Федеральное агентство морского и речного транспорта

Федеральное государственное бюджетное образовательное учреждение высшего образования

ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МОРСКОГО И РЕЧНОГО ФЛОТА

имени адмирала С.О. МАКАРОВА

КАФЕДРА ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ И ИНФОРМАТИКИ

А. Н. Егоров, А. Е. Журавлев, А. А. Базунов, О. В. Румянцев

**МОДЕЛИРОВАНИЕ**

**КОМПЬЮТЕРНЫХ СЕТЕЙ**

**УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ**

Санкт-Петербург

Издательство ГУМРФ им. адм. С.О. Макарова

2015

УДК 512

ББК 22.12

**Рецензент**:

*Марлей В. Е.*  
д-р техн. наук, проф., зав. кафедрой вычислительных систем и информатики Государственного университета морского и речного флота имени адмирала С. О. Макарова

**А.Н. Егоров и др.** Моделирование компьютерных сетей: учебно-методическое пособие / А.Н. Егоров, А.Е. Журавлев, А.А. Базунов, О.В Румянцев — СПб.: Изд-во ГУМРФ имени адмирала С. О. Макарова, 2015. — 191 с.

В учебно-методическом пособии рассматриваются основные методы проектирования и моделирования компьютерных сетей, в которых используется оборудование Cisco Systems. Детально описываются процессы построения локальных и глобальных корпоративных сетей, приводятся типовые конфигурации коммутаторов и маршрутизаторов Cisco. В качестве среды разработки используется учебная версия программы Cisco Packet Tracer 6, которая является сложной средой симуляции, визуализации и оценки компьютерных сетей уровня CCNA.

Учебное пособие предназначено для студентов второго и третьего курсов, обучающихся по направлениям 230700.62 «Прикладная информатика» и 230400.62 «Информационные системы и технологии» и изучающих курсы компьютерных сетей и инфокоммуникационных систем в качестве основной литературы. Учебно-методическое пособие также может быть использовано студентами, аспирантами и преподавателями в ходе подготовки к экзамену для получения профессиональной сертификации Cisco CCNA.

**УДК 512**

**ББК 22.12**

© А.Н. Егоров, А.Е. Журавлев, А.А Базунов, О.В Румянцев 2015.

© Государственный университет морского и речного флота имени адмирала С. О. Макарова, 2015.

Оглавление

[ВВЕДЕНИЕ 5](#_Toc419447582)

[Лабораторная работа №1. среда Cisco Packet Tracer 6](#_Toc419447583)

[1.1. Обзор интерфейса 6](#_Toc419447584)

[1.2. Логическое рабочее пространство 9](#_Toc419447585)

[1.3. Обзор режима реального времени 12](#_Toc419447586)

[1.4. Обзор режима симуляции 14](#_Toc419447587)

[1.5. Физическое рабочее пространство 15](#_Toc419447588)

[1.6. Контрольные задания 20](#_Toc419447589)

[Лабораторная работа №2. Технология виртуальных локальных сетей VLAN и протокол VTP 21](#_Toc419447590)

[2.1. Цели и задачи 21](#_Toc419447591)

[2.2. Теоретические сведения 21](#_Toc419447592)

[2.3. Методические указания 25](#_Toc419447593)

[2.4. Заключение 31](#_Toc419447594)

[2.5. Контрольные задания 33](#_Toc419447595)

[Лабораторная работа №3. Отказоустойчивые связи в компьютерных сетях 34](#_Toc419447596)

[3.1. Цели и задачи 34](#_Toc419447597)

[3.2. Теоретические сведения 34](#_Toc419447598)

[3.3. Методические указания 41](#_Toc419447599)

[3.4. Заключение 47](#_Toc419447600)

[3.5. Контрольные задания 48](#_Toc419447601)

[Лабораторная работа №4. Коммутаторы третьего уровня и Организация IP-подсетей 49](#_Toc419447602)

[4.1. Цели и задачи 49](#_Toc419447603)

[4.2. Теоретические сведения 49](#_Toc419447604)

[4.3. Методические указания 53](#_Toc419447605)

[4.4. Заключение 62](#_Toc419447606)

[4.5. Контрольные задания 62](#_Toc419447607)

[Лабораторная работа №5. списки доступа ACL 64](#_Toc419447608)

[5.1. Цели и задачи 64](#_Toc419447609)

[5.2. Теоретические сведения 64](#_Toc419447610)

[5.3. Методические указания 69](#_Toc419447611)

[5.4. Заключение 75](#_Toc419447612)

[5.5. Контрольные задания 76](#_Toc419447613)

[Лабораторная работа №6. Маршрутизаторы и Статические маршруты 77](#_Toc419447614)

[6.1. Цели и задачи 77](#_Toc419447615)

[6.2. Теоретические сведения 77](#_Toc419447616)

[6.3. Методические указания 80](#_Toc419447617)

[6.4. Заключение 89](#_Toc419447618)

[6.5. Контрольные задания 90](#_Toc419447619)

[6.6. Легенда 91](#_Toc419447620)

[Лабораторная работа №7. Динамическая маршрутизация. Протоколы RIP, OSPF и EIGRP 92](#_Toc419447621)

[7.1. Цели и задачи 92](#_Toc419447622)

[7.2. Теоретические сведения 92](#_Toc419447623)

[7.3. Методические указания 98](#_Toc419447624)

[7.4. Заключение 108](#_Toc419447625)

[7.5. Контрольные задания 109](#_Toc419447626)

[Лабораторная работа №8. механизм трансляции сетевых адресов nat 110](#_Toc419447627)

[8.1. Цели и задачи 110](#_Toc419447628)

[8.2. Теоретические сведения 110](#_Toc419447629)

[8.3. Методические указания 114](#_Toc419447630)

[8.4. Заключение 119](#_Toc419447631)

[8.5. Контрольные задания 120](#_Toc419447632)

[8.6. Легенда 122](#_Toc419447633)

[Лабораторная работа №9. Распределенные сети. Технология Frame Relay. 124](#_Toc419447634)

[9.1. Цели и задачи 124](#_Toc419447635)

[9.2. Теоретические сведения 124](#_Toc419447636)

[9.3. Методические указания 128](#_Toc419447637)

[9.4. Заключение 136](#_Toc419447638)

[9.5. Контрольные задания 137](#_Toc419447639)

[9.6. Легенда 140](#_Toc419447640)

[Лабораторная работа №10. Виртуальные частные сети VPN 141](#_Toc419447641)

[10.1. Цели и задачи 141](#_Toc419447642)

[10.2. Теоретические сведения 141](#_Toc419447643)

[10.3. Методические указания 146](#_Toc419447644)

[10.4. Заключение 153](#_Toc419447645)

[10.5. Контрольные задания 154](#_Toc419447646)

[10.6. Легенда 156](#_Toc419447647)

[Лабораторная работа №11. Беспроводные сети 158](#_Toc419447648)

[11.1. Цели и задачи 158](#_Toc419447649)

[11.2. Теоретические сведения 158](#_Toc419447650)

[11.3. Методические указания 161](#_Toc419447651)

[11.4. Заключение 168](#_Toc419447652)

[11.5. Контрольные задания 169](#_Toc419447653)

[Лабораторная работа №12. двойной стек протоколов IP v4 / IP v6 171](#_Toc419447654)

[12.1. Цели и задачи 171](#_Toc419447655)

[12.2. Теоретические сведения 171](#_Toc419447656)

[12.3. Методические указания 176](#_Toc419447657)

[12.4. Заключение 181](#_Toc419447658)

[12.5. Контрольные задания 182](#_Toc419447659)

[Лабораторная работа №13. Аттестационный проект 183](#_Toc419447660)

[13.1. Цели и задачи 183](#_Toc419447661)

[13.2. Задания проекта 184](#_Toc419447662)

[13.3. Легенда 188](#_Toc419447663)

[Заключение 190](#_Toc419447664)

[Библиографический список 191](#_Toc419447665)

ВВЕДЕНИЕ

В современном мире информационные технологии развиваются крайне быстрыми темпами, поэтому на сегодняшний день очень актуальна проблема подготовки высококвалифицированных кадров. Действующие образовательные программы высших учебных заведений часто не справляются с этой задачей, поскольку в большей степени ориентированы на изучение фундаментально-теоретических и академических знаний, из-за чего студенты после завершения обучения не имеют практического производственного опыта работы в реальных условиях. Данное учебно-методическое пособие призвано решить проблему недостатка практических знаний в области проектирования и построения компьютерных сетей у выпускников вузов и ориентировано на студентов, обучающихся по программе «прикладной бакалавриат».

Лидером в области сетевых технологий долгое время является Cisco Systems, одна из крупнейших в мире компаний, специализирующихся в области разработки и продажи сетевого оборудования. Именно её продукцию активно используют при построении локальных и глобальных компьютерных сетей, поэтому будущим сетевым инженерам стоит начинать своё обучение в привязке к оборудованию Cisco. Большой проблемой в этом случае является невозможность изучения сетевых технологий на примере реальных устройств в силу их высокой стоимости. Для решения этой проблемы компания Cisco разработала и поддерживает программу Cisco Packet Tracer — сложный симулятор, который позволяет смоделировать и оценить компьютерную сеть, использующую в качестве связующего оборудования устройства Cisco.

Данное учебно-методическое пособие представляет собой комплекс лабораторных работ, которые должны быть выполнены в среде Cisco Packet Tracer. Первая лабораторная работа целиком посвящена описанию интерфейса и основным функциям программы, в остальных детально описаны приемы построения локальных и глобальных сетей, решаются вопросы настройки различных сетевых протоколов и технологий. Каждая из лабораторных работ состоит из описания решаемых в ней задач, кратких теоретических сведений об изучаемых технологиях, методических указаний по выполнению работы, а также списка контрольных заданий, которые предлагается выполнить студенту самостоятельно для закрепления пройденного материала.

# среда Cisco Packet Tracer

## Обзор интерфейса

По умолчанию при запуске Cisco Packet Tracer 6 появится следующий интерфейс ():

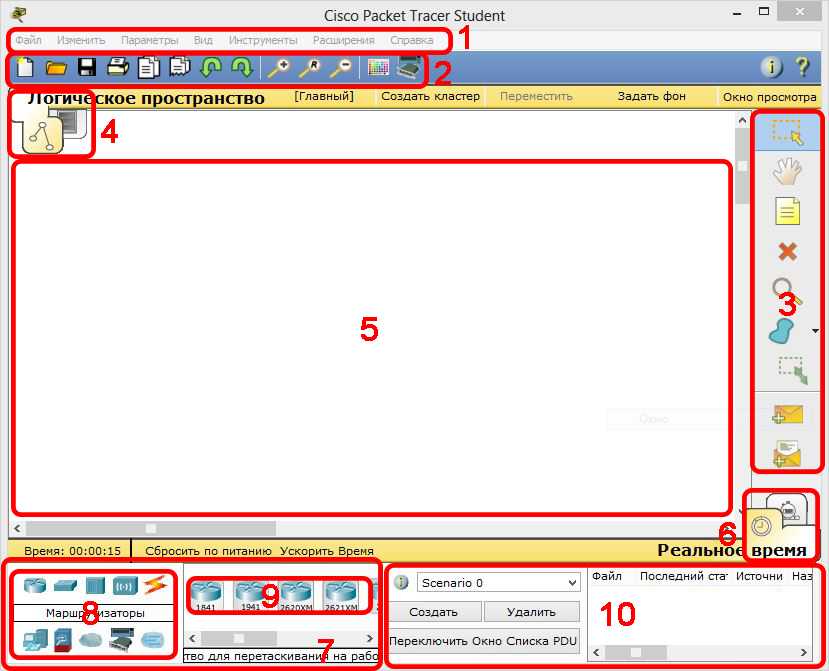


Рис. 1.1. Главное окно Cisco Packet Tracer.

Этот исходный интерфейс содержит десять компонентов, их названия и описания приведены ниже ():

Таблица .. Основные компоненты интерфейса Cisco Packet Tracer

| № | Название | Описание |
| --- | --- | --- |
| 1. | **Панель Меню** | Эта панель содержит меню **File (Файл)**, **Edit (Изменить)**, **Options (Параметры)**, **View (Вид)**, **Tools (Инструменты)**, **Extensions (Расширения)** и **Help (Справка)**. Включает в себя команды **Open (Открыть)**, **Save (Сохранить)**, **Save as Pkz (Сохранить как Pkz), Print (Печать)** и **Preferences (Настройки)**. |
| 2. | **Панель основных команд** | На данной панели расположены иконки к командам **File (Файл)** и **Edit (Изменить)**. Также здесь находятся кнопки **Copy (Копировать)**, **Paste (Вставить)**, **Undo (Отменить)**, **Redo (Повторить)**, **Zoom (Увеличить)**, **Drawing Palette (Панель рисования)** и **Custom Devices Dialog (Окно пользовательских устройств)**. Справа расположена кнопка **Network Information (Информация о сети)**. |
| 3. | **Панель инструментов** | Этот раздел обеспечивает доступ к основным инструментам: **Select (Выбрать)**, **Move Layout (Переместить слой)**, **Place Note (Сделать пометку)**, **Delete (Удалить)**, **Inspect (Проверить)**, **Resize Shape (Изменить размер формы)**, **Add Simple PDU (Добавить простой PDU)** и **Add Complex PDU (Добавить сложный PDU)**. |
| 4. | **Логическое / Физическое рабочее пространство и панель навигации** | Вы можете переключаться между физическим и логическим пространствами с помощью вкладок, расположенных в данном разделе. В логическом пространстве этот раздел также позволяет вам вернуться на предыдущий уровень в кластере, а также использовать функции **New Cluster (Создать кластер)**, **Move Object (Переместить)**, **Set Tiled Background (Задать фон)** и **Viewport (Окно просмотра)**. В физическом рабочем пространстве этот раздел позволит вам производить навигацию сквозь физические локации, а также использовать функции **New City (Новый город)**, **New Building (Новое здание)**, **New Closet (Новая стойка)**, **Move Object (Переместить)**, **Set Background (Задать фон)**, включать **Grid (Сетка)**, и входить в **Working Closet (Рабочая стойка)**. |
| 5. | **Рабочая область** | Пространство, в котором создается сеть, просматривается симуляция и статистика. |
| 6. | **Панель переключения Режим реального времени /Режим симуляции** | Вы можете переключаться между режимами реального времени и симуляции с помощью данного раздела интерфейса. Этот раздел также содержит кнопки **Power Cycle Device (Сбросить по питанию), Fast Forward Time (Ускорить время), Play Control (Управление воспроизведением)** и кнопку включения **Event List (Список событий)** в режиме симуляции. Помимо этого, он содержит часы, показывающие относительное время в разных режимах. |
| 7. | **Компоненты сети** | В этом разделе можно выбирать оборудование и соединения для дальнейшего использования в рабочей области. В нем содержатся разделы **Device-Type Selection (Выбор видов оборудования)** и **Device-Specific Selection (Выбор устройств)**. |
| 8. | **Выбор видов оборудования** | Этот раздел содержит различные виды устройств и доступные типы соединений между ними. Содержимое раздела **Device-Specific Selection (Выбор устройств)** изменяется в зависимости от типа выбранного устройства. |
| 9. | **Выбор устройств** | В этом разделе выбираются конкретные модели устройств и соединений для дальнейшего перемещения в рабочую область. |
| 10. | **Раздел пользовательских пакетов** | Это окно управляет пакетами, помещенными в сеть в ходе симуляции. |

Если вы не уверены, к чему относится та или иная часть интерфейса, наведите на нее указатель для отображения аннотации. Для более подробного изучения интерфейса программы вы можете использовать справку Packet Tracer:

* Справка ⇒ Содержимое ⇒ Раздел «Начало работы» ⇒ Обзор интерфейса.
* Справка ⇒ Содержимое ⇒ Раздел «Учебные материалы».

## Логическое рабочее пространство

Packet Tracer использует две схемы представления вашей сети: логическое и физическое. Логическое пространство позволяет вам строить логическую топологию сети, не обращая внимания на физические аспекты вроде размера и расположения. Физическое пространство позволяет вам физически распределять устройства по городам, зданиям и шкафам оборудования. В Packet Tracer сначала вы выстраиваете логическую сеть, а затем распределяете ее по физическому пространству. Большую часть работы пользователь проводит в логическом рабочем пространстве.

Далее будет рассмотрен процесс добавления устройств и создания соединения между ними:

1. На панели выбора видов оборудования кликните по разделу конечных устройств (или воспользуйтесь комбинацией клавиш Ctrl+Alt+V).
2. Нажмите на иконку рабочей станции (PC-PT), а затем по пустому пространству в рабочей области. Повторите данную операцию для добавления еще одной рабочей станции.
3. Теперь необходимо соединить рабочие станции. На панели выбора видов оборудования выберите пункт «Соединения» (Connections) (Ctrl+Alt+O), а затем выберите тип соединения «Медный перекрестный» (Copper Cross-over), который выглядит как пунктирный штрих.
4. Последовательно нажмите сначала на одну, а затем на другую рабочую станцию, выбирая порты для подключения (FastEthernet0).

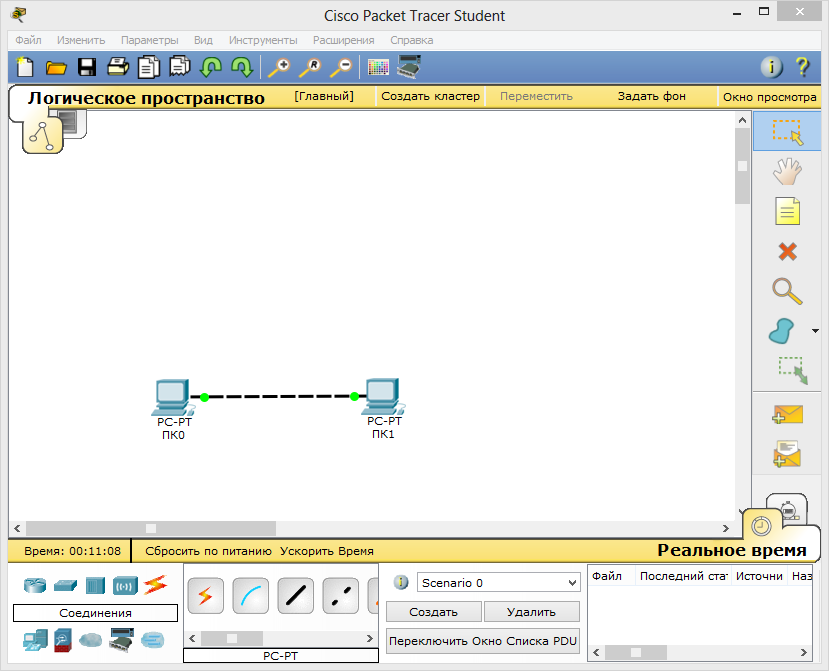


Рис. .. Создание соединения между двумя рабочими станциями

Packet Tracer поддерживает широкий спектр сетевых соединений. Каждый тип кабеля может быть подключен только к определенным типам интерфейсов. Полный список всех возможных типов соединений между устройствами представлен ниже ():

Таблица .. Типы сетевых соединений в Cisco Packet Tracer

| Тип кабеля | Описание |
| --- | --- |
| **Консольный** | Консольные соединения могут быть сделаны между ПК и маршрутизаторами или коммутаторами. Некоторые условия должны быть выполнены для правильной работы консольной сессии на ПК: скорость на обоих концах соединения должна совпадать, должно быть 7 или 8 битов данных, параметр «parity» (четность) должен быть одинаковым, должно быть 1 или 2 стоповых бита (могут быть разными на разных концах), параметр «flow control» (управление потоком) может быть любым (но должен совпадать на концах). |
| **Медный прямой** | Этот кабель обеспечивает стандартное Ethernet-соединение для устройств, которые работают на разных уровнях OSI (например, концентратор – маршрутизатор, коммутатор – ПК, маршрутизатор – концентратор). Он может соединяться со следующими портами: 10 Мбит/c медь (Ethernet), 100 Мбит/c медь (Fast Ethernet), и 1000 Мбит/c медь (Gigabit Ethernet). |
| **Медный перекрестный** | Этот кабель обеспечивает стандартное Ethernet-соединение для устройств, которые работают на одинаковых уровнях OSI (например, концентратор – концентратор, ПК – ПК, ПК – принтер). Он может соединяться со следующими портами: 10 Мбит/c (Ethernet), 100 Мбит/c (Fast Ethernet), и 1000 Мбит/c (Gigabit Ethernet). |
| **Волоконно-оптический** | Волоконно-оптический кабель используется для соединений между волоконно-оптическими портами (100 Мбит/c или 1000 Мбит/c). |
| **Телефонный** | Соединения по телефонной линии могут быть установлены только между устройствами с модемными портами. Пример такого соединения – конечное устройство (например, ПК) подключается к сетевому облаку. |
| **Коаксиальный** | Коаксиальный кабель используется для соединения коаксиальных портов. Пример: модем, подключенный к облаку Packet Tracer. |
| Серийный DCE и DTE | Серийные соединения, часто используемые для WAN-каналов, должны проходить между серийными портами. Помните, что вы должны включить тактирование (clocking) на стороне DCE для правильной работы линейного протокола. Тактирование на стороне DTE опционально. Определить, какая из сторон является DCE можно по маленькой иконке с часами рядом с портом. Если в типе соединения выбрать «**Serial DCE»**, а затем соединить два устройства, то первое устройство автоматически станет стороной DCE, а второе – стороной DTE (и наоборот, при выборе «**Serial DTE»** первое устройство станет стороной DTE, а второе – стороной DCE). |
| **Октальный** | Восьмипортовый асинхронный кабель предоставляет высокоплотный коннектор на одном конце, и восемь коннекторов RJ-45 на другом. |

Обратите внимание на зеленые огоньки рядом с устройствами. Они называются индикаторами соединения. Статус любого соединения отображается цветом, список всех возможных индикаторов соединения приведен ниже ():

Таблица .. Индикаторы соединений в Cisco Packet Tracer

| Цвет индикатора соединения | Описание |
| --- | --- |
| **Ярко-зеленый** | Физическое соединение установлено. Однако это не указывает на статус линейного протокола. |
| **Мигающий зеленый** | Имеется активность на соединении. |
| **Красный** | Физическое соединение не установлено. Не обнаруживается никаких сигналов. |
| **Оранжевый** | Порт в состоянии блокировки из-за STP. Такое состояние появляется только на коммутаторах. |
| **Черный** | Используется только на консольных соединениях. Черный цвет указывает на то, что консольный кабель соединен с правильным портом. |

## Обзор режима реального времени

В режиме **реального времени (Realtime)** ваша сеть моделирует работу сети с ходом реального времени, в пределах использованных моделей протоколов. Сеть незамедлительно отвечает на ваши действия, как это происходило бы с реальными устройствами. Например, как только вы установите соединение Ethernet, индикаторы соединения загорятся мгновенно, отображая состояние подключения. Когда вы вводите команду в консоли (такие как ***ping*** или ***show***), результат или ответ генерируется и отображается моментально. Все действия в сети, в том числе и прохождение пакетов, происходят в режиме реального времени.

Для начала необходимо научиться получать информацию об устройстве и его статистику с помощью всплывающего меню. В режиме реального времени статистика устройств обновляется постоянно с течением времени. Для того чтобы проверить устройство, выполните следующие шаги:

1. Выберите инструмент «Проверить» (Inspect), нажав на значок лупы на панели инструментов (горячая клавиша – «I»).
2. Наведите указатель на ПК0 ()

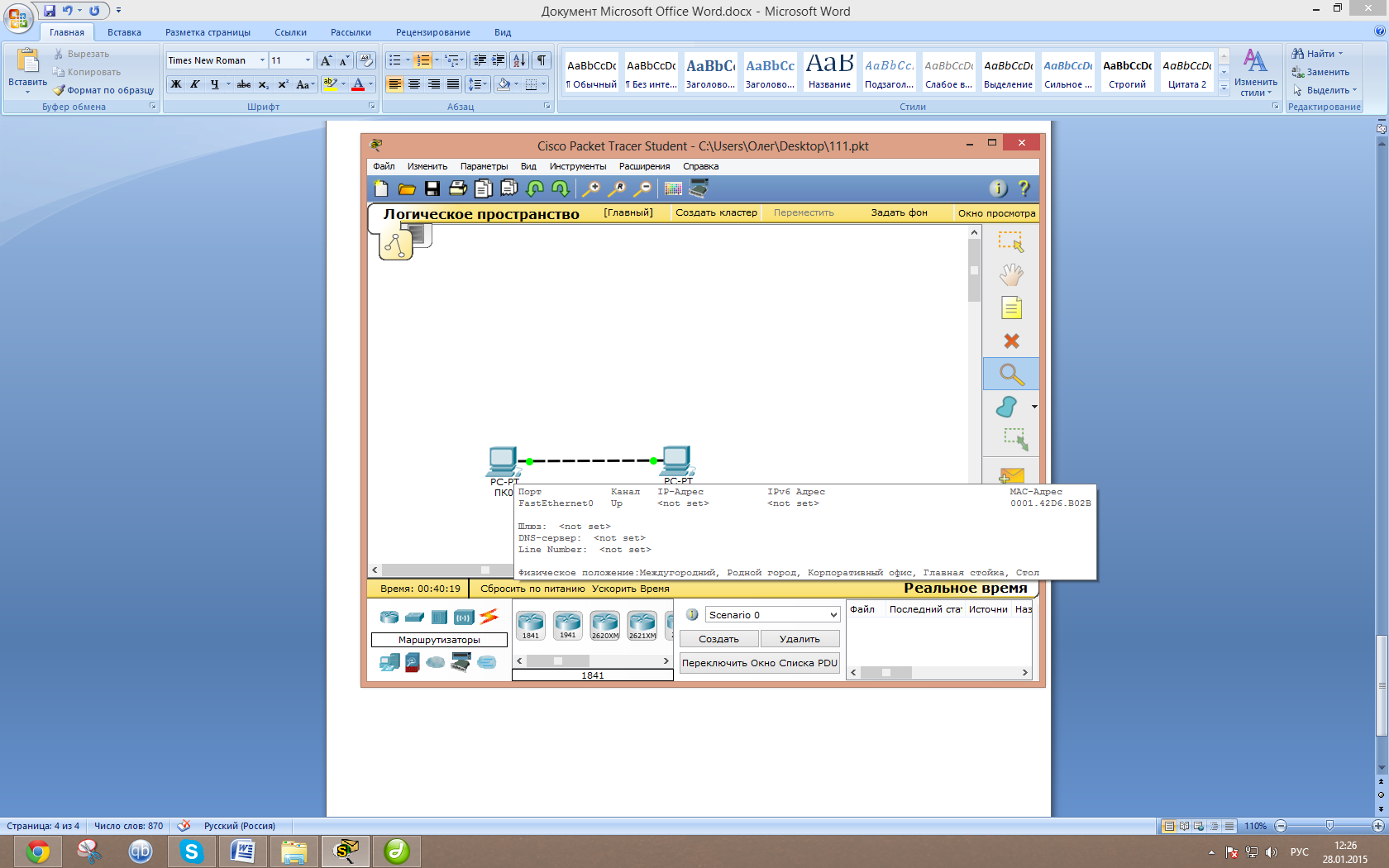


Рис. .. Проверка устройства

Многие параметры установлены в значение ***<not set>*** (не установлено). Необходимо задать для рабочих станций значения IP-адреса и маски подсети. Для этого последовательно выполните следующие действия:

1. Выберите исходный инструмент «Выбрать» (Select) на панели инструментов, или нажав клавишу «Esc».
2. Нажмите на устройство, расположенное на рабочей области. Откроется окно конфигурации устройства.
3. Перейдите на вкладку «Рабочий стол» (Desktop). В нем содержатся ярлыки для настройки и тестирования оборудования.
4. Выберите ярлык «Настройка IP» (Ip Configuration). В появившемся окне введите следующие значения в полях IP-адрес и Маска Подсети соответственно: 192.168.10.10 и 255.255.255.0.
5. Закройте окно. Настройки при этом сохраняются.
6. Аналогично укажите следующие значения IP-адреса и Маски Подсети для второй рабочей станции: 192.168.10.20 и 255.255.255.0.

Теперь можно проверить связь между двумя машинами:

1. На рабочем столе выберите ярлык «Командная строка» (Command Prompt). Введите следующую команду: ***ping 192.168.10.10***. Если все было настроено правильно, то вы должны получать ответы от другого ПК ()

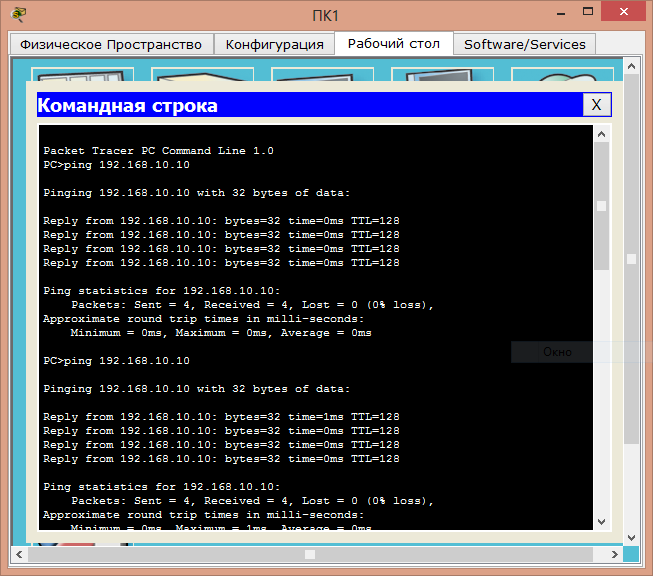


Рис. .. Проверка связи между двумя рабочими станциями.

1. Проверку связи командой ***ping*** иногда называют проверкой связи с помощью echo-запросов. В Сisco Packet Tracer также можно использовать инструмент «Добавить простой PDU» (Add Simple PDU) для выполнения таких запросов. Выберите его на панели инструментов или с помощью горячей клавиши «P».
2. Последовательно нажмите на оба ПК для совершения передачи PDU (Protocol Data Unit – единица данных протокола).
3. Для проверки успешности операции исследуйте лог событий в нижнем правом углу интерфейса. Там должна появиться соответствующая запись ().

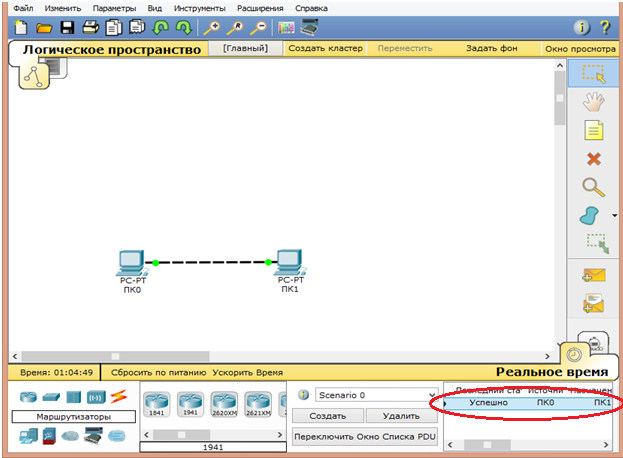


Рис. .. Запись об успешном прохождении пакета

## Обзор режима симуляции

В режиме симуляции (Simulation) вы можете «заморозить» время; вам доступен непосредственный контроль над временем прохождения пакетов. Вы можете наблюдать за сетью в пошаговом режиме, или по действиям, управляя скоростью воспроизведения. Вы можете устанавливать сценарии, такие как отправка echo-запроса от одного устройства к другому. Однако ничего не произойдет до тех пор, пока вы не захватите или не воспроизведете что-либо. Когда вы захватываете или воспроизводите анимацию, вы видите графическое представление пакетов, перемещающихся от одного устройства к другому. Вы можете приостанавливать симуляцию, или перематывать её вперед и назад во времени, исследуя различную информацию о конкретных пакетах и устройствах в конкретные моменты. Хотя остальные аспекты сети будут всё еще работать в режиме реального времени. Например, если вы отключите порт, его индикатор соединения мгновенно станет красным.

Перейдя в режим симуляции и посмотрев на окно событий, можно заметить, что запрос, успешно переданный в режиме реального времени, в режиме симуляции будет иметь статус «в процессе» (in progress). Так как в режиме симуляции возможно управляем временем, для отправления пакета необходимо его запустить.

1. Нажмите кнопку «Авто Захват/Воспроизведение» (Auto Capture/Play) на панели симуляции чтобы воспроизвести анимацию.
2. Следите за тем, как движется PDU (иконка конверта) по сети. Когда echo-ответ будет доставлен, вы увидите несколько записей в окне списка событий, которые появлялись по ходу анимации. Эти записи являются отметками движения пакетов по сети.

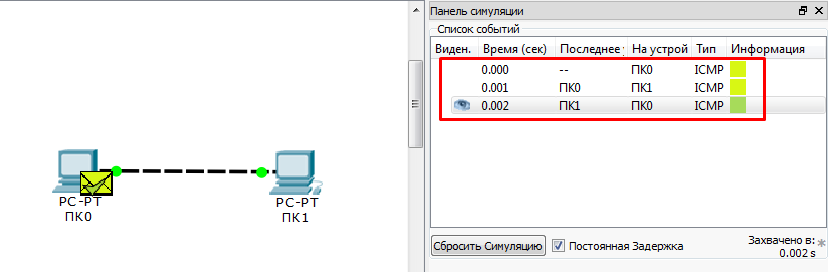


Рис. .. Список событий в режиме Симуляции

1. Нажмите на кнопку «Сбросить Симуляцию» (Reset Simulation) для удаления всех событий и возврату к первоначальному состоянию сети.
2. Для пошагового просмотра анимации нажимайте кнопку «Захват/Вперед» (Capture/Forward). Это позволит вам яснее представить поведение пакета в сети.
3. Для удаления задачи из списка нажмите на кнопку «Удалить» или нажмите два раза по полю пакета, находящегося в таблице в нижнем правом углу интерфейса в столбце «Удалить» (delete).

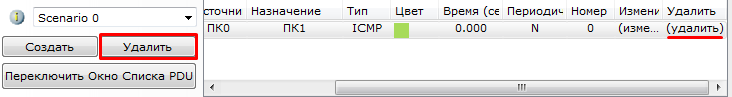


Рис. .. Удаление простого PDU из сети

## Физическое рабочее пространство

Цель физического рабочего пространства – дать физическое измерение вашей сети. Это даст вам чувство масштаба и размещения (того, как ваша сеть выглядела бы в реальных условиях).

Физическое пространство поделено на четыре слоя, которые отображают физический размер окружения: «Междугородний» (Intercity), «Город» (City), «Здание» (Building),и «Рабочая стойка» (Wiring closet). Самым масштабным окружением является междугороднее. Оно может включать в себя множество городов. Каждый город содержит много зданий, а каждое здание может содержать большое количество рабочих стоек. Рабочая стойка предоставляет вид, отличный от остальных. Это место, в котором вы непосредственно видите созданные в логическом рабочем пространстве устройства, расположенные в шкафах с оборудованием и на столах. Три других слоя предоставляют миниатюры других слоев в качестве иконок для перехода на следующий слой. Такое расположение является стандартным в физическом рабочем пространстве, но устройства из рабочих стоек могут быть перенесены в любой другой слой. При перемещении устройства в другой слой, оно возвращается к иконке логического рабочего пространства, хотя они могут быть изменены на любую желаемую картинку.

При переходе в физическое рабочее пространство изначальным видом является междугородний (или «карта»). По умолчанию, междугородний вид содержит один объект типа город, названный «Родной город» (Home city). Вы можете перетаскивать указателем иконку города для его перемещения по карте. Вы также можете кликнуть по иконке города, чтобы переместиться на карту этого города. Родной город содержит одно здание, именуемое «Корпоративный офис» (Corporate office). Это здание, как и объект родной город в междугороднем виде, может быть перемещено в пределах города. Нажмите на иконку здания, чтобы переместиться на карту интерьера. Все здания ограничены одним этажом.

Корпоративный офис содержит одну стандартную рабочую стойку «Главная стойка» (Main Wiring Closet). Нажмите на её иконку, чтобы просмотреть содержимое. Также вы можете вернуться к любым другим предыдущим уровням, нажав на кнопку «Назад» (Back).

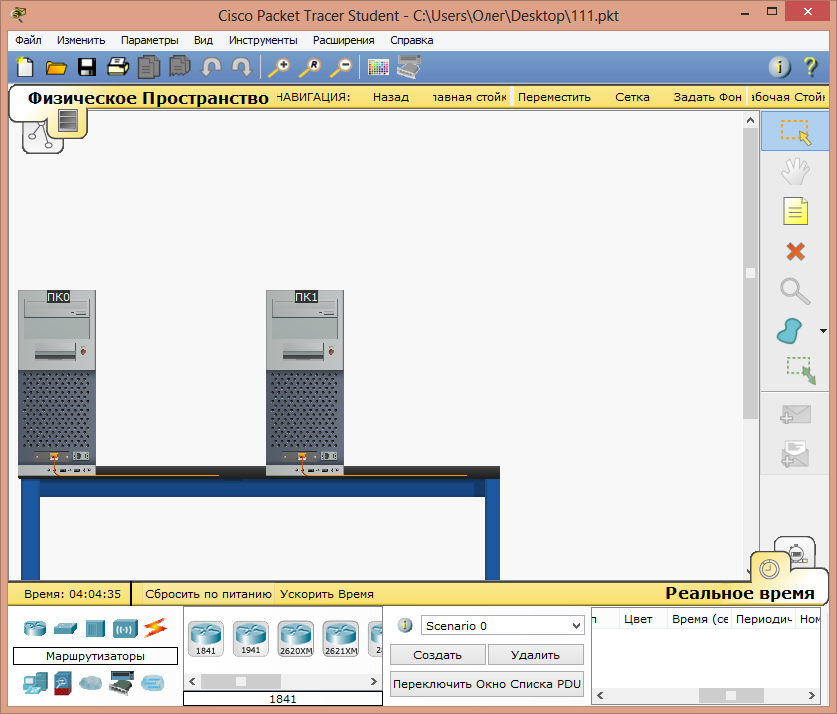


Рис. .. Вид рабочей стойки в физическом рабочем пространстве

«Главная стойка» изначально содержит все устройства, которые были созданы в логическом рабочем пространстве. Она приблизительно располагает эти устройства по шкафам и столам, чтобы вам было наглядно видно физическое расположение этих устройств. Вид рабочей стойки также отображает подключенные порты и статусы индикаторов соединения устройств. При нажатии на устройство, отображается его окно конфигурации, аналогично логическому рабочему пространству.

Физическое рабочее пространство позволяет вам создавать новые локации для расширения вашей физической топологии. В междугороднем окружении возможно создавать города, нажимая на кнопку «Новый город» (New City). Вы можете располагать новые здания и рабочие стойки на междугородней карте с помощью кнопок «Новое здание» (New Building) и «Новая стойка» (New Closet).

Для перемещения любого элемента на физическом пространстве нажмите на кнопку «Переместить объект» (Move Object) на панели физического пространства, а затем по объекту, который будет перемещен. После нажатия на устройство появляется расширяющееся окно, отображающее иерархическое расположение физического рабочего пространства. Щелкните по уровню, на который вы хотите переместить выбранное устройство. Когда вы переместите устройство на новый уровень, оно появится в верхнем левом углу рабочей области.

Для детального изучения физического рабочего пространства и его ограничений необходимо создать простую беспроводную сеть из двух рабочих станций и одной точки доступа:

1. Вернитесь в логическое рабочее пространство и добавьте на рабочую область две рабочие станции PC-PT и одну беспроводную точку доступа AccessPoint-PT.
2. Зайдите в окно конфигурации рабочей станции. Появится вкладка конфигурации физического вида устройства. В этой вкладке возможно заменять модули для устройств.
3. Для того чтобы приступить к замене стандартного модуля на беспроводной, необходимо выключить машину. Нажмите на кнопку питания, располагающуюся на лицевой панели устройства.
4. Перетяните имеющийся модуль из ПК в список модулей, освобождая слот в рабочей станции ().



Рис. .. Замена модуля устройства

1. Перетяните модуль WMP300N из списка модулей в свободный слот. Этот модуль обеспечит поддержку беспроводных соединений.
2. Включите питание машины и закройте окно.
3. Между рабочей станцией и точкой доступа на рабочей области должна появиться связь в виде прямых волн. Повторите аналогичные действия для другой рабочей станции.

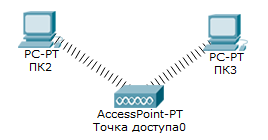


Рис. .. Беспроводная сеть в логическом рабочем пространстве

1. Перейдите обратно в физическое рабочее пространство и, оказавшись в главной стойке, перенесите один из компьютеров с беспроводным модулем за пределы офиса, прямо на городские улицы.
2. Откройте городской вид. Обратите внимание, что вокруг офиса показана область действия точки доступа, в которую не входит перемещенный компьютер ().

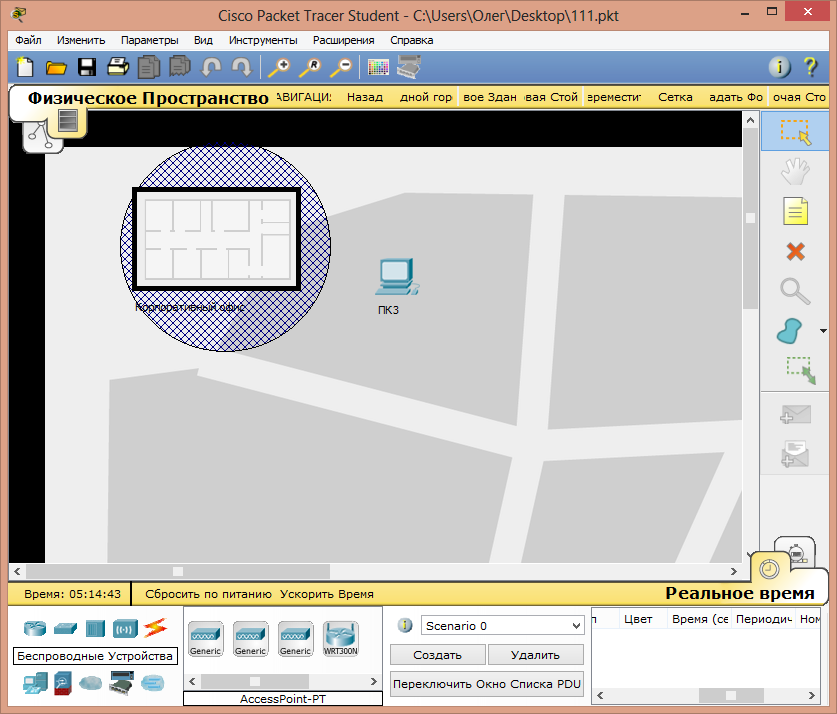


Рис. .. Рабочая станция вне зоны действия точки доступа

1. Вернувшись на логическое рабочее пространство, убедитесь, что связь между одной из ваших рабочих станций и точкой доступа нарушена. Это произошло вследствие вывода рабочей станции за пределы зоны действия точки доступа.

Теперь проверим ограничения физического рабочего пространства при работе с кабельными соединениями. Подключение Ethernet ограничено длиной кабеля в 100 метров. Для Ethernet не существует частичной связи, оно либо в пределах длины в 100 метров (имеет подключение) либо вне (нет подключения). Для проверки, нужно вытянуть кабель между соединенными рабочими станциями на длину более ста метров. Для этого необходимо переместить рабочую станцию за пределы города и отодвинуть достаточно далеко (). Чтобы посмотреть длину кабеля, наведите на него указатель.



Рис. .. Проверка длины кабеля при соединении Ethernet

Вернитесь на логическое рабочее пространство, вы должны увидеть, что индикаторы соединения между рабочими станциями загорелись красным. Если индикаторы все еще зеленые, убедитесь, что в настройках программы стоит галочка рядом с пунктом «Включить эффект длины кабеля» (Enable Cable Length Effects) (Параметры ⇒ Настройки или «Ctrl+R»).

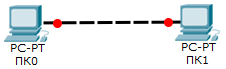


Рис. .. Неактивное соединение между рабочими станциями

## Контрольные задания

1. Установить коммутатор между двумя рабочими станциями, находящимися на расстоянии более ста метров друг от друга для восстановления соединения между ними.
2. Создать в физическом рабочем пространстве еще один город с офисом внутри него. В этом офисе создать рабочую стойку. Добавить по одной рабочей станции в рабочие стойки в разных городах и соединить их оптическим кабелем, предварительно оснастив машины подходящими модулями.
3. Подключить рабочую станцию с модулем 1CFE и ноутбук с модулем WPC300N к одному серверу.
4. С помощью инструмента «Добавить сложный PDU» (Add Complex PDU) запустить в сеть серию повторных echo-запросов с одного компьютера на другой с интервалом 5 секунд.
5. Просмотреть сетевую конфигурацию рабочей станции с помощью командой строки (команды ***ipconfig*** и ***ipconfig /all***).

# Технология виртуальных локальных сетей VLAN и протокол VTP

## Цели и задачи

Целью данной лабораторной работы является получение практических навыков при работе с технологией виртуальных локальных сетей (VLAN) и протоколом VTP.

Для достижения данной цели будут выполнены следующие задачи:

* изучение технологии создания виртуальных локальных сетей на коммутаторах Cisco с помощью интерфейса командной строки CLI;
* настройка интерфейсов коммутатора в режим accessдля связей коммутатор – узел;
* настройка интерфейсов коммутатора в режим trunkдля создания VLAN-магистралей на связях коммутатор – коммутатор;
* изучение трех основных режимов протокола VTP – server, client и transparent;
* конфигурация отдельных VTP-доменов и паролей к ним.

## Теоретические сведения

В данной лабораторной работе будет рассмотрена возможность создания и настройки виртуальных локальных сетей. При проектировании довольно часто возникает необходимость в разделении одной сети на несколько логических блоков (например, разделение на отделы) независимо от физического расположения устройств. В локальных сетях все устройства находятся в одном и том же широковещательном домене, это означает, что при отправке любым устройством кадра с широковещательным сообщением, копию этого кадра получат все остальные устройства. Технология VLAN (Virtual Local Area Network) позволяет помещать одни устройства в один широковещательный домен, а другие – в другой, создавая тем самым несколько широковещательных доменов. Эти широковещательные домены, создаваемые коммутаторами, называются виртуальными локальными сетями. 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.

Если VLAN-ceти используются в сетях, в которых имеется несколько соединенных коммутаторов, то в коммутаторах необходимо использовать VLАN-магистрали в сегментах, находящихся между этими коммутаторами. Создание такой магистрали приводит к тому, что в коммутаторах применяется процесс, называемый назначением тегов VLAN-ceти. С eгo помощью коммутатор-отправитель добавляет заголовок к кадру перед его отправкой по магистрали. Этот дополнительный заголовок включает поле идентификатора VLAN-ceти (VLAN ID), с помощью которого коммутатор-отправитель может ввести идентификатор VLAN-ceти, а коммутатор-получатель - определить, к какой VLАN-сети относится полученный кадр.

Таким образом, порты коммутатора, поддерживающие VLAN, можно разделить на два множества:

1. **Тегированные** порты (или транковые порты, trunk-порты в терминологии Cisco) – между ними строятся VLAN-магистрали, используются для связи коммутатор – коммутатор.
2. **Нетегированные** порты (или порты доступа, access-порты в терминологии Cisco) – для связи коммутатор – узел.

По умолчанию все порты коммутатора считаются нетегированными членами VLAN 1 (так называемый native VLAN – «родной» VLAN). В процессе настройки или работы коммутатора они могут быть перемещены в другие VLAN.

Trunk-интерфейсы могут работать в различных режимах:

* **auto** — порт находится в автоматическом режиме и будет переведён в состояние trunk, только если порт на другом конце находится в режиме trunk или desirable. Если порты на обоих концах находятся в режиме auto, то trunk применяться не будет;
* **desirable** — порт находится в режиме «готов перейти в состояние trunk»; периодически передает DTP-кадры порту на другом конце, запрашивая удаленный порт перейти в состояние trunk;
* **trunk** — порт постоянно находится в состоянии trunk, даже если порт на другом конце не поддерживает этот режим;
* **nonegotiate** — порт готов перейти в режим trunk, но при этом не передает DTP-кадры порту на другом конце. Этот режим используется для предотвращения конфликтов с другим «не-cisco» оборудованием. В этом случае коммутатор на другом конце должен быть вручную настроен на использование в режиме trunk.

Режим trunkиспользуется для настройки статической VLAN-магистрали, а режимы auto, desirable и nonegotiate используются для динамической настройки VLAN-магистралей с помощью протокола DTP (Dynamic Trunk Protocol – динамический транковый протокол).

При работе с виртуальными локальными сетями с оборудованием Cisco нельзя не упомянуть о протоколе VTP (VLAN Trunking Protocol - транкинговый протокол сетей VLAN). Это собственный протокол корпорации Cisco, который предоставляет средства, с помощью которых коммутаторы Cisco могут обмениваться информацией о конфигурации VLAN-ceти. В частности, протокол VTР обеспечивает передачу анонсов с информацией, позволяющей узнать о существовании каждой VLAN-ceти по ее идентификатору VLAN-ceти и имени VLAN-ceти. Но протокол VTР не анонсирует сведения о том, какие интерфейсы коммутатора относятся к той или иной VLAN-ceти.

На коммутаторах Cisco протокол VTP может работать в трёх режимах:

1. **Server** (режим по умолчанию):

* может создавать, изменять и удалять VLAN из командной строки коммутатора;
* генерирует объявления VTP и передает объявления от других коммутаторов;
* может обновлять свою базу данных VLAN при получении информации не только от других VTP-серверов, но и от других VTP-клиентов в одном домене, если полученная конфигурация имеет более высокий номер версии;
* сохраняет информацию о настройках VLAN в файле vlan.dat во flash-памяти.

1. **Client**:

* в этом режиме невозможно создавать, изменять и удалять VLAN из командной строки коммутатора;
* передает объявления от других коммутаторов;
* синхронизирует свою базу данных VLAN при получении информации от VTP-серверов или других VTP-клиентов, если полученная конфигурации имеет более высокий номер версии;
* сохраняет информацию о настройках VLAN в файле vlan.dat во flash-памяти.

1. **Transparent**:

* возможно создавать, изменять и удалять VLAN из командной строки коммутатора, но только для локального коммутатора;
* не генерирует объявления VTP;
* передает объявления от других коммутаторов;
* не обновляет свою базу данных VLAN при получении информации по VTP;
* сохраняет информацию о настройках VLAN в NVRAM;
* всегда использует номер версии конфигурации равный нулю.

Процесс ввода в действие протокола VTP начинается с создания VLAN-ceти на коммутаторе, который находится в серверном режиме. После этого VTP-сервер распространяет информацию об изменениях в конфигурации VLAN-ceтeй с помощью сообщений VTР, передаваемых только через VLAN-магистрали по всей сети. Затем серверы и VTР-клиенты обрабатывают полученные сообщения VTР, обновляют свои базы данных с конфигурацией протокола VTР на основе этих сообщений и независимо от других передают обновления протокола VTР по своим магистралям. Процесс, в ходе которого на одном из серверов изменяется конфигурация VLAN-сетей и все остальные коммутаторы VTP усваивают новую конфигурацию, называется **синхронизацией**.

Серверы и клиенты VTР принимают решение о том, следует ли реагировать на полученное обновление протокола VTР и обновлять свои конфигурации VLAN­ceтeй на основании того, произошло ли увеличение номера версии конфигурации базы данных VLAN-ceтeй. После каждого изменения VTP-сервером своей конфигурации VLAN-ceти этот сервер увеличивает текущий номер версии конфигурации на 1. Этот новый номер версии конфигурации отражается в сообщениях об обновлениях протокола VTР. После получения этого обновления другими коммутаторами, они обновляют свою конфигурацию VLAN-ceтeй. Кроме того, серверы и клиенты VТР рассылают периодические сообщения VТР через каждые 5 минут на тот случай, если каким-либо вновь введенным в сеть коммутаторам потребуется информация о конфигурации VLAN-ceти.

**Примечание**. Описание процессов моделирования для этой лабораторной работы можно найти в справке Packet Tracer: Справка ⇒ Содержимое ⇒ раздел «Моделирование» ⇒ Лаб. работа №2.

## Методические указания

1. Для начала нужно добавить коммутатор 2960-24TT и четыре узла PC-PT на логическое рабочее пространство, а также установить соединения между коммутатором и узлами по типу «медный прямой».
2. Для каждого узла следует настроить IP-адреса и маски подсетей.

* IP-адреса для узлов назначить в диапазоне 192.168.1.1 (узел 1) – 192.168.1.4 (узел 4);
* маску подсети для каждого узла установить в значение 255.255.255.0

**Примечание**. При проектировании виртуальных локальных сетей лучше придерживаться правила «один VLAN - одна подсеть», однако в рамках данной лабораторной работы лучше использовать одну подсеть на все VLAN. Это упрощение нужно для того, чтобы можно было проверить работоспособность виртуальных локальных сетей с помощью инструмента «Добавить простой PDU» (Add Simple PDU) или с помощью команды ***ping*** на узле.

1. Индикаторы соединений на стороне коммутатора некоторое время будут гореть оранжевым светом, а затем загорятся зеленым. Для того чтобы сократить время ожидания можно нажать на кнопку «Ускорить Время» (Fast Forward Time).

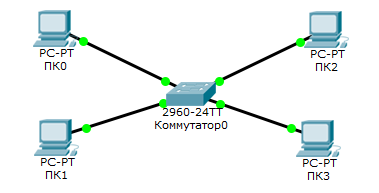


Рис. .. Соединение коммутатора и четырех узлов

1. Нажмите на коммутатор и перейдите на вкладку «СLI». Появится интерфейс командной строки коммутатора. Из этого интерфейса в дальнейшем будет проводиться большая часть настроек коммутатора. По умолчанию, коммутатор находится в пользовательском режиме, но для того, чтобы изменять конфигурацию, необходимо зайти в привилегированный режим. Для этого введите команду ***enable*** (или сокращенную запись ***en***). Символ «***#***» после названия устройства в CLI указывает на то, что включен привилегированный режим.
2. Введите команду ***show vlan brief***. Появится список всех VLAN на данном коммутаторе. По умолчанию все порты коммутатора принадлежат виртуальной локальной сети с номером 1.
3. Для создания новогоVLAN необходимо зайти в режим глобальной конфигурации из терминала. Для этого введите команду ***configure terminal*** (сокращенная запись – ***conf t***). Надпись «***(config)***» после имени устройства в CLI обозначает, что включен режим глобальной конфигурации.
4. Создайте VLAN с номером 2, для этого введите команду ***vlan 2***. Устройство перейдет в режим конфигурации VLAN. (на это указывает надпись «***(config-vlan)***» после имени устройства в CLI). Теперь нужно задать имя виртуальной локальной сети с помощью команды ***name <имя\_vlan\_сети>***. Придумайте и задайте любое имя для этой виртуальной локальной сети (например, ***name vlan2***).
5. Введите команду ***exit*** (сокращенно – ***ex***) для выхода из режима конфигурации VLAN. Коммутатор перейдет в режим конфигурации. Теперь нужно добавить интерфейсы в созданную виртуальную локальную сеть. Добавьте два узла (например, fa0/3 и fa0/4) в сеть VLAN 2. Для этого введите команду ***interface range fastethernet0/3-4*** (сокращенно – ***interface range fa0/3-4***). Устройство перейдет в режим конфигурации диапазона интерфейсов («***config-if-range***» после имени). Для конфигурирования одного интерфейса используется команда ***interface <имя\_интерфейса>***.
6. В режиме конфигурации диапазона интерфейсов введите команду switchport access vlan 2. Данная команда переместит интерфейсы fa0/3 и fa0/4 в виртуальную локальную сеть с номером 2, а также переведет порты в режим access.
7. С помощью команды ***exit*** вернитесь в привилегированный режим коммутатора. Возможно, придется ввести эту команду несколько раз. Посмотрите список всех VLAN (***show vlan brief***). Должна появиться новая строчка с именем созданного VLAN, а в столбце Ports должны быть указаны порты fa0/3 и fa0/4.

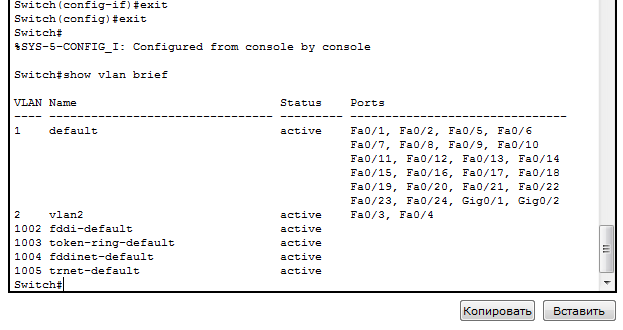


Рис. .. Вывод команды ***show vlan brief***

1. С помощью инструмента «Добавить простой PDU» (Add Simple PDU) проверьте связь между узлами из разных виртуальных локальных сетей. Трафик не должен проходить!

Далее будет рассмотрен пример настройки VLAN-магистрали между двумя коммутаторами, а также будет произведена конфигурация протокола VTP в серверном и клиентском режимах.

Предположим, что имеется задача: в одном здании на разных этажах находится два коммутатора. К каждому коммутатору подключены некоторые узлы, коммутаторы также связаны между собой. Требуется разделить сеть на два логических отдела таким образом, чтобы в каждом отделе были узлы из разных этажей.

Для решения этой задачи потребуется добавить на логическое рабочее пространство еще один коммутатор и два узла. Для настройки IP-адресов на новых узлах можно взять адреса 192.168.1.5 и 192.168.1.6, а маску подсети установить в значение 255.255.255.0. Соедините устройства (), используя между коммутаторами кабель «Медный прямой», а также интерфейс GigabitEthernet0/1. Данный сегмент будет использоваться в качестве VLAN-магистрали, а значит по нему будет ходить трафик из всех VLAN, поэтому логично использовать интерфейсы с высокой пропускной способностью.



Рис. .. Исходная сеть из двух коммутаторов и узлов

По умолчанию, узлы ПК4 и ПК5 будут относиться к VLAN1, причем Коммутатор1 даже не будет знать о том, что на Коммутатор0 была создана VLAN2. Это можно проверить, если ввести в CLI Коммутатора1 команду ***show vlan brief***. Для синхронизации базы данных VLAN-сетей нужно настроить протокол VTP, создав для этих двух коммутаторов свой VTP-домен и пароль. Но сначала нужно установить VLAN-магистраль между двумя коммутаторами.

1. На Коммутатор0 зайдите в привилегированный режим, а затем в режим конфигурации. Введите команду ***interface gigabitethernet0/1*** (сокращенно - ***interface gi0/1***).
2. Переведите порт в режим ***dynamic desirable*** для создания динамической VLAN-магистрали с помощью команды ***switchport mode dynamic desirable***. Также можно настроить статическую VLAN-магистраль командой ***switchport mode trunk***.
3. Перейдите в CLI Коммутатора1 и проведите те же настройки, обратите внимание, что для динамической VLAN-магистрали можно указать режим ***dynamic auto***.
4. Для проверки введите команду ***show interfaces trunk*** из привилегированного режима ().

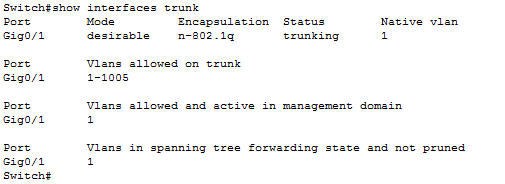


Рис. 2.4. Вывод команды ***show interfaces trunk***

Важно, чтобы в выводе этой команды на обоих коммутаторах в столбце «Status» было указано значение «trunking». Таким образом, для создания статической VLAN-магистрали требуется установить режим trunk на портах двух коммутаторов, соединенных между собой, а для создания динамической VLAN-магистрали достаточно режима dynamic desirable на одном порту, и dynamic auto на другом.

Теперь VLAN-магистраль настроена, однако в выводе команды ***show vlan brief*** на Коммутатор1 все еще не отображается созданная на Коммутатор0 VLAN2. Это происходит потому, что по умолчанию оба этих коммутатора находятся в собственных VTP-доменах. Необходимо поместить коммутаторы в один VTP-домен, для этого:

1. В CLI Коммутатора0 войдите в режим конфигурации (***conf t***), а затем наберите команду ***vtp domain <имя\_домена>***. Будет установлено новое имя VTP-домена.
2. С помощью команды ***vtp password <пароль\_vtp\_домена>*** установите пароль для домена.
3. Проверьте статус VTP-протокола, для этого используется команда show vtp status. В выводе этой команды можно посмотреть информацию о номере версии протокола VTP («VTP Version»), номере версии конфигурации («configuration revision»), максимальном числе поддерживаемых VLAN («Maximum VLANs supported locally»), числе существующих в данный момент времени VLAN («Number of existing VLANs»), роли коммутатора в VTP-протоколе («VTP Operating Mode»), а также имени VTP-домена («VTP Domain Name»).

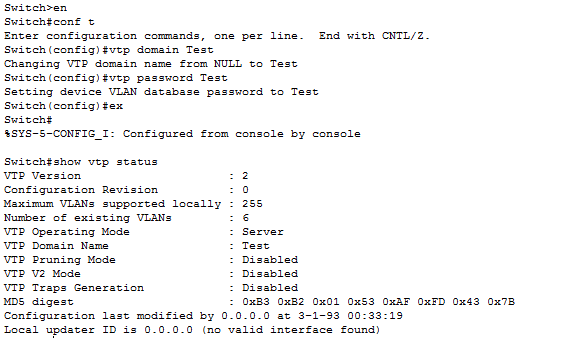


Рис. .. Конфигурация VTP-домена.

1. Перейдите в CLI Коммутатор1. Введите такие же настройки, а затем введите команду ***vtp mode client*** для включения режима VTP-клиента. Команда ***vtp mode*** может принимать три аргумента, соответствующие трем режимам работы VTP – server, client и transparent.
2. Теперь в выводе команды ***show vlan brief*** на Коммутатор1 должна появиться запись о существовании VLAN2. Также в выводе команды ***show vtp status*** на обоих коммутаторах должен быть одинаковый номер версии конфигурации (configuration revision). Сейчас он равен 0, но он будет увеличиваться с каждым изменением VLAN-сетей.
3. Чтобы проверить работу VTP-протокола в деталях, перейдите в Режим Симуляции.
4. Измените фильтры таким образом, чтобы отслеживать только трафик VTP.
5. Коммутатор0 является VTP-сервером, только он может добавлять и удалять информацию о VLAN-сетях. Создайте VLAN3 с помощью команд, изученных ранее.
6. В списке событий должны появиться записи о VTP-трафике. Начался процесс синхронизации**.** Посмотрите весь процесс по шагам с помощью кнопки «Захват/Вперед» и «Назад».



Рис. .. VTP-синхронизация в режиме симуляции

1. Вернитесь в режим реального времени. При выводе команды ***show vtp status*** номер версии конфигурации должен увеличиться. Это можно заметить в строке «Configuration Revision».

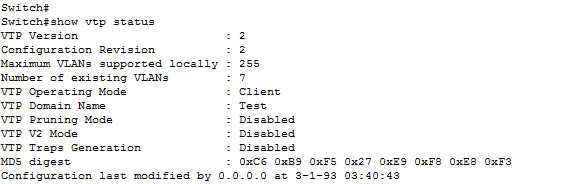


Рис. .. Вывод команды ***show vtp status***

1. Удалите созданную VLAN3 с помощью команды ***no vlan 3***, которая запускаетсяиз режима конфигурации.
2. Для окончания задания добавьте ПК5 в VLAN2, таким образом получив разделение сети на логические отделы вне зависимости от физического нахождения на разных этажах здания.

## Заключение

Распределение узлов по разным виртуальным локальным сетям имеет массу преимуществ, вот некоторые из них:

* уменьшение количества широковещательного трафика в сети, это снижает издержки, которые связаны с пребыванием каждого узла в VLAN-сети;
* VLAN не привязан к местоположению устройств и поэтому устройства, находящиеся на расстоянии друг от друга, все равно могут быть в одном VLAN независимо от местоположения. Это позволяет создавать более гибкие проекты, в которых пользователи могут быть сгруппированы по отделам или по работающим вместе коллективам;
* достижение более высокой степени безопасности за счет выделения узлов, предназначенных для работы с конфиденциальными данными, в отдельные VLAN-ceти;
* отделение трафика, передаваемого IР-телефонами, от трафика, передаваемого персональными компьютерами, к которым подключены эти телефоны;
* уменьшение рабочей нагрузки на средства протокола STP (Spanning Tree Protocol) путем ограничения размеров VLAN-ceти до отдельного коммутатора доступа;
* протокол VTP поддерживает систему доменных имен, с помощью которой можно создавать разные VTP-домены для разных отделов. Это позволяет иметь несколько независимых баз данных VLAN.

VLAN обеспечивают гибкость в разработке и внедрении инфраструктуры коммутируемой сети. Сети, в которых используется разделение на виртуальные локальные сети можно легко перестраивать согласно потребностям пользователей. Сети VLAN является частью любой серьезной сетевой разработки, однако необходимо понимать потребности пользователей и пути потоков информации до внедрения виртуальных сетей. Нужно тщательно взвесить преимущества использования дополнительных VLAN с точки зрения производительности и администрирования.

Однако внедрение VLAN в локальные сети также имеет следующие недостатки:

* повышение стоимости оборудования, поддерживающего VLAN. Не каждый коммутатор поддерживает возможность использования виртуальных локальных сетей, а протоколы DTP и VTP являются проприетарными разработками компании Cisco, это означает, что использование этих протоколов возможно только на оборудовании Cisco, которое по стоимости является одним из самых дорогих;
* сложность конфигурации нескольких VTP-доменов в сети.

## Контрольные задания

1. Имеется трехэтажный офис, на каждом этаже расположены по три узла и по одному коммутатору. Коммутатор на первом этаже связан с коммутатором на втором этаже, а он в свою очередь связан с коммутатором на третьем этаже. Разделить сеть на логические отделы программистов (4 узла), тестеров (3 узла) и администраторов (2 узла). Коммутатор-сервер VTP должен находиться на этаже с отделом администраторов, остальные коммутаторы должны быть в клиентском режиме. Настроить динамические VLAN-магистрали на связях между коммутаторами.
2. Пять коммутаторов соединены между собой по топологии «Звезда». Центральный коммутатор играет роль моста между другими коммутаторами, поэтому он должен иметь как минимум 4 модуля Gigabit Ethernet. К каждому коммутатору подключены по два узла. Разделить сеть на 2 логических отдела по 4 узла в каждом. Для каждого отдела настроить свой VTP-домен и пароль. Для каждого VTP-домена выделить коммутатор-сервер и коммутатор-клиент, а также разбить отдел на подотделы по 2 узла. Настроить статические VLAN-магистрали на связях между коммутаторами. Центральный коммутатор должен работать в прозрачном (transparent) режиме VTP.
3. В двух офисах расположены 12 узлов и некоторое количество коммутаторов. С их помощью разделить узлы на отделы торговли, производства, и кадров. В каждом отделе не может быть меньше двух узлов. Отдел торговли имеет отдельный VTP-домен, в котором определены отделы бухгалтерии и продаж.
4. Имеется два здания по два этажа в каждом. На каждом этаже имеется коммутатор и некоторое количество узлов. На первых этажах зданий располагается отдел производства, а вторые этажи занимает отдел разработки. Здания связаны между собой через оптоволоконный кабель с помощью коммутаторов на первых этажах (используйте на первых этажах здания коммутаторы с модулями Gigabit Ethernet для оптоволоконных кабелей). Связать этажи разных зданий в логические отделы со своим VTP-доменом. Настроить статическую VLAN-магистраль между зданиями, а магистрали между этажами сделать динамическими.

# Отказоустойчивые связи в компьютерных сетях

## Цели и задачи

Целью данной лабораторной работы является получение необходимых теоретических и практических знаний, требующихся для построения отказоустойчивых соединений в компьютерных сетях.

Для достижения данной цели будут выполнены следующие задачи:

* построение отказоустойчивых соединений методом резервирования каналов связи;
* изучение работы протоколов STP и RSTP, а также их аналогов для оборудования Cisco (PVST и RPVST);
* изучение основных настроек протокола STP – выбор корневого коммутатора и управление приоритетом устройства;
* ознакомление с опциональными настройками протокола STP – функциями PortFast и BPDU Guard;
* настройка статического и динамического агрегирования каналов (технология EtherChannel).

## Теоретические сведения

При проектировании сетей рано или поздно возникает вопрос создания отказоустойчивых соединений на наиболее важных участках сети, например, на магистралях между коммутаторами. Такие соединения служат для обеспечения бесперебойной работы сети, а в случае сбоя на каком-либо канале связи гарантируется быстрое восстановление работоспособности.

Отказоустойчивые соединения создаются с помощью двух методов:

1. **Резервирование** каналов связи: прокладываются дополнительные соединения между устройствами, но в работе участвует только одно. В случае отказа одного соединения связь не прерывается, а включается в работу резервный (запасной) канал.
2. **Агрегирование** каналов связи: дополнительные физические соединения объединяются в одно логическое. Одновременно в работе участвуют сразу все соединения, при этом повышается пропускная способность.

Однако в связи с наличием в локальных сетях избыточных каналов связи появляется вероятность того, что кадры начнут бесконечно долго циркулировать в сети, что снижает её производительность. Поэтому в локальных сетях используется протокол связующего дерева (Spanning Tree Protocol — STP), который позволяет применять избыточные каналы в локальной сети и вместе с тем предотвращает возможность бесконечной циркуляции кадров в этой локальной сети через резервные каналы. Если протокол STP введен в действие, то коммутаторы блокируют некоторые порты, поэтому кадры через эти порты не перенаправляются. Согласно протоколу STP выбор блокируемых портов осуществляется так, чтобы был только один активный путь между любой парой сегментов локальной сети. В результате сохраняется возможность доставлять кадры на любое устройство и вместе с тем не возникают проблемы, обусловленные зацикливанием кадров в сети. Иными словами, действие протокола STP можно описать просто как выбор интерфейсов, которые должны применяться для перенаправления трафика.

В приведены итоговые сведения о трех основных категориях проблем, возникающих в случае отказа от применения протокола STP в локальной сети с избыточными каналами связи.

Таблица .. Проблемы в сетях с избыточной топологией

| Проблема | Описание |
| --- | --- |
| Широковещательные штормы | Повторное перенаправление кадра по одним и тем же каналам связи, что приводит к непроизводительному потреблению значительной части пропускной способности каналов. |
| Нестабильность таблиц MAC-адресов | Непрекращающееся обновление таблиц МАС-адресов коммутаторов с вводом в них неправильных записей в ответ на появление циркулирующих кадров, что приводит к отправке кадров в несоответствующие им местонахождения. |
| Многократная передача кадров | Побочный эффект появления циркулирующих кадров, под действием которого многочисленные копии одного и того же кадра доставляются на узел назначения и работа узла нарушается. |

Протокол STP предотвращает возникновение циклов благодаря тому, что все порты каждого моста или коммутатора переводятся в состояние пересылки или в состояние блокирования. Интерфейсы, находящиеся в состоянии пересылки, действуют обычным образом, перенаправляя и получая кадры, а интерфейсы в состоянии блокирования не обрабатывают никаких кадров, кроме сообщений протокола STP. При этом если отказывает канал, использовавшийся для пересылки, то порт, находящийся в режиме блокирования, выйдет из него в ходе конвергенции. Под **конвергенцией** протокола STP подразумевается процесс, в ходе которого все коммутаторы обнаруживают, что произошли какие-то изменения в топологии локальной сети, поэтому необходимо пересмотреть принятые решения о том, в каких портах трафик блокируется и в каких перенаправляется.

В протоколе STP используются три описанных ниже критерия, позволяющие определить, должен ли интерфейс быть переведен в состояние пересылки:

* с помощью протокола STP выбирается корневой коммутатор. В ходе дальнейшей работы протокола STP все рабочие интерфейсы корневого коммутатора переводятся в состояние пересылки;
* в каждом некорневом коммутаторе осуществляется поиск того из портов, который имеет наименьшую административно устанавливаемую стоимость маршрута передачи пакетов между ним и корневым коммутатором. Согласно протоколу STP интерфейс с наименьшей стоимостью связи с корневым коммутатором, который принято называть корневым портом некорневого коммутатора, переводится в состояние пересылки;
* к одному и тому же сегменту Ethernet может быть подключено несколько коммутаторов. Коммутатор с наименьшей административно устанавливаемой стоимостью передачи от себя к корневому коммутатору по сравнению с другими коммутаторами, подключенными к тому же сегменту, переводит свой подключенный к сегменту интерфейс в состояние пересылки. Коммутатор с наименьшей стоимостью маршрута передачи в каждом сегменте именуется выделенным мостом, а интерфейс такого моста, подключенный к соответствующему сегменту, именуется назначенным портом (designated port — DP).

В топологии корневым становится коммутатор с наименьшим идентификатором моста (Bridge ID). Только один коммутатор может быть корневым. Для того чтобы выбрать корневой коммутатор, все коммутаторы отправляют сообщения BPDU, указывая себя в качестве корневого коммутатора. Если коммутатор получает BPDU от коммутатора с меньшим Bridge ID, то он перестает анонсировать информацию о том, что он корневой и начинает передавать BPDU коммутатора с меньшим Bridge ID. В итоге только один коммутатор останется корневым.

Bridge ID состоит из двух полей:

* **приоритет** — поле, которое позволяет административно влиять на выборы корневого коммутатора. Размер — 2 байта;
* **MAC-адрес** — используется как уникальный идентификатор, который, в случае совпадения значений приоритетов, позволяет выбрать корневой коммутатор. Так как MAC-адреса уникальны, то и Bridge ID уникален, так что какой-то коммутатор обязательно станет корневым.

В приведены итоговые сведения о том, по каким причинам протокол STP переводит порт в состояние блокирования или перенаправления.

Таблица .. Правила определения состояния портов в протоколе STP

| Порт | Состояние | Описание |
| --- | --- | --- |
| Все порты корневого коммутатора | Перенаправление | Корневой коммутатор всегда является назначенным коммутатором для всех подключенных сегментов. |
| Корневой порт каждого некорневого коммутатора | Перенаправление | Порт коммутатора, при передаче через который обеспечивается наименьшая стоимость маршрута к корневому коммутатору. |
| Выделенный порт каждой локальной сети | Перенаправление | Коммутатор, для которого стоимость перенаправления BPDU-блока в сегмент является наименьшей, представляет собой выделенный коммутатор. |
| Все прочие рабочие порты | Блокирование | Порт в состоянии блокирования не используется для перенаправления кадров, также не рассматриваются как предназначенные для перенаправления какие-либо кадры, полученные через соответствующий интерфейс. |

На втором этапе процесса функционирования протокола STP каждый некорне­вой коммутатор выбирает среди своих портов один и только один корневой порт. Порт коммутатора, который имеет кратчайший путь к корневому коммутатору, называется корневым портом. У любого не корневого коммутатора может быть только один корневой порт. Корневой порт выбирается на основе меньшего Root Path Cost (стоимость пути до корневого коммутатора) – это общее значение стоимости всех каналов связи до корневого коммутатора. Эта стоимость определяется пропускной способностью канала, чем больше пропускная способность, тем меньше стоимость пути. Если стоимости до корневого коммутатора совпадает у двух портов, то выбор корневого порта происходит на основе меньшего Bridge ID коммутатора. Если и Bridge ID коммутаторов до корневого коммутатора совпадает, то тогда корневой порт выбирается на основе Port ID.

Конечный этап работы протокола STP по созданию топологии STP состоит в выборе выделенного порта для каждого сегмента локальной сети. Назначенным портом в каждом сегменте локальной сети является тот порт коммутатора, который анонсирует в этом сегменте локальной сети BPDU-пакеты с самой низкой стоимостью.

Одним из существенных недостатков протокола STPявляется долгое время конвергенции. Весь процесс занимает от 30 до 50 секунд – это довольно долго, если рассматривать это время с позиции отказоустойчивости сети. Для сокращения времени конвергенции был создан протокол RSTP (Rapid Spanning Tree Protocol). В нем, как правило, оно составляет меньше 10 се­кунд, а в некоторых случаях 1 – 2 секунды.

На оборудовании Cisco протоколы STP и RSTP должны работать в условиях наличия нескольких виртуальных локальных сетей. Для этого существуют проприетарные расширения Cisco для этих протоколов – PVST и Rapid PVST. Главной особенностью этих протоколов является создание отдельного экземпляра STP-процесса для каждого VLAN в сети.

Помимо развертывания протокола RSTP одним из наилучших способов уменьшения времени конвергенции протокола STP состоит в том, чтобы вообще исключить конвергенцию. Альтернативой протоколу RSTP может служить технология агрегирования каналов, в терминологии Cisco называемая **EtherChannel**. Агрегирование каналов позволяет решить две задачи - повысить пропускную способность канала, а также обеспечить резерв на случай выхода из строя одного из каналов. Суть технологии заключается в логическом объединении двух или более физических каналов связи в один логический.

Для агрегирования каналов на оборудовании Cisco может быть использован один из трёх вариантов:

1. Протокол LACP (Link Aggregation Control Protocol) - стандартный протокол динамической агрегации каналов связи.
2. Протокол PAgP (Port Aggregation Protocol) - проприетарный протокол Cisco, аналог LACP.
3. Статическое агрегирование без использования протоколов.

Так как LACP и PAgP решают одни и те же задачи (с небольшими отличиями по возможностям), то лучше использовать стандартный протокол, это позволит использовать агрегирование каналов в связке с оборудованием других производителей.

К преимуществам динамического агрегирования по протоколу LACP можно отнести согласование настроек с удаленной стороной, которое позволяет избежать ошибок и петель в сети. Также имеется поддержка standby-интерфейсов, которая позволяет агрегировать до 16-ти портов, 8 из которых будут активными, а остальные в режиме standby.Из недостатков можно выделить дополнительную задержку при поднятии агрегированного канала или изменении его настроек.

Напротив, статическое агрегирование не имеет дополнительной задержки при поднятии агрегированного канала, но также не имеет согласования настроек с удаленной стороной, что может привести к образованию петель в сети.

В качестве дополнительных настроек для коммутаторов, участвующих в действии протоколов STP и RSTP будут рассмотрены режимы PortFast и BPDU Guard.

Режим **PortFast** позволяет коммутатору немедленно переводить порт в состояние пересылки после того, как порт становится физически активным, минуя все этапы выбора топологии STP и исключая состояния самообучения и прослушивания. Но единственными портами, в которых можно без опасений разрешить использование режима PortFast, являются те порты, в отношении которых известно, что к ним не подключены какие-либо мосты, коммутаторы или другие устройства, участвующие в работе протокола STP. Режим PortFast в наибольшей степени подходит для соединения с устройствами конечных пользователей. Если режим PortFast установлен в портах, подключенных к устройствам конечных пользователей, то сразу после загрузки персонального компьютера конечного пользователя порт коммутатора может переходить в состояние пересылки протокола STP и перенаправления трафика. Если же режим PortFast не применяется, то каждый порт должен ожидать подтверждения коммутатором того, что этот порт является назначенным, а затем ожидать завершения времени пребывания интерфейса в переходных состояниях прослушивания и самообучения, прежде чем перейти в состояние пересылки.

Технология **BPDU Guard**, предусмотренная компанией Cisco защищает неизменность топологии сети, а главное препятствует злоумышленникам подключать устройства с низким приоритетом, чтобы заставить остальных коммутаторов думать, что в сети появился новый корневой коммутатор и перестроить всю топологию относительно атакующего устройства. Действие технологии заключается в следующем: происходит отключение порта при обнаружении ситуации, в ко­торой через пользовательский порт поступают какие-либо BPDU-блоки. Таким об­разом, данное средство безопасности становится особенно полезным применитель­но к портам, которые должны служить исключительно в качестве портов доступа (access-порты) и ни в коем случае не подключаться к другим коммутаторам. Кроме того, средство BPDU Guard часто используется в том же интерфейсе, в котором разрешен режим PortFast, поскольку порт с разрешенным режимом PortFast сразу после включения переходит в состояние пересылки, поэтому вероятность перенаправления через него кадров и создания кольцевых маршрутов повышается.

**Примечание**. Описание процессов моделирования для этой лабораторной работы можно найти в справке Packet Tracer: Справка ⇒ Содержимое ⇒ раздел «Моделирование» ⇒ Лаб. работа №3.

## Методические указания

1. Добавьте на рабочую область один коммутатор 2960-24TT и один узел PC-PT и соедините их с помощью кабеля «медный прямой». Повторите эту операцию еще два раза.
2. Имеющиеся на рабочей области коммутаторы также соедините между собой с помощью кабеля «медный перекрестный». Таким образом была создана избыточная топология (). В коммутаторах Cisco при стандартных настройках включен протокол STP. При правильном выполнении инструкций в такой топологии одно соединение между коммутаторами должно блокироваться.

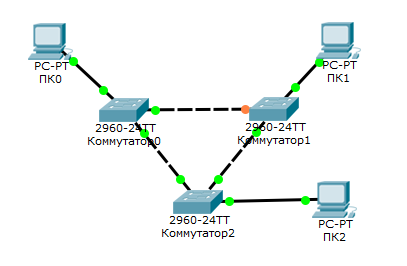


Рис. .. Избыточная сетевая топология

1. Войдите в консоль одного из коммутаторов и в привилегированном режиме введите команду ***show spanning-tree*** (сокращенно ***sh span***). С помощью данной функции на экран выводятся установки STP для коммутатора (), такие как режим spanning-tree (ieee), приоритет коммутатора (32769), приоритеты портов (128), стоимости портов (в таблице в столбце cost), таймеры spanning-tree, роли и статусы портов (Desg, FWD), а также другая информация. В случае просмотра корневого коммутатора также можно заметить надпись «***This bridge is the root***».
2. Последовательно вводя команду ***show spanning-tree***на всех коммутаторах, определите, какой коммутатор является корневым.

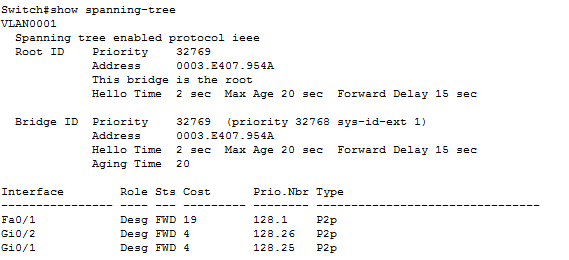


Рис. .. Настройки STP по умолчанию для коммутатора 2960-24TT

1. Попробуйте изменить корневой коммутатор. Для этого в любом некорневом коммутаторе перейдите в режим конфигурации и введите команду ***spanning-tree vlan 1 root primary*** (в таком виде команда меняет корневой коммутатор только для VLAN1). Значение приоритета коммутатора должно уменьшиться на 4096. Проверьте у коммутатора наличие статуса корневого и обратите внимание на то, как изменилась индикация соединений в топологии.

Следующим шагом будет установка корневых коммутаторов для разных VLAN в случае их множественного наличия.

1. Установите IP-адреса для ПК0, ПК1 и ПК2 в диапазоне от 192.168.1.1 до 192.168.1.3, также задайте значение маски подсети – 255.255.255.0.
2. Создайте новую VLAN 2 и настройте VTP-домен, а также установите VLAN-магистрали (материалы ).

Воспользуйтесь командой ***spanning-tree vlan <номер\_vlan> root primary*** для назначения разных корневых коммутаторов для разных VLAN. В итоге для VLAN1 должен быть один корневой коммутатор, а для VLAN2 другой. Осуществите проверку с помощью команды ***show spanning-tree***. Коммутатор должен является корневым по отношению к VLAN2, но некорневым по отношению к VLAN1 ().

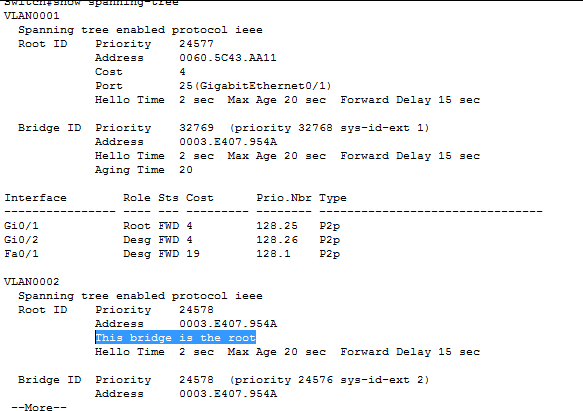


Рис. .. Выбор разных корневых коммутаторов для разных VLAN

Далее будет рассмотрен процесс конвергенции и переход на использование протокола RSTP.

1. В текущей топологии выключите канал связи между корневым и любым подключенным к нему коммутатором. Для этого на корневом коммутаторе зайдите в режим конфигурирования интерфейса и наберите команду ***shutdown*** (сокращенно ***sh***). Отслеживая показатель времени, обратите внимание на то, как долго будет производиться конвергенция.

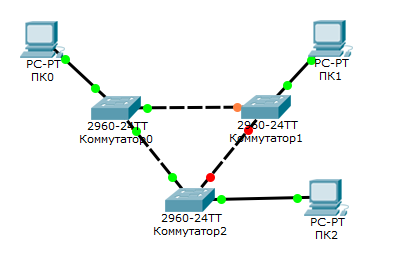


Рис. .. Начало процесса конвергенции

На показано, как между корневым Коммутатор2 и некорневым Коммутатор1 был закрыт канал связи. Далее начинается процесс конвергенции, в это время заблокированный порт проходит через состояния прослушивания и обучения, и только потом устанавливается в режим перенаправления. Для того чтобы процесс конвергенции проходил быстрее, необходимо перейти к протоколу RSTP.

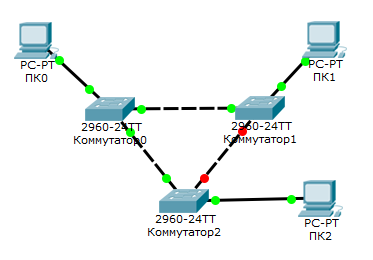


Рис. .. Окончание процесса конвергенции

1. Восстановите закрытый канал связи с помощью команды ***no shutdown*** (сокращенно ***no sh***).
2. В режиме конфигурации введите следующую команду: ***spanning-tree mode rapid-pvst***. Это позволит перейти к использованию протокола RPVST, проприетарного расширения Cisco для протокола RSTP.
3. Проверьте переключение протокола с помощью команды ***show spanning-tree***.

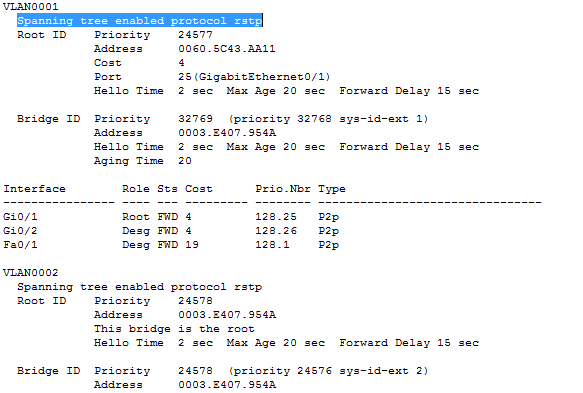


Рис. .. Включение протокола RPVST

1. Включите протокол RPVST на двух оставшихся коммутаторах.
2. Вновь выключите канал связи между корневым и некорневым коммутатором. Сравните скорость конвергенции. Она должна быть существенно выше, чем ранее.

Далее будут рассмотрены дополнительные настройки для протоколов связующего дерева:

1. Для настройки конфигурации режима PortFast на всех портах доступа (access-порты) в консоли выбранного коммутатора войдите в режим конфигурации, а затем наберите команду ***spanning-tree portfast default***. Чтобы включить PortFast только для одного интерфейса, нужно ввести команду ***spanning-tree portfast*** из режима конфигурации выбранного интерфейса. Для отключения PortFast на интерфейсе служит команда ***spanning-tree portfast disable***.
2. Последовательно включите режим PortFast на всех access-портах в сети.
3. Введите команду ***spanning-tree bpduguard enable*** для запуска службы BPDU Guard. Отключение опции производится командой ***spanning-tree bpduguard disable***.
4. Включите BPDU Guard для всех access-интерфейсов в сети.

В заключительной части работы будет рассмотрена задача агрегирования каналов. Каждое соединение Gigabit Ethernet будет заменено на агрегированный канал, состоящий из двух подключений Fast Ethernet.

1. Удалите все имеющиеся соединения между коммутаторами и замените их соединениями Fast Ethernet по два канала между коммутаторами, аналогично предыдущей топологии. Так как имеется три коммутатора, между ними будут установлены отказоустойчивые каналы с помощью трех разных способов агрегирования.
2. Для первой группы портов (канал связи между Коммутатор0 и Коммутатор2) выберите статическое агрегирование. Войдите в режим конфигурации двух интерфейсов на одном из коммутаторов. Для этого воспользуйтесь командой ***interface range <номер первого интерфейса-номер последнего интерфейса>*** (произойдет переход в режим конфигурации диапазона всех интерфейсов от первого до последнего).
3. Перед настройкой агрегирования лучше выключить физические интерфейсы. Достаточно отключить их с одной стороны, настроить агрегирование с двух сторон, а затем восстановить связь. Отключите интерфейсы с помощью команды ***shutdown***.
4. Воспользуйтесь командой ***channel-group <номер группы> mode on*** для объединения двух портов в одну группу. Номер группы должен быть одинаковым для всех портов, принадлежащих одному агрегированному каналу.
5. Перейдите к настройке интерфейсов другого коммутатора и добавьте два порта в эту же группу. Таким образом, в одной группе должно находиться по 2 порта от двух коммутаторов.
6. Вернитесь к настройке интерфейсов первого коммутатора, и с помощью команды ***no shutdown*** (сокращенно ***no sh***) восстановите связь.
7. Проверить наличие портов в группе можно командой ***show etherchannel summary*** (сокращенно ***sh eth sum***).

Статическое агрегирование между Коммутатор0 и Коммутатор2 настроено. Теперь будет произведена настройка динамического агрегирования по протоколу LACP между Коммутатор1 и Коммутатор2.

1. Зайдите в режим конфигурации интерфейсов Коммутатор2 и отключите их. Введите команду ***channel-protocol lacp***, тем самым настраивая интерфейсы на работу с протоколом LACP.
2. Сгруппируйте интерфейсы командой ***channel-group <номер группы> mode active***.
3. Перейдите в режим конфигурации интерфейсов Коммутатор1 и повторите эти настройки, но команду ***channel-group*** измените на ***channel-group <номер группы> mode passive***.
4. Вернитесь к настройке Коммутатор2 и включите интерфейсы, а затем проверьте группировку с помощью команды ***show etherchannel summary***.

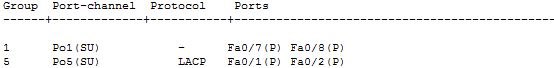


Рис. .. Вывод команды ***show etherchannel summary*** на Коммутаторе2

Динамическое агрегирование с помощью протокола PAgPаналогично настройке по протоколу LACP, но команды конфигурации принимают следующий вид:

* команда ***channel-protocol lacp*** заменяется на ***channel-protocol pagp***;
* команда ***channel-group <номер группы> mode active*** заменяется на ***channel-group <номер группы> mode desirable***;
* команда ***channel-group <номер группы> mode passive*** заменяется на ***channel-group <номер группы> mode auto***.

Итоговая сеть с настроенными агрегированными каналами должна выглядеть следующим образом:

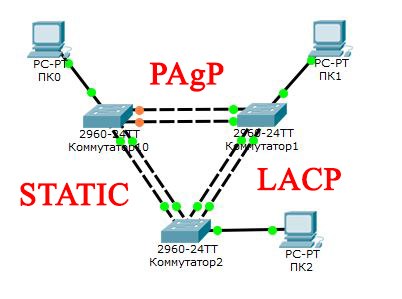


Рис. .. Итоговый вид сети с настроенными агрегированными каналами

Обратите внимание на внешний вид сети. Канал связи между Коммутатор0 и Коммутатор1 имеет два заблокированных интерфейса, которые, по сути, являются одним логическим портом. Протокол STP для агрегированных каналов работает так же, как и для обычных.

**Примечание**. При создании VLAN-магистралей между коммутаторами с настроенным агрегированием каналов нужно входить в режим конфигурации логического интерфейса. Названия логических интерфейсов можно посмотреть командой ***show etherchannel summary*** в столбце «port-channel». Чтобы зайти в режим конфигурации логического интерфейса используйте команду ***interface <имя\_port\_channel>***.

## Заключение

Гибкое владение службами протокола связующего дерева и агрегированием каналов позволяет специалистам следующее:

* предотвращать широковещательные штормы в сети;
* создавать устойчивые к аварийным ситуациям каналы связи;
* эффективно распределять трафик как в работающей, так и в повреждённой сети;
* увеличивать безопасность сети.

За счет конфигурируемости STP в топологии специалист может настраивать роли коммутаторов и портов таким образом, чтобы распределить стабильное соединение на самом устойчивом к поломкам участке.

## Контрольные задания

1. Модифицировать задание №1 из лабораторной работы №2. Проложить отказоустойчивые соединения между этажами с помощью резервации каналов по технологии Fast Ethernet. Корневым коммутатором назначить коммутатор на втором этаже. Включить протокол RPVST на всех коммутаторах. Все access-порты настроить в режим PortFast, а также активировать режим BPDU Guard.
2. Модифицировать задание №2 из лабораторной работы №2. Проложить отказоустойчивые соединения между центральным и остальными коммутаторами с помощью агрегирования каналов по протоколу LACP (использовать Gigabit Ethernet). Настроить VLAN-магистрали между логическими интерфейсами. Все access-порты настроить в режим PortFast, а также активировать режим BPDU Guard.
3. Модифицировать задание №3 из лабораторной работы №2. Соединить отделы торговли, производства и кадров через коммутаторы по топологии «звезда». Между коммутаторами установить отказоустойчивые соединения с помощью статического агрегирования каналов по технологии Fast Ethernet. Включить протокол RPVST на всех коммутаторах. Настроить VLAN-магистрали между логическими интерфейсами. Все access-порты настроить в режим PortFast, а также активировать режим BPDU Guard.
4. Модифицировать задание №4 из лабораторной работы №2. Проложить отказоустойчивые соединения между двумя этажами в каждом здании с помощью динамического агрегирования каналов по протоколу PAgP (использовать Gigabit Ethernet). Между зданиями проложить резервный оптоволоконный канал связи. Включить протокол RPVST на всех коммутаторах. Настроить VLAN-магистрали между логическими интерфейсами. Все access-порты настроить в режим PortFast, а также активировать режим BPDU Guard.

# Коммутаторы третьего уровня и Организация IP-подсетей

## Цели и задачи

Основной целью данной лабораторной работы является изучение возможностей коммутаторов третьего уровня по маршрутизации трафика между виртуальными локальными сетями.

Для достижения данной цели будут выполнены следующие задачи:

* конфигурация работы коммутатора третьего уровня в качестве коммутатора уровня распределения;
* изучение процесса сегментирования (разбиения) сети на третьем уровне модели OSI;
* разбиение сети на IP-подсети статически и с помощью протокола динамической настройки узла DHCP;
* настройка IP-маршрутизации на коммутаторе третьего уровня для получения связи между виртуальными локальными сетями.

## Теоретические сведения

В предыдущих лабораторных работах взаимодействие узлов в сети было организовано с помощью коммутаторов второго (канального) уровня модели OSI. Однако при проектировании больших сетей с множеством сегментов встает вопрос об использовании оборудования, работающего на третьем (сетевом) уровне модели OSI. К такому оборудованию относятся специальные коммутаторы третьего уровня, речь о которых пойдет в этой лабораторной работе, а также маршрутизаторы, которые будут рассмотрены в последующих работах. Для лучшего понимания роли коммутаторов второго и третьего уровней в сети необходимо привести сравнение:

Коммутаторы второго уровня модели OSI:

* коммутация трафика осуществляется на основе MAC-адресов, а также с помощью идентификаторов VLAN-сетей;
* выступают в качестве коммутаторов уровня доступа – предоставляют доступ к сети конечным устройствам (например, ПК);
* имеют возможность первичного логического разбиения сети на сегменты с помощью технологии VLAN. Однако связь устройств из разных виртуальных локальных сетей может быть настроена только с помощью устройств третьего уровня модели OSI;
* стоимость коммутаторов второго уровня существенно ниже коммутаторов третьего уровня при одинаковом количестве портов, поэтому для подключения конечных устройств выгоднее использовать коммутаторы второго уровня.

Коммутаторы третьего уровня модели OSI:

* поддержка IP-маршрутизации. Коммутаторы третьего уровня могут не только разбить сеть на виртуальные локальные сети, но также поддерживают маршрутизацию трафика между этими сегментами на основе IP-адресов;
* выступают в качестве коммутаторов уровня распределения – подключаются к коммутаторам уровня доступа для сокращения количества связей между ними;
* обладают высокой производительностью по сравнению с маршрутизаторами. Для маршрутизации трафика внутри сети предпочтительнее использовать коммутаторы третьего уровня, а для связи с внешними сетями рекомендуется использовать маршрутизаторы.

Ключевой особенностью коммутаторов третьего уровня является возможность маршрутизации трафика между виртуальными локальными сетями, но для такой маршрутизации необходимо для каждой VLAN выделить отдельную IP-подсеть. Задача выделения подсети сводится к правильному назначению IP-адресов и масок для всех сетевых соединений в рамках сегмента. Рассмотрим процесс разбиения сети на подсети на примере:

Имеется предприятие c некоторым количеством логических отделов, требуется разделить сеть с адресом 192.168.0.0 и маской 255.255.255.0 на несколько подсетей в соответствии с правилом «один VLAN – одна подсеть», учитывая требуемое количество узлов в каждой подсети:

* отдел разработки: 120 узлов;
* отдел тестирования: 60 узлов;
* отдел распространения: 25 узлов;
* отдел бухгалтерии: 10 узлов;
* отдел кадров: 5 узлов.

Начинать делить сеть нужно от самой большей требуемой подсети к самой меньшей. В данном примере самая большая требуемая подсеть – отдел разработки, в котором нужно выделить 120 узлов. Необходимо записать исходную маску подсети в двоичном виде ():

Таблица .. Исходная маска подсети в десятичном и двоичном видах

|  |  |
| --- | --- |
| Десятичный вид | Двоичный вид |
| 255.255.255.0 | 11111111.11111111.11111111.00000000 |

Количество доступных для назначения адресов в сети определяется по формуле, где «x» - количество нулевых бит в маске подсети, а «-2» - количество недоступных IP-адресов (широковещательный адрес и адрес самой подсети). Из этой формулы следует, что доступное количество адресов с маской 255.255.255.0 равняется 254 (. Теперь нужно подобрать такое значение «x», при котором количество адресов будет минимально возможным для выделения 120 узлам. Для этого удобно использовать ():

Таблица .. Соотношение значений «X» и количества доступных адресов

|  |  |
| --- | --- |
| Значение «X» | Количество доступных адресов |
| 8 | 254 |
| 7 | 126 |
| 6 | 62 |
| 5 | 30 |
| 4 | 14 |
| 3 | 6 |
| 2 | 2 |
| 1 | 0 |

Минимальное значение «x» для выделения адресов 120 узлам – 7. Это означает, что маска подсети будет состоять из семи нулевых бит. Далее следует применить эту маску к исходному IP-адресу для получения двух подсетей (жирным цветом выделена часть сети):

1. **11000000.10101000.00000000.0**0000000 (сеть 192.168.0.0 с маской 255.255.255.128).
2. **11000000.10101000.00000000.1**0000000 (сеть 192.168.0.128 с маской 255.255.255.128).

Первая подсеть будет представлять собой отдел разработки, а вторую подсеть требуется разбить на две подсети по 62 узла в каждом для выделения адресов на отдел тестирования.

1. **11000000.10101000.00000000.10**000000 (сеть 192.168.0.128 с маской 255.255.255.192).
2. **11000000.10101000.00000000.11**000000 (сеть 192.168.0.192 с маской 255.255.255.192).

Таким образом, для отдела тестирования выделяется подсеть 192.168.0.128 с маской 255.255.255.192, в которой диапазон доступных для назначения адресов начинается с адреса 192.168.0.129 до адреса 192.168.0.191 (итого 62 адреса).

Далее следует разбить подсеть 192.168.0.192 еще на две подсети:

1. **11000000.10101000.00000000.110**00000 (сеть 192.168.0.192 с маской 255.255.255.224).
2. **11000000.10101000.00000000.111**00000 (сеть 192.168.0.224 с маской 255.255.255.224).

Отделу распространения теперь принадлежит подсеть 192.168.0.192 с маской 255.255.255.224, с диапазоном адресов от 192.168.0.193 до 192.168.0.223 (30 адресов).

Тем же способом разбивается подсеть 192.168.0.224:

1. **11000000.10101000.00000000.1110**0000 (сеть 192.168.0.224 с маской 255.255.255.240).
2. **11000000.10101000.00000000.1111**0000 (сеть 192.168.0.240 с маской 255.255.255.240).

Отделу бухгалтерии будет соответствовать подсеть 192.168.0.224 с маской 255.255.255.240 (диапазон 192.168.0.225 – 192.168.0.239, итого 14 адресов).

Последним шагом будет выделение подсети для отдела кадров:

1. **11000000.10101000.00000000.11110**000 (сеть 192.168.0.240 с маской 255.255.255.248).
2. **11000000.10101000.00000000.11111**000 (сеть 192.168.0.248 с маской 255.255.255.248).

Таким образом, отделу кадров будет принадлежать подсеть 192.168.0.240 с маской 255.255.255.248, с диапазоном адресов от 192.168.0.241 до 192.168.0.247 (6 адресов).

Таблица .. Выделенные подсети для отделов

| Название отдела | Диапазон доступных адресов | Маска подсети |
| --- | --- | --- |
| Разработки | 192.168.0.1 – 192.168.0.127 | 255.255.255.128 |
| Тестирования | 192.168.0.129 – 192.168.0.191 | 255.255.255.192 |
| Распространения | 192.168.0.193 – 192.168.0.223 | 255.255.255.224 |
| Бухгалтерии | 192.168.0.225 – 192.168.0.239 | 255.255.255.240 |
| Кадров | 192.168.0.241 – 192.168.0.247 | 255.255.255.248 |

Для практического решения задачи сегментирования сети на третьем уровне модели OSI необходимо настроить интерфейс каждого сетевого соединения – заполнить поля «IP-адрес» и «Маска подсети», опционально указать основной шлюз и адрес DNS-сервера. Такую настройку можно провести статически, что означает настройку вручную каждого устройства в сети, либо динамически с помощью протокола DHCP (Dynamic Host Configuration Protocol — протокол динамической настройки узла). Статическая настройка обычно используется для настройки серверов, а также если в сети небольшое количество устройств. Однако для сетей с большим количеством узлов необходимо настраивать DHCP-сервер.

Процесс получения IP-адреса от сервера состоит из четырех этапов:

1. Обнаружение DHCP. Клиент выполняет широковещательный запрос по всей физической сети с целью обнаружить доступные DHCP-серверы. Он отправляет сообщение типа DHCPDISCOVER.
2. Предложение DHCP. Получив сообщение от клиента, сервер определяет требуемую конфигурацию клиента в соответствии с указанными сетевым администратором настройками. Сервер отправляет ему ответ (DHCPOFFER), в котором предлагает IP-адреса.
3. Запрос DHCP. Выбрав одну из конфигураций, предложенных DHCP-серверами, клиент отправляет запрос DHCPREQUEST.
4. Подтверждение DHCP. Сервер подтверждает запрос и направляет сообщение DHCPACK клиенту. После этого клиент настраивает свой сетевой интерфейс в соответствии с полученной конфигурацией.

**Примечание**. Описание процессов моделирования для этой лабораторной работы можно найти в справке Packet Tracer: Справка ⇒ Содержимое ⇒ раздел «Моделирование» ⇒ Лаб. работа №4.

## Методические указания

В данной лабораторной работе будет рассмотрена задача объединения четырех офисов с помощью нескольких коммутаторов второго уровня и одного коммутатора третьего уровня. Каждый офис имеет один коммутатор уровня доступа, к которому подключаются конечные устройства. Коммутаторы уровня доступа объединяются с помощью коммутатора уровня распределения. Один из четырех офисов отведен под серверную комнату, в остальных офисах расположены ПК пользователей.

Расположите необходимые устройства на рабочей области ():

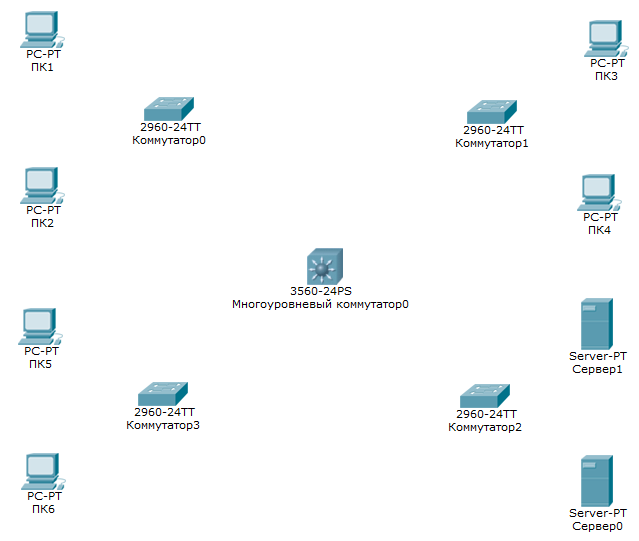


Рис. .. Необходимые устройства для выполнения лабораторной работы

Для разделения данной сети на логические сегменты предлагается разбить сеть с адресом 192.168.0.0 и маской 255.255.255.0 на несколько подсетей следующим образом:

* подсеть 1: 20 узлов;
* подсеть 2: 20 узлов;
* подсеть 3: 4 узла (подсеть серверов);
* подсеть 4: 10 узлов.

На прямоугольниками помечены разные подсети:

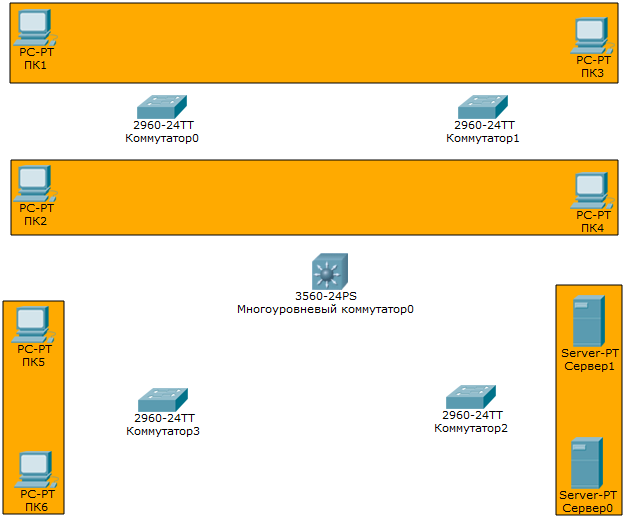


Рис. .. Расположение подсетей на логическом рабочем пространстве

Далее будет описан процесс соединения устройств и настройки первичной сегментации сети с помощью технологии VLAN:

1. Соедините коммутаторы уровня доступа с конечными устройствами с помощью соединений типа «медный прямой».
2. Соедините коммутаторы уровня доступа с коммутатором уровня распределения с помощью соединений типа «медный перекрестный». На таких связях потребуется отказоустойчивый канал, поэтому продублируйте соединения.

**Примечание**. В силу высокой нагрузки на коммутатор третьего уровня, следует по возможности использовать каналы связи с самой высокой пропускной способностью. Однако в рамках ограничений Cisco Packet Tracer коммутаторы третьего уровня представлены только одной моделью – Cisco 3560, которая имеет только 2 модуля Gigabit Ethernet, поэтому отказоустойчивые связи будут строиться на интерфейсах Fast Ethernet.

1. Настройте статическое агрегирование каналов между коммутаторами уровня доступа и коммутатором уровня распределения (материалы ). Не забудьте выключить интерфейсы командой ***shutdown*** перед настройкой агрегации, иначе возможен переход некоторых интерфейсов в состояние блокирования из-за работы протокола STP.
2. Агрегированные каналы необходимо настроить на работу в режиме **trunk**. На коммутаторе третьего уровня зайдите в режим конфигурации логического интерфейса с помощью команды ***interface <имя\_логического\_интерфейса>***. Имена логических интерфейсов можно посмотреть командой ***show etherchannel summary***. Далее введите команду ***switchport mode trunk***.

**Примечание**. Может появиться ошибка ***Command rejected: An interface whose trunk encapsulation is «Auto» cannot be configured to «trunk» mode.*** Это происходит из-за того, что динамическое определение инкапсуляции (ISL или 802.1Q) работает только с динамическими режимами настройки (LACP и PAgP). Для того чтобы настроить интерфейс в статическом режиме, необходимо инкапсуляцию также настроить статически. Это делается с помощью команды ***switchport trunk encapsulation dot1q***. После ввода этой команды повторите команду ***switchport mode trunk***. Таким же образом настройте в режим trunk все соединения между коммутатором третьего уровня и коммутаторами второго уровня. Не забудьте, что настраивать интерфейсы нужно с двух сторон!

1. Сконфигурируйте коммутатор третьего уровня как VTP-сервер, а коммутаторы второго уровня как VTP-клиенты (материалы ). Создайте на коммутаторе третьего уровня четыре виртуальные локальные сети с номерами 2, 3, 4, 5. Первый VLAN останется по умолчанию для всех интерфейсов, не участвующих в работе сети. Если VTP-сервер был настроен правильно, то на остальных коммутаторах виртуальные локальные сети создадутся автоматически.
2. Переведите интерфейсы коммутаторов второго уровня, связанные с конечными устройствами, в режим access. Не забудьте указать VLAN, которому принадлежит интерфейс (команда ***switchport access vlan <номер\_vlan>***).

После выполнения всех настроек сеть должна пройти этап первичной сегментации на втором уровне модели OSI. Устройства, находящиеся в одном VLAN, должны успешно выполнять echo-запросы между собой, но устройства из разных виртуальных локальных сетей не должны иметь связи. Для обеспечения маршрутизации трафика между виртуальными локальными сетями нужно настроить коммутатор третьего уровня на IP-маршрутизацию, но сначала требуется разделить сеть на подсети по правилу «один VLAN – одна подсеть». Исходя из условий задачи, первоначальный IP-адрес сети – 192.168.0.0 с маской 255.255.255.0. Первая подсеть должна иметь 20 доступных для назначения адресов, значит, исходя из таблицы в теоретической части лабораторной работы, нужна маска с пятью нулевыми битами – 255.255.255.224. Таким образом, диапазон доступных адресов для первой подсети будет 192.168.0.1 – 192.168.0.31.

Далее будет рассмотрен процесс настройки IP-адресов и масок для устройств в первой подсети:

1. Зайдите в режим конфигурации коммутатора третьего уровня (***conf t***). Нужно назначить IP-адрес для VLAN2, этот адрес будет маршрутом по умолчанию для всех устройств в этой виртуальной локальной сети. Введите команду ***interface vlan 2***. Устройство перейдет в режим конфигурации интерфейса (***config-if*** после ***#***).
2. Присвойте IP-адрес этому VLAN командой ***ip address 192.168.0.1 255.255.255.224***. Синтаксис команды: ***ip address <IP-адрес> <Маска\_подсети>***. Теперь этот IP-адрес можно указывать в качестве основного шлюза для конечных устройств, состоящих в VLAN2.

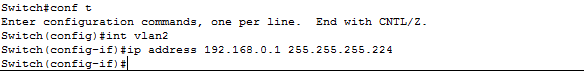


Рис. . Назначение IP-адреса для VLAN2

1. Зайдите на рабочий стол ПК1, перейдите к настройке IP. Заполните поля так, как показано на . Обратите внимание, что основным шлюзом необходимо указывать IP-адрес, заданный на коммутаторе третьего уровня.

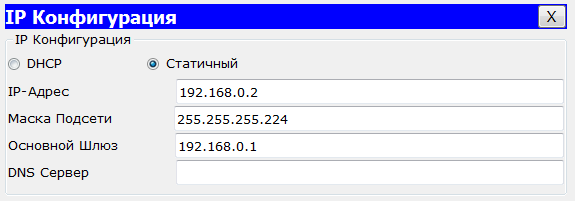


Рис. .. Настройка IP-адреса на ПК1

1. Аналогично IP-адрес ПК3 (192.168.0.3).
2. Повторите шаги 1-4 для настройки IP-адресов на всех устройствах VLAN 3, 4 и 5.

Ниже приведены все значения для заполнения ():

Таблица .. IP-адреса и маски для всех интерфейсов VLAN

|  |  |  |  |
| --- | --- | --- | --- |
| Название интерфейса/устройства | IP-адрес | Маска подсети | Основной шлюз |
| VLAN3 | 192.168.0.33 | 255.255.255.224 | - |
| ПК2 | 192.168.0.34 | 255.255.255.224 | 192.168.0.33 |
| ПК4 | 192.168.0.35 | 255.255.255.224 | 192.168.0.33 |
| VLAN4 | 192.168.0.81 | 255.255.255.248 | - |
| Сервер0 | 192.168.0.82 | 255.255.255.248 | 192.168.0.81 |
| Сервер1 | 192.168.0.83 | 255.255.255.248 | 192.168.0.81 |
| VLAN5 | 192.168.0.65 | 255.255.255.240 | - |
| ПК5 | 192.168.0.66 | 255.255.255.240 | 192.168.0.65 |
| ПК6 | 192.168.0.67 | 255.255.255.240 | 192.168.0.65 |

1. После выполнения всех настроек нужно включить IP-маршрутизацию на коммутаторе третьего уровня. Зайдите в режим конфигурации (***conf t***) и введите команду ***ip routing***.
2. С помощью echo-запросов проверьте соединения различных устройств в сети. Теперь даже устройства из разных виртуальных локальных сетей должны иметь связь между собой. Обратите внимание, что команду ***ping <ip-адрес>*** можно выполнять как на ПК, так и на любом коммутаторе.

Заключительной частью лабораторной работы будет настройка протокола DHCP для автоматизации процесса получения IP-адресов устройствами в сети. Сначала будет рассмотрен способ настройки DHCP на выделенном сервере, а затем способ конфигурации коммутатора третьего уровня в роли DHCP-сервера.

Настройка протокола DHCP на Сервер0:

1. Нажмите на Сервер0 и перейдите на вкладку «Службы». Слева выберите пункт «DHCP». Откроется меню настроек протокола DHCP на Сервер0. Необходимо последовательно создать три пула для раздачи адресов, каждый пул соответствует одной подсети.
2. Заполните поле «Имя пула»: DHCP-VLAN2.
3. В поле «Основной шлюз» введите IP-адрес VLAN2, который был назначен на коммутаторе третьего уровня: 192.168.0.1.
4. В поле «DNS-сервер» необходимо указать какой-либо DNS-сервер, например, 8.8.8.8 (публичный DNS-сервер Google).
5. Заполните начальный IP-адрес (192.168.0.0) и маску подсети (255.255.255.224).
6. В поле «Максимальное кол-во пользователей» введите 30 (количество доступных для назначения IP-адресов).
7. Нажмите кнопку «Добавить», а затем «Сохранить».
8. Аналогичным образом создайте пулы для VLAN3 и VLAN5 (для VLAN4 не нужно создавать пул, потому что в этой виртуальной локальной сети находятся только серверы, а для них рекомендуется настраивать статический IP-адрес). Обратите внимание, что поля «Имя пула», «Основной шлюз», «Начальный IP-адрес», «Маска подсети», а также «Максимальное кол-во пользователей» будут отличаться для разных VLAN. Поле «DNS-сервер» может совпадать.
9. Включите службу DHCP, отметив «Вкл» рядом с именем интерфейса.

После создания трех пулов должны получиться следующие настройки:

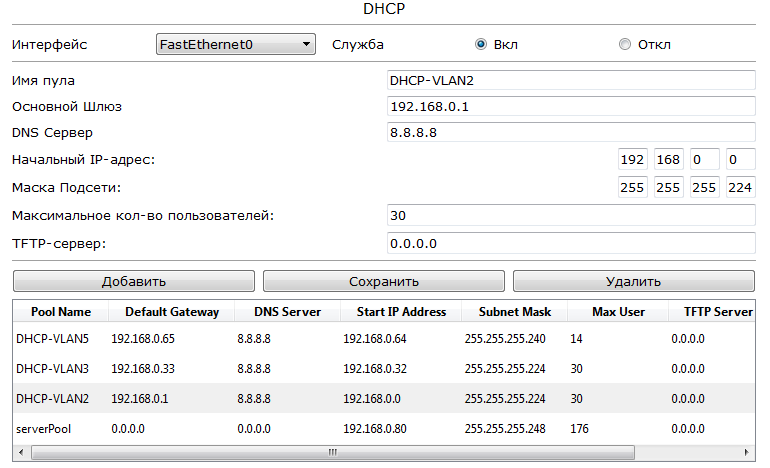


Рис. .. Настройка DHCP-сервера

Теперь необходимо настроить агента DHCP-Relay на коммутаторе третьего уровня. Суть DHCP-Relay заключается в пересылке широковещательного пакета от клиента одноадресатным пакетом DHCP-серверу, поэтому для каждого VLAN, на который будет приходить сообщение DHCPDISCOVER необходимо указать IP-адрес DHCP-сервера:

1. На коммутаторе третьего уровня войдите в режим конфигурации интерфейса VLAN2 командой ***interface vlan2***.
2. Укажите адрес DHCP-сервера с помощью команды ***ip helper-address 192.168.0.82***.
3. Аналогичные действия проведите для VLAN3 и VLAN5.

Проверьте работу DHCP-сервера. Зайдите в настройки IP-адреса любого ПК и отметьте пункт «DHCP». Через некоторое время автоматически заполнятся все поля и появится надпись: «Успешный DHCP запрос».

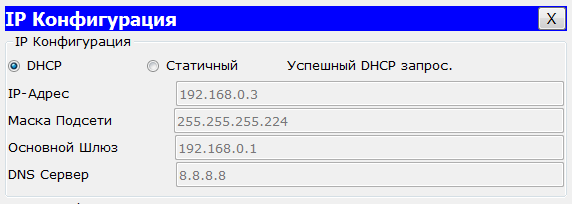


Рис. .. Автоматическое получение IP-адреса с помощью протокола DHCP

В качестве DHCP-сервера может также выступать коммутатор третьего уровня. Это может быть полезно, если в сети не присутствует сервер, но присутствует множество узлов. Выключите существующий DHCP-сервер:

1. В настройках сервера выключите службу DHCP, отметив «Откл» во вкладке «Службы».
2. На коммутаторе третьего уровня в режиме конфигурации VLAN-интерфейса введите команду ***no ip helper-address 192.168.0.83***, тем самым удаляя перенаправление клиентских широковещательных сообщений DHCPDISCOVER к DHCP-серверу.

Теперь можно перейти к настройке DHCP-сервера на коммутаторе третьего уровня. Введите команды так, как показано на рисунках ниже:

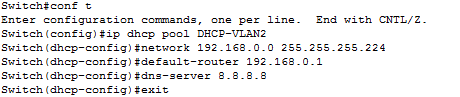


Рис. . Настройка DHCP для VLAN2

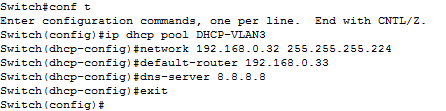


Рис. . Настройка DHCP для VLAN3

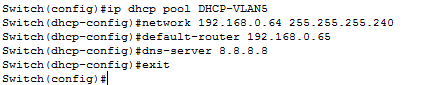


Рис. .. Настройка DHCP для VLAN5

После выполнения всех настроек обязательно проверьте работу протокола DHCP с помощью способа, описанного выше. Также на коммутаторе третьего уровня можно посмотреть список всех выданных IP-адресов. Это можно сделать из привилегированного режима командой ***show ip dhcp binding***.

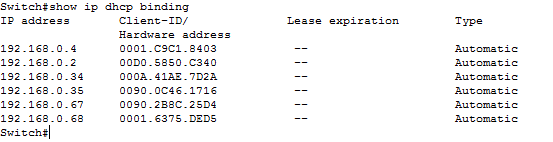


Рис. .. Вывод команды show ip dhcp binding

## Заключение

Умение настраивать коммутаторы третьего уровня в связке с коммутаторами второго уровня позволяет сетевым инженерам строить иерархическую модель сети. В такой модели каждый коммутатор имеет свою роль: коммутатор уровня доступа или коммутатор уровня распределения. Внедрение такой модели в проект сети позволяет:

* маршрутизировать трафик между виртуальными локальными сетями на третьем уровне модели OSI;
* снизить количество соединений между коммутаторами;
* повысить производительность сети за счет распределения трафика на одном высокопроизводительном устройстве;
* централизовать всю инфраструктуру сети для достижения простоты в управлении ресурсами;
* обеспечить стабильность и безопасность работы для пользователей за счет отказоустойчивости соединений с коммутатором уровня распределения.

## Контрольные задания

1. Модифицировать задание №1 из лабораторной работы №2. Добавить в сеть коммутатор третьего уровня, подключить к нему коммутаторы второго уровня, расположенные на этажах. Организовать отказоустойчивость по технологии динамического агрегирования LACP. Добавить сервер, настроить автоматическую выдачу IP-адресов с помощью DHCP. Разбить сеть на подсети:

* отдел программистов: 4 узла;
* отдел тестеров: 3 узла;
* отдел администраторов. 2 узла;
* серверная: 1 узел.

В качестве начального IP-адреса сети взять 192.168.10.0 с маской 255.255.255.0.

1. Модифицировать задание №2 из лабораторной работы №2. Заменить центральный коммутатор второго уровня на коммутатор третьего уровня. Организовать отказоустойчивость по технологии статического агрегирования каналов. Настроить DHCP на коммутаторе третьего уровня. Разбить сеть на подсети:

* отдел 1: 111 узлов;
* отдел 2: 55 узлов;
* отдел 3: 10 узлов;
* отдел 4: 20 узлов.

В качестве начального IP-адреса сети взять 192.168.20.0 с маской 255.255.255.0.

1. Модифицировать задание №3 из лабораторной работы №2. Добавить в сеть коммутатор третьего уровня, подключить к нему коммутаторы второго уровня. Организовать отказоустойчивость по технологии динамического агрегирования PAgP. Добавить сервер, настроить автоматическую выдачу IP-адресов с помощью DHCP. Разбить сеть на подсети:

* отдел производства: 5 узла;
* отдел кадров: 3 узла;
* отдел бухгалтерии: 2 узла;
* отдел продаж: 2;
* серверная: 1 узел.

В качестве начального IP-адреса сети взять 192.168.30.0 с маской 255.255.255.0.

1. Модифицировать задание №4 из лабораторной работы №2. Добавить коммутатор третьего уровня, подключить к нему коммутаторы второго уровня. Организовать отказоустойчивость по технологии статического агрегирования каналов. Настроить DHCP на коммутаторе третьего уровня. Разбить сеть на подсети:

* отдел производства: 62 узла;
* отдел разработки: 30 узла.

В качестве начального IP-адреса сети взять 192.168.40.0 с маской 255.255.255.0.

# списки доступа ACL

## Цели и задачи

Основная цель данной лабораторной работы – получение практических навыков работы со стандартными и расширенными списками доступа на оборудовании Cisco.

Будут решены следующие задачи:

* изучение функционала и особенностей стандартных и расширенных списков доступа;
* создание и настройка стандартных списков доступа для фильтрации трафика по IP-адресу отправителя;
* создание и настройка расширенных списков доступа для фильтрации трафика по различным критериям (IP-адрес, порт, протокол);
* настройка удаленного подключения к оборудованию Cisco с помощью протокола Telnet, применение списков доступа для ограничения таких подключений.

## Теоретические сведения

В результате применения списков управления доступом (**access list**, или сокращенно **ACL**) маршрутизатор или коммутатор третьего уровня (а также многие другие устройства) отбрасывает некоторые пакеты, учитывая критерии, которые определены сетевым инженером в списках. Назначение этих фильтров состоит в блокировании нежелательного трафика в сети, что позволяет не только создавать препятствия перед злоумышленниками, пытающимися проникнуть в сеть, но и не позволить служащим самой компании обращаться к тем системам, которые для них должны быть закрыты.

Ниже перечислены некоторые важные особенности списков управления доступом Cisco:

* фильтрация пакетов может осуществляться по мере их поступления в интерфейс, еще до принятия решений о маршрутизации (список на **входящий** трафик);
* фильтрация пакетов может производиться перед выходом из интерфейса, после принятия решений о маршрутизации (список на **исходящий** трафик);
* в программном обеспечении Cisco IOS для указания на то, что пакет должен быть отфильтрован, используется термин **deny** (запретить), а для пропуска пакета далее – термин **permit** (разрешить);
* если в списке управления доступом определено несколько инструкций, то пакет сравнивается с каждой инструкцией последовательно до тех пор, пока не будет найдена та инструкция, которой соответствует пакет;
* в конце каждого списка управления доступом находится неявная инструкция, запрещающая весь трафик (deny all). Поэтому, если пакет не соответствует ни одной из инструкций в списке управления доступом, он отбрасывается.

Списки управления доступом делятся на 5 видов:

1. **Стандартные** (standard) – позволяют фильтровать трафик по одному единственному критерию – IP-адрес отправителя.
2. **Расширенные** (extended) – позволяют фильтровать трафик по пяти различным критериям: IP-адрес отправителя, IP-адрес получателя, порт отправителя, порт получателя, а также протокол, инкапсулированный в пакет.
3. **Рефлексивные** (reflexive) – предоставляют возможность предотвращать атаки определенного класса, направленные на бреши в системе безопасности, поскольку позволяют отдельно пропускать через устройство каждый разрешенный TCP- или UDP-сеанс. Для этого предусмотрено, чтобы устройство реагировало определенным образом, обнаруживая первый пакет в новом сеансе обмена данными между двумя узлами. Реагируя на появление пакета, устройство добавляет в список управления доступом инструкцию permit, в результате чего разрешается прохождение в сеансе трафика, характеризующегося применением определенных IP-адресов отправителя и получателя, а также конкретного порта.
4. **Динамические** (dynamic) – связывают применение списка управления доступом с процессом аутентификации пользователя. Если аутентификация прошла успешно, то устройство динамически добавляет запись в начало списка, разрешая прохождение трафика, от­правителем которого является узел, прошедший проверку подлинности.
5. **Временные** (time-based) – позволяют добавлять ограничения по време­ни в команды конфигурации. В некоторых случаях может потребоваться проверка пакетов с учетом критериев в списке управления доступом, но только в определен­ное время дня или даже в определенные дни недели.

В данной лабораторной работе будут подробно рассматриваться только стандартные и расширенные списки управления доступом, так как они имеют наиболее широкий спектр применения в корпоративных сетях. Поэтому далее будут приведены сведения, которые характеризуют только эти два вида списков управления доступом.

Существует два разных синтаксиса для обозначения списков управления доступом:

* «Старый» синтаксис – для идентификации используются номера. За стандартными ACL закреплены номера 1-99 и 1300-1999, за расширенными – 100-199 и 2000-2699;
* «Новый» синтаксис – для идентификации используется имя, выбранное администратором.

Независимо от того, используются ли стандартные или расширенные списки управления доступом, можно дать устройству указание, должна ли проверка проводиться с учетом всего IP-адреса или только части IP-адреса. Для этого используются **инвертированные маски подсети**.

Маски с инвертированными битами описывают 32-битовый номер, как и маски подсети. В отличие от последних, нулевые биты (0) в инвертированной маске служат для устройства указанием, что при выполнении операции сопоставления необходимо сравнивать соответствующие им биты в адресе с инструкцией списка управления доступом. Двоичные единицы (1) в инвертированной маске указывают устройству, что обозначенные ими биты не должны сравниваться. Например, инвертированная маска 0.0.0.0 указывает на то, что должен быть сопоставлен весь IP-адрес, а маска 255.255.255.255 рассматривается как сопоставляемая с любыми адресами. Инвертированная маска 0.0.0.0 в Cisco IOS может быть заменена на ключевое слово ***host***, а маска 255.255.255.255 – на ключевое слово ***any***.

Общий синтаксис команды настройки конструкции стандартного списка управления доступом выглядит следующим образом: ***access-list*** <***номер\_списка***> <***deny*** | ***permit***> <***отправитель***> <***инвертированная\_маска\_отправителя***>.

Примеры стандартных списков управления доступом:

* ***access-list 1 deny host 192.168.0.1* –** инструкция фильтрует все пакеты, в которых IP-адрес отправителя равен 192.168.0.1;
* ***access-list 1 permit any*** – инструкция разрешает все пакеты с любыми IP-адресами;
* ***access-list 1 deny 192.168.1.0 0.0.0.255*** – инструкция фильтрует пакеты, в которых IP-адрес отправителя принадлежит подсети 192.168.1.0.

Расширенные списки управления доступом позволяют проводить проверку по многим критериям, поэтому синтаксис соответствующей команды невозможно записать в виде одной универсальной команды. В такие списки также можно вводить наименования протоколов и номера портов. Ниже приведены таблицы, в которых указана необходимая информация о приложениях и соответствующих им стандартных номеров портов, а также операторы, которые используются при проверке номеров портов:

Таблица ... Приложения и соответствующие им номера портов

|  |  |  |  |
| --- | --- | --- | --- |
| Номер порта | Протокол | Приложение | Ключевое слово с обозначением названия приложения в синтаксисе команды *access-list* |
| 20 | TCP | FTP | *data ftp-data* |
| 21 | TCP | FTP | *ftp* |
| 22 | TCP | SSH | *-* |
| 23 | TCP | Telnet | *telnet* |
| 25 | TCP | SMTP | *smtp* |
| 53 | TCP, UDP | DNS | *domain* |
| 67,68 | UDP | DHCP | *nameserver* |
| 69 | UDP | TFTP | *tftp* |
| 80 | TCP | HTTP(WWW) | *www* |
| 110 | TCP | POP3 | *pop3* |
| 161 | UDP | SNMP | *snmp* |
| 443 | TCP | SSL | *-* |
| 16384-32767 | UDP | Передача голоса (VoIP) | *-* |

Таблица .. Операторы, использующиеся при проверке номеров портов

|  |  |
| --- | --- |
| Оператор в команде *access-list* | Значение |
| *eq* | Равно |
| *neq* | Не равно |
| *lt* | Меньше |
| *gt* | Больше |
| *range* | Диапазон номеров портов |

Примеры расширенных списков управления доступом:

* ***access-list 101 deny ip any host 192.168.1.1*** – инструкция фильтрует IP-пакеты с любым адресом отправителя и адресом получателя 192.168.1.1;
* ***access-list 101 deny tcp any host 192.168.1.1 eq telnet*** – инструкция фильтрует TCP-пакеты с любым адресом отправителя, адресом получателя 192.168.1.1 и номером порта получателя 23 (используется ключевое слово ***telnet***);
* ***access-list 101 permit tcp host 192.168.2.1 eq smtp any*** – инструкция разрешает TCP-пакеты с адресом отправителя 192.168.2.1, номером порта отправителя 25 (***smtp***), и любым IP-адресом получателя.

Компания Cisco также разработала рекомендации для применения списков управления доступом, ниже приведены некоторые из них:

* размещайте стандартные ACL как можно ближе к по­лучателю, т.к они часто уничтожают важные пакеты, нужные другим сетям;
* размещайте расширенные ACL как можно ближе к отправителю пакета, чтобы сразу же отбросить определенные типы пакетов;
* размещайте более специфичные (т.е. узкие) правила проверки ближе к началу списка управления доступом;
* прежде чем вносить изменения в ACL, удалите его в интерфейсе, в котором он был задан (с помощью команды ***no ip access-group***);
* создавайте списки управления доступом с помощью текстового редактора, а затем вносите готовые команды конфигурации на устройство с использованием копирования и встав­ки.

**Примечание**. Описание процессов моделирования для этой лабораторной работы можно найти в справке Packet Tracer: Справка ⇒ Содержимое ⇒ раздел «Моделирование» ⇒ Лаб. работа №5.

## Методические указания

В качестве исходной будет использоваться сеть филиала предприятия, которая была смоделирована в прошлой лабораторной работе. Для начала проверьте связь различных устройств с помощью команды ***ping***. Echo-запросы должны успешно выполняться между всеми устройствами в сети. Это важно, потому что далее с помощью списков управления доступом связь между некоторыми устройствами будет ограничиваться.

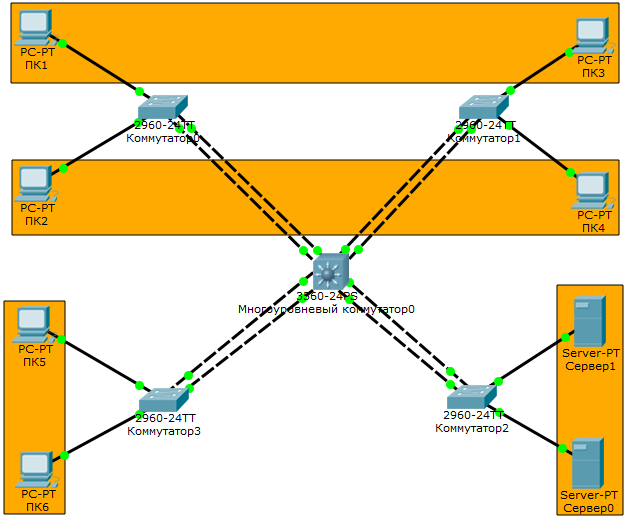


Рис. .. Исходная сеть предприятия

Для создания простейшего стандартного списка управления доступом последовательно выполните следующие действия:

1. Предположим, что нужно ограничить доступ ПК1 к Сервер1. Необходимо принять решение о том, на каком интерфейсе оптимальнее всего расположить список управления доступом, а также в каком направлении будет осуществляться фильтрация трафика. Следуя рекомендациям Cisco, стандартные ACL лучше всего располагать как можно ближе к получателю, то есть на сегменте от коммутатора третьего уровня до Коммутатор2. Списки доступа можно располагать как на физических интерфейсах, так и на логических, в данном случае будет использоваться логический интерфейс VLAN4. Оптимальнее всего будет фильтровать исходящий трафик на этом интерфейсе, чтобы снизить нагрузку на Сервер1. Зайдите в CLI Многоуровневого коммутатора0, а затем в режим конфигурации интерфейса Vlan 4 (***conf t*** ⇒ ***int vlan 4***). Здесь необходимо указать список управления доступа и направление фильтрации. Введите команду ***ip access-group 1 out***. Номер 1 указывает на будущий список доступа, а ключевое слово ***out*** определяет, что фильтроваться будет исходящий трафик.
2. Теперь нужно создать сам список управления доступа. Создание всех ACL происходит из режима глобальной конфигурации. Введите команду ***access-list 1 deny host 192.168.0.2*** (возможно у вас будет другой IP-адрес на ПК1, тогда введите его). Теперь все пакеты, исходящие из интерфейса VLAN4 будут отбрасываться, если IP-адрес отправителя будет равен 192.168.0.2. Однако на этом настройка не окончена, потому что все остальные пакеты также будут отбрасываться из-за неявной инструкции ***deny ip any any*** которая расположена в конце каждого списка управления доступом.
3. Введите команду ***access-list 1 permit any***. Это позволит пропускать весь остальной трафик, не удовлетворяющий первой инструкции созданного ACL. Обратите внимание, что инструкции для списка доступа должны быть введены именно в таком порядке, иначе трафик от ПК1 все равно будет проходить до Сервер1, т.к он удовлетворяет инструкции ***access-list 1 permit any***.
4. Проверьте работу списка управления доступом. Попробуйте создать echo-запрос от ПК1 до Сервер1. Он должен заканчиваться неудачей.

Созданный стандартный список доступа обладает явным недостатком – он фильтрует трафик только от одного узла-отправителя. А что если необходимо заблокировать трафик от нескольких узлов? Очевидно, что писать множество инструкций не самый лучший вариант. Вместо этого можно написать одну инструкцию, которая будет фильтровать трафик от множества узлов, например, от всей подсети, в которой состоит ПК1. Для этого в списке управления доступом необходимо указать IP-адрес подсети и инвертированную маску. Рассмотрим пример создания такого списка:

1. Удалите ранее созданный ACL с помощью команды ***no access-list 1***, также в режиме конфигурации интерфейса VLAN4 удалите указание на этот список командой ***no ip access-group 1 out***.
2. Не выходя из конфигурации интерфейса VLAN4, введите указание на новый список командой ***ip access-group Test-access out***. В этой команде «Test-access» является именем списка управления доступом. Использование именованных списков вместо нумерованных – это «новый» синтаксис для обозначения ACL.
3. В режиме конфигурации введите команду ***ip access-list standard Test-access***. Коммутатор должен перейти в режим конфигурации списка управления доступом с именем «Test-access». На это указывает надпись «***(config-std-nacl)***» после имени устройства в CLI.
4. Теперь необходимо последовательно ввести инструкции для созданного ACL. Чтобы выполнялась фильтрация трафика от всей подсети, в которой состоит ПК1, необходимо указать IP-адрес этой подсети (192.168.0.0), а также инвертированную маску, которую необходимо вычислить с помощью вычитания стандартной маски подсети из маски 255.255.255.255. Каждый октет маски вычитается отдельно, поэтому если стандартная маска подсети равна 255.255.255.224, то инвертированная маска будет равна 0.0.0.31.Итоговая инструкция будет выглядеть следующим образом: ***deny 192.168.0.0 0.0.0.31***.
5. Вторая инструкция будет разрешать весь трафик, который не удовлетворяет условию первой инструкции – ***permit any***.
6. Проверьте работу созданного списка управления доступом – узел ПК3, который находится с ПК1 в одной подсети теперь не должен иметь доступа к Сервер1.

Побочным эффектом от списка доступа с такой конфигурацией является невозможность связи узлов ПК1 и ПК3 с Сервером0, поскольку он находится в той же подсети, что и Сервер1, а значит трафик у обоих серверов обрабатывается логическим интерфейсом VLAN4.

Для того, чтобы ограничить связь ПК1 и ПК3 только с Сервер1 необходимо использовать расширенные списки управления доступом. Однако, чтобы продемонстрировать полный функционал таких списков, задание следует усложнить. Предположим, что требуется ограничить доступ двум подсетям (с которыми ассоциированы VLAN2 и VLAN3) к Сервер1 по любому другому протоколу, кроме FTP (чтобы оставить возможность пользоваться файловым сервером). Исходя из рекомендаций Cisco по использованию списков управления доступом, расширенные ACL следует размещать как можно ближе к отправителю, это означает, что список следует установить на интерфейсах VLAN2 и VLAN3 с фильтрацией на входящий трафик. Следует просчитать инвертированную маску подсети таким образом, чтобы она покрывала диапазоны IP-адресов сразу двух подсетей. Для этого сначала возьмем обычную маску подсети 255.255.255.192, с помощью которой покрывается диапазон из 64 IP-адресов (192.168.0.0 – 192.168.0.64), а затем вычтем ее из маски 255.255.255.255. Итоговая инвертированная маска будет равна 0.0.0.63. Далее следует составить инструкции для будущего списка управления доступом, помещая самые узкие правила проверок в начало, а самые широкие – в конец. Ниже приведены эти инструкции в том порядке, в котором они должны быть в итоговом ACL:

***permit tcp 192.168.0.0 0.0.0.63 host 192.168.0.82 eq ftp***

***deny ip 192.168.0.0 0.0.0.63 host 192.168.0.82***

***permit ip any any***

Первая инструкция разрешает проходить TCP-пакетам с IP-адресом отправителя из подсети 192.168.0.0 и маской 255.255.255.192, IP-адресом получателя 192.168.0.82, и портом получателя 21. Вторая инструкция блокирует весь остальной трафик из этой подсети, если он направлен к узлу с IP-адресом 192.168.0.82, а третья инструкция разрешает проходить всем пакетам, не попавшим под условия других инструкций. Предварительный список управления доступом создан, теперь необходимо реализовать его на Многоуровневый коммутатор0:

1. Удалите предыдущий ACL (***no ip access-list standard Test-access***) и указание на него (***no ip access-group Test-access out***).
2. Зайдите в режим конфигурации и создайте расширенный ACL с помощью команды ***ip access-list extended ftp***. Здесь ***ftp*** – имя списка, а ключевое слово ***extended*** указывает на то, что созданный список управления доступом – расширенный.
3. Последовательно введите все инструкции, описанные ранее:

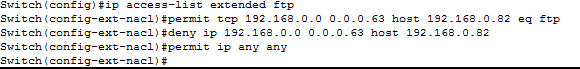


Рис. .. Создание расширенного списка управления доступом

1. Перейдите в режим конфигурации логического интерфейса VLAN2, затем введите команду ***ip access-group ftp in***. Повторите эту же команду для логического интерфейса VLAN 3.
2. Проверьте работу созданного списка управления доступом. С любых узлов, входящих в рассматриваемые подсети, отправьте echo-запросы до Сервер1, они должны заканчиваться неудачей. Также проверьте можно ли обратиться к Сервер1 по протоколу ftp, для этого воспользуйтесь кнопкой «Добавить сложный PDU», а затем укажите применение (FTP) и адрес назначения (192.168.0.82), а также порт источника (21). Такой PDU должен успешно доходить.

До сих пор, настройка всех устройств в Cisco Packet Tracer происходила через встроенную вкладку CLI, однако реальные устройства Cisco настраиваются напрямую через консольный порт, который есть на каждом коммутаторе или маршрутизаторе, или виртуально через удаленный доступ. Если для того, чтобы настроить устройство через консольный порт, необходимо находиться рядом с устройством, то для удаленного доступа настройка устройства может осуществляться с любого узла в сети, поэтому важно предотвратить нежелательные подключения с помощью списков управления доступом, тем самым обеспечив дополнительную безопасность сети. Далее будет рассмотрен процесс создания удаленного подключения к Многоуровневый коммутатор0 с помощью протокола Telnet:

1. Сначала необходимо создать учетную запись пользователя с паролем и уровнем привилегий. Зайдите в режим конфигурации и введите команду ***username admin privilege 15 password cisco***. Будет создана учетная запись с именем пользователя admin, уровнем привилегий 15 (максимальные), и паролем cisco.
2. Введите команду ***line vty 0 4***. Устройство перейдет в режим конфигурации виртуальной терминальной линии (сокращ. vty) под номером 0 4 (это значение по умолчанию).
3. Введите команду ***transport input telnet***. Теперь устройство будет готово к использованию протокола Telnet для входящих подключений.
4. Необходимо включить аутентификацию через имя пользователя и пароль с помощью команды ***login local***. Теперь все удаленные подключения будут защищены паролем.
5. Проверьте удаленное подключение. Зайдите в консоль на узле ПК5 и введите команду ***telnet 192.168.0.65***. Должен появиться запрос на имя пользователя и пароль. Пройдите аутентификацию с помощью имени пользователя admin и пароля cisco.

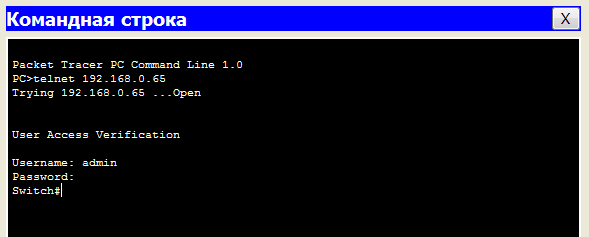


Рис. .. Удаленное подключение по протоколу Telnet

С помощью списков управления доступом возможно ограничить количество узлов, с которых будет возможно удаленное подключение. Для этого необходимо создать расширенный ACL с несколькими инструкциями. Предположим, что подсеть, в которой состоят ПК5 и ПК6 – это подсеть администраторов, для них будет доступно удаленное подключение по Telnet, для всех остальных это подключение будет запрещено.

Инвертированная маска для этой подсети будет равна 0.0.0.15 (обычная маска – 255.255.255.240), список управления доступом будет включен на всех логических интерфейсах Многоуровневого коммутатора0, фильтрация будет осуществляться на входящий трафик. Список инструкций будет выглядеть следующим образом:

***permit tcp 192.168.0.64 0.0.0.15 host 192.168.0.65 eq telnet***

***deny tcp 192.168.0.0 0.0.0.255 any eq telnet***

***permit ip any any***

Далее будет описан процесс создания расширенного списка управления доступа c заданной конфигурацией:

1. Зайдите в режим конфигурации и наберите команду ***ip access-list extended Telnet***.
2. Последовательно введите все инструкции, описанные ранее:

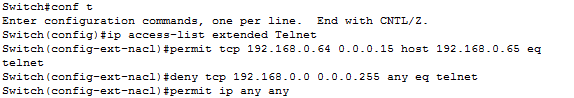


Рис. .. Создание расширенного списка управления доступом

1. Перейдите в режим конфигурации диапазона интерфейсов VLAN 2 – 6 с помощью команды ***interface range vlan 2-6***.
2. Введите команду ***ip access-group Telnet in***, указывая всем логическим интерфейсам на ACL с именем «Telnet».
3. Проверьте удаленное подключение по протоколу Telnet. Узлы ПК5 и ПК6 должны успешно подключаться и проходить аутентификацию, любые другие узлы должны выдавать ошибку:

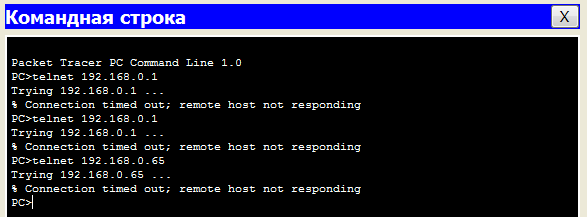


Рис. .. Ошибка «хост не отвечает»

## Заключение

Навыки работы со стандартными и расширенными списками управления доступом позволяют сетевым инженерами обеспечить первоначальную защиту сети от злоумышленников, а также обеспечивают фильтрацию трафика, оптимизируя тем самым загрузку сети. Также списки управления доступом могут применяться для:

* фильтрации обновлений маршрутизации и установки приоритета пакетов (QoS);
* построения тоннелей виртуальной частной сети (VPN). ACL определяют, какой трафик следует шифровать и пропускать через VPN-туннель;
* разграничения доступа к оборудованию (Установка паролей и ограничений);
* настройки конфигурации службы трансляции сетевых адресов (NAT);
* для использования Policy-based Routing (PBR) – маршрутизации на основе некоторых политик, установленных администратором.

Владение рефлексивными, динамическими и временными списками управления доступом еще сильнее расширяет область применения ACL, позволяя решать сложные узконаправленные задачи на предприятиях, такие как адаптация к внешним угрозам, автоматическое изменение уровня доступа для устройств и пользователей в зависимости от топологии сети, а также смена привилегий в зависимости от времени суток.

## Контрольные задания

1. Модифицировать задание №1 из лабораторной работы №4. Запретить доступ к серверу всем узлам в сети, кроме тех, которые находятся в отделе администраторов, сохранив возможность обращаться только по протоколу HTTP. Настроить на коммутаторе третьего уровня удаленные подключения по Telnet, ограничить такие подключения всем, кроме администраторов.
2. Модифицировать задание №2 из лабораторной работы №4. Запретить доступ узлам из отдела 1 в отдел 3 и 4 и наоборот. Запретить доступ узлам из отдела 2 в отдел 4 по всем портам, чей номер больше 21. Выделить один узел из отдела 1, которому будет дана возможность обращаться к узлам из отдела 2, всем остальным запретить доступ.
3. Модифицировать задание №3 из лабораторной работы №4. Запретить доступ к серверу всем узлам из отдела производства, остальным отделам разрешить обращаться к серверу только по портам 1541 и 1560-1591 (диапазон).
4. Модифицировать задание №4 из лабораторной работы №4. Разрешить общаться узлам из двух отделов только по следующим протоколам – TFPT, FTP, HTTP. Настроить на коммутаторе третьего уровня удаленные подключения по Telnet, ограничить такие подключения всем, кроме двух выбранных администраторов, каждый из которых должен находиться в разных зданиях.

# Маршрутизаторы и Статические маршруты

## Цели и задачи

В рамках данной лабораторной работы будет решаться проблема соединения и взаимодействия нескольких компьютерных сетей между собой.

В процессе выполнения будут решаться следующие задачи:

* изучение роли и функций маршрутизатора в локальной сети;
* создание и настройка подинтерфейсов на маршрутизаторе для обеспечения возможности маршрутизации трафика между виртуальными локальными сетями;
* настройка статической маршрутизации в масштабах совокупности сетей;
* настройка сервера системы доменных имен (DNS-сервер);
* создание корпоративной почты для двух филиалов компании (E-Mail-сервер).

## Теоретические сведения

В прошлой лабораторной работе в качестве маршрутизирующего оборудования был использован коммутатор третьего уровня, он выполнял задачу маршрутизации трафика внутри локальной сети. Однако если требуется настроить связь с внешними сетями, предпочтительнее использовать маршрутизатор. Рассмотрим особенности этих устройств:

Коммутатор третьего уровня:

* высокая производительность;
* возможность маршрутизации большого количества локального трафика;
* аппаратная реализация Cisco Express Forwarding;
* отсутствие поддержки NAT, Route-map, шейпинга;
* отсутствие возможности подсчета и шифрования трафика;
* отсутствие поддержки VPN-туннелей;
* отсутствие поддержки технологии SPI.

Маршрутизатор:

* относительно низкая производительность;
* маршрутизация большого количества локальных сетей практически невозможна, высока вероятность деградации сервиса при использовании QoS, ACL NBAR и других функций, приводящих к анализу приходящего на интерфейсы трафика;
* программная реализация Cisco Express Forwarding;
* поддержка NAT, Route-map и шейпигна;
* возможность подсчета и шифрования трафика;
* поддержка VPN-туннелей;
* поддержка технологии SPI.

Таким образом, главная особенность маршрутизатора в том, что он умеет очень гибко управлять трафиком, но обладает сравнительно низкой производительностью при работе внутри локальной сети. Коммутатор третьего уровня наоборот обладает высокой производительностью, но имеет ограниченный функционал при работе с трафиком, а это значит, что в случае подключения локальной сети к сети Интернет или построении VPN-канала с удаленными филиалами нужно использовать маршрутизатор.

Осуществляя маршрутизацию, маршрутизатор, как правило, использует адрес получателя, указанный в пакетных данных, и определяет по таблице маршрутизации путь, по которому следует передать данные. Если в таблице маршрутизации для адреса нет описанного маршрута, пакет отбрасывается.

Таблица маршрутизации содержит информацию, на основе которой маршрутизатор принимает решение о дальнейшей пересылке пакетов. Таблица состоит из некоторого числа записей — маршрутов, в каждой из которых содержится адрес сети получателя, адрес следующего узла, которому следует передавать пакеты, административное расстояние — степень доверия к источнику маршрута и некоторый вес записи — метрика. Метрики записей в таблице играют роль в вычислении кратчайших маршрутов к различным получателям. В зависимости от модели маршрутизатора и используемых протоколов маршрутизации, в таблице может содержаться некоторая дополнительная служебная информация. Пример:

***192.168.64.0/16 [110/49] via 192.168.1.2, 00:34:34, FastEthernet0/0.1***

Здесь 192.168.64.0/16 — сеть назначения, 110 – административное расстояние, 49 — метрика маршрута, 192.168.1.2 — адрес следующего маршрутизатора, которому следует передавать пакеты для сети 192.168.64.0/16, 00:34:34 — время, в течение которого был известен этот маршрут, FastEthernet0/0.1 — интерфейс маршрутизатора, через который можно достичь «соседа» 192.168.1.2.

Таблица маршрутизации может составляться двумя способами:

* **статическая маршрутизация** - записи в таблице вводятся и изменяются вручную. Такой способ требует вмешательства администратора каждый раз, когда происходят изменения в топологии сети. С другой стороны, он является наиболее стабильным и требующим минимума аппаратных ресурсов маршрутизатора для обслуживания таблицы. Вся маршрутизация при этом происходит без участия каких-либо протоколов маршрутизации. При задании статического маршрута обычно указывается адрес сети (на которую маршрутизируется трафик), маска сети, а также адрес узла, который отвечает за дальнейшую маршрутизацию (или подключен к маршрутизируемой сети напрямую). Опционально можно указать метрику (цену) маршрута. На некоторых устройствах можно указывать интерфейс, на который следует направить трафик сети и указать дополнительные условия, согласно которым выбирается маршрут.
* **динамическая маршрутизация** - записи в таблице обновляются автоматически при помощи одного или нескольких протоколов маршрутизации — RIP, OSPF, IGRP, EIGRP, IS-IS, BGP и тд. Кроме того, маршрутизатор строит таблицу оптимальных путей к сетям назначения на основе различных критериев — количества промежуточных узлов, пропускной способности каналов, задержки передачи данных и т. п. Критерии вычисления оптимальных маршрутов чаще всего зависят от протокола маршрутизации, а также задаются конфигурацией маршрутизатора. Такой способ построения таблицы позволяет автоматически держать таблицу маршрутизации в актуальном состоянии и вычислять оптимальные маршруты на основе текущей топологии сети. Однако динамическая маршрутизация оказывает дополнительную нагрузку на устройства, а высокая нестабильность сети может приводить к ситуациям, когда маршрутизаторы не успевают синхронизировать свои таблицы, что приводит к противоречивым сведениям о топологии сети в различных её частях и потере передаваемых данных.

**Примечание**. Описание процессов моделирования для этой лабораторной работы можно найти в справке Packet Tracer: Справка ⇒ Содержимое ⇒ раздел «Моделирование» ⇒ Лаб. работа №6.

## Методические указания

В рамках данной лабораторной работы будет рассмотрена задача настройки связи между двумя филиалами предприятия с помощью маршрутизаторов. Откройте проект сети, получившийся в ходе выполнения предыдущей лабораторной работы. Для начала необходимо создать второй филиал компании. Разместите устройства следующим образом ():

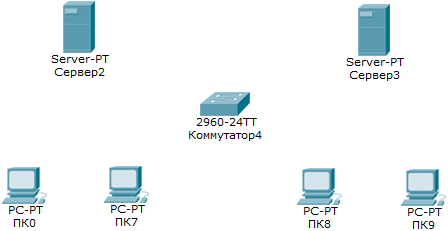


Рис. .. Устройства второго филиала

Второй филиал будет использовать новую сеть с адресом 192.168.1.0 и маской 255.255.255.0, содержащую несколько подсетей ():

* подсеть 1: 8 узлов;
* подсеть 2: 8 узлов;
* подсеть 3: 4 узла (подсеть серверов).

Локальная сеть второго филиала включает в себя малое количество устройств, поэтому нецелесообразно использовать коммутатор третьего уровня для маршрутизации трафика внутри сети, с этой задачей успешно справится и маршрутизатор.

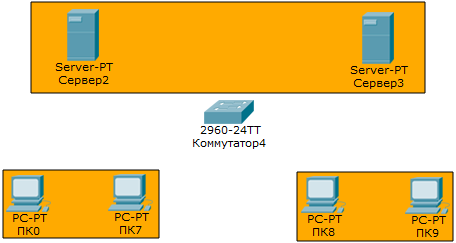


Рис. .. Подсети второго филиала

Настройте сеть созданного филиала:

1. Соедините конечные устройства с коммутатором второго уровня с помощью кабеля «медный прямой».
2. Проведите уже знакомые вам операции по созданию VLAN (материалы ).
3. Распределите устройства по сегментам VLAN. В итоге должно получиться три виртуальных локальных сети.
4. Добавьте два маршрутизатора 2620XM и один Router-PT-Empty (Generic) на рабочую область чуть ниже сетей филиалов ().

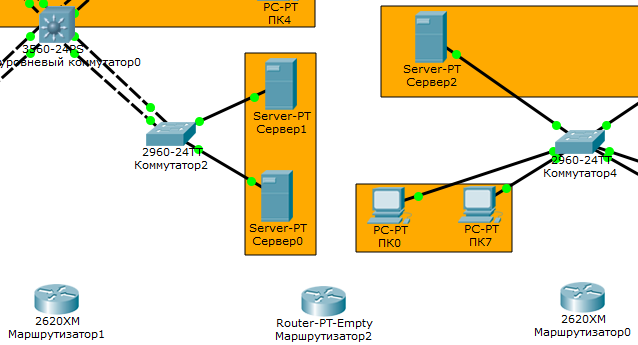


Рис. .. Расположение маршрутизаторов на рабочем пространстве

1. Соедините Маршрутизатор0 с Коммутатор4 с помощью кабеля «медный перекрёстный». Далее необходимо настроить магистраль между маршрутизатором и коммутатором. Для этого зайдите в конфигурирование интерфейса коммутатора и введите команду ***switchport mode trunk***.

Следующим шагом будет настройка адресов и масок для виртуальных локальных сетей на маршрутизаторе:

Таблица .. IP-адреса и маски подсетей для VLAN второго филиала

|  |  |  |
| --- | --- | --- |
| Интерфейс | IP-адрес | Маска подсети |
| VLAN2 | 192.168.1.1 | 255.255.255.248 |
| VLAN3 | 192.168.1.9 | 255.255.255.248 |
| VLAN4 | 192.168.1.17 | 255.255.255.248 |

1. Зайдите в режим конфигурирования маршрутизатора. (***conf t***).
2. В первую очередь, на маршрутизаторе необходимо включить физический интерфейс, так как по умолчанию он выключен. Для этого воспользуйтесь командой конфигурирования интерфейса ***no shutdown (no sh)***. Также, следует учитывать, что на этот порт маршрутизатора приходится несколько VLAN, поэтому следующим пунктом будет настройка подинтерфейсов (разделение физического интерфейса на несколько логических). Каждому подинтерфейсу будет соответствовать отдельная VLAN (команда ***interface vlan <номер\_vlan>*** на коммутаторе третьего уровня исполняет аналогичную функцию).
3. Для создания подинтерфейса и перехода в режим его конфигурирования воспользуйтесь командой ***int fa0/0.2***, где параметр ***fa0/0*** определяет физический порт, на котором будет создан подинтерфейс, а параметр ***.2*** обозначает номер подинтерфейса.
4. Введите команду ***encapsulation dot1q 2***, где параметр ***2*** отвечает за номер той VLAN, с которой будет ассоциирован подинтерфейс.
5. Введите адрес и маску подсети, используя команду ***ip address <IP\_адрес> <Маска\_подсети>***.
6. Включите подинтерфейс с помощью команды ***no sh***.
7. Повторите пункты 3-6 для двух оставшихся VLAN.
8. Проверьте статус подинтерфейсов, воспользовавшись командой ***show run***.

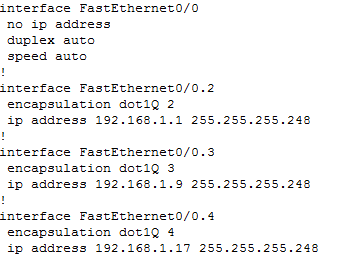


Рис. .. Список подинтерфейсов маршрутизатора

Теперь следует настроить протокол DHCP:

1. Настройте протокол DHCP на Сервер2 (см. лаб. раб. №4).
2. Настройте агента DHCP-Relay на VLAN-интерфейсах коммутатора и на подинтерфейсах маршрутизатора, использую команду ***ip helper-address <IP-адрес\_DHCP-сервера>***.
3. Измените настройку IP-адреса на всех рабочих станциях на «Dynamic», проверяя таким образом работу протокола DHCP.

На примере предыдущих действий был рассмотрен способ подключения сети с несколькими VLAN к маршрутизатору, используя коммутатор второго уровня. Следующим шагом является подключение сети уже имеющегося первого филиала к маршрутизатору. Первый филиал имеет в составе сети коммутатор третьего уровня, поэтому алгоритм подключения будет несколько иным.

1. Соедините Многоуровневый коммутатор0 и Маршрутизатор1 с помощью кабеля «медный прямой».
2. Создайте новую VLAN (VLAN6) на коммутаторе третьего уровня, а также виртуальный интерфейс (***interface vlan 6***).
3. Присвойте этому интерфейсу адрес 192.168.2.1 и маску 255.255.255.0. В дальнейшем, для простоты все «соединительные» сегменты между маршрутизаторами и коммутатором третьего уровня в данной лабораторной работе будут использовать каждый свой регистр адресов с маской 24 бита.
4. Определите интерфейс, который соединяет маршрутизатор и коммутатор третьего уровня, как access-порт, так как VLAN6 будет единственной на этом сегменте.
5. Перейдите в CLI на Маршрутизатор1 и включите на нём физический интерфейс. Как и говорилось выше, на данном сегменте имеется лишь одна VLAN, следовательно, отпадает необходимость настраивать на маршрутизаторе подинтерфейсы.
6. Определите на этом интерфейсе IP-адрес 192.168.2.2 с маской 255.255.255.0.

Связь между коммутатором и маршрутизатором установлена, однако маршрутизатор всё ещё не имеет доступа к конечным устройствам, так как необходима настройка статических маршрутов для сети 192.168.0.0. Зайдите в режим глобальной конфигурации на Маршрутизатор1 и последовательно выполните следующие команды (рис. 6.5):

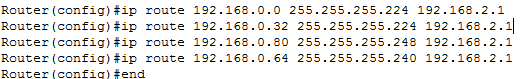


Рис. .. Настройка статических маршрутов в сети первого филиала

В команде ***ip route*** последовательно записываются три аргумента:

1. IP-адрес сети назначения.
2. Маска сети назначения.
3. IP-адрес интерфейса, через который будет проложен маршрут к сети назначения.

После выполнения всех команд обязательно проверьте маршруты в подсети с помощью echo-запросов (ping). Настройка маршрутизаторов в сетях обоих филиалов закончена, далее следует связать эти филиалы. Расстояние между филиалами превышает 100м, поэтому соединение между маршрутизаторами будет строиться на оптическом кабеле.

1. По умолчанию, маршрутизаторы не содержат необходимых модулей для подключения через оптический кабель. Добавьте в свободные слоты Маршрутизатор1 и 2 подходящие модули (NM-1FE-FX), предварительно сохранив конфигурации устройств (вкладка Конфигурация ⇒ NVRAM ⇒ Сохранить) и выключив их.
2. Добавьте два оптических модуля PT-ROUTER-NM-1FFE в Маршрутизатор2.
3. Соедините маршрутизаторы и настройте IP-адреса для интерфейсов ()

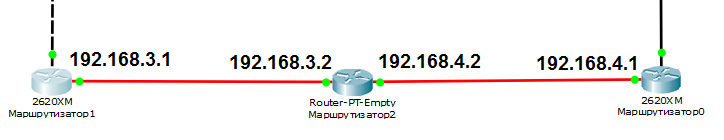


Рис. .. Связи между маршрутизаторами

На данном этапе возникла необходимость провести маршруты из одной сети в другую и наоборот. В первую очередь необходимо добавить маршрут по умолчанию для многоуровневого коммутатора в сети первого филиала. Таким образом, все пакеты, доставляемые на этот коммутатор и адресуемые неизвестной сети, будут отправляться на указанный адрес.

1. Перейдите в режим глобальной конфигурации многоуровневого коммутатора и введите команду ***ip route 0.0.0.0 0.0.0.0 192.168.2.2***.
2. Далее необходимо настроить статические маршруты на маршрутизаторах. Войдите в режим глобальной конфигурации Маршрутизатор1. Введите команду ***ip route 0.0.0.0 0.0.0.0 192.168.3.2***, добавляя тем самым маршрут по умолчанию, который указывает на интерфейс Маршрутизатор2.
3. Теперь нужно добавить маршруты от Маршрутизатор1 до всех подсетей первого филиала. Можно добавить маршруты для каждой его подсети (), однако, удобнее установить один суммированный маршрут до всей сети филиала (). Таким образом, с помощью замены маски с 255.255.255.248 на 255.255.255.0 сокращается количество необходимых команд с трех до одной.



Рис. .. Настройка группы статических маршрутов



Рис. .. Конфигурирование суммированного статического маршрута

1. Для Маршрутизатор0 достаточно добавить только маршрут по умолчанию до Маршрутизатор2 (***ip route 0.0.0.0 0.0.0.0 192.168.4.2***).
2. Для центрального маршрутизатора необходимо два маршрута:

* Маршрут до первого филиала через Маршрутизатор1.
* Маршрут до второго филиала через Маршрутизатор2.

Оба этих маршрута необходимо сделать суммированными, потому что иначе придется добавлять целых семь маршрутов (столько же, сколько и подсетей). Добавьте эти маршруты используя маску 255.255.255.0, как показано на рисунке ниже:



Рис. .. Настройка маршрута на устройстве Маршрутизатор2

При правильной настройке всех статических маршрутов, узлы одного филиала становятся доступны для узлов другого. Обязательно проверьте связи устройств из разных филиалов с помощью echo-запросов! Итоговая сеть должна иметь следующий вид ():

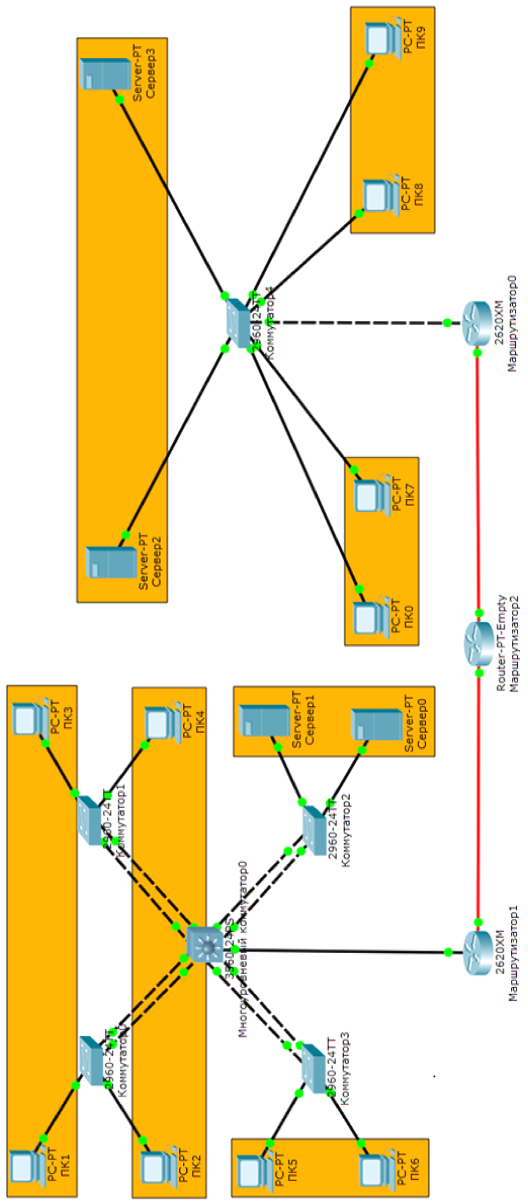


Рис. .. Общий вид сети

Финальным этапом работы является настройка корпоративной почты для того, чтобы пользователи двух филиалов могли общаться между собой. В эту задачу входит конфигурирование DNS-сервера (нужен для получения IP-адреса по имени хоста) и E-mail-серверов. Прежде чем приступить к дальнейшим действиям, необходимо отключить DHCP-сервер на многоуровневом коммутаторе в первом филиале с помощью команды ***no service dhcp*** и настроить DHCP-сервер на Сервер0, как это было сделано в рамках предыдущей лабораторной работы.

Так как в данной работе настройка DNS и E-mail-серверов будет производиться на отдельных устройствах, необходимо выбрать два свободных сервера. Например, Сервер3 из второго филиала будет DNS-сервером, а Сервер1 из первого филиала – E-mail-сервером. (Сервер2 и Сервер0 выполняют функции DHCP-серверов).

1. На всех серверах во вкладке «Конфигурация» установите значение DNS-Сервера на IP-адрес Сервер3. Также измените значение поля DNS-сервера в пулах адресов на DHCP-серверах.
2. Зайдите в настройку службы DNS на Сервер3. Введите в таблицу адреса всех серверов и присвойте каждому из них уникальное имя, а затем запустите службу.

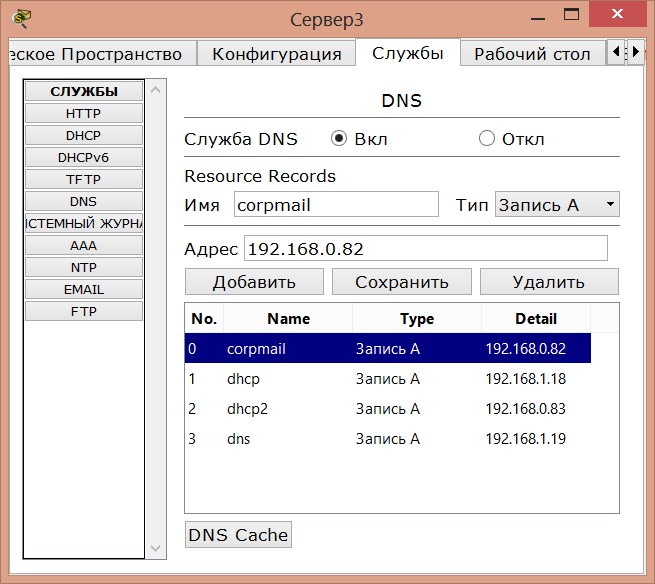


Рис. .. Настройка DNS-сервера

1. Теперь перейдите к настройкам службы EMAIL на Сервер1. Здесь необходимо указать имя домена (например, ***corpmail.com***), а затем добавить пользователей корпоративной почты и их пароли.

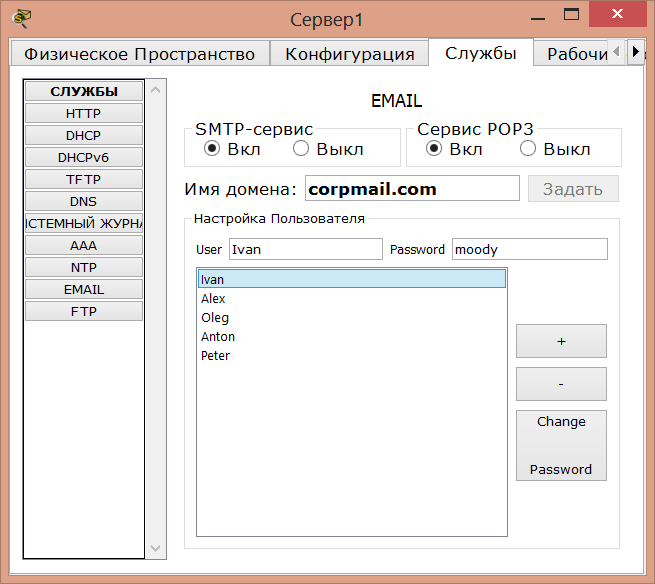


Рис. .. Настройка E-mail-сервера

1. В любой рабочей станции зайдите на рабочий стол и нажмите на ярлык «Email».
2. Настройте почтовый клиент на компьютере, правильно заполнив все поля в соответствии с конфигурацией E-mail-сервера.

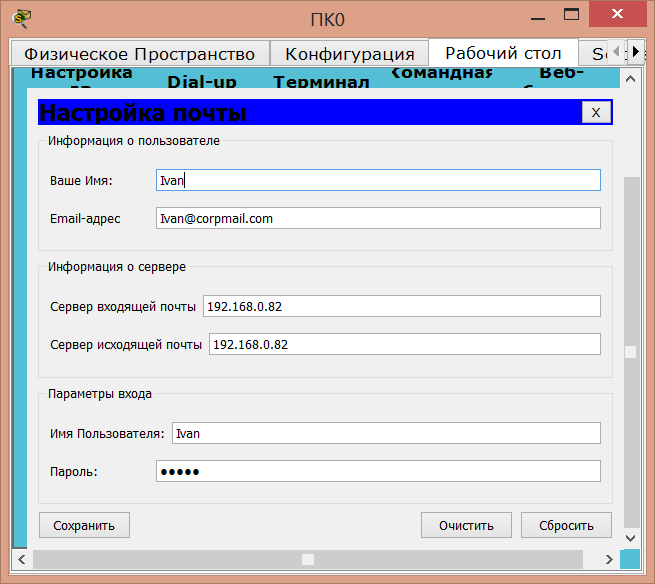


Рис. .. Настройка почтового клиента

1. Сохраните настройки и проделайте аналогичную операцию для другой рабочей станции.
2. Удостоверьтесь, что почта настроена правильно, послав письмо на компьютер с настроенным почтовым клиентом.

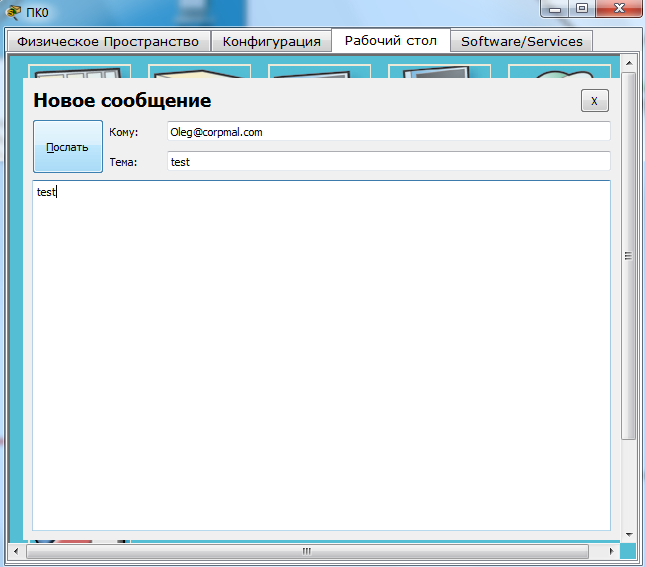


Рис. .. Проверка корпоративной почты

1. На компьютере-получателе зайдите в почтовый клиент и нажмите на кнопку «Получить». Вы должны увидеть полученное сообщение в таблице снизу.

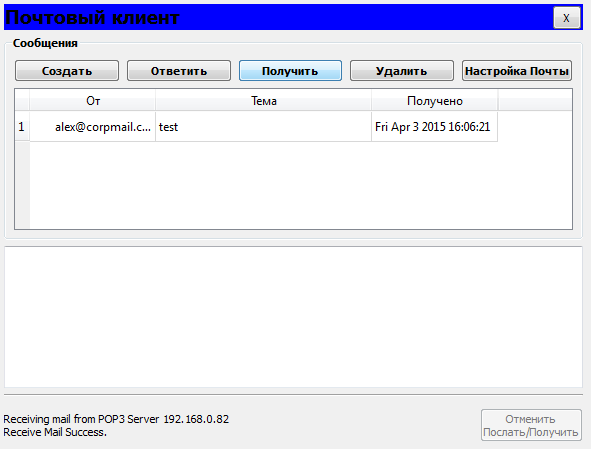


Рис. .. Полученное сообщение

1. Выполните настройку клиентов на оставшихся узлах в сети и проверьте работу корпоративной почты между двумя филиалами.

## Заключение

Настройка статических маршрутов является ценным навыком даже несмотря на широкое использование динамической маршрутизации, Статическая маршрутизация обладает рядом преимуществ, которые позволят:

* легко настроить предсказуемые маршруты между сетями, которые моментально могут быть задействованы;
* обеспечить маршрутизацию тупиковой сети;
* снизить использование ресурсов в сети, за счет отсутствия постоянной необходимости просчитывать маршрут;
* обеспечить безопасное соединение без «лазеек».

Использование статической маршрутизации дает преимущества небольшим локальным сетям или отдельным сегментам сети с медленным каналом, в которых дополнительная нагрузка в виде служебного трафика влияет на скорость передачи данных. В средних и больших сетях статическая маршрутизация применима только в сочетании с динамической, что повышает эффективность сети и облегчает ее администрирование.

## Контрольные задания

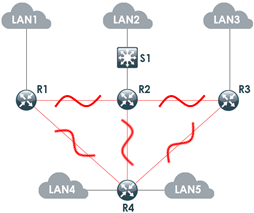


Рис. .. Схема сети задания №1

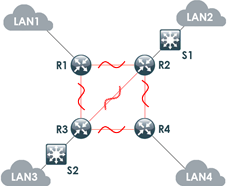


Рис. .. Схема сети задания №2

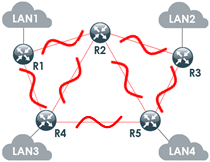


Рис. .. Схема сети задания №3

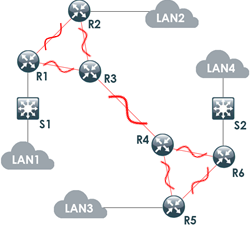


Рис. .. Схема сети задания №4

Выполните построение корпоративной сети, используя топологию в соответствии с вашим номером варианта. Настройте статические маршруты для каждого маршрутизатора, IP-адреса для интерфейсов и конечных устройств, а также содержание локальных сетей (количество устройств и их расположение) выберите самостоятельно. В локальных сетях настройте DHCP-сервера, а также DNS-сервер (один или несколько) и E-mail-сервер.

## Легенда

|  |  |
| --- | --- |
| Термин | Описание |
|  | Локальная вычислительная сеть |
|  | Коммутатор третьего уровня |
|  | Маршрутизатор |
|  | Волоконно-оптический кабель |
|  | Кабель «Медный прямой» |

# Динамическая маршрутизация. Протоколы RIP, OSPF и EIGRP

## Цели и задачи

Цель данной лабораторной работы – изучение основ динамической маршрутизации в сетях при помощи протоколов RIP, OSPF и EIGRP.

В процессе выполнения лабораторной работы будут решаться следующие задачи:

* изучение основных функций динамической маршрутизации;
* настройка loopback-интерфейсов на маршрутизаторах;
* настройка динамической маршрутизации по протоколам RIP, OSPF и EIGRP на маршрутизаторах Cisco;
* проверка отказоустойчивости сети, изучение таблиц маршрутизации;
* включение аутентификации на протоколах OSPF и EIGRP.

## Теоретические сведения

Маршрутизаторы строят таблицы маршрутизации на основе трех основных типов маршрутов: напрямую подключенные к устройству маршруты, статические маршру­ты и маршруты, полученные от протоколов динамической маршрутизации. Можно строить сети, используя только первые два типа маршрутов, однако сети, в которых используется динамическая маршрутизация обладают двумя серьезными преимуществами – автоматическим добавлением маршрутов и отказоустойчивостью. В операционной системе Cisco IOS поддерживаются многие протоколы динамической маршрутизации, однако все они выполняют примерно одинаковые функции, перечисленные ниже:

1. Получение информации об IP-подсетях от смежных устройств.
2. Анонсирование маршрутной информации об IP-подсетях смежным устройствам.
3. Если обнаружено более одного маршрута к какой-либо подсети, то выбор наилучшего маршрута на основе метрики.
4. Если происходит изменение топологии сети, например, отказ какого-либо канала связи, то запускается процесс конвергенции - уведомление других устройств о пропадании маршрута и выбор нового оптимальный маршрута.

Все протоколы IP-маршрутизации делятся на два больших класса:

* **IGP** — протокол маршрутизации, разработанный для использования внутри одной автономной системы (autonomous system — AS);
* **EGP** — протокол маршрутизации, предназначенный для маршрутизации между автономными системами.

Под автономной системой понимают сеть, находящуюся под единым административным управлением и принадлежащую одной организации. Все автономные системы имеют свой уникальный идентификатор, называемый номером автономной системы (AS number — ASN).

На сегодняшний день среди протоколов из класса EGP единственным использующимся является протокол граничного шлюза (Border Gateway Proto­col – BGP), а среди протоколов из класса IGP активно используются множество протоколов, наиболее популярными из них являются протоколы RIP, OSPF, IGRP, EIGRP, IS-IS и т.д.

Алгоритм, лежащий в основе протокола маршрутизации, определяет принцип его работы и методы обработки информации. Под термином алгоритм протокола маршрутизации понимается логика и процессы, используемые в различных протоколах маршрутизации, чтобы получить все маршруты в сети, выбрать из них наилучшие маршруты ко всем подсетям, а также обеспечить как можно более быструю конвергенцию протокола в ответ на изменения топологии сети.

Существует три больших класса алгоритмов для IGP-протоколов маршрутизации:

* дистанционно-векторные (называемые также алгоритмами Беллмана-Форда), по этим алгоритмам работает протокол RIP;
* алгоритмы с учетом состояния каналов (link-state), по этим алгоритмам работают протоколы OSPF и IS-IS;
* сбалансированные гибридные (их также называют расширенными дистанционно-векторными), по этим алгоритмам работает протокол EIGRP.

Наилучший маршрут в протоколах маршрутизации к какой-либо подсети выби­рается на основании определенной характеристики — **метрики**. Чем меньше метри­ка маршрута, тем более оптимальным является маршрут. Ниже, в , перечислены наиболее популярные протоколы маршрутизации и их метрики:

Таблица .. Метрики для протоколов динамической маршрутизации

|  |  |  |
| --- | --- | --- |
| Протокол | Метрика | Описание |
| RIP | Счетчик промежуточных маршрутизаторов или хопов (Hop count). | Количество маршрутизаторов (транзитных устройств) между данным маршрутизатором и сетью-получателем. |
| OSPF | Стоимость (Cost). | Сумма стоимостей всех каналов по маршруту следования пакета; стоимость обычно основана на значении полосы пропускания. |
| EIGRP | Композитная метрика, включающая в себя значение полосы пропускания и задержку (bandwidth and delay). | Рассчитывается исходя из значения полосы пропускания самого «медленного» канала на маршруте и кумулятивной задержки для такого маршрута. |

Если в сети есть резервные каналы и используется единственный протокол маршрутизации, каждый маршрутизатор может обнаружить несколько маршрутов к одной подсети, а затем выбрать оптимальный, используя метрику. Тем не менее, на практике часто возникают ситуации, когда в сети одновременно используется несколько протоколов маршрутизации. В такой ситуации маршрутизатор может получить несколько маршрутов к одной и той же подсети через несколько протоколов маршрутизации, и в таком случае метрики не помогут в выборе оптимального маршрута, поскольку метрики разных протоколов не совместимы между собой. В Cisco IOS эта проблема решается за счет присвоения административного расстояния (administrative distance — AD) каждому протоколу маршрутизации. Система IOS выбирает маршрут от протокола маршрутизации с меньшим значением AD. В приведены административные расстояния для наиболее распространенных источников маршрутов.

Таблица .. Административные расстояния для источников маршрутов

| Источник маршрутной информации | Административное расстояние |
| --- | --- |
| Напрямую подключенные сети | 0 |
| Статические маршруты | 1 |
| EIGRP | 90 |
| IGRP | 100 |
| OSPF | 110 |
| IS-IS | 115 |
| RIP | 120 |
| Неизвестный или недостоверный | 255 |

Ниже будет дано подробное описание работы трех протоколов маршрутизации – RIP, OSPF и EIGRP, так как именно эти протоколы будут использоваться в практической части лабораторной работы.

### Дистанционно-векторный протокол RIP

Двумя важными понятиями для протокола RIP являются дистанция и вектор. Когда процесс маршрутизации завершился и маршрутизатор знает маршрут к некоторой подсети, такой маршрут характеризуется двумя параметрами: дистанцией (метрикой) и выходным интерфейсом (вектором или направлением). Никакой дополнительной информации о маршрутах у маршрутизатора нет, поэтому он имеет ограниченное представление о ее структуре. Маршрутизаторы, использующие RIP периодически пересылают так называемые полные анонсы маршрутов, в которых перечислены все известные устройству сети. Такие анонсы по умолчанию происходят раз в 30 секунд, что довольно сильно нагружает низкоскоростные линии связи.

Когда в сети происходит какое-либо изменение, например, пропадает маршрут, то маршрутизатор, обнаруживший изменение, мгновенно пересылает триггерный анонс маршрутизации, содержащий только измененную информацию (частичный анонс), а именно — откорректированный маршрут с так называемой «бесконечной» метрикой. Максимальная метрика (количество транзитных устройств или хопов) для протокола RIP – 15, поэтому в частичных анонсах используется метрика, равная 16, что определяется процессом RIP как «бесконечная». Другие маршрутизаторы в сети тоже рассылают такие анонсы, корректируя свою таблицу маршрутизации.

Протокол RIP работает на 7 уровне (уровень приложений) стека TCP/IP, используя UDP порт 520. В современных сетевых средах RIP — не самое лучшее решение для выбора в качестве протокола маршрутизации, так как его возможности уступают более современным протоколам, таким как EIGRP и OSPF. Ограничение на 15 хопов не дает применять его в больших сетях. Основным преимуществом данного протокола является простота конфигурации.

### Link-state протокол OSPF

При использовании протокола OSPF маршрутизаторы рассылают очень подробную информацию о топологии сети друг другу. Такой процесс называется лавинной рассылкой (flooding), и когда он завершается, у всех маршрутизаторов в домене маршрутизации есть одинаковая информация о сети. Маршрутизаторы используют такую информацию, хранящуюся в оперативной памяти в виде некоторой структуры, называемой базой данных состояния каналов (link-state database — LSDB), для расчета наиболее оптимального маршрута к каждой известной им подсети. Лавинная рассылка создает повышенную нагрузку на устройства, поэтому протокол OSPF более требователен к вычислительным ресурсам, чем протоколы RIP и EIGRP.

Протокол OSPF анонсирует маршруты с помощью большого числа разнообразных сообщений, которые обобщенно называются анонсами состояния каналов (link-state advertisements — LSA). Существует много типов анонсов LSA, и их можно разделить на два больших класса:

* анонсы LSA маршрутизаторов (router LSA) - содержат некоторое число-идентификатор маршрутизатора (router ID), IP-адреса интерфейса маршрутизатора и маски, состояние каждого интерфейса и стоимость маршрута через интерфейс;
* анонсы LSA каналов (link LSA) идентифицируют каждый канал (или подсеть) и маршрутизаторы, подключенные к такому каналу. В них также содержится информация о состоянии канала.

После того как LSA-анонсы были лавинообразно разосланы, даже если в сети ничего не меняется, анонсы периодически пересылаются повторно, что очень похоже на принцип работы дистанционно-векторных протоколов маршрутизации. Однако, в отличии от протокола RIP, который рассылает анонсы раз в 30 секунд, протокол OSFP рассылает повторно LSA-анонсы по отдельности в соответствии с отдельным таймером для каждого анонса один раз в 30 минут. В результате в стабильно работающей сети протокол OSPF загружает намного меньшую полосу пропускания, чем протокол RIP. Если что-то в записи LSA меняется, то анонс рассылается мгновенно.

На следующем этапе используется другая не менее важная технология: установка маршрутов в таблицу IP-маршрутизации, в частности создание записей, содержащих адрес подсети, маску, выходной интерфейс и адрес следующего транзит­ного устройства (next-hop). Чтобы выполнить такую задачу, используется алгоритм поиска первого кратчайшего пути Дейкстры (Dijkstra Shortest Path First — SPF).

В протоколе OSPF необходимо уникальным образом идентифицировать каждый маршрутизатор. OSPF-маршрутизатору нужен некоторый идентификатор, чтобы определить, какое именно устройство переслало OSPF-сообщение. Такой идентификатор называют идентификатором маршрутизатора (router ID — RID). В протоколе OSPF идентификаторы представляют собой 32-битовые номера, записанные в точечно-десятичном формате, поэтому в качестве идентификатора удобно использовать IP-адрес, обычно это адрес loopback-интерфейса, иначе называемый адресом интерфейса обратной петли.

Если сеть состоит из большого количества устройств (более 50 маршрутизаторов) или большого количества подсетей (более 100), то рекомендуется использовать механизм разделения сети на логические зоны (area). Он позволяет маршрутизаторам хранить в своей памяти только информацию об устройствах из своей зоны, а также уменьшает нагрузку на вычислительные ресурсы, поскольку алгоритм поиска первого кратчайшего пути Дейкстры анализирует меньшую базу LSDB.

### Сбалансированный гибридный протокол EIGRP

В протоколе EIGRP существует три основных этапа работы.

* обнаружение соседних устройств – EIGRP-маршрутизаторы рассылают Hello-сообщения, чтобы обнаружить соседние маршрутизаторы и проверить их основные конфигурационные параметры;
* обмен топологической информацией – соседние (часто называемые смежными) устройства обмениваются полной информацией о топологии сети при включении, а впоследствии пересылают друг другу только частичные анонсы, содержащие информацию об изменениях в сетевой топологии;
* выбор оптимальных маршрутов – каждый EIGRP-маршрутизатор анализирует топологическую таблицу и выбирает из нее маршруты с наименьшей метрикой к каждой подсети.

Обновления маршрутов пересылаются посредством надежного транспортного протокола (Reliable Transport Protocol — RTP). Самая важная функция этого протокола (как и в протоколе маршрутизации OSPF) — повторная пересылка маршрутной информации, если сообщение было потеряно. За счет использования механизма RTP в протоколе EIGRP уменьшается вероятность возникновения кольцевых маршрутов.

В EIGRP отсутствует механизм логического разбиения сети на зоны, поэтому в больших сетях предпочтительнее использовать OSPF, однако в средних и малых сетях протокол EIGRP выигрывает у OSPF из-за меньшей загрузки на вычислительные ресурсы, а также из-за более быстрого процесса конвергенции, хотя в OSPF данный процесс тоже проходит достаточно быстро. Главным минусом протокола EIGRP является то, что он является проприетарной разработкой компании Cisco, поэтому использовать данный протокол в сетях с устройствами от других производителей нельзя.

**Примечание**. Описание процессов моделирования для этой лабораторной работы можно найти в справке Packet Tracer: Справка ⇒ Содержимое ⇒ раздел «Моделирование» ⇒ Лаб. работа №7.

## Методические указания

В качестве исходных данных для выполнения данных будет использоваться сеть из прошлой лабораторной работы. Прежде чем приступить к настройке протоколов динамической маршрутизации, требуется заменить имеющиеся маршрутизаторы и связи между ними:

1. Удалите имеющиеся маршрутизаторы из логического рабочего пространства и добавьте три новых маршрутизатора Router-PT-Empty и один сервер.
2. В первые два маршрутизатора необходимо добавить следующие модули: PT-ROUTER-NM-1CFE для связей с сетями филиалов по Fast Ethernet, один модуль PT-ROUTER-NM-1FFE для волоконно-оптической связи по Fast Ethernet, и один модуль PT-ROUTER-NM-1FGE для волоконно-оптической связи по Gigabit Ethernet.
3. В третий маршрутизатор добавьте один модуль PT-ROUTER-NM-1CFE и два модуля PT-ROUTER-NM-1FGE.
4. Соедините маршрутизаторы с сетями филиалов, а также друг с другом, настройте IP-адреса на интерфейсах так, как показано на (используйте маску 255.255.255.0):

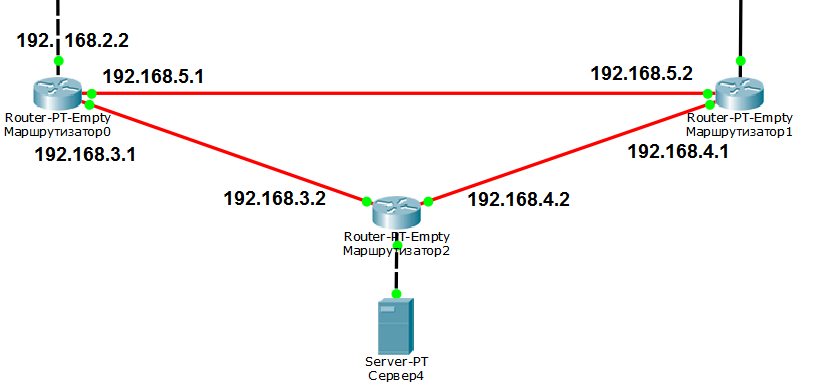


Рис. .. Расположение и связи между маршрутизаторами

Связь между Маршрутизатор0 и Маршрутизатор1 должна быть организована по Fast Ethernet, а связи с Маршрутизатор2 по Gigabit Ethernet. Это важно, т.к. в дальнейшем будет производиться проверка выбора оптимальных маршрутов разным протоколами динамической маршрутизации.

1. На Маршрутизатор1 должны быть настроены подинтерфейсы точно также, как это было сделано в предыдущей лабораторной работе. Не забудьте добавить ***ip helper-address*** на подинтерфейсах для правильной работы DHCP-сервера.
2. Установите IP-адрес на Сервер4 (192.168.6.2 с маской 255.255.255.0) и IP-адрес на интерфейсе Маршрутизатор2, который связан с этим сервером (192.168.6.1 с маской 255.255.255.0).
3. Последним шагом будет настройка loopback-интерфейсов на всех устройствах, которые будут участвовать в маршрутизации. Зайдите в CLI Многоуровневого коммутатор0 и из режима глобальной конфигурации введите команду ***interface lo0***. Затем присвойте этому интерфейсу IP-адрес 1.1.1.1 с маской 255.255.255.255. Таким же образом настройте loopback-интерфейсы на всех маршрутизаторах в сети. Маршрутизатор0 будет иметь IP-адрес 2.2.2.2, Маршрутизатор1 – адрес 3.3.3.3, а Маршрутизатор2 – адрес 4.4.4.4.

Теперь можно приступить к настройке протоколов динамической маршрутизации. Сохраните проект в текущем виде, в дальнейшем этот проект будет использоваться как исходный для настройки каждого из трех протоколов динамической маршрутизации.

### Динамическая маршрутизация по протоколу RIP

1. Зайдите в CLI Маршрутизатор0. В режиме глобальной конфигурации введите команду ***router rip***. Устройство перейдет в режим конфигурации протокола, об этом свидетельствует надпись «***(config-router)***» после имени устройства.
2. Введите команду ***version 2***. Это даст понять устройству, что будет использоваться вторая версия протокола. Первая версия RIP – устаревший протокол, который не поддерживает безклассовую адресацию, поэтому в данной лабораторной будет использоваться только RIP второй версии.
3. Теперь нужно перечислить все сети, на интерфейсах которых должен быть включен протокол RIP. Для Маршрутизатор0 такими сетями являются:

* Сеть 192.168.2.0, в которой находятся интерфейсы Маршрутизатор0 и Многоуровневого коммутатор0.
* Сеть 192.168.3.0, в которой находятся интерфейсы Маршрутизатор0 и Маршрутизатор2.
* Сеть 192.168.5.0, в которой находятся интерфейсы Маршрутизатор0 и Маршрутизатор1.

Перечислите эти сети с помощью команды ***network <адрес\_сети>***.

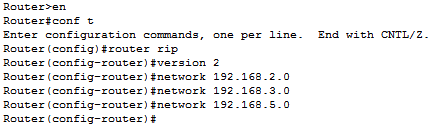


Рис. .. Настройка протокола RIP

1. Введите команду ***no auto-summary***. Это позволит выключить автоматическое суммирование маршрутов. Компания Cicso рекомендует использовать эту опцию, если в сети имеется деление на подсети с масками разной длины.

Далее следует повторить такую же настройку на оставшихся маршрутизаторах, а также на Многоуровневом коммутатор0, поскольку он также участвует в процессе маршрутизации. Отличаться будут только сети, которые перечисляются командой ***network <адрес\_сети>***. Ниже приведены конфигурации для этих устройств:

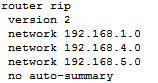


Рис. .. Конфигурация Маршрутизатор1

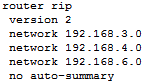


Рис. .. Конфигурация Маршрутизатор2

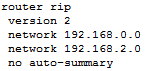


Рис. .. Конфигурация Многоуровневого коммутатор0

Обратите внимание, что сеть 192.168.1.0, хотя и разделена на подсети, для Маршрутизатоа1 указывается как сеть класса С. Это объясняется тем, что протокол RIP должен принимать именно классовую сеть в качестве аргумента для команды ***network***. Однако RIPv2 поддерживает безклассовую адресацию, поэтому при работе протокол автоматически определит количество подсетей. Теперь можно проанализировать таблицу маршрутизации. Зайдите в CLI Маршрутизатор0 и введите команду ***show ip route***.

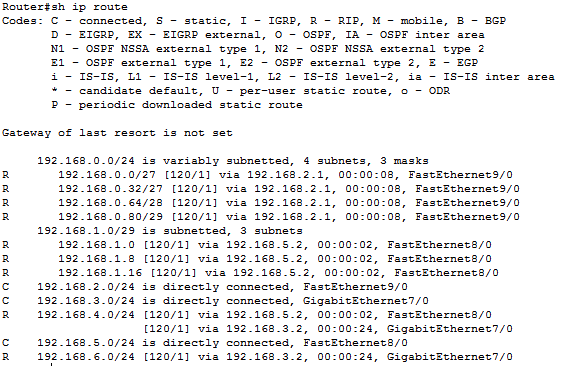


Рис. .. Вывод команды ***show ip route*** на Маршрутизаторе0

Как видно из таблицы маршрутизации, множество маршрутов получены с помощью протокола RIP (об этом свидетельствует буква «R» в начале записи). Буквой «C» обозначаются напрямую подключенные маршруты. В квадратных скобках указаны административное расстояние маршрута (120) и метрика маршрута (1), также указан интерфейс, через который следует пересылать данные по этому маршруту.

Теперь проверьте отказоустойчивость сети. Для этого зайдите на любой ПК из одного филиала (например, ПК3) и пошлите echo-запросы к ПК из другого филиала (например ПК7). В процессе следует выключить интерфейс, соединяющий Маршрутизатор0 и Маршрутизатор1 и посмотреть, как быстро произойдет конвергенция и восстановление связи. По умолчанию, команда ***ping*** ***<ip-адрес>*** отправляет только 4 echo-запроса, поэтому для проверки отказоустойчивости удобнее использовать расширенную версию команды: ***ping <ip-адрес> -n <количество\_запросов>***. Введите такую команду на ПК3, а затем выключите интерфейс, соединяющий Маршрутизатор0 и Маршрутизатор1.

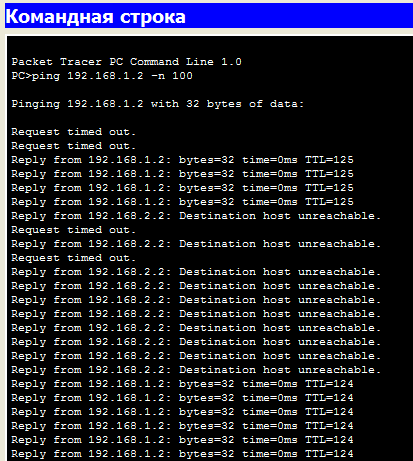


Рис. .. Проверка отказоустойчивости сети при включенном RIP

Время конвергенции у протокола RIP довольно большое, об этом свидетельствуют множество записей «Destination host unreachable». В конечном итоге связь все равно восстанавливается, только через другой маршрут. Чтобы это проверить, еще раз проанализируйте таблицу маршрутизации на Маршрутизатор0. Если раньше сеть 192.168.1.0 была доступна через сеть 192.168.5.0, то теперь она доступна через 192.168.3.0 (обратите внимание, что метрика у такого маршрута равняется 2).



Рис. .. Вывод команды ***show ip route*** на Маршрутизатор0

### Динамическая маршрутизация по протоколу OSPF

1. Зайдите в CLI Маршрутизатора0. В режиме глобальной конфигурации введите команду ***router ospf 1***. Здесь «1» - идентификатор процесса OSPF. Одновременно могут работать сразу несколько процессов OSPF, однако в данной задаче это не требуется.
2. Перечислите все сети, на интерфейсах которых должен быть задействован протокол OSPF. Команда ***network*** в протоколе OSPF имеет следующий вид: ***network <адрес\_сети> <инвертированная\_маска> area <номер\_зоны>***.

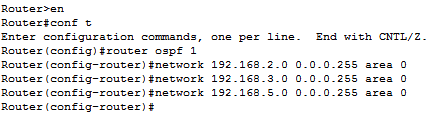


Рис. .. Настройка протокола OSPF на Маршрутизатор0

1. Аналогично настройте протокол OSPF на всех маршрутизаторах в сети, а также на Многоуровневом коммутатор0. Обратите внимание, что идентификатор процесса OSPF и номер зоны должны быть одинаковыми для всех устройств. Стоит отметить, что команда ***no auto-summary*** недоступна для протокола OSPF т.к. этот протокол работает по алгоритму учета состояния каналов.
2. Теперь можно протестировать работу протокола. Зайдите в режим симуляции и создайте echo-запрос от ПК3 до ПК7. Проследите, по какому маршруту передаются данные. Он будет проходить от Маршрутизатор0 к Маршрутизатор1.

В силу того, что OSPF – протокол с учетом состояния каналов, было бы логично предположить, что оптимальным маршрутом будет маршрут через Маршрутизатор2, потому что пропускная способность на каналах связи между Маршрутизатор2 и другими маршрутизаторами в 10 раз больше (Gigabit Ethernet), чем пропускная способность канала между Маршрутизатор0 и Маршрутизатор1 (Fast Ethernet). Для того, чтобы понять, почему в качестве оптимального маршрута выступает сегмент с меньшей пропускной способностью, нужно в CLI Маршрутизатор0 ввести команду ***show ip ospf interface***. На показан вывод этой команды, из которого следует, что параметр «cost» (стоимость) для интерфейсов Fast Ethernet и Gigabit Ethernet совпадают.

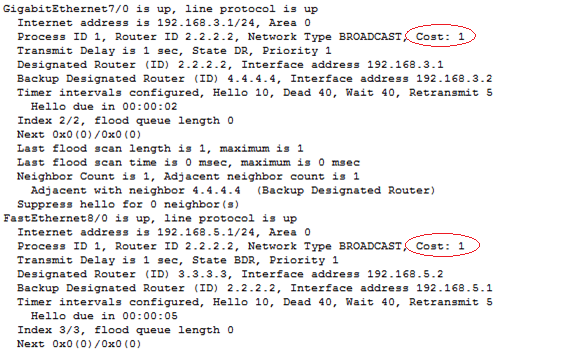


Рис. .. Вывод команды ***show ip ospf interface*** на Маршрутизатор0

Параметр «cost» рассчитывается по следующей формуле:

**Исходная полоса пропускания / Полоса пропускания интерфейса**

Исходная полоса пропускания по умолчанию равна 100, что означает 100 Мбит/с, а полоса пропускания интерфейса берется из настроек интерфейса. При применении данной формулы к интерфейсу Gigabit Ethernet получается, что стоимость должна быть равна 0.1 (100/1000), однако в Cisco IOS параметр стоимости записывается как целое число, поэтому значение принимается как единица. Именно поэтому стандартные настройки для исходной полосы пропускания не подходят в сетях, в которых используется Gigabit Ethernet вместе с Fast Ethernet. Компания Cisco рекомендует поменять значение исходной полосы пропускания на устройстве. Для этого зайдите в режим конфигурации процесса OSPF (***router ospf 1***), а затем введите команду ***auto-cost reference-bandwidth 1000***, где «1000» - значение для исходной полосы пропускания. Введите данную команду на всех устройствах в сети, а затем еще раз посмотрите стоимости интерфейсов:

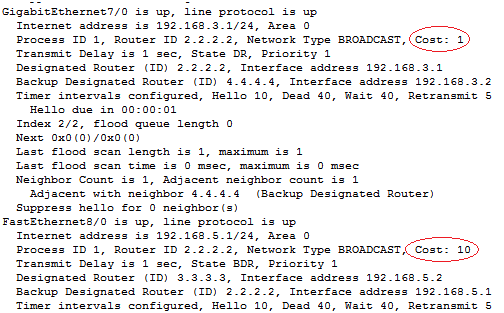


Рис. .. Вывод команды ***show ip ospf interface*** на Маршрутизатор0

Теперь оптимальный маршрут должен быть скорректирован, проверьте это в режиме симуляции. Также стоит провести проверку отказоустойчивости - выключите интерфейс, соединяющий Маршрутизатор2 и Маршрутизатор1 во время выполнения расширенной команды ***ping*** на ПК3:

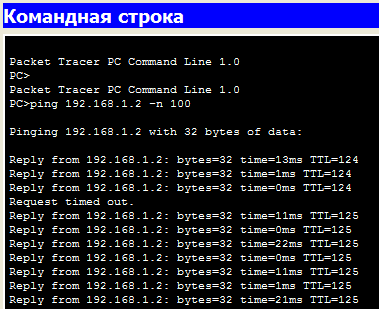


Рис. .. Проверка отказоустойчивости при включенном протоколе OSPF

Время конвергенции у протокола OSPF намного быстрее, чем у протокола RIP, об этом свидетельствует тот факт, что при проверке отказоустойчивости неудачно выполнился только один запрос.

Последним этапом станет настройка аутентификации для протокола OSPF. Отсутствие такой аутентификации на сегодняшний день является очень существенным недостатком, поскольку может привести к проблемам с безопасностью и работоспособностью сети, когда злоумышленник, например, перехватывает чужие маршруты и анонсирует неправильные маршруты какому-либо маршрутизатору. В протоколе OSPF есть три типа аутентификации: один из них называют null-аутентификацией («без аутентификации»); во втором используется простой текстовый пароль, который легко взламывается; в третьем типе аутентификации пароль зашифровывается с помощью хеша MD5, это делает его самым надежным выбором из перечисленных. Для включения аутентификации с помощью хэша MD5 на каком-либо интерфейсе, нужно последовательно выполнить следующие действия:

1. Включить аутентификацию командой ***ip ospf authentication message-digest***.
2. Указать ключ и его идентификатор при помощи команды ***ip ospf message-digest-key <идентификатор\_ключа> md5 <ключ>***.

Данные команды работают только на маршрутизаторах, на коммутаторах третьего уровня аутентификация не поддерживается, поэтому эти настройки следует ввести только на тех интерфейсах маршрутизаторов, которые имеют линии связи между собой. Важно, чтобы идентификатор ключа и сам ключ совпадали на обоих концах линии связи.

1. Проверьте работу аутентификации с помощью команды ***show ip ospf interface***. В выводе этой команды должны присутствовать следующие строчки: «***Message digest authentication enabled***», а затем ***«Youngest key id is 1»***. Они указывают на то, что на интерфейсе включена аутентификация с помощью хэша MD5.

### Динамическая маршрутизация по протоколу EIGRP

1. Зайдите в CLI Маршрутизатора0. В режиме глобальной конфигурации введите команду ***router eigrp 1***. Как и в OSPF, «1» - это идентификатор процесса.
2. Команды конфигурации EIGRP очень похожи на команды конфигурации OSPF, однако в EIGRP нет поддержки логического разбиения на зоны, поэтому команда network принимает следующий вид: ***network <адрес\_сети> <инвертированная\_маска>***. С помощью этой команды перечислите все сети, на интерфейсах которых должен быть задействован протокол EIGRP.
3. Отключите автосуммирование маршрутов командой ***no auto-summary***.
4. Повторите данные действия на оставшихся маршрутизаторах, а также на Многоуровневом коммутатор0.

Стоит отметить, что после завершения всех настроек оптимальный путь от сети первого филиала до сети второго будет проходить через Маршрутизатор2, т.е EIGRP автоматически просчитывает правильные метрики даже для маршрутов с высокоскоростными интерфейсами Gigabit Ethernet. Проверьте отказоустойчивость протокола по способу, описанному ранее.

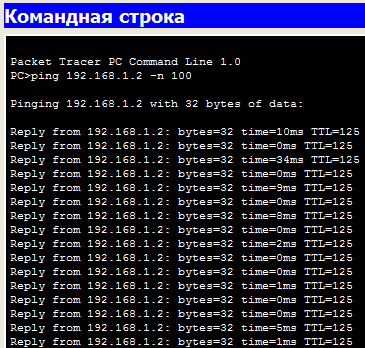


Рис. .. Проверка отказоустойчивости при включенном протоколе EIGRP

Время конвергенции протокола EIGRP в данной сети еще быстрее, чем при использовании OSPF, при проверке не было ни одного неудачно выполненного запроса. Настройка аутентификация для протокола EIGRP выполняется следующим образом:

1. С помощью команды ***key chain <название\_цепочки>*** в режиме глобальной конфигурации устройства создайте цепочку ключей (эта команда переводит CLI в режим конфигурирования цепочки).
2. Укажите идентификатор ключа с помощью команды ***key <идентификатор>***, эта команда также переводит CLI в режим конфигурирования ключа.
3. Задайте ключ (т.е. пароль) для аутентификации командой ***key-string*** **<значение>** в режиме конфигурирования ключа.
4. Включите MD5-аутентификацию для протокола EIGRP на интерфейсе для определенного номера автономной системы (ASN) с помощью команды ***ip authentication mode eigrp <номер-АС> md5*** в режиме конфигу­рирования интерфейса.
5. Привяжите правильную цепочку ключей к интерфейсу. Для этого перейдите в режим конфигурирования интерфейса и введите команду ***ip authentication key-chain eigrp <номер-АС>*** <***назва­ние\_цепочки>***.
6. Повторите эти действия на всех интерфейсах маршрутизаторов, которые учавствуют в динамической маршрутизации (коммутаторы третьего уровня не поддерживают аутентификацию). Обратите внимание, что идентификатор ключа и сам ключ должны совпадать на обоих концах линии связи.

На показан процесс настройки аутентификации для протокола EIGRP на Маршрутизатор0.

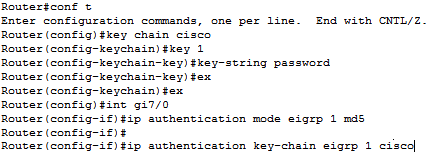


Рис. .. Настройка аутентификации для протокола EIGRP

## Заключение

В настоящее время трудно представить сеть, в которой бы использовалась только статическая маршрутизация. Такие сети не обладают отказоустойчивостью, и вынуждают сетевых инженеров каждый раз редактировать таблицы маршрутизации на устройствах при любом изменении топологии сети. Динамическая маршрутизация решает проблему отказоустойчивости, а также позволяет маршрутизаторам автоматически добавлять новые маршруты и искать оптимальные. Навыки настройки динамической маршрутизации для различных протоколов гарантированно пригодятся любому сетевому инженеру, например, для маленьких сетей достаточно использовать простой в конфигурировании протокол RIP, для средних и больших сетей предпочтительнее использовать OSPF, так как он поддерживает технологию логического разбиения сети на зоны и обладает быстрым временем конвергенции. Наконец, в сетях, состоящих только из оборудования Cisco выгоднее всего использовать протокол EIGRP, так как он сочетает в себе быстрое время конвергенции от протокола OSPF и относительную простоту конфигурации от протокола RIP. Однако, при использовании динамической маршрутизации сеть становится менее предсказуемой, поэтому сетевой инженер также должен обладать некоторым уровнем знаний, который бы позволил ему выявлять и решать проблемы, возникающие при неправильной работе протоколов.

## Контрольные задания

1. Модифицировать задание №1 из Лабораторной работы №6. Заменить статическую маршрутизацию на динамическую маршрутизацию по протоколу RIP
2. Модифицировать задание №2 из Лабораторной работы №6. Заменить статическую маршрутизацию на динамическую маршрутизацию по протоколу EIGRP, а также включить аутентификацию с помощью хэша MD5.
3. Модифицировать задание №3 из Лабораторной работы №6. Заменить статическую маршрутизацию на динамическую маршрутизацию по протоколу OSPF, а также включить аутентификацию с помощью хэша MD5.
4. Модифицировать задание №4 из Лабораторной работы №6. Заменить статическую маршрутизацию на динамическую маршрутизацию по протоколу OSPF, а также включить аутентификацию с помощью хэша MD5.

# механизм трансляции сетевых адресов nat

## Цели и задачи

Целью данной лабораторной работы является получение навыков по соединению локальных сетей с глобальной сетью Интернет. Для этого предлагается изучить основы конфигурирования механизма трансляции сетевых адресов NAT на оборудовании Cisco.

В процессе выполнения работы будут решаться следующие задачи:

* изучение применения частной и публичной сетевой адресации;
* изучение базовых принципов использования трансляции NAT;
* изучение экономного расходования адресного пространства протокола IPv4;
* настройка нескольких вариантов NAT – статического, динамического, а также перегруженного (PAT).

## Теоретические сведения

При первоначальном проектировании сети Интернет предполагалось, что каждая организация запрашивает и получает один или несколько зарегистрированных классовых сетевых IP-номеров (адресов). Администраторы следили за тем, чтобы ни один из адресов IP-сетей не дублировался. До тех пор, пока каждая организация использовала только IP-адреса в зарегистрированном номере сети, IР-адреса не дублировались, и IP-маршрутизация работала без проблем. В течение определенного периода подсоединение к Интернету только через один или несколько зарегистрированных сетевых номеров функционировало благополучно.

Однако уже в начале 1990-х годов стало очевидно, что сеть Интернет растет столь быстро, что уже к середине 1990-х годов все номера IP-сетей будут исчерпаны (назначены). Возникли опасения, что доступные номера сетей будут полностью исчерпаны и некоторые организации уже не смогут подключиться к Интернету. Главным долгосрочным решением проблемы масштабируемости IP-адресов могло бы стать только увеличение размера IP-адреса. Один этот факт был наиболее существенной предпосылкой появления версии 6 протокола IP (IPv6). В протоколе IPv6 используется 128-битовый адрес вместо 32-битового в IPv4. Используя прежний или улучшенный процесс назначения уникальных диапазонов адресов каждой организации, подключенной к Интернету, протокол IPv6 может без проблем обеспечивать доступ к Интернету всех организаций и отдельных пользователей планеты.

Краткосрочным решением проблемы масштабируемости IP-адресов стал механизм трансляции сетевых адресов NAT (Network Adress Translation). Для того чтобы понять основную функцию этого механизма, необходимо рассмотреть такое понятие как частная адресация. Некоторые компьютеры, вероятно, никогда не будут подсоединяться к сети Интернет. IP-адреса этих компьютеров могут быть дубликатами зарегистрированных IP-адресов в Интернете. При проектировании IP-адресации для такой сети организация может выбрать и использовать произвольные сетевые адреса, но только если они используются для внутренних целей офиса. Существуют специальные группы IP-адресов, которые предназначены только для использования внутри локальных сетей организаций. Список этих адресов приведен ниже ().

Таблица .. Диапазоны адресов частных интрасетей

|  |  |  |
| --- | --- | --- |
| Диапазон IP-адресов | Класс сети | Количество сетей |
| 10.0.0.0-10.255.255.255 | A | 1 |
| 172.16.0.0-172.16.255.255 | B | 16 |
| 192.168.0.0-192.168.255.255 | C | 256 |

Таким образом, если сеть использует для адресации какие-либо IP-адреса из этой таблицы, то такая сеть является частной интрасетью. Главным недостатком таких сетей является невозможность подключения к глобальной сети Интернет, и именно эту проблему успешно решает механизм трансляции сетевых адресов NAT.

Трансляция адресов заключается в том, что есть некоторое NAT-устройство, например, сервер или маршрутизатор, который имеет один или несколько публичных адресов. Клиенты с частными адресами пытаются отправить запросы напрямую получателю в сети Интернет, но все данные по пути попадают на такое NAT-устройство, а затем оно заменяет адрес отправителя: вместо частного адреса клиента, устройство ставит в это поле один из своих публичных адресов, после чего данные отправляется в сеть. Таким образом, на выходе с NAT-устройства во всех пакетах стоит публичный адрес отправителя и публичный адрес получателя. На обратном пути публичный адрес заменяется на частный, и клиент успешно получает данные, не зная о преобразовании IP-адресов.

В процессе трансляции сетевых адресов могут применяется 4 разных адреса, обозначаемые разными терминами ().

Таблица .. Типы сетевых адресов в NAT

|  |  |
| --- | --- |
| Термин | Определение |
| Внутренний локальный адрес (Inside local), также называемый «внутренний частный». | При типичном проектировании NAT термин «внутренний» относится к адресу, используемому для узла на предприятии. Внутренним локальным называется действующий IP-адрес, назначенный узлу в частной сети предприятия. |
| Внутренний глобальный адрес (Inside global), также называемый «внутренний публичный» | Трансляция NAT использует внутренний глобальный адрес для представления внутреннего узла, когда пакет пересылается через внешнюю сеть, обычно через сеть Интернет. |
| Внешний глобальный адрес (Outside global), также называемый «внешний публичный» | Термин «внешний» относится к адресу, используемому для узла вне предприятия. Внешний глобальный адрес представляет собой реальный IP-адрес, назначенный узлу, который находится в сети Интернет. |
| Внешний локальный адрес (Outside local), также называемый «внешний частный» | NAT может транслировать внешние IP-адреса, т.е. IP-адреса, представляющие узел вне сети предприятия, хотя эта опция не очень популярна. Когда NAT-устройство пересылает пакет из внутренней сети во внешнюю, используя NAT для изменения внешнего адреса, IР-адрес, представляющий внешний узел в качестве IP-адреса получателя в заголовке пакета, называется внешним локальным IP-адресом. |

Всё вышеперечисленное является общими принципами работы NAT. Однако существуют разные способы организации этого процесса:

* **Статический NAT** – на NAT-устройстве организована трансляция одного конкретного внутреннего локального адреса в один конкретный внутренний глобальный адрес. Необходимо иметь публичный зарегистрированный IP-адрес для каждого узла в сети, которому нужен доступ в Интернет, поэтому такой способ не позволяет экономить адресное пространство IPv4. Такой тип NAT часто используется для серверов, на которых установлен статический IP-адрес. Кроме того, при использовании этого типа трансляции обеспечивается доступ из внешней сети.
* **Динамическая трансляция NAT** – на NAT-устройстве имеется пул свободных внутренних глобальных адресов, и конфигурация позволяет клиентам из некоего множества внутренних локальных адресов проходить трансляцию. В этом случае для очередного клиента изнутри в пуле выбирается очередной свободный адрес и происходит трансляция. Стоит отметить, что пул свободных внутренних глобальных адресов может быть меньше, чем количество узлов, которым необходим доступ в Интернет. Однако одновременно получить доступ в Интернет могут ровно столько устройств, сколько адресов имеется в пуле, поэтому этот способ позволяет лишь частично экономить адресное пространство IPv4.
* **Перегруженный NAT (PAT)** – это механизм NAT, затрагивающий не только третий, но и четвёртый уровень модели OSI. Используется, когда количество клиентов превышает размер пула внутренних глобальных адресов. В этом случае клиенты могут транслироваться на один и тот же внутренний глобальный адрес, однако при этом изменяется номер порта (TCP или UDP). PAT позволяет значительно сэкономить адресное пространство и является самым популярным способом организации NAT, однако он также вносит дополнительные ограничения на перечень работающих протоколов.

**Примечание**. Описание процессов моделирования для этой лабораторной работы можно найти в справке Packet Tracer: Справка ⇒ Содержимое ⇒ раздел «Моделирование» ⇒ Лаб. работа №8.

## Методические указания

Так как в программе Cisco Packet Tracer нет возможности подключать устройства к сети Интернет, для проверки настроек трансляции сетевых адресов будет использоваться отдельный маршрутизатор (устройство провайдера) и сервер, которые будут иметь публичные адреса. В качестве исходной будет использоваться сеть из предыдущей лабораторной работы (сеть с динамической маршрутизацией по EIGRP). Прежде чем приступить к настройке NAT, последовательно выполните следующие действия:

1. Добавьте новый маршрутизатор Router-PT-Empty между устройствами Маршрутизатор2 и Сервер4. Он будет играть роль маршрутизатора провайдера.
2. Установите на этот маршрутизатор модули PT-ROUTER-NM-1FGE и PT-ROUTER-NM-1CFE
3. Установите модуль PT-ROUTER-NM-1FGE в Маршрутизатор2. Таким образом Маршрутизатор2 должен иметь три волоконно-оптических интерфейса Gigabit Ethernet.
4. Соедините Маршрутизатор2 с Маршрутизатором3 волоконно-оптическим кабелем, а Маршрутизатор3 и Сервер4 – кабелем типа «медный перекрестный».
5. Для наглядности обозначьте границу перехода от частной сети к глобальной. Добавьте облако Cloud-PT-Emtpy и поместите его между Маршрутизатор2 и Маршрутизатор3.

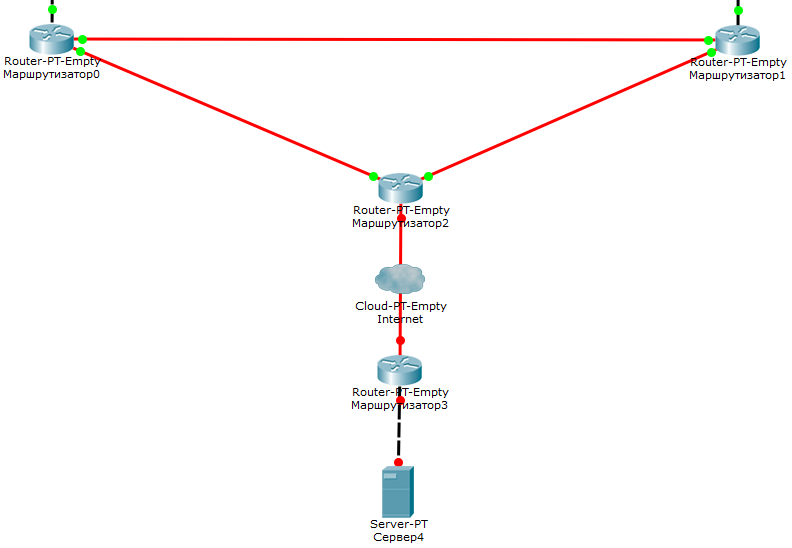


Рис. .. Симуляция сети Интернет

Теперь необходимо настроить IP-адреса для устройств Маршрутизатор3 и Сервер4, указать внутренний глобальный адрес для сети компании на устройстве Маршрутизатор2 и добавить его в таблицу маршрутизации:

1. Назначьте интерфейсам устройства Маршрутизатор3 публичные адреса (Например, 109.172.10.2 с маской 255.255.255.0 интерфейсу, который связывает Маршрутизатор3 и Маршрутизатор2, и 109.172.20.1 с маской 255.255.255.0 интерфейсу, который связывает Маршрутизатор3 и Сервер4).
2. Укажите на Сервер4 соответствующие предыдущим настройкам IP-адрес (109.172.20.2), маску подсети (255.255.255.0) и основной шлюз (109.172.20.1).
3. Назначьте публичный IP-адрес интерфейсу Маршрутизатора2, который связывает Маршрутизатор2 и Маршрутизатор3 (например, 109.172.10.1 с маской 255.255.255.0).
4. Теперь необходимо добавить маршрут по умолчанию для Маршрутизатора2. Логично, что это будет маршрут к интерфейсу Маршрутизатора3. В режиме глобальной конфигурации введите ***ip route 0.0.0.0 0.0.0.0 109.172.10.2***. Таким образом, весь трафик, для которого нет маршрутов, будет автоматически посылаться на интерфейс с адресом 109.172.10.2.
5. Из режима глобального конфигурирования устройства Маршрутизатор2 зайдите в режим конфигурирования EIGRP с помощью команды ***router eigrp 1***.
6. Введите команду ***no network 192.168.6.0***, удаляя неиспользуемую сеть 192.168.6.0 из динамической маршрутизации EIGRP.
7. Протокол EIGRP (а также RIP и OSPF) могут распространять маршруты по умолчанию. Это очень полезная функция, так как всего лишь с помощью одной команды можно распространить маршрут по умолчанию до интерфейса 109.172.10.2 на все устройства, в которых работает протокол динамической маршрутизации. Введите команду ***redistribute static*** из режима конфигурирования протокола EIGRP, а затем посмотрите таблицы маршрутизации на Маршрутизатор0 и Маршрутизатор1. Вы должны увидеть следующий маршрут ():

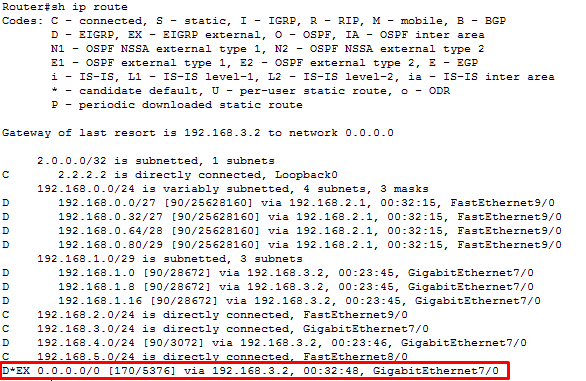


Рис. .. Маршрут по умолчанию, распространенный с помощью EIGRP

Далее следует приступить к настройке трансляции сетевых адресов.

### Конфигурирование статической трансляции NAT

1. На Маршрутизатор2 зайдите в режим конфигурирования интерфейса с внутренним глобальным адресом (109.172.10.1).
2. Обозначьте роль данного интерфейса с помощью команды ***ip nat outside***. Эта команда указывает, что данный интерфейс находится во внешней части схемы NAT.
3. Выполните команду ***ip nat inside*** на внутренних интерфейсах данного маршрутизатора (они соединяют Маршрутизатор2 с маршрутизаторами 0 и 1). Эта команда указывает, что интерфейсы находятся во внутренней части схемы NAT.
4. В режиме глобальной конфигурации настройте статическое преобразование с помощью команды ***ip nat inside source static <внутренний\_локальный\_адрес><внутренний\_глобальный\_адрес>***. Статическое преобразование часто используется для того, чтобы из внешней сети появился доступ к серверам, расположенным внутри закрытой локальной сети. В двух филиалах компании расположено 4 сервера, поэтому для каждого из них необходимо настроить NAT. Для этого выполните следующие команды:

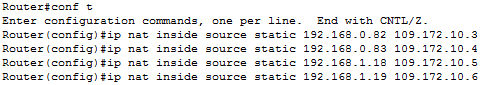


Рис. .. Настройка статической трансляции NAT

1. Зайдите на Сервер4 и попробуйте послать echo-запросы на внутренние сервера компании, однако в команде ***ping*** указывайте внутренние глобальные адреса.
2. В ходе выполнения echo-запросов на Маршрутизаторе2 выполните команду ***show ip nat translations***.

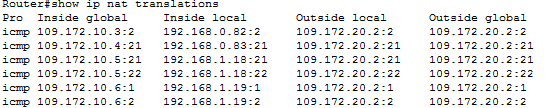


Рис. .. Вывод команды ***show ip nat translations*** на Маршрутизаторе2

1. Зайдите в режим симуляции и отправьте простой PDU из Сервер0 на Сервер4. Проследите путь PDU до Маршрутизатор2. Нажмите на PDU в тот момент, когда он будет находиться на Маршрутизатор2. Откроется окно «Информация о PDU на устройстве: Маршрутизатор2». Перейдите на вкладку «Детали входящего PDU» и посмотрите адрес источника в поле SRC\_IP, он должен быть внутренним локальным.



Рис. .. Содержимое PDU при входе на интерфейс Маршрутизатор2

1. Перейдите на вкладку «Детали исходящего PDU» и посмотрите поле SRC\_IP, адрес должен быть уже внутренним глобальным.

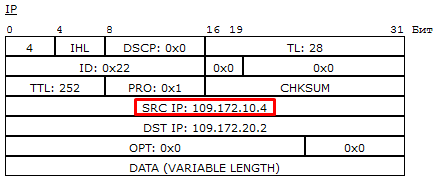


Рис. .. Содержимое PDU на выходе из Маршрутизатор2

Таким образом настраивается статическая трансляция сетевых адресов. Такой способ организации NAT является самым простым в конфигурации, однако он не экономит адресное пространство IPv4. Следующим шагом будет настройка динамической трансляции сетевых адресов, этот способ позволяет частично сэкономить адресное пространство IPv4, но также является более трудным в конфигурации.

### Конфигурирование динамической трансляции NAT

1. Удалите имеющееся статическое транслирование на устройстве Маршрутизатор2 с помощью следующих команд:

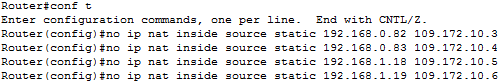


Рис. .. Удаление статической трансляции сетевых адресов

Роли интерфейсов (***ip nat inside*** и ***ip nat outside***) удалять не нужно, потому что они требуются для любого способа организации NAT.

1. Сконфигурируйте список доступа, в котором будут перечислены все IP-адреса, для которых требуется трансляция NAT:

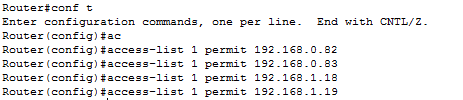


Рис. .. Создание стандартного списка доступа

1. Создайте пул внутренних глобальных IP-адресов командой ***ip nat pool <имя\_пула> <первый\_адрес\_пула> <последний\_адрес\_пула> netmask <маска>***. Адресов в пуле может быть меньше, чем адресов в списке доступа, но тогда одновременно выход во внешнюю сеть получат только те узлы, которые успели получить свободные внутренние глобальные адреса, для остальных доступ будет закрыт. Для выделения пула из четырех адресов с именем «servers» и маской 255.255.255.0 введите следующую команду: ***ip nat pool servers 109.172.10.3 109.172.10.6 netmask 255.255.255.0***.
2. Включите динамическую трансляцию NAT. Для этого из режима глобальной конфигурации введите команду ***ip nat inside source list 1 pool servers***, где «1» – номер списка доступа, а «servers***»*** – имя пула внутренних глобальных адресов.
3. Проверьте работу динамической трансляции сетевых адресов с помощью echo-запросов от серверов компании до Сервер4.

Завершающим этапом будет настройка трансляции сетевых адресов по способу перегруженного NAT (PAT), который является самым популярным способом организации NAT и может существенно сэкономить адресное пространство IPv4, при этом обеспечивая доступ во внешнюю сеть для большого количества устройств.

### Конфигурирование перегруженного NAT (PAT)

1. Отмените все предыдущие команды по настройке динамической трансляции сетевых адресов (повторите все команды настроек, вводя перед ними ключевое слово ***no***). Оставить следует только команды ***ip nat inside*** и ***ip nat outside***.
2. PAT может обеспечить доступ во внешнюю сеть 65-ти тысячам устройств имея при этом всего один внутренний глобальный адрес. В текущей локальной сети двух филиалов устройств гораздо меньше, поэтому можно попробовать обеспечить доступом в интернет их все. Для этого создайте список доступа с одним простым правилом: ***access-list 1 permit any***.
3. Включите PAT с помощью следующей команды глобальной конфигурации: ***ip nat inside source list 1 int gi9/0 overload***, где «1» - номер списка доступа, «gi9/0» - интерфейс, соединяющий Маршрутизатор2 и Маршрутизатор3 и имеющий внутренний глобальный IP-адрес, а ключевое слово overload – указание на то, что включается перегрузка NAT.
4. Проверьте работу PAT, посылая echo-запросы от различных устройств в локальной сети до Сервер4, а также посмотрите список трансляций с помощью команды ***show ip nat translations***.

## Заключение

Трансляция сетевых адресов NAT позволяет обеспечить доступом Интернет локальные сети предприятий, а также обладает рядом преимуществ:

* минимизация использования публичных адресов;
* повышенная гибкость использования адресов;
* возможность изменения внешних адресов без необходимости изменять адресный план локальной сети;
* повышенная безопасность в связи с тем, что из сети Интернет нельзя обратиться к внутренним устройствам напрямую.

Также существуют некоторые недостатки при использовании NAT:

* уменьшение производительности в связи с дополнительными действиями на NAT-устройстве;
* проблемы с работой некоторых протоколов;
* сложности при организации туннелей.

Несмотря на то, что некоторые протоколы не работают через NAT, абсолютно все корпоративные сети, в которых нужен доступ в сеть Интернет, используют трансляцию сетевых адресов, поэтому навыки настройки различных видов NAT обязательно пригодятся любому сетевому специалисту.

## Контрольные задания

1. Модифицировать задание №1 из Лабораторной работы №7:

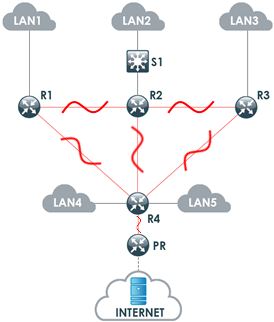


Рис. .. Схема сети задания №1

Реализовать эмуляцию сети интернет с помощью сервера и маршрутизатора провайдера (**PR**), настроить PAT на интерфейсе маршрутизатора R4 для LAN1, LAN2, LAN3. Из сетей LAN4 и LAN5 выбрать сервера, для которых сконфигурировать статический NAT.

1. Модифицировать задание №2 из Лабораторной работы №7:

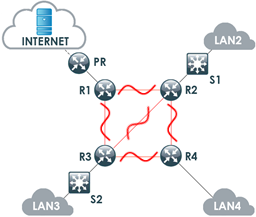


Рис. .. Схема сети задания №2

Вместо LAN1 из предыдущего задания, разместить сервер и маршрутизатора провайдера (**PR**), настроить PAT на интерфейсе маршрутизатора R1 для LAN2 и LAN3. Из сети LAN4 и выбрать группу узлов, для которых сконфигурировать динамический NAT.

1. Модифицировать задание №3 из Лабораторной работы №7:

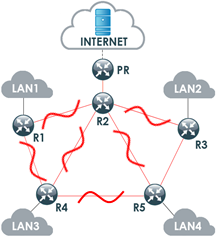


Рис. .. Схема сети задания №3

Реализовать эмуляцию сети интернет с помощью сервера и маршрутизатора провайдера (**PR**), настроить PAT на интерфейсе маршрутизатора R2 для LAN1 и LAN2. Из сетей LAN3 и LAN4 выбрать сервера, для которых сконфигурировать статический NAT, а также группу узлов, для которых сконфигурировать динамический NAT.

1. Модифицировать задание №4 из Лабораторной работы №7:

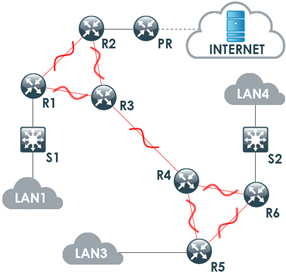


Рис. .. Схема сети задания №4

Вместо LAN2 из предыдущего задания, разместить сервер и маршрутизатора провайдера (**PR**), настроить PAT на интерфейсе маршрутизатора R2 для LAN1 и LAN4. Из сети LAN3 выбрать сервера, для которых сконфигурировать статический NAT.

## Легенда

| Термин | Описание |
| --- | --- |
|  | Локальная вычислительная сеть |
|  | Коммутатор третьего уровня |
|  | Маршрутизатор |
|  | Сервер, находящийся в сети Интернет, и имеющий публичный IP-адрес |
|  | Волоконно-оптический кабель |
|  | Кабель «Медный прямой» |
|  | Кабель «Медный перекрестный» |

# Распределенные сети. Технология Frame Relay.

## Цели и задачи

Основной целью данной лабораторной работы является изучение аспектов построения распределенных сетей на примере одной из популярных технологий - Frame Relay.

В процессе выполнения будут решаться следующие задачи:

* изучение терминологии и концепции Frame Relay;
* решение проблем адресации в среде Frame Relay на втором и третьем уровнях модели OSI;
* настройка маршрутизаторов Cisco на работу по технологии Frame Relay без использования подинтерфейсов;
* настройка маршрутизаторов Cisco на работу по технологии Frame Relay с использованием подинтерфейсов.

## Теоретические сведения

В предыдущих лабораторных работах были рассмотрены основные технологии, используемые при построении локальных вычислительных сетей. В данной лабораторной работе впервые вводится такое понятие как распределенная сеть, иначе называемая глобальной компьютерной сетью (Wide Area Network, WAN). Распределенная сеть охватывает большие территории и включает в себя множество узлов, объединяя локальные вычислительные сети так, чтобы каждый узел мог взаимодействовать с остальными участниками глобальной сети. Одной из наиболее распространенных WAN-технологий в современных сетях является среда Frame Relay.

Frame Relay (англ. «ретрансляция кадров») представляет собой набор WAN-стандартов, с помощью которых можно построить эффективные WAN-службы, в которых пары маршрутизаторов пересылают данные напрямую друг другу по логическим виртуальным каналам. Сети Frame Relay являются средами с многостанционным доступом, т.е. к соединению может быть подключено более двух устройств. В отличие от локальных сетей, в среде Frame Relay на канальном уровне нет широковещания, поэтому данную технологию также называют нешироковещательной средой с многостанционным доступом (nonbroadcast multiaccess — NBMA). Более того, поскольку среда Frame Relay является многостанционной, в ней нужно использовать некоторую разновидность адреса, чтобы идентифицировать удаленный маршрутизатор-получатель. На представлена физическая топология сети Frame Relay и связанная с ней терминология.

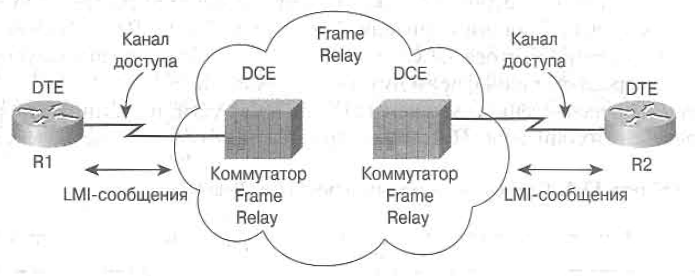


Рис. .. Компоненты сети Frame Relay

Между маршрутизаторами клиента (R1, R2) и коммутаторами Frame Relay провайдера услуги прокладывается выделенная линия, которую называют **каналом доступа** (access link). Для работы с такими каналами используются специальные интерфейсы на маршрутизаторах, называемые серийными или последовательными. Чтобы отслеживать работоспособность такого канала, устройства, не относящиеся к Frame Relay-сети провайдера, называемые терминальным оборудованием канала передачи данных (Data Terminal Equipment — DTE), периодически обмениваются служебными сообщениями с коммутатором Frame Relay. Такие тестовые сообщения (keepalive) вместе с другими служебными кадрами описаны в протоколе интерфейса локального управления (Local Management Interface — LMI). Маршрутизаторы с точки зрения технологии Frame Relay являются DTE-устройствами, а коммутаторы — DCE (Data Communications Equipment — коммуникационное оборудование канала передачи данных).

Следует отметить, что на показана физическая схема сети Frame Relay, а логическая схема будет выглядеть несколько по-другому. Логическая схема виртуальных каналов показана на .



Рис. .. Виртуальные каналы сети Frame Relay

Логический маршрут между двумя DTE-устройствами представляет собой виртуальный канал. Пунктирной линией на рисунке показан виртуальный канал, и в дальнейшем на рисунках используется именно такая линия для обозначения логических маршрутов. На также указаны идентификаторы соединения канального уров­ня (Data-Link Connection Identifier — DLCI) в качестве адреса в сети Frame Relay; с их помощью идентифицируют виртуальные каналы, по которым должны пересы­латься кадры. Идентификаторы DLCI являются локально значимыми, т.е. они должны быть уникальными только в локальном канале доступа к сети.

В табл. 9.1 перечислены компоненты Frame Relay-сети, показанные на рис. 9.1 и 9.2, а также приведено их описание:

Таблица . Терминология и концепции Frame Relay

|  |  |
| --- | --- |
| Термин | Описание |
| Виртуальный канал (Virtual Circuit — VC) | Логический канал, представляющий собой маршрут, по которому передаются кадры между DTE-устройствами. |
| Терминальное оборудование передачи данных (Data Terminal Equipment — DTE) | DTE-устройства представляют собой оборудование на стороне клиента услуги Frame Relay. Обычно размещаются на стороне пользователя. |
| Коммуникационное оборудование передачи данных (Data Communications Equipment — DCE) | DCE-устройства представляют собой оборудование на стороне провайдера услуги Frame Relay. В качестве таких устройств используются коммутаторы Frame Relay. |
| Идентификатор соединения канального уровня (Data-Link Connection Identifier — DLCI) | Адрес в технологии Frame Relay, используемый для идентификации виртуальных каналов |
| Нешироковещателъная среда с многостанционным доступом (Nonbroadcast Multiaccess — NBMA) | Сеть, в которой не рассылаются широковещательные кадры и пакеты, но в которой может быть больше двух устройств |
| Локальный интерфейс управления (Local Management Interface — LMI) | Протокол, используемый между DTE- и DCE-устройствами для управления соединением. |

В сети Frame Relay необязательно между всеми узлами сети попарно должны быть сконфигурированы виртуальные каналы. Топология, в которой все узлы соединены каналами называют **полносвязной** (связь все со всеми). Если не все пары устройств соединены между собой, то топологию называют **неполносвязной**. В неполносвязной сети есть свои преимущества и недостатки по сравнению с полносвязной топологией. Главное преимущество — такая топология дешевле, поскольку провайдер обычно взимает плату за каждый виртуальный канал по отдельности. Недостаток вполне очевиден: длина пути между отправителем и получателем может увеличится, на пути появятся дополнительные транзитные маршрутизаторы, которые будут вынуждены выполнять роль ретрансляторов. Если объем пересылаемых данных в сети невелик, то обычно используется неполносвязную топологию; если же данных передается много, то более дорогая полносвязная топология будет более эффективной.

Следует помнить о двух основных проблемах технологии Frame Relay:

* выбор правильной схемы IP-адресации для FR-интерфейсов;
* обработка широковещательных сообщений.

В реализации технологии Frame Relay от компании Cisco есть три варианта разбивки подсетей и IP-адресов для Frame Relay-интерфейсов:

1. Одна подсеть для всех DTE-устройств. Сеть с использованием единой подсети для адресации исключительно проста и позволяет сэкономить адресное пространство.
2. Выделение одной подсети на каждый VC-канал. Такая топология сети Frame Relay больше рас­пространена по сравнению с предыдущей, поскольку многие организации стремятся сгруппировать приложения и серверы и развернуть их в некоторой центральной точ­ке сети, а основной трафик в сети курсирует между удаленными узлами и такими центральными серверами. Использование набора подсетей вместо одной большой подсети приводит к тому, что часть IP-адресов теряется, однако позволяет решить некоторые проблем протоколов маршрутизации в среде Frame Relay.
3. Гибридный подход. Такой подход предполагает выделение сегментов сети с полносвязной топологией и использование в них одной подсети для DTE-устройств, для всех остальных сегментов (неполносвязных) используется одна подсеть на каждый VC-канал.

В технологии Frame Relay можно пересылать копии широковещательных сообщений через все виртуальные каналы, но в ней нет аналога широковещательных сообщений локальной сети. Тем не менее, маршрутизаторам приходится пересылать широковещательные сообщения, чтобы несколько сетевых служб корректно работали. В частности, анонсы различных протоколов маршрутизации рассылаются с помощью либо широковещания, либо многоадресатной рассылки. Решить проблемы широковещания в технологии Frame Relay можно двумя способами.

Первый реализуется за счет того, что операционная система Cisco IOS может рассылать копии широковещательных сообщений через виртуальные каналы, если в конфигурации устройства указать соответствующие настройки. Если в сети используется всего несколько виртуальных каналов, такая конфигурация вполне обоснована.

Второй вариант решения заключается в том, что маршрутизатор пытается минимизировать негативные последствия от применения первого варианта решения. Маршрутизатор размещает копии широковещательных сообщений в специальных выходных очередях, отделенных от очередей пользовательского трафика, поэтому пользователь не замечает всплеска задержек и потерь пакетов, когда через виртуальные каналы рассылаются широковещательные сообщения.

**Примечание**. Описание процессов моделирования для этой лабораторной работы можно найти в справке Packet Tracer: Справка ⇒ Содержимое ⇒ раздел «Моделирование» ⇒ Лаб. работа №9.

## Методические указания

В качестве исходной будет использоваться сеть из (например, сеть с динамической маршрутизацией по OSPF). Прежде чем приступить к настройке среды Frame Relay, требуется добавить новые устройства на логическое рабочее пространство, настроить IP-адреса для интерфейсов, а также кластеризовать локальные сети филиалов для более удобной организации проекта:

1. Удалите с логического рабочего пространства сервер, соединенный с Маршрутизатор2.
2. На Маршрутизатор2 замените модуль PT-ROUTER-NM-1CFE на модуль PT-ROUTER-NM-1S. Данный модуль позволит подключаться к облаку Frame Relay через серийный кабель. Перед заменой модуля обязательно сохраните конфигурацию устройства!
3. Зайдите в режим конфигурации OSPF на Маршрутизатор2 (***router ospf 1***) и удалите сеть 192.168.6.0 (***no network 192.168.6.0 0.0.0.255 area 0***), так как она больше не используется.
4. Теперь необходимо кластеризовать сети филиалов. В Cisco Packet Tracer существует функция объединения нескольких устройств в кластер – отдельную группу, которая на логическом рабочем пространстве будет отображаться как отдельный элемент. Для создания кластера выделите все устройства сети первого филиала, включая Маршрутизатор0, а затем нажмите кнопку «Создать кластер», которая находится в разделе навигации:
5. Этим же способом кластеризуйте сеть второго филиала.
6. Далее следует добавить следующие новые устройства на логическое рабочее пространство: два маршрутизатора Cicso 1841 (самая простая модель, доступная в Packet Tracer), два коммутатора второго уровня Cisco 2960, два ПК PC-PT, а также облако Cloud-PT из раздела «Эмуляция WAN».
7. В новые маршрутизаторы стоит добавить модуль HWIC-2T, который предоставляет по два серийных интерфейса для подключения к облаку Frame Relay.
8. Соедините Маршрутизатор2, Маршрутизатор3 и Маршрутизатор4 с облаком Frame Relay с помощью кабеля «Серийный DTE». Помните, что DTE устанавливается на стороне клиента, поэтому всегда начинайте соединение с маршрутизатора!
9. Соедините Маршрутизатор3 и Коммутатор5, а также Коммутатор5 и ПК10 с помощью кабеля «Медный прямой». Точно также соедините Маршрутизатор4, Коммутатор6 и ПК11.
10. Проверьте итоговый вид сети (), а также настройте IP-адреса для устройств так (используйте маски 255.255.255.0). Не забудьте указать основные шлюзы для узлов (192.168.6.1 для ПК10 и 192.168.6.2 для ПК11). Новые сети 192.168.6.0 и 192.168.7.0 отражают территориально удаленные филиалы компании, доступ к которым будет производиться через провайдера по технологии Frame Relay.

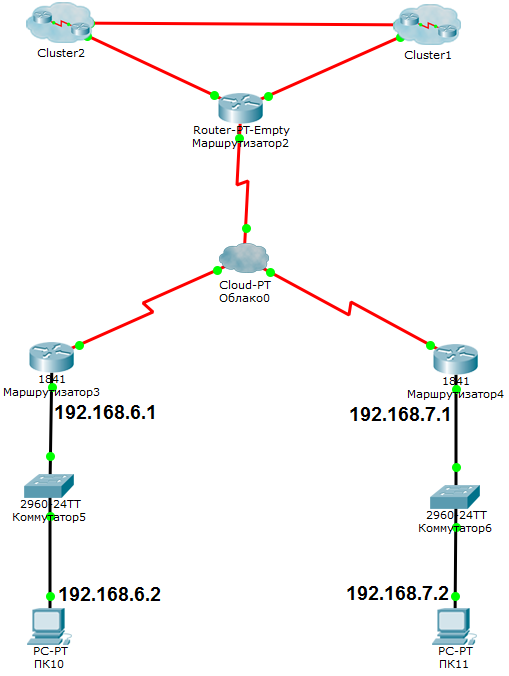


Рис. .. Итоговый вид сети

Стоит отметить, что новые сети представлены в упрощенном виде, однако для тестирования настроек Frame Relay этого достаточно. Сохраните проект в текущем виде, в дальнейшем этот проект будет использоваться как исходный для конфигурации Frame Relay двумя способами:

1. Настройка Frame Relay без использования подинтерфейсов на маршрутизаторах, реализация неполносвязной (а затем полносвязной) топологии сети с выделением одной подсети для всех DTE-устройств. Также в этом способе будет использована статическая маршрутизация (динамическая в этом способе не работает).
2. Настройка Frame Relay с использованием подинтерфейсов на маршрутизаторах, реализация полносвязной топологии сети с выделением одной подсети на один VC-канал. Также в этом способе будет использована динамическая маршрутизация по OSPF.

### Конфигурация без использования подинтерфейсов

Первым действием будет настройка облака провайдера в Cisco Packet Tracer. Требуется создать виртуальные каналы и указать DLCI, которые на них используются:

1. Нажмите на облако провайдера и перейдите на вкладку «Конфигурация».
2. В данном способе конфигурации будет реализована неполносвязная топология сети, в которой Маршрутизатор2 будет выступать в роли регулятора трафика от Маршрутизатор3 до Маршрутизатор4 и наоборот. Необходимо создать 4 виртуальных канала, которые будут использовать маршрутизаторы для связи друг с другом. Зайдите в конфигурацию интерфейса Serial0, который соединяет Маршрутизатор2 и Облако0. В поле «DLCI» введите номер DLCI – 203 (именно такой идентификатор удобно отражает маршрут Маршрутизатор2 ⇒ Облако0⇒ Маршрутизатор3). В поле «Имя» также введите 203, а затем нажмите кнопку «Добавить».
3. Этим же способом создайте виртуальный канал для маршрута Маршрутизатор2 ⇒ Облако0 ⇒ Маршрутизатор4.

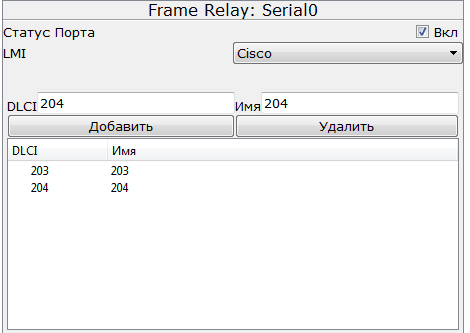


Рис. .. Создание виртуальных каналов для интерфейса Serial0

1. Для интерфейса Serial1, который соединяет Маршрутизатор3 и Облако0, создайте виртуальный канал с номером 302. (Маршрутизатор3 ⇒ Облако0⇒ Маршрутизатор2).
2. Для интерфейса Serial2, который соединяет Маршрутизатор4 и Облако0, создайте виртуальный канал с номером 402. (Маршрутизатор4 ⇒ Облако0⇒ Маршрутизатор2).
3. Нажмите на кнопку «Frame Relay» в меню выбора конфигураций. Здесь необходимо настроить связи между виртуальными каналами и серийными интерфейсами Облака0. Одна связь работает сразу в обе стороны, поэтому добавьте только две записи в таблицу (термин «Sublink» в Packet Tracer означает виртуальный канал):



Рис. .. Добавление связей в облако Frame Relay

На этом конфигурация облака провайдера закончена, теперь необходимо перейти к настройке маршрутизаторов:

1. Перейдите в режим конфигурации серийного интерфейса Маршрутизатор2 и выполните следующие команды:

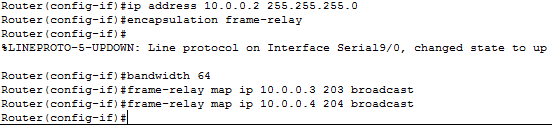


Рис. . Настройка Маршрутизатор2 на работу с Frame Relay

Здесь первая команда указывает IP-адрес для интерфейса. Вторая команда – ***encapsulation frame-relay*** указывает тип инкапсуляции для интерфейса, тем самым подготавливая его для работы в этой среде. Команда ***bandwidth 64*** указывает скорость канала связи – 64Кбит/с. Вручную указывать скорость канала нужно для того, чтобы протоколы маршрутизации правильно считали метрику для маршрутов, проходящих через провайдера. Следующие две команды статически связывают преобразование между IP-адресом и идентификатором DLCI. Маршрутизатор3 будет иметь IP-адрес 10.0.0.3, а DLCI 203 используется на маршруте Маршрутизатор2 ⇒ Облако0 ⇒ Маршрутизатор3, таким образом с помощью этой команды установлено статическое преобразование. Аргумент ***broadcast*** нужен для того, чтобы при отправке широковещательных сообщений они разбивались на множество однонаправленных кадров (среда Frame Relay не поддерживает широковещательный трафик в традиционном варианте).

1. Аналогично настройте серийные интерфейсы Маршрутизатор3 и Маршрутизатор4:



Рис. . Настройка Маршрутизатора3 на работу с Frame Relay

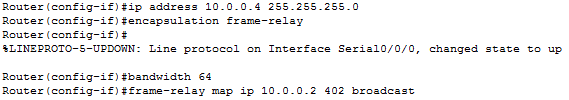


Рис. .. Настройка Маршрутизатора4 на работу с Frame Relay

1. Далее необходимо настроить статическую маршрутизацию на всех маршрутизаторах. Для Маршрутизатор2 добавьте два маршрута – до сетей 192.168.6.0 и 192.168.7.0. Сделайте это с помощью команд ***ip route 192.168.6.0 255.255.255.0*** ***10.0.0.3*** и ***ip route 192.168.7.0 255.255.255.0 10.0.0.4***
2. Для Маршрутизатор3 и Маршрутизатор4 нужны только маршруты по умолчанию – до интерфейса 10.0.0.2. Добавьте такой маршрут командой ***ip route 0.0.0.0 0.0.0.0 10.0.0.2***.
3. Настройте распространение статических маршрутов через протокол OSPF на Маршрутизатор2. Это необходимо т.к. трафик в сетях первого и второго филиала маршрутизируется по протоколу OSPF, с помощью этой настройки будет обеспечена связь этих филиалов с сетями, находящимися за облаком провайдера. На Маршрутизатор2 войдите в режим конфигурации протокола OSPF (***router ospf 1***), а затем введите команду ***redistribute static***.

На этом настройка среды Frame Relay закончена. Обязательно проверьте связь между различными устройствами с помощью echo-запросов. Также зайдите в режим симуляции и проследите путь PDU от ПК10 до ПК11. Он должен идти по следующему маршруту: ПК10 ⇒ Коммутатор5 ⇒ Маршрутизатор3 ⇒ Облако0 ⇒ Маршрутизатор2 ⇒ Облако0 ⇒ Маршрутизатор4 ⇒ Коммутатор6 ⇒ ПК11. Таким образом, Маршрутизатор2 выступает в роли регулятора трафика, поэтому он будет подвергаться повышенным нагрузкам, которые могут стать критическими, если данных передается большое количество. Для снижения нагрузки на Маршрутизатор2 нужно реализовать полносвязную топологию сети, добавив виртуальный канал от Маршрутизатор3 до Маршрутизатор4 напрямую через Облако0. Сделайте это самостоятельно используя вышеописанные команды.

### Конфигурация с использованием подинтерфейсов

Отличие этого способа от предыдущего в том, что для каждого DLCI используется свой подинтерфейс на маршрутизаторе. Это требуется для работы динамической маршрутизации в среде Frame Relay. Также будет использоваться правило «одна подсеть на один VC-канал». В перечислены IP-адреса, которые будут использоваться на подинтерфейсах маршрутизаторов (на всех IP-адресах использована маска 255.255.255.252):

Таблица .. IP-Адреса подинтерфейсов маршрутизаторов

|  |  |  |
| --- | --- | --- |
| Устройство | Подинтерфейс | IP-адрес |
| Маршрутизатор2 | .203 | 10.0.0.1 |
| Маршрутизатор2 | .204 | 10.0.0.5 |
| Маршрутизатор3 | .302 | 10.0.0.2 |
| Маршрутизатор3 | .304 | 10.0.0.9 |
| Маршрутизатор4 | .402 | 10.0.0.6 |
| Маршрутизатор4 | .403 | 10.0.0.10 |

1. В облаке провайдера добавьте следующие виртуальные каналы: 203 и 204 на интерфейсе Serial0; 302 и 304 на интерфейсе Serial1; 402 и 403 на интерфейсе Serial2.
2. Добавьте новые связи в Облако0 ().

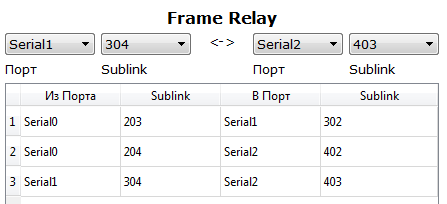


Рис. .. Добавление связей в облако Frame Relay

1. Введите на всех серийных интерфейсах всех маршрутизаторов команду ***encapsulation frame-relay***. Теперь все созданные подинтерфейсы будут использовать инкапсуляцию Frame Relay.
2. Зайдите в CLI Маршрутизатор2 и выполните следующие команды (название серийного интерфейса у вас может отличаться):

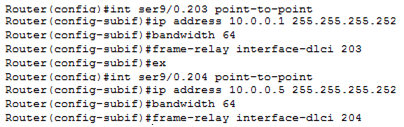


Рис. .. Конфигурация подинтерфейсов на Маршрутизаторе2

Здесь при создании подинтерфейса используется аргумент ***point-to-point***, который указывает, что связь будет построена по типу точка-точка. Затем устанавливается IP-адрес и маска, а также скорость канала связи (***bandwidth 64***). Команда ***frame-relay interface-dlci 203*** настраивает соответствие между подинтерфейсом и идентификатором DLCI.

1. Аналогично сконфигурируйте подинтерфейсы на Маршрутизатор3 и Маршрутизатор4:

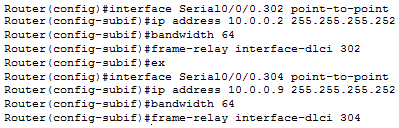


Рис. .. Конфигурация подинтерфейсов на Маршрутизатор3

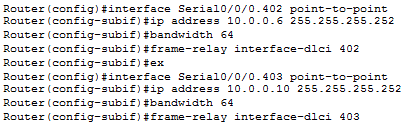


Рис. .. Конфигурация подинтерфейсов на Маршрутизатор4

1. Настройте loopback-интерфейсы на Маршрутизаторе3 (например, 5.5.5.5 с маской 255.255.255.255) и Маршрутизаторе4 (например, 6.6.6.6 с маской 255.255.255.255). Это нужно для того, чтобы включить эти маршрутизаторы в общий процесс протокола OSPF.
2. Зайдите в режим конфигурации процесса OSPF (***router ospf 1***) на Маршрутизаторах3 и 4, а затем установите исходную полосу пропускания (***auto-cost reference-bandwidth 1000***).
3. Сконфигурируйте протокол OSPF на маршрутизаторах, добавив все сети, с которыми они связаны:



Рис. .. Конфигурация OSPF на Маршрутизатор2



Рис. .. Конфигурация OSPF на Маршрутизатор3



Рис. .. Конфигурация OSPF на Маршрутизатор4

На этом основная конфигурация закончена. Обязательно проверьте работу сети с помощью echo-запросов, а также настройте аутентификацию для новых маршрутизаторов (материалы ).

## Заключение

В настоящее время технология Frame Relay широко применяется при построении распределённых корпоративных сетей, а также в составе решений, связанных с обеспечением гарантированной пропускной способности канала передачи данных. Следует отметить, что популярность этой технологии постепенно уменьшается, и ее вытесняют виртуальные частные сети. Тем не менее, сегодня каналы Frame Relay активно используются многими компаниями, поэтому эту технологию следует знать и уметь конфигурировать. Среда Frame Relay обладает следующими плюсами:

* множество виртуальных каналов на один серийный интерфейс;
* динамическое перераспределение полосы между каналами;
* высокая скорость коммутации/передачи за счет использования выделенного канала связи;
* широкое распространение сетей Frame Relay в мире.

Однако данная технология также имеет некоторые недостатки:

* для правильной работы требуется тщательная настройка оборудования;
* не имеет возможности корректно осуществлять передачу данных для приложений требующих малого времени задержки при передаче данных (видео- или аудиоинформация, передающаяся в реальном времени);
* необходимость использовать провайдера в качестве поставщика услуги;
* отсутствие проверки возможных ошибок в передающихся пакетах данных.

## Контрольные задания

1. Модифицировать задание №1 из Лабораторной работы №6. Постройте корпоративную сеть, используя следующую топологию:

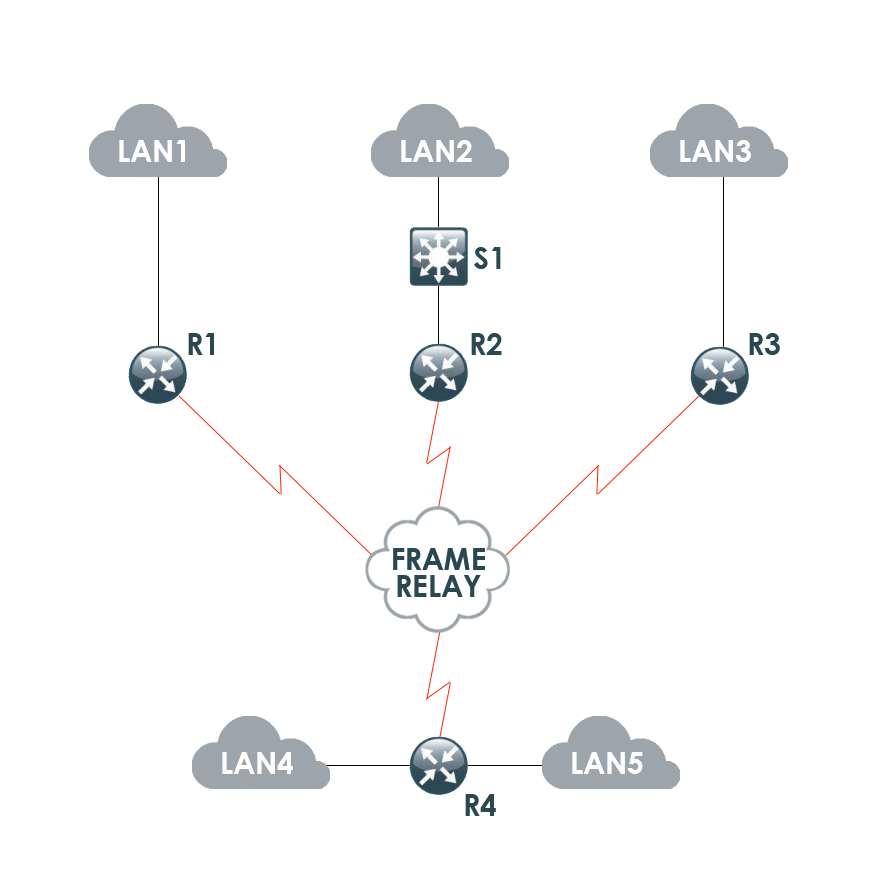


Рис. .. Схема сети задания №1

Реализуйте полносвязную топологию сети Frame Relay с использованием подинтерфейсов, Применяйте правило «одна подсеть для всех DTE-устройств», настройте динамическую маршрутизацию по протоколу RIP.

1. Модифицировать задание №2 из Лабораторной работы №6. Постройте корпоративную сеть, используя следующую топологию:

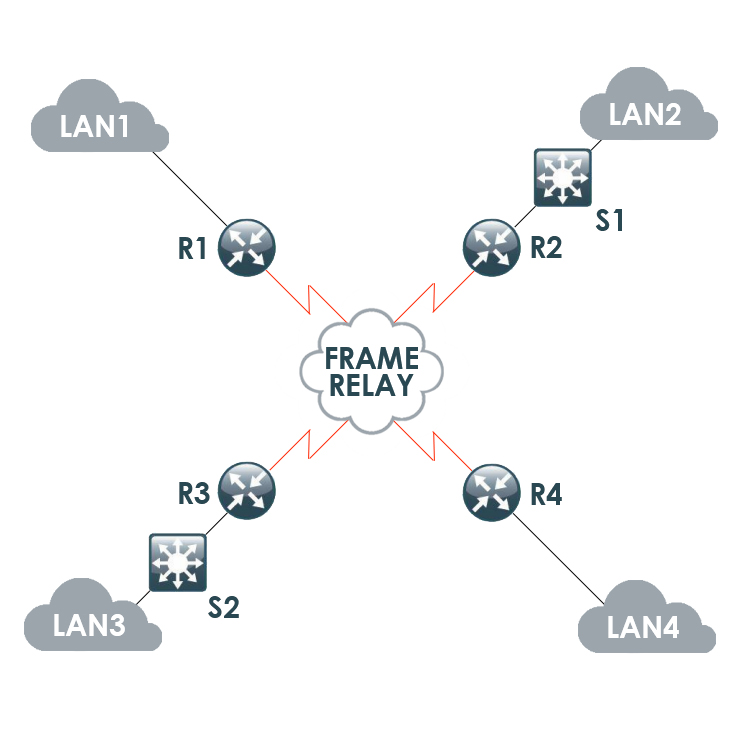


Рис. .. Схема сети задания №2

Реализуйте полносвязную топологию сети Frame Relay с использованием подинтерфейсов, Применяйте правило «одна подсеть на один VC-канал», настройте динамическую маршрутизацию по протоколу EIGRP.

1. Модифицировать задание №3 из Лабораторной работы №6. Постройте корпоративную сеть, используя следующую топологию:

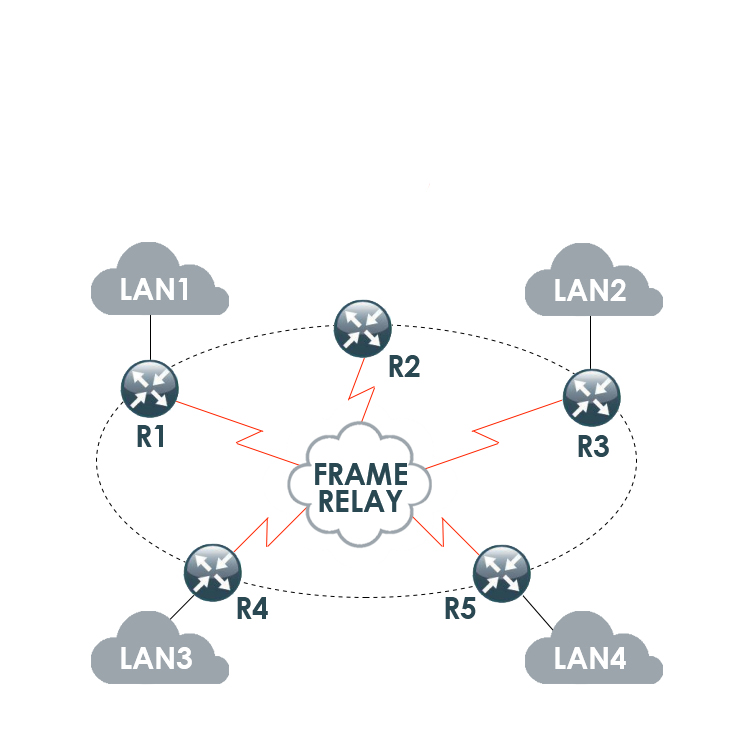


Рис. .. Схема сети задания №3

Реализуйте неполносвязную топологию сети Frame Relay без использования подинтерфейсов, Применяйте правило «одна подсеть для всех DTE-устройств», настройте статическую маршрутизацию.

1. Модифицировать задание №4 из Лабораторной работы №6. Постройте корпоративную сеть, используя следующую топологию:

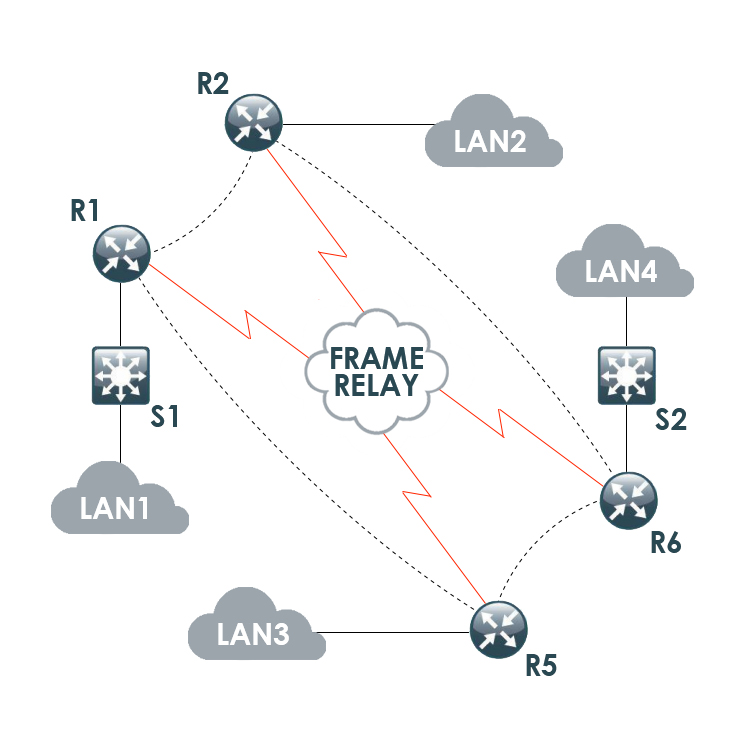


Рис. .. Схема сети задания №4

Реализуйте неполносвязную топологию сети Frame Relay с использованием подинтерфейсов, Применяйте правило «одна подсеть на один VC-канал», настройте динамическую маршрутизацию по протоколу OSPF.

## Легенда

|  |  |
| --- | --- |
| Термин | Описание |
|  | Локальная вычислительная сеть |
|  | Коммутатор третьего уровня |
|  | Маршрутизатор |
|  | Облако провайдера Frame Relay |
|  | Серийный кабель DCE/DTE |
|  | Виртуальный канал связи (VC) |
|  | Кабель «Медный прямой» |

# Виртуальные частные сети VPN

## Цели и задачи

Целью данной лабораторной работы является изучение еще одного популярного метода построения распределенных сетей – VPN.

В процессе выполнения будут решаться следующие задачи:

* изучение концепции и типов виртуальных частных сетей;
* изучение стандарта IPSec и входящих в него протоколов;
* настройка VPN-туннелей между маршрутизаторами Cisco на базе технологии IPSec;
* применение трех различных алгоритмов шифрования (DES, 3DES, AES) для обеспечения конфиденциальности передаваемых данных.

## Теоретические сведения

Виртуальная частная сеть VPN (Virtual private network) на сегодняшний день является набирающим популярность методом построения распределенной сети. В сравнении с технологией Frame Relay виртуальные частные сети не менее надежны в плане защиты информации, однако в несколько раз дешевле. Основной идеей этого метода является построение одного или нескольких сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Физически данные передаются через недостоверные каналы связи, поэтому потенциальный злоумышленник имеет возможность перехватить и использовать передающуюся информацию. Для обеспечения надежности при передаче трафика через VPN-сети должны быть решены следующие задачи:

* конфиденциальность (Privacy) – третье лицо не должно иметь возможности скопировать данные или ознакомиться с информацией, которая передается по сети Интернет;
* аутентификация (Authentication) – проверка того, действительно ли отправитель пакетов VPN — истинное устройство, а не такое, которое используется злоумышленником;
* целостность данных (Data integrity) – проверка, при которой выясняется, не подвергался ли изменениям пакет при передаче через Интернет;
* пересылка недостоверной информации (Antireplay) – третье лицо не должно иметь возможности копировать пакеты данных, отосланные истинным отправителем, а затем пересылать эти пакеты, выдавая себя за истинного отправителя.

Для решения перечисленных выше задач двумя устройствами создается виртуальная частная сеть, которую иногда называют VPN-туннелем (VPN tunnel). Такие устройства добавляют еще один заголовок к оригинальному пакету. В этот заголовок включаются поля, наличие которых позволяет VPN-устройствам выполнять перечисленные выше функции. Устройства также отвечают за шифрование оригинальных пакетов. Таким образом, подразумевается, что никто не дешифровал содержимое пакетов, даже если удалось скопировать пакеты при передаче через сеть Интернет.

В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть. Также можно выделить три типа VPN-сетей:

* внутрикорпоративные сети VPN (intranet VPN) – соединяют все компьютеры двух узлов сети одной организации;
* межкорпоративные сети VPN (extranet VPN) – соединяют все компьютеры двух узлов сетей разных организаций, поддерживающих партнерские отношения;
* VPN-сети удаленного доступа (remote access VPN) – соединяют отдельных пользователей с корпоративной сетью.

VPN-сеть может быть построена с помощью различных устройств, среди них маршрутизаторы, адаптивные устройства безопасности (Cisco ASA), VPN-концентраторы (устаревший продукт Cisco), а также обычные ПК с установленным VPN-клиентом.

Лидером в области защиты IP-сетей является стандарт **IPSec**. Это название — не аббревиатура, а сокращенная версия наименования в серии документов RFC (RFC 4301; архитектура безопасности Интернет-протокола — Security Architecture for the Internet Protocol), для которой употребляется название «IPSecurity» или сокращенная версия — «IPSec». Технология IPSec определяет набор функций, таких как аутентификация и шифрование, а также соответствующие правила для каждой из них.

Стандарт IPSec включает в себя целых три протокола, каждый со своими функциями:

1. **ESP** (Encapsulating Security Payload – безопасная инкапсуляция полезной нагрузки) занимается непосредственно шифрованием данных, а также может обеспечивать аутентификацию источника и проверку целостности данных.
2. **AH** (Authentication Header – заголовок аутентификации) отвечает за аутентификацию источника и проверку целостности данных.
3. **IKE** (Internet Key Exchange protocol – протокол обмена ключами) используется для формирования IPSec SA (Security Association), согласования работы участников защищенного соединения. Используя этот протокол, участники договариваются, какой алгоритм шифрования будет использоваться, по какому алгоритму будет производиться проверка целостности, а также как аутентифицировать друг друга. Под термином SA понимается набор параметров защищенного соединения, который может использоваться обеими сторонами соединения. У каждого соединения есть ассоциированный с ним SA.

Процесс шифрования в технологии IPSec не сложно понять. При шифровании в этом протоколе используется несколько алгоритмов, фактически — математические формулы, которые должны соответствовать определенным требованиям. Прежде всего, формулы нужно выбирать так, чтобы одна использовалась для шифрования данных, а другая — для расшифровывания. Шифрование данных в VPN-сетях на базе технологии IPSec происходит следующим образом ():

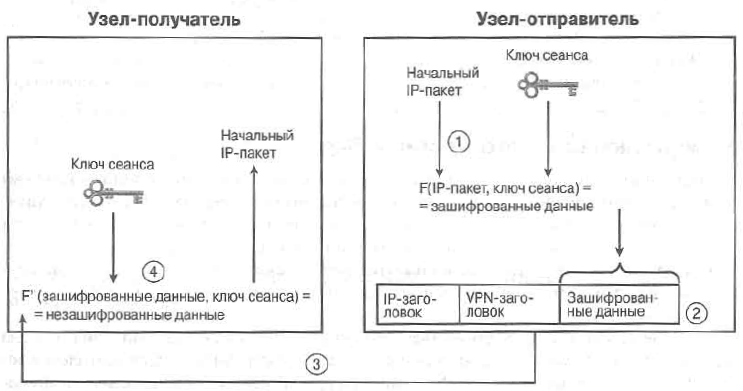


Рис. .. Шифрование данных в технологии IPSec

1. Устройство-отправитель в сети VPN подставляет исходные данные и ключ шифрования в формулу, по которой производится шифрование.
2. Устройство-отправитель инкапсулирует зашифрованные данные в пакет с новым IP-заголовоком и VPN-заголовок.
3. Устройство-отправитель пересылает этот пакет устройству-получателю сети VPN.
4. Устройство-получатель в сети VPN выполняет расшифровывание с использованием соответствующей формулы. В нее подставляются зашифрованные данные и ключ шифрования, значение которого совпадает с тем, которое использовалось в устройстве-отправителе сети VPN.

Технология IPSec поддерживает несколько алгоритмов шифрования. Одни из них разработаны совсем недавно и более эффективны, а другие имеют какие-то свои преимущества. В частности, длина ключа существенно влияет на стойкость алго­ритма. Например, алгоритмы на многоразрядных ключах гораздо сложнее взломать, но их скорость обработки устройствами ниже. Основные алгоритмы шифрования, используемые на оборудовании Cisco, перечислены ниже:

Таблица .. Алгоритмы шифрования в VPN-сетях

| Алгоритм шифрования | Размерность ключа, бит | Описание |
| --- | --- | --- |
| Стандарт шифрования данных (Data Encryption Standard — DES) | 56 | Устаревший и не такой надежный, как другие алгоритмы шифрования |
| Тройной DES/3-DES (Triple DES) | 56x3 | Последовательно применяются три разных DES-ключа длиной 56 бит. Таким образом, улучшается надежность по сравнению с алгоритмом DES |
| Улучшенный стандарт шифрования (Advanced Encryption Standard — AES) | 128-256 | Наиболее эффективный алгоритм шифрования на сегодняшний день. Обеспечивает высокую стойкость к шифрованию, менее ресурсозатратен, чем 3-DES |

Технология IPSec предоставляет несколько вариантов аутентификации и проверки целостности данных. Аутентификацией называют процесс или последовательность действий, выполнив которые, VPN-устройство может подтвердить, что полученный пакет данных отправлен действительно доверенным участником информационного обмена. Проверка целостности данных, иногда называемая аутентификацией сообщений, позволяет получателю удостовериться в том, что данные не были изменены при передаче.

За проверку целостности данных в VPN-сетях отвечает заголовок аутентификации (Authentication Header — АН), в котором используются общие (симметричные) ключи, как и в процессе шифрования, но для так называемых хеш-функций (hash function), а не формул шифрования. Хеш-функция работает по принципу контрольной последовательности кадра (Frame Check Sequence — FCS), но обеспечивает более высокий уровень безопасности. Хеш-алгоритм — это разновидность математической функции, называемой хеш-кодом идентификации сообщений (Hashed-based Message Authentication Code — HMAC). При использовании хеш-функции на выходе алгоритма получается небольшое число, которое сохраняется в одном из VPN- заголовков. Отправитель рассчитывает значение хеш-функции и помещает значение в заголовок. Получатель повторно рассчитывает значение хеш-функции с использованием ключа (который одинаков для обеих сторон) и сравнивает с тем, которое записано в заголовке. Если значения совпадают, значит, и отправитель, и получатель в формулу подставляли одинаковые данные. Таким образом, получатель удостоверяется, что сообщение не изменилось при передаче через сеть. При проверке целостности данных на основе хеш-функций используется секретный ключ. Его длина должна быть как минимум в два раза больше длины ключа для шифрования данных, поэтому на сегодняшний день уже разработано несколько разновидностей технологии НМАС. Например, в соответствии с алгоритмом MD5 используются ключи длиной 128 бит, поэтому он может быть использован для сетей VPN с ключами шифрования DES длиной 56 бит.

**Примечание**. Описание процессов моделирования для этой лабораторной работы можно найти в справке Packet Tracer: Справка ⇒ Содержимое ⇒ раздел «Моделирование» ⇒ Лаб. работа №10.

## Методические указания

В данной лабораторной работе будет выполнена настройка внутрикорпоративной VPN-сети, которая объединяет три филиала компании посредством нескольких VPN-туннелей, каждый из которых будет использовать различные алгоритмы шифрования и проверки целостности данных. В качестве исходной будет использоваться сеть из лабораторной работы №8 (Frame Relay без подинтерфейсов). Прежде чем приступить к настройке VPN, выполните следующие действия:

1. Удалите облако провайдера Frame Relay из логического рабочего пространства.
2. Сохраните конфигурации Маршрутизаторов 2, 3, и 4, а затем удалите из устройств модули с серийными интерфейсами.
3. Добавьте маршрутизатор Cisco 2811 на логическое рабочее пространство (далее он будет обозначаться как Маршрутизатор5). В него также необходимо добавить модуль NM-1FE2W.
4. В Маршрутизатор2 необходимо добавить модуль PT-ROUTER-NM-1CFE, а затем связать Маршрутизатор2 и Маршрутизатор5 каналом связи «медный перекрестный». Таким же каналом связи соедините Маршрутизатор5 и Маршрутизатор3, а также Маршрутизатор5 и Маршрутизатор4.
5. Настройте IP-адреса на интерфейсах маршрутизаторов так, как показано на рисунке (используйте маску 255.255.255.0):

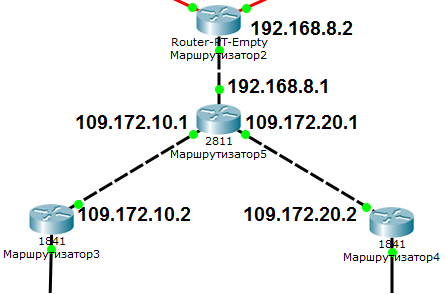


Рис. .. Настройка IP-адресов интерфейсов маршрутизатора.

1. Трафик между Маршрутизаторами 3, 4 и 5 будет проходить через сеть Интернет, именно поэтому внешние интерфейсы этих маршрутизаторов имеют публичные IP-адреса. Пометьте сеть Интернет, добавив два пустых облака CLOUD-PT-EMPTY и расположив их между маршрутизаторами так, как показано на рисунке:

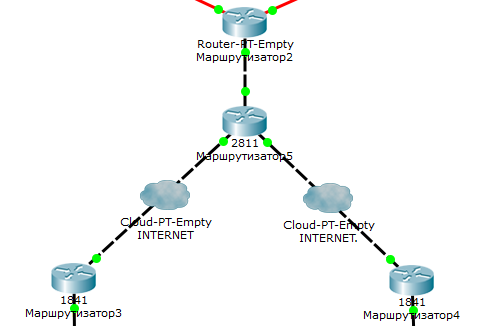


Рис. .. Изображение сети Интернет с помощью двух облаков

1. Необходимо настроить маршруты по умолчанию на маршрутизаторах 3 и 4. Зайдите в CLI Маршрутизатор3 и удалите старый маршрут по умолчанию (***no ip route 0.0.0.0 0.0.0.0 10.0.0.2***), а затем добавьте новый (***ip route 0.0.0.0 0.0.0.0 109.172.10.1***). Аналогичные действия проделайте на Маршрутизатор4 (***no ip route 0.0.0.0 0.0.0.0 10.0.0.2***, затем ***ip route 0.0.0.0 0.0.0.0 109.172.20.1***).
2. Настройте маршрутизацию на Маршрутизатор2. Удалите старые недействительные маршруты до подсетей 192.168.6.0 и 192.168.7.0. Затем установите маршрут по умолчанию до Маршрутизатора5, войдите в режим конфигурации процесса OSPF и добавьте новую сеть 192.168.8.0, а также распространите маршрут по умолчанию с помощью команды ***redistribute static*** (в протоколе OSPF для распространения маршрутов по умолчанию необходимо добавить настройку ***default-information originate*, без нее распространяться будут только статические маршруты, но не маршруты по умолчанию). Все перечисленные конфигурационные команды приведены ниже:**

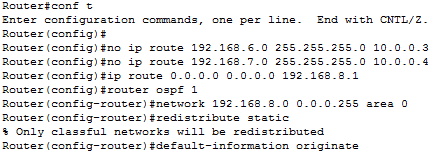


Рис. .. Настройка маршрутизации на Маршрутизатор2

1. Настройте статические маршруты на Маршрутизаторе5 ().

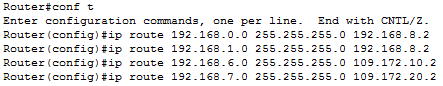


Рис. .. Настройка статических маршрутов на Маршрутизатор5.

Теперь можно приступить к настройке VPN-туннелей:

1. Первый туннель будет связывать сеть 192.168.6.0, находящуюся за Маршрутизатор3, и сети 192.168.0.0 и 192.168.1.0, находящиеся за Маршрутизатор5. Сначала необходимо создать access-list, в котором будет описано, какой трафик должен быть зашифрован и передан по VPN-туннелю ().

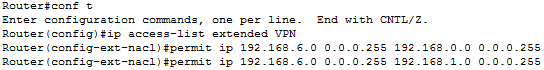


Рис. .. Создание расширенного списка доступа на Маршрутизатор3

Список является расширенным, и пропускает через себя только трафик, идущий из сети 192.168.6.0 в сеть 192.168.0.0 или 192.168.1.0.

1. Для построения VPN-туннеля, двум маршрутизаторам нужно договориться, какие алгоритмы/механизмы защиты они будут использовать для своего защищенного соединения. Для конфигурации этих параметров настраивается протокол IKE. В документации Cisco термины IKE и ISAKMP, как правило, взаимозаменяемы. Процесс конфигурации состоит из двух фаз: настройка политики ISAKMP, а затем настройка transform-set и криптокарты. Настройте политику ISAKMP на Маршрутизатор3 ()

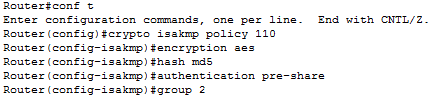


Рис. .. Настройка политики ISAKMP на Маршрутизатор3

Здесь «110» - идентификатор, обозначающий приоритет этой политики по сравнению с другими. Если на маршрутизаторе настроены сразу несколько политик, то первоначально для установления VPN-туннеля используется политика с наименьшим идентификатором. Команда ***encryption aes*** устанавливает алгоритм шифрования – AES. Команда ***hash md5*** указывает, что будет использоваться хэш-функция, работающая по алгоритму MD5. Команда ***Authentication pre-share*** нужна для того, чтобы указать тип аутентификации – использование предустановленных общих ключей. Наконец, ***group 2*** – это группа в алгоритме Диффи-Хеллмана, данная группа является оптимальным выбором между быстродействием (самая быстрая – group 1) и надежностью (самая надежная – group 5).

1. Перейдите в режим глобальной конфигурации и создайте ключ для аутентификации. Используйте команду ***crypto isakmp key cisco address 109.172.10.1***, в которой «***cisco***» - ключ, а «***109.172.10.1***» - IP-адрес интерфейса маршрутизатора, с которым устанавливается VPN-туннель (в данном случае это Маршрутизатор5).
2. Теперь необходимо создать ***transform-set***. Под этим термином подразумевается объект, который описывает параметры второй фазы. Введите команду ***crypto ipsec transform-set VPN-SET esp-aes esp-md5-hmac*** из режима конфигурации. Здесь «***VPN-SET***» - имя transform-set, «***esp-aes***» - алгоритм шифрования (обязательно должен совпадать с тем, что указывался в политике ISAKMP в первой фазе), «***esp-md5-hmac***» - алгоритм хэширования (также должен совпадать с алгоритмом, указанным в политике ISAKMP).
3. Далее требуется создать криптокарту (crypto map). Это объект, в котором находятся наборы правил, относящиеся к разным туннелям IPsec. К интерфейсу может быть применена только **одна** crypto map. Для того чтобы отличать правила, относящиеся к разным туннелям, правила группируются в наборы, которые объединяет общий порядковый номер правила. Для создания криптокарты введите следующие команды:

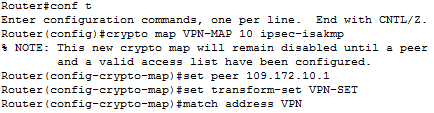


Рис. .. Создание криптокарты

Здесь команда ***crypto map VPN-MAP 10 ipsec-isakmp*** создает криптокарту с именем «VPN-MAP» и набором правил с номером «10». Команда ***set peer 109.172.10.1*** указывает противоположный маршрутизатор, с которым строится VPN-туннель, ***set transform-set VPN-SET*** привязывает transform-set с именем «VPN-SET» к криптокарте, а команда ***match address VPN*** устанавливает access-list, который будет использоваться в VPN-туннеле.

1. Привяжите криптокарту к интерфейсу. Зайдите в конфигурацию интерфейса, который связывает Маршрутизатор3 и Маршрутизатор5, а затем введите команду ***crypto map VPN-MAP***. Настройка VPN-туннеля на Маршрутизатор3 на этом заканчивается, далее нужно указать точно такие же параметры на Маршрутизатор5.
2. Перейдите в CLI Маршрутизатор5 и повторите все введенные ранее команды, однако замените IP-адрес 109.172.10.1 на 109.172.10.2. Список всех команд в том порядке, в котором они должны быть введены, приведен ниже:

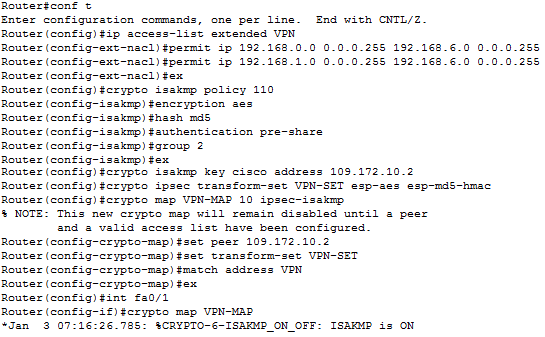


Рис. .. Настройка VPN-туннеля на Маршрутизатор5

1. Проверьте связь между сетями 192.168.6.0 и 192.168.0.0. Echo-запросы должны успешно завершаться.
2. После проверки echo-запросами, введите команду ***show crypto ipsec*** ***sa*** на любом из маршрутизаторов, учавствующих в процессе шифрования трафика:

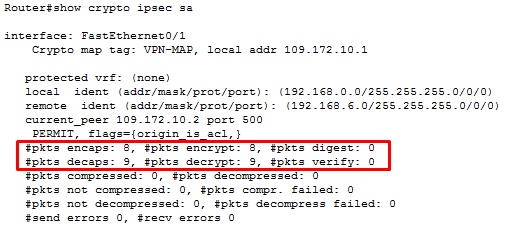


Рис. .. Вывод команды ***show crypto ipsec sa***

Выделенные строки указывают, сколько пакетов было зашифровано, а сколько – расшифровано. Это доказывает, что VPN-туннель успешно работает и защищает весь трафик, проходящий через него.

Далее необходимо настроить аналогичный VPN-туннель, который будет соединять сеть 192.168.7.0 с сетями 192.168.0.0 и 192.168.1.0. Однако параметры этого туннеля будут отличаться – вместо алгоритма шифрования AES будет использоваться алгоритм DES, а вместо хэш-функции MD5 будет использоваться SHA (Secure Hash Algorithm). Ниже приведены конфигурационные команды, которые необходимо ввести на Маршрутизатор4 для настройки такого туннеля:

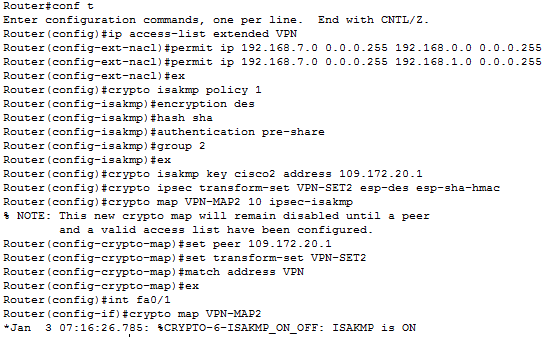


Рис. .. Настройка второго VPN-туннеля на Маршрутизатор4

Обратите внимание, что название интерфейса, к которому будет привязана криптокарта, должно совпадать с названием интерфейса, который связывает Маршрутизатор4 и Маршрутизатор5. Далее перечислены конфигурационные команды, которые необходимо ввести на Маршрутизатор5:

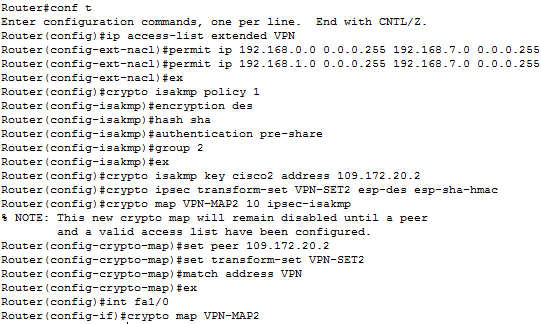


Рис. .. Настройка второго VPN-туннеля на Маршрутизатор5

Завершающим этапом данной лабораторной работы будет настройка третьего VPN-туннеля, который будет шифровать трафик от сети 192.168.6.0 до сети 192.168.7.0. Этот туннель будет использовать алгоритм шифрования 3DES и алгоритм хэширования MD5. В третьем VPN-туннеле не потребуется создавать новые криптокарты на маршрутизаторах, можно добавить группу правил в существующие, изменив при этом номер группы этих правил ():

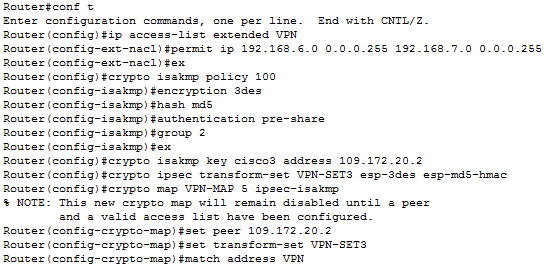


Рис. .. Настройка третьего VPN-туннеля на Маршрутизатор3

Обратите внимание, что IP-адрес в командах конфигурации – 109.172.20.2. При конфигурации VPN-туннеля необходимо указывать конечный IP-адрес, т.е тот адрес, на интерфейсе которого трафик должен быть расшифрован. Физически данные будут проходить через Маршрутизатор5, однако VPN-туннель – логический, поэтому фактически в параметрах можно указывать любой IP-адрес, необязательно чтобы он принадлежал интерфейсу на другом конце физического канала связи.

Далее перечислены конфигурационные команды, которые необходимо ввести на Маршрутизаторе4:

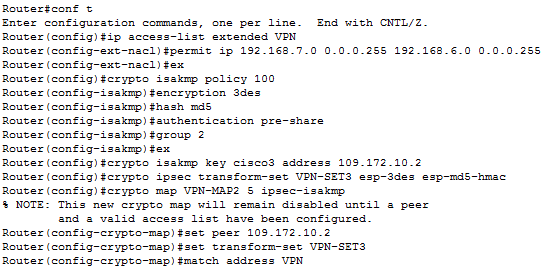


Рис. .. Настройка третьего VPN-туннеля на Маршрутизатор4

На этом настройка VPN-сети завершена. Не забудьте проверьте связь сетей с помощью echo-запросов.

## Заключение

Технология VPN отвечает основополагающим критериям сохранности информации: целостность, конфиденциальность, авторизованный доступ. В сравнении с сетями на основе Frame Relay виртуальные частные сети не менее надежны в плане защиты информации, однако в несколько раз дешевле, что делает данную технологию более привлекательной для использования с распределенными сетями.

Технология VPN обладает следующими плюсами:

* возможность развертывания распределенной сети без использования посредников (провайдеров);
* надежная конфиденциальность передаваемой информации;
* возможность использования широкого спектра VPN-устройств;
* не требует подключения дополнительных линий связи, потому что данные между удаленными сетями проходят через сеть Интернет.

Внедрение VPN в корпоративную сеть также имеет ряд недостатков:

* из-за необходимости шифровать и расшифровывать трафик, VPN-устройства сильнее расходуют свои вычислительные ресурсы, что может сказаться на пропускной способности сети;
* отсутствие устоявшихся стандартов аутентификации и обмена шифрованной информацией;
* отсутствие единых, надежных способов управления VPN-сетями;
* сетевые инженеры должны обладать высоким уровнем знаний при работе с VPN-сетями, так как эту технологию трудно настраивать и поддерживать.

## Контрольные задания

1. Модифицировать задание №1 из Лабораторной работы №6. Постройте корпоративную сеть, используя следующую топологию:

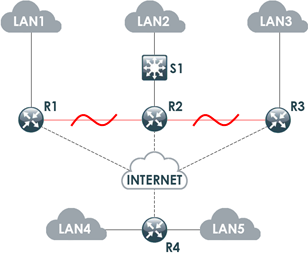


Рис. .. Схема сети задания №1

Постройте VPN-туннели между следующими сетями: LAN1 – LAN4, LAN1 – LAN5, LAN2 – LAN4, LAN2 – LAN5, LAN3 – LAN4, LAN3 – LAN5. Параметры VPN-туннелей: алгоритм шифрования – AES, алгоритм хэширования – MD5.Настройте статическую маршрутизацию, следите за тем, чтобы IP-адреса интерфейсов маршрутизаторов, выходящих в сеть Интернет, были публичными.

1. Модифицировать задание №2 из Лабораторной работы №6. Постройте корпоративную сеть, используя следующую топологию:

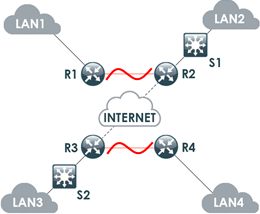


Рис. .. Схема сети задания №2

Постройте VPN-туннели между следующими сетями: LAN1 – LAN3, LAN1 – LAN4, LAN2 – LAN3, LAN2 – LAN4. Параметры VPN-туннелей: алгоритм шифрования – 3DES, алгоритм хэширования – SHA. Настройте статическую маршрутизацию, следите за тем, чтобы IP-адреса интерфейсов маршрутизаторов, выходящих в сеть Интернет, были публичными.

1. Модифицировать задание №3 из Лабораторной работы №6. Постройте корпоративную сеть, используя следующую топологию:

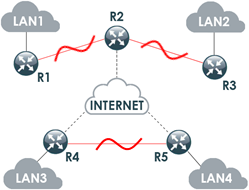


Рис. .. Схема сети задания №3

Постройте VPN-туннели между следующими сетями: LAN1 – LAN3, LAN1 – LAN4, LAN2 – LAN3, LAN2 – LAN4. Параметры VPN-туннелей: алгоритм шифрования – DES, алгоритм хэширования – MD5. Настройте статическую маршрутизацию, следите за тем, чтобы IP-адреса интерфейсов маршрутизаторов, выходящих в сеть Интернет, были публичными.

1. Модифицировать задание №4 из Лабораторной работы №6. Постройте корпоративную сеть, используя следующую топологию:

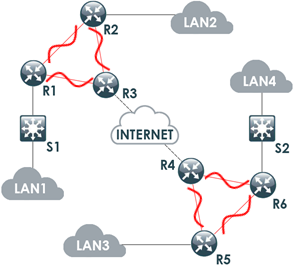


Рис. .. Схема сети задания №4

Постройте VPN-туннели между следующими сетями: LAN1 – LAN3, LAN1 – LAN4, LAN2 – LAN3, LAN2 – LAN4. Параметры VPN-туннелей: алгоритм шифрования – AES, алгоритм хэширования – SHA. Настройте статическую маршрутизацию, следите за тем, чтобы IP-адреса интерфейсов маршрутизаторов, выходящих в сеть Интернет, были публичными.

## Легенда

| Термин | Описание |
| --- | --- |
|  | Локальная вычислительная сеть |
|  | Коммутатор третьего уровня |
|  | Маршрутизатор |
|  | Глобальная сеть Интернет |
|  | Кабель «Медный перекрестный» |
|  | Волоконно-оптический кабель |
|  | Кабель «Медный прямой» |

# Беспроводные сети

## Цели и задачи

Целью данной лабораторной работы является получение практических навыков для построения беспроводных компьютерных сетей.

В процессе выполнения работы будут решаться следующие задачи:

* изучение концепций, вариантов применения и режимов работы беспроводных компьютерных сетей;
* построение беспроводной локальной сети в Cisco Packet Tracer, используя устройство Cisco Linksys WRT300N.;
* настройка основных параметров беспроводной сети – IP-адресов интерфейсов, DHCP-сервера и SSID;
* конфигурация защищенного режима беспроводной сети с помощью технологии WPA2.

## Теоретические сведения

По определению, беспроводные компьютерные сети — это технология, позволяющая создавать вычислительные сети, полностью соответствующие стандартам для обычных проводных сетей без использования кабельной проводки. В качестве носителя информации в таких сетях выступают радиоволны СВЧ-диапазона. Беспроводные сети можно с легкостью внедрять в места, где невозможно проложить кабель (например, вне зданий). Также использование таких сетей на предприятии может существенно расширить круг устройств, которые могут пользоваться ресурсами локальной сети (ноутбуки, мобильные телефоны, планшеты). Существует два основных направления применения беспроводных компьютерных сетей:

* работа в замкнутом пространстве (офисы, филиалы компании);
* соединение удаленных локальных сетей (или удаленных сегментов локальной сети).

Для организации беспроводной сети в замкнутом пространстве применяются передатчики с всенаправленными антеннами. Стандарт IEEE 802.11 определяет два режима работы таких сетей:

* **Ad-hoc** («точка-точка»): простая сеть, в которой связь между станциями (клиентами) устанавливается напрямую, без использования специальной точки доступа.
* **Клиент-сервер**: беспроводная сеть, состоящая как минимум из одной точки доступа, подключенной к проводной сети, и некоторого набора беспроводных клиентских станций. В большинстве сетей необходимо обеспечить доступ к файловым серверам, принтерам и другим устройствам, подключенным к проводной локальной сети, поэтому чаще всего используется режим клиент-сервер.

Комплексы для объединения локальных сетей по топологии делятся на два вида:

* топология «точка-точка»: организуется радиомост между двумя удаленными сегментами сети;
* топология «звезда»: одна из станций является центральной и взаимодействует с другими удаленными станциями. При этом центральная станция имеет всенаправленную антенну, а другие удаленные станции — однонаправленные антенны.

Беспроводные сети, в отличие от классических проводных сетей, являются менее защищенными от атак злоумышленников так как в связи с общей доступностью среды передачи данных появляется уязвимость каналов к прослушиванию и подмене сообщений. Все продукты для беспроводных сетей, соответствующие стандарту IEEE 802.11, предлагают следующие уровни безопасности:

1. Технология **DSSS**: поток требующих передачи данных «разворачивается» по каналу шириной 20 МГц в рамках диапазона ISM с помощью схемы ключей дополнительного кода (Complementary Code Keying, CCK). Для декодирования принятых данных получатель должен установить правильный частотный канал и использовать ту же самую схему CCK.
2. Идентификатор **SSID**: уникальное имя сети, включаемое в заголовок пакетов данных и управления IEEE 802.11. Позволяет различать отдельные беспроводные сети, которые могут действовать в одном и том же месте или области. Беспроводные клиенты и точки доступа используют его, чтобы проводить фильтрацию и принимать только те запросы, которые имеют правильный SSID. Таким образом, пользователь не сможет обратиться к точке доступа, если только ему не предоставлен верный SSID.
3. **MAC ID**: уникальное число, присваиваемое в процессе производства каждой сетевой карте. Когда клиентский ПК пытается получить доступ к беспроводной сети, точка доступа должна сначала проверить MAC-адрес клиента. Точно так же и клиентский ПК должен знать имя точки доступа.
4. Механизм шифрования данных (WEP, WPA, WPA2) обеспечивает еще один уровень безопасности, однако его использование ведет к снижению пропускной способности сети.

Несмотря на этот недостаток, технологии шифрования данных заслуживают более подробного описания:

* Механизм **WEP** (Wired Equivalent Privacy) использует алгоритм шифрования RC4 с 40- или 128-разрядными ключами. Процесс расшифровки данных, закодированных с помощью WEP, заключается в выполнении логической операции «исключающее ИЛИ» (XOR) над ключевым потоком и принятой информацией. Ключ WEP рекомендуется периодически менять, чтобы гарантировать целостность системы безопасности. В настоящее время данная технология является устаревшей, так как ее взлом может быть осуществлен всего за несколько минут.
* Механизм **WPA** и **WPA2** (Wi-Fi Protected Access) представляет собой обновлённую программу сертификации устройств беспроводной связи. WPA2 поддерживает шифрование в соответствии со стандартом AES, аутентификацию с использованием EAP (Extensible Authentication Protocol, расширяемый протокол аутентификации), а также систему централизованного управления безопасностью (чаще всего в этих целях используется RADIUS-сервер).

Таким образом, для проникновения в беспроводную сеть злоумышленник должен решить целый ряд задач: иметь оборудование, совместимое с используемым в сети, знать идентификатор сети SSID, быть занесенным в таблицу разрешенных MAC-адресов в точке доступа, а также знать ключ WPA или WEP. Выполнить все это практически невозможно, поэтому вероятность несанкционированного вхождения в беспроводную сеть, в которой приняты предусмотренные стандартом меры безопасности, можно считать очень низкой.

**Примечание**. Описание процессов моделирования для этой лабораторной работы можно найти в справке Packet Tracer: Справка ⇒ Содержимое ⇒ раздел «Моделирование» ⇒ Лаб. работа №11.

## Методические указания

В данной лабораторной работе будет выполнена настройка двух беспроводных сетей, которые расширяют круг пользователей локальных сетей филиалов, позволяя подключаться к ним с помощью ноутбуков, планшетов и смартфонов. В качестве исходной будет использоваться сеть из лабораторной работы №10 (Виртуальная частная сеть VPN). Настройте первую беспроводную сеть, последовательно выполнив следующие действия:

1. Добавьте на логическое рабочее пространство беспроводной маршрутизатор Cisco Linksys WRT300N из вкладки «Беспроводные устройства». Соедините Коммутатор5 с Беспроводным маршрутизатором0 с помощью кабеля «Медный прямой». При соединении устройств используйте интерфейс маршрутизатора под названием «Internet».
2. Добавьте ноутбук Laptop-PT на логическое рабочее пространство, замените стоящий по умолчанию модуль PT-LAPTOP-NM-1CFE на модуль беспроводной связи WPC300N. Через несколько секунд Ноутбук0 автоматически соединится с Беспроводным маршрутизатором0 с помощью беспроводной связи:

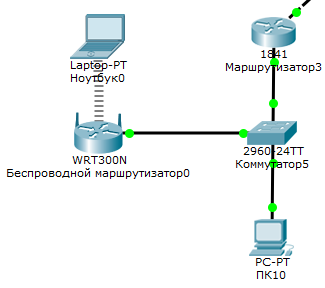


Рис. .. Автоматическое подключение Ноутбук0 к беспроводной сети

1. Зайдите на рабочий стол Ноутбука0 и откройте «Веб-браузер». В адресной строке наберите «http://192.168.0.1». По умолчанию, устройство Linksys WRT300N имеет именно такой IP-адрес, а также раздает IP-адреса всем подключенным к нему устройствам из диапазона 192.168.0.100 – 192.168.0.50 (работает как DHCP-сервер).
2. В окне авторизации введите имя пользователя «admin» и пароль «admin». Такие значения полей также являются значениями по умолчанию для устройств Linksys WRT300N.
3. Появится графический интерфейс конфигурации маршрутизатора Linksys WRT300N. В силу того, что сеть 192.168.0.1 уже используется, необходимо поменять IP-адрес самого маршрутизатора, а также диапазон адресов, которые выдает DHCP-сервер. В меню конфигураций под названием «Internet setup» (настройка Интернета) в строчке «Internet connection type» (тип подключения к Интернету) выберите пункт «Static IP» (статический IP). Заполните появившиеся поля так, как показано на :



Рис. .. Настройка внешнего IP-адреса Беспроводный маршрутизатор0

Таким образом был настроен IP-адрес Беспроводного маршрутизатора0 по отношению к остальной сети (192.168.6.3), маска подсети (255.255.255.0), а также шлюз по умолчанию (192.168.6.1).

1. В меню конфигураций под названием «Network setup» (настройка сети, под ней подразумевается внутренняя сеть беспроводного маршрутизатора) в строчке «Router IP» (IP маршрутизатора) введите IP-адрес 192.168.8.1 и маску подсети 255.255.255.0. Также в этом разделе можно настроить диапазон IP-адресов для выдачи DHCP-сервером, однако значения по умолчанию вполне приемлемы. Теперь сохраните настройки, нажав на кнопку «Save settings».

Через несколько секунд веб-браузер выдаст ошибку «Request timeout». Это происходит потому, что IP-адрес маршрутизатора был изменен, поэтому адрес 192.168.0.1 более недоступен.

**Примечание.** В дальнейшем каждое важное изменение в настройке беспроводной сети будет приводить к ошибке в веб-браузере, поэтому далее конфигурация Беспроводного маршрутизатор0 будет производиться без использования удаленного подключения через Ноутбук0. На логическом рабочем пространстве можно щелкнуть по Беспроводному маршрутизатор0 и выбрать вкладку «GUI», откуда и продолжить настройку беспроводной сети. Стоит отметить, что реальное оборудование всегда приходится настраивать через удаленное подключение.

Теперь необходимо настроить уровни безопасности:

1. В GUI Беспроводный маршрутизатор0 выберите вкладку «Wireless». В меню «Basic Wireless Settings» (базовые параметры беспроводной сети) можно настроить режим беспроводной сети (Network mode), установить идентификатор SSID (Network name), поменять полосу пропускания (Radio band, Standard Channel), а также включить или выключить режим широковещательной рассылки SSID (SSID Broadcast). Важно поменять идентификатор SSID со значения «Default» на другое (например, WLAN1), а также выключить (Disable) режим широковещательной рассылки SSID для того, чтобы сделать беспроводную сеть закрытой. Остальные настройки можно оставить по умолчанию. Сохраните конфигурацию, нажав на кнопку «Save settings».
2. Перейдите в меню «Wireless Security» (безопасность беспроводной сети) и выберите режим безопасности (Security Mode) – WPA2 Personal. Далее введите ключевую фразу (Passphrase), например, «cisco123», а затем сохраните конфигурацию. Стоит отметить, что выбор ключевой фразы напрямую влияет на защищенность беспроводной сети, по современным стандартам безопасной считается сеть с ключевой фразой в 20 символов.
3. Также следует поменять пароль для удаленного подключения к маршрутизатору. Делается это на вкладке «Administration» (административные настройки) в меню «Management» (управление).

Можно заметить, что Ноутбук0 и Беспроводной маршрутизатор0 потеряли связь. Для восстановления соединения необходимо создать профиль для подключения к беспроводной сети на Ноутбук0. Для этого нажмите на ярлык «Беспроводные настройки» на рабочем столе Ноутбук0. Появится окно конфигурации беспроводного адаптера ноутбука ():



Рис. .. Графический интерфейс беспроводного адаптера ноутбука

Надпись «No association with access point» означает, что связь с точкой доступа не установлена. Перейдите на вкладку «Profiles» (профили) для создания нового профиля для подключения к беспроводной сети.

1. В появившейся таблице профилей существует один профиль по умолчанию (Default), сбоку перечислены основные параметры этого профиля. Для добавления нового профиля нажмите на кнопку «New» (новый), затем введите имя профиля (например, WLAN1).
2. В следующем окне можно выбрать одну из доступных беспроводных сетей, однако в данном случае таких сетей нет (так как в настройках маршрутизатора была отключена широковещательная рассылка идентификатора SSID). Нажмите на кнопку «Advanced setup» (расширенные настройки).
3. Далее выберите режим беспроводной сети «Infrastructure mode» (инфраструктурный режим или «клиент-сервер») и введите идентификатор SSID – WLAN1. Нажмите кнопку «Next» (далее). В следующем окне предлагается настроить IP-адрес интерфейса Ноутбук0, однако на Беспроводный маршрутизатор0 уже настроен DHCP-сервер, поэтому оставьте настройки по умолчанию и еще раз нажмите кнопку «Next».
4. Появится окно «Wireless security» (безопасность беспроводной сети), в котором нужно выбрать режим «WPA2-Personal». В следующем окне необходимо ввести ключевую фразу, которая совпадает с установленной на беспроводном маршрутизаторе (cisco123).
5. В следующем окне будут перечислены все введенные настройки, проверьте их, а затем нажмите кнопку «Save» (сохранить).

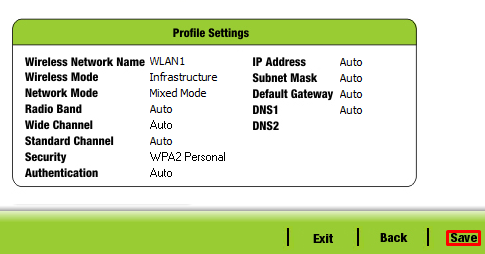


Рис. .. Параметры созданного профиля

1. Далее появится окно, извещающее о том, что профиль успешно создан. Нажмите на кнопку «Connect to network», и через несколько секунд Ноутбук0 подключится к беспроводной сети, об этом будет свидетельствовать надпись «You have successfully connected to the access point».
2. Для окончательного завершения построения беспроводной сети, добавьте на логическое рабочее пространство смартфон (PDA-PT) и планшет (TabletPC-PT), повторите шаги 11-17 по созданию профилей для каждого из устройств.

Беспроводная сеть примет следующий вид:

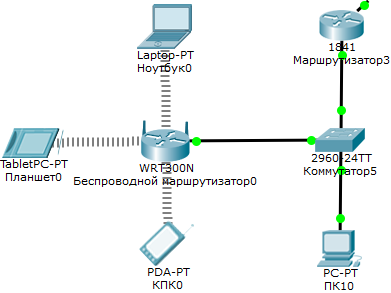


Рис. .. Беспроводная сеть с несколькими устройствами

Проверьте связь различных устройств друг с другом, а также с ПК10 и Маршрутизатор3 с помощью echo-запросов.

Теперь необходимо построить вторую беспроводную сеть:

1. Добавьте на логическое рабочее пространство еще один беспроводной маршрутизатор Cisco Linksys WRT300N, а также еще один ноутбук, планшет, и смартфон. Соедините маршрутизатор с Коммутатором6, а также замените модуль ноутбука на беспроводной.
2. В настройках Беспроводный маршрутизатор1 настройте IP-адрес интерфейса для связи с внешней сетью (192.168.7.3), маску подсети (255.255.255.0), а также шлюз по умолчанию (192.168.7.1).
3. Настройте внутренний IP-адрес беспроводного маршрутизатора (192.168.9.1 с маской 255.255.255.0). Настройки DHCP-Сервера можно оставить по умолчанию.
4. Обязательно повторно запросите IP-адреса на всех устройствах, подключенных к беспроводной сети. Новые адреса будут выдаваться DHCP-сервером из диапазона 192.168.9.100 – 192.168.9.150.
5. Повторите настройки уровней безопасности сети, так, как это было описано выше.

Вторая беспроводная сеть должна иметь следующий вид:

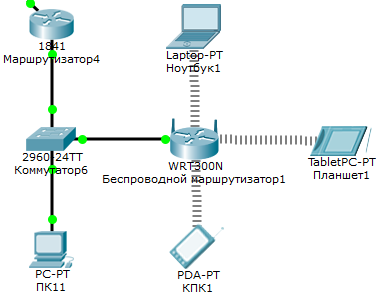


Рис. .. Итоговый вид сети

1. Теперь можно перейти к настройке еще одного уровня безопасности беспроводной сети – фильтрации устройств по MAC-адресу. В графическом интерфейсе Беспроводный маршрутизатор1 перейдите на вкладку «Wireless», далее в меню «Wireless MAC Filter» (фильтр MAC-адресов). В появившемся окне необходимо включить фильтр, установив переключатель в положение «Enabled». Также необходимо установить переключатель «Access Resolution» (правило доступа) в положение «Permit PCs listed below to access wireless network» (разрешить ПК, перечисленным ниже, доступ к беспроводной сети).

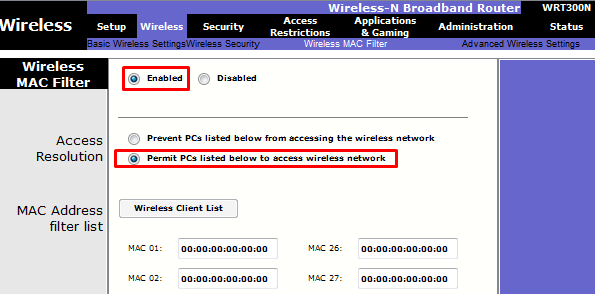


Рис. .. Настройки фильтра MAC-Адресов

1. Теперь необходимо добавить MAC-Адреса в список ниже. Для того чтобы узнать MAC-Адрес какого-либо устройства, достаточно в командной строке устройства ввести команду ***ipconfig /all***.

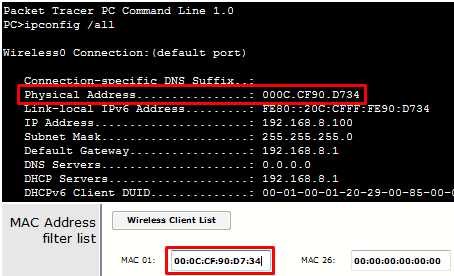


Рис. .. Добавление MAC-адреса в список разрешенных для доступа

На этом настройка беспроводных сетей закончена. Убедитесь, что на двух сетях настроены все уровни безопасности (SSID без широковещания, шифрование по WPA2, а также фильтрация по MAC-адресу). Самостоятельно настройте VPN-туннели до остальных филиалов компании (см. материалы лабораторной работы №10), а также настройте статическую маршрутизацию на маршрутизаторах, учитывая новые беспроводные сети (см. материалы лабораторной работы №5).

## Заключение

Беспроводные компьютерные сети позволяют повысить мобильность сотрудников в офисных или производственных помещениях, вдобавок исключив затраты на монтаж и обслуживание проводной сети. Беспроводные сети имеет смысл использовать в компаниях с небольшим количеством рабочих мест или при наличии большого количества беспроводных устройств (ноутбуков, смартфонов, планшетов). На сегодняшний день чаще всего используются одновременно и проводные и беспроводные сети, поэтому каждый сетевой специалист обязан уметь конфигурировать беспроводные маршрутизаторы также эффективно, как и обычные.

Беспроводные сети обладают следующими плюсами:

* простота и скорость развертывания сети, так как не требуется прокладка каналов связи;
* меньшая стоимость по сравнению с проводными сетями;
* возможность подключения ноутбуков, смартфонов, планшетов, а также других устройств, имеющих беспроводные адаптеры.

Однако внедрение беспроводных сетей в корпоративную инфраструктуру также имеет ряд недостатков:

* сравнительно низкая надежность по сравнению с проводными сетями;
* низкая устойчивость к взлому при неправильной настройке (WEP очень быстро взламывается, WPA2 требует ключевую фразу как минимум из 20 символов для обеспечения безопасности);
* скорость передачи делится между всеми устройствами в пределах обслуживания их одной и той же точкой доступа. Это значит, что если точка доступа предоставляет скорость передачи данных 300 Мбит/с и к ней будет одновременно подключено 5 устройств, то скорость для каждого устройства составит 300 / 5 = 60 Мбит/с. А поскольку объем передаваемой служебной информации может достигать 30-40%, итоговая скорость передачи может составлять всего 36 Мбит/с на каждое устройство. Этот факт необходимо учитывать при проектировании сети.

## Контрольные задания

1. Модифицировать задание №1 из Лабораторной работы №7. Добавить в LAN4 и LAN5 беспроводные маршрутизаторы и настроить все уровни безопасности, а также подключить некоторое количество пользователей. Сконфигурировать динамическую маршрутизацию во всей сети так, чтобы обеспечить связь беспроводных сетей с проводными.
2. Модифицировать задание №2 из Лабораторной работы №7. Добавить в LAN2 и LAN3 беспроводные маршрутизаторы и настроить все уровни безопасности, а также подключить некоторое количество пользователей. Сконфигурировать динамическую маршрутизацию во всей сети так, чтобы обеспечить связь беспроводных сетей с проводными.
3. Модифицировать задание №3 из Лабораторной работы №7. Добавить в LAN3 и LAN4 беспроводные маршрутизаторы и настроить все уровни безопасности, а также подключить некоторое количество пользователей. Сконфигурировать динамическую маршрутизацию во всей сети так, чтобы обеспечить связь беспроводных сетей с проводными.
4. Модифицировать задание №4 из Лабораторной работы №6. Добавить в LAN1 и LAN4 беспроводные маршрутизаторы и настроить все уровни безопасности, а также подключить некоторое количество пользователей. Сконфигурировать статическую маршрутизацию во всей сети так, чтобы обеспечить связь беспроводных сетей с проводными.

# двойной стек протоколов IP v4 / IP v6

## Цели и задачи

Целью данной лабораторной работы является обзор возможностей протокола IPv6, а также получение навыков построения локальных сетей, используя данный протокол отдельно, либо вместе с протоколом IPv4.

В процессе выполнения работы будут решаться следующие задачи:

* изучение вопросов адресации и маршрутизации в протоколе IPv6;
* конфигурация IPv6-адресов на маршрутизаторах Cisco;
* настройка динамической маршрутизации по протоколам RIPng, OSPFv3, EIGRP IPv6;
* реализация двойного стека протоколов IPv4/IPv6 на маршрутизаторах Cisco.

## Теоретические сведения

Шестая версия протокола IP (IPv6) обеспечивает окончательное решение проблемы исчерпания адресов протокола IPv4 в глобальном адресном пространстве сети Интернет, используя 128-битовый адрес и предоставляя около 1038 адресов по сравнению со всего лишь 4х109 адресами в протоколе IPv4. Предстоящий переход на протокол IPv6 будет, вероятно, вызван потребностью в большем количестве адресов. Практически каждый мобильный телефон сегодня поддерживает передачу данных через Интернет, что требует использования IP-адреса, некоторые производители даже склоняются к мнению, что все их устройства должны иметь IР-функции.

Стратегия назначения адресов для протокола IPv6 проста и может быть обобщена в приведенных ниже положениях:

* открытые адреса IPv6 группируются (численно) по крупным географическим регионам;
* в каждом регионе пространство адресов подразделяется провайдерами ISP (Internet Service Provider) в данном регионе;
* для каждого провайдера ISP в регионе адресное пространство подразделяется для каждого клиента.

Назначением адресов протокола IPv6 занимаются те же организации, которые назна­чают адреса для протокола IPv4. Этим процессом управляет агентство Интернета по на­значению сетевых адресов (Internet Coiporation for Assigned Network Numbers — ICANN). Агентство ICANN выделяет один или более диапазонов ад­ресов региональным реестрам (Regional Internet Registry — RIR), которых насчитывается пять — они примерно покрывают Северную Амери­ку, Центральную/Южную Америку, Европу, Азию/Тихоокеанский регион и Африку. Эти регионы RIR далее подразделяют свои адресные пространства на меньшие части, назначая префиксы провайдерам ISP и регистрам меньшего размера (ранга). Провайде­ры ISP далее назначают меньшие диапазоны адресов своим пользователям.

Соглашения протокола IPv6 используют 32 шестнадцатеричных номера, которые для представления 128-битового адреса протокола IPv6 организованы в 8 квартетов по 4 шестнадцатеричные цифры, разделенные двоеточиями, например:

2340:1111:АААА:0001:1234:5678:9АВС:0001

Также существуют два соглашения, которые позволяют сократить запись IPv6-адреса:

* можно опустить все ведущие нули в любом квартете;
* можно представить один или более последовательных квартетов, которые состоят из полностью шестнадцатеричных нулей, двумя двоеточиями, однако только для одного такого вхождения в конкретном адресе.

Например, адрес FE00:0000:0000:0001:0000:0000:0000:0056 может быть сокращен двумя способами, т.к имеются два места, в которых один или более квартетов содержат четыре шестнадцатеричных нуля:

* FE00::1:0:0:56;
* FE00:0:0:1::56.

Два последовательных двоеточия означают, что один или более октетов состоят только из нулей, однако такое сокращение не может использоваться дважды, поскольку такая запись была бы неоднозначной. Поэтому сокращение FE00::1::56 было бы недействительным.

Префиксы протокола IPv6 представляют собой диапазон или блок последовательных адресов IPv6. Число, которое представляет диапазон адресов, называемое префиксом, обычно можно увидеть в таблицах маршрутизации протокола IPv6, точно так же, как можно увидеть IP-номера подсетей в таблицах маршрутизации протокола IPv4. Префиксы протокола IPv6 записываются в виде некоторого значения, косой черты (/) и числовой длины префикса. Как и для префиксов протокола IPv4 (сокращенная запись маски подсети), последняя часть номера, исключая длину префикса, представляется бинарными нулями. Номера префиксов протокола IPv6 также могут сокращаться. Например:

2000:1234:5678:9АВС:1234:5678:9АВС:1111/64

Это значение представляет собой полный 128-битовый IP-адрес без возможности его сокращения. Однако при записи или наборе префикса все биты, находящиеся за длиной префикса, равны бинарным нулям. Префикс, в котором находится адрес, выглядит следующим образом:

2000:1234:5678:9АВС:0000:0000:0000:0000/64

В сокращенном виде он будет выглядеть так:

2000:1234:5678:9АВС::/64

Если длина префикса не кратна 16, то граница между префиксной частью адреса и частью, относящейся к узлу, проходит внутри квартета. В таких случаях значение префикса должно включать в себя все значения последнего октета в префиксной части. Например, если бы только что рассмотренный адрес с длиной префикса /64 имел вместо этого длину префикса /56, то префикс включал бы в себя все три первых квартета (всего — 48 бит), плюс 8 первых битов четвертого октета. Последние 8 бит (последние две шестнадцатеричные цифры) четвертого октета были бы бинарными нулями. В соответствии с соглашением оставшаяся часть четвертого октета после установки бинарных нулей выглядела бы следующим образом:

2000:1234:5678:9А00::/56

Ниже обобщены некоторые ключевые положения записи префиксов протокола IPv6:

* префикс имеет то же значение, что и адрес IP в группе первых битов, определяемой длиной префикса;
* все биты, находящиеся после битов, количество которых определяется длиной префикса, равны бинарным нулям;
* префикс может быть сокращен по тем же правилам, которые применяются к адресам IPv6;
* если длина префикса не соответствует границе квартета, то следует записать значение для всего квартета;

Все IPv6-адреса можно разделить на три категории:

1. **Одноадресатные** (Unicast). IP-адреса предназначены для отдельного интерфейса с тем, чтобы позволить одному узлу отправлять и получать данные.
2. **Многоадресатные** (Multicast). IP-адреса, которые представляют динамическую группу узлов, с целью отправки пакетов всем текущим членам данной группы.
3. **Одноадресатный резервный адрес** (Anycast). При выборе такого типа адреса серверы, которые поддерживают одну и ту же функцию, могут использовать один и тот же одноадресатный IP-адрес; при этом пакеты, посылаемые клиентами, пересылаются на ближайший сервер, что позволяет балансировать нагрузку между различными серверами.

В IPv6-адресации также существуют канальные локальные адреса. Протокол IPv6 использует эти адреса при отправке пакетов по локальной подсети; маршрутизаторы не пересылают пакеты, получателями которых являются канальные локальные адреса, в другие подсети. Канальные локальные адреса могут быть полезными для функций, выполнение которых не требует передачи пакетов в другие подсети, например, в процессе начальной загрузки и настройки узел может автоматически получить собственный канальный локальный IP-адрес без отправки пакета за пределы подсети. Узел получает свой адрес IPv6, который можно использовать для первых служебных сообщений. Канальные локальные адреса происходят из диапазона FE80::/10, т.е. под ними подразумеваются все адреса, которые начинаются со значений FE80, FE90, FEA0 и FEB0. При этом не требуется какого-либо специального конфигурирования, потому что узел формирует эти адреса, используя первые 10 бит шестнадцатеричного значения FE80 (двоичное значение 1111111010), дополняет их 54 бинарными нулями, а последние 64 бит являются идентификатором интерфейса узла.

Как и в технологии IPv4, большинство протоколов маршрутизации технологии IPv6 являются протоколами внутреннего шлюза (IGP), а протокол граничного шлюза (BGP) является единственным протоколом внешнего шлюза (EGP). Все протоколы IGP и протокол BGP были обновлены для поддержки IPv6, а также получили новые названия – RIPng (Протокол RIP следующего поколения), OSPFv3 (OSPF третьей версии), MP-BGP4 (Многопротокольный BGP-4), EIGRP IPv6 (EIGRP для IPv6).

В каждый из указанных протоколов маршрутизации пришлось внести изменения для поддержки протокола IPv6. В частности, были изменены сообщения, используемые для отправки и получения информации о маршрутизации; в них используются заголовки IPv6 вместо заголовков IPv4, и в этих заголовках используются адреса протокола IPv6. Тем не менее протоколы маршрутизации по-прежнему сохраняют многие из своих внутренних функций. Например, протокол RIPng, основанный на протоколе RIP-2, остается дистанционно-векторным протоколом, использующим в качестве метрики количество переходов, а максимальным допустимым количеством переходов остается 15. Протокол OSPFv3, созданный специально для поддержки протокола IPv6, остается протоколом с учетом состояния канала, использующим стоимость в качестве метрики, однако многие внутренние детали в нем изменены, в частности типы анонсов состояния канала (LSA).

Мгновенный переход от протокола IPv4 к протоколу IPv6 невозможен. На переход от IPv4 к IPv6 может потребоваться несколько лет, если не десятилетий. Однако уже сейчас существует несколько способов перехода к полному или частичному использованию IPv6:

* **Двойной стек** (dual stack): узел или маршрутизатор использует одновременно оба протокола — IPv4 и IPv6. Для узла это означает, что с каждой его платой сетевого интерфейса связаны как адрес IPv4, так и адрес IPv6, что позволяет узлу пересылать пакеты IPv4 другим узлам этого протокола, и узел может отправлять пакеты IPv6 другим узлам IPv6. Для маршрутизаторов такая настройка означает, что в дополнение к обычным IP-адресам и протоколам маршрутизации IPv4 в них сконфигурированы адреса и протоколы маршрутизации IPv6.
* **Туннелирование**: инкапсуляция пакета IPv6 в пакет протокола IPv4. После этого пакет IPv4 может пересылаться по уже существующей объединенной сети IPv4, а другое устройство удаляет заголовок IPv4 и извлекает из него первоначальный пакет IPv6.
* Трансляция между протоколами IPv4 и IPv6 с использованием службы **NAT-PT** (Network Address Translation-Protocol Translation).

**Примечание**. Описание процессов моделирования для этой лабораторной работы можно найти в справке Packet Tracer: Справка ⇒ Содержимое ⇒ раздел «Моделирование» ⇒ Лаб. работа №12.

## Методические указания

В данной лабораторной работе будет выполнена настройка сети, которая будет использовать двойной стек протоколов IPv4/IPv6, а также будет рассмотрена настройка динамических протоколов маршрутизации для IPv6: RIPng, OSPFv3 и EIGRP IPv6.

Прежде чем приступить к настройке двойного стека, последовательно выполните следующие действия по добавлению и расположению устройств на логическом рабочем пространстве:

1. Добавьте 2 узла PC-PT, 2 сервера Server-PT, 2 маршрутизатора Cisco 2811, а также 4 коммутатора 2960.
2. В каждый из маршрутизаторов следует добавить модуль NM-1FE-FX (Fast Ethernet по волоконно-оптическому каналу связи).
3. Соедините устройства так, как показано на :



Рис. .. Исходный вид сети

Основная идея двойного стека для этой сети – организовать работу по протоколу IPv4 между устройствами ПК0 и Сервер0, а между устройствами ПК1 и Сервер1 использовать IPv6. Маршрутизатор0 и Маршрутизатор1 будут настроены на маршрутизацию по обоим протоколам. Настройте IP-адреса узлов и интерфейсов маршрутизаторов, использующих IPv4 (используйте маску 255.255.255.0):

1. ПК: 192.168.0.2, основной шлюз: 192.168.0.1.
2. Порт Маршрутизатор0, связанный с Коммутатор0: 192.168.0.1.
3. Порт Маршрутизатор0, который связан с Маршрутизатором1: 192.168.1.1.
4. Порт Маршрутизатор1, который связан с Маршрутизатор0: 192.168.1.2.
5. Порт Маршрутизатор1, связанный с Коммутатор1: 192.168.2.1.
6. Сервер0: 192.168.2.2, основной шлюз: 192.168.2.1.

Процесс настройки IPv6-адресов для оставшихся узлов и интерфейсов будет рассмотрен более подробно:

1. Зайдите в настройку IP-адреса из рабочего стола ПК1, и заполните нижние поля так, как показано на :

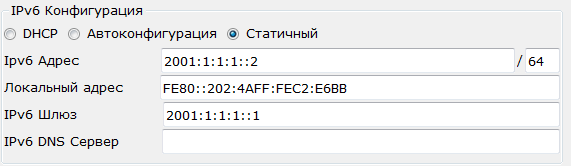


Рис. .. Конфигурация IPv6-адреса на ПК1

IPv6-адрес записывается в сокращенной записи, полная запись для этого адреса имеет вид **2001:0001:0001:0001**:0000:0000:0000:0002 (жирным шрифтом выделена часть адреса, относящаяся к префиксу).

1. Аналогично настройте IPv6-адреса для Сервер1:

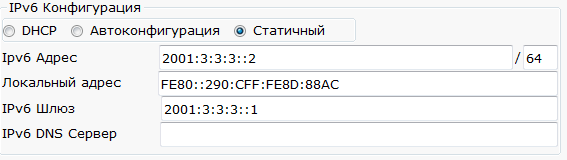


Рис. .. Конфигурация IPv6-адреса на Сервер1

1. Настройте IPv6-адреса для интерфейсов Маршрутизатора0 с помощью команды ***ipv6 address <адрес>/<длина префикса>***:

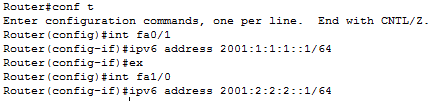


Рис. .. Настройка IPv6-адресов на интерфейсах Маршрутизатор0

Обратите внимание, что в данном примере fa0/1 – интерфейс, соединяющий Маршрутизатор0 и Коммутатор2, fa1/0 – интерфейс, соединяющий Маршрутизатор0 и Маршрутизатор1.

1. Настройте IPv6-адреса для интерфейсов Маршрутизатор1:

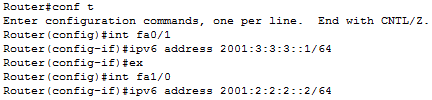


Рис. .. Настройка IPv6-адресов на интерфейсах Маршрутизатор1

Здесь fa0/1 – интерфейс, соединяющий Маршрутизатор1 и Коммутатор3, fa1/0 – интерфейс, соединяющий Маршрутизатор1 и Маршрутизатор0.

1. Настройте loopback-интерфейсы на Маршрутизатор0 (1.1.1.1 с маской 255.255.255.255) и Маршрутизаторе1 (2.2.2.2 с маской 255.255.255.255).

Теперь на всех устройствах настроены IPv4- и IPv6-адреса, однако не сконфигурирована динамическая маршрутизация. Сохраните проект в текущем виде, в дальнейшем он будет использоваться в качестве исходного для настройки трех динамических протоколов маршрутизации.

### Двойной стек с использованием RIP2/RIPng

1. Настройте протокол RIP2 на Маршрутизатор0 и Маршрутизатор1 (материалы ).
2. Настройте протокол RIPng на Маршрутизатор0:

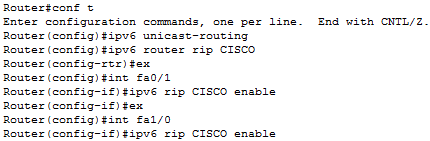


Рис. .. Настройка RIPng на Маршрутизаторе0

Здесь ***ipv6 unicast-routing*** – глобальная команда для включения маршрутизации IPv6, ***ipv6 router rip CISCO*** – создание процесса протокола RIPng с именем CISCO, ***ipv6 rip CISCO enable*** – включение процесса CISCO на интерфейсах Маршрутизатор0.

1. Аналогичным образом настройте протокол RIPng на Маршрутизатор1 – команды для конфигурации совпадают полностью, за исключением, возможно, имен интерфейсов.
2. Выполните проверку связи с помощью echo-запросов от ПК1 до Сервер1:

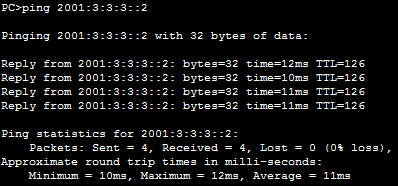


Рис. .. Проверка связи между ПК1 до Сервер1

Также выполните проверку связи между ПК0 и Сервер0, если echo-запросы выполняются успешно, значит двойной стек успешно работает на двух маршрутизаторах.

1. Выполните команду ***show ipv6 route*** на Маршрутизатор0, и проанализируйте таблицу маршрутизации:

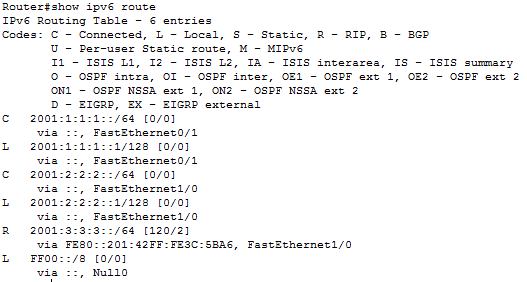


Рис. .. Таблица маршрутизации для протокола IPv6 на Маршрутизатор0

Из таблицы следует, что маршрутизатор записывает в нее канальные локальные адреса (буква «L» рядом с маршрутом), а также использует их для передачи данных в другие подсети («via FE80::201:42FF:FE3C:5BA6»).

### Двойной стек с использованием OSPF/OSPFv3

1. Настройте протокол OSPF на Маршрутизатор0 и Маршрутизатор1 (материалы ):
2. Настройте протокол OSPFv3 на Маршрутизатор0:

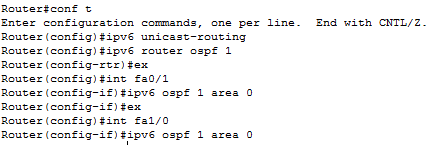


Рис. .. Настройка OSPFv3 на Маршрутизатор0

Здесь ***ipv6 unicast-routing*** – глобальная команда для включения маршрутизации IPv6, ***ipv6 router ospf 1*** – создание процесса протокола OSPFv3 с номером «1», ***ipv6 ospf 1 area 0*** – включение процесса протокола OSPF с номером «1» и зоной «0» на интерфейсах Маршрутизатор0.

1. Аналогичным образом настройте OSPFv3 на Маршрутизатор1, а затем проверьте связь ПК1-Сервер1 и ПК0-Сервер0.

### Двойной стек с использованием EIGRP/EIGRP IPv6

1. Настройте протокол EIGRP на Маршрутизатор0 и Маршрутизатор1 (материалы ):
2. Настройте протокол EIGRP IPv6 на Маршрутизатор0:

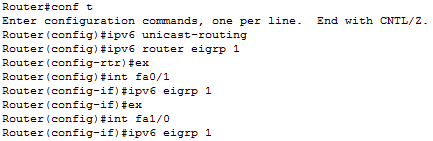


Рис. . Настройка EIGRP IPv6 на Маршрутизатор0

Здесь ***ipv6 unicast-routing*** – глобальная команда для включения маршрутизации IPv6, ***ipv6 router eigrp 1*** – создание процесса протокола EIGRP IPv6 для автономной системы с номером «1», ***ipv6 eigrp 1*** – включение процесса EIGRP IPv6 на интерфейсах Маршрутизатор0.

1. Аналогичным образом настройте OSPFv3 на Маршрутизатор1, а затем проверьте связь ПК1-Сервер1 и ПК0-Сервер0.

## Заключение

Хотя основной причиной перехода на использование в сетях протокола IPv6 является потребность в большем количестве IP-адресов, протокол IPv6 также содержит ряд других привлекательных функций и средств миграции. Ниже перечислены некоторые из них:

* службы назначения адресов – назначение адресов в протоколе IPv6 облегчает повторную нумерацию, динамическое выделение адресов и их восстановление, а также удобные функции для мобильных устройств, позволяющие перемещаться и сохранять свои IP-адреса (таким образом устраняется необходимость в закрытии и повторном открытии приложения);
* агрегирование – огромное пространство адресов протокола IPv6 значительно облегчает агрегирование блоков адресов в Интернете;
* отсутствие необходимости в применении трансляции NAT/PAT –использование на всех устройствах, открытых зарегистрированных уникальных адресов, устраняет необходимость в трансляции NAT/PAT, а также снимает проблемы VPN-туннелирования, вызываемые использованием NAT;
* IPsec – В протоколе IPv6 обязательно используется эта технология;
* усовершенствованный заголовок – в заголовок IPv6 внесены некоторые улучшения по сравнению с протоколом IPv4. В частности, маршрутизаторам теперь не нужно заново вычислять контрольную сумму заголовка для каждого пакета, что уменьшает служебную нагрузку при обработке пакета. Кроме того, заголовок содержит метку пакета, позволяющую легко идентифицировать пакеты, пересылаемые по одному и тому же соединению протокола TCP или UDP.

Происходящий во всем мире переход от технологии IPv4 к IPv6 будет не единичным событием и даже не событием года. Скорее, это будет долгий процесс, который уже начался. У сетевых инженеров возникла и растет потребность в более глубоком изучении протокола IPv6, так как после того, как адресное пространство в IPv4 закончится, два стека протоколов IPv4 и IPv6 будут использоваться параллельно (dual stack), с постепенным увеличением доли трафика IPv6 по сравнению с IPv4, что в итоге должно привести к полному и окончательному переходу на IPv6.

## Контрольные задания

1. Модифицировать задание №1 из Лабораторной работы №7. Реализуйте двойной стек IPv4/IPv6 на всех маршрутизаторах (R1 – R4), а также настройте протокол RIPng для маршрутизации трафика между локальными сетями (LAN1 – LAN5).
2. Модифицировать задание №2 из Лабораторной работы №7. Реализуйте двойной стек IPv4/IPv6 на всех маршрутизаторах (R1 – R4) и коммутаторах третьего уровня (S1-S2), а также настройте протокол EIGRP IPv6 для маршрутизации трафика между локальными сетями (LAN1 – LAN4).
3. Модифицировать задание №3 из Лабораторной работы №7. Реализуйте двойной стек IPv4/IPv6 на всех маршрутизаторах (R1 – R5), а также настройте протокол OSPFv3 для маршрутизации трафика между локальными сетями (LAN1 – LAN4).
4. Модифицировать задание №4 из Лабораторной работы №7. Реализуйте двойной стек IPv4/IPv6 на всех маршрутизаторах (R1 – R6) и коммутаторах третьего уровня (S1-S2), а также настройте протокол OSPFv3 для маршрутизации трафика между локальными сетями (LAN1 – LAN4).

# Аттестационный проект

## Цели и задачи

Главная цель аттестационного проекта – проверить знания, полученные при выполнении комплекса из двенадцати лабораторных работ, представленных в данном учебно-методическом пособии. Задания, которые предлагается выполнить, направлены на закрепление изученного материала по проектированию и построению компьютерных сетей.

Аттестационный проект представляет собой законченный проект корпоративной сети, смоделированный в Cisco Packet Tracer на логическом и физическом рабочих пространствах. Все устройства в сети по умолчанию должны иметь связь друг с другом, а также удовлетворять всем ограничениям, связанным с их физическим расположением.

Ниже приведен перечень полезных советов, которых стоит придерживаться при работе над аттестационным проектом:

* Ознакомьтесь с описанием различных процессов моделирования в Cisco Packet Tracer. Описание доступно из программы по следующему пути: Справка ⇒ Содержимое ⇒ раздел «Моделирование».
* После добавления новых устройств в проект полезно сразу же расположить их на физическом рабочем пространстве.
* Если некоторые устройства после расположения на физическом рабочем пространстве теряют связь с остальной сетью, то решением данной проблемы может служить добавление коммутатора, который будет играть роль ретранслятора для этих устройств.
* Для более детального изучения процесса расположения устройств на физическое рабочее пространство используйте справку Packet Tracer: Справка ⇒ Содержимое ⇒ раздел «Рабочее пространство ⇒ Физическое Рабочее Пространство.
* Тщательно проектируйте списки доступа при выполнении заданий по NAT и VPN, важно чтобы ACL не обрабатывали одинаковый трафик, одна технология будет мешать работе другой.
* Используйте расширенную команду ping для проверки связи между устройствами, очень часто возникают ситуации, при которых стандартных четырех echo-запросов бывает недостаточно.
* Используйте режим симуляции для отслеживания ошибок в настройке сети. Он помогает локализовать сегмент сети, в котором происходит потеря данных.

## Задания проекта

### Проектное задание №1

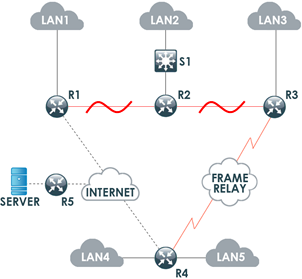


Рис. .. Схема сети задания №1

1. Во всех локальных сетях разбить устройства по VLAN. Настроить статические VLAN-магистрали и VTP-домены.
2. Настроить отказоустойчивые связи с коммутатором S1 по технологии резервации каналов. Включить RSTP, PortFast, BPDUGuard.
3. Организовать эффективное деление узлов по подсетям в локальных сетях, настроить DHCP-серверы.
4. Ограничить связь LAN1 и LAN3 с помощью ACL по протоколам FTP, SMTP, POP3. Настроить подключение по Telnet для S1 и ограничить его для всех узлов, кроме узлов из LAN2.
5. Реализовать динамическую маршрутизацию по протоколу RIP. Настроить DNS-сервер, а также корпоративную почту.
6. Настроить PAT для маршрутизаторов R1 и R4. Для серверов в локальных сетях настроить статический NAT.
7. Настройте связь LAN3-LAN4 и LAN3-LAN5 по технологии Frame Relay без использования подинтерфейсов.
8. Создать VPN-туннели для следующих сетей: LAN1 – LAN4, LAN1 – LAN5, LAN2 – LAN4, LAN2 – LAN5. Параметры VPN-туннелей: алгоритм шифрования – DES, алгоритм хэширования – MD5.
9. В LAN2 настроить беспроводную сеть, для LAN1, LAN2 и LAN3 реализовать двойной стек IPv4/IPv6, а также настроить RIPng.

### Проектное задание №2

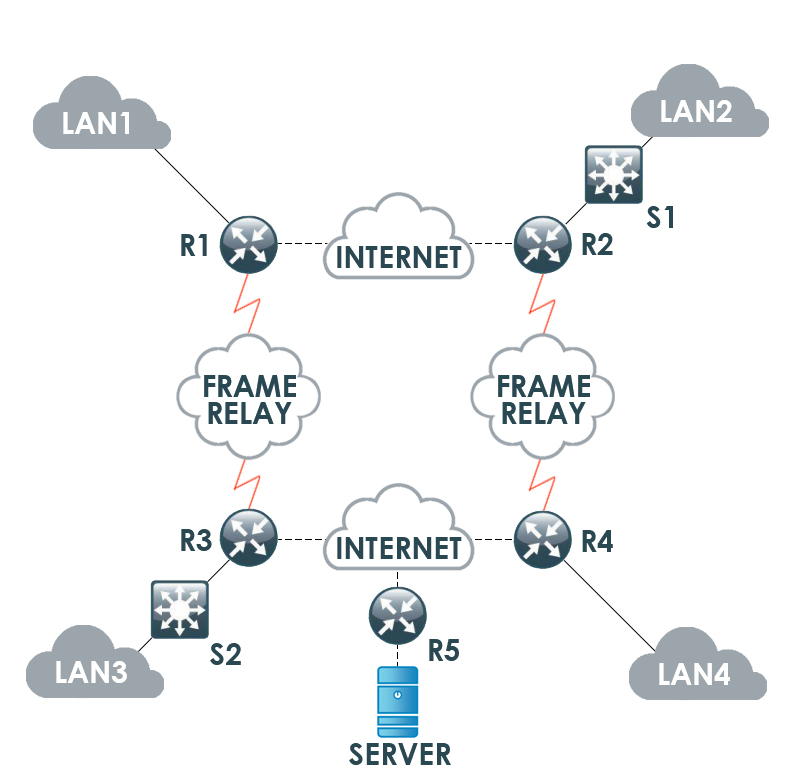


Рис. .. Схема сети задания №2

1. Во всех локальных сетях разбить устройства по VLAN. Настроить динамические VLAN-магистрали и VTP-домены.
2. Настроить отказоустойчивые связи с коммутаторами S1 и S2 с помощью статического агрегирования каналов.
3. Организовать эффективное деление узлов по подсетям в локальных сетях, настроить DHCP-серверы.
4. Закрыть возможность пользования корпоративной почтой для LAN4, закрыть доступ в Интернет для LAN1 с помощью ACL.
5. Реализовать динамическую маршрутизацию по протоколу EIGRP, настроить аутентификацию. Настроить DNS- и EMAIL-серверы.
6. Настроить PAT для маршрутизаторов R3 и R4. Выбрать группу пользователей из LAN3 и настроить для них динамический NAT.
7. Настройте связь LAN1-LAN2 и LAN2-LAN4 по технологии Frame Relay без использования подинтерфейсов.
8. Создать VPN-туннели для следующих сетей: LAN1 – LAN2, LAN3 – LAN4. Параметры VPN-туннелей: алгоритм шифрования – AES, алгоритм хэширования – SHA.
9. В LAN2 и LAN3 настроить беспроводные сети, в LAN3 реализовать двойной стек IPv4/IPv6.

### Проектное задание №3

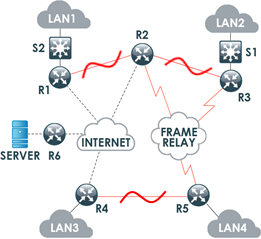


Рис. .. Схема сети задания №3

1. Во всех локальных сетях разбить устройства по VLAN. Настроить статические VLAN-магистрали и VTP-домены.
2. Настроить отказоустойчивые связи с коммутаторами S1 и S2 с помощью динамического агрегирования каналов по LACP.
3. Организовать эффективное деление узлов по подсетям в локальных сетях, настроить DHCP-серверы.
4. Ограничить связь LAN1 и LAN2 с помощью ACL по протоколам HTTP, TFTP, SNMP. Настроить подключение по Telnet для S1 и S2, выделить группу администраторов из LAN1 для которых разрешить такие подключения, остальным запретить.
5. Реализовать динамическую маршрутизацию по протоколу OSPF. Настроить DNS-сервер, а также корпоративную почту.
6. Настроить PAT для маршрутизаторов R1, R2 и R4. Для серверов в локальных сетях настроить статический NAT.
7. Реализуйте полносвязную топологию Frame Relay с использованием подинтерфейсов.
8. Создать VPN-туннели для следующих сетей: LAN1 – LAN3, LAN1 – LAN4, LAN2 – LAN3, LAN2 – LAN4. Параметры VPN-туннелей: алгоритм шифрования – 3DES, алгоритм хэширования – MD5.
9. В LAN1 и LAN2 настроить беспроводную сеть, для LAN3 и LAN4 реализовать двойной стек IPv4/IPv6, а также настроить OSPFv3.

### Проектное задание №4

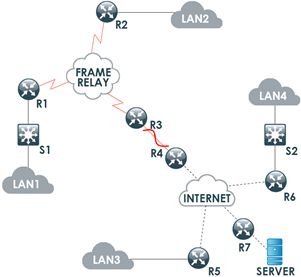


Рис. .. Схема сети задания №4

1. Во всех локальных сетях разбить устройства по VLAN. Настроить статические VLAN-магистрали и VTP-домены.
2. Настроить отказоустойчивые связи с коммутаторами S1 и S2 с помощью динамического агрегирования каналов по PAgP.
3. Организовать эффективное деление узлов по подсетям в локальных сетях, настроить DHCP-серверы.
4. Закрыть доступ в Интернет для группы узлов из LAN3 и LAN4 с помощью ACL. Ограничить связь между LAN1 и LAN3.
5. Реализовать динамическую маршрутизацию по протоколу OSPF. Настроить DNS-сервер, а также корпоративную почту.
6. Настроить PAT для маршрутизаторов R4, R5 и R6. Выбрать группу пользователей из LAN4 и настроить для них динамический NAT.
7. Реализуйте полносвязную топологию Frame Relay с использованием подинтерфейсов.
8. Создать VPN-туннели для следующих сетей: LAN1 – LAN3, LAN1 – LAN4, LAN2 – LAN3, LAN2 – LAN4, LAN3 – LAN 4. Параметры VPN-туннелей: алгоритм шифрования – AES, алгоритм хэширования – MD5.
9. В LAN1 и LAN4 настроить беспроводную сеть, в LAN4 реализовать двойной стек IPv4/IPv6.

## Легенда

|  |  |
| --- | --- |
| Термин | Описание |
|  | Локальная вычислительная сеть |
|  | Коммутатор третьего уровня |
|  | Маршрутизатор |
|  | Глобальная сеть Интернет |
|  | Кабель «Медный перекрестный» |
|  | Волоконно-оптический кабель |
|  | Кабель «Медный прямой» |
|  | Облако провайдера Frame Relay |
|  | Серийный кабель DCE/DTE |

Заключение

В данном учебно-методическом пособии были рассмотрены основные методы проектирования и построения компьютерных сетей. В частности, были решены вопросы первичной и основной сегментации сети (виртуальные локальные сети VLAN и IP-подсети), обеспечения отказоустойчивости соединений на важных участках (резервирование каналов связи в связке с использованием протоколов STP и RSTP, технология агрегирования каналов EtherChannel), а также настройки статической и динамической маршрутизации в локальных сетях, использующих коммутаторы третьего уровня или маршрутизаторы Cisco. Некоторые из предложенных для изучения тем касались проблем обеспечения безопасности сети (списки управления доступом, конфигурация режимов аутентификации в протоколах OSPF и EIGRP). Также были описаны два наиболее популярных способа организации распределенных компьютерных сетей – Frame Relay и VPN. В заключение, рассматривались варианты решения глобальной проблемы нехватки адресного пространства протокола IPv4 (использование трансляции сетевых адресов NAT, переход на использование протокола IPv6 путем внедрения технологии двойного стека). После выполнения лабораторных работ и контрольных заданий, у студента должны сформироваться базовые практические навыки, необходимые для эффективного развертывания небольших и средних корпоративных сетей.

Знания, полученные из данного учебно-методического пособия возможно применять в ходе подготовки к экзамену для получения профессиональной сертификации Cisco – CCENT (Сіsco Certified Entry Networking Technician - Сертифицированный Техник Сетей Cisco) или CCNA (Cisco Certified Network Associate – Сертифицированный Cisco Сетевой Специалист). Данные сертификации - первые и самые популярные среди всех сертификаций Cisco, они являются весомым аргументом в пользу подтверждения квалификации сотрудника при трудоустройстве. В дальнейшем, специалисты Cisco имеют возможность получать более высокие ступени сертификаций при должном совершенствовании знаний и навыков.

Стоит отметить, что другие производители сетевого оборудования (D-Link, Huawei и т.п) часто заимствуют синтаксис командного интерфейса Cisco IOS. Этот факт облегчает процесс настройки устройств этих производителей, в том случае если в компьютерных сетях не используется оборудование Cisco.

Библиографический список

1. Боллапрагада В., Мэрфи К. Структура операционной системы Cisco IOS / В. Боллапрагада, К. Мэрфи, Р. Уайт. – М.: Вильямс, 2002. – 208с.
2. Бройдо В. Л. Вычислительные системы, сети и телекоммуникации / В. Л. Бройдо – СПб.: Питер, 2003. – 688 с.: ил.
3. Бэрри Н. Компьютерные сети: Бэрри Нанс. Пер. с англ.- М.: Восточная Книжная Компания, 1996. – 400 с.: ил.
4. Гук М. Аппаратные средства локальных сетей. Энциклопедия / М. Гук, - СПб.: Питер, 2004. – 573 с.: ил.
5. Иванов В. Компьютерные коммуникации. Учебный курс. Иванов В. – СПб.: Питер 2002. – 224 с.: ил.
6. Кульгин М. В. Компьютерные сети. Практика построения. Для профессионалов. 2-е изд. / М. В. Кульгин. СПб.: Питер, 2003. 462 с.: ил.
7. Леммл Т. Cisco Certified Network Associate. Учебное руководство / Леммл Т. – 2-е изд. М.: Лори, 2002. – 576
8. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 / Одом У. – 2-е изд. М.: Вильямс, 2010. – 672с.
9. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND2 / Одом У. – 2-е изд. М.: Вильямс, 2011. – 736с.
10. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. 3-е изд./ В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 2006. – 958 с.: ил.
11. Олифер В. Г., Олифер Н. А. Основы сетей передачи данных: курс лекций: учебное пособие / Издание второе / В. Г. Олифер, Н. А. Олифер / - М.:ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2005. – 176 с.
12. Таненбаум Э. Компьютерные сети. 4-е изд. / Э. Таненбаум. – СПб.: Питер, 2003. – 992 с.: ил.
13. Уэнстром М. Организация защиты сетей Cisco / Уэнстром М. – М.: Вильямс, 2005. – 768с.

**Егоров Александр Николаевич***,* канд. техн. наук

**Журавлев** **Антон Евгеньевич***,* канд. техн. наук

**Базунов Александр Альбертович**

**Румянцев Олег Валерьевич**

**МОДЕЛИРОВАНИЕ**

**КОМПЬЮТЕРНЫХ СЕТЕЙ**

*Учебно-методическое пособие*



199106, Санкт-Петербург, 22-я линия, 9

тел./факс 812 -322-33-42, 322-77-26

e-mail:izdat@gumrf.ru

|  |  |
| --- | --- |
| Ответственный за выпуск:  Редактор:  Компьютерная верстка: | Сатикова Т.Ф.  . |

Подписано в печать \_\_\_\_\_\_\_\_\_\_\_\_\_

Формат 60x90/16. Бумага офсетная. Гарнитура Times New Roman

Усл. печ. л. \_\_\_\_Тираж 100 экз. Заказ №\_\_\_\_\_\_\_