ними, в обмене данными, в быстром получении информации. Поэтому естественным образом происходит интенсивное развитие технологий беспроводных коммуникаций. Особенно это актуально в отношении беспроводных сетей, или так называемых WLAN-сетей (Wireless Local Area Network). Сети Wireless LAN - это беспроводные локальные сети (вместо обычных проводов в них используются радиоволны). Установка таких сетей рекомендуется там, где развертывание кабельной системы невозможно или экономически нецелесообразно.

Беспроводные сети особенно эффективны на предприятиях, где сотрудники активно перемещаются по территории во время рабочего дня с целью обслуживания клиентов или сбора информации (крупные склады, агентства, офисы продаж, учреждения здравоохранения и др.).

Благодаря функции роуминга между точками доступа пользователи могут перемещаться по территории покрытия сети Wi-Fi без разрыва соединения.

WLAN-сети имеют ряд преимуществ перед обычными кабельными сетями:

- WLAN-сеть можно очень быстро развернуть, что очень удобно при проведении презентаций или в условиях работы вне офиса;
- пользователи мобильных устройств при подключении к локальным беспроводным сетям могут легко перемещаться в рамках действующих зон сети;
- скорость современных сетей довольно высока (теоретически - до 300 Мб/с), что позволяет использовать их для решения очень широкого спектра задач;
- WLAN-сеть может оказаться единственным выходом, если невозможна прокладка кабеля для обычной сети.

Вместе с тем необходимо помнить об ограничениях беспроводных сетей. Это, как правило, все-таки меньшая скорость, подверженность влиянию помех и более сложная схема обеспечения безопасности передаваемой информации.

Сегмент Wi-Fi сети может использоваться как самостоятельная сеть, либо в составе более сложной сети, содержащей как беспроводные, так и обычные проводные сегменты. Wi-Fi сеть может использоваться:

- для беспроводного подключения пользователей к сети;
- для объединения пространственно разнесенных подсетей в одну общую сеть там, где кабельное соединение подсетей невозможно или нежелательно;
- для подключения к сетям провайдера Internet-услуги вместо использования выделенной проводной линии или обычного модемного соединения.

1.1. Основные элементы беспроводной сети

Для построения беспроводной сети используются Wi-Fi адаптеры и точки доступа.

Адаптер (рис. 1.1) представляет собой устройство, которое подключается через слот расширения PCI, PCMCIA, CompactFlash. Существуют также адаптеры с подключением через порт USB 2.0. Wi-Fi адаптер выполняет ту же функцию, что и сетевая карта в проводной сети. Он служит для подключения компьютера пользователя к беспроводной сети. Благодаря платформе Centrino все современные ноутбуки имеют встроенные адаптеры Wi-Fi, совместимые со многими современными стандартами. Wi-Fi адаптерами, как правило, снабжены и КПК (карманные персональные компьютеры), что также позволяет подключать их к беспроводным сетям.

Для доступа к беспроводной сети адаптер может устанавливать связь непосредственно с другими адаптерами. Такая сеть называется *беспроводной одноранговой сетью* или *Ad Hoc* ("к случаю"). Адаптер также может устанавливать связь через специальное устройство - *точку доступа*. Такой режим называется *инфраструктурой*.

Для выбора способа подключения адаптер должен быть настроен на использование либо Ad Hoc, либо инфраструктурного режима.

Точка доступа (рис. 1.2) представляет собой автономный модуль со встроенным микрокомпьютером и приемно-передающим устройством.



Рис. 1.1. Wi-Fi адаптеры

Через точку доступа осуществляется взаимодействие и обмен информацией между беспроводными адаптерами, а также связь с проводным сегментом сети. Таким образом, точка доступа играет роль коммутатора.



Рис. 1.2. Точка доступа

Точка доступа имеет сетевой интерфейс (uplink port), при помощи которого она может быть подключена к обычной проводной сети. Через этот же интерфейс может осуществляться и настройка точки.

Точка доступа может использоваться как для подключения к ней клиентов (базовый режим точки доступа), так и для взаимодействия с другими точками доступа с целью построения распределенной сети (Wireless Distributed System - WDS). Это режимы беспроводного моста "точка-точка" и "точка - много точек", беспроводный клиент и повторитель.

Доступ к сети обеспечивается путем передачи широкополосных сигналов через эфир. Принимающая станция может получать сигналы в диапазоне работы нескольких передающих станций. Станция-приемник использует идентификатор зоны обслуживания (Service Set Identifier - SSID) для фильтрации получаемых сигналов и выделения того, который ей нужен.

Зоной обслуживания (Service Set - SS) называются логически сгруппированные устройства, обеспечивающие подключение к беспроводной сети.

Базовая зона обслуживания (Basic Service Set - BSS) - это группа станций, которые связываются друг с другом по беспроводной связи. Технология BSS предполагает наличие особой станции, которая называется *точкой доступа* (access point).

2. Стандарты IEEE 802.11

Из всех существующих стандартов беспроводной передачи данных IEEE 802.11 на практике чаще всего используются всего три стандарта, определенные Инженерным институтом электротехники и радиоэлектроники (IEEE): 802.11b, 802.11a и 802.11g.

Благодаря высокой скорости передачи данных (до 11 Мбит/с), практически эквивалентной пропускной способности обычных проводных локальных сетей Ethernet, а также ориентации на диапазон 2,4 ГГц, стандарт IEEE 802.11b был наиболее популярен у производителей оборудования для беспроводных сетей до появления и широкого распространения стандарта

IEEE 802.11g. Поскольку оборудование, работающее на максимальной скорости 11 Мбит/с, имеет меньший радиус действия, чем на более низких скоростях, стандартом 802.11b предусмотрено автоматическое снижение скорости при ухудшении качества сигнала.

Стандарт IEEE 802.11a имеет наибольшую ширину полосы из семейства стандартов 802.11 при скорости передачи данных до 54 Мбит/с. В отличие от базового стандарта, ориентированного на область частот 2,4 ГГц, спецификациями 802.11a предусмотрена работа в диапазоне 5 ГГц. В качестве метода модуляции сигнала выбрано ортогональное частотное мультиплексирование (OFDM). К недостаткам 802.11a относятся более высокая потребляемая мощность радиопередатчиков для частот 5 ГГц, а также, меньший радиус действия.

Стандарт IEEE 802.11g является логическим развитием 802.11b и предполагает передачу данных в том же частотном диапазоне. Кроме того, стандарт 802.11g полностью совместим с 802.11b, то есть любое устройство 802.11g должно поддерживать работу с устройствами 802.11b. Максимальная скорость передачи в стандарте 802.11g составляет 54 Мбит/с, поэтому сегодня это наиболее распространенный стандарт беспроводной связи. При разработке стандарта 802.11g рассматривались две отчасти конкурирующие технологии: метод ортогонального частотного разделения OFDM и метод двоичного пакетного сверточного кодирования PBCC, опционально реализованный в стандарте 802.11b. В результате стандарт 802.11g содержит компромиссное решение: в качестве базовых применяются технологии OFDM и CCK, а опционально предусмотрено использование технологии PBCC.

В настоящее время происходит постепенное внедрение более высокоскоростного стандарта IEEE 802.11n, не смотря на то, что он еще не утвержден официально.

Набор стандартов 802.11 определяет целый ряд технологий реализации физического уровня (Physical Layer Protocol - PHY), которые могут быть использованы подуровнем 802.11 MAC:

- Уровень PHY стандарта 802.11 со скачкообразной перестройкой частоты (FHSS) в диапазоне 2,4 ГГц.
- Уровень PHY стандарта 802.11 с расширением спектра методом прямой последовательности (DSSS) в диапазоне 2,4 ГГц.
- Уровень PHY стандарта 802.11b с комплементарным кодированием в диапазоне 2,4 ГГц.
- Уровень PHY стандарта 802.11a с ортогональным частотным мультиплексированием (OFDM) в диапазоне 5 ГГц.
- Расширенный физический уровень (Extended Rate Physical Layer - ERP) стандарта 802.11g в диапазоне 2,4 ГГц.

Основное назначение физических уровней стандарта 802.11 - обеспечить механизмы беспроводной передачи для подуровня MAC, а также поддерживать выполнение вторичных функций, таких как оценка состояния беспроводной среды и сообщение о нем подуровню MAC. Уровни MAC и PHY разрабатывались так, чтобы они были независимыми. Именно независимость между MAC и подуровнем PHY и позволила использовать дополнительные высокоскоростные физические уровни, описанные в стандартах 802.11b, 802.11a и 802.11g.

Каждый из физических уровней стандарта 802.11 имеет два подуровня:

- Physical Layer Convergence Procedure (PLCP). Процедура определения состояния физического уровня.
- Physical Medium Dependent (PMD). Подуровень физического уровня, зависящий от среды передачи.

На рис. 2.1 показано, как эти подуровни соотносятся между собой и с вышестоящими уровнями в модели взаимодействия открытых систем (Open System Interconnection - OSI).

Подуровень PLCP по существу является уровнем обеспечения взаимодействия, на котором осуществляется перемещение элементов данных протокола MAC (MAC Protocol Data Units - MPDU) между MAC-станциями с использованием подуровня PMD, на котором реализуется тот или иной метод передачи и приема данных через беспроводную среду. Подуровни PLCP и PMD отличаются для разных вариантов стандарта 802.11.

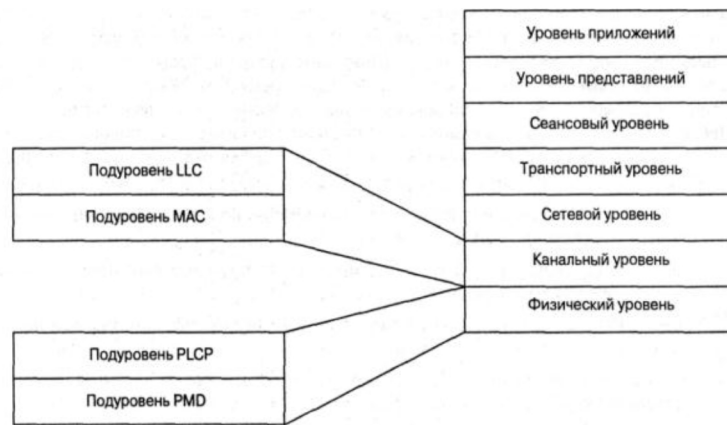


Рис. 2.1. Подуровни уровня РНУ

2.1. Стандарт IEEE 802.11g

Стандарт IEEE 802.11g по сути представляет собой перенесение схемы модуляции OFDM, прекрасно зарекомендовавшей себя в 802.11a, из диапазона 5 ГГц в область 2,4 ГГц при сохранении функциональности устройств стандарта 802.11b.

Одним из основных требований к спецификации 802.11g была обратная совместимость с устройствами 802.11b. Разработчики 802.11g предусмотрели ССК-модуляцию для скоростей до 11 Мбит/с и OFDM для более высоких скоростей. Сети стандартов 802.11 при работе используют принцип CSMA/CA - множественный доступ к каналу связи с контролем несущей и предотвращением коллизий. Ни одно устройство 802.11 не должно начинать передачу, пока не убедится, что эфир в его диапазоне свободен от других устройств.

Однако если в зоне слышимости окажутся устройства 802.11b и 802.11g, причем обмен будет происходить между устройствами 802.11g посредством OFDM, то оборудование 802.11b просто не поймет, что другие устройства сети ведут передачу, и попытается начать трансляцию. Чтобы не допустить подобной ситуации, предусмотрена возможность работы в смешанном режиме - ССК-OFDM.

Информация в сетях 802.11 передается кадрами. Каждый информационный кадр включает два основных поля: преамбулу с заголовком и информационное поле (рис. 2.2).

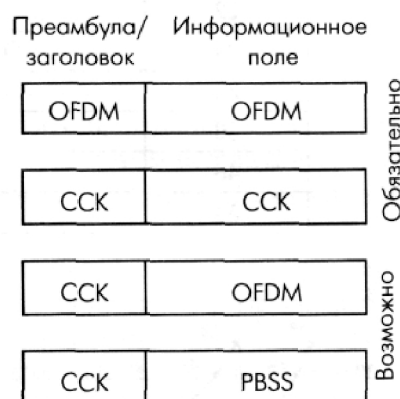


Рис. 2.2. Кадры IEEE 802.11g в различных режимах модуляции

Преамбула содержит синхропоследовательность и код начала кадра, заголовок - служебную информацию, в том числе о типе модуляции, скорости и продолжительности передачи кадра. В режиме ССК-OFDM преамбула и заголовок модулируются методом ССК (реально - путем прямого расширения спектра DSSS посредством последовательности Баркера, поэтому в стандарте 802.11g этот режим именуется DSSS-OFDM), а информационное поле - методом OFDM. Таким образом, все устройства 802.11b, постоянно "прослушивающие" эфир, принимают заголовки кадров и узнают, сколько времени будет транслироваться кадр 802.11g. В этот период они "молчат". Естественно, пропускная способность сети падает, поскольку скорость передачи преамбулы и заголовка - 1 Мбит/с.

Устройства стандарта 802.11g должны быть совместимыми со всеми модификациями оборудования 802.11b и не создавать взаимных помех. Диапазон поддерживаемых скоростей отражен в таблице 2.1.

Таблица 2.1. Возможные скорости и тип модуляции в спецификации IEEE 802.11g

Скорость, Мбит/с	Тип модуляции	
	Обязательно	Допустимо
1	Последовательность Баркера	
2	Последовательность Баркера	
5,5	CCK	PBCC
6	OFDM	OFDM
9		OFDM, CCK-OFDM
11	CCK	PBCC
12	OFDM	CCK-OFDM
18		OFDM, CCK-OFDM
22		PBCC
24	OFDM	CCK-OFDM
33		PBCC
36		OFDM, CCK-OFDM
48		OFDM, CCK-OFDM
54		OFDM, CCK-OFDM

В таблице 2.2 представлена сводная информация по параметрам физических уровней для семейства стандартов 802.11.

Таблица 2.2. Стандарты физического уровня

Параметр	802.11 DSSS	802.11 FHSS	802.11b	802.11a	802.11g
Частотный диапазон (ГГц)	2,4	2,4	2,4	5	2,4
Максимальная скорость передачи данных (Мбит/с)	2	2	11	54	54
Технология	DSSS	FHSS	CCK	OFDM	OFDM
Тип модуляции (для максимальной скорости передачи)	QPSK	GFSK	QPSK	64-QAM	64-QAM
Число неперекрывающихся каналов	3	3	3	15	3

3. Режимы работы устройств в беспроводной сети и особенности их организации

3.1. Режим Ad Hoc

В режиме *Ad Hoc* (рис. 3.1) клиенты устанавливают связь непосредственно друг с другом. Устанавливается одноранговое взаимодействие по типу "точка-точка", и компьютеры взаимодействуют напрямую без применения точек доступа. При этом создается только одна зона обслуживания, не имеющая интерфейса для подключения к проводной локальной сети.

Основное достоинство данного режима - простота организации: он не требует дополнительного оборудования (точки доступа). Режим может применяться для создания временных сетей для передачи данных (пример настройки для режима Ad Hoc рассмотрен в приложении). Для организации долговременных беспроводных сетей следует использовать инфраструктурный режим.

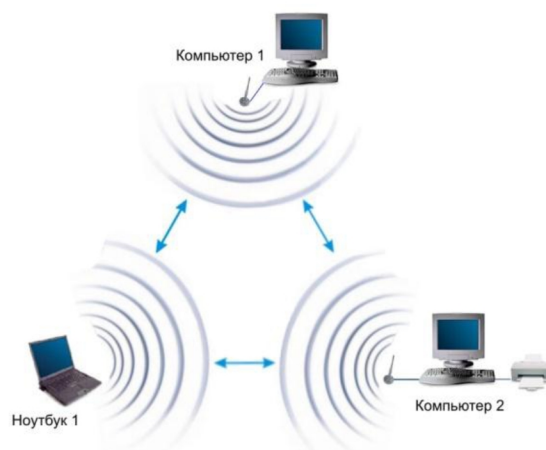


Рис. 3.1. Ad Нос

Однако необходимо иметь в виду, что режим Ad Нос позволяет устанавливать соединение на скорости не более 11 Мбит/с, независимо от используемого оборудования. Реальная скорость обмена данными будет ниже и составит не более $11/N$ Мбит/с, где N - число устройств в сети. Дальность связи составляет не более ста метров, а скорость передачи данных быстро падает с увеличением расстояния.

3.2. Инфраструктурный режим

В этом режиме точки доступа обеспечивают связь клиентских компьютеров (рис. 3.2). Точку доступа можно рассматривать как беспроводной коммутатор. Клиентские станции не связываются непосредственно одна с другой, а связываются с точкой доступа, и она уже направляет пакеты адресатам.

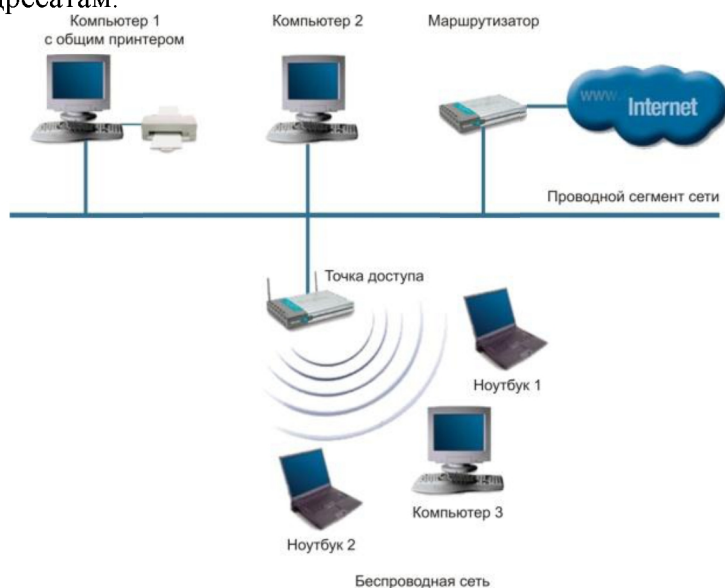


Рис. 3.2.

Точка доступа имеет порт Ethernet, через который базовая зона обслуживания подключается к проводной или смешанной сети - к сетевой *инфраструктуре*.

Пример 3.1. Настройка беспроводной точки доступа для работы беспроводной сети в инфраструктурном режиме.

Настройка производится через проводной интерфейс, т.е. используя Ethernet-соединение. Хотя можно это делать и через беспроводной интерфейс, но это не рекомендуется, т.к. при достаточно большом количестве точек доступа может возникнуть путаница в настройках.

1. В окне *Сетевые подключения* отключите сетевые и беспроводные адаптеры. В контекстном меню необходимо выбрать "Отключить" для каждого адаптера. В результате все компьютеры будут изолированы друг от друга, сетевых подключений нет.

2. Настраиваем сетевые адаптеры для связи с точкой доступа.

Подключения по локальной сети → Свойства → Протокол TCP/IP → Свойства

«Использовать следующий IP-адрес». Укажите адрес 192.168.0.xxx, где xxx - номер вашего компьютера (1, 2, 3 и т.д). Укажите маску 255.255.255.0.

На лабораторных работах в классе 220-1 для этих целей используется, как обычно, приложение NetSetMan.

3. Подключаем точку доступа.

Соединяем точку доступа сетевым кабелем с сетевым адаптером одного из компьютеров, подаем питание. Сбрасываем настройки точки. Для этого в течение пяти секунд нажимаем и удерживаем кнопку reset. Не отключаем питание при нажатой reset! Время загрузки точки - около 20 секунд. По окончании загрузки на точке загораются индикаторы Power и LAN.

Включите кабельное соединение. В браузере Internet Explorer наберите <http://192.168.0.50>. Появится приглашение на ввод имени и пароля (рис. 3.3).

4. Начинаем настройку.

Введите в качестве имени пользователя "admin" с пустым паролем. Настроим сначала IP-адрес точки. Это нужно лишь в том случае, когда у вас много точек доступа. На вкладке *Home* нажимаем кнопку *Lan* (слева). Выставляем адрес 192.168.0.xxx, где xxx - уникальный номер точки. Маска 255.255.255.0.

По завершении настройки следует нажать "Apply", чтобы перезагрузить точку с новыми настройками.

5. Включение режима точки доступа.

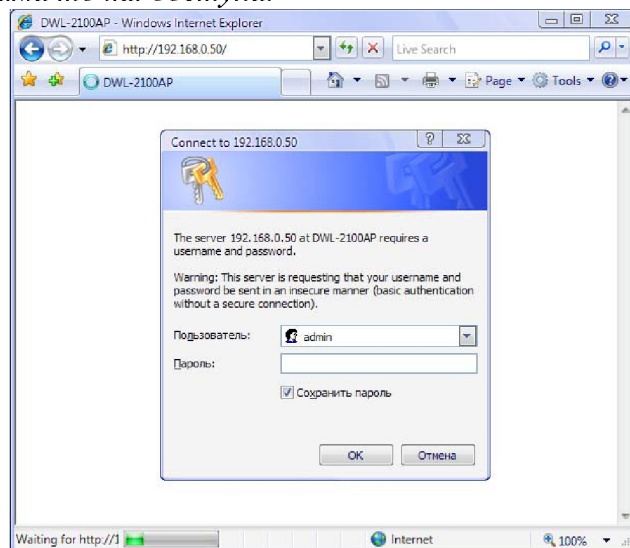


Рис. 3.3.

Дождитесь загрузки точки и введите в браузере новый адрес <http://192.168.0.xxx>. На вкладке *Home* нажмите кнопку *Wireless* (слева).

Устанавливаем (рис. 3.4):

Mode (режим): Access Point (AP).

SSID: *W_Network_# (1,2,3)*.

SSID Broadcast: Enable.

Channel: *(1,6,11)*

Authentication: Open System.

Encryption: Disable.

Выбранные установки не обеспечивают безопасность беспроводного подключения и используются только с целью обучения.

Если нужно сделать более тонкие настройки, перейдите на вкладку *Advanced* (краткое описание всех параметров есть на вкладке *Help*).

В заключение необходимо «применить» настройки, нажав "Apply", чтобы перезагрузить точку доступа с новыми настройками.

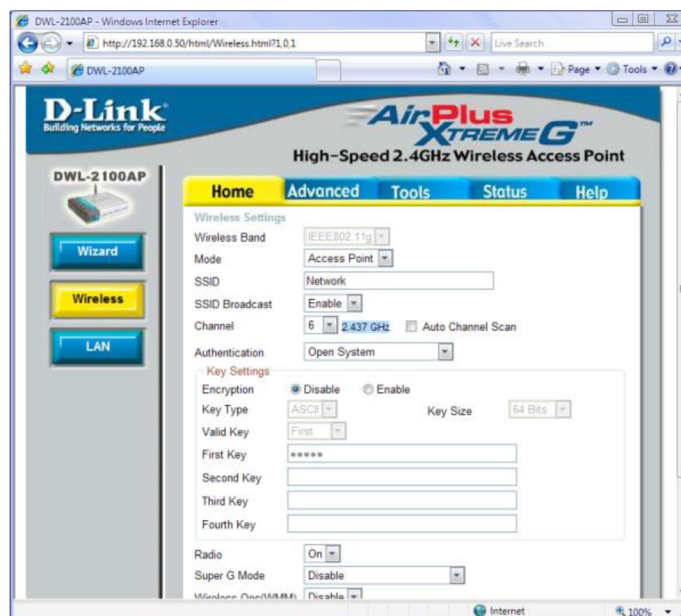


Рис. 3.4.

Если нет необходимости связывать настроенные точки доступа с существующей проводной локальной сетью (LAN), точку доступа от сетевого интерфейса можно отключить.

Пример 3.2. Настройка беспроводных клиентов для работы беспроводной сети в инфраструктурном режиме.

Будем считать, что на клиентской стороне используется беспроводной USB-адаптер. Все настройки для других типов адаптеров (PCI, PCMCIA, ExpressCard и т. д.) проводятся аналогичным образом. Будем также считать, что при подключении адаптера был установлен драйвер, который идет в комплекте со всем беспроводным оборудованием. В окне *Сетевые подключения* должен быть значок *Беспроводное сетевое соединение* (рис. 3.5)

Настроить беспроводной адаптер компьютера можно двумя способами:

- с помощью встроенной службы Windows XP или Windows Vista;
- программой D-Link AirPlus XtremeG Wireless Utility, которая идет в комплекте с оборудованием D-Link.

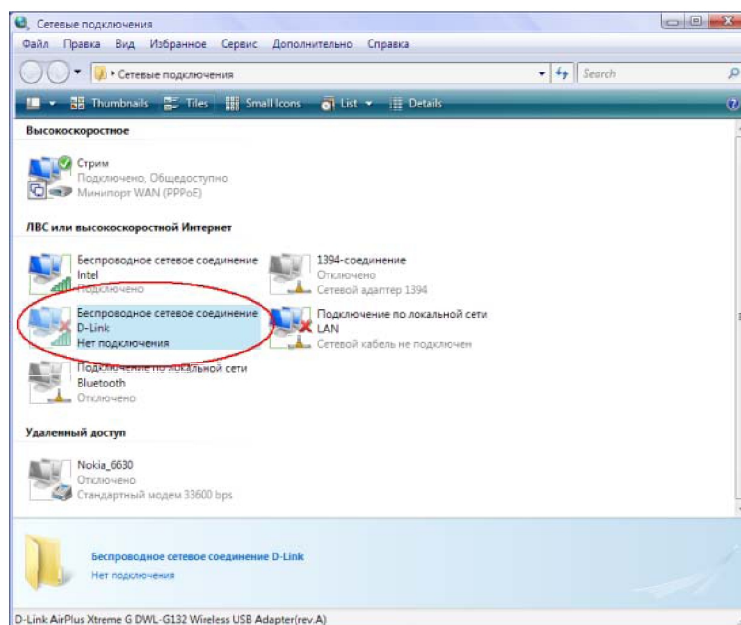


Рис. 3.5

1. Настройка подключения с помощью встроенной службы Windows.

При установке интерфейса, при наличии встроенной утилиты Windows, дополнительные программы не требуются. Но для этого необходимо установить галочку *Использовать Windows*

для настройки сети на вкладке *Беспроводные сети* в свойствах беспроводного соединения (рис. 3.6).

Перед установкой соединения необходимо настроить статические IP-адреса. Они настраиваются в свойствах беспроводного соединения, на вкладке *Общие*, в свойствах *Протокол Интернета (TCP/IP)* (рис. 3.7). На лабораторных работах в классе 220-1 для этих целей используется, как обычно, приложение NetSetMan.

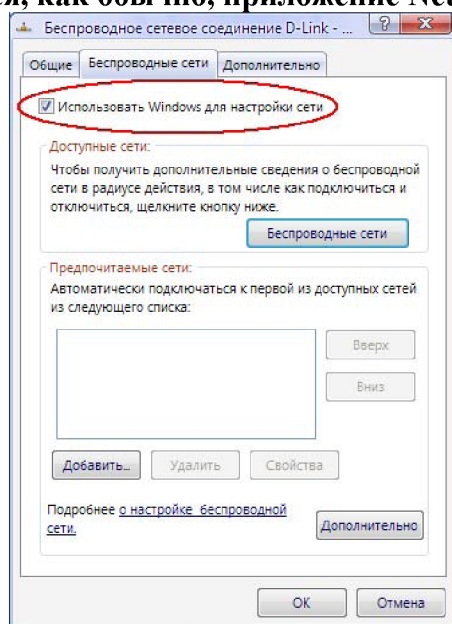


Рис. 3.6

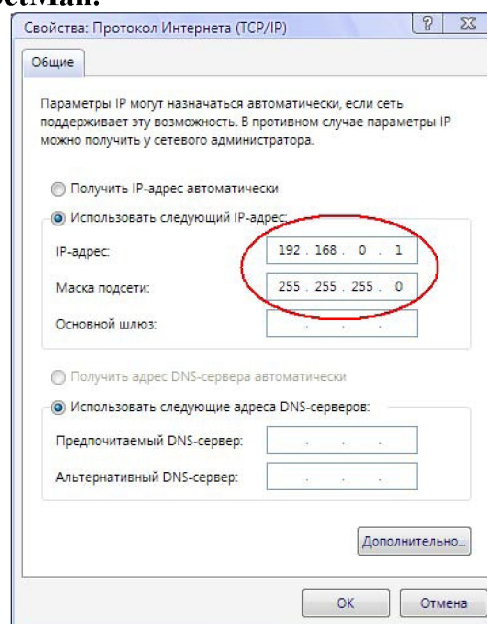


Рис. 3.7

Теперь двойным щелчком левой кнопки мыши по беспроводному интерфейсу (рис. 3.5) запустим службу Windows (рис. 3.8), и в основном окне выбираем появившуюся сеть с нужным нам SSID (например, PHOUSE_AP). Если используется шифрование, вводим ключ доступа. После завершения настройки проверяем командой `ping` наличие подключения.

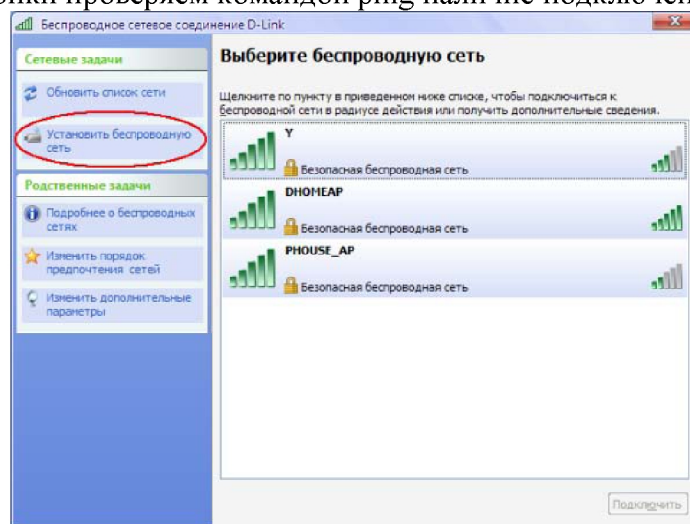


Рис. 3.8

2. Настройка подключения с помощью программы D-Link AirPlus XtremeG Wireless Utility.

В этом случае надо установить эту программу (если она еще не установлена) и убрать галочку *Использовать Windows для настройки сети*, показанную на рис. 3.6.

Первый способ. Запустив эту программу на компьютере, переходим (1) на вкладку *Настройка* (рис. 3.9).

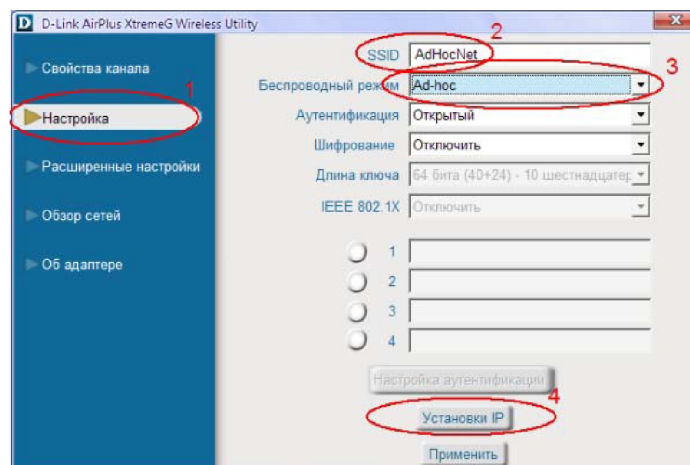


Рис. 3.9

Затем вводим SSID созданной ранее нужной нам сети (2), выбираем режим **Infrastructure** (3) и задаем (если не сделали это ранее в программе **NetSetMan**) IP-адрес с маской (4) беспроводного интерфейса (требуется права администратора). Аутентификацию и шифрование задаем в соответствии настройками точки доступа. Если требуются дополнительные настройки, их можно произвести на вкладке *Расширенные настройки*.

Второй способ. Запускаем эту программу и открываем вкладку *Обзор сетей* (1) (рис. 3.10).

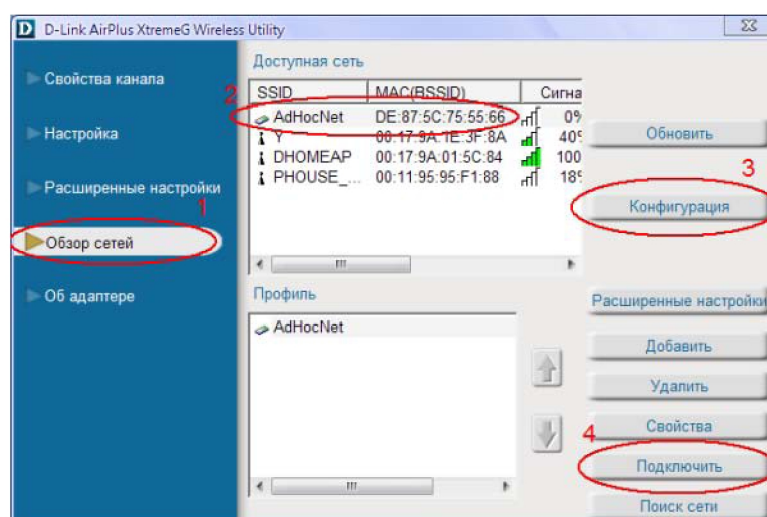


Рис. 3.10

В появившемся окне следует выбрать созданную ранее нужную нам сеть (2) (для настройки IP-адреса компьютера, если не сделали это ранее в программе **NetSetMan**, нажать кнопку *Конфигурация* (3)). Затем нужно нажать кнопку *Подключить* (4), и при совпадении ключа доступа беспроводной адаптер подключится к точке доступа. Обновление списка доступных сетей производится нажатием кнопки *Обновить*.

После завершения настройки беспроводного клиента проверяем командой ping наличие подключения.

3.3. Режимы WDS и WDS with AP

Термин **WDS (Wireless Distribution System)** расшифровывается как "распределенная беспроводная система". В этом режиме точки доступа соединяются только между собой, образуя мостовое соединение. При этом каждая точка может соединяться с несколькими другими точками. Все точки в этом режиме должны использовать один и тот же канал, поэтому количество точек, участвующих в образовании моста, не должно быть чрезмерно большим. Подключение клиентов осуществляется только по проводной сети через uplink-порты точек (рис. 3.11).

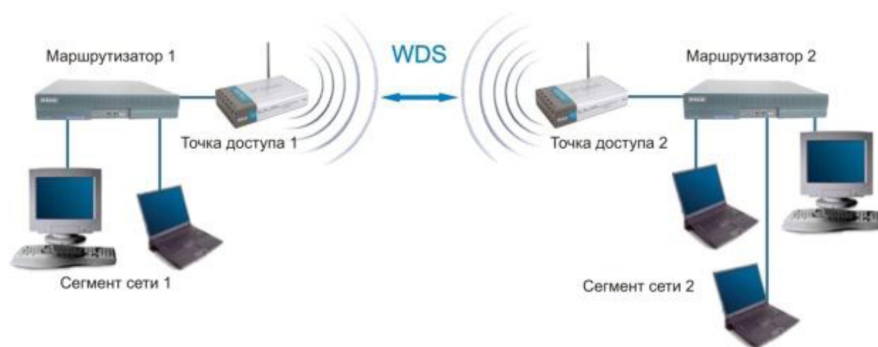


Рис. 3.11. Мостовой режим

Режим беспроводного моста, аналогично проводным мостам, служит для объединения подсетей в общую сеть. С помощью беспроводных мостов можно объединять проводные LAN, находящиеся как в соседних зданиях, так и на расстоянии до нескольких километров. Это позволяет объединить в сеть филиалы и центральный офис, а также подключать клиентов к сети провайдера Internet (рис. 3.12).

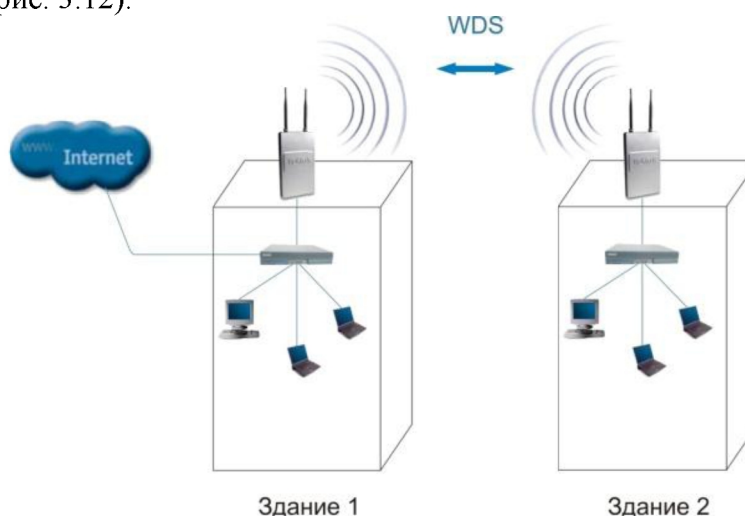


Рис. 3.12. Мостовой режим между зданиями

Беспроводной мост может использоваться там, где прокладка кабеля между зданиями нежелательна или невозможна. Данное решение позволяет достичь значительной экономии средств и обеспечивает простоту настройки и гибкость конфигурации при перемещении офисов.

К точке доступа, работающей в режиме моста, подключение беспроводных клиентов невозможно. Беспроводная связь осуществляется только между парой точек, реализующих мост.

Термин **WDS with AP (WDS with Access Point)** означает "распределенная беспроводная система, включающая точку доступа", т.е. с помощью этого режима можно не только организовать мостовую связь между точками доступа, но и одновременно подключить клиентские компьютеры (рис. 3.13). Это позволяет достичь существенной экономии оборудования и упростить топологию сети. Данная технология поддерживается большинством современных точек доступа.

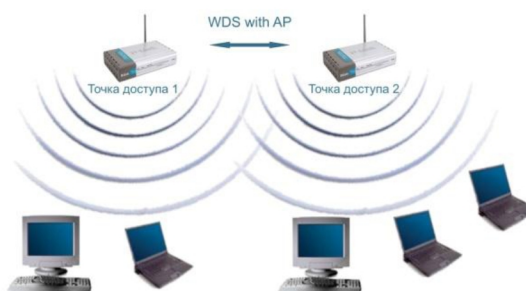


Рис. 3.13. Режим WDS with AP

Тем не менее, необходимо помнить, что все устройства в составе одной WDS with AP работают на одной частоте и создают взаимные помехи, что ограничивает количество клиентов до 15-20 узлов. Для увеличения количества подключаемых клиентов можно использовать несколько WDS-сетей, настроенных на разные неперекрывающиеся каналы и соединенные проводами через uplink-порты.

Пример 3.3. Создадим мост "точка - много точек" (рис. 3.14). Для этого нам понадобится не менее трех точек доступа.

1. *Настраиваем IP-адрес проводным интерфейсам точек доступа:*

Отключаем беспроводные интерфейсы и запускаем браузер Internet Explorer, в адресной строке вводим 192.168.0.50, по умолчанию логин: admin, пароль пустой.

Для каждой точки доступа заходим на вкладку Home → LAN и в поле IP address вводим: 192.168.0.5X, где X - номер точки доступа (например, 1, 2, 3 и т. д.).

2. *Настраиваем мостовое соединение, показанное на рис. 3.14.*

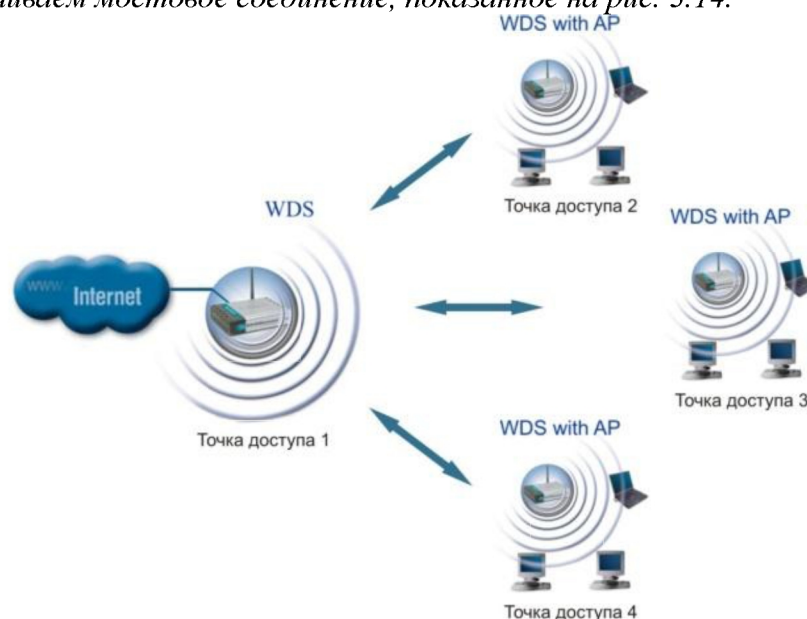


Рис. 3.14. Настройка моста "точка - много точек"

(1) Заходим на вкладку Home → Wireless в каждой точке доступа, устанавливаем режим (Mode): для первой - WDS (рис. 3.15), для второй, третьей и т.д. - WDS with AP (рис. 3.15).

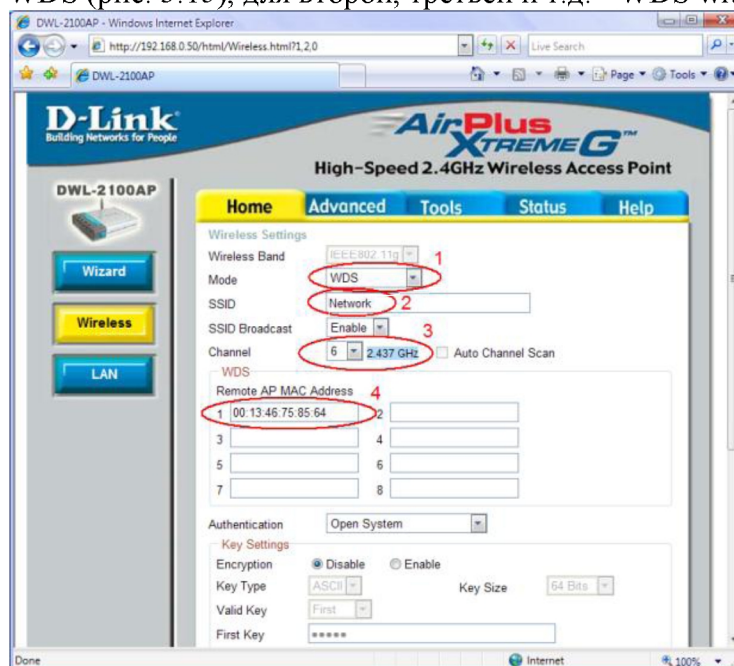


Рис. 3.15.

(2) Все точки доступа, реализующие мост, **должны** иметь одинаковый SSID, например: *W_Network*.

(3) Все точки доступа, реализующие мост, **должны** использовать один и тот же канал, например: 6.

(4) Для первой точки доступа в поле Remote AP MAC Address указываем MAC-адреса второй, третьей и т.д. точек, а для второй, третьей и т.д. точек доступа указываем MAC-адрес первой точки (**топология «звезда», она же «общая шина»**).

Применяем настройки, и после перезагрузки точки доступа войдут в режим моста.

3. *Проверяем соединение:*

Подключаемся беспроводными адаптерами ко второй, третьей и т.д. точке доступа.

Командой ping последовательно проверяем адреса всех точек, затем адреса других компьютеров в сети.

3.4. Режим клиента

Для подключения компьютеров, не имеющих беспроводных адаптеров, к беспроводной сети можно использовать точку доступа в режиме "клиента" (рис. 3.16).

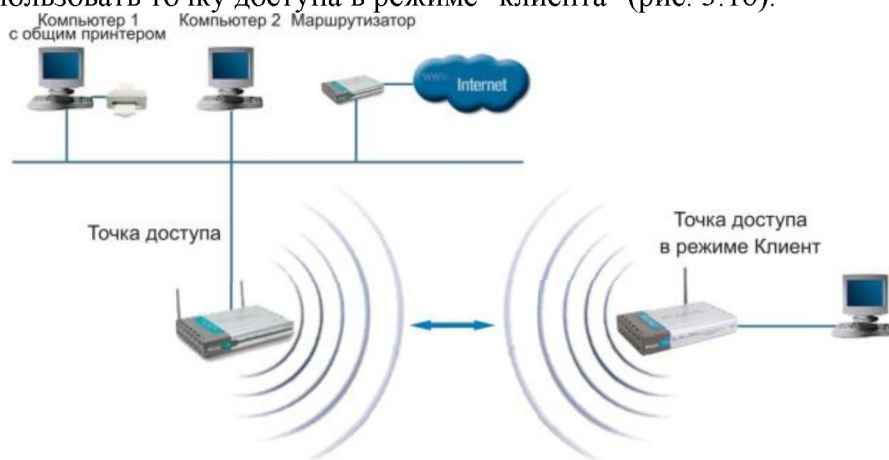


Рис. 3.16. Режим клиента

При помощи точки доступа, функционирующей в режиме клиента, к беспроводной сети подключается только одно устройство. Этот режим не включен в стандарт 802.11 и поддерживается не всеми производителями.

4. Организация и планирование беспроводных сетей

При организации беспроводной локальной сети необходимо учитывать некоторые особенности окружающей среды. На качество и дальность работы связи влияет множество физических факторов: число стен, перекрытий и других объектов, через которые должен пройти сигнал. Обычно расстояние зависит от типа материалов и радиочастотного шума от других электроприборов в помещении. Для улучшения качества связи надо следовать базовым принципам:

1. Сократить число стен и перекрытий между абонентами беспроводной сети - каждая стена и перекрытие отнимает от максимального радиуса от 1 м до 25 м. Расположить точки доступа и абонентов сети так, чтобы количество преград между ними было минимальным.

2. Проверить угол между точками доступа и абонентами сети. Стена толщиной 0,5 м при угле в 30 градусов для радиоволны становится стеной толщиной 1 м. При угле в 2 градуса стена становится преградой толщиной в 12 м! Надо стараться расположить абонентов сети так, чтобы сигнал проходил под углом в 90 градусов к перекрытиям или стенам.

3. Строительные материалы влияют на прохождение сигнала по-разному - целиком металлические двери или алюминиевая облицовка негативно сказываются на передаче радиоволн. Желательно, чтобы между абонентами сети не было металлических или железобетонных препятствий.

4. С помощью программного обеспечения проверки мощности сигнала надо позиционировать антенну на лучший прием.

5. Удалить от абонентов беспроводных сетей, по крайней мере, на 1-2 метра электроприборы, генерирующие радиопомехи, микроволновые печи, мониторы, электромоторы, ИБП. Для уменьшения помех эти приборы должны быть надежно заземлены.

6. Если используются беспроводные телефоны стандарта 2,4 ГГц или оборудование X-10 (например, системы сигнализации), качество беспроводной связи может заметно ухудшиться или прерваться.

Для типичного жилья расстояние связи не представляет особой проблемы. Если обнаружена неуверенная связь в пределах дома, то надо расположить точку доступа между комнатами, которые следует связать беспроводной сетью.

Для обнаружения точек доступа, попадающих в зону действия беспроводной сети, и определения каналов, на которых они работают, можно использовать программу **Network Stumbler** (<http://www.stumbler.net/>) или программу **InSSIDer**. С ее помощью также можно оценить соотношение "сигнал-шум" на выбранных каналах.

4.1. Офисная сеть

Простая беспроводная сеть для небольшого офиса или домашнего использования (Small Office / Home Office - SOHO) может быть построена на основе одной точки доступа (рис. 4.1).

Для организации сети адаптеры переводятся в режим инфраструктуры, а точка доступа - в режим точки доступа. При этом создается одна зона обслуживания, в которой находятся все пользователи сети.



Рис. 4.1. Офисная сеть

При размещении точки доступа при развертывании малой сети следует обеспечить достаточное качество связи на всех рабочих местах, а также удобство в размещении самой точки. Типовое решение - закрепить точку доступа непосредственно на фальш-потолке, при этом провода электропитания и проводной сети будут проходить над фальш-потолком либо в коробах.

Необходимо иметь в виду, что при расширении сети и увеличении количества пользователей скорость связи будет падать (пропорционально числу пользователей). Наибольшее разумное количество пользователей обычно составляет 16-20. Помимо этого скорость и качество связи зависят и от расстояния между клиентом и точкой. Эти соображения могут потребовать расширения базовой сети.

Для расширения сети можно использовать uplink-порт точки доступа. Он может использоваться как для объединения базовых зон обслуживания в сеть, так и для интеграции в имеющуюся проводную или беспроводную инфраструктуру, например для обеспечения пользователей доступом к разделяемым ресурсам других подразделений или для подключения к Internet.

При расширении сети необходимо следить, чтобы частоты соседних точек доступа не перекрывались во избежание взаимных помех и снижения скорости передачи. Это достигается настройкой соседних точек на неперекрывающиеся по частоте каналы 1, 6 и 11. Чередую каналы

таким образом, что соседние точки с каналами 1, 6 и 11 окажутся в вершинах равностороннего треугольника, можно охватить беспроводной связью сколь угодно большую площадь без перекрытия частот (рис. 4.2).

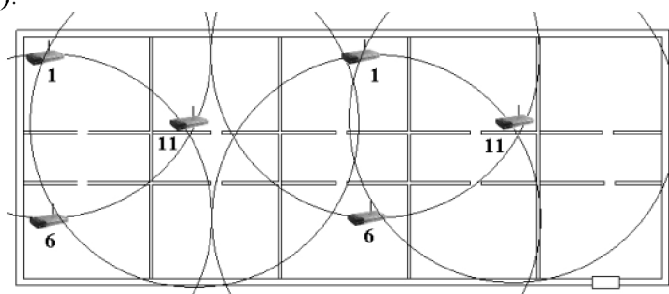


Рис. 4.2. Расширение беспроводной сети

На развертывание беспроводных сетей используемые приложения оказывают влияние по-разному. Наиболее важные факторы - это:

- Расчетная скорость в пересчете на одного клиента;
- Типы используемых приложений;
- Задержки в передаче данных.

Расчетная скорость каждого клиента уменьшается с вводом в зону обслуживания новых клиентов. Следовательно, если дома или в офисе используются требовательные к скорости приложения (например, программа Internet-телефонии Skype), необходимо увеличить количество точек доступа на единицу площади (рис. 4.3).

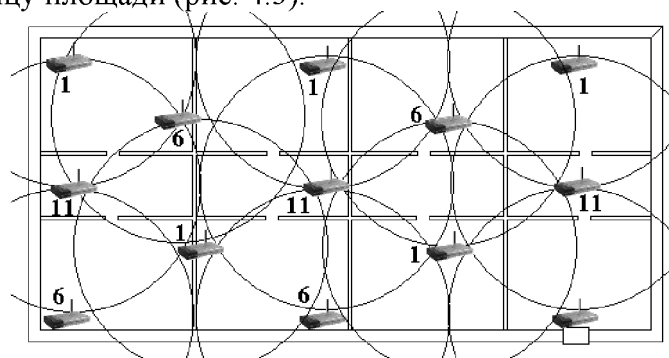


Рис. 4.3. Расширение беспроводной сети с максимальной скоростью

Для определения границы действия точек доступа используется ноутбук с установленной программой Network Stumbler (**InSSIDer**). Она показывает, на какой скорости будет работать адаптер в зависимости от расстояния от точки доступа. По мере удаления скорость автоматически падает, и при достижении порогового уровня необходимо ставить новую точку.

Объединение всех точек доступа в офисе в локальную сеть можно осуществить несколькими способами. Самым простым и распространенным методом организации является объединение через проводную инфраструктуру (рис. 4.4).



Рис. 4.4. Объединение точек доступа через проводную инфраструктуру

В таком случае устанавливается коммутатор, к которому подключаются точки доступа посредством витой пары через uplink-порт. Также к этому коммутатору можно подвести широкополосный Internet. Преимуществом такого подключения является простота настройки зоны

действия точек доступа на разные каналы, недостатком - прокладка проводов от точек доступа к коммутатору.

Второй способ - подключение с использованием расширенного режима WDS (рис. 4.5).

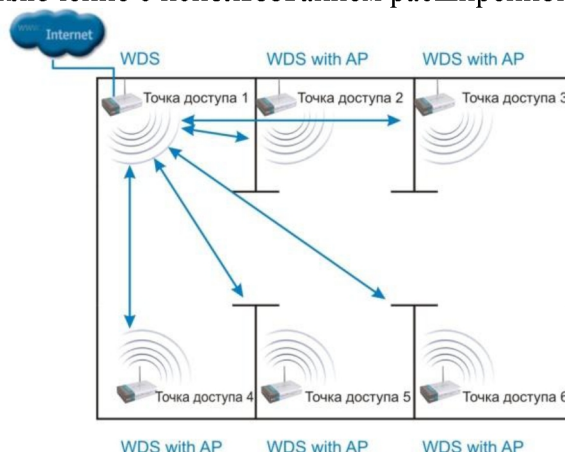


Рис. 4.5. Объединение точек доступа с использованием расширенного режима WDS

Одна точка доступа, которая имеет подключение к Internet, переводится в мостовой режим WDS, остальные точки настраиваются на тот же канал, что и первая, и устанавливается режим WDS with AP. Использование такого способа нежелательно, т.к. все точки работают на одном канале, и при достаточно большом их количестве резко уменьшается скорость. Рекомендуется устанавливать не более 2-3 точек.

Третий способ подключения аналогичен предыдущему но дополнительно к каждой точке доступа через проводной интерфейс подключена еще одна точка, работающая на другом канале, для организации связи в одной комнате (рис. 4.6).

Здесь переводятся те точки доступа в режим WDS, которые будут связаны с первой, а остальные через проводные интерфейсы подключаются к ним. Они должны работать в режиме точки доступа и на других каналах, чтобы не было коллизий. Преимуществом такого способа подключения является полное отсутствие проводной инфраструктуры (за исключением связи между соседними точками), недостатком - высокая стоимость, в связи с большим количеством точек доступа, и использование одного канала для связи с базовой точкой.

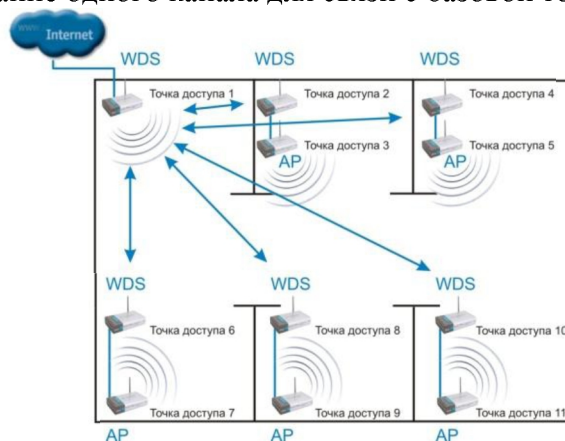


Рис. 4.6. Объединение точек доступа с дополнительными точками

Чтобы пользователь мог передвигаться от одной точки доступа к другой без потери доступа к сетевым службам и разрыва соединения, во всем оборудовании компании D-Link предусмотрена функция роуминга.

Роуминг - это возможность радиоустройства перемещаться за пределы действия базовой станции и, находясь в зоне действия "гостевой" станции, иметь доступ к "домашней" сети (рис. 4.7).



Рис. 4.7. Роуминг

При организации роуминга все точки доступа, обеспечивающие роуминг, конфигурируются на использование одинакового идентификатора зоны обслуживания (SSID). Все точки доступа относятся к одному ширококвещательному домену, или одному *домену роуминга*.

Механизм определения момента времени, когда необходимо начать процесс роуминга, не определен в стандарте 802.11, и, таким образом, оставлен на усмотрение поставщиков оборудования. Наиболее простой широко распространенный алгоритм переключения заключается в том, что адаптер взаимодействует с одной точкой вплоть до того момента, когда уровень сигнала не упадет ниже допустимого предела. После этого осуществляется поиск точки доступа с одинаковым SSID и максимальным уровнем сигнала, и переподключение к ней.

Роуминг включает значительно больше процессов, чем необходимо для поиска точки доступа, с которой можно связаться. Опишем некоторые из задач, которые должны решаться в ходе роуминга на канальном уровне:

- Предыдущая точка доступа должна определить, что клиент уходит из ее области действия.
- Предыдущая точка доступа должна буферизовать данные, предназначенные для клиента, осуществляющего роуминг.
- Новая точка доступа должна показать предыдущей, что клиент успешно переместился в ее зону.
- Предыдущая точка доступа должна послать буферизованные данные новой точке доступа.
- Предыдущая точка доступа должна определить, что клиент покинул ее зону действия.
- Точка доступа должна обновить таблицы MAC-адресов на коммутаторах инфраструктуры, чтобы избежать потери данных перемещающегося клиента.

4.2. Сеть между несколькими офисами

Беспроводная связь может использоваться для объединения подсетей отдельных зданий, например центрального офиса и филиалов, там, где прокладка кабеля между зданиями нежелательна или невозможна (рис. 4.8).

Для организации связи между зданиями могут использоваться внешние беспроводные точки, работающие в режиме моста. Через uplink-порт внешняя точка подключается к обычному коммутатору и через него обеспечивает связь со всеми компьютерами подсети.

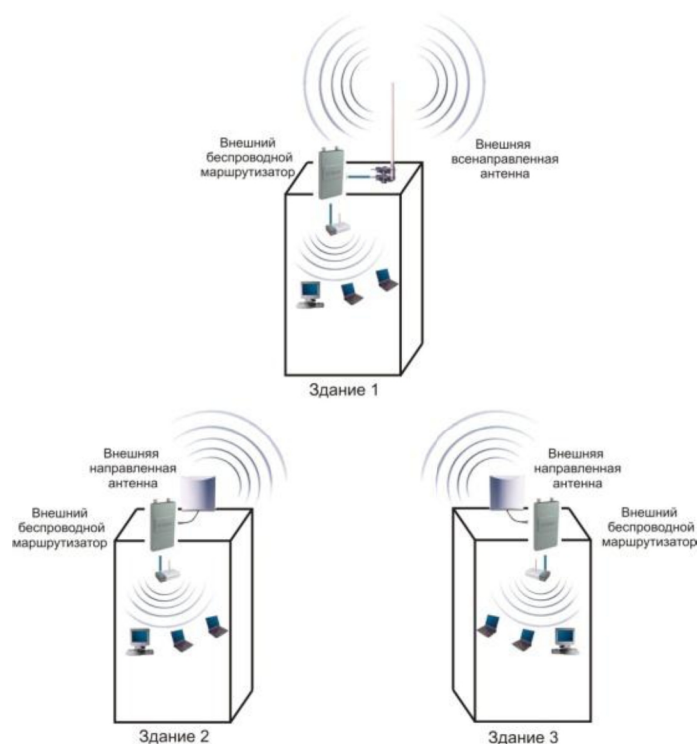


Рис. 4.8. Сеть между несколькими офисами

Внешние беспроводные точки имеют водонепроницаемый термостатированный корпус, систему грозовой защиты, систему питания Power-over-Ethernet. Благодаря сменной антенне можно обеспечивать устойчивую радиосвязь на расстоянии до нескольких километров на специализированные узконаправленные антенны.

При организации внешней беспроводной связи особое внимание следует обратить на обеспечение безопасности передачи данных, в связи с ее большей уязвимостью, как при прослушивании, так и в случае прямого физического воздействия. Поэтому рекомендуется использовать точки доступа, специально предназначенные для наружного применения и позволяющие задействовать аутентификацию, контроль доступа и шифрование передаваемых данных.

Необходимо также обратить внимание на то, что для внешних точек предусмотрена более сложная процедура получения разрешений на использование частот. Правила применения радиочастотного спектра в России приведены в статье 22 "**Регулирование использования радиочастотного спектра**" Федерального закона "О связи" в редакции от 09.02.2007 № 14-ФЗ.

5. Аутентификация в беспроводных сетях

Основными стандартами аутентификации в беспроводных сетях являются стандарты IEEE 802.11, WPA, WPA2 и 802.1x. Рассмотрим основы этих стандартов.

5.1. Стандарт IEEE 802.11 сети с традиционной безопасностью

Стандарт IEEE 802.11 с традиционной безопасностью (Tradition Security Network - TSN) предусматривает два механизма аутентификации беспроводных абонентов: *открытую аутентификацию* (Open Authentication) и *аутентификацию с общим ключом* (Shared Key Authentication). В аутентификации в беспроводных сетях также широко используются два других механизма, выходящих за рамки стандарта 802.11, а именно назначение *идентификатора беспроводной локальной сети* (Service Set Identifier - SSID) и *аутентификация абонента по его MAC-адресу* (MAC Address Authentication).

Идентификатор беспроводной локальной сети (SSID) представляет собой атрибут беспроводной сети, позволяющий логически отличать сети друг от друга. В общем случае абонент беспроводной сети должен задать у себя соответствующий SSID для того, чтобы получить доступ к требуемой беспроводной локальной сети. SSID ни в коей мере не обеспечивает конфиденциальность данных, равно как и не аутентифицирует абонента по отношению к точке радиодоступа беспроводной локальной сети. Существуют точки доступа, позволяющие разделить

абонентов, подключаемых к точке на несколько сегментов, - это достигается тем, что точка доступа может иметь не один, а несколько SSID.

Аутентификация в стандарте IEEE 802.11 ориентирована на аутентификацию абонентского устройства радиодоступа, а не конкретного абонента как пользователя сетевых ресурсов. Процесс аутентификации абонента беспроводной локальной сети IEEE 802.11 состоит из следующих этапов (рис. 5.1):

1. Абонент (Client) посылает фрейм Probe Request во все радиоканалы.
2. Каждая точка радиодоступа (Access Point - AP), в зоне радиовидимости которой находится абонент, посылает в ответ фрейм Probe Response.
3. Абонент выбирает предпочтительную для него точку радиодоступа и посылает в обслуживаемый ею радиоканал запрос на аутентификацию (Authentication Request).
4. Точка радиодоступа посылает подтверждение аутентификации (Authentication Response).
5. В случае успешной аутентификации абонент посылает точке радиодоступа фрейм ассоциации (Association Request).
6. Точка радиодоступа посылает в ответ фрейм подтверждения ассоциации (Association Response).
7. Абонент может теперь осуществлять обмен пользовательским трафиком с точкой радиодоступа и проводной сетью.

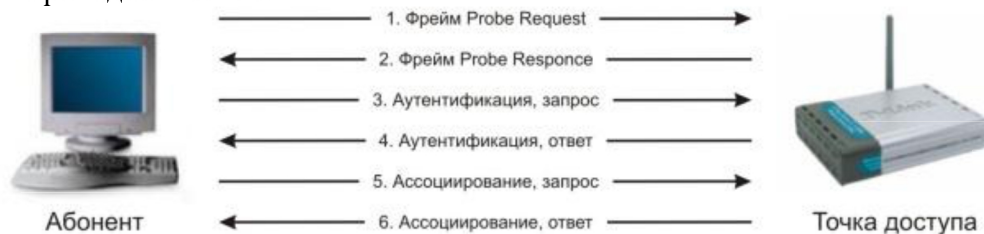


Рис. 5.1. Аутентификация по стандарту 802.11

Рассмотрим этот процесс несколько подробнее. При активизации беспроводный абонент начинает поиск точек радиодоступа в своей зоне радиовидимости с помощью управляющих фреймов Probe Request. Фреймы Probe Request посылаются в каждый из радиоканалов, поддерживаемых абонентским радиоинтерфейсом, чтобы найти все точки радиодоступа с необходимыми клиенту идентификатором SSID и поддерживаемыми скоростями радиообмена. Каждая точка радиодоступа из находящихся в зоне радиовидимости абонента, удовлетворяющая запрашиваемым во фрейме Probe Request параметрам, отвечает фреймом Probe Response, содержащим синхронизирующую информацию и данные о текущей загрузке точки радиодоступа. Абонент определяет, с какой точкой радиодоступа он будет работать, путем сопоставления поддерживаемых ими скоростей радиообмена и загрузки. После того как предпочтительная точка радиодоступа определена, абонент переходит в фазу аутентификации.

Открытая аутентификация, по сути не является алгоритмом аутентификации в привычном понимании. Точка радиодоступа удовлетворит любой запрос открытой аутентификации. На первый взгляд использование этого алгоритма может показаться бессмысленным, однако следует учитывать, что разработанные в 1997 году методы аутентификации IEEE 802.11 ориентированы на быстрое логическое подключение к беспроводной локальной сети. Вдобавок к этому многие IEEE 802.11-совместимые устройства представляют собой портативные блоки сбора информации (сканеры штрих-кодов и т. п.), не имеющие достаточной процессорной мощности, необходимой для реализации сложных алгоритмов аутентификации.

В процессе открытой аутентификации происходит обмен сообщениями двух типов:

- запрос аутентификации (Authentication Request);
- подтверждение аутентификации (Authentication Response).

Таким образом, при открытой аутентификации возможен доступ любого абонента к беспроводной локальной сети. Если в беспроводной сети шифрование не используется, любой абонент, знающий идентификатор SSID точки доступа, получит доступ к сети. При использовании точками доступа шифрования WEP сами ключи шифрования становятся средством кон-

троля доступа. Если абонент не располагает корректным WEP-ключом, то даже в случае успешной аутентификации он не сможет ни передавать данные через точку доступа, ни расшифровывать данные, переданные точкой доступа.

Аутентификация с общим ключом является вторым методом аутентификации стандарта IEEE 802.11. Она требует настройки у абонента статического ключа шифрования WEP. Процесс аутентификации иллюстрирует рис. 5.2:

1. Абонент посылает точке радиодоступа запрос аутентификации, указывая при этом необходимость использования режима аутентификации с общим ключом.
2. Точка радиодоступа посылает подтверждение аутентификации, содержащее Challenge Text.
3. Абонент шифрует Challenge Text своим статическим WEP-ключом и посылает точке радиодоступа запрос аутентификации.
4. Если точка радиодоступа в состоянии успешно расшифровать запрос аутентификации и содержащийся в нем Challenge Text, она посылает абоненту подтверждение аутентификации, таким образом, предоставляя доступ к сети.



Рис. 5.2. Аутентификация с общим ключом

Аутентификация абонента по его MAC-адресу не предусмотрена стандартом IEEE 802.11, однако поддерживается многими производителями оборудования для беспроводных сетей, в том числе D-Link. При аутентификации по MAC-адресу происходит сравнение MAC-адреса абонента либо с хранящимся локально списком разрешенных адресов легитимных абонентов, либо с помощью внешнего сервера аутентификации (рис. 5.3). Аутентификация по MAC-адресу используется в дополнение к открытой аутентификации и аутентификации с общим ключом стандарта IEEE 802.11 для уменьшения вероятности доступа посторонних абонентов.



Рис. 5.3. Аутентификация с помощью внешнего сервера

Рассмотрим, в чем состоят уязвимости механизмов аутентификации 802.11:

1. Идентификатор SSID регулярно передается точками радиодоступа в специальных фреймах Beacon. Несмотря на то, что эти фреймы играют чисто информационную роль в радиосети, т. е. совершенно "прозрачны" для абонента, сторонний наблюдатель в состоянии с легкостью определить SSID с помощью анализатора трафика протокола 802.11, например Sniffer Pro Wireless. Некоторые точки радиодоступа, в том числе D-Link, позволяют административно запретить широковещательную передачу SSID внутри фреймов Beacon. Однако и в этом случае SSID можно легко определить путем захвата фреймов Probe Response, посылаемых точками радиодоступа. Идентификатор SSID не разрабатывался для использования в качестве механизма обеспечения безопасности. Вдобавок к этому отключение широковещательной передачи SSID точками радиодоступа может отразиться на совместимости оборудования беспроводных сетей различных производителей при использовании в одной радиосети.

2. Открытая аутентификация не позволяет точке радиодоступа определить, является абонент легитимным или нет. Это становится заметной брешью в системе безопасности в том случае, если в беспроводной локальной сети не используется шифрование WEP

D-Link не рекомендует эксплуатацию беспроводных сетей без шифрования WEP. В тех случаях, когда использование шифрования WEP не требуется или невозможно (например, в беспроводных локальных сетях публичного доступа), методы аутентификации более высокого уровня могут быть реализованы посредством Internet-шлюзов.

3. Аутентификация с общим ключом требует настройки у абонента статического WEP-ключа для шифрования Challenge Text, отправленного точкой радиодоступа. Точка радиодоступа аутентифицирует абонента посредством дешифрации его ответа на Challenge и сравнения его с отправленным оригиналом. Обмен фреймами, содержащими Challenge Text, происходит по открытому радиоканалу, а значит, подвержен атакам со стороны наблюдателя (Man in the middle Attack). Наблюдатель может принять как нешифрованный Challenge Text, так и тот же Challenge Text, но уже в зашифрованном виде (рис. 5.4). Шифрование WEP производится путем выполнения побитовой операции XOR над текстом сообщения и ключевой последовательностью, в результате чего получается зашифрованное сообщение (Cipher-Text). Важно понимать, что в результате выполнения побитовой операции XOR над зашифрованным сообщением и ключевой последовательностью мы имеем текст исходного сообщения. Таким образом, наблюдатель может легко вычислить сегмент ключевой последовательности путем анализа фреймов в процессе аутентификации абонента.

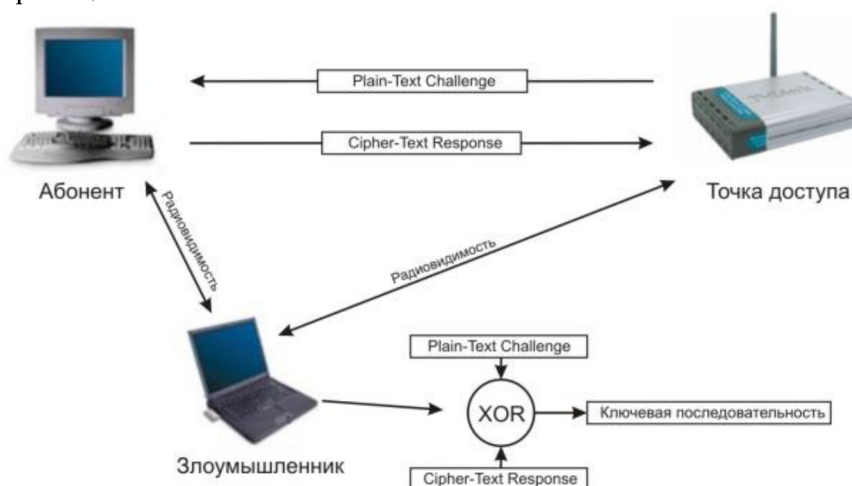


Рис. 5.4. Уязвимость аутентификации с общим ключом

4. Уязвимость аутентификации по MAC-адресу. Стандарт IEEE 802.11 требует передачи MAC-адресов абонента и точки радиодоступа в открытом виде. В результате в беспроводной сети, использующей аутентификацию по MAC-адресу, злоумышленник может обмануть метод аутентификации путем подмены своего MAC-адреса легитимным. Подмена MAC-адреса возможна в беспроводных адаптерах, допускающих использование локально администрируемых MAC-адресов. Злоумышленник может воспользоваться анализатором трафика протокола IEEE 802.11 для выявления MAC-адресов легитимных абонентов.

5.2. Спецификация WPA

До мая 2001 г. стандартизация средств информационной безопасности для беспроводных сетей 802.11 относилась к ведению рабочей группы IEEE 802.11e, но затем эта проблематика была выделена в самостоятельное подразделение. Разработанный стандарт 802.11i призван расширить возможности протокола 802.11, предусмотрев средства шифрования передаваемых данных, а также централизованной аутентификации пользователей и рабочих станций.

Основные производители Wi-Fi оборудования в лице организации WECA (Wireless Ethernet Compatibility Alliance), иначе именуемой Wi-Fi Alliance, устав ждать ратификации стандарта IEEE 802.11i, совместно с IEEE в ноябре 2002 г. анонсировали спецификацию **Wi-Fi Protected Access (WPA)**, соответствие которой обеспечивает совместимость оборудования различных производителей.

Новый стандарт безопасности WPA обеспечивает уровень безопасности куда больший, чем может предложить WEP. Он перебрасывает мостик между стандартами WEP и 802.11i и имеет немаловажное преимущество, которое заключается в том, что микропрограммное обес-

печение более старого оборудования может быть заменено без внесения аппаратных изменений.

IEEE предложила *временный протокол целостности ключа* (Temporal Key Integrity Protocol, TKIP).

Основные усовершенствования, внесенные протоколом TKIP:

- *Потфреймовое изменение ключей шифрования*. WEP-ключ быстро изменяется, и для каждого фрейма он другой;
- *Контроль целостности сообщения*. Обеспечивается эффективный контроль целостности фреймов данных с целью предотвращения скрытых манипуляций с фреймами и воспроизведения фреймов;
- *Усовершенствованный механизм управления ключами*.

WPA может работать в двух режимах: **Enterprise** (корпоративный) и **Pre-Shared Key** (персональный).

В первом случае хранение базы данных и проверка аутентичности по стандарту 802.1x в больших сетях обычно осуществляются специальным RADIUS (Remote Authentication Dial-In User Service) сервером.

Во втором случае подразумевается применение WPA всеми категориями пользователей беспроводных сетей, т.е. имеет место упрощенный режим, не требующий сложных механизмов. Этот режим называется **WPA-PSK** (Pre-Shared Key) и предполагает введение одного пароля на каждый узел беспроводной сети (точку доступа, беспроводной маршрутизатор, клиентский адаптер, мост). До тех пор, пока пароли совпадают, клиенту будет разрешен доступ в сеть. Можно заметить, что подход с использованием пароля делает WPA-PSK уязвимым для атаки методом подбора, однако этот режим избавляет от путаницы с ключами WEP, заменяя их целостной и четкой системой на основе цифро-буквенного пароля.

Таким образом, **WPA/TKIP** - это решение, предоставляющее больший по сравнению с WEP уровень безопасности, направленное на устранение слабостей предшественника и обеспечивающее совместимость с более старым оборудованием сетей 802.11 без внесения аппаратных изменений в устройства.

5.3. Стандарт сети 802.11i с повышенной безопасностью (WPA2)

В июне 2004 г. IEEE ратифицировал давно ожидаемый стандарт обеспечения безопасности в беспроводных локальных сетях - 802.11i.

WPA - практическое решение, обеспечивающее достаточный уровень безопасности для беспроводных сетей. Однако WPA - компромиссное решение. Оно все еще основано на алгоритме шифрования RC4 и протоколе TKIP. Вероятность выявления каких-либо слабых мест хотя и мала, но все же существует.

Абсолютно новая система безопасности, лишенная недостатков WEP, представляет собой лучшее долгосрочное и к тому же расширяемое решение для безопасности беспроводных сетей. С этой целью комитет по стандартам принял решение разработать систему безопасности с нуля. Это новый стандарт **802.11i**, также известный как **WPA2** и выпущенный тем же Wi-Fi Alliance.

Стандарт 802.11i использует концепцию повышенной безопасности (Robust Security Network - RSN), предусматривающую, что беспроводные устройства должны обеспечивать дополнительные возможности. Это потребовало изменений в аппаратной части и программном обеспечении, т.е. сеть, полностью соответствующая RSN, стала несовместимой с существующим оборудованием WEP. В переходный период поддерживается как оборудование RSN, так и WEP (на самом деле WPA/TKIP было решением, направленным на сохранение инвестиций в оборудование), но в дальнейшем устройства WEP начнут отмирать.

802.11i приложим к различным сетевым реализациям, и может задействовать TKIP, но по умолчанию RSN использует **AES (Advanced Encryption Standard)** и CCMP (Counter Mode CBC MAC Protocol) и, таким образом, является более мощным расширяемым решением.

В концепции RSN применяется AES в качестве системы шифрования, подобно тому, как алгоритм RC4 задействован в WPA. Однако механизм шифрования куда более сложен и не

страдает от проблем, свойственных WEP. AES - блочный шифр, оперирующий блоками данных по 128 бит. CCMP, в свою очередь, - протокол безопасности, используемый AES. Он является эквивалентом TKIP в WPA. CCMP вычисляет MIC, прибегая к хорошо известному и проверенному методу Cipher Block Chaining Message Authentication Code (CBC-MAC). Изменение даже одного бита в сообщении приводит к совершенно другому результату.

Одной из слабых сторон WEP было управление секретными ключами. Многие администраторы больших сетей находили его неудобным. Ключи WEP не менялись длительное время (или никогда), что облегчало задачу злоумышленникам.

RSN определяет иерархию ключей с ограниченным сроком действия, сходную с TKIP. В AES/CCMP, чтобы вместить все ключи, требуется 512 бит - меньше, чем в TKIP. В обоих случаях мастер-ключи используются не прямо, а для вывода других ключей. К счастью, администратор должен обеспечить единственный мастер-ключ. Сообщения состоят из 128-битного блока данных, зашифрованного секретным ключом такой же длины (128 бит). Хотя процесс шифрования сложен, администратор опять-таки не должен вникать в нюансы вычислений. Конечным результатом является шифр, который гораздо сложнее, чем даже WPA.

802.11i (WPA2) - это наиболее устойчивое, расширяемое и безопасное решение, предназначенное в первую очередь для крупных предприятий, где управление ключами и администрирование доставляет множество хлопот.

Стандарт 802.11i разработан на базе проверенных технологий. Механизмы безопасности были спроектированы с нуля в тесном сотрудничестве с лучшими специалистами по криптографии и имеют все шансы стать тем решением, которое необходимо беспроводным сетям. Хотя ни одна система безопасности от взлома не застрахована, 802.11i - это решение, на которое можно полагаться, в нем нет недостатков предыдущих систем. И, конечно, WPA пригоден для адаптации уже существующего оборудования, и только когда его ресурсы будут окончательно исчерпаны, можно будет заменить его новым, полностью соответствующим концепции RSN.

Производительность канала связи, как свидетельствуют результаты тестирования оборудования различных производителей, падает на 5-20% при включении как WEP, так и WPA. Однако испытания того оборудования, в котором включено шифрование AES вместо TKIP, не показали сколько-нибудь заметного падения скорости. Это позволяет надеяться, что WPA2-совместимое оборудование дает долгожданный надежно защищенный канал без потерь в производительности.

WPA2, как и WPA, может работать в двух режимах: *Enterprise* (корпоративный) и *Pre-Shared Key* (персональный).

Пример 5.1. Настройка точки доступа с применением персональной спецификации, т.е. **WPA2-PSK**.

1. Подключаемся к точке доступа по проводному интерфейсу, вводим режим, SSID, канал, как было описано ранее в примерах 3.1 и 3.3. Далее в поле Authentication (Аутентификация) ставим WPA2-PSK (рис. 5.5).



Рис. 5.5.

2. Выбираем тип шифрования (Cipher Type). Возможные варианты: AUTO, TKIP, AES. Если выставлено AUTO, точка доступа будет подстраивать тип шифрования под первого подключившегося клиента. Следует по возможности использовать наиболее надежный вариант – **AES**, при условии поддержки этого типа шифрования всеми беспроводными устройствами нашей сети.

3. Выставляем интервал обновления группового ключа (Group Key Update Interval), который задается в секундах (или оставляем его значение по умолчанию).

4. **Вводим в поле PassPhrase ключ любой длины, но не менее 8 символов, например secretpass.**

После применения настроек, на клиентской стороне надо выставить те же самые параметры и подключиться к точке доступа.

5.4. Стандарт 802.1x/EAP (Enterprise-режим)

Проблемы, с которыми столкнулись разработчики и пользователи сетей на основе стандарта 802.11, вынудили искать новые решения защиты **корпоративных** беспроводных сетей. Были выявлены компоненты, влияющие на системы безопасности беспроводной локальной сети:

1. Архитектура аутентификации.
2. Механизм аутентификации.
3. Механизм обеспечения конфиденциальности и целостности данных.

Алгоритм аутентификации Extensible Authentication Protocol или EAP (расширяемый протокол идентификации) поддерживает централизованную аутентификацию элементов инфраструктуры беспроводной сети и ее пользователей с возможностью динамической генерации ключей шифрования.

Архитектура IEEE 802.1x включает в себя следующие обязательные логические элементы (рис. 5.6):

- Клиент (Supplicant) - находится в операционной системе абонента;
- Аутентификатор (Authenticator) - находится в программном обеспечении точки радиодоступа;
- Сервер аутентификации (Authentication Server) - находится на RADIUS-сервере.

IEEE 802.1x предоставляет абоненту беспроводной локальной сети лишь средства передачи атрибутов серверу аутентификации и допускает использование различных методов и алгоритмов аутентификации. Задачей сервера аутентификации является поддержка разрешенных политикой сетевой безопасности методов аутентификации.

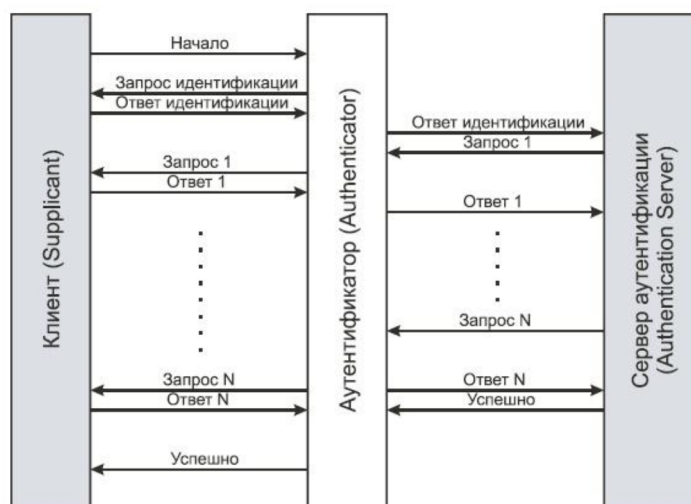


Рис. 5.6. Архитектура IEEE 802.1x

Аутентификатор, находясь в точке доступа, создает логический порт для каждого клиента на основе его идентификатора ассоциирования. Логический порт имеет два канала для обмена данными. Неконтролируемый канал беспрепятственно пропускает трафик из беспроводного сегмента в проводной и обратно, в то время как контролируемый канал требует успешной аутентификации для прохождения фреймов.

Таким образом, в терминологии стандарта 802.1x точка доступа играет роль коммутатора в проводных сетях Ethernet. Очевидно, что проводной сегмент сети, к которому подключена точка доступа, нуждается в сервере аутентификации. Его функции обычно выполняет RADIUS-сервер, интегрированный с той или иной базой данных пользователей, в качестве которой может выступать стандартный RADIUS, LDAP, NDS или Windows Active Directory. Коммерческие беспроводные шлюзы высокого класса могут реализовывать как функции сервера аутентификации, так и аутентификатора.

Первоначально стандарт 802.1x задумывался для того, чтобы обеспечить аутентификацию пользователей на канальном уровне в коммутируемых проводных сетях.

Алгоритмы аутентификации стандарта 802.11 могут обеспечить клиента динамическими, ориентированными на пользователя ключами. Но тот ключ, который создается в процессе аутентификации, не является ключом, используемым для шифрования фреймов или проверки целостности сообщений. В стандарте WPA для получения всех ключей используется так называемый *мастер-ключ* (Master Key).

В стандарте 802.1x аутентификация пользователей на канальном уровне выполняется по протоколу EAP, который был разработан Группой по проблемам проектирования Internet (IETF). Протокол EAP - это замена протокола CHAP (Challenge Handshake Authentication Protocol - протокол взаимной аутентификации), который применяется в PPP (Point to Point Protocol - протокол соединения "точка-точка"), он предназначен для использования в локальных сетях. Спецификация EAPOL определяет, как фреймы EAP инкапсулируются во фреймы 802.3, 802.5 и 802.11. Обмен фреймами между объектами, определенными в стандарте 802.1x, схематично изображен на рис. 5.7.

EAP является "обобщенным" протоколом в системе аутентификации, авторизации и учета (Authentication, Authorization, and Accounting - AAA), обеспечивающим работу разнообразных методов аутентификации. AAA-клиент (сервер доступа в терминологии AAA, в беспроводной сети представлен точкой радиодоступа), поддерживающий EAP, может не понимать конкретных методов, используемых абонентом и сетью в процессе аутентификации. Сервер доступа туннелирует сообщения протокола аутентификации, циркулирующие между абонентом и сервером аутентификации. Сервер доступа интересуется лишь факт начала и окончания процесса аутентификации.



Рис. 5.7. Механизм аутентификации в 802.1x/EAP

Наглядно уровни архитектуры 802.1x показаны на рис. 5.8. Здесь в качестве механизма обеспечения конфиденциальности и целостности данных выступают стандарты шифрования WPA и WPA2.

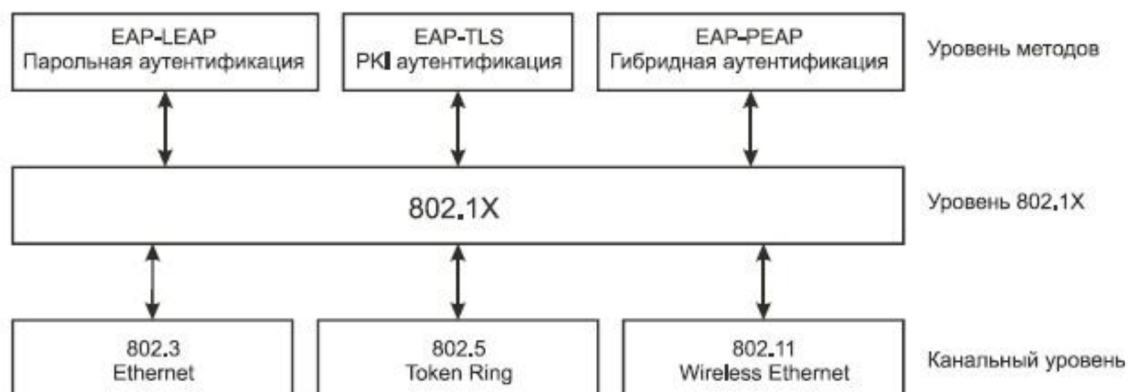


Рис. 5.8. Уровни архитектуры 802.1x

**Список контрольных вопросов
к лабораторной работе
Беспроводные сети Wi-Fi**

1. Перечислите и охарактеризуйте основные элементы беспроводной сети.
2. Опишите стандарт IEEE 802.11 и его варианты (a, b, g, n).
3. Назначение, ограничения, достоинства и недостатки режима работы беспроводной сети Ad Hoc.
4. Назначение, достоинства и недостатки инфраструктурного режима работы беспроводной сети.
5. Назначение, ограничения, достоинства и недостатки режимов работы беспроводной сети WDS и WDS with AP.
6. Структура и характеристики типичной офисной беспроводной сети.
7. Особенности организации беспроводной связи между удаленными локальными сетями (Правила применения радиочастотного спектра в России приведены в статье 22 "Регулирование использования радиочастотного спектра" Федерального закона "О связи" в редакции от 09.02.2007 № 14-ФЗ. См. отдельный файл)
8. Аутентификация и шифрование в беспроводных сетях. Стандарт IEEE 802.11 сети с традиционной безопасностью (WEP).
9. Аутентификация и шифрование в беспроводных сетях. Спецификация WPA.
10. Аутентификация и шифрование в беспроводных сетях. Стандарт сети 802.11i с повышенной безопасностью (WPA2).
11. Аутентификация и шифрование в беспроводных сетях. Стандарт 802.1x/EAP (Enterprise-режим).

**ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ОТЧЕТА
ПО ЛАБОРАТОРНОЙ РАБОТЕ**

Отчет по лабораторной работе должен содержать:

1. Титульный лист (см. образец).
2. Заполненную форму отчета (см. п. 6 задания). Чертежи локальных сетей с настройками.
3. Письменный ответ на указанный преподавателем контрольный вопрос.

Отчет предоставляется преподавателю в письменной/печатной форме.

Образец титульного листа отчета

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Самарский государственный аэрокосмический университет
имени академика С.П. Королева
(национальный исследовательский университет)»

Факультет информатики
Кафедра технической кибернетики

ОТЧЕТ

по лабораторной работе по дисциплине
Компьютерные телекоммуникации
на тему

Беспроводные сети Wi-Fi

Выполнили студенты 63X группы Фамилия И.О.
Фамилия И.О.
Фамилия И.О.

Беспроводные сети Wi-Fi

Дополнительные материалы:

Приложение Б. Правила использования радиочастотного спектра

В соответствии со статьей 22 **"Регулирование использования радиочастотного спектра"** Федерального закона "О связи" в редакции от 09.02.2007 N 14-ФЗ:

Выдержка из статьи 22 ФЗ "О связи"

4. Использование в Российской Федерации радиочастотного спектра осуществляется в соответствии со следующими принципами: разрешительный порядок доступа пользователей к радиочастотному спектру; платность использования радиочастотного спектра; недопустимость бессрочного выделения полос радиочастот, присвоения радиочастот или радиочастотных каналов; прозрачность и открытость процедур распределения и использования радиочастотного спектра.

5. Средства связи, иные радиоэлектронные средства и высокочастотные устройства, являющиеся источниками электромагнитного излучения, подлежат регистрации. Перечень радиоэлектронных средств и высокочастотных устройств, подлежащих регистрации, и порядок их регистрации определяются Правительством Российской Федерации. Радиоэлектронные средства, используемые для индивидуального приема программ телевизионного вещания и радиовещания, сигналов персональных радиовыводов (радиопейджеры), электронные изделия бытового назначения и средства персональной радионавигации, не содержащие радиоизлучающих устройств, используются на территории Российской Федерации с учетом ограничений, предусмотренных законодательством Российской Федерации, и регистрации не подлежат. Использование без регистрации радиоэлектронных средств и высокочастотных устройств, подлежащих регистрации в соответствии с правилами настоящей статьи, не допускается.

В соответствии со статьей 24 **"Выделение полос радиочастот и присвоение (назначение) радиочастот или радиочастотных каналов"**, право на использование радиочастотного спектра предоставляется посредством выделения полос радиочастот и присвоения радиочастот или радиочастотных каналов. Использование радиочастотного спектра без соответствующего разрешения не допускается.

Присвоение радиочастот или радиочастотных каналов для радиоэлектронных средств (РЭС) гражданского назначения осуществляется Федеральным агентством связи (Россвязь) по заключению радиочастотной службы при Россвязи на основании заявлений граждан Российской Федерации или заявлений российских юридических лиц.

Порядок получения разрешений для беспроводных сетей в диапазоне 2,4 ГГц в России

1. Внутриофисные системы беспроводной передачи данных

Порядок использования полосы радиочастот 2400-2483,5 МГц для внутриофисных систем передачи данных определен Решением ГКРЧ (Государственной Комиссии по радиочастотам) № 04-03-04-003 от 6 декабря 2004 г. Это Решение значительно упростило процедуру получения разрешительных документов и определило возможность использования

внутриофисного оборудования Wi-Fi без оформления разрешений на использование радиочастот.

Выдержка из Решения ГКРЧ № 04-03-04-003 от 6 декабря 2004 г.

3. Разрешить гражданам Российской Федерации и российским юридическим лицам использование на вторичной основе радиочастот в пределах полосы радиочастот 2400-2483,5 МГц для эксплуатации внутри-офисных систем передачи данных, указанных в прилагаемом перечне (приложение № 2), на территории Российской Федерации без оформления разрешений на использование радиочастот, при выполнении следующих условий:

- эксплуатации РЭС внутриофисных систем передачи данных только внутри зданий, закрытых складских помещений и производственных территорий;
- регистрации РЭС внутриофисных систем передачи данных установленным в Российской Федерации порядком.

В приложение № 2 к Решению ГКРЧ № 04-03-04-003 включено, в частности, следующее внутриофисное оборудование D-Link:

DWL-1000AP+, DWL-1040AP+, DWL-900AP+, DWL-650+, DWL-520+, DWL-120+, DI-714P+, DI-614+, DWL-G520, DWL-G650, DWL-2100AP, DI-624, DWL-G520+, DWL-G650+, DWL-2000AP+, DI-624+, DI-724P+, DI-824VUP+, DSL-G604T, DWL-G120, DWL-G122, DWL-G510, DWL-G630, DWL-G730AP, DI-524, DWL-3200AP.

2) Уличные операторские сети беспроводной передачи данных.

Для получения разрешения на использование полосы частот 2400-2483,5 МГц (стандарты 802.11b/g) для эксплуатации РЭС этой группы применяется частично упрощенный порядок на основе Решения ГКРЧ от 25 сентября 2000 г. (протокол № 2/7). Для этих систем не требуется оформления частных решений ГКРЧ для каждого конкретного заявителя, при условии соответствия технических параметров беспроводного оборудования основным тактико-техническим характеристикам, определенным в Решении ГКРЧ №05-10-01-001 от 28 ноября 2005 года.

3) Bluetooth.

Порядок использования на территории Российской Федерации радиоэлектронных средств технологии Bluetooth, работающих в полосе частот 2400-2483,5 МГц, определен Решением ГКРЧ № 25/2 от 31.03.03.

Данное Решение ГКРЧ определяет возможность использования, приобретения и эксплуатации радиоэлектронных средств технологии Bluetooth с максимальной излучаемой мощностью не более 2,5 мВт без оформления разрешений органов государственной радиочастотной службы и без последующей регистрации этих РЭС в указанных органах.

Радиоэлектронные средства технологии Bluetooth с максимальной излучаемой мощностью не более 100 мВт разрешается использовать при условии выполнения требований Решения ГКРЧ № 04-03-04-003.

Порядок получения разрешений для беспроводных сетей в диапазоне 5 ГГц в России

В диапазоне 5 ГГц порядок назначения радиочастот одинаковый как для уличных

операторских сетей, так и для внутриофисных сетей беспроводной передачи данных.

Для получения разрешения на использование радиочастот в других диапазонах, в том числе в диапазоне 5 ГГц (стандарт 802.11a), необходимо предварительно получить частное Решение ГКРЧ.

Действующие решения ГКРЧ:

Решение ГКРЧ от 30 июля 2001 г., протокол № 11/1

Решение ГКРЧ от 23 декабря 2002 г. , протокол № 23/5

Решение ГКРЧ № 05-10-01-001 от 28 ноября 2005 г.

Ответственность

Статьи 24 "**Выделение полос радиочастот и присвоение (назначение) радиочастот или радиочастотных каналов**" и 25 "**Контроль за излучениями радиоэлектронных средств и (или) высокочастотных устройств**" Федерального закона "О связи" № 126-ФЗ в редакции от 09.02.2007 № 14-ФЗ определяют процедуры, связанные с нарушением условий, установленных при выделении полосы радиочастот и правил использования радиочастотного спектра.

Выдержка из статьи 24 ФЗ "О связи"

10. В случае выявления нарушения условий, установленных при выделении полосы радиочастот либо присвоении (назначении) радиочастоты или радиочастотного канала, разрешение на использование радиочастотного спектра пользователями радиочастотным спектром для радиоэлектронных средств гражданского назначения может быть приостановлено органом, выделившим полосу радиочастот либо присвоившим (назначившим) радиочастоту или радиочастотный канал в соответствии с пунктами 2 и 3 настоящей статьи на срок, необходимый для устранения этого нарушения, но не более чем на девяносто дней.

11. Разрешение на использование радиочастотного спектра прекращается во внесудебном порядке или срок действия такого разрешения не продлевается по следующим основаниям: заявление пользователя радиочастотным спектром; аннулирование лицензии на осуществление деятельности в области оказания услуг связи, если такая деятельность связана с использованием радиочастотного спектра; истечение срока, указанного при присвоении (назначении) радиочастоты или радиочастотного канала, если этот срок не был продлен в установленном порядке или если заблаговременно, не менее чем за тридцать дней, не была подана заявка на его продление; использование радиоэлектронных средств и (или) высокочастотных устройств в противоправных целях, наносящих вред интересам личности, общества и государства; невыполнение пользователем радиочастотным спектром условий, установленных в решении о выделении полосы радиочастот либо присвоении (назначении) радиочастоты или радиочастотного канала; невнесение пользователем радиочастотным спектром платы за его использование в течение тридцати дней со дня установленного срока платежа; ликвидация юридического лица, которому было выдано разрешение на использование радиочастотного спектра; неустранение нарушения, послужившего основанием для приостановления разрешения на использование радиочастотного спектра.

12. При наличии в документах, представленных заявителем, недостоверной или искаженной информации, повлиявшей на принятие решения о выделении полосы радиочастот либо присвоении (назначении) радиочастоты или радиочастотного канала, орган, выделивший

полосу радиочастот либо присвоивший (назначивший) радиочастоту или радиочастотный канал, вправе обратиться в суд с требованием о прекращении или непродлении срока действия разрешения на использование радиочастотного спектра.

13. При прекращении или приостановлении разрешения на использование радиочастотного спектра плата, внесенная за его использование, не возвращается.

Выдержка из статьи 25 ФЗ "О связи"

1. Контроль за излучениями радиоэлектронных средств и (или) высокочастотных устройств (радиоконтроль) осуществляется в целях: проверки соблюдения пользователем радиочастотным спектром правил его использования; выявления неразрешенных для использования радиоэлектронных средств и прекращения их работы; выявления источников радиопомех; выявления нарушения порядка и правил использования радиочастотного спектра, национальных стандартов, требований к параметрам излучения (приема) радиоэлектронных средств и (или) высокочастотных устройств; обеспечения электромагнитной совместимости; обеспечения эксплуатационной готовности радиочастотного спектра.

2. Радиоконтроль является составной частью государственного управления использованием радиочастотного спектра и международно-правовой защиты присвоения (назначения) радиочастот или радиочастотных каналов. Радиоконтроль за радиоэлектронными средствами гражданского назначения осуществляется радиочастотной службой. Порядок осуществления радиоконтроля определяется Правительством Российской Федерации.

В процессе радиоконтроля для изучения параметров излучений радиоэлектронных средств и (или) высокочастотных устройств, подтверждения нарушения установленных правил использования радиочастотного спектра может проводиться запись сигналов контролируемых источников излучений.

Такая запись может служить только в качестве доказательства нарушения порядка использования радиочастотного спектра и подлежит уничтожению в порядке, установленном законодательством Российской Федерации.

Использование такой записи в иных целях не допускается, и виновные в таком использовании лица несут установленную законодательством Российской Федерации ответственность за нарушение неприкосновенности частной жизни, личной, семейной, коммерческой и иной охраняемой законом тайны.

В соответствии с постановлением Правительства РФ от 30 июня 2004 г. № 318 контроль за излучением радиоэлектронных средств осуществляется Федеральной службой по надзору в сфере связи (Россвязьнадзор), территориальными органами Россвязьнадзора и их структурными подразделениями на основании Постановления Правительства РФ от 1 апреля 2005 г. № 175 "Об утверждении правил осуществления радиоконтроля в Российской Федерации".

Согласно статье 68 ФЗ "О связи" **"Ответственность за нарушение законодательства Российской Федерации в области связи"** в случаях и в порядке, которые установлены законодательством Российской Федерации, лица, нарушившие законодательство Российской Федерации в области связи, несут уголовную, административную и гражданско-правовую ответственность.

2011 г.

Дополнение (www.dlink.ru FAQ):

Вопрос: Каков порядок использования частоты 5 ГГц в России ?

Ответ:

В соответствии с действующим законодательством, регламентирующим порядок использования радиочастотного ресурса в России, можно выделить два типа оборудования беспроводного доступа. Для каждой из групп характерны свои особенности использования радиочастотного ресурса в полосе частот 5150-5350 МГц и 5650-6425 МГц и свой порядок получения разрешительных документов.

Внутриофисные системы беспроводной передачи данных:

1. Решение ГКРЧ от 7 мая 2007 г. № 07-20-03-001 "О выделении полос радиочастот устройствам малого радиуса действия"
2. Решение ГКРЧ от 15 декабря 2009 г. № 09-05-09 "О внесении изменений в решение ГКРЧ от 7 мая 2007 г. № 07-20-03-001 «О выделении полос радиочастот устройствам малого радиуса действия»"

Данные Решения ГКРЧ позволяют использовать оборудование беспроводных локальных сетей малого радиуса действия стандартов 802.11a, 802.11n внутри закрытых помещений в диапазоне частот 5150-5250 МГц без оформления отдельных решений ГКРЧ и разрешений на использование радиочастот или радиочастотных каналов. При этом пользователи должны осуществить регистрацию своих беспроводных устройств в установленном в Российской Федерации порядке.

Уличные сети беспроводной передачи данных:

1. Решение ГКРЧ от 26.09.2005 г. № 05-08-01-001 "О результатах исследований по определению условий совместного использования полосы частот 5725-6425 МГц радиоэлектронными средствами фиксированной спутниковой и фиксированной служб"
2. Решение ГКРЧ от 28 ноября 2005 г. № 05-10-01-001 "Об использовании полос радиочастот радиоэлектронными средствами фиксированного беспроводного доступа"
3. Решение ГКРЧ от 15 декабря 2009 г. № 09-05-03 "Об использовании полос радиочастот 5150-5350 МГц и 5650-6425 МГц радиоэлектронными средствами фиксированного беспроводного доступа"

Данные Решения ГКРЧ требуют получения в установленном порядке разрешения на использование радиочастот или радиочастотных каналов на основании заключения экспертизы о возможности использования заявленных РЭС и их электромагнитной совместимости (ЭМС) с действующими и планируемыми для использования РЭС. Также необходимо осуществлять регистрацию РЭС фиксированного беспроводного доступа в установленном порядке.

Вопрос: Каков порядок использования частоты 2,4 ГГц в России ?

Ответ:

В соответствии с действующим законодательством, регламентирующим порядок использования радиочастотного ресурса в России, можно выделить три типа оборудования беспроводного доступа. Для каждой из групп характерны свои особенности использования радиочастотного ресурса в полосе частот 2400-2483,5 МГц и свой порядок получения разрешительных документов.

1. Внутриофисные системы беспроводной передачи данных:

1. Решение ГКРЧ от 7 мая 2007 г. № 07-20-03-001 "О выделении полос радиочастот устройствам малого радиуса действия"
2. Решение ГКРЧ от 15 декабря 2009 г. № 09-05-09 "О внесении изменений в решение ГКРЧ от 7 мая 2007 г. № 07-20-03-001 «О выделении полос радиочастот устройствам малого радиуса действия»"

Данные Решения ГКРЧ позволяют использовать оборудование беспроводных локальных сетей малого радиуса действия стандартов 802.11b, 802.11g, 802.11n внутри закрытых помещений в диапазоне частот 2400-2483,5 МГц без оформления отдельных решений ГКРЧ и разрешений на использование радиочастот или радиочастотных каналов. При этом пользователи должны осуществить регистрацию своих беспроводных устройств в установленном в Российской Федерации порядке.

2. Уличные операторские сети беспроводной передачи данных:

1. Решение ГКРЧ от 25 сентября 2000 г. (протокол № 2/7), (приложение)
2. Решение ГКРЧ от 28 ноября 2005 г. № 05-10-01-001

Данные Решения ГКРЧ требуют получения в установленном порядке разрешения на использование радиочастот или радиочастотных каналов на основании заключения экспертизы о возможности использования заявленных РЭС и их электромагнитной совместимости (ЭМС) с действующими и планируемыми для использования РЭС. Также необходимо осуществлять регистрацию РЭС фиксированного беспроводного доступа в установленном порядке.

3. Bluetooth:

1. Решение ГКРЧ от 7 мая 2007 г. № 07-20-03-001 "О выделении полос радиочастот устройствам малого радиуса действия"
2. Решение ГКРЧ от 15 декабря 2009 г. № 09-05-09 "О внесении изменений в решение ГКРЧ от 7 мая 2007 г. № 07-20-03-001 «О выделении полос радиочастот устройствам малого радиуса действия»"

Для Bluetooth действует безлицензионный порядок использования.