

Оглавление.....	3
Введение.....	5
Раздел 1. Интерфейс Cisco Packet Tracer.....	6
1.1. Главное окно Cisco Packet Tracer.....	6
1.2. Оборудование и линии связи в Cisco Packet Tracer.....	8
1.3. Физическая комплектация оборудования.....	11
Контрольные вопросы.....	14
Раздел 2. Режим симуляции.....	15
Лабораторная работа №1. Режим симуляции в Cisco Packet Tracer.....	15
Контрольные вопросы.....	21
Раздел 3. Сетевые службы.....	22
Лабораторная работа №2. Настройка сетевых сервисов.....	22
Контрольные вопросы.....	27
Раздел 4. Основные команды операционной системы Cisco IOS.....	28
Лабораторная работа №3. Знакомство с командами IOS.....	30
Контрольные вопросы.....	36
Раздел 5. Статическая маршрутизация.....	37
Лабораторная работа №4. Настройка статической маршрутизации.....	37
Лабораторная работа №5. Построение таблиц маршрутизации.....	41
Самостоятельная работа №1.....	42
Контрольные вопросы.....	43
Раздел 6. Динамическая маршрутизация.....	44
Лабораторная работа №6. Настройка протокола RIP.....	45
Лабораторная работа №7. Настройка протокола RIP в корпоративной сети.....	47
Самостоятельная работа №2.....	49
Лабораторная работа №8. Настройка протокола OSPF.....	50
Контрольные вопросы.....	52
Раздел 7. Служба NAT.....	53
Лабораторная работа №9. Преобразование сетевых адресов NAT.....	55
Контрольные вопросы.....	59
Раздел 8. Виртуальные локальные сети VLAN.....	60
Лабораторная работа № 10. Настройка VLAN на одном коммутаторе Cisco.....	60
Лабораторная работа № 11. Настройка VLAN на двух коммутаторах Cisco.....	66
Лабораторная работа № 12. Настройка VLAN в корпоративной сети.....	72
Самостоятельная работа №3.....	77
Контрольные вопросы.....	78
Раздел 9. Многопользовательский режим работы.....	79
Лабораторная работа № 13. Многопользовательский режим работы.....	79
Самостоятельная работа №4.....	86
Контрольные вопросы.....	87
Раздел 10. Списки управления доступом ACL (Access Control List).....	88
Лабораторная работа № 14. Списки доступа.....	92
Самостоятельная работа №5.....	94
Самостоятельная работа №6.....	95

Самостоятельная работа №7.....	96
Самостоятельная работа №8.....	97
Контрольные вопросы.....	98
Литература.....	99

Введение.

Cisco Packet Tracer - это эмулятор сети, созданный компанией Cisco. Данное приложение позволяет строить сети на разнообразном оборудовании в произвольных топологиях с поддержкой разных протоколов.

Программное решение Cisco Packet Tracer позволяет имитировать работу различных сетевых устройств: маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров, IP-телефонов и т.д. Работа с интерактивным симулятором дает ощущение настройки реальной сети, состоящей из десятков или даже сотен устройств.

Настройки, в свою очередь, зависят от характера устройств: одни можно настроить с помощью команд операционной системы Cisco IOS, другие – за счет графического веб-интерфейса, третьи – через командную строку операционной системы или графические меню.

Благодаря такому свойству Cisco Packet Tracer, как режим визуализации, пользователь может отследить перемещение данных по сети, появление и изменение параметров IP-пакетов при прохождении данных через сетевые устройства, скорость и пути перемещения IP-пакетов. Анализ событий, происходящих в сети, позволяет понять механизм ее работы и обнаружить неисправности.

Cisco Packet Tracer может быть использован не только как симулятор, но и как сетевое приложение для симулирования виртуальной сети через реальную сеть, в том числе Интернет. Пользователи разных компьютеров, независимо от их местоположения, могут работать над одной сетевой топологией, производя ее настройку или устраняя проблемы. Эта функция многопользовательского режима Cisco Packet Tracer может применяться для организации командной работы.

В Cisco Packet Tracer пользователь может симулировать построение не только логической, но и физической модели сети и, следовательно, получать навыки проектирования. Схему сети можно наложить на чертеж реально существующего здания или даже города и спроектировать всю его кабельную проводку, разместить устройства в тех или иных зданиях и помещениях с учетом физических ограничений, таких как длина и тип прокладываемого кабеля или радиус зоны покрытия беспроводной сети.

Симуляция, визуализация, многопользовательский режим и возможность проектирования делают Cisco Packet Tracer уникальным инструментом для обучения сетевым технологиям.

Раздел 1. Интерфейс Cisco Packet Tracer

1.1. Главное окно Cisco Packet Tracer

На рис.1.1. представлен интерфейс программы, разделенный на области.

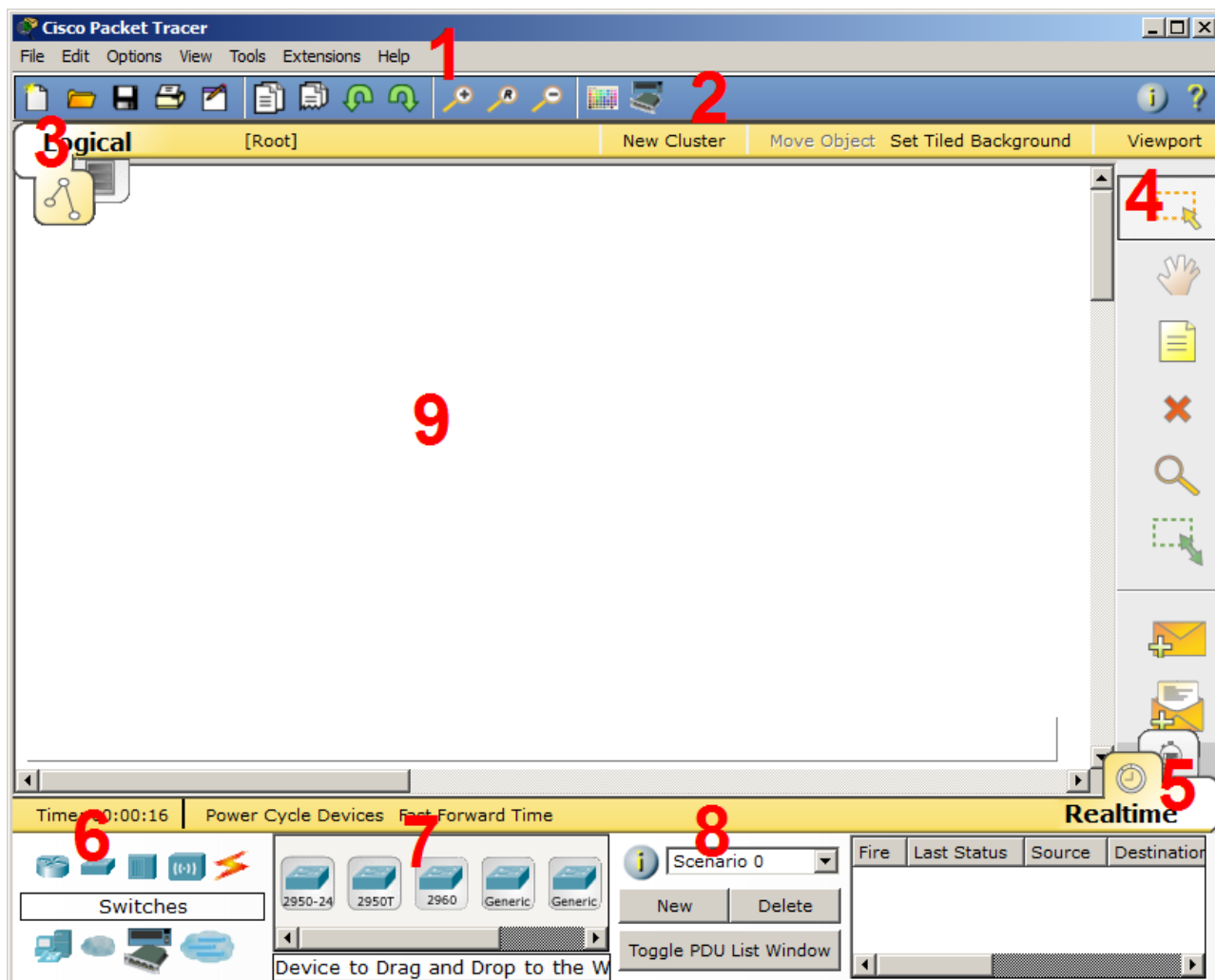


Рис.1.1. Интерфейс программы Cisco Packet Tracer.

1. Главное меню программы со следующим содержимым:
 - Файл - содержит операции открытия/сохранения документов;
 - Правка - стандартные операции "копировать/вырезать, отменить/повторить";
 - Настройки - говорит само за себя;
 - Вид - масштаб рабочей области и панели инструментов;
 - Инструменты - цветовая палитра и кастомизация конечных устройств;
 - Расширения - мастер проектов, многопользовательский режим и несколько прибулуд, которые из СРТ (так я иногда буду ласково называть Cisco Packet Tracer) могут сделать целую лабораторию;
 - Помощь - ни за что не угадаете, что там содержится;
2. Панель инструментов, часть которых просто дублирует пункты меню;

3. Переключатель между логической и физической организацией;
4. Ещё одна панель инструментов, содержит инструменты выделения, удаления, перемещения, масштабирования объектов, а так же формирование произвольных пакетов;
5. Переключатель между реальным режимом (Real-Time) и режимом симуляции;
6. Панель с группами конечных устройств и линий связи;
7. Сами конечные устройства, здесь содержатся всевозможные коммутаторы, узлы, точки доступа, проводники.
8. Панель создания пользовательских сценариев;
9. Рабочее пространство.

Пример размещения цветовых областей (рис.1.2), позволяющий например отделять визуально одну подсеть от другой.

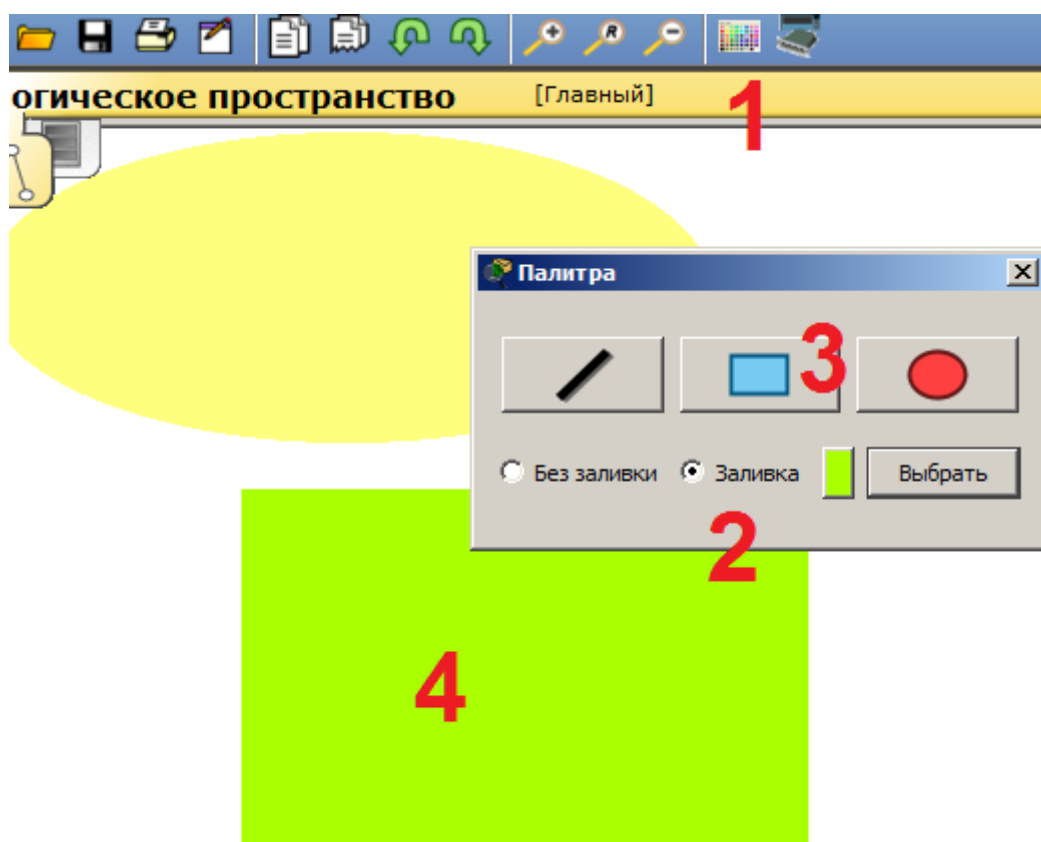


Рис.1.2. Пример размещения цветовых областей.

Для установки цветных областей выполните следующие действия:

- 1 - На панели инструментов выбираем соответствующий значок;
- 2 - Выбираем режим области "Заливка", например;
- 3 - Выбираем цвет и форму;
- 4 - Рисуем область на рабочем пространстве.

Можно также добавить подпись и перемещать/масштабировать эту область.

2.2. Оборудование и линии связи в Cisco Packet Tracer

Маршрутизаторы



Маршрутизаторы используются для поиска оптимального маршрута передачи данных на основании специальных алгоритмов маршрутизации, например выбор маршрута (пути) с наименьшим числом транзитных узлов.



Работают на сетевом уровне модели OSI.

Коммутаторы



Концентраторы



Концентратор повторяет пакет, принятый на одном порту на всех остальных портах.

Беспроводные устройства



Беспроводные технологии Wi-Fi и сети на их основе. Включает в себя точки доступа.





Линии связи








С помощью этих компонентов создаются соединения узлов в единую схему. Packet Tracer поддерживает широкий диапазон сетевых соединений (см. табл. 1.1).

Каждый тип кабеля может быть соединен лишь с определенными типами интерфейсов.

Таблица 1.1. Типы кабелей.

Тип кабеля	Описание
Консоль 	Консольное соединение может быть выполнено между ПК и маршрутизаторами или коммутаторами. Должны быть выполнены некоторые требования для работы консольного сеанса с ПК: скорость соединения с обеих сторон должна быть одинаковой, должно быть 7 бит данных (или 8 бит) для обеих сторон, контроль четности должен быть одинаковым, должно быть 1 или 2 стоповых бита (но они не обязательно должны быть одинаковыми), а поток данных может быть чем угодно для обеих сторон.
Медный прямой 	Этот тип кабеля является стандартной средой передачи Ethernet для соединения устройств, который функционирует на разных уровнях OSI. Он должен быть соединен со следующими типами портов: медный 10 Мбит/с (Ethernet), медный 100 Мбит/с (Fast Ethernet) и медный 1000 Мбит/с (Gigabit Ethernet).
Медный кроссовер 	Этот тип кабеля является средой передачи Ethernet для соединения устройств, которые функционируют на одинаковых уровнях OSI. Он может быть соединен со следующими типами портов: медный 10 Мбит/с (Ethernet), медный 100 Мбит/с (Fast Ethernet) и медный 1000 Мбит/с (Gigabit Ethernet)
Оптика 	Оптоволоконная среда используется для соединения

	между оптическими портами (100 Мбит/с или 1000 Мбит/с).
Телефонный 	Соединение через телефонную линию может быть осуществлено только между устройствами, имеющими модемные порты. Стандартное представление модемного соединения - это конечное устройство (например, ПК), дозванивающееся в сетевое облако.
Коаксиальный 	Коаксиальная среда используется для соединения между коаксиальными портами, такие как кабельный модем, соединенный с облаком Packet Tracer.
Серийный DCE  Серийный DTE 	Соединения через последовательные порты, часто используются для связей WAN. Для настройки таких соединений необходимо установить синхронизацию на стороне DCE-устройства. Синхронизация DTE выполняется по выбору. Сторону DCE можно определить по маленькой иконке “часов” рядом с портом. При выборе типа соединения Serial DCE, первое устройство, к которому применяется соединение, становится DCE-устройством, а второе - автоматически станет стороной DTE. Возможно и обратное расположение сторон, если выбран тип соединения Serial DTE.

Конечные устройства



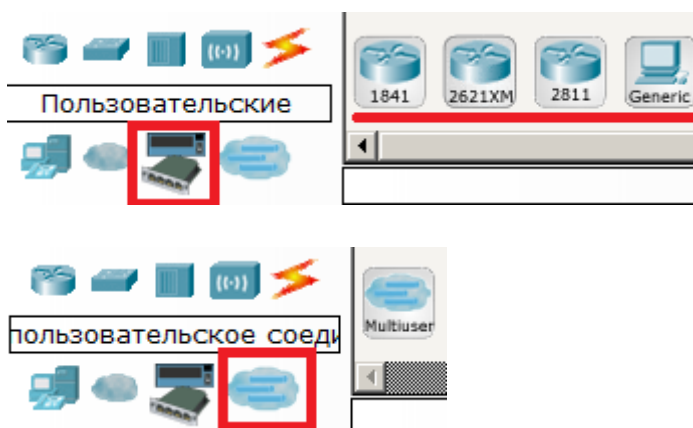
Здесь представлены конечные узлы, хосты, сервера, принтеры, телефоны и т.д.

Эмуляция Интернета



Пример эмуляция глобальной сети. Модем DSL, "облако" и т.д.

Пользовательские устройства и облако для многопользовательской работы



Устройства можно комплектовать самостоятельно. Можно создавать произвольные подключения.

2.3. Физическая комплектация оборудования

Установите в рабочем поле роутер Cisco 1841 В настройках на роутере открываем его **физическую конфигурацию** (рис.1.3).

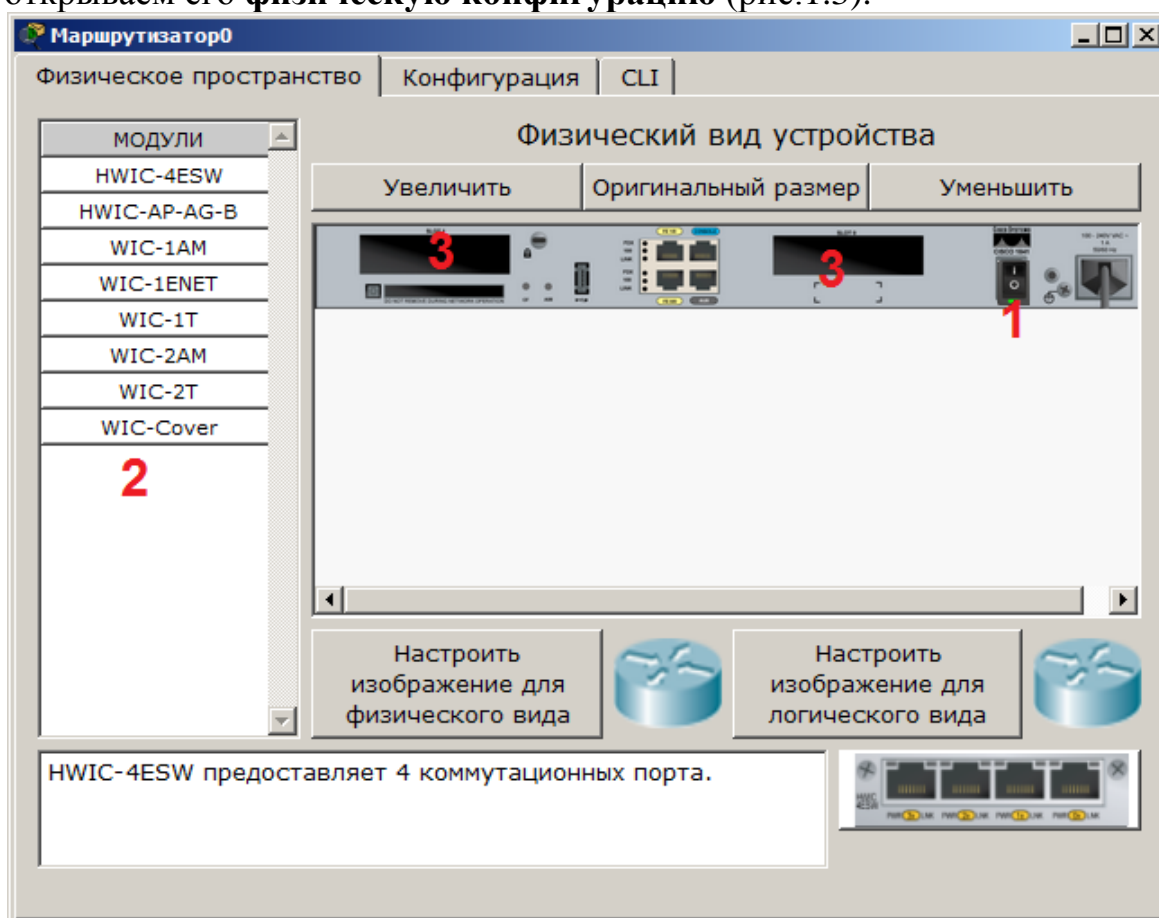


Рис.1.3. Физическая конфигурация устройства.

Слева, как мы видим, список модулей (цифра 2), которыми можно укомплектовать данный роутер. Сейчас в нем 2 пустоты (цифра 3). В них можно вложить эти модули. Разумеется, эту операцию нужно производить при выключенном питании (цифра 1).

Модули WIC (HWIC, VWIC) это платы расширения, увеличивающие функционал устройства:

:

1. **WIC** - WAN interface card. the first original models.
2. **HWIC**- high-speed wan interface card- the evolution of wic that is now in use on the ISR routers.
3. **VIC** - voice interface card, support voice only.
4. **VIC2** - evolution of the above
5. **VWIC** - voice and wan interface card. An E1/T1 card that can be user for voice or data.
6. **VWIC2** - evolution of the above

Например для компьютера есть платы, подключаемые к PCI-шине (TV-тюнеры, звуковые карты, USB-разветвители, сетевые карты), так и здесь. Вообще, устройство Cisco - это тот же системный блок со своей операционкой и многими сетевыми картами, который может делать что-то только с сетью.

Ниже предствалена информация о каждом модуле:

- **HWIC - 4ESW** - высокопроизводительный модуль с 4-мя коммутационными портами Ethernet под разъем RJ-45. Позволяет сочетать в маршрутизаторе возможности коммутатора.
- **HWIC-AP-AG-B** - это высокоскоростная WAN-карта, обеспечивающая функционал встроенной точки доступа для роутеров линейки Cisco 1800 (модульных), Cisco 2800 и Cisco 3800. Данный модуль поддерживает радиоканалы Single Band 802.11b/g или Dual Band 802.11a/b/g.
- **WIC-1AM** включает в себя два разъема RJ-11 (телефонка), используемых для подключения к базовой телефонной службе. Карта использует один порт для соединения с телефонной линией, другой может быть подключен к аналоговому телефону для звонков во время простоя модема.
- **WIC-1ENET** - это однопортовая 10 Мб/с Ethernet карта для 10BASE-T Ethernet LAN.
- **WIC-1T** предоставляет однопортовое последовательное подключение к удаленным офисам или устаревшим серийным сетевым устройствам, например SDLC концентраторам, системам сигнализации и устройствам packet over SONET (POS).
- **WIC-2AM** содержит два разъема RJ-11, используемых для подключения к базовой телефонной службе. В WIC-2AM два модемных порта, что позволяет использовать оба канала для соединения одновременно.

- **WIC-2T** - 2-портовый синхронный/асинхронный серийный сетевой модуль предоставляет гибкую поддержку многих протоколов с индивидуальной настройкой каждого порта в синхронный или асинхронный режим. Применения для синхронной/асинхронной поддержки представляют:
 - низкоскоростную агрегацию (до 128 Кб/с);
 - поддержку dial-up модемов;
 - синхронные или асинхронные соединения с портами управления другого оборудования и передачу устаревших протоколов типа Bi-sync и SDLC.
- **WIC-Cover** - стенка для WIC слота, необходима для защиты электронных компонентов и для улучшения циркуляции охлаждающего воздушного потока.

Для изменения комплектации оборудования необходимо:

отключить питание, кликнув мышью на кнопке питания, перетащить мышью модуль **4ESW** в свободный слот и включить питание. Подождать окончания загрузки роутера. В конфигурации GUI можем увидеть появившиеся 4 новых интерфейса (рис.1.4).

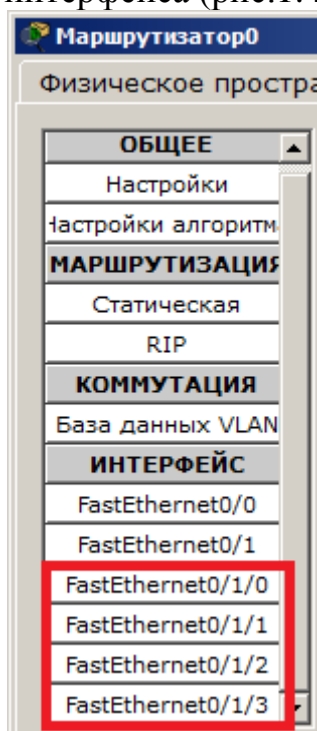


Рис.1.4. Конфигурация интерфейсов устройства.

Остальные устройства комплектуются аналогично. Добавляются новые модули Ethernet (10/100/1000), оптоволоконные разъемы нескольких типов, адаптеры беспроводной сети. На рабочий компьютер есть возможность добавить например микрофон с наушниками, жесткий диск для хранения данных.

Контрольные вопросы

1. Какая плата расширения обеспечивает функционал встроенной точки доступа?
2. Какая плата расширения предоставляет однопортовое последовательное подключение к удаленным офисам или устаревшим серийным сетевым устройствам?
3. Как называется высокопроизводительный модуль с 4-мя коммутационными портами Ethernet под разъем RJ-45?
4. Перечислите сетевые карты, позволяющие подключаться к WAN сетям?
5. Какой тип интерфейса следует выбрать при создании кластера?
6. Назовите модели коммутаторов третьего уровня?
7. Какой тип кабеля следует использовать при соединении роутеров между собой?
8. Укажите серии магистральных маршрутизаторов.
9. В каких случаях используется интерфейс SERIAL?
10. Как организовать связь двух магистральных маршрутизаторов?
11. Перечислите все возможные режимы работы программы Cisco Paket Tracer?
12. Назовите модели коммутаторов второго уровня?
13. Перечислите все типы связей, используемых в Cisco Paket Tracer и укажите их назначение.

Раздел 2. Режим симуляции.

Cisco Packet Tracer содержит инструмент для симуляции работы сети, в котором можно имитировать и симулировать состояние работы сети и практически любые сетевые события. Например можно проследить, как будет реагировать сеть в случае сбоев или например что произойдет, если отсоединить какой либо кабель или отключить питание одного из сетевых устройств.

Режим симуляции позволяет проследить структуру пакета и просмотреть, с какими параметрами пакет проходит по уровням модели OSI.

Лабораторная работа №1. Режим симуляции в Cisco Packet Tracer.

Состав сети: 4 узла, сервер, принтер и два концентратора. Концентраторы между собой соединяются кроссовым кабелем (рис.2.1).

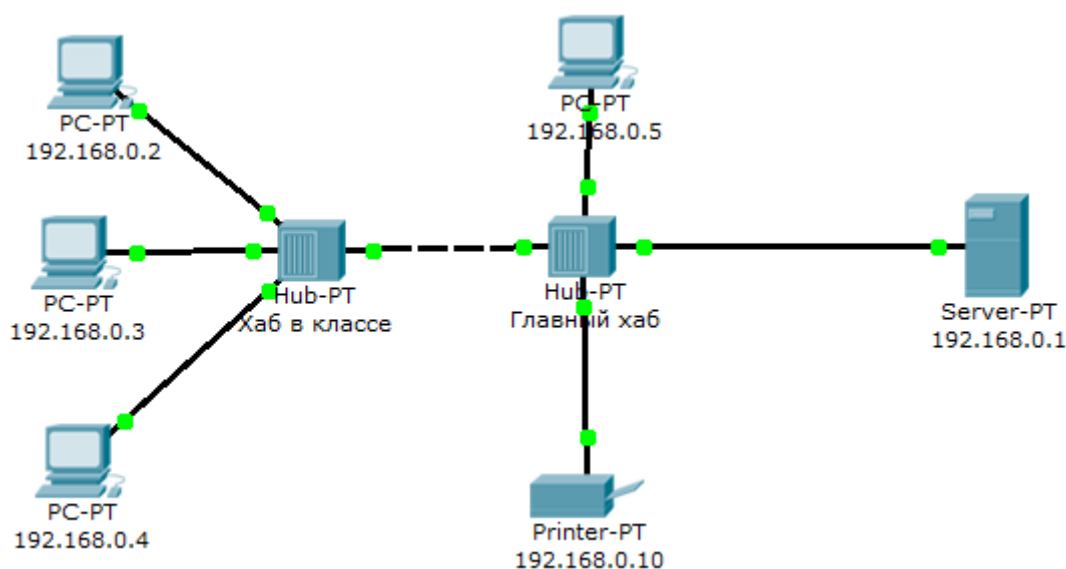


Рис.2.1. Схема сети.

Нужно перейти в режим симуляции (Shift+S), либо кликнув на иконку симуляции в правом нижнем углу рабочего пространства. Здесь мы видим окно событий, кнопка сброса (очищает список событий), управление воспроизведением и фильтр протоколов. Предложено много протоколов, но отфильтруем пока только ICMP, это исключит случайный трафик между узлами.

Для перехода к следующему событию используем кнопку "Вперёд", либо автоматика (рис.2.2).

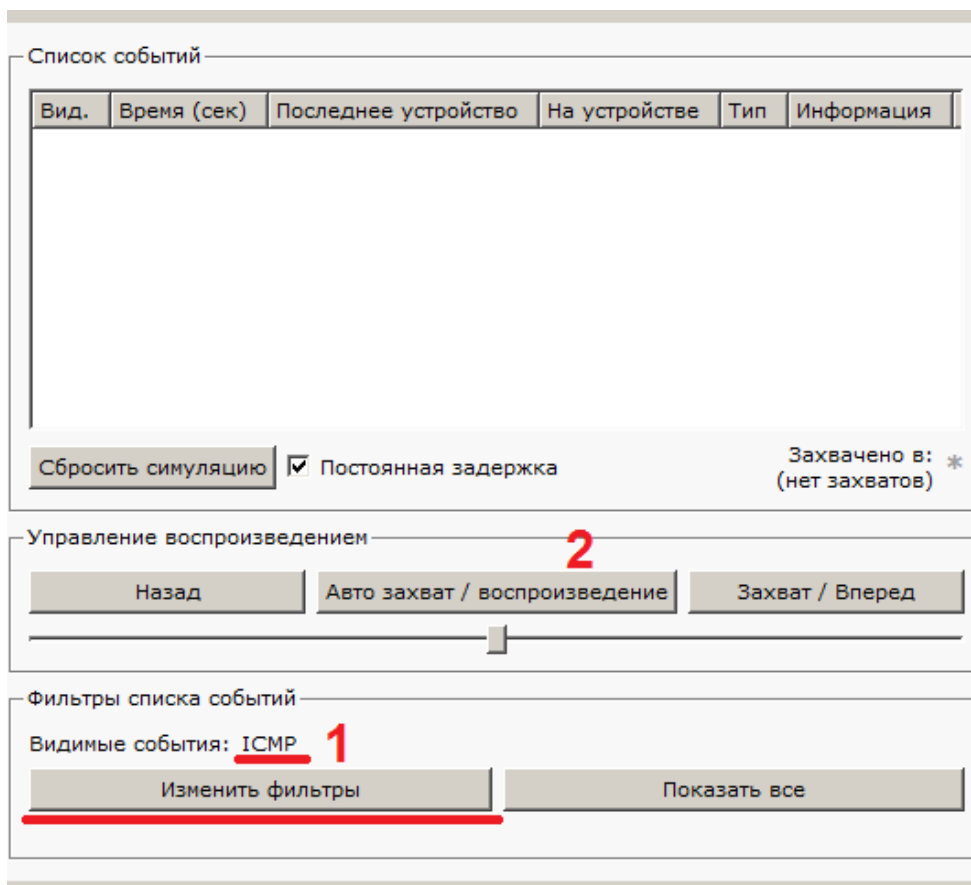


Рис.2.2. Интерфейс симулятора.

Посылаем PING-запрос.

С одного из узлов попробуем пропинговать другой узел. Выбираем далеко расположенные узлы, чтобы наглядней увидеть, как будут проходить пакеты по сети в режиме симуляции. Итак, входим на узел .4 и пошлём пинг-запрос на узел .5.

С розового узла пингуем зелёный. На розовом узле образовался пакет (конвертик), который ждёт (иконка паузы на нём). Запустить пакет в сеть можно нажав кнопку "Вперёд" в окне симуляции (рис.2.3).

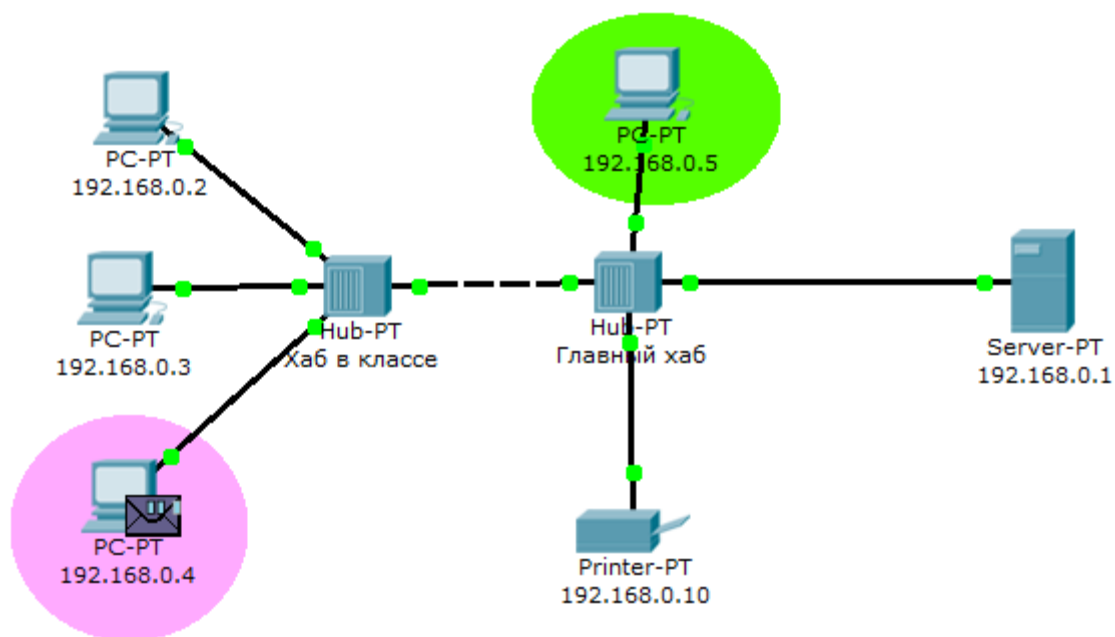


Рис.2.3. Демонстрация работы симулятора.

Так же в окне симуляции мы увидим этот пакет, отметив его тип (ICMP) и источник (192.168.0.4) – рис.2.4.

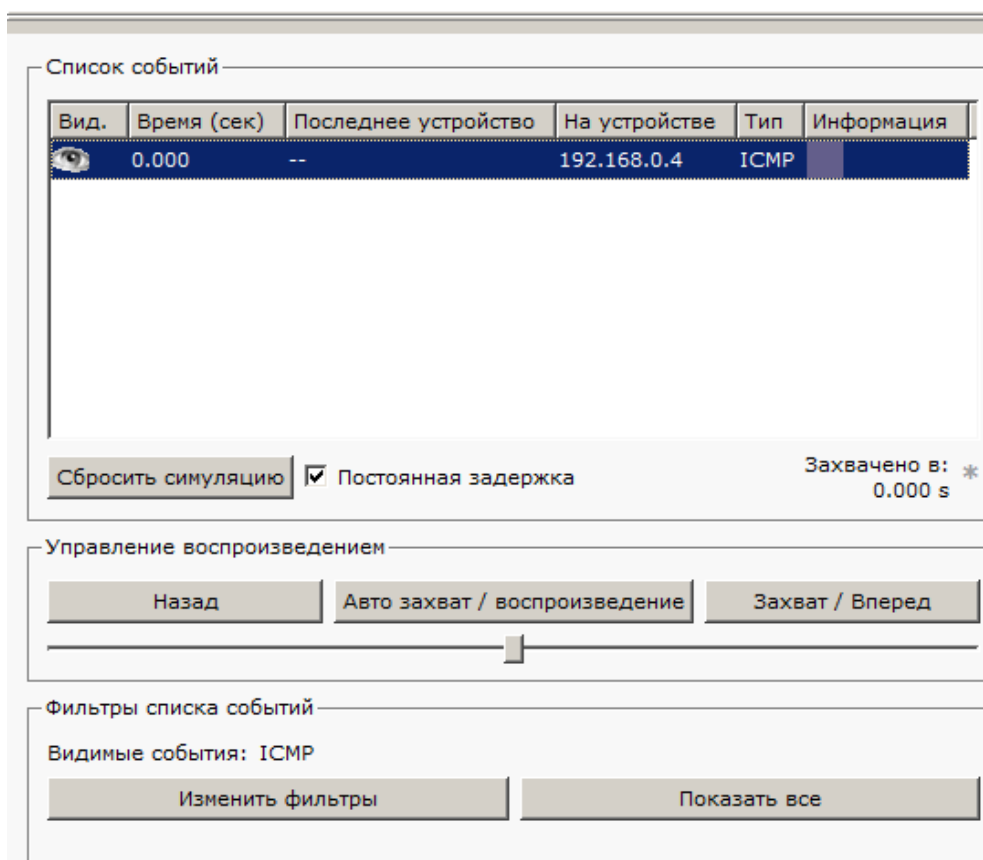


Рис.2.4. Мониторинг работы протоколов.

Клик на пакете покажет нам подробную информацию. При этом мы увидим модель OSI. Сразу видно, что на 3-ем уровне (сетевой) возник пакет на исходящем направлении, который пойдёт до второго уровня, затем до первого, на физическую среду и передастся на следующий узел (рис.2.5).

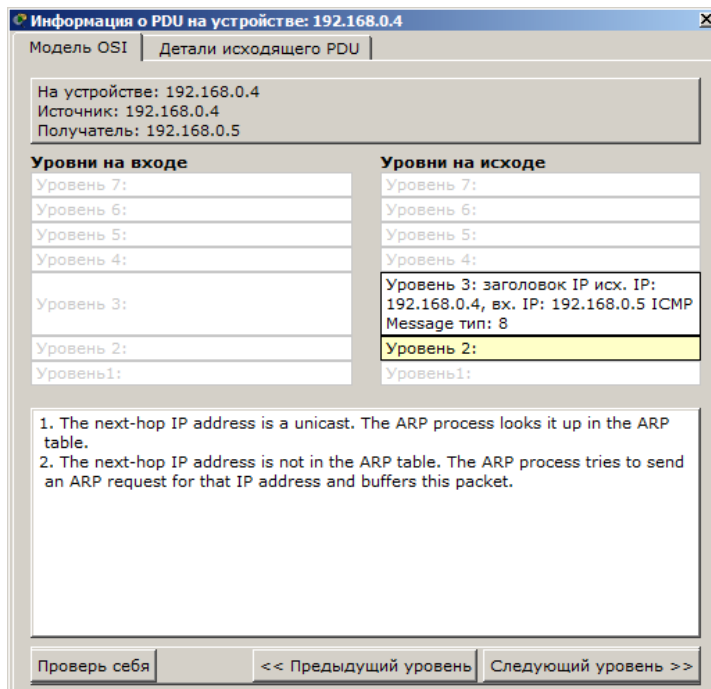


Рис.2.5. Мониторинг работы на модели OSI.

А на другой вкладке можно посмотреть структуру пакета (рис.2.6).

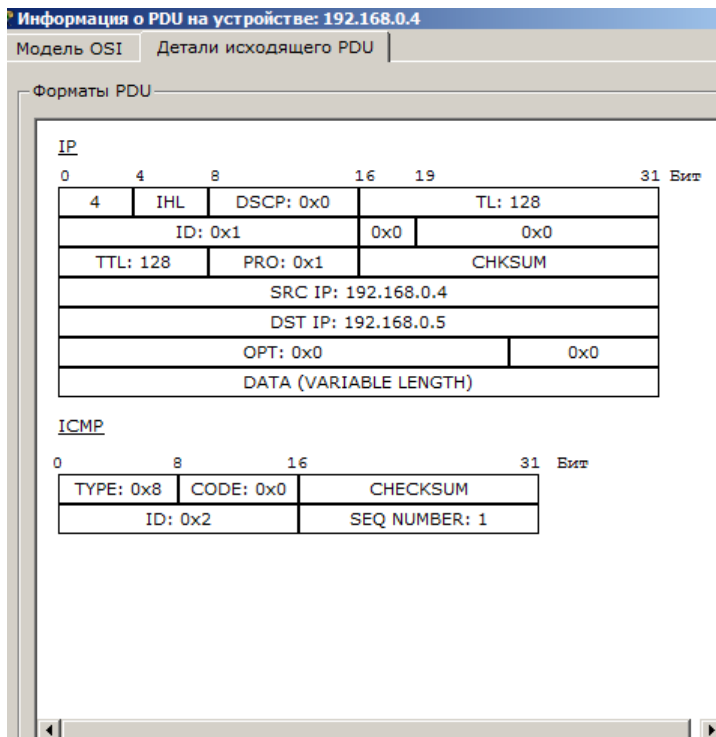


Рис.2.6. Структура пакета.

Нажмём кнопку "Вперёд". И пакет тут же двинется к концентратору. Это единственное сетевое подключение с этой стороны (2.7).

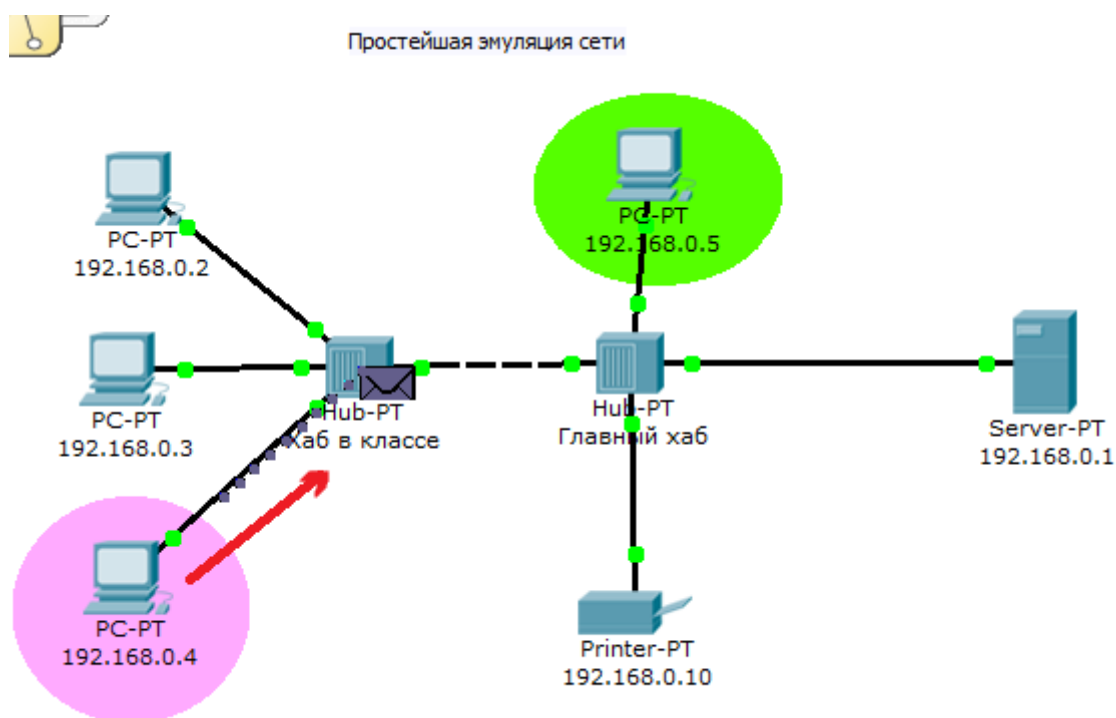


Рис.2.7. Прохождение пакета. Первый этап.

Концентратор повторяет пакет на всех остальных портах в надежде, что на одном из них есть адресат (рис.2.8)

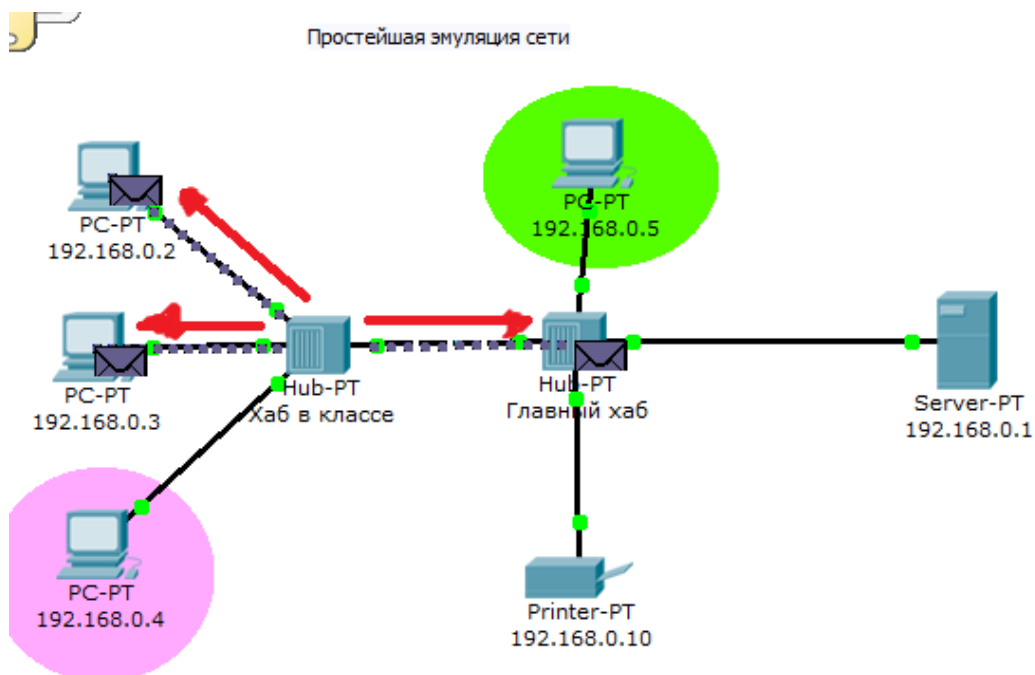


Рис.2.8. Прохождение пакета. Второй этап.

Если пакеты каким-то узлам не предназначены, они просто игнорируют их (рис.2.9).

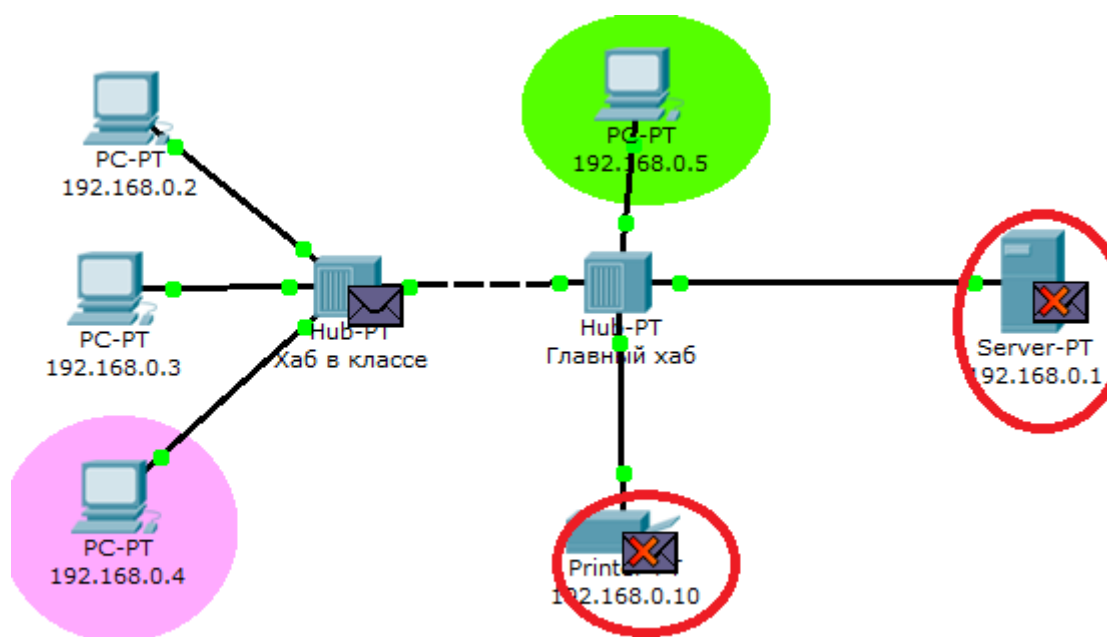


Рис.2.9. Прохождение пакета. Третий этап.

Когда пакет вернётся обратно, то увидим подтверждение соединения:

Контрольные вопросы.

1. Для чего используется режим симуляции?
2. Как просмотреть прохождение пакета по уровням модели OSI?
3. Можно ли определить причину того, что посланный в режиме симуляции пакет не дошел до адресата и на каком этапе произошел сбой работы сети?
4. Укажите в составе пакета IP адреса отправителя и получателя.
5. Как изменить фильтры списка событий?
6. Как в режиме симуляции определить, какие протоколы были задействованы в работе сети?
7. Как в режиме симуляции проследить изменение содержимого пакета при прохождении его по сети?
8. Перечислите основные возможности режима симуляции.

Раздел 3. Сетевые службы.

Эмулятор Cisco Packet Tracer позволяет проводить настройку таких сетевых сервисов, как: HTTP, DHCP, TFTP, DNS, NTP, EMAIL, FTP в составе сервера сети. Рассмотрим настройку некоторых из них.

Лабораторная работа №2. Настройка сетевых сервисов.

Создайте следующую схему сети, представленную на рис. 3.1:

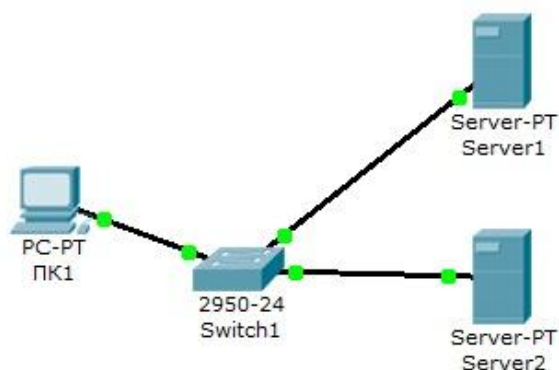


Рис.3.1. Схема сети.

Задача:

Настроить сеть следующим образом:

1 - Server1 – DNS и Web сервер;

2 - Server2 – DHCP сервер;

3 - Компьютер ПК1 получает параметры протокола TCP/IP с DHCP сервера и открывает сайт www.rambler.ru на Server1.

Этап 1.

Задайте параметры протокола TCP/IP на ПК1 и серверах.

Войдите в конфигурацию ПК1 и установите настройку IP через DHCP сервер рис.3.2.

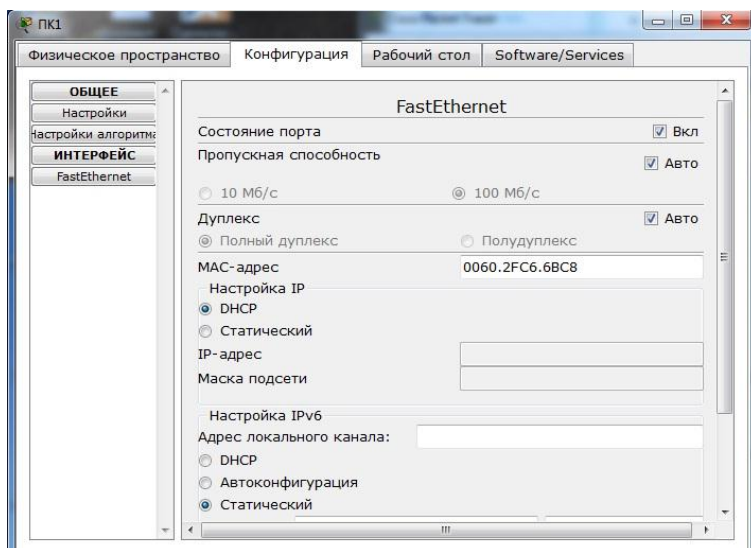


Рис. 3.2. Настройка IP на ПК1.

Задайте в конфигурации серверов следующие настройки IP:

Server1: IP адрес – 10.0.0.1, маска подсети – 255.0.0.0

Server2: IP адрес – 10.0.0.2, маска подсети – 255.0.0.0

Этап 2. Настройте службу DNS на Server1.

Для этого в конфигурации Server1 войдите на вкладку DNS и задайте две ресурсные записи в прямой зоне DNS:

1 – в ресурсной записи типа A свяжите доменное имя компьютера с его IP адресом рис.3.3 и нажмите кнопку ДОБАВИТЬ:

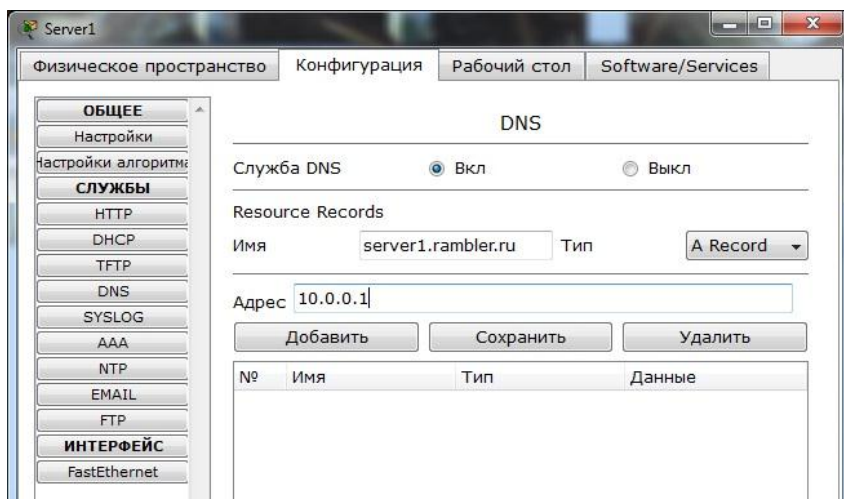


Рис.3.3. Ввод ресурсной записи типа A.

2 – в ресурсной записи типа CNAME свяжите псевдоним сайта с компьютером (рис.3.4):

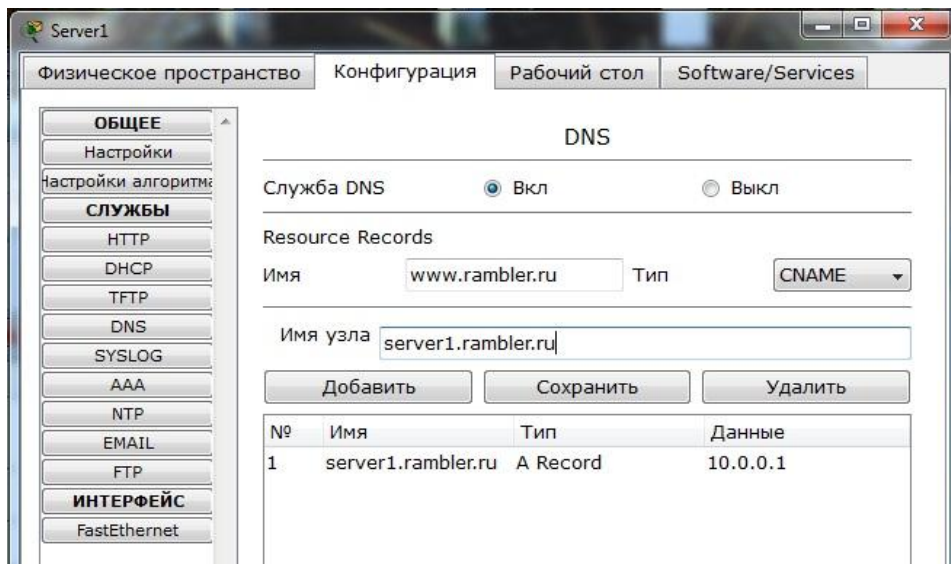


Рис.3.4. Ввод ресурсной записи типа CNAME.

В конфигурации Server1 войдите на вкладку HTTP и задайте стартовую страницу сайта WWW.RAMBLER.RU (рис.3.5):

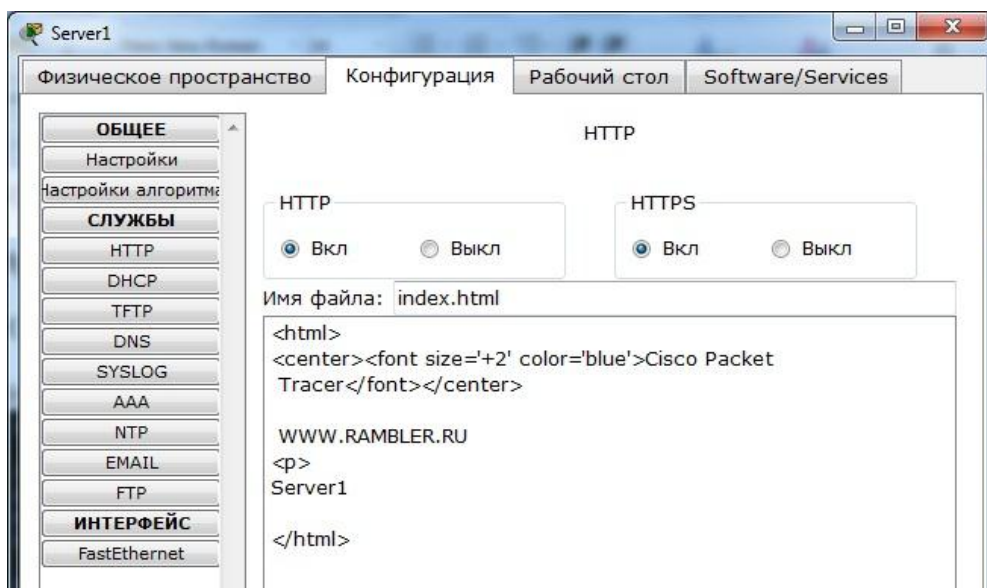


Рис.3.5. Стартовая страница сайта.

Включите командную строку на Server1 и проверьте работу службы DNS. Для проверки прямой зоны DNS сервера введите команду

SERVER>nslookup www.rambler.ru

Если все правильно, то вы получите отклик, представленный на рис.3.6, с указанием полного доменного имени DNS сервера в сети и его IP адрес.

```
SERVER>nslookup www.rambler.ru

Server: [10.0.0.1]
Address: 10.0.0.1

Non-authoritative answer:
Name:   server1.rambler.ru
Address: 10.0.0.1

Aliases:   server1.rambler.ru

SERVER>
```

Рис. 3.6. Проверка прямой зоны DNS.

Этап 3. Настройте DHCP службу на Server2.

Для этого войдите в конфигурацию Server2 и на вкладке DHCP настройте службу (рис.3.7):

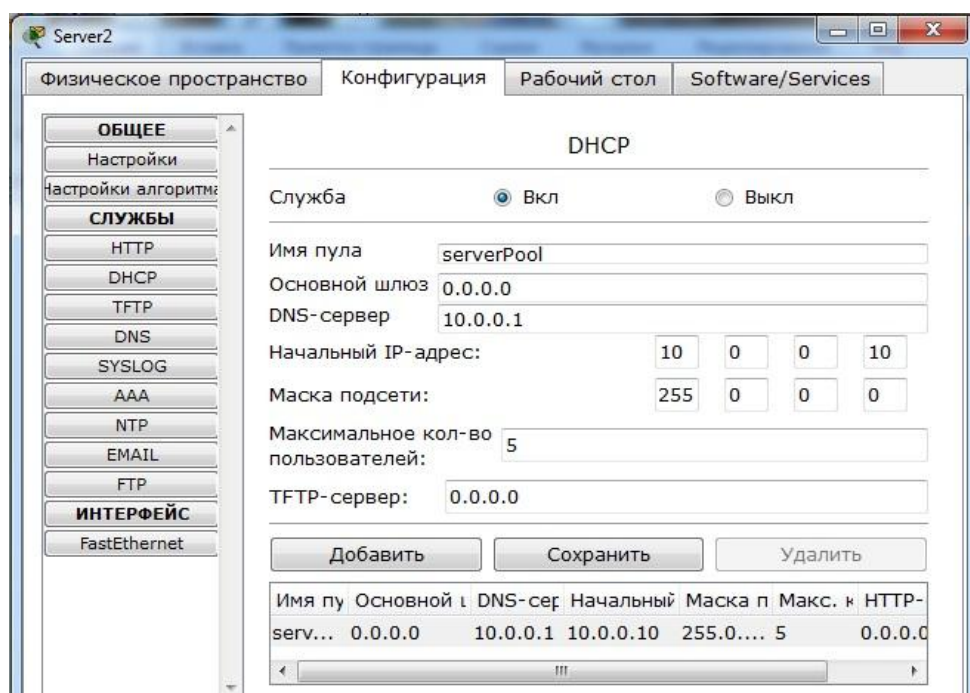


Рис. 3.7. Настройка DHCP сервера.

Этап 3. Проверка работы клиента.

Войдите в конфигурации хоста ПК1 на рабочий стол и в командной строке сконфигурируйте протокол TCP/IP.

Командой

PC>**ipconfig /release**

сбросьте старые параметры IP адреса, а командой:

PC>**ipconfig /renew**

получите новые параметры с DHCP сервера (рис.3.8):

```
PC>ipconfig /release

IP Address. . . . .: 0.0.0.0
Subnet Mask. . . . .: 0.0.0.0
Default Gateway. . . . .: 0.0.0.0
DNS Server. . . . .: 0.0.0.0

PC>ipconfig /renew

IP Address. . . . .: 10.0.0.10
Subnet Mask. . . . .: 255.0.0.0
Default Gateway. . . . .: 0.0.0.0
DNS Server. . . . .: 10.0.0.1

PC>
```

Рис.3.8. Конфигурация протокол TCP/IP клиента.

Откройте сайт WWW.RAMBLER.RU в браузере на клиенте (рис.3.9):

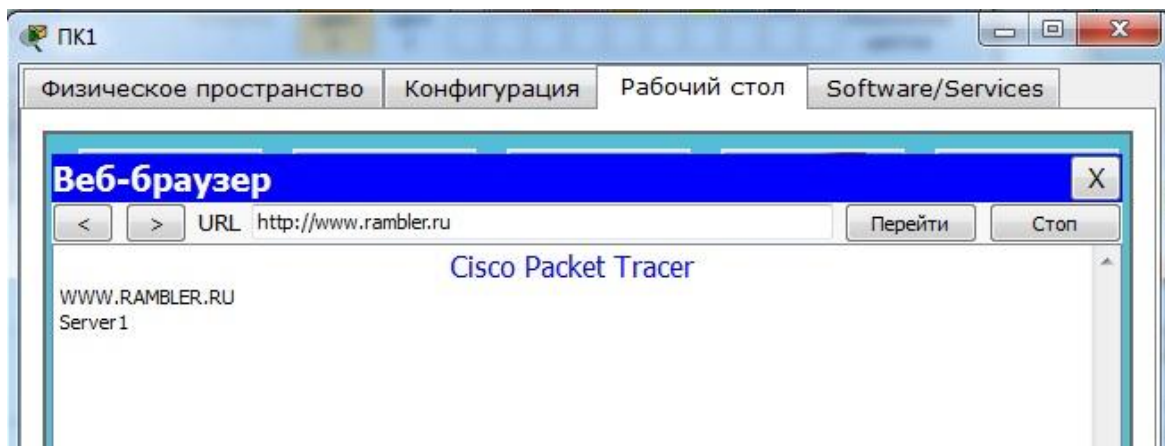


Рис.3.9. Проверка работы клиента.

Контрольные вопросы.

1. Что такое рекурсивный запрос DNS и какова схема его работы?
2. Укажите назначение типов ресурсных записей в прямой и обратной зонах DNS.
3. Как на DNS сервере настраивается пересылка пакетов на другие DNS сервера?
4. Опишите работу службы DHCP.
5. Как настраивается клиент DHCP?
6. Укажите местоположения папки с контентом Web узла и FTP сервера.
7. Как определяется состав обратных зон DNS сервера в корпоративной сети.
8. Продемонстрируйте настройку служба DNS в Cisco Paket Tracer?
9. Продемонстрируйте настройку служба DHCP в Cisco Paket Tracer?
10. Продемонстрируйте настройку служба FTP в Cisco Paket Tracer?
11. Продемонстрируйте настройку аивается WEB сервер в Cisco Paket Tracer?

Раздел 4. Основные команды операционной системы Cisco IOS.

Для настройки сетевого оборудования в вашем распоряжении имеются разнообразные команды операционной системы Cisco IOS.

При входе в сетевое устройство командная строка имеет вид:

```
Switch>
```

Команды, доступные на пользовательском уровне являются подмножеством команд, доступных в привилегированном режиме. Эти команды позволяют выводить на экран информацию без смены установок сетевого устройства.

Чтобы получить доступ к полному набору команд, необходимо сначала активизировать привилегированный режим.

Press ENTER to start.

```
Switch>
```

```
Switch> enable
```

```
Switch#
```

Выход из привилегированного режима:

```
Switch# disable
```

```
Switch>
```

О переходе в привилегированный режим будет свидетельствовать появление в командной строке приглашения в виде знака #.

Из привилегированного уровня можно получать информацию о настройках системы и получить доступ к режиму глобального конфигурирования и других специальных режимов конфигурирования, включая режимы конфигурирования интерфейса, подынтерфейса, линии, сетевого устройства, карты маршрутов и т.п.

Для выхода из системы IOS необходимо набрать на клавиатуре команду `exit` (выход):

```
Switch> exit
```

Возможна работа в следующих режимах:

- Пользовательский режим — это режим просмотра, в котором пользователь может только просматривать определённую информацию о сетевом устройстве, но не может ничего менять. В этом режиме приглашение имеет вид:

```
Switch>
```

- Привилегированный режим— поддерживает команды настройки и тестирования, детальную проверку сетевого устройства, манипуляцию с конфигурационными файлами и доступ в режим конфигурирования. В этом режиме приглашение имеет вид:

```
Switch#
```

- Режим глобального конфигурирования — реализует мощные однострочные команды, которые решают задачи конфигурирования. В том режиме приглашение имеет вид:

```
Switch(config)#
```

Команды в любом режиме IOS распознаёт по первым уникальным символам. При нажатии табуляции IOS сам дополнит команду до полного имени.

При вводе в командной строке любого режима имени команды и знака вопроса (?) на экран выводятся комментарии к команде. При вводе одного знака результатом будет список всех команд режима. На экран может выводиться много экранов строк, поэтому иногда внизу экрана будет появляться подсказка - More -. Для продолжения следует нажать enter или пробел.

Команды режима глобального конфигурирования определяют поведение системы в целом. Кроме этого, команды режима глобального конфигурирования включают команды перехода в другие режимы конфигурирования, которые используются для создания конфигураций, требующих многострочных команд. Для входа в режим глобального конфигурирования используется команда привилегированного режима `configure`. При вводе этой команды следует указать источник команд конфигурирования:

- terminal (терминал),
- memory (энергонезависимая память или файл),
- network (сервер tftp (Trivial ftp -упрощённый ftp) в сети).

По умолчанию команды вводятся с терминала консоли, например:

```
Switch(config)# (commands)
Switch(config)#exit
Switch#
```

Команды для активизации частного вида конфигурации должны предваряться командами глобального конфигурирования. Так для конфигурации интерфейса, на возможность которой указывает приглашение

```
Switch(config-if)#
```

сначала вводится глобальная команда для определения типа интерфейса и номера его порта:

```
Switch#conf t
Switch(config)#interface type port
Switch(config-if) #(commands)
Switch(config-if) #exit
Switch(config) #exit
```

Лабораторная работа №3. Знакомство с командами IOS.

Основные команды сетевого устройства

1. Войдите сетевое устройство Router1

```
Router>
```

2. Мы хотим увидеть список всех доступных команд в этом режиме. Введите команду, которая используется для просмотра всех доступных команд:

```
Router>?
```

Клавишу Enter нажимать не надо.

3. Теперь войдите в привилегированный режим

```
Router>enable
Router#
```

4. Просмотрите список доступных команд в привилегированном режиме

```
Router#?
```

5. Перейдём в режим конфигурации

```
Router#config terminal
Router(config) #
```

6. Имя хоста сетевого устройства используется для локальной идентификации. Когда вы входите в сетевое устройство, вы видите Имя хоста перед символом режима (">" или "#"). Это имя может быть использовано для определения места нахождения.

Установите "Router1" как имя вашего сетевого устройства.

```
Router(config) #hostname Router1
Router1(config) #
```

7. Пароль доступа позволяет вам контролировать доступ в привилегированный режим. Это очень важный пароль, потому что в привилегированном режиме можно вносить конфигурационные изменения. Установите пароль доступу "parol".

```
Router1 (config) #enable password parol
```

7. Давайте испытаем этот пароль. Выйдите из сетевого устройства и попытайтесь зайти в привилегированный режим.

8.

```
Router1>en  
Password:*****  
Router1#
```

Здесь знаки: ***** - это ваш ввод пароля. Эти знаки на экране не видны.

Основные Show команды.

Перейдите в пользовательский режим командой disable. Введите команду для просмотра всех доступных show команд.

```
Router1>show ?
```

1. Команда show version используется для получения типа платформы сетевого устройства, версии операционной системы, имени файла образа операционной системы, время работы системы, объём памяти, количество интерфейсов и конфигурационный регистр.

2. Просмотр времени:

```
Router1>show clock
```

3. Во флеш-памяти сетевого устройства сохраняется файл-образ операционной системы Cisco IOS. В отличие от оперативной памяти, в реальных устройствах флеш память сохраняет файл-образ даже при сбое питания.

```
Router1>show flash
```

4. ИКС сетевого устройства по умолчанию сохраняет 10 последних введенных команд

```
Router1>show history
```

5. Две команды позволят вам вернуться к командам, введенным ранее. Нажмите на стрелку вверх или <ctrl> P.

6. Две команды позволят вам перейти к следующей команде, сохранённой в буфере.

Нажмите на стрелку вниз или <ctrl> N

7. Можно увидеть список хостов и IP-Адреса всех их интерфейсов

```
Router1>show hosts
```

8. Следующая команда выведет детальную информацию о каждом интерфейсе

```
Router1>show interfaces
```

9. Следующая команда выведет информацию о каждой telnet сессии:

```
Router1>show sessions
```

10. Следующая команда показывает конфигурационные параметры терминала:

```
Router1>show terminal
```

11. Можно увидеть список всех пользователей, подсоединённых к устройству по терминальным линиям:

```
Router1>show users
```

12. Команда

```
Router1>show controllers
```

показывает состояние контроллеров интерфейсов.

13. Перейдём в привилегированный режим.

```
Router1>en
```

14. Введите команду для просмотра всех доступных show команд.

```
Router1#show ?
```

Привилегированный режим включает в себя все show команды пользовательского режима и ряд новых.

15. Посмотрим активную конфигурацию в памяти сетевого устройства. Необходим привилегированный режим. Активная конфигурация автоматически не сохраняется и будет потеряна в случае сбоя электропитания. Чтобы сохранить настройки роутера используйте следующие команды:

сохранение текущей конфигурации:

```
Router# write memory
```

Или

```
Router# copy run start
```

Просмотр сохраненной конфигурации:

```
Router# Show configuration
```

или

```
Router1#show running-config
```

В строке more, нажмите на клавишу пробел для просмотра следующей страницы информации.

16. Следующая команда позволит вам увидеть текущее состояние протоколов третьего уровня:

```
Router#show protocols
```

Введение в конфигурацию интерфейсов.

Рассмотрим команды настройки интерфейсов сетевого устройства.

На сетевом устройстве Router1 войдём в режим конфигурации:

```
Router1#conf t
```

```
Router1( config) #
```

2. Теперь мы хотим настроить Ethernet интерфейс. Для этого мы должны зайти в режим конфигурации интерфейса:

```
Router1( config) #interface FastEthernet0/0
```

```
Router1( config-if) #
```

3. Посмотрим все доступные в этом режиме команды:

```
Router1( config-if) #?
```

Для выхода в режим глобальной конфигурации наберите exit. Снова войдите в режим конфигурации интерфейса:

```
Router1( config) #int fa0/0
```

Мы использовали сокращенное имя интерфейса.

4. Для каждой команды мы можем выполнить противоположную команду, поставив перед ней слово no. Следующая команда включает этот интерфейс:

```
Router1 (config-if) #no shutdown
```

5. Добавим к интерфейсу описание:

```
Router1 (config-if) #description Ethernet interface on Router 1
```

Чтобы увидеть описание этого интерфейса, перейдите в привилегированный режим и выполните команду `show interface` :

```
Router1 (config-if) #end
```

```
Router1#show interface
```

6. Теперь присоединитесь к сетевому устройству Router 2 и поменяйте имя его хоста на Router2:

```
Router#conf t
```

```
Router (config) #hostname Router2
```

Войдём на интерфейс FastEthernet 0/0:

```
Router2 (config) #interface fa0/0
```

Включите интерфейс:

```
Router2 (config-if) #no shutdown
```

Теперь, когда интерфейсы на двух концах нашего Ethernet соединения включены на экране появится сообщение о смене состояния интерфейса на активное.

7. Перейдём к конфигурации последовательных интерфейсов. Зайдём на Router1.

Проверим, каким устройством выступает наш маршрутизатор для последовательной линии связи: окончательным устройством DTE (data terminal equipment), либо устройством связи DCE (data circuit):

```
Router1#show controllers fa0/1
```

Если видим сообщение:

```
DCE cable
```

то наш маршрутизатор является устройством связи и он должен задавать частоту синхронизации тактовых импульсов, используемых при передаче данных. Частота берётся из определённого ряда частот.


```
Router1#conf t  
Router1 (config) #int fa0/1  
Router1 (config-if) #clock rate ?
```

Выберем частоту 64000

```
Router1 (config-if) #clock rate 64000
```

и включаем интерфейс

```
Router1 (config-if) #no shut
```

Контрольные вопросы.

1. Какой командой можно посмотреть текущие настройки роутера?
2. Какими командами настраивается сетевой интерфейс роутера.
3. Как просмотреть конфигурационные настройки коммутатора?
4. Как определить распределение VLANов по портам коммутатора?
5. Перечислите основные режимы конфигурации при настройке коммутатора.
6. Перечислите основные режимы конфигурации при настройке роутера.
7. Как посмотреть таблицу маршрутизации на роутере?
8. Какие команды формируют таблицу маршрутизации роутера?
9. Какими командами настраиваются VLANы на коммутаторе?
10. Какими командами настраивается взаимодействие между VLANами?

Раздел 5. Статическая маршрутизация

Протоколы маршрутизации - это правила, по которым осуществляется обмен информации о путях передачи пакетов между маршрутизаторами. Протоколы характеризуются временем сходимости, потерями и масштабируемостью. В настоящее время используется несколько протоколов маршрутизации.

Одна из главных задач маршрутизатора состоит в определении наилучшего пути к заданному адресату. Маршрутизатор определяет пути (маршруты) к адресатам или из статической конфигурации, введённой администратором, или динамически на основании маршрутной информации, полученной от других маршрутизаторов. Маршрутизаторы обмениваются маршрутной информацией с помощью протоколов маршрутизации.

Маршрутизатор хранит таблицы маршрутов в оперативной памяти. Таблица маршрутов это список наилучших известных доступных маршрутов. Маршрутизатор использует эту таблицу для принятия решения куда направлять пакет.

В случае статической маршрутизации администратор вручную определяет маршруты к сетям назначения.

В случае динамической маршрутизации – маршрутизаторы следуют правилам, определяемым протоколами маршрутизации для обмена информацией о маршрутах и выбора лучшего пути.

Статические маршруты не меняются самим маршрутизатором. Динамические маршруты изменяются самим маршрутизатором автоматически при получении информации о смене маршрутов от соседних маршрутизаторов. Статическая маршрутизация потребляет мало вычислительных ресурсов и полезна в сетях, которые не имеют нескольких путей к адресату назначения. Если от маршрутизатора к маршрутизатору есть только один путь, то часто используют статическую маршрутизацию.

Лабораторная работа №4. Настройка статической маршрутизации.

Проведем настройку статической маршрутизации с помощью графических мастеров интерфейса Cisco Packet Tracer.

Создайте схему сети, представленную на рис.5.1.

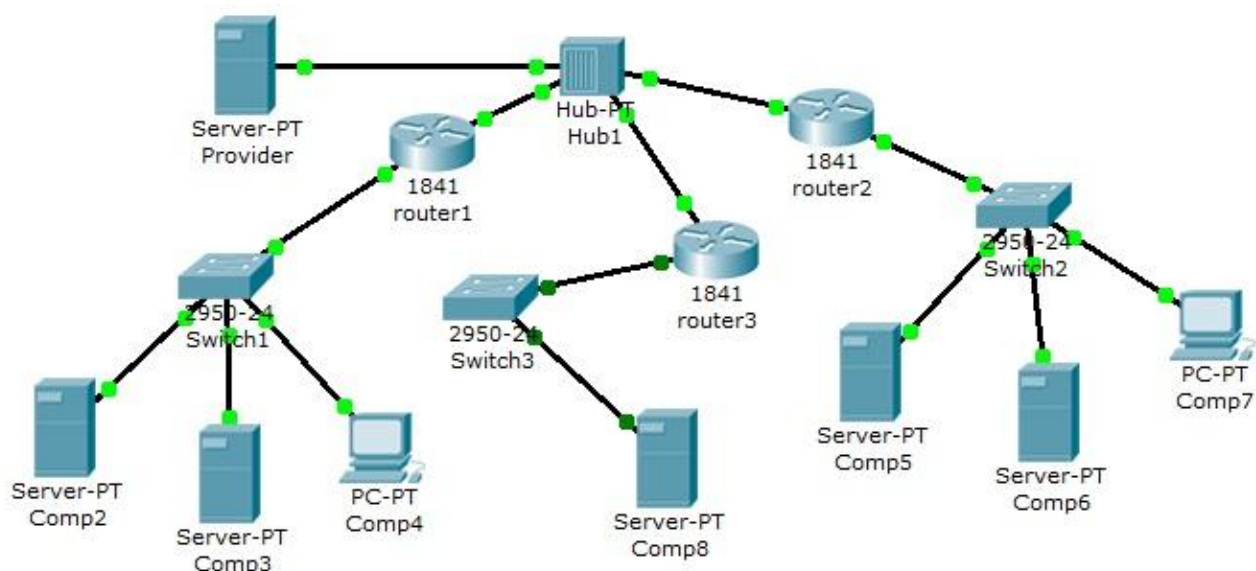


Рис.5.1. Схема сети.

На данной схеме представлена корпоративная сеть, состоящая из следующих компонентов:

Сеть 1 – на Switch1 замыкается сеть первой организации (таблица 5.1):

Таблица 5.1. Сеть первой организации.

компьютер	IP адрес	Функции
Comp2	192.168.1.2/24	DNS и HTTP сервер
Comp3	192.168.1.3/24	DHCP сервер
Comp4	Получен с DHCP сервера	Клиент сети

В данной сети на Comp2 установлен DNS и Web сервер с сайтом организации. На Comp3 установлен DHCP сервер. Компьютер Comp4 получает с DHCP сервера IP адрес, адрес DNS сервера провайдера (сервер Provider) и шлюз. Шлюз в сети – 192.168.1.1/24.

Сеть 2 – на Switch2 замыкается сеть второй организации (таблица 5.2):

Таблица 5.2. Сеть второй организации.

компьютер	IP адрес	Функции
Comp5	10.0.0.5/8	DNS и HTTP сервер
Comp6	10.0.0.6/8	DHCP сервер
Comp7	Получен с DHCP сервера	Клиент сети

В данной сети на Comp5 установлен DNS и Web сервер с сайтом организации.

На Comp4 установлен DHCP сервер. Компьютер Comp7 получает с DHCP сервера IP адрес, адрес DNS сервера провайдера (сервер Provider) и шлюз. Шлюз в сети – 10.0.0.1/8.

Сеть 3 – на Hub1 замыкается городская сеть 200.200.200.0/24. В сети установлен DNS сервер провайдера (компьютер Provider с IP адресом - 200.200.200.10/24), содержащий данные по всем сайтам сети (Comp2, Comp5, Comp8).

Сеть 4 – маршрутизатор Router3 выводит городскую сеть в интернет через коммутатор Switch3 (сеть 210.210.210.0/24). На Comp8 (IP адрес 210.210.210.8/24, шлюз 210.210.210.3/24.) установлен DNS и Web сервер с сайтом.

Маршрутизаторы имеют по два интерфейса:

Router1 – 192.168.1.1/24 и 200.200.200.1/24.

Router2 – 10.0.0.1/8 и 200.200.200.2/24.

Router3 – 210.210.210.3/24 и 200.200.200.3/24.

Задача:

1 – настроить сети организаций;

2 – настроить DNS сервер провайдера;

3 – настроить статические таблицы маршрутизации на роутерах;

4 – проверить работу сети – на каждом из компьютеров - Comp4, Comp7 и Comp8. С каждого из них должны открываться все три сайта корпоративной сети.

В предыдущих лабораторных работах рассматривалась настройка сетевых служб и DNS сервера. Приступим к настройке статической маршрутизации на роутерах. Поскольку на представленной схеме четыре сети, то таблицы маршрутизации как минимум должны содержать записи к каждой из этих сетей – т.е. четыре записи. На роутерах Cisco в таблицах маршрутизации как правило не прописываются пути к сетям, к которым подсоединены интерфейсы роутера. Поэтому на каждом роутере необходимо внести по две записи.

Настройте первый роутер.

Для этого войдите в конфигурацию маршрутизатора и в интерфейсах установите IP адрес и маску подсети. Затем в разделе МАРШРУТИЗАЦИЯ откройте вкладку СТАТИЧЕСКАЯ, внесите данные (рис.5.2) и нажмите кнопку ДОБАВИТЬ:

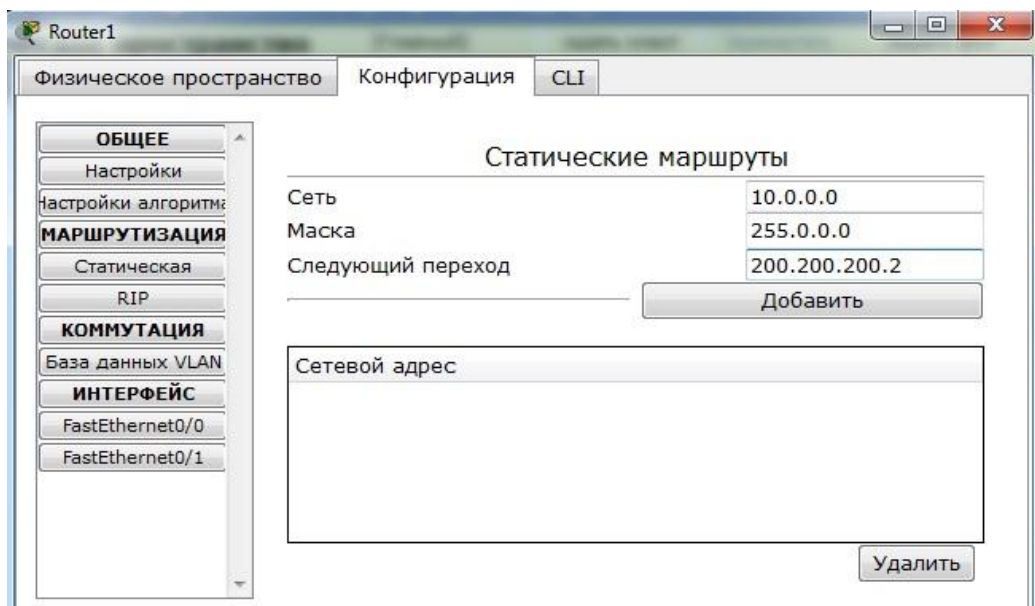


Рис.5.2. Данные для сети 10.0.0.0/8.

В результате у вас должны появиться две записи в таблице маршрутизации (рис.5.3):

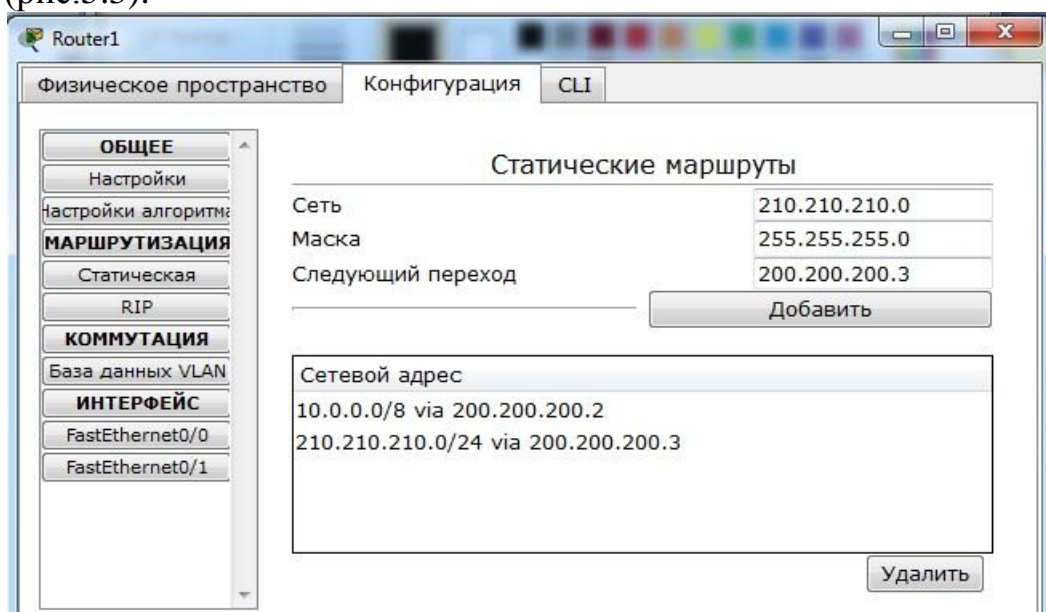


Рис.5.3. Формирование статической таблицы маршрутизации.

Чтобы посмотреть полную настройку таблицы маршрутизации, выберите в боковом графическом меню инструмент ПРОВЕРКА (пиктограмма лупы), щелкните в схеме на роутере и выберите в раскрывающемся меню пункт ТАБЛИЦА МАРШРУТИЗАЦИИ.

После настройки всех роутеров в вашей сети станут доступны IP адреса любого компьютера и вы сможете открыть любой сайт с компьютеров Comp4, Comp7 и Comp8.

Лабораторная работа №5. Построение таблиц маршрутизации.

Выполните самостоятельно следующую работу, схема сети для которой представлена на рис.5.4.

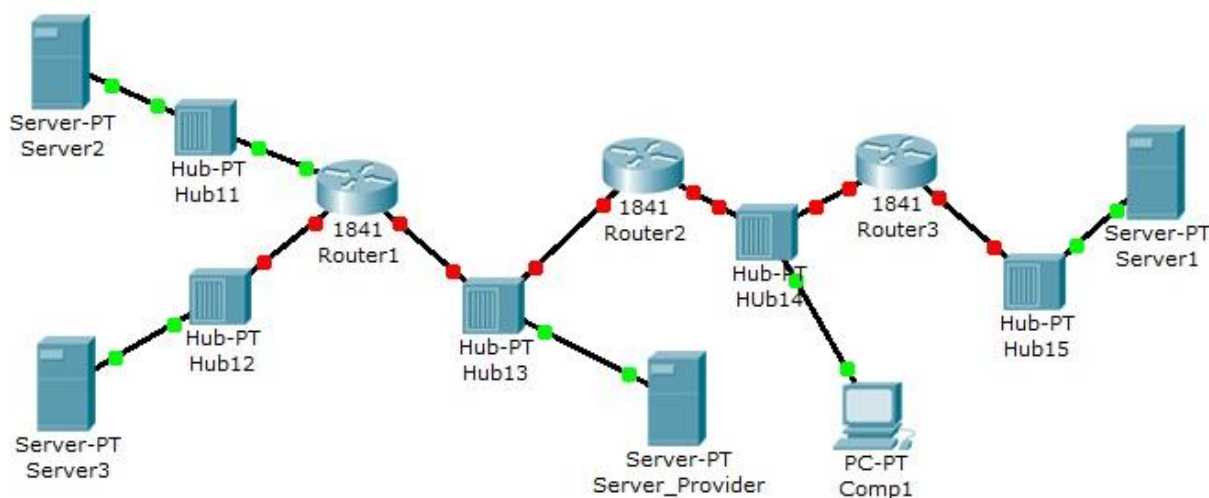


Рис.5.4. Схема сети.

Пять концентраторов представляют следующие пять сетей:

Hub11 – сеть 11.0.0.0

Hub12 – сеть 12.0.0.0

Hub13 – сеть 13.0.0.0

Hub14 – сеть 14.0.0.0

Hub15 – сеть 15.0.0.0

Router 1 имеет дополнительный сетевой интерфейс, который добавляется из модуля WIC-1ENET при выключенном роутере.

В сети три Web узла на Server1, Server2 и Server3.

Сервера и компьютер имеют произвольные IP адреса со шлюзами своих роутеров.

Интерфейсы роутеров определяются сетью на концентраторе и номером роутера.

Например для Router3: 15.0.0.3 и 14.0.0.3

Задание:

компьютер Comp1 должен открыть все три сайта на серверах корпоративной сети. В настройках Comp1 в качестве DNS сервера указан DNS сервер провайдера на Server_Provider.

Самостоятельная работа №1

Корпоративная сеть 15.0.0.0/8 разбита на десять подсетей, из них в данный момент задействовано шесть подсетей в шести разных подразделениях организации.

Состав сети:

- три маршрутизатора;
- шесть коммутаторов (по одному в каждом отделе на подсеть);
- один компьютер в каждой сети.

Задание.

- 1 – рассчитайте параметры подсетей и задайте на компьютерах IP адрес, маску и шлюз в каждой отдельной подсети;
- 2 – создайте произвольную топологию сети, соединив маршрутизаторы с подсетями в любом порядке. При этом соедините роутеры между собой произвольно – напрямую, через штатные коммутаторы подразделения или дополнительные коммутаторы;
- 3 – проверьте работоспособность корпоративной сети командой PING – все компьютеры должны быть доступны.

Контрольные вопросы.

1. В чем преимущества статической маршрутизации?
2. Дайте характеристику параметрам статической таблицы маршрутизации?
3. Какие этапы при установке устройства присущи маршрутизаторам компании Cisco, но отсутствуют у коммутаторов?
4. Какую из указанных ниже команд можно встретить в интерфейсе командной строки маршрутизатора, но не коммутатора?
 - команда cloc rate;
 - команда ip address маска адрес;
 - команда ip address dhcp;
 - команда interface vlan 1
5. Чем отличаются интерфейсы командной строки маршрутизатора и коммутатора компании Cisco?
6. Какая из указанных ниже команд не покажет настройки IP-адресов и масок в устройстве?
 - show running-config;
 - show protocol тип номер;
 - show ip interface brief;Show version
7. Перечислите основные функции маршрутизатора в соответствии с уровнями модели OSI.
8. Приведите классификацию маршрутизаторов по областям применения.
9. Перечислите основные технические характеристики маршрутизаторов.
10. Дайте характеристику основным сериям маршрутизаторов компании Cisco.
11. Приведите перечень протоколов маршрутизации и дайте им краткие характеристики.
12. Приведите перечень поддерживаемых маршрутизаторами интерфейсов для локальных и глобальных сетей и определите их назначение.
13. Приведите перечень поддерживаемых маршрутизаторами сетевых протоколов и определите их назначение.

Раздел 6. Динамическая маршрутизация.

Статическая маршрутизация не подходит для больших, сложных сетей потому, что обычно сети включают избыточные связи, многие протоколы и смешанные топологии.

Маршрутизаторы в сложных сетях должны быстро адаптироваться к изменениям топологии и выбирать лучший маршрут из многих кандидатов. IP сети имеют иерархическую структуру. С точки зрения маршрутизации сеть рассматривается как совокупность автономных систем. В автономных подсистемах больших сетей для маршрутизации на остальные автономные системы широко используются маршруты по умолчанию.

Динамическая маршрутизация может быть осуществлена с использованием одного и более протоколов. Эти протоколы часто группируются согласно того, где они используются. Протоколы для работы внутри автономных систем называют внутренними протоколами шлюзов (interior gateway protocols (IGP)), а протоколы для работы между автономными системами называют внешними протоколами шлюзов (exterior gateway protocols (EGP)). К протоколам IGP относятся RIP, RIP v2, IGRP, EIGRP, OSPF и IS-IS. Протоколы EGP3 и BGP4 относятся к EGP. Все эти протоколы могут быть разделены на два класса: дистанционно-векторные протоколы и протоколы состояния связи.

Дистанционно-векторная маршрутизация.

Маршрутизаторы используют метрики для оценки или измерения маршрутов. Когда от маршрутизатора к сети назначения существует много маршрутов, и все они используют один протокол маршрутизации, то маршрут с наименьшей метрикой рассматривается как лучший. Если используются разные протоколы маршрутизации, то для выбора маршрута используется административные расстояния, которые назначаются маршрутам операционной системой маршрутизатора. RIP использует в качестве метрики количество переходов (хопов).

Дистанционно-векторная маршрутизация базируется на алгоритме Белмана-Форда. Через определённые моменты времени маршрутизатор передаёт соседним маршрутизаторам всю свою таблицу маршрутизации. Такие простые протоколы как RIP и IGRP просто распространяют информацию о таблицах маршрутов через все интерфейсы маршрутизатора в широковещательном режиме без уточнения точного адреса конкретного соседнего маршрутизатора.

Соседний маршрутизатор, получая широковещание, сравнивает информацию со своей текущей таблицей маршрутов. В неё добавляются маршруты к новым сетям или маршруты к известным сетям с лучшей метрикой. Происходит удаление несуществующих маршрутов. Маршрутизатор добавляет свои

собственные значения к метрикам полученных маршрутов. Новая таблица маршрутизации снова распространяется по соседним маршрутизаторам

Лабораторная работа №6. Настройка протокола RIP.

Создайте схему, представленную на рис.6.1.

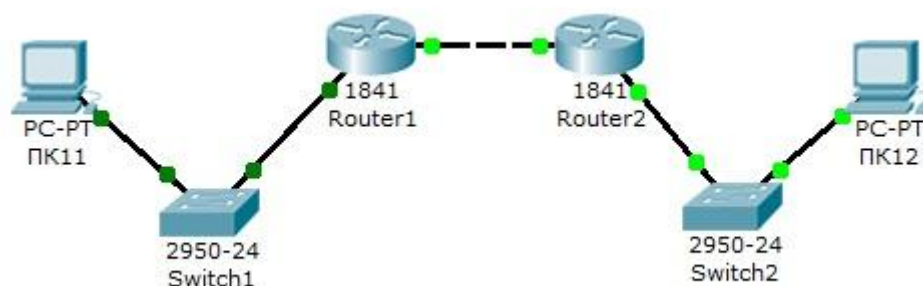


Рис.6.1. Схема сети.

На схеме представлены следующие три сети:

Switch1 – сеть 10.11.0.0/16.

Switch2 – сеть 10.12.0.0/16.

Сеть для роутеров - 10.10.0.0/16.

Введите на устройствах следующую адресацию:

Маршрутизаторы имеют по два интерфейса:

Router1 – 10.11.0.1/16 и 10.10.0.1/16.

Router2 – 10.10.0.2/16 и 10.12.0.1/16.

ПК11 - 10.11.0.11/16 .

ПК12 - 10.12.0.12/16 .

Проведем настройку протокола RIP на маршрутизаторе Router1.

Войдите в конфигурации в консоль роутера и выполните следующие настройки (при вводе команд маску подсети можно не указывать, т.к. она будет браться автоматически из настроек интерфейса роутера):

Войдите в привилегированный режим:

```
Router1>en
```

Войдите в режим конфигурации:

```
Router1>#conf t
```

Войдите в режим конфигурирования протокола RIP:

```
Router1 (config) #router rip
```

Подключите клиентскую сеть к роутеру:

Router1 (config-router) #**network 10.11.0.0**

Подключите вторую сеть к роутеру:

Router1 (config-router) #**network 10.10.0.0**

Задайте использование второй версии протокол RIP:

Router1 (config-router) #**version 2**

Выйдите из режима конфигурирования протокола RIP:

Router1 (config-router) #**exit**

Выйдите из консоли настроек:

Router1 (config) #**exit**

Сохраните настройки в память маршрутизатора:

Router1>#**write memory**

Аналогично проведите настройку протокола RIP на маршрутизаторе Router2.

Проверьте связь между компьютерами ПК11 и ПК12 командой **ping**.

Если связь есть – все настройки сделаны верно.

Лабораторная работа №7. Настройка протокола RIP в корпоративной сети.

Создайте схему, представленную на рис.6.2.

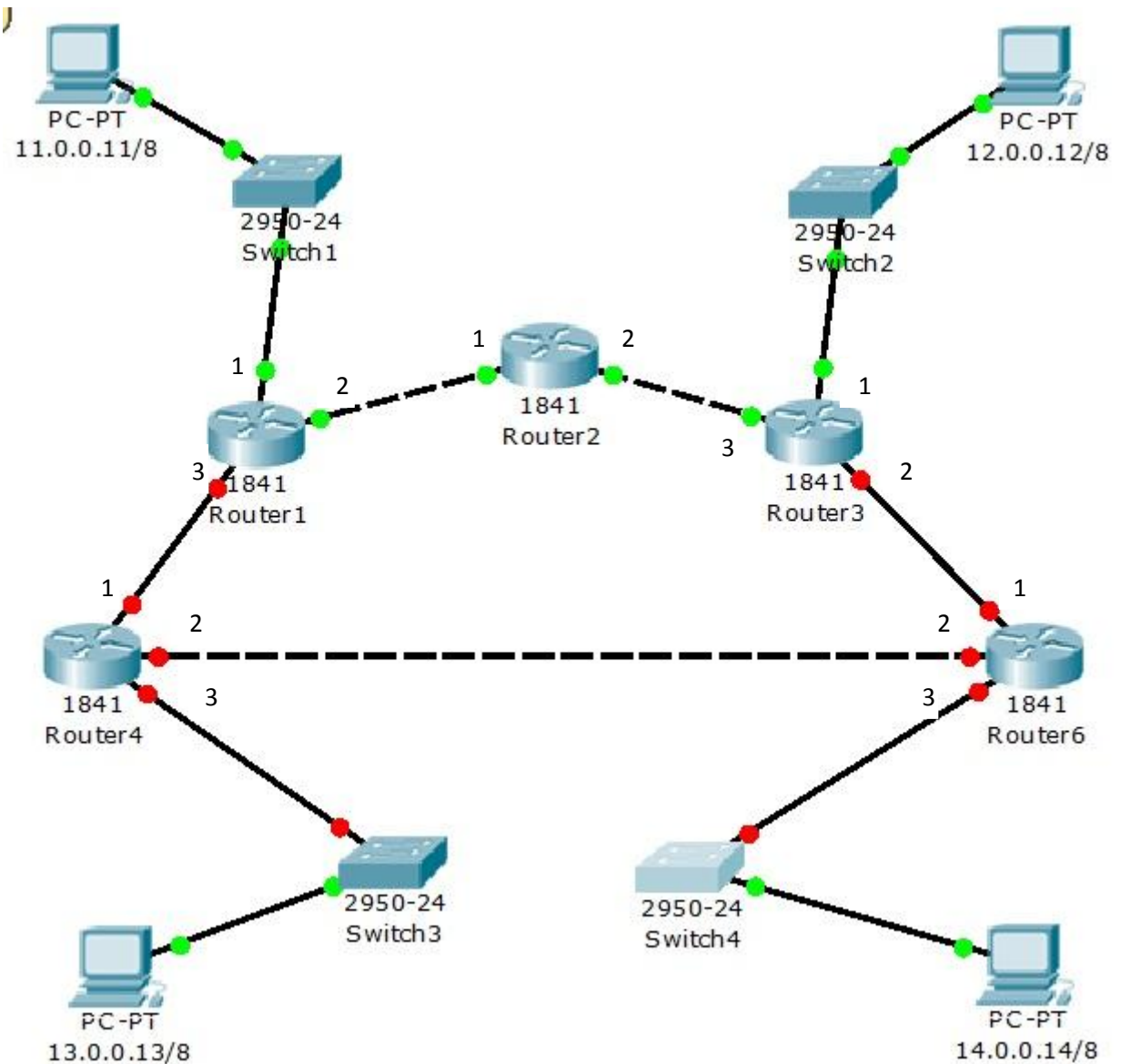


Рис.6.2. Схема сети.

В четырех сетях: 11.0.0.0/8, 12.0.0.0/8, 13.0.0.0/8 и 14.0.0.0/8 установлены компьютеры с адресами:

Comp1 – 11.0.0.11, маска 255.0.0.0

Comp2 – 12.0.0.12, маска 255.0.0.0

Comp3 – 13.0.0.13, маска 255.0.0.0

Comp4 – 14.0.0.14, маска 255.0.0.0

Между ними находится корпоративная сеть с шестью маршрутизаторами. На маршрутизаторах заданы следующие интерфейсы:
Таблица 6.1.

Маршрутизатор	Интерфейс 1	Интерфейс 2	Интерфейс 3
Router1	11.0.0.1/8	21.0.0.1/8	31.0.0.1/8
Router2	21.0.0.2/8	51.0.0.2/8	
Router3	12.0.0.3/8	61.0.0.3/8	51.0.0.3/8
Router4	31.0.0.4/8	81.0.0.4/8	13.0.0.4/8
Router6	61.0.0.6/8	81.0.0.6/8	14.0.0.6/8

Настройте маршрутизацию по протоколу RIP на каждом из роутеров.
Для этого:

- 1 - настройте все маршрутизаторы, как это было показано в лабораторной работе №6;
 - 2 – проверьте настройку маршрутизаторов по таблице маршрутизации.
- Чтобы убедиться в том, что маршрутизатор действительно правильно сконфигурирован и работает корректно, просмотрите таблицу RIP роутера, используя команду `show` следующим образом:

Router#**show ip route rip**

Например для шестого маршрутизатора Router6 таблица будет иметь следующий вид (Рис.6.3):

```
Router6>en
Router6#show ip route rip
R    11.0.0.0/8 [120/2] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    12.0.0.0/8 [120/1] via 61.0.0.3, 00:00:08, Ethernet0/0/0
R    13.0.0.0/8 [120/1] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    21.0.0.0/8 [120/2] via 61.0.0.3, 00:00:08, Ethernet0/0/0
      [120/2] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    31.0.0.0/8 [120/1] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    51.0.0.0/8 [120/1] via 61.0.0.3, 00:00:08, Ethernet0/0/0
Router6#
```

Рис. 6.3. Таблица маршрутизации RIP.

Данная таблица показывает, что к сети 21.0.0.0 есть два пути: через Router4 (сеть 81.0.0.0) и через Router3 (сеть 61.0.0.0).

Проведите диагностику сети:

- 1 – проверьте правильность настройки с помощью команд **ping** и **tracert** в консоли каждого компьютера;
- 2 – проведите ту же диагностику сети при выключенном маршрутизаторе Router6.

3 - проверьте связь между компьютерами с адресами 12.0.0.12 и 13.0.0.13. Количество промежуточных роутеров при прохождении пакета по сети при включенном и выключенном роутере 6 должно быть разным. При включенном Router6 должно быть на единицу меньше, чем при выключенном.

Самостоятельная работа №2.

Создайте схему, представленную на рис.7.4.

Задание.

1. Настройте корпоративную сеть с использованием протокола RIP.
2. Проверьте связь между компьютерами Comp1 и Comp3 с помощью команд **ping** и **tracert** при включенном и выключенном пятом маршрутизаторе.
3. Проверьте связь между компьютерами ПК0 и Comp1 с помощью команд **ping** и **tracert** при включенном и выключенном втором маршрутизаторе.

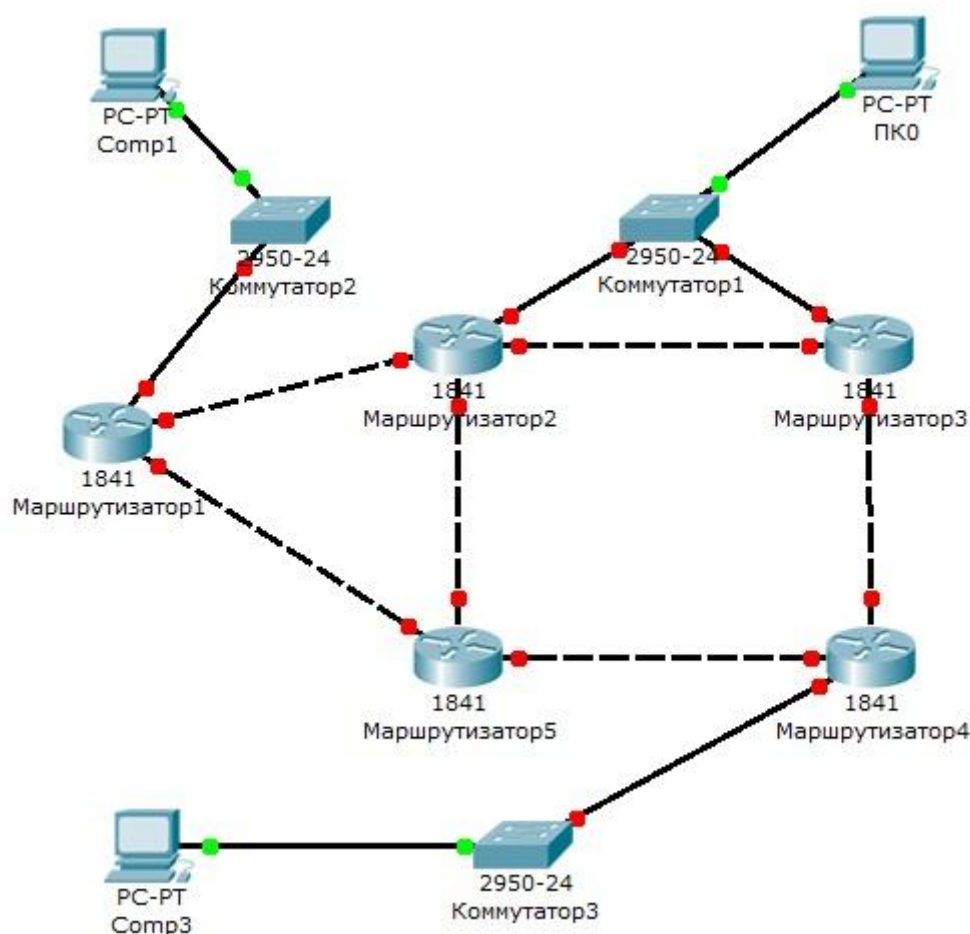


Рис.6.4. Схема сети.

Протоколы состояния связи.

Эти протоколы предлагают лучшую масштабируемость и сходимость по сравнению с дистанционно-векторными протоколами. Работа протоколов базируется на алгоритме Дейкстры, который часто называют алгоритмом «кратчайший путь – первым» (shortest path first SPF)). Наиболее типичным представителем является протокол OSPF (Open Shortest Path First).

Маршрутизатор берёт в рассмотрение состояние связи интерфейсов других маршрутизаторов в сети. Маршрутизатор строит полную базу данных всех состояний связи в своей области, то есть имеет достаточно информации для создания своего отображения сети. Каждый маршрутизатор затем самостоятельно выполняет SPF-алгоритм на своём собственном отображении сети или базе данных состояний связи для определения лучшего пути, который заносится в таблицу маршрутов. Эти пути к другим сетям формируют дерево с вершиной в виде локального маршрутизатора.

Маршрутизаторы извещают о состоянии своих связей всем маршрутизаторам в области. Такое извещение называют LSA (link-state advertisements).

В отличие от дистанционно-векторных маршрутизаторов, маршрутизаторы состояния связи могут формировать специальные отношения со своими соседями.

Имеет место начальный наплыв LSA пакетов для построения базы данных состояний связи. Далее обновление маршрутов производится только при смене состояний связи или, если состояние не изменилось в течение определённого интервала времени. Если состояние связи изменилось, то частичное обновление пересылается немедленно. Оно содержит только состояния связей, которые изменились, а не всю таблицу маршрутов.

Администратор, заботящийся об использовании линий связи, находит эти частичные и редкие обновления эффективной альтернативой дистанционно-векторной маршрутизации, которая передаёт всю таблицу маршрутов через регулярные промежутки времени. Протоколы состояния связи имеют более быструю сходимость и лучшее использование полосы пропускания по сравнению с дистанционно-векторными протоколами. Они превосходят дистанционно-векторные протоколы для сетей любых размеров, однако имеют два главных недостатка: повышенные требования к вычислительной мощности маршрутизаторов и сложное администрирование.

Лабораторная работа №8. Настройка протокола OSPF.

Возьмите схему сети, представленную на рисб.1.

Проведем настройку протокола OSPF на маршрутизаторе Router1.

Войдите в конфигурации в консоль роутера и выполните следующие настройки (при вводе команд маску подсети можно не указывать, т.к. она будет браться автоматически из настроек интерфейса роутера):

Войдите в привилегированный режим:

```
Switch>en
```

Войдите в режим конфигурации:

```
Switch1#conf t
```

Войдите в режим конфигурирования протокола OSPF:

```
Router1 (config) #router ospf 1
```

В команде `router ospf <идентификатор_процесса>` под идентификатором процесса понимается уникальное числовое значение для каждого процесса роутинга на маршрутизаторе. Данное значение должно быть больше в интервале от 1 до 65535. В OSPF процессам на роутерах одной зоны принято присваивать один и тот же идентификатор.

Подключите клиентскую сеть к роутеру:

```
Router1 (config-router) #network 10.11.0.0
```

Подключите вторую сеть к роутеру:

```
Router1 (config-router) #network 10.10.0.0
```

Задайте использование второй версии протокол OSPF:

```
Router1 (config-router) #version 2
```

Выйдите из режима конфигурирования протокола OSPF:

```
Router1 (config-router) #exit
```

Выйдите из консоли настроек:

```
Router1 (config) #exit
```

Сохраните настройки в память маршрутизатора:

```
Switch1#write memory
```

Аналогично проведите настройку протокола OSPF на маршрутизаторе Router2.

Контрольные вопросы.

1. В чем различие между топологической и дистанционно-векторной маршрутизацией?
2. Опишите схему работы протокола RIP.
3. Опишите схему работы протокола OSPF.
4. Перечислите основные этапы установки маршрутизатора.
5. Опишите четыре этапа загрузки маршрутизатора.
6. Какие из указанных ниже протоколов работают по дистанционно-векторному алгоритму и каковы их основные различия?
 - RIP;
 - IGRP;
 - EIGRP;
 - OSPF
7. Дайте характеристику классам протоколов маршрутизации.
8. Приведите классификацию протоколов маршрутизации на основе алгоритмов их работы.
9. Сделайте сравнение классовых и бесклассовых протоколов маршрутизации.
10. Сделайте сравнение протоколов маршрутизации внутреннего шлюза.
11. Опишите этапы настройки протокола маршрутизации RIP-2.

Раздел 7. Служба NAT.

NAT (Network Address Translation) — трансляция сетевых адресов, технология, которая позволяет преобразовывать (изменять) IP адреса и порты в сетевых пакетах.

NAT используется чаще всего для осуществления доступа устройств из сети предприятия(дома) в Интернет, либо наоборот для доступа из Интернет на какой-либо ресурс внутри сети.

Сеть предприятия обычно строится на частных IP адресах. Согласно RFC 1918 под частные адреса выделено три блока:

10.0.0.0 — 10.255.255.255 (10.0.0.0/255.0.0.0 (/8))

172.16.0.0 — 172.31.255.255 (172.16.0.0/255.240.0.0 (/12))

192.168.0.0 — 192.168.255.255 (192.168.0.0/255.255.0.0 (/16))

Эти адреса не маршрутизируются в Интернете, и провайдеры должны отбрасывать пакеты с такими IP адресами отправителей или получателей.

Для преобразования частных адресов в Глобальные (маршрутизируемые в Интернете) применяют NAT.

Помимо возможности доступа во внешнюю сеть (Интернет), NAT имеет ещё несколько положительных сторон. Так, например, трансляция сетевых адресов позволяет скрыть внутреннюю структуру сети и ограничить к ней доступ, что повышает безопасность. А ещё эта технология позволяет экономить Глобальные IP адреса, так как под одним глобальным адресом в Интернет может выходить множество хостов.

Настройка NAT на маршрутизаторах Cisco под управлением IOS включает в себя следующие шаги

1. Назначить внутренний (Inside) и внешний (Outside) интерфейсы
Внутренним интерфейсом обычно выступает тот, к которому подключена локальная сеть. Внешним — к которому подключена внешняя сеть, например сеть Интернет провайдера.
2. Определить для кого (каких ip адресов) стоит делать трансляцию.
3. Выбрать какой вид трансляции использовать
4. Осуществить проверку трансляций

Существует три вида трансляции Static NAT, Dynamic NAT, Overloading.

Static NAT — Статический NAT, преобразование IP адреса один к одному, то есть сопоставляется один адрес из внутренней сети с одним адресом из внешней сети.

Dynamic NAT — Динамический NAT, преобразование внутреннего адреса/ов в один из группы внешних адресов. Перед использованием динамической трансляции, нужно задать nat-пул внешних адресов

Overloading — позволяет преобразовывать несколько внутренних адресов в один внешний. Для осуществления такой трансляции используются порты, поэтому иногда такой NAT называют PAT (Port Address Translation). С помощью PAT можно преобразовывать внутренние адреса во внешний адрес, заданный через пул или через адрес на внешнем интерфейсе.

Список команд для настройки NAT:

обозначение Интернет интерфейса:

```
interface FastEthernet0/0  
ip nat outside
```

обозначение локального интерфейса:

```
interface Vlan1  
ip nat inside
```

создание списка IP, имеющего доступ к NAT:

```
ip access-list extended NAT  
permit ip host 192.168.??? ??? any
```

включение NAT на внешнем интерфейсе:

```
ip nat inside source list NAT interface FastEthernet0/0 overload
```

Посмотреть существующие трансляции можно командой "show ip nat translations".

Отладка запускается командой "debug ip nat"

Настройка Static NAT

```
router(config)#ip nat inside source static <local-ip> <global-ip>  
router(config)#interface fa0/4  
router(config-if)#ip nat inside  
router(config)#interface fa0/4
```

```
router(config-if)#exit
router(config)#interface s0
router(config-if)#ip nat outside
```

Настройка Dynamic NAT

```
router(config)#ip nat pool name start-ip end-ip {netmask netmask | prefix-length
prefix-length}
router(config)#access-list <acl-number> permit <source-IP> [source-wildcard]
router(config)#ip nat inside source list <acl-number> pool <name>
router(config)#interface fa0/4
router(config-if)#ip nat inside
router(config-if)#exit
router(config)#interface s0
router(config-if)#ip nat outside
```

Настройка Overloading

```
router(config)#access-list acl-number permit source-IP source-wildcard
router(config)#ip nat inside source list acl-number interface interface overload
router(config)#interface fa0/4
router(config-if)#ip nat inside
router(config-if)#exit
router(config)#interface s0
router(config-if)#ip nat outside
```

Лабораторная работа №9. Преобразование сетевых адресов NAT.

В данной работе необходимо решить задачу вывода компьютеров локальной сети организации в интернет. Локальная сеть настроена в частной адресации – в сети 10.0.0.0, адреса которой не имеют выхода в интернет. Для решения этой задачи необходимо настроить службу NAT. Схема сети представлена на рис.7.1.

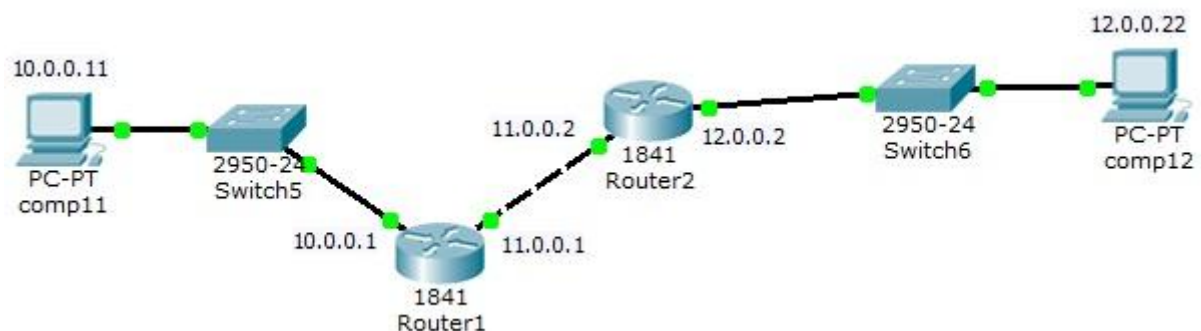


Рис. 7.1. Схема сети.

Создайте сеть, представленную на рис.1. Задайте имена устройств и адресацию, как показано на рис.1.

В данный момент NAT на роутере не настроен, мы можем убедиться в этом, используя режим симуляции.

Перейдите в этот режим и посмотрите состав пакета при прохождении через оба роутера (рис. 7.2).

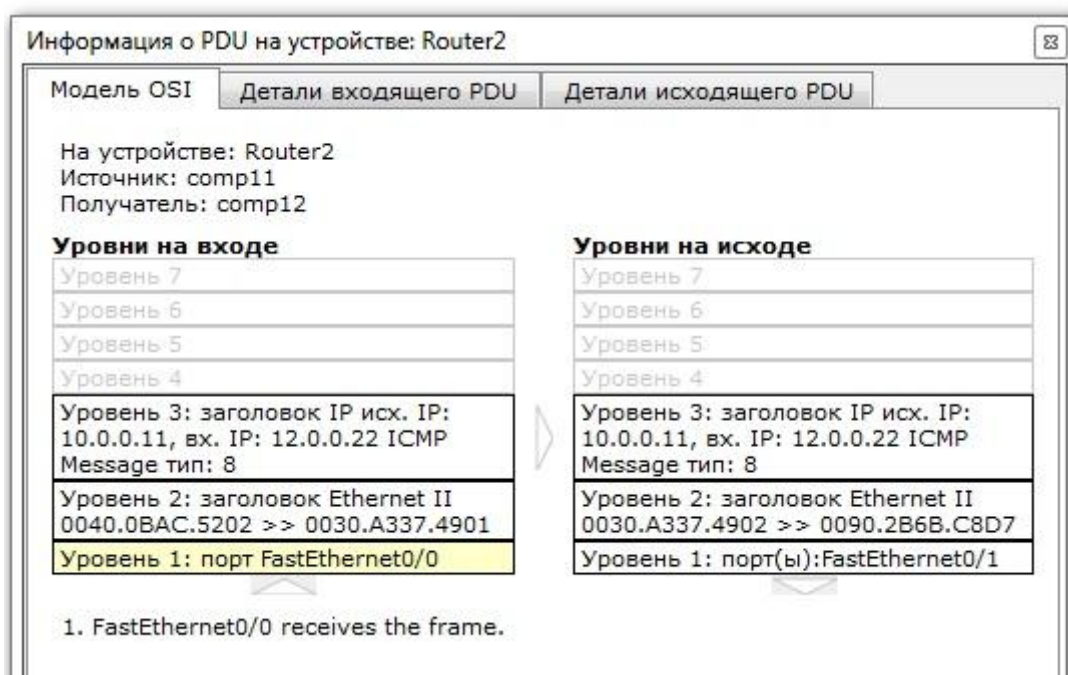


Рис.7.2. Параметры пакета при прохождении Router2.

При прохождении пакета через второй маршрутизатор IP адрес отправителя не изменился (10.0.0.11).

Сконфигурируем NAT на маршрутизаторе Router1.

Для настройки NAT на роутере нам необходимо будет выполнить следующие шаги:

1. зайти в настройки Router1, во вкладку CLI
2. для входа в режим администратора ввести команду enable (en)
Router>**en**

Для входа в режим настройки вводим команду config t

Router#**config t**

3. Интерфейс FastEthernet 0/0 наш внутренний интерфейс, к которому подключены рабочие станции. Для настройки NAT на роутере необходимо это

обозначить в настройках. Это можно сделать при помощи следующих команд:
входим в настройки интерфейса:

```
Router(config) #int FastEthernet 0/0
```

объявляем интерфейс внутренним интерфейсом:

```
Router(config-if) #ip nat inside
```

выходим из настроек интерфейса

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

4. Аналогично настраиваем интерфейс FastEthernet 0/1, который подключен к сети провайдера, лишь с тем различием, что он будет являться внешним интерфейсом NAT:

входим в настройки интерфейса:

```
Router(config) #int FastEthernet 0/1
```

объявляем интерфейс внешним интерфейсом NAT:

```
Router(config-if) #ip nat outside
```

выходим из настроек интерфейса:

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

5. Задаем пул внешних адресов, в которые будут транслироваться внутренние адреса. Для задания пула, содержащего только один адрес – адрес внешнего интерфейса роутера - необходимо ввести команду:

```
Router(config) #ip nat pool natpool 11.0.0.0 11.0.0.1 netmask 255.0.0.0
```

При задании пула адресов необходимо указать первый и последний адреса из входящей в пул последовательности адресов. Если в пуле 1 адрес (как в нашем случае) необходимо указать его 2 раза.

6. Задаем список доступа:

```
Router(config) #access-list 34 permit any
```

Важно: 34 – число от 1 до 99 обозначает № списка доступа и задается администратором. Any – ключевое слово, означает, что список доступа будет разрешать пакеты с любым адресом отправителя.

7. Наконец вводим последнюю команду, которая, собственно, и включает NAT на Router0. Команда, бесспорно, является основной, но без задания всех предыдущих параметров она работать не будет.

Router(config) #**ip nat inside source list 34 pool natpool overload**

Данная команда говорит роутеру, что у всех пакетов, полученных на внутренний интерфейс и разрешенных списком доступа номер 34, адрес отправителя будет транслирован в адрес из NAT пула “natpool”. Ключ overload указывает, что трансляции будут перегружены, позволяя нескольким внутренним узлам транслироваться на один IP адрес.

Теперь NAT настроен. Можем убедиться в этом послав пакет из любой рабочей станции в подсети на сервер yandex.ru (пакет пройдет). Если мы рассмотрим прохождение пакета подробнее, перейдя в режим симуляции, то увидим, что при прохождении пакета через Router1 адрес отправителя изменился(NAT настроен).

Контрольные вопросы.

1. Опишите все возможные схемы работы службы NAT.
2. Какие частные IP адреса используются службой NAT в каждом классе адресов?
3. Перечислите преимущества и недостатки службы NAT.
4. Перечислите этапы настройки службы NAT.
5. Опишите схему проверки работы службы NAT.
6. Опишите основные проблемы в работе сервера NAT.

Раздел 8. Виртуальные локальные сети VLAN.

VLAN (аббр. от англ. Virtual Local Area Network) — логическая ("виртуальная") локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети.

VLAN'ы могут быть настроены на коммутаторах, маршрутизаторах, других сетевых устройствах.

Преимущества:

- 1 - Облегчается перемещение, добавление устройств и изменение их соединений друг с другом.
- 2 - Достигается большая степень административного контроля вследствие наличия устройства, осуществляющего между сетями VLAN маршрутизацию на 3-м уровне.
- 3 - Уменьшается потребление полосы пропускания по сравнению с ситуацией одного широковещательного домена.
- 4 - Сокращается непроизводительное использование CPU за счет сокращения пересылки широковещательных сообщений.
- 5 - Предотвращение широковещательных штормов и предотвращение петель.

Лабораторная работа № 10. Настройка VLAN на одном коммутаторе Cisco.

В данной работе рассматривается настройка VLAN на коммутаторе фирмы Cisco на его портах доступа. Создайте сеть, логическая топология которой представлена на рис.9.1. Компьютеры соединены коммутатором Cisco 2960-24TT. В таблице 9.1 приведены адреса компьютеров.

Задача данной работы – сделать две независимые группы компьютеров: ПК0, ПК1 и ПК2 должны быть доступны только друг для друга, вторая независимая группа - компьютеры ПК3 и ПК4. Для этого создадим два отдельных VLAN (рис.8.1)

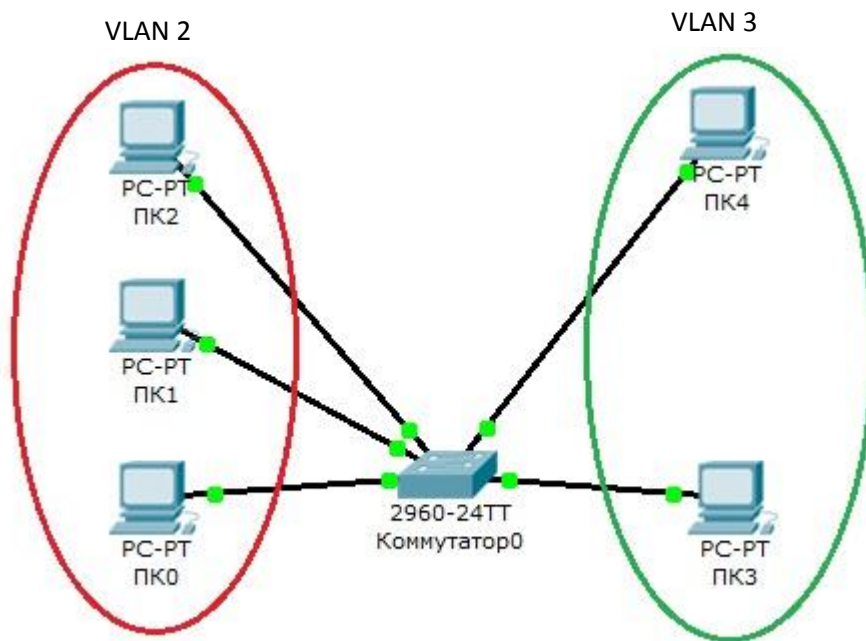


Рис. 8.1. Схема сети с одним коммутатором.

Таблица 8.1.

Компьютер	IP адрес	Порт коммутатора
ПК0	10.0.0.1/8	1
ПК1	10.0.0.2/8	2
ПК2	10.0.0.3/8	3
ПК3	10.0.0.4/8	4
ПК4	10.0.0.5/8	5

Далее будем считать, что ПК0, ПК1 и ПК2 находятся в VLAN 2, а ПК3 и ПК4 находятся в VLAN 3.

Для проверки конфигурации хоста ПК0 выполним команду `ipconfig`. Результат выполнения команды на рисунке 8.2. При желании можно выполнить аналогичную проверку на остальных хостах.

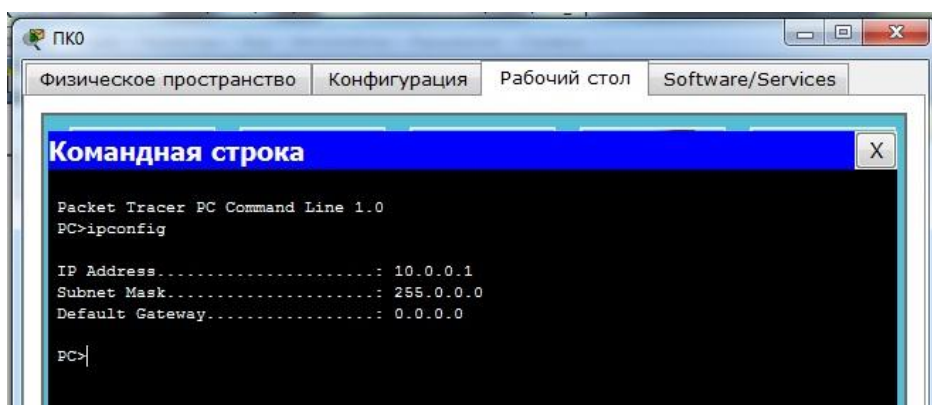


Рис.8.2. Проверка конфигурации хоста

Используя команду PING проверим связь между всеми компьютерами. Сейчас они в одной сети и все доступны друг для друга

Теперь займемся настройкой VLAN 2 и VLAN3, чтобы структурировать сети на коммутаторе и навести в них порядок.

Далее перейдем к настройке коммутатора. Откроем его консоль. Для того чтобы это выполнить в Packet Tracer дважды щелкните левой кнопкой мыши по коммутатору в рабочей области.

В открывшемся окне перейдите на вкладку CLI. Вы увидите окно консоли. Нажмите Enter, чтобы приступить к вводу команд. Информация, которая в данный момент отражена на консоли, свидетельствует о том что интерфейсы FastEthernet0/1 – FastEthernet0/5 находятся в рабочем состоянии.

Перейдем в привилегированный режим выполнив команду **enable**:

```
Switch>en  
Switch#
```

Посмотрим информацию о существующих на коммутаторе VLAN-ах (рис.8.3). Для этого выполним следующую команду:

```
Switch#sh vl br
```

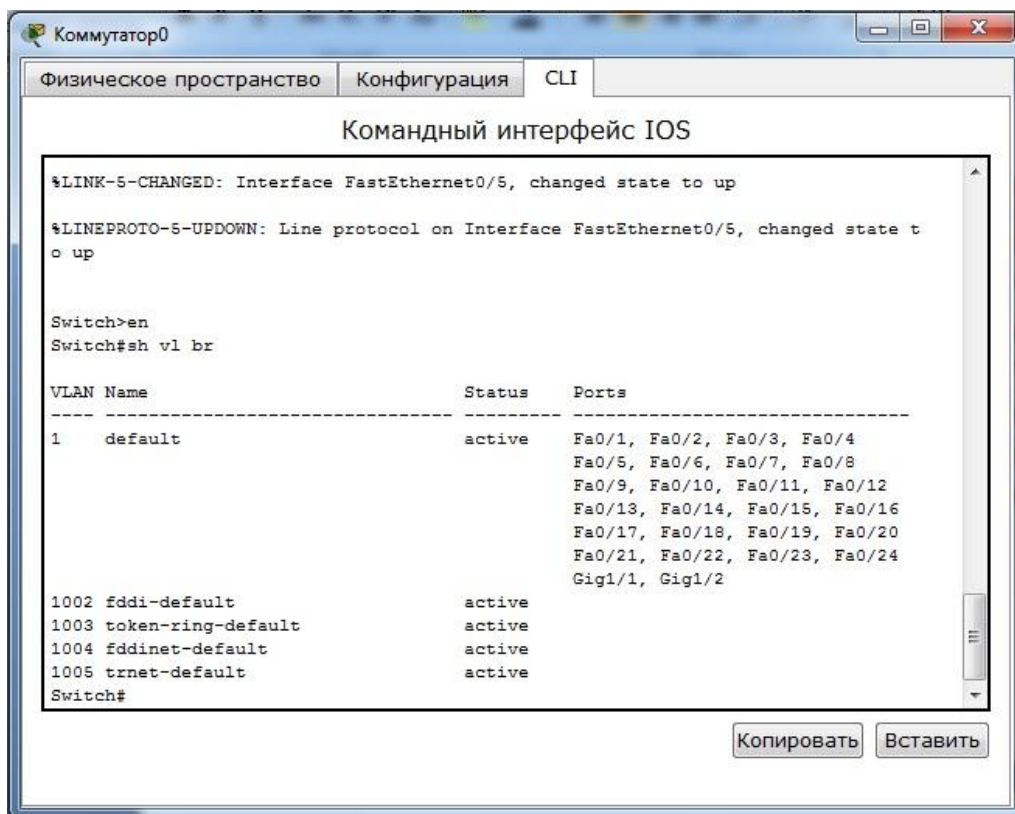


Рис.8.3. Просмотр информации о VLAN на коммутаторе.

В результате выполнения команды на экране появится: номера VLAN – первый столбец, название VLAN - второй столбец, состояние VLAN (работает он в данный момент или нет) – третий столбец, порты принадлежащие к данному VLAN – четвертый столбец. Как мы видим по умолчанию на коммутаторе существует пять VLAN-ов. Все порты коммутатора по умолчанию принадлежат VLAN 1. Остальные четыре VLAN являются служебными и используются не очень часто.

Для реализации сети, которую мы запланировали сделать, создадим на коммутаторе еще два VLAN. Для этого в привилегированном режиме выполните следующую команду:

```
Switch#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch(config)#
```

для перехода в режим конфигурации. Вводим команду VLAN 2. Данной командой вы создадите на коммутаторе VLAN с номером 2. Указатель ввода Switch(config)# изменится на Switch(config-vlan)# это свидетельствует о том, что вы конфигурируете уже не весь коммутатор в целом, а только отдельный VLAN, в данном случае VLAN номер 2. Если вы используете команду «vlan x», где x номер VLAN, когда VLAN x еще не создан на коммутаторе, то он будет автоматически создан и вы перейдете к его конфигурированию. Когда вы находитесь в режиме конфигурирования VLAN, возможно изменение параметров выбранной виртуальной сети, например можно изменить ее имя с помощью команды name.

Для достижения поставленной в данном посте задачи, сконфигурируем VLAN 2 следующим образом:

```
Switch(config)#vlan 2
```

```
Switch(config-vlan)#name subnet_10
```

```
Switch(config)#interface range fastEthernet 0/1-3
```

```
Switch(config-if-range)#switchport mode access
```

```
Switch(config-if-range)#switchport access vlan 2
```

Разберем данную конфигурацию. Как уже говорилось ранее командой VLAN 2, мы создаем на коммутаторе новый VLAN с номером 2. Команда **name subnet_10** присваивает имя subnet_10 виртуальной сети номер 2. Выполняя команду **interface range fastEthernet 0/1-3** мы переходим к конфигурированию интерфейсов fastEthernet0/1, fastEthernet0/2 и fastEthernet0/3 коммутатора. Ключевое слово **range** в данной команде, указывает на то, что мы будем конфигурировать не один единственный порт, а целый диапазон портов, в

принципе ее можно не использовать, но тогда последние три строки придется заменить на:

```
Switch(config) #interface fastEthernet 0/1
Switch(config-if) #switchport mode access
Switch(config-if) #switchport access vlan 2
Switch(config) #interface fastEthernet 0/2
Switch(config-if) #switchport mode access
Switch(config-if) #switchport access vlan 2
Switch(config) #interface fastEthernet 0/3
Switch(config-if) #switchport mode access
Switch(config-if) #switchport access vlan 2
```

Команда **switchport mode access** конфигурирует выбранный порт коммутатора, как порт доступа (аксес порт).

Команда **switchport access vlan 2** указывает, что данный порт является портом доступа для VLAN номер 2.

Выйдите из режима конфигурирования, дважды набрав команду **exit** и просмотрите результат конфигурирования (рис.8.4), выполнив уже знакомую нам команду **sh vl br** еще раз:

```
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
%SYS-S-CONFIG_I: Configured from console by console

Switch#sh vl br
```

VLAN	Name	Status	Ports
1	default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gig1/1, Gig1/2
2	subnet_10	active	Fa0/1, Fa0/2, Fa0/3
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
Switch#
```

Рис.8.4. Распределение портов на VLAN.

На коммутаторе появился еще один VLAN с номером 2 и именем subnet_10, портами доступа которого являются fastEthernet0/1, fastEthernet0/2 и fastEthernet0/3.

Далее аналогичным образом создадим VLAN 3 с именем subnet_192 и сделаем его портами доступа интерфейсы fastEthernet0/4 и fastEthernet0/5. Результат должен получиться следующим (рис.8.5):

```
Switch#sh vl br
```

VLAN Name	Status	Ports
1 default	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig1/1 Gig1/2
2 subnet_10	active	Fa0/1, Fa0/2, Fa0/3
3 subnet_192	active	Fa0/4, Fa0/5
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Рис.8.5. Распределение портов на VLAN.

В принципе уже все готово и наша сеть настроена. Осталось лишь ее немного протестировать. Перейдите в консоль компьютера ПК0. Пропингуйте с него остальные компьютеры сети. Компьютеры ПК1 и ПК2 доступны, а компьютеры ПК3 и ПК4 не доступны. Все пять компьютеров теоретически должны находиться в одной подсети 10.0.0.0/8 и видеть друг друга, на практике они находятся в разных виртуальных локальных сетях и поэтому не могут взаимодействовать между собой.

Лабораторная работа № 11. Настройка VLAN на двух коммутаторах Cisco.

Создайте сеть, логическая топология которой представлена на рис.8.6. Компьютеры соединены коммутатором Cisco 2950-24. В таблице 8.2 приведены адреса компьютеров.

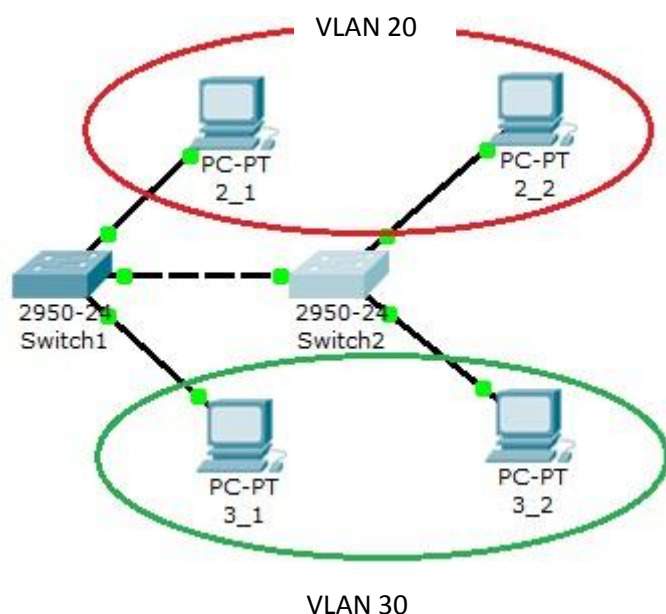


Рис.8.6. Схема сети.

Таблица 8.2.

Компьютер	IP адрес	Коммутатор	Порт коммутатора	Вилан
2_1	10.0.0.1/8	Switch1	1	VLAN 20
2_2	10.0.0.3/8	Switch2	1	VLAN 20
3_1	10.0.0.2/8	Switch1	2	VLAN 30
3_2	10.0.0.4/8	Switch2	2	VLAN 30

Далее будем считать, что 2_1 и 2_2 находятся в VLAN 20, а 3_1 и 3_2 находятся в VLAN 30.

Проверим связность получившейся сети. Для этого пропингуем с 2_1 все остальные компьютеры. Поскольку пока в сети нет разделения на VLAN, то все компьютеры должны быть доступны.

Теперь займемся настройкой VLAN 20 и VLAN30, чтобы структурировать сети на коммутаторах.

Перейдите к настройке коммутатора Switch1. Откройте его консоль. В открывшемся окне перейдите на вкладку CLI, войдите в привилегированный режим и настройте VLAN 20 и VLAN30 согласно таблице 2.

Создайте на коммутаторе VLAN 20. Для этого в привилегированном режиме выполните следующую команду:

```
Switch1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

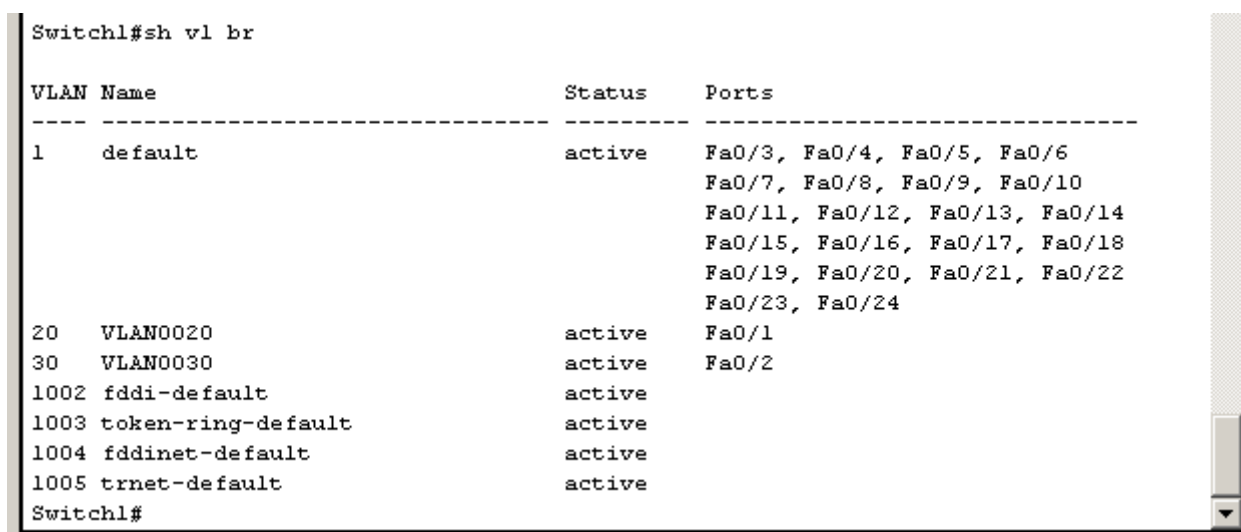
для перехода в режим конфигурации и настройте VLAN 20 и VLAN 30 следующим образом:

```
Switch1 (config) #vlan 20
Switch1 (config) #interface fastEthernet 0/1
Switch1 (config-if-range) #switchport mode access
Switch1 (config-if-range) #switchport access vlan 20
Switch1 (config-if-range) #exit
Switch1 (config) #vlan 30
Switch1 (config) #interface fastEthernet 0/2
Switch1 (config-if-range) #switchport mode access
Switch1 (config-if-range) #switchport access vlan 30
```

Просмотрите информацию о существующих на коммутаторе VLAN-ах командой:

Switch1#**sh vl br**

У вас должен получиться результат, показанный на рис.8.7.



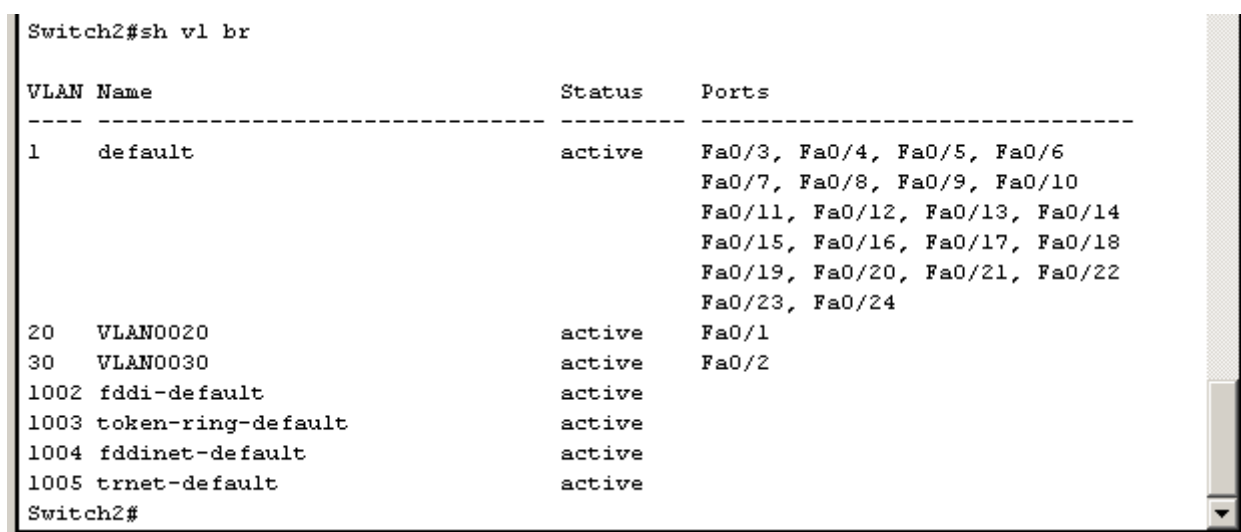
```
Switch1#sh vl br
```

VLAN Name	Status	Ports
1 default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
20 VLAN0020	active	Fa0/1
30 VLAN0030	active	Fa0/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Switch1#

Рис. 8.7. Конфигурация Switch1.

Аналогичным образом сконфигурируйте Switch2 (рис. 8.8).



```
Switch2#sh vl br
```

VLAN Name	Status	Ports
1 default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
20 VLAN0020	active	Fa0/1
30 VLAN0030	active	Fa0/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Switch2#

Рис. 8.7. Конфигурация Switch2.

Поскольку в данный момент нет обмена информации о вилланах, то компьютеры будут пинговать только себя.

Теперь организуем магистраль обмена между коммутаторами. Для этого настроим третий порт на каждом коммутаторе как транковый.

Войдите в консоль коммутатора Switch1 и задайте транковый порт:

```
Switch1>en
Switch1#conf t
Switch1 (config) #interface fastEthernet 0/3
Switch1 (config) #switchport mode trunk
Switch1 (config) #no shutdown
Switch1 (config) #exit
```

Откройте конфигурацию коммутатора на интерфейсе FastEthernet0/3 и убедитесь, что порт транковый (рис.8.8).

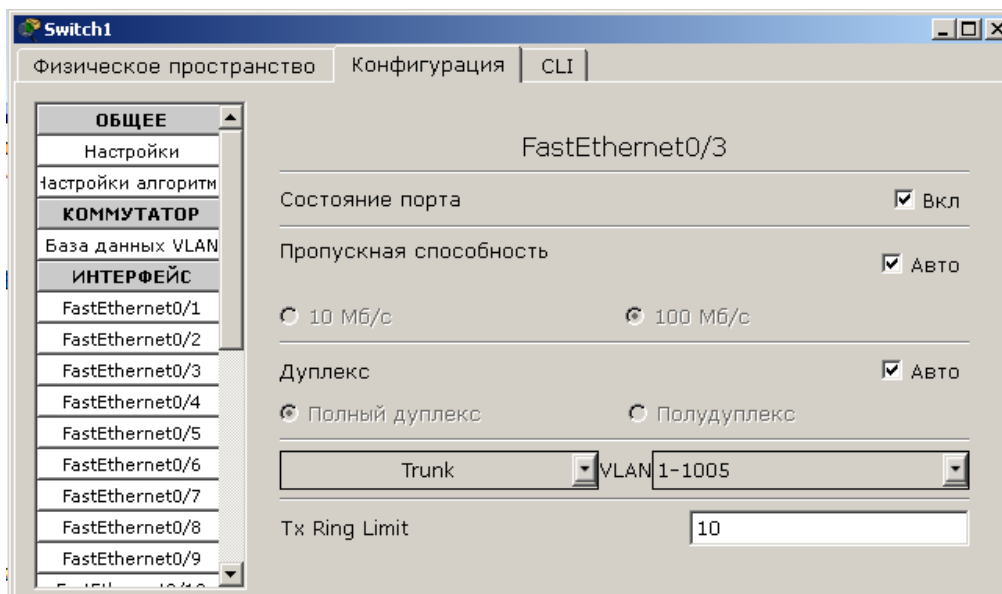


Рис.8.8. Конфигурация интерфейса FastEthernet0/3.

На коммутаторе Switch2 интерфейс FastEthernet0/3 автоматически настроится как транковый.

Теперь компьютеры, входящие в один виллан должны пинговаться. У вас должна появиться связь между компьютерами 2_1 и 2_2, а так же между 3_1 и 3_2. Но компьютеры в другом виллане будут недоступны.

Сохраните схему сети.

Теперь объединим две виртуальные сети с помощью маршрутизатора. Добавьте в схему сети маршрутизатор, как показано на рис.8.9. Маршрутизатор соединен с интерфейсами **fastEthernet 0/4** коммутаторов.

Разобьем нашу сеть 10.0.0.0 на две подсети: 10.2.0.0 и 10.3.0.0. Для этого поменяйте IP адреса и маску подсети на 255.255.0.0, как указано в таблице 8.3.

Таблица 8.3.

Компьютер	IP адрес	Коммутатор	Порт коммутатора	Вилан
2_1	10.2.0.1/16	Switch1	1	VLAN 20
2_2	10.2.0.3/16	Switch2	1	VLAN 20
3_1	10.3.0.2/16	Switch1	2	VLAN 30
3_2	10.3.0.4/16	Switch2	2	VLAN 30

Компьютеры должны пинговаться в пределах одного виллана и одной подсети.

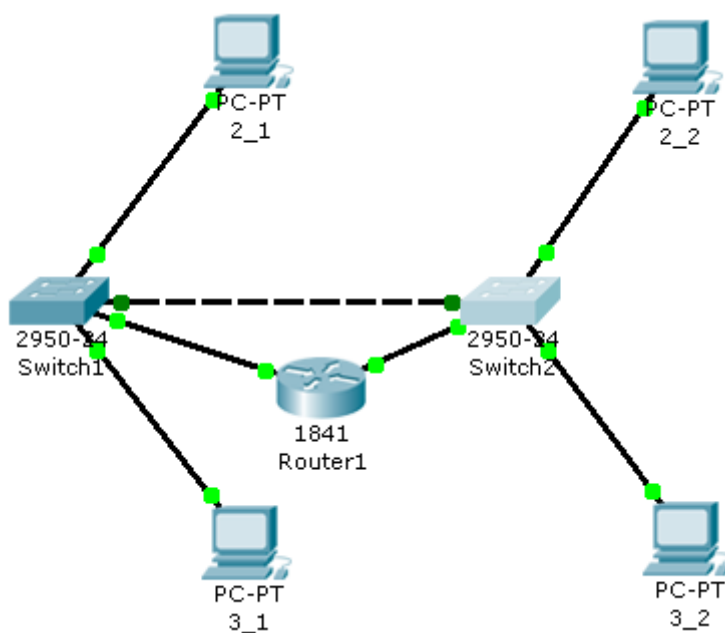


Рис. 8.9. Схема сети.

Обозначим на коммутаторах интерфейсы, подсоединенные к маршрутизатору в виртуальные сети.

Войдите в конфигурацию первого коммутатора Switch1 и задайте параметры четвертого порта:

```

Switch1 (config) #interface fastEthernet 0/4
Switch1 (config-if) #switchport access vlan 20

```

Проверьте настройки первого коммутатора Switch1 (рис.8.10):

```
Switch1#sh vl br
```

VLAN Name	Status	Ports
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
20 VLAN0020	active	Fa0/1, Fa0/4
30 VLAN0030	active	Fa0/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
Switch1#
```

Рис.8.10. Настройки коммутатора Switch1.

Войдите в конфигурацию второго коммутатора Switch2 и задайте параметры четвертого порта:

```
Switch2 (config) #interface fastEthernet 0/4  
Switch2 (config-if) #switchport access vlan 30
```

Проверьте настройки второго коммутатора Switch2 (рис.8.11):

```
Switch2#sh vl br
```

VLAN Name	Status	Ports
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
20 VLAN0020	active	Fa0/1
30 VLAN0030	active	Fa0/2, Fa0/4
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
Switch2#
```

Рис.8.11. Настройки коммутатора Switch2.

Войдите в конфигурацию маршрутизатора и настройте IP адреса на маршрутизаторе:

```
Router1 (config-if) #interface fa0/0  
Router1 (config-if) #ip address 10.2.0.254 255.255.0.0  
Router1 (config-if) #no shutdown  
Router1 (config-if) #interface fa0/1
```

```
Router1(config-if) #ip address 10.3.0.254 255.255.0.0
Router1(config-if) #no shutdown
```

С этого момента мы установили маршрутизацию между двумя подсетями. Осталось установить шлюзы на компьютерах (таблица 8.4).

Таблица 8.4.

Компьютер	Gataway
2_1	10.2.0.254
2_2	10.2.0.254
3_1	10.3.0.254
3_2	10.3.0.254

Проверьте доступность компьютеров в сети. Теперь все компьютеры должны быть доступны и все адреса должны пинговаться.

Лабораторная работа № 12. Настройка VLAN в корпоративной сети.

Создайте следующую схему сети (рис.8.12):

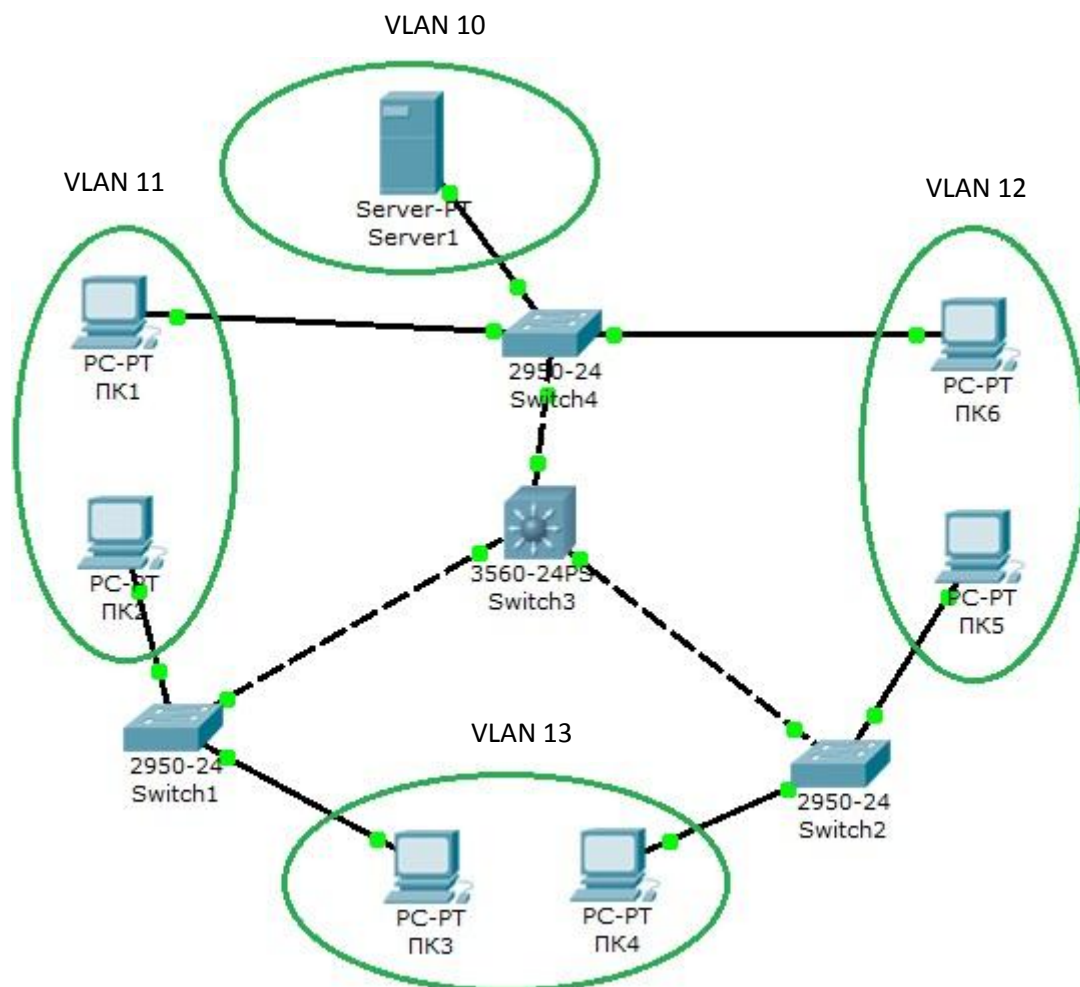


Рис.8.12. Схема корпоративной сети.

Состав сети:

- три коммутатора второго уровня распределения 2950-24 (Switch1, Switch2, Switch4);
- центральный коммутатор третьего уровня 3560-24PS (Switch3), выполняющий роль роутера;
- сервер (Server1);
- три подсети по два узла в каждой

Задача:

Для любого вилана могут быть доступны только узлы этого же вилана и сервер Server1.

В таблице 8.5 и 8.6 приведены данные для установки параметров компьютеров и коммутаторов.

Таблица 8.5. Конфигурация компьютеров.

Компьютер	IP адрес	Коммутатор	Порт коммутатора	VLAN
ПК1	10.11.0.11/16	Switch4	4	VLAN 11
ПК2	10.11.0.2/16	Switch1	1	VLAN 11
ПК3	10.13.0.3/16	Switch1	2	VLAN 13
ПК4	10.13.0.4/16	Switch2	1	VLAN 13
ПК5	10.12.0.5/16	Switch2	2	VLAN 12
ПК6	10.12.0.6/16	Switch4	2	VLAN 12
Server1	10.10.0.7/16	Switch4	1	VLAN 10

Таблица 8.6. Связь коммутаторов по портам.

Порт центрального коммутатора Switch3	Порт коммутатора второго уровня распределения
1	Switch1 – 3 порт
2	Switch4 – 3 порт
3	Switch2 – 3 порт

После настройки всех коммутаторов установите самостоятельно шлюзы на всех компьютерах и сервере.

Сконфигурируйте центральный коммутатор:

Этап 1.

Перейдите к конфигурации центрального коммутатора Switch3 и создайте на нем базу VLAN.

1. Создайте VLAN 10:

```
Switch3>en  
Switch3#conf t  
Switch3 (config) #vlan 10  
Switch3 (config-vlan) #exit
```

2. Создайте VLAN 11, VLAN 12 и VLAN 13.

3. Настройте протокол VTP в режиме сервера:

```
Switch3 (config) #vtp domain HOME  
Switch3 (config) #vtp password HOME  
Switch3 (config) #vtp mode server
```

4. Просмотрите информацию о конфигурации VTP:

```
Switch#sh vtp status
```

5. Настройте все интерфейсы на транк:

```
Switch3 (config) #int fa0/1  
Switch3 (config-if) #switchport mode trunk  
Switch3 (config-if) #exit
```

и повторите эти настройки для второго и третьего интерфейсов.

Этап 2.

Перейдите к конфигурации коммутатора Switch4 и переведите его в режим client:

1. Создайте на коммутаторе VLAN 10 и задайте в нем порт 1 как access порт:

```
Switch4>en  
Switch4#conf t  
Switch4 (config) #vlan 10  
Switch4 (config-vlan) #exit  
Switch4 (config) #int fa0/1  
Switch4 (config-if) #switchport access vlan 10  
Switch4 (config-if) #switchport mode access  
Switch4 (config-if) #no shut
```

2. Создайте на коммутаторе VLAN 11 и задайте в нем порт 4 как access порт.

3. Создайте на коммутаторе VLAN 12 и задайте в нем порт 2 как access порт.

4. Переведите коммутатор в режим client:

```
Switch4 (config) #vtp domain HOME
```

```
Switch4 (config) #vtp password HOME  
Switch4 (config) #vtp mode client
```

ВАЖНО! При вводе имени домена и пароля соблюдайте нужный регистр.

Этап 4.

Перейдите к конфигурации коммутатора Switch1 и выполните следующие настройки:

.

1. Создайте на коммутаторе VLAN 11 и задайте в нем порт 1 как access порт.
2. Создайте на коммутаторе VLAN 13 и задайте в нем порт 2 как access порт.
3. Переведите коммутатор в режим client.

Этап 5.

Перейдите к конфигурации коммутатора Switch2.

1. Создайте на коммутаторе VLAN 12 и задайте в нем порт 2 как access порт.
2. Создайте на коммутаторе VLAN 13 и задайте в нем порт 1 как access порт.
3. Переведите коммутатор в режим client.

Этап 6.

Проверьте работоспособность сети на канальном уровне модели OSI.

После установки всех настроек таблица VLAN разойдется по коммутаторам с помощью протокола VTP.

В результате компьютеры, расположенные в одном виллане, будут доступны друг для друга, а другие компьютеры недоступны. Проверьте связь командой PING между следующими парами компьютеров:

- ПК1 – ПК2;
- ПК3 – ПК4;
- ПК5 – ПК6.

Если Вы все сделали правильно, то ping между парами пройдет, если нет – проверьте следующие установки:

- транковыми портами являются: на Switch3 все порты, на Switch1, Switch2 и Switch4 – третий порт;
- соединения интерфейсов на коммутаторах;
- названия и пароли доменов на каждом коммутаторе (команда sh vtp status);
- привязку интерфейсов к вилланам на коммутаторах (команда sh vl br).

Этап 7.

Настройка маршрутизации на центральном коммутаторе.

Создадим интерфейсы для каждого VLAN.

Настройка интерфейса для vlan 10 (шлюз по умолчанию):

```
Switch3 (config) #int vlan 10
```



```
Switch3 (config-if) #ip address 10.10.0.1 255.255.0.0  
Switch3 (config-if) #no shut  
Switch3 (config-if) #exit
```

Повторите эти настройки для каждого VLAN, задавая адрес IP: 10.[VLAN].0.1 и маску /16.

После этого зайдите в настройки каждого компьютера и установите нужный шлюз по умолчанию. Например для ПК1 – 10.11.0.1.

Включите маршрутизацию командой:

```
Switch3 (config) #ip routing
```

Этап 8.

Проверьте работоспособность сети на сетевом уровне модели OSI.

После включения маршрутизации все компьютеры будут доступны с любого хоста.

Этап 9.

Выполним основную задачу работы: для любого вилана могут быть доступны только узлы этого же вилана и сервер Server1.

Для этого введем следующие ограничения на трафик сети:

- 1 - Разрешить пакеты от любого хоста к серверу.
- 2 - Разрешить пакеты от сервера до любого хоста.
- 3 – Трафик от одной подсети к этой же подсети разрешить.
- 4 – Правило по умолчанию: запретить всё остальное.

Ограничения на трафик сети задаются с помощью команды фильтрации **access-list**. Данная команда задает критерии фильтрации в списке опций разрешения и запрета, называемом списком доступа. Списки доступа имеют два правила: **permit** – разрешить и **deny** – запретить. Данные правила либо пропускают пакет дальше по сети, либо блокируют его доступ.

Более подробно списки доступа будут рассмотрены в лабораторной работе №14.

Открываем центральный коммутатор (Switch3) и меняем его конфигурацию с помощью команды фильтрации **access-list**:

```
Switch3 (config) #ip access-list extended 100
```

(создается расширенный список доступа под номером 100)

```
Switch3 (config-ext-nacl) #permit ip any 10.10.0.0 0.0.0.255
```

```
Switch3 (config-ext-nacl) #permit ip 10.10.0.0 0.0.0.255 any
```

(разрешается доступ к сети 10.10.0.0/24)

```
Switch3 (config-ext-nacl) #permit ip 10.11.0.0 0.0.0.255 10.11.0.0 0.0.0.255
```

```
Switch3(config-ext-nacl)#permit ip 10.12.0.0 0.0.0.255 10.12.0.0 0.0.0.255
```

```
Switch3(config-ext-nacl)#permit ip 10.13.0.0 0.0.0.255 10.13.0.0 0.0.0.255
```

(разрешается: доступ из сети 10.11.0.0/24 в эту же сеть;
 доступ из сети 10.12.0.0/24 в эту же сеть;
 доступ из сети 10.13.0.0/24 в эту же сеть).

```
Switch3(config-ext-nacl)#exit
```

Теперь этот access-list наложим на конкретный интерфейс и применим ко всем VLAN-ам на входящий трафик (опция **in** – на входящий трафик, **out** – на исходящий трафик):

```
Switch3(config)#int vlan 10
```

```
Switch3(config-if)#ip access-group 100 in
```

Этот шаг повторяем для каждого из VLAN-ов.

В результате получим:

для любого вилана могут быть доступны только узлы этого же вилана и сервер Server1.

Самостоятельная работа №3.

На предприятии имеется два отдела, схема сетей которых представлена на рис.8.13.

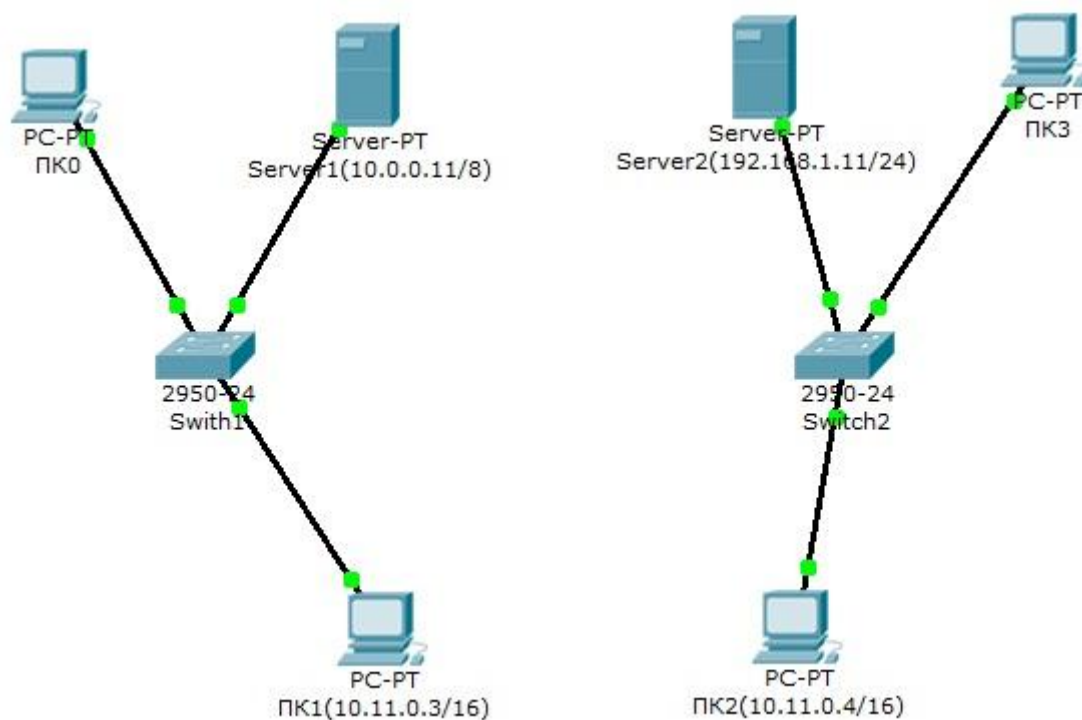


Рис.8.13. Схема сетей отделов предприятия.

Отдел 1 – Switch1, отдел 2 – Switch2.

В каждой сети имеется сервер со службами DHCP, DNS и HTTP (на серверах Server1 и Server2 расположены интернет-сайты отделов).

Компьютеры ПК0 и ПК3 с DHCP серверов своих сетей получают параметры IP адреса и шлюз.

Компьютеры ПК1 и ПК2 находятся в отдельной сети в одном VLAN.

Задание:

Дополните схему сети маршрутизатором или коммутатором третьего уровня, чтобы обеспечить работу корпоративной сети в следующих режимах:

1 - компьютеры ПК0 и ПК3 должны открывать сайты каждого отдела;

2 – компьютеры ПК1 и ПК2 должны быть доступны только друг для друга.

Контрольные вопросы.

1. Для чего создаются виртуальные локальные сети? Каковы их достоинства?
2. Как связываются между собой VLAN и порты коммутатора?
3. Как обеспечивается общение между узлами разных виртуальных сетей?
4. Как обеспечивается управление виртуальными локальными сетями?
5. Можно ли построить VLAN на нескольких коммутаторах? Как это сделать?
6. Для чего служит идентификатор кадра (tag)? Где он размещается?
7. Что такое транк? Как он создается на коммутаторе и маршрутизаторе?
8. Какие команды используются для назначения VLAN на интерфейсы?
9. Какие команды используются для создания транковых соединений?
10. Какие команды используются для верификации VLAN?

Раздел 9. Многопользовательский режим работы.

В программе Cisco Packet Tracer может быть использована функция многопользовательского режима, которая применяется для организации командной работы.

Данный режим работы позволяет делать подключение к сетям, одновременно созданным в разных сессиях работающих программ Cisco Packet Tracer на одном или разных компьютерах. В результате, например, на разных компьютерах могут быть созданы отдельные сегменты корпоративной сети, которые могут быть объединены в единую корпоративную сеть с использованием многопользовательского режима работы.

Лабораторная работа № 13. Многопользовательский режим работы.

В данной работе будет продемонстрировано создание объединенной сети на основе двух разных сетей, созданных в двух отдельно запущенных сессиях программы Cisco Packet Tracer на одном компьютере.

Вы создадите две одновременно работающие сессии программы Cisco Packet Tracer, дважды запустив ее на выполнение.

В первой открытой сессии программы будет создана и настроены две сети: сеть 1 - 11.0.0.0 и сеть 2 - 12.0.0.0. Во второй сессии программы – сеть 11.0.0.0.

Работа в сессии 1.

Запустите программу Cisco Packet Tracer (первая сессия) и создайте две сети (сеть 11.0.0.0 и 12.0.0.0) по схеме, представленной на рис.9.1:

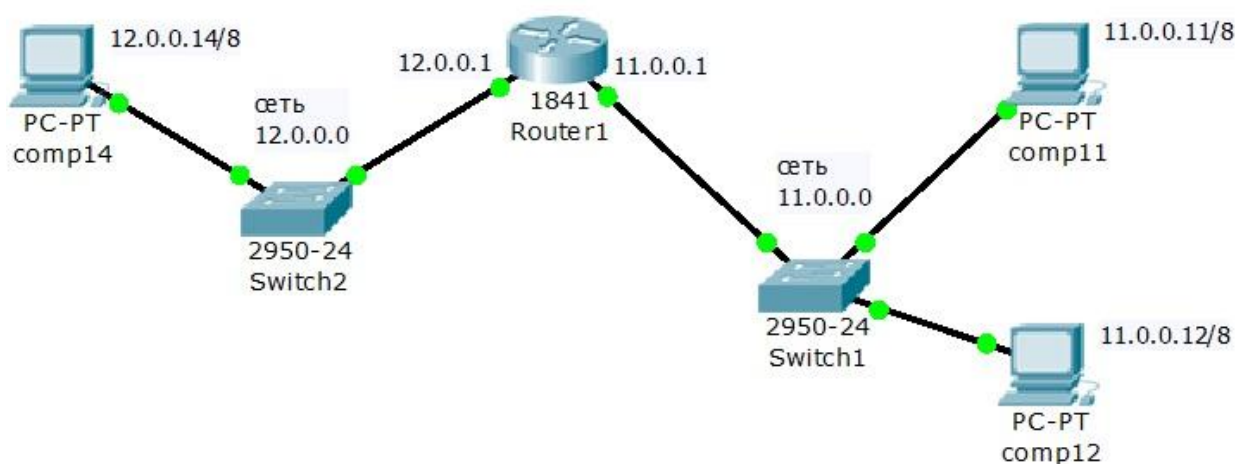


Рис.9.1. Первая сессия – сети 11.0.0.0 и 12.0.0.0.

Задайте названия устройств, как показано на схеме.

Задайте параметры протокола TCP/IP и шлюзы для компьютеров comp11, comp12 и comp14, как показано на схеме (рис.13.1).

Работа в сессии 2.

Не выключая текущую сессию работающей программы, создайте вторую сессию работы программы, запустив повторно Cisco Packet Tracer и создайте сеть по схеме, представленной на рис.9.2:

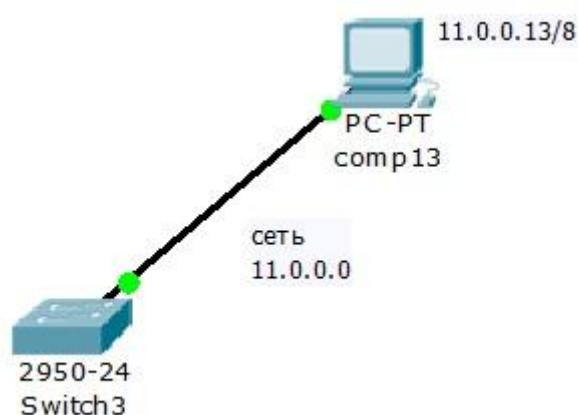


Рис.9.2. Вторая сессия – сеть 11.0.0.0.

Задайте названия устройств и параметры протокола TCP/IP для компьютера comp13, как показано на схеме (рис.9.2).

В результате вы получите работающие сети в разных сессиях программы Cisco Packet Tracer (рис.9.3):

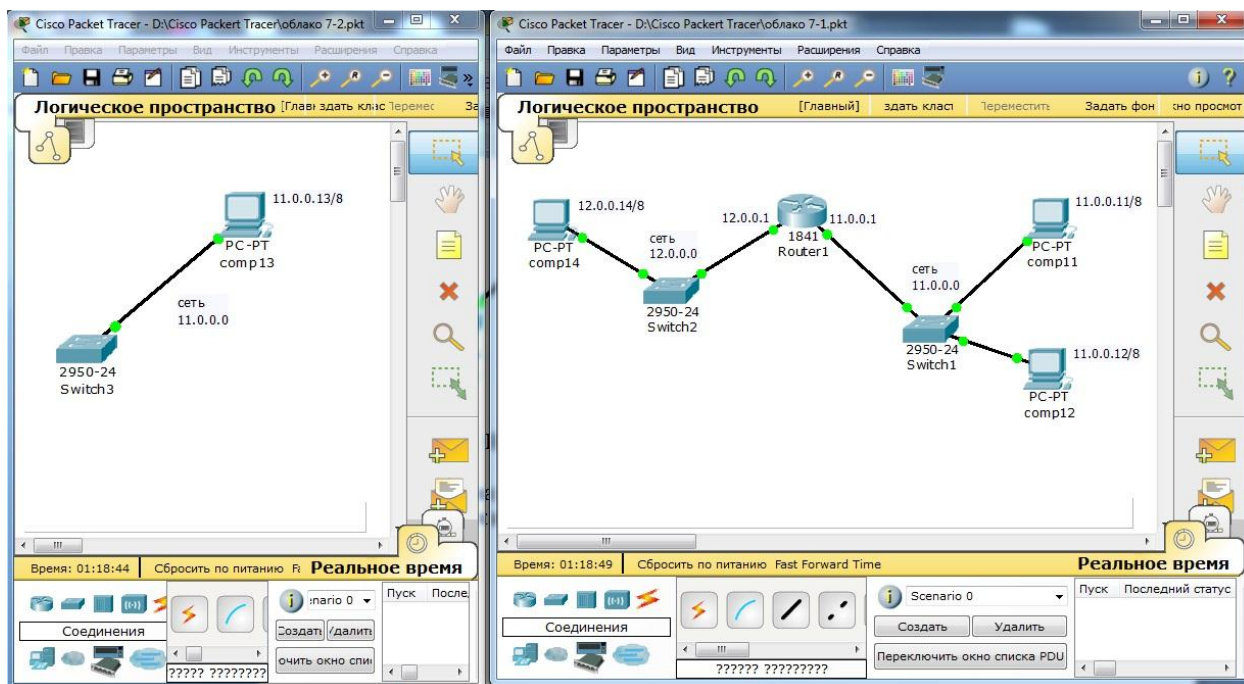


Рис.9.3. Исходные настройки.

Создание многопользовательского соединения.

Для создания многопользовательского соединения необходимо соединить сети, созданных в разных сессиях запущенной программы Cisco Packet Tracer. Для этого выбирается общая сеть (сеть 11.0.0.0), через которую будет проходить соединение и указываются порты соединения: для одной сети – входящий порт, а для другой – выходящий порт.

Объединение сетей в разных сессиях проведем через коммутаторы Switch1 (первая сессия) и Switch3 (вторая сессия).

Для создания многопользовательского соединения необходимо провести следующие этапы настройки:

Этап 1 – подключение к многопользовательскому облаку.

Этап 2 – открытие портов на устройствах, через которые проводится подключение (Switch1 и Switch3).

Этап 3 – создание общего канала связи многопользовательского подключения.

Этап 1 – подключение к многопользовательскому облаку.

Откройте первую сессию.

Создайте многопользовательское подключение. Для этого в инструментах выберите группу «пользовательское соединение» и внесите на схему сети устройство «Multiuser» (рис.9.4):

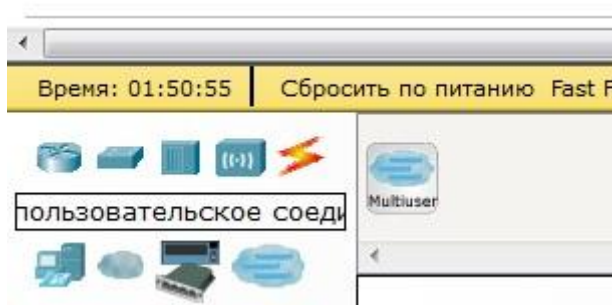


Рис.9.4. Создание многопользовательского подключения.

Соедините коммутатор Switch1 с новым устройством (рис. 9.5). Для этого в группе «Соединения» выберите тип кабеля «Медный кроссовер» и соедините четвертый порт коммутатора FastEthernet0/4 с облаком многопользовательского соединения. При этом задействуйте функцию «Создать новый канал».

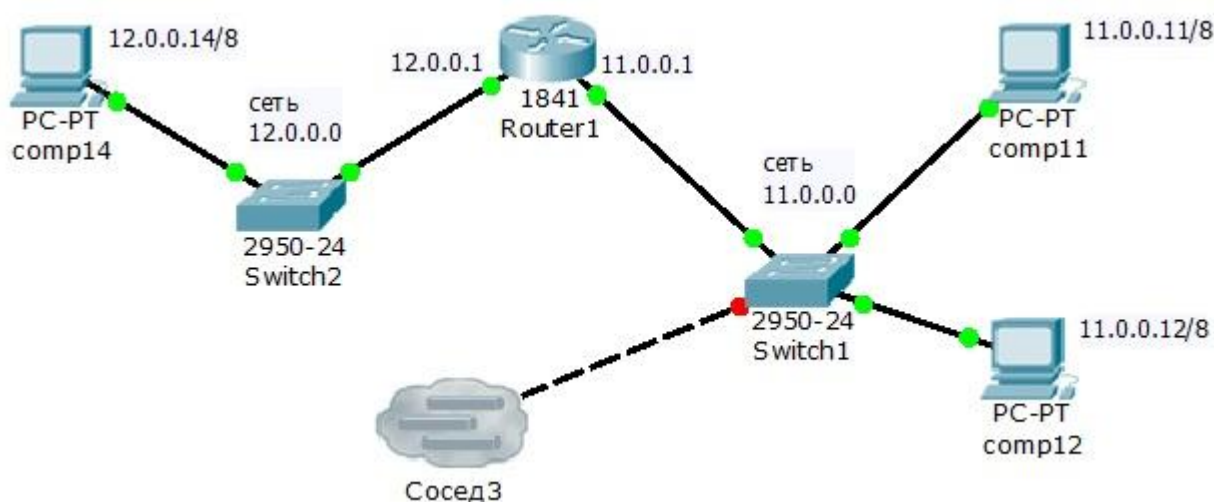


Рис.9.5. Подключение коммутатора к многопользовательскому каналу.

Этап 2 – открытие портов на устройствах, через которые проводится подключение.

Теперь для объединения сетей в разных сессиях необходимо открыть порты на коммутаторах. Пусть это будет четвертый порт на Switch1 и Switch3. Для этого в каждой сессии в главном меню выберите «Расширения» – «Многопользовательский режим» - «Видимость порта» (рис. 9.6).

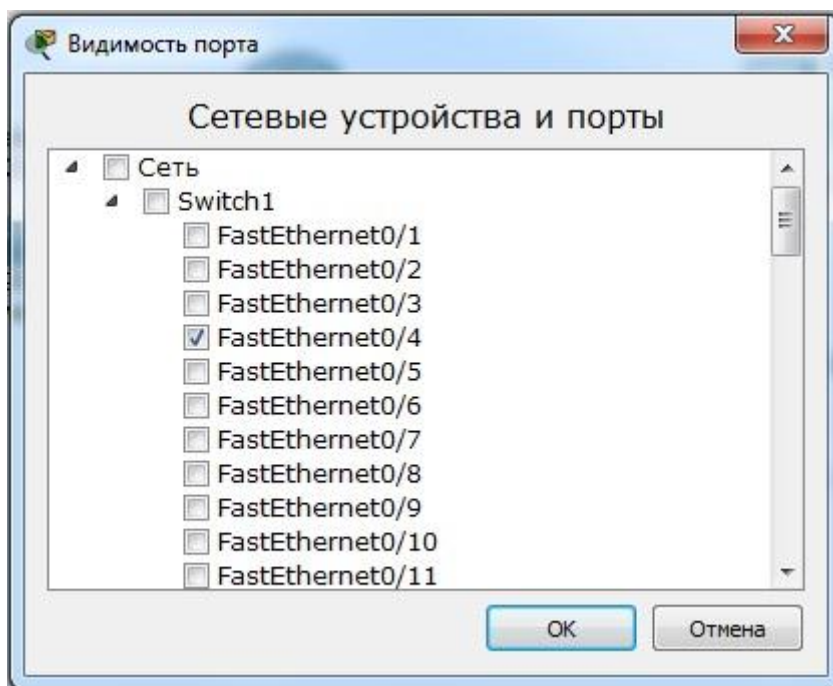


Рис. 9.6. Включение четвертого порта коммутатора.

Этап 3 – создание общего канала доступа многопользовательского подключения.

Необходимо выбрать реально работающую сеть для создания общего канала доступа. Возможны два варианта:

вариант 1 – вы делаете многопользовательское соединение на разных компьютерах;

вариант 2 - вы делаете многопользовательское соединение на одном компьютере в разных сессиях программы

В первом случае подключение ведется через реальный IP адрес компьютера в локальной сети.

Во втором случае возможны два варианта подключения:

- через Localhost по адресу 127.0.0.1;

- через реальный IP адрес компьютера в локальной сети.

Переключитесь во вторую сессию.

Для этого в главном меню выберите «Расширения» – «Многопользовательский режим» - «Прослушивание» (рис. 9.7). Уберите пароль и в разделах «Существующие удаленные сети» и «Новые удаленные сети» включите режим «Напоминание».

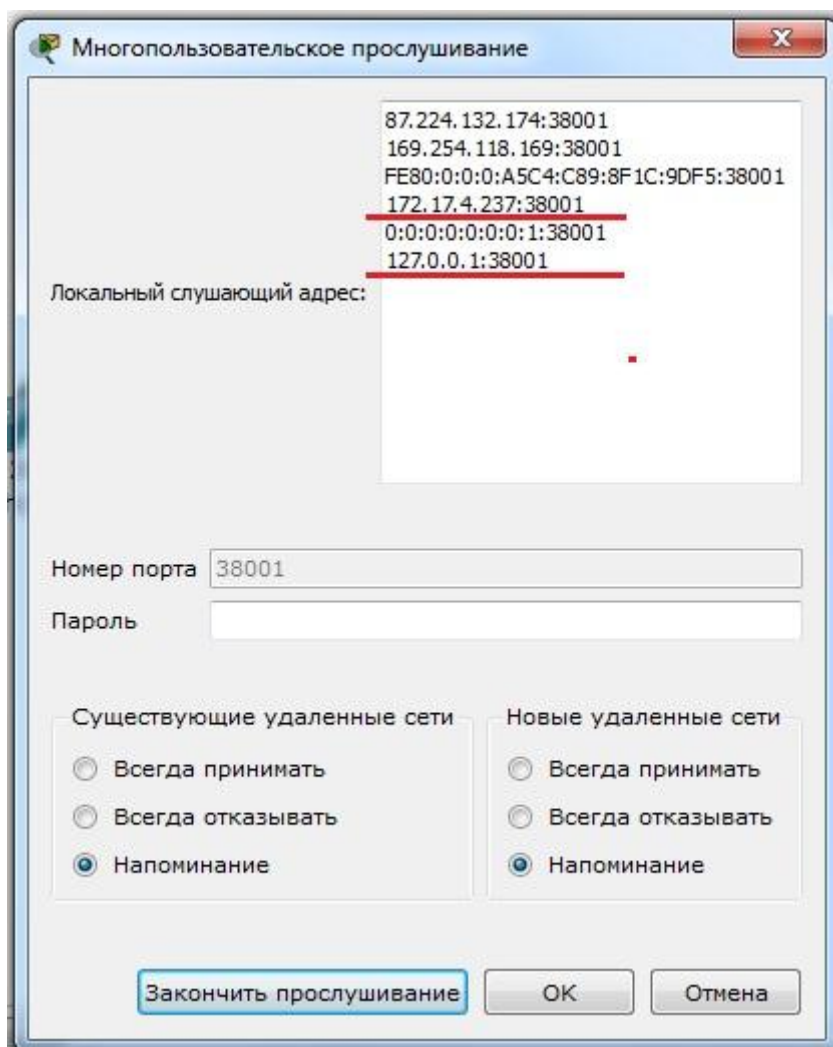


Рис. 9.7. Настройка общего канала доступа.

В верхней части показаны прослушиваемые сети. В нашем случае это сеть 172.17.0.0 и localhost.

Сеть 172.17.0.0 – локальная сеть, к которой подключен наш компьютер.

Точка входа задается ip адресом и портом: ip адрес 172.17.4.237, порт входа 38001.

Localhost – сеть 127.0.0.0, ip адрес 127.0.0.1, порт 38001.

Сделаем подключение через localhost.

Переключитесь в первую сессию.

Зайдите в настройки устройства «Сосед3».

Выберите тип соединения «Исходящее» и задайте имя общей сети в вашей топологии «Lan 11.0.0.0», задайте точку входа в сеть 2 - localhost:38001 и нажмите кнопку «Соединить» (рис. 9.8):

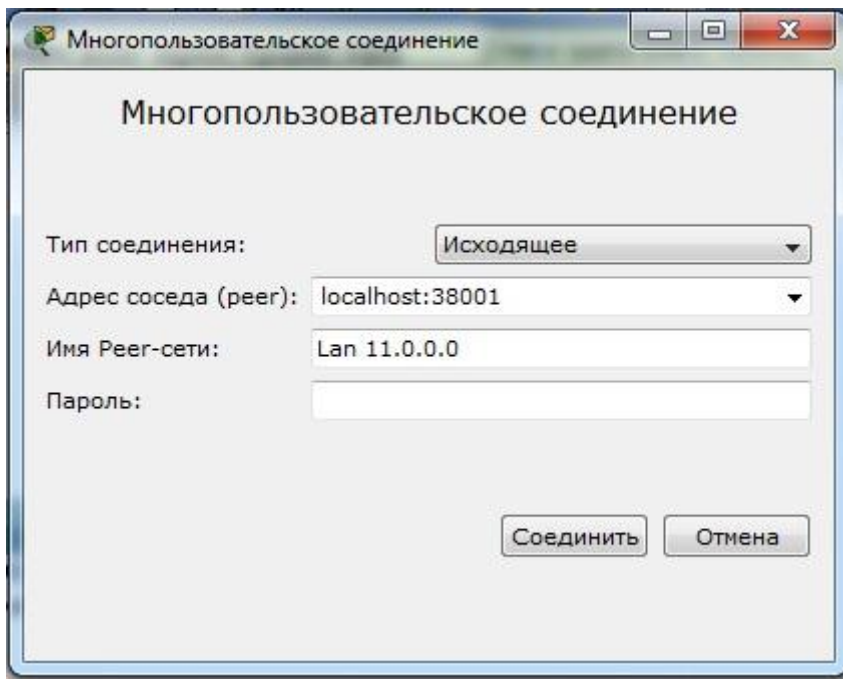


Рис. 9.8. Выбор точки входа.

В результате во второй сессии появится уведомление о соединении (рис.13.9):

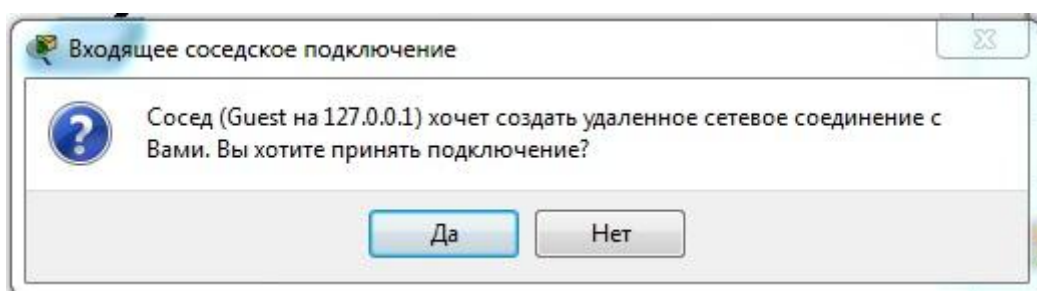


Рис. 9.9.Создание соединения.

В результате во второй сессии появится облако многопользовательского соединения.

Соедините созданное облако с коммутатором Swith3.

Для этого в группе «Соединения» выберите тип кабеля «Медный кроссовер» и соедините четвертый порт FastEthernet0/4 на Swith3 с облаком многопользовательского соединения через Канал0 (рис.9.10):

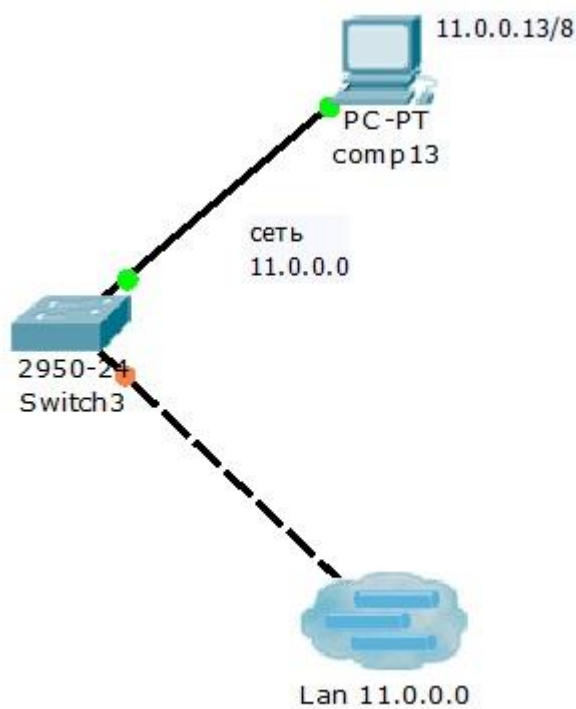


Рис.9.10. Подключение второй сессии к общему каналу.

Проверьте командой **ping** связь всех компьютеров во всех сетях между собой.

Самостоятельная работа №4.

Создайте многопользовательское соединение двух разных сессий на одном компьютере.

Используя статическую маршрутизацию создайте в каждой сессии по две сети.

Состав каждой сети: клиентский компьютер и сервер с сайтом.

Задание: все компьютеры должны открывать все сайты в обеих сессиях.

Контрольные вопросы.

1. Перечислите основные возможности многопользовательского режима работы.
2. Как организуется сеанс связи в многопользовательском режиме работы?
3. Перечислите типы соединений в многопользовательском режиме работы?
4. Через какие сетевые устройства и порты организуется связь в многопользовательском режиме работы?
5. Какие сети выбираются для общего канала доступа?
6. Опишите этапы создания многопользовательского соединения.
7. Как определяются порты для организации сеанса связи при организации многопользовательского режима работы?

Раздел 10. Списки управления доступом ACL (Access Control List).

Списки доступа позволяют создавать правила управления трафиком, по которым будет происходить межсетевое взаимодействие как в локальных, так и в корпоративных сетях.

Существует шестнадцать типов списков доступа, но наиболее часто используются два типа: **standart** – стандартные (номера с 1 по 99) и **extended** – расширенные (номера с 100 по 199 или с 2000 по 2699). Различия между этими двумя списками заключаются в возможности фильтровать пакеты не только по IP – адресу, но и по другим различным параметрам.

Стандартные списки обрабатывают только входящие IP адреса источников, т.е. ищут соответствие только по IP адресу отправителя. Расширенные списки работают со всеми адресами корпоративной сети и дополнительно могут фильтровать трафик по портам и протоколам.

Работа списка доступа напрямую зависит от порядка следования строк в этом списке, где в каждой строке записано правило обработки трафика. Просматриваются все правила списка с первого до последнего по порядку, но просмотр завершается, как только было найдено первое соответствие, т.е. для пришедшего пакета было найдено правило, под которое он подпадает. После этого остальные правила списка игнорируются. Если пакет не подпал ни под одно из правил, то включается правило по умолчанию:

access-list номер_списка deny any

которое запрещает весь трафик по тому интерфейсу сетевого устройства, к которому данный список был применен.

Для того, чтобы начать использовать список доступа, необходимо выполнить следующие три этапа:

- 1 – создать список;
- 2 – наполнить список правилами обработки трафика;
- 3 – применить список доступа к интерфейсу устройства на вход или на выход этого интерфейса.

Этап первый – создание списка доступа:

Стандартный список:

```
Switch3 (config) #ip access-list standart 10
```

(создается стандартный список доступа под номером 10, в данном случае создается на коммутаторе)

Расширенный список:

```
Router1 (config) #ip access-list extended 100
```

(создается расширенный список доступа под номером 100, в данном случае создается на маршрутизаторе).

Этап второй – ввод правил в список доступа:

Каждое, правило в списке доступа содержит три важных элемента:

- 1 - число, идентифицирующее список при обращении к нему в других частях конфигурации маршрутизатора или коммутатора третьего уровня;
- 2 - инструкцию **deny** (запретить) или **permit** (разрешить);
- 3 - идентификатор пакета, который задается по одному из трех вариантов:
 - адрес сети (например 192.168.2.0 0.0.0.255) – где вместо маски подсети указывается шаблон маски подсети;
 - адрес хоста (host 192.168.2.1);
 - любой IP адрес (**any**).

Пример стандартного списка доступа №10:

```
access-list 10 deny host 11.0.0.5
access-list 10 deny 12.0.0.0 0.255.255.255
access-list 10 permit any
```

В этом списке:

- запрещен весь трафик хосту с IP адресом 11.0.0.5;
- запрещен весь трафик в сети 12.0.0.0/8 (в правиле указывается не реальная маска подсети, а ее шаблон);
- весь остальной трафик разрешен.

В расширенных списках доступа вслед за указанием действия ключами **permit** или **deny** должен находиться параметр с обозначением протокола (возможны протоколы IP, TCP, UDP, ICMP), который указывает, должна ли выполняться проверка всех пакетов IP или только пакетов с заголовками ICMP, TCP или UDP. Если проверке подлежат номера портов TCP или UDP, то должен быть указан протокол TCP или UDP (службы FTP и WEB используют протокол TCP).

При создании расширенных списков в правилах доступа можно включать фильтрацию трафика по протоколам и портам. Для указания портов в правиле доступа указываются следующие обозначения (таблица 10.1):

Таблица 10.1.

обозначение	действие
lt n	Все номера портов, меньшие n.
gt n	Все номера портов, большие n.
eq n	Порт n
neq n	Все порты, за исключением n.
range n m	Все порты от n до m включительно.

Распространенные приложения и соответствующие им стандартные номера портов приведены в следующей таблице 10.2:

Таблица 10.2.

Номер порта	Протокол	Приложение	Ключевое слово в команде access_list
20	TCP	FTP	data ftp_data
21	TCP	Управление сервером FTP	ftp
22	TCP	SSH	
23	TCP	Telnet	telnet
25	TCP	SMTP	Smtп
53	UDP, TCP	DNS	Domain
67, 68	UDP	DHCP	nameserver
69	UDP	TFTP	Tftp
80	TCP	HTTP (WWW)	www
110	TCP	POP3	pop3
161	UDP	SNMP	Snmp

Пример расширенного списка доступа №111:

```
! Запретить трафик на порту 80 (www-трафик)  
ip access-list 111 deny tcp any any eq 80  
ip access-list 111 deny ip host 10.0.0.15 host 12.0.0.5  
ip access-list 111 permit ip any any
```

interface ethernet0

```
! Применить список доступа 111 к исходящему трафику  
ip access-group 111 out
```

В этом списке внешние узлы не смогут обращаться на сайты внутренней сети, т.к. список доступа был применен на выход (для внешних узлов) интерфейса, а так же узлу 10.0.0.15 запрещен доступ к узлу 12.0.0.5
Остальной трафик разрешен.

Этап третий – применение списка доступа.

Списки доступа могут быть использованы для двух типов устройств:

- 1 – на маршрутизаторе;
- 2 - на коммутаторе третьего уровня.

На каждом интерфейсе может быть включено два списка доступа: только один список доступа для входящих пакетов и только один список для исходящих пакетов.

Каждый список работает только с тем интерфейсом, на который он был применен и не действует на остальные интерфейсы устройства, если он там не применялся.

Однако один список доступа может быть применен к разным интерфейсам.

Применение списка доступа к устройству осуществляется следующими командами:

```
interface ethernet0/0/0  
ip access-group 1 in  
ip access-group 2 out
```

В данном случае к интерфейсу ethernet0/0/0 применили два списка доступа: список доступа №1 – на вход интерфейса (т.е. для внутренних адресов); список доступа №2 – на выход интерфейса (применение к внешней сети).

Чтобы просмотреть все созданные списки доступа и применение их к интерфейсам устройства используйте следующие команды:

Команда просмотра списков доступа:

```
Router# Sh access-list
```

Просмотр текущей конфигурации устройства и привязки списков к интерфейсам:

```
Router# Show running-config
```

Просмотр сохраненной конфигурации:

```
Router# Show configuration
```

Сохранение текущей конфигурации:

```
Router# write memory
```

Или

```
Router# copy run start
```

Команда удаления списка доступа:

```
interface ethernet0/0/0 - выбор нужного интерфейса  
no access-list номер_списка – удаление списка в выбранном интерфейсе
```

Лабораторная работа № 14. Списки доступа.

Создайте схему сети, как показано на рис.10.1.

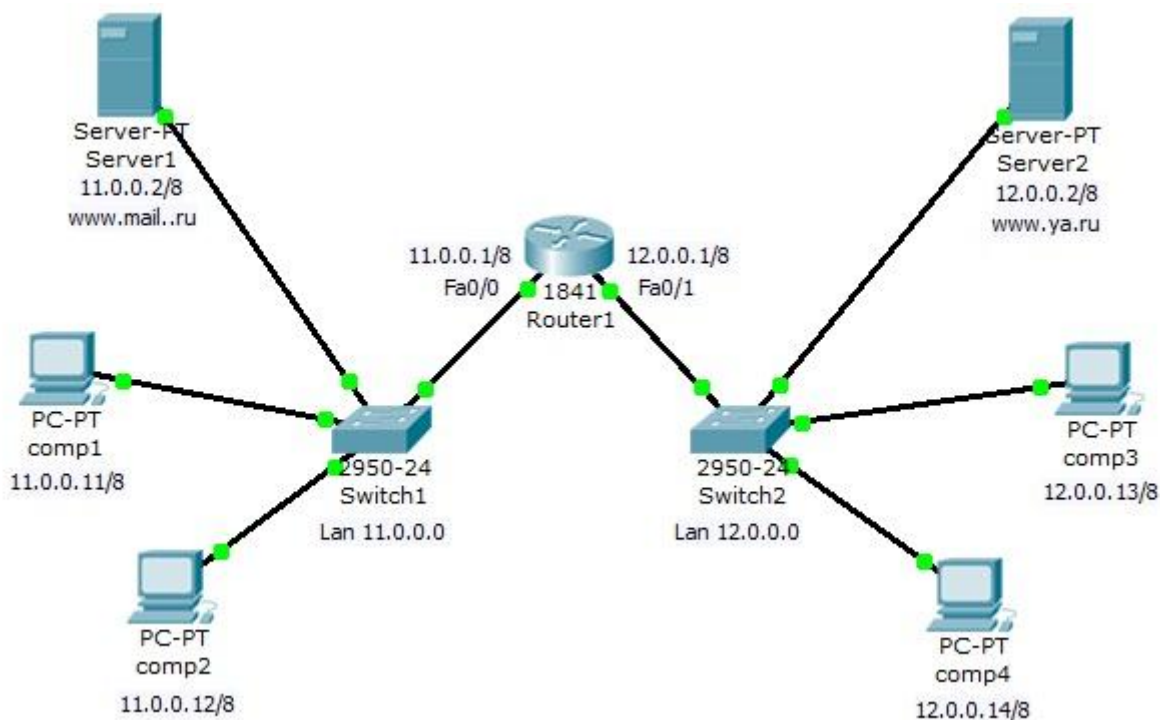


Рис.10.1. Схема корпоративной сети.

Задача:

- 1 - Компьютеры comp1 и comp2 должны открывать все сайты, но им запрещено входить на компьютеры comp3 и comp4.
- 2 - Компьютеры comp3 и comp4 доступны друг для друга и должны открывать только сайт своей сети, сеть 11.0.0.0 для них недоступна.

Создадим стандартный список доступа, где укажем правила блокировки на хосты comp3 и comp4 и применим этот список на выход интерфейса Fa0/0. Включите привилегированный режим и войдите в конфигурацию роутера:

```
Router1>en
Router1#conf t
```

Создадим стандартный список доступа и введем правила доступа:

```
Router1 (config) #ip access-list standard 10
Router1 (config-std-nacl) #deny host 12.0.0.13
Router1 (config-std-nacl) #deny host 12.0.0.14
Router1 (config-std-nacl) #permit any
```

Здесь мы разрешили весь трафик, за исключением двух адресов: 12.0.0.13 и 12.0.0.14.

Просмотрим созданный список доступа в настройках роутера. Для этого надо выйти из режима конфигурации роутера и ввести команду просмотра списков на устройстве **sh access-list**:

```
Router1#sh access-list  
Standard IP access list 10  
    deny host 12.0.0.13  
    deny host 12.0.0.14  
    permit any  
Router1#
```

Применим созданный список на выход интерфейса Fa0/0:

```
Router1#  
Router1#conf t  
Router1 (config) #interface fa0/0  
Router1 (config-if) #ip access-group 10 out
```

В результате того, что список доступа был применен к выходу интерфейса сети 11.0.0.0 мы получили следующую политику доступа:

1 – пакеты, входящие на роутер из сети 11.0.0.0 получают блокировку на два внешних адреса – 12.0.0.13 и 12.0.0.14;
2 – всем внешним пакетам, входящим из роутера в сеть 11.0.0.0 разрешается все, кроме двух адресов - 12.0.0.13 и 12.0.0.14 (этим адресам запрещен вход в сеть 11.0.0.0)

Просмотрим привязку списка доступа к интерфейсу Fa0/0 в конфигурации роутера:

```
Router1 (config-if) #exit  
Router1 (config) #exit  
Router1#  
Router1#sh running-config
```

Используя данную команду, вы увидите полную конфигурацию роутера, в том числе и привязку списка доступа к конкретному интерфейсу (в данном случае на выход интрфейса):

```
interface FastEthernet0/0  
ip address 11.0.0.1 255.0.0.0  
ip access-group 10 out  
duplex auto
```

speed auto

!

Проверьте созданную политику доступа к ресурсам сети. Должны выполняться следующие правила:

- 1 - компьютеры comp3 и comp4 доступны друг для друга и должны открывать только сайт своей сети, вход в сеть 11.0.0.0 им заблокирован;
- 2 – сервера Server2 доступен всем ресурсам сети;
- 3 - компьютерам comp1 и comp2 доступны все ресурсы, кроме адресов 12.0.0.13 и 12.0.0.14.

Самостоятельная работа №5.

Создайте сеть, представленную на рис 10.2.

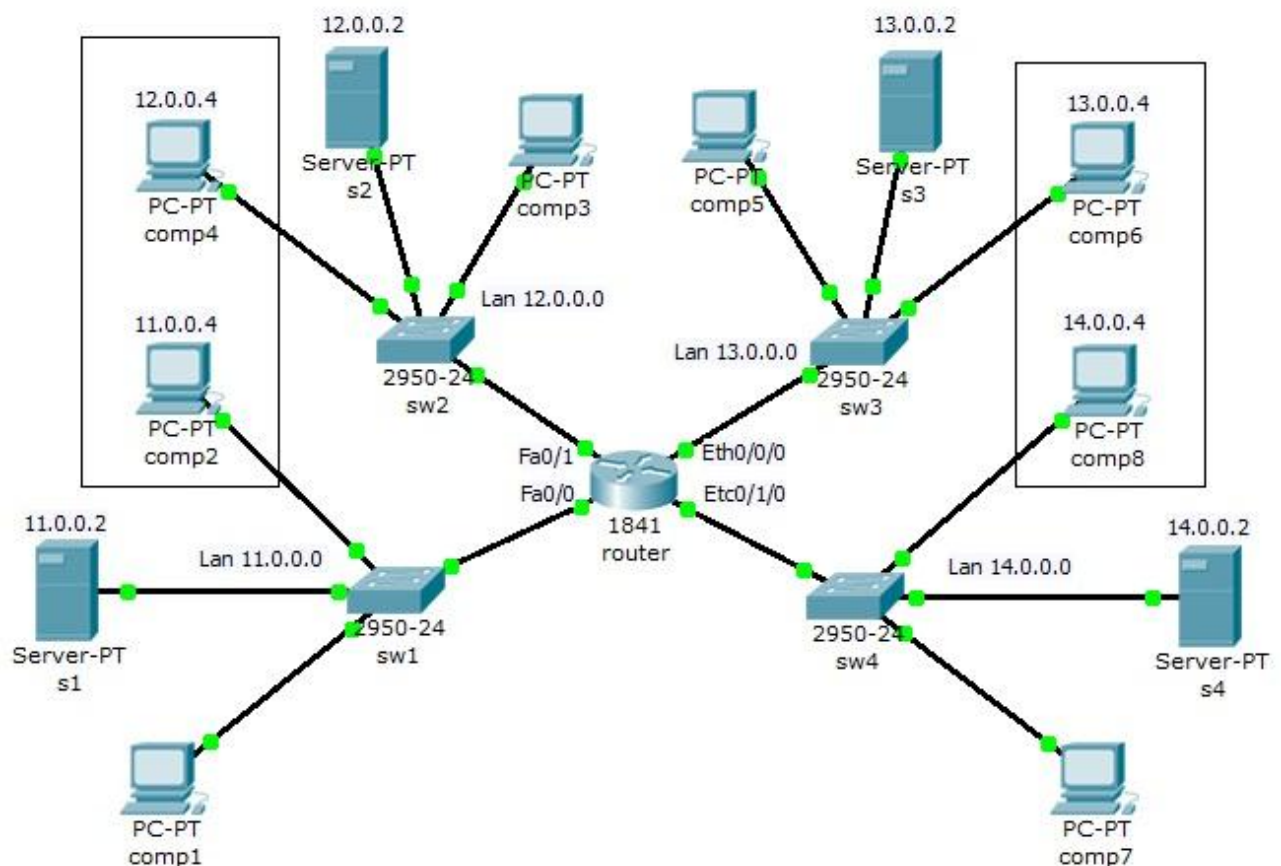


Рис.10.2. Схема корпоративной сети.

Корпоративная сеть состоит из четырех сетей:

- сеть 1 – 11.0.0.0/8;
- сеть 2 – 12.0.0.0/8;
- сеть 3 – 13.0.0.0/8;
- сеть 4 – 14.0.0.0/8.

В каждой сети на сервере установлен Web сайт.

Задание:

Компьютеру comp2 доступны только компьютеры своей сети и comp4.

Компьютеру comp4 доступны только компьютеры своей сети и comp2.

Компьютеру comp8 доступны только компьютеры своей сети и comp6.

Компьютеру comp6 доступны только компьютеры своей сети и comp8.

Компьютеры comp1, comp3, comp5 и comp7 должны открывать все сайты на серверах S1, S2, S3 и S4.

Самостоятельная работа №6.

Создайте сеть, представленную на рис 10.3.

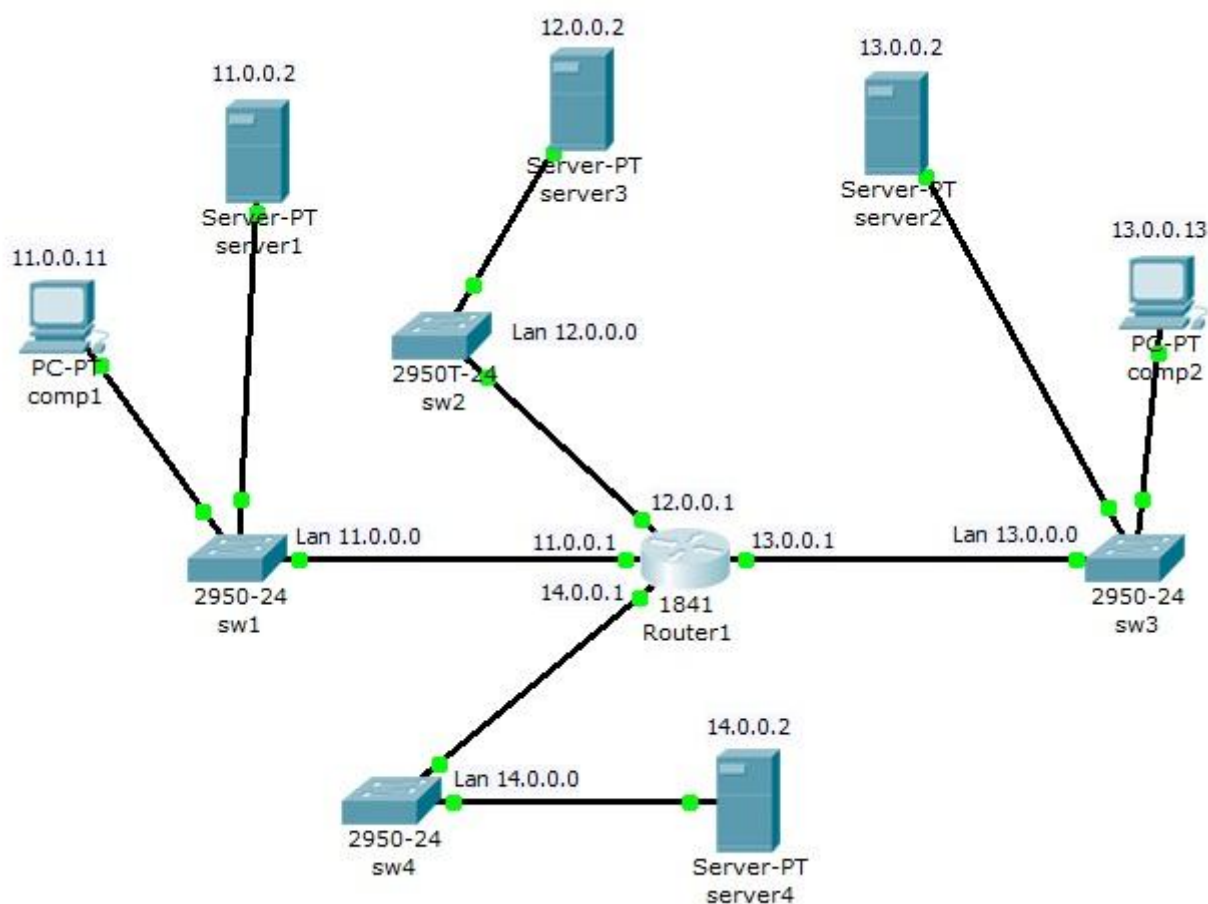


Рис.10.3 Схема корпоративной сети.

Корпоративная сеть состоит из четырех сетей:

сеть 1 – 11.0.0.0/8;

сеть 2 – 12.0.0.0/8;

сеть 3 – 13.0.0.0/8;

сеть 4 – 14.0.0.0/8.

В каждой сети на сервере установлен Web сайт.

Задание:

- 1 - Сеть 14.0.0.0 недоступна из сети 11.0.0.0.
- 2 - Компьютерам comp1 и comp2 разрешить открытие сайта на server3, но запретить прослушивание server3 по команде ping.
- 3 – Компьютеру comp1 разрешить доступ на server2, но запретить открытие сайта на этом сервере.
- 4 – Компьютеру comp2 разрешить доступ на server1, но запретить открытие сайта на server1, разрешить доступ и открытие сайта на server4.

Самостоятельная работа №7.

Создайте схему сети, представленную на рис.10.4. Задайте сети и адресацию произвольно.

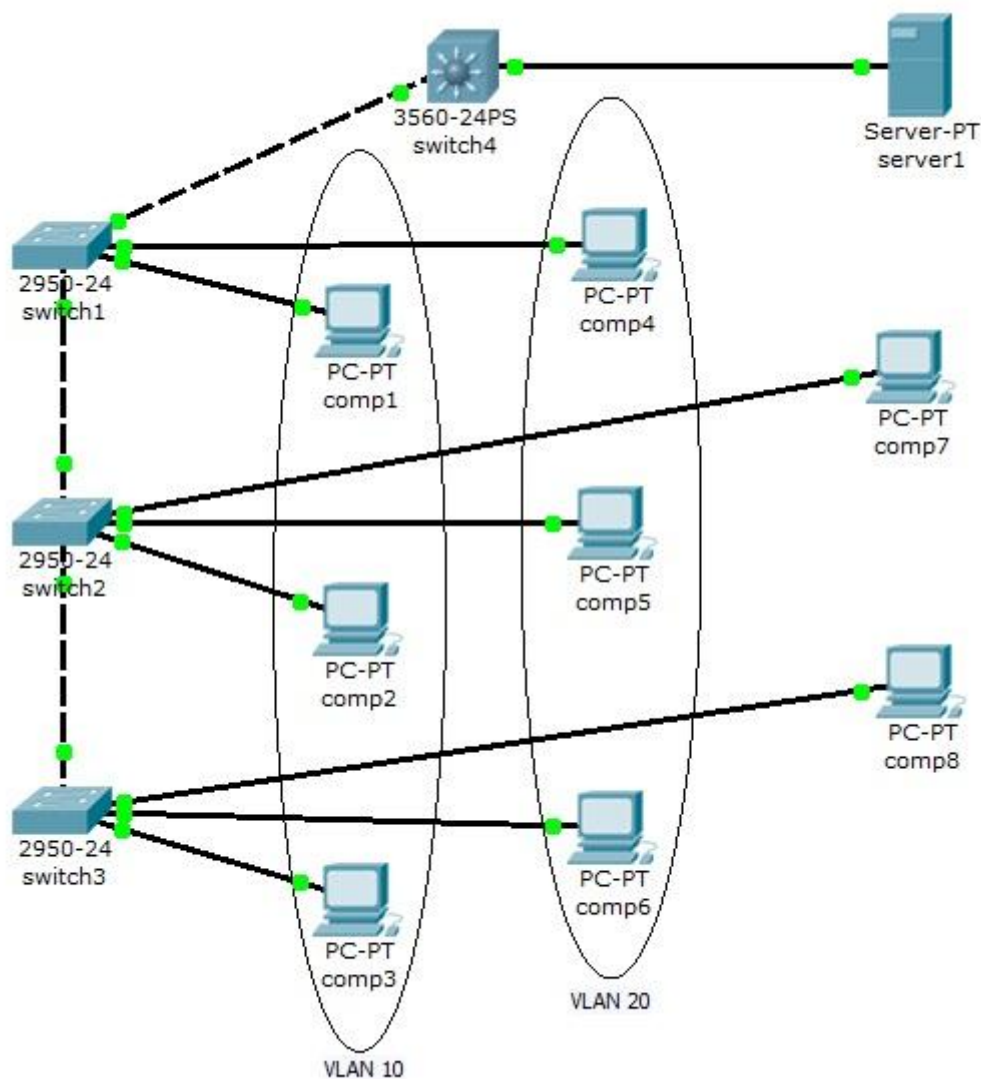


Рис.10.4. Схема корпоративной сети.

Задание:

1 – компьютеры comp1, comp2 и comp3 находятся в одном VLAN 10, доступны только друг для друга и имеют доступ к server1.

2 – компьютеры comp4, comp5 и comp6 находятся в одном VLAN 20, доступны только друг для друга и имеют доступ к server1.

3 - компьютеры comp7 и comp8 доступны только друг для друга и имеют доступ к server1.

Самостоятельная работа №8.

Создайте схему сети, представленную на рис.10.5.

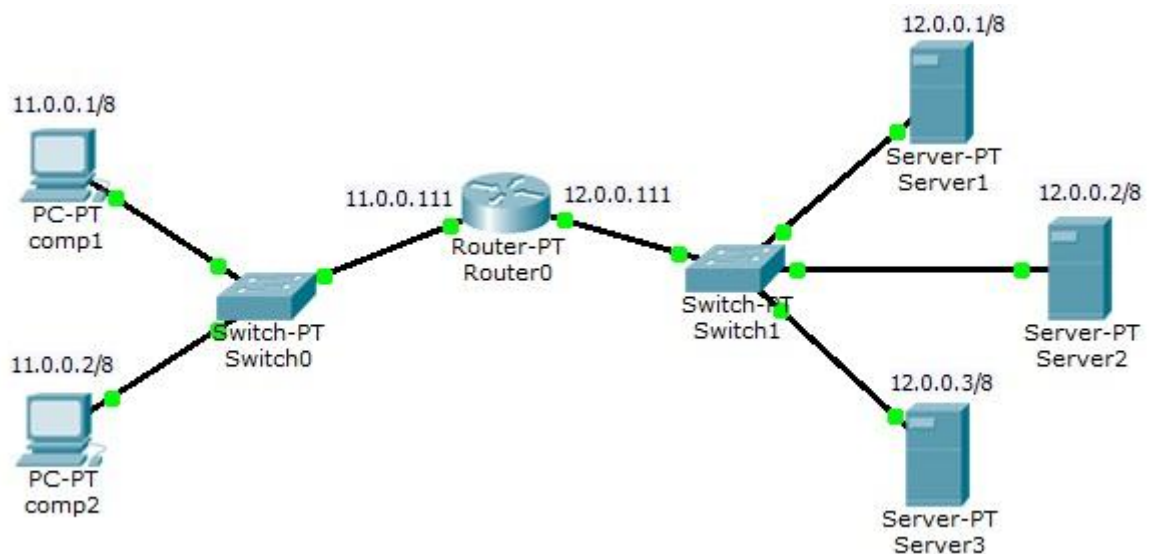


Рис. 10.5. Схема корпоративной сети.

На всех трех серверах установлены службы Web и FTP.

Создайте списки доступа, задающие для компьютеров comp1 и comp2 следующие правила доступа в сети:

Компьютер comp1:

Server1 – разрешить доступ на FTP;

Server2 - разрешить доступ на Web;

Server3 - разрешить доступ на Web и FTP.

Компьютер comp2:

Server1 – разрешить доступ на Web;

Server2 - разрешить доступ на FTP;

Server3 - разрешить доступ на Web и FTP.

Контрольные вопросы.

1. Какие параметры контролирует расширенные списки доступа?
2. Приведите пример команды, разрешающей передачу пакетов от хоста на все веб-сервера.
3. Перечислите основные типы списков доступа.
4. Что такое шаблон маски подсети и приведите примеры его использования в списках доступа.
5. Какое правило обработки сетевого трафика задает следующий список доступа: `Ip access-list 111 deny tcp any any eq 80`
6. Локальная сеть соединена с роутером по интерфейсу Fa0/0, а внешняя сеть соединена по интерфейсу Fa0/1. Из локальной сети запрещен вход во внешнюю сеть, а из внешней сети запрещено входить на FTP сервер, расположенный во внутренней сети. Для реализации этих правил был создан список доступа. Назовите интерфейс и в каком направлении (на вход или на выход), к которому следует применить созданный список доступа.
7. Для какого варианта не может быть проведено сравнение на основе расширенного списка доступа IP?
 - протокол;
 - IP адрес отправителя;
 - IP адрес получателя;
 - имя файла для передачи по протоколу FTP.
8. Назовите, какой шаблон маски соответствует сети 10.16.0.0/12?
9. В списке доступа содержится следующее правило:
`Permit any host 192/168/1/1/it 25`
Какие номера портов оно обрабатывает?
10. Напишите правило доступа для входа в сеть 51.52.32.0/21

Литература.

1. Д. Бони. Руководство по Cisco IOS. Изд. Питер, Русская Редакция, 2008, 786 с.
2. К. Кеннеди, К. Гамильтон. Принципы коммутации в локальных сетях Cisco. Изд. Вильямс, 2003, 976 с.
3. Джером Ф. Димарцио. Маршрутизаторы CISCO. Пособие для самостоятельного изучения. Изд. Символ-Плюс, 2003, 512 с.
4. И.В. Руденко Маршрутизаторы CISCO для IP-сетей. Изд. КУДИЦ-ОБРАЗ, 2003, 656 с.
5. Вито Амато. Основы организации сетей Cisco. Том 1. Изд. Вильямс, 2002, 512 с.
6. Тодд Леммл, Кевин Хейлз. CCNP: Настройка коммутаторов CISCO. Экзамен 640-504. Изд. Лори, 2002 464 с.
7. Уэнделла Одома. «Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 640- 822» (3-е издание). Изд. Вильямс, серия Cisco Press, 2013.
8. Cisco ICND 1. Руководство для студента. Изд. Cisco, 2009.
9. Документация к программе Cisco Packet Tracer.
10. Интернет – ресурсы: www.cisco.com, litr-admin.ru.