МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
ОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
им. Ф.М. ДОСТОЕВСКОГО

Д.Н. Лавров

ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО КОММУТАЦИИ И МАРШРУТИЗАЦИИ

Омск

ИЗДАТЕЛЬСТВО
ОМСКОГО ГОСУДАРСТВЕННОГО
УНИВЕРСИТЕТА

2013

УДК 004.7
ББК 32.973.202
Л 136

Рекомендовано к изданию
редакционно-издательским советом ОмГУ

Рецензенты:
д-р физ.-мат. наук, проф. *С. И. Горлов*,
канд. техн. наук *Д. М. Бречка*

Лавров, Д.Н.

Л 136 Лабораторный практикум по коммутации и маршрутизации / Д.Н. Лавров. – Омск : Изд-во Ом. гос. ун-та, 2013. – 99 с.

ISBN 978-5-7779-1563-4

Лабораторный практикум разработан для поддержки курсов, читаемых в рамках академической программы «Сетевая академия Cisco», и нацелен на выработку базовых навыков управления сетевым оборудованием. Практикум призван стать помощником и путеводителем в освоении сетевых технологий.

Для студентов очной и заочной форм обучения, изучающих дисциплины «Коммутация и маршрутизация» и «Удалённый доступ и компьютерные сети», специальностей «Компьютерная безопасность» и «Вычислительные машины, комплексы, системы и сети», направлений подготовки «Информационная безопасность», «Информатика и вычислительная техника», «Прикладная информатика».

УДК 004.7
ББК 32.973.202

ISBN 978-5-7779-1563-4

Оглавление

Предисловие

Данный практикум лабораторных работ создан для поддержки курсов, читаемых в рамках программы «Сетевая академия Cisco»[1]. Хотя большинство лабораторных работ можно выполнить на симуляторах без консультаций преподавателя, это не означает, что настоящая книга является самоучителем. Нет, без «живого» железа и непосредственного общения с преподавателем обучение будет неполным и незавершённым. Кроме того, некоторые работы невозможно выполнить без предварительной подготовки преподавателем самой лабораторной.

Практикум призван стать помощником и путеводителем в освоении сетевых технологий. Лабораторные работы охватывают все основные темы программы «Сетевая академия Cisco», вырабатывают основные базовые навыки работы с сетевым оборудованием. Это экспресс-курс, программа-минимум, книга «Это должен знать каждый» для сетевых администраторов[2].

Каждая лабораторная состоит из трёх основных разделов: «Методический материал» — основные теоретические сведения для проведения лабораторных работ; «Задания к лабораторной работе» — задания, необходимые для закрепления теоретического материала; «Контрольная работа» — вопросы по теории предыдущих и текущей лабораторных или по материалу, важному с теоретической точки зрения, но не вошедшему в методические части предыдущих лабораторных.

Если Вы зачислены в Сетевую академию Cisco, то большинство лабораторных можете выполнить на базе лаборатории коммутации и маршрутизации ФКН ОмГУ. В домашних условиях можно использовать симулятор Cisco PacketTracer или оболочку GNS3 для виртуальной машины Dynamips[3]. Симулятор Cisco PacketTracer достаточен для большинства лабораторных, но многие команды в нём не реализованы, поэтому выполнение лабораторных в симуляторе необходимо подкреплять выполнением лабораторных на реальном оборудовании сетевой лаборатории.

---

[1] URL: `http://cisco.netacad.com`

[2] Так называлась книга по гражданской обороне, изданная в СССР, URL: `http://wasteland.ag.ru/other/civil-defence/manuals/instruction.pdf`

[3] Использование GNS3 предполагает, что у Вас имеется лицензионная версия Cisco IOS, поддерживаемая Dynamips.

Глава 1
Знакомство с оборудованием

1.1. Методический материал

Цель лабораторной — ознакомить слушателей с оснащением лаборатории, рассмотреть основные виды её сетевых устройств, изучить устройство маршрутизаторов и коммутаторов, виды и назначение их интерфейсов, ознакомиться с интерфейсом командной строки консоли управления сетевым устройством.

Лаборатория коммутации маршрутизации факультета компьютерных наук ОмГУ оснащена следующим оборудованием:

1. Маршрутизаторы Cisco 2620 — 2 шт.
2. Маршрутизатор Cisco 2621 — 1 шт.
3. Маршрутизаторы Cisco 2801 — 3 шт.
4. Маршрутизаторы Cisco 871 — 5 шт.
5. Маршрутизаторы Cisco 851 — 1 шт.
6. Коммутаторы Cisco Catalyst 2950 — 3 шт.
7. Коммутатор D-Link — 1 шт. Используется для поддержания связности компьютеров лаборатории
8. Концентратор D-Link — 1 шт. Историческая реликвия, используется в лабораторных по перехвату и анализу трафика и балансировки нагрузки.
9. Персональные компьютеры с установленной на них операционной системой Ubuntu — 20 шт.

1.1.1. Устройство маршрутизатора

Маршрутизатор Cisco представляет собой специализированный компьютер, оснащённый специализированной операционной системой Cisco IOS (Internetwork Operation System). Архитектура операционной системы разработана для быстрого выполнения задач третьего (сетевого) уровня модели OSI (Open System Interconnection). Первая задача — это задача маршрутизации: выбор оптимального пути следования пакета данных. Вторая задача — это задача коммутации пакета: определение связи между оптимальным маршрутом и собственным интерфейсом маршрутизатора и перенаправления пакета на этот интерфейс.

Как и любой компьютер, маршрутизатор в общих чертах, конечно,

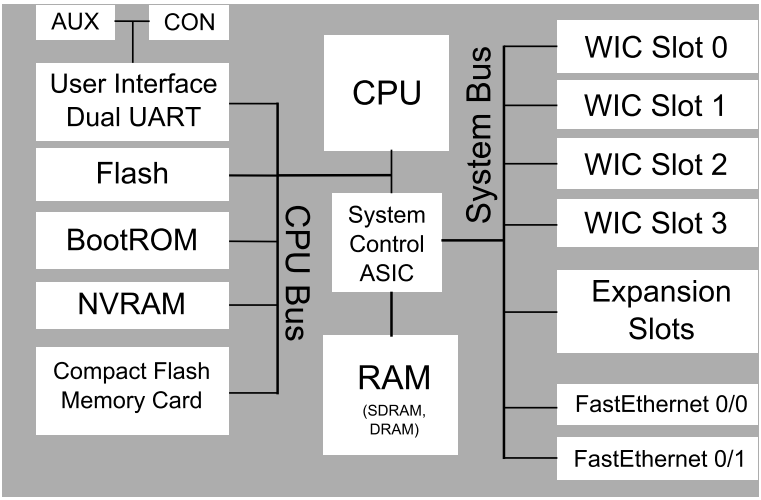


Рис. 1.1. Логическая схема устройства маршрутизатора

можно представлять как вычислительное устройство следующей архитектуры. Имеется две шины: шина процессора и системная шина. К *шине процессора* (CPU Bus) подключены: трансмиттер для поддержки работы управляющих портов (консольного — con и дополнительного — aux), карт памяти flash, постоянной памяти ROM, системой контроля потоков данных между памятью, интерфейсами и центральным процессором. К системе контроля потоков данных подключена и оперативная память.

К *системной шине* (System Bus) подключены все сетевые интерфейсы и упомянутая система контроля потоков данных.

Обобщённую логическую схему компонент маршрутизатора можно увидеть на рис. 1.1. Обобщённая схема построена на основе схем [1, с.17] и [2, с.7] маршрутизаторов серий 1800 и 2600.

1.1.2. Виды памяти

Итак, маршрутизатор имеет четыре вида памяти:

1. Оперативная память RAM (Random Access Memory) — содержит развёрнутый образ операционной системы, файл текущей конфигурации `running-config`, таблицы маршрутизации, запущенные процессы, кэши маршрутов, ARP-кэш, буфер приёма/передачи IP-пакетов и другую информацию, требующую оперативной обра-

ботки.

2. Постоянная ROM или BootROM (Read Only Memory) — вид постоянной памяти, в которой прошиваются инструкции начального загрузчика, урезанная версия IOS, программное обеспечение для тестирования оборудования (процедура POST — Power On Self Test).
3. Flash — энергонезависимая, как и ROM, память, которая хранит сжатый запакованный образ операционной системы. Может быть перезаписана. Flash играет роль жесткого диска обычного компьютера.
4. NVRAM (Nonvolatile RAM) — энергонезависимая оперативная память. Хранит настройки маршрутизатора, применяемые после включения питания или перезагрузки. Файл с настройками называется `startup-config`. Память перезаписываемая.

1.1.3. Сетевые интерфейсы

В маршрутизаторах серии 2800 в лабораторных условиях обычно используются два типа сетевых интерфейсов. Первый тип — это WAN Interface Card (WIC), последовательный интерфейс. Он предназначен для передачи данных в глобальных распределённых сетях (WAN). Карты WIC, установленные в маршрутизаторы лаборатории, имеют маркировку WIC 2A/S, что означает, что они имеют два порта и способны вести передачу до 128 кб/с в синхронном или асинхронном режиме.

Внутренняя нумерация интерфейсов (изнутри Cisco IOS) — двухуровневая для серии 2600 и трёхуровневая для серии 2800. В трехуровневой нумерации первая цифра означает тип интерфейса. Для WIC-карт и VIC-карт (Voice Interface Card) — это цифра 0. Тип определяется производителем и может быть уточнён в документации маршрутизаторов. В нашем случае это поле практически всегда будет иметь значение ноль. Вторая цифра — это номер слота. Слоты нумеруются справа налево, начиная с ноля. Обычно они подписаны и поиск номера не вызывает трудностей. Третий номер — номер порта на сетевой карте. Порты нумеруются снизу вверх. Например: Serial 0/2/1 означает, что интерфейс относится к WIC или VIC картам, карточка вставлена во второй слот и интерфейс связан с первым портом.

Двухуровневая нумерация аналогична, но не использует поле «тип интерфейса».

Второй тип сетевых интерфейсов, предназначенных для передачи данных, — это FastEthernet-интерфейсы. Они имеют внутренние имена

Рис. 1.2. Переходник USB – COM (RS232)

FastEthernet 0/0 и FastEthernet 0/1 и соответствующую маркировку на корпусе маршрутизатора.

1.1.4. Интерфейсы управления

К интерфейсам управления относятся консольный (CONsole) и дополнительный (AUXulary) порты[1].

Консольный порт помечен голубым цветом. Консольный порт соединяется через rollover кабель голубого цвета с последовательным портом (COM-портом) компьютера. С помощью специальных программ эмуляции терминала можно через этот порт передавать коды нажатых клавиш на клавиатуре компьютера и отображать на его экране компьютера сообщения маршрутизатора.

Две наиболее часто используемые программы — это стандартная утилита Windows Hyperterminal и мультиплатформенная утилита Putty. Для подключения необходимо указать номер COM-порта (н-р. COM1 или COM2) и скорость подключения 9600.

В современных компьютерах выводы COM-портов могут отсутствовать. В этом случае следует приобрести специальные переходники USB-COM (рис. 1.2).

[1]Слово «порт» очень многозначно. В данном контексте имеется в виду сетевой интерфейс.

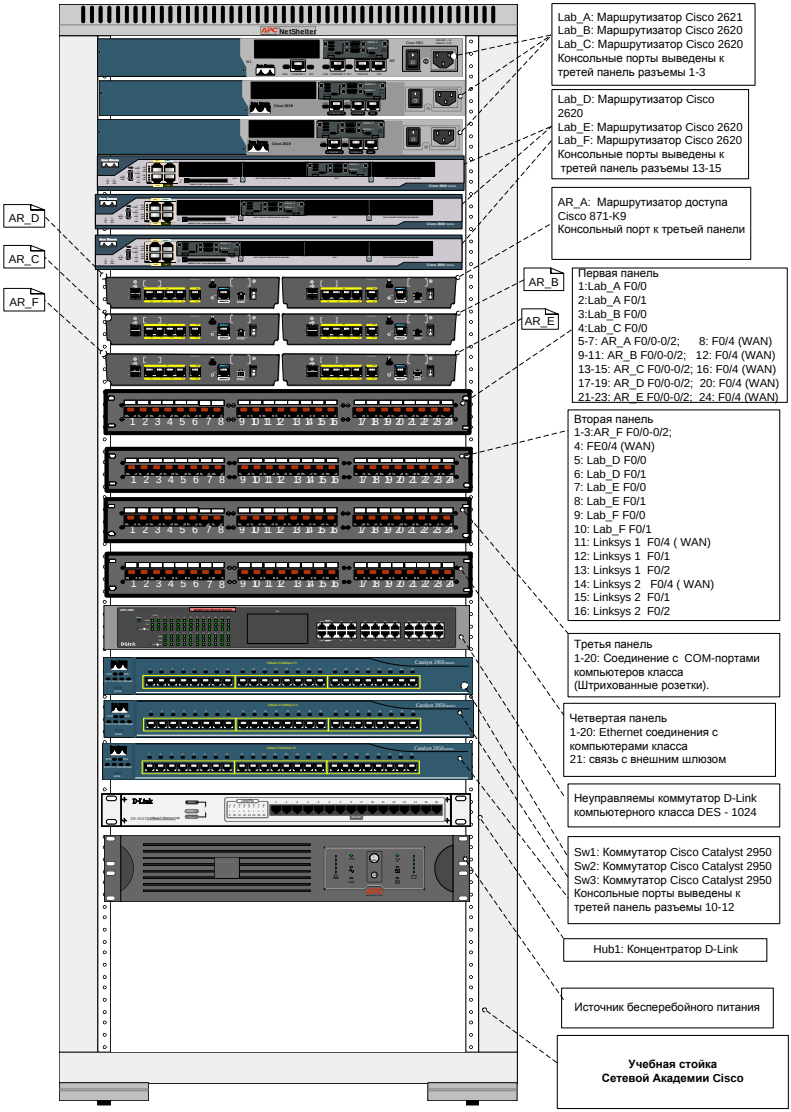


Рис. 1.3. Схема размещения оборудования в стойке лаборатории

Дополнительный порт, или AUX-порт, используется аналогично консольному, но в отличие от него требует предварительной настройки в Cisco IOS. AUX-порт имеет ограничения: через него нельзя выполнять ряд системных операций, таких, как сброс пароля и восстановление повреждённого образа Cisco IOS.

1.1.5. Устройство лаборатории коммутации и маршрутизации

Всё сетевое оборудование размещается в закрытой стойке. В компьютерном классе возле каждого компьютера размещены две розетки. Каждая пара розеток имеет свой номер. Первая нумеруется цифрой – порядковым номером, а вторая — порядковым номером и штрихом. Нумерованная розетка предназначена для локальной сети FastEthernet, штрихованная — для консольного подключения к сетевым устройствам.

В стойке установлены четыре коммутационные панели. Нумерация устройств и панелей ведётся сверху вниз. Нумерация слотов маршрутизатора ведётся справа налево. Нумерация портов коммутаторов — слева направо. В самую нижнюю, четвертую коммутационную панель, выведены концы кабеля от нумерованных розеток так, что номер розетки совпадает с номером разъёма коммутационной панели. Прямым кабелем через эту четвертую коммутационную панель все компьютеры заведены в неуправляемый коммутатор D-Link, для поддержания работоспособности компьютерного класса.

Штрихованные розетки выведены в третью консольную коммутационную панель аналогичным образом: номер штрихованной розетки соединён с соответствующим гнездом коммутационной панели с тыльной стороны. С лицевой стороны прямым кабелем розетка заведена непосредственно в консольный порт какого-либо устройства.

Первая и вторая коммутационные панели предназначены для подключения FastEthernet интерфейсов маршрутизаторов. Кабель из FastEthernet интерфейсов заведён с тыльной стороны в коммутационную панель.

С помощью дополнительных кроссовых пачкордов, соединяя гнёзда первой или второй коммутационной панели с гнёздами четвёртой панели, можно создать соединение любого компьютера с любым маршрутизатором.

Схема подключений дана на рис. 1.3. Кроме схемы помочь разобраться в подключениях помогут надписи на кабелях. Например С4 на кабеле, идущем от маршрутизатора Cisco 871, означает, что кабель предполагается подключить в четвёртый порт консольной (третьей) коммутационной панели. Если на кабеле стоит маркировка Е20, — это

означает подключение к гнезду первой коммутационной панели, а E26 — ко второму гнезду второй коммутационной панели (всего в панели 24 гнезда, второй номер получается продолжением сквозной нумерации на вторую панель: $26 - 24 = 2$).

1.1.6. Интерфейс командной строки CLI

Будем считать, что мы уже подключились к маршрутизатору через консольный порт. После включения маршрутизатора происходит загрузка Cisco IOS[1]. После загрузки мы попадаем в интерпретатор командной строки (CLI — Command Line Interface). Если на маршрутизаторе установлены заводские настройки (то есть никто его не пытался ещё настроить, `startup-config` отсутствует или пуст), то предлагается диалог для настройки маршрутизатора. Если Вы хотите отказаться от него и выполнить настройку вручную, то следует на первый вопрос ответить NO или нажать сочетание клавиш `Ctrl+C`. После этого мы попадаем в пользовательский режим командной строки (User EXEC Mode). Подсказка командной строки будет выглядеть при этом следующим образом: `Router>`.

В этом режиме можно выполнять всего лишь некоторые диагностические команды. Полный список команд пользовательского режима можно увидеть, если набрать в командной строке символ `"?"`.

Одна из команд этого режима переводит нас в так называемый привилегированный режим (Privileged EXEC Mode). Это команда `enable`. Подсказка командной строки привилегированного режима будет выглядеть при этом так `Router#`. В этом режиме можно получить доступ к расширенному списку команд, который позволяет перезагружать маршрутизатор, сохранять внесённые на нем изменения конфигурации, устанавливать время внутренних часов, переходить в режим конфигурирования и т.д.

Для перехода в режим конфигурирования с терминала используется команда `configure` с параметром `terminal`. При входе в режим конфигурирования изменяется подсказка командной строки, теперь она выглядит так: `Router(config)#`.

Из режима глобального конфигурирования можно попасть в другие подрежимы конфигурирования: режим конфигурирования подключений, режим конфигурирования маршрутизации, режим конфигурирования интерфейса и т.п.

[1]Подробнее о процессе загрузки будет рассказано в следующих разделах.

Таблица 1.1. «Горячие» клавиши редактирования командной строки

Комбинация клавиш	**Описание**
Tab	Позволяет по сокращению подобрать подходящую команду
Ctrl+A	Переместиться на начало командной строки
Ctrl+Z	Выход из режима конфигурирования
Ctrl+N	Отобразить первую выполненную команду из кэша
Ctrl+P или ↑	Отобразить последнюю выполненную команду
Ctrl+Shift+6	Прервать выполняемую операцию (например, ping)
Ctrl+Break	Прервать нормальный ход загрузки IOS, переход в режим rommon
Ctrl+F или →	Переместиться вперед на один символ
Ctrl+B или ←	Переместиться назад на один символ
Esc+F	Переместиться вперед на одно слово
Esc+B	Переместиться назад на одно слово
Ctrl+E	Переместиться в конец командной строки

```
Router>enable
Router#configure terminal
Router(config)#line console 0
Router(config-line)#line console 0
Router(config-line)#exit
Router(config)#interface FastEthernet 0
Router(config-if)#end
Router#
```

Упрощённая схема переходов представлена на рис. 1.4.

1.1.7. Основные команды

В табл. 1.1 представлены основные сочетания клавиш, используемые при редактировании командной строки.

Следующая таблица 1.2 содержит сводку наиболее часто используемых команд.

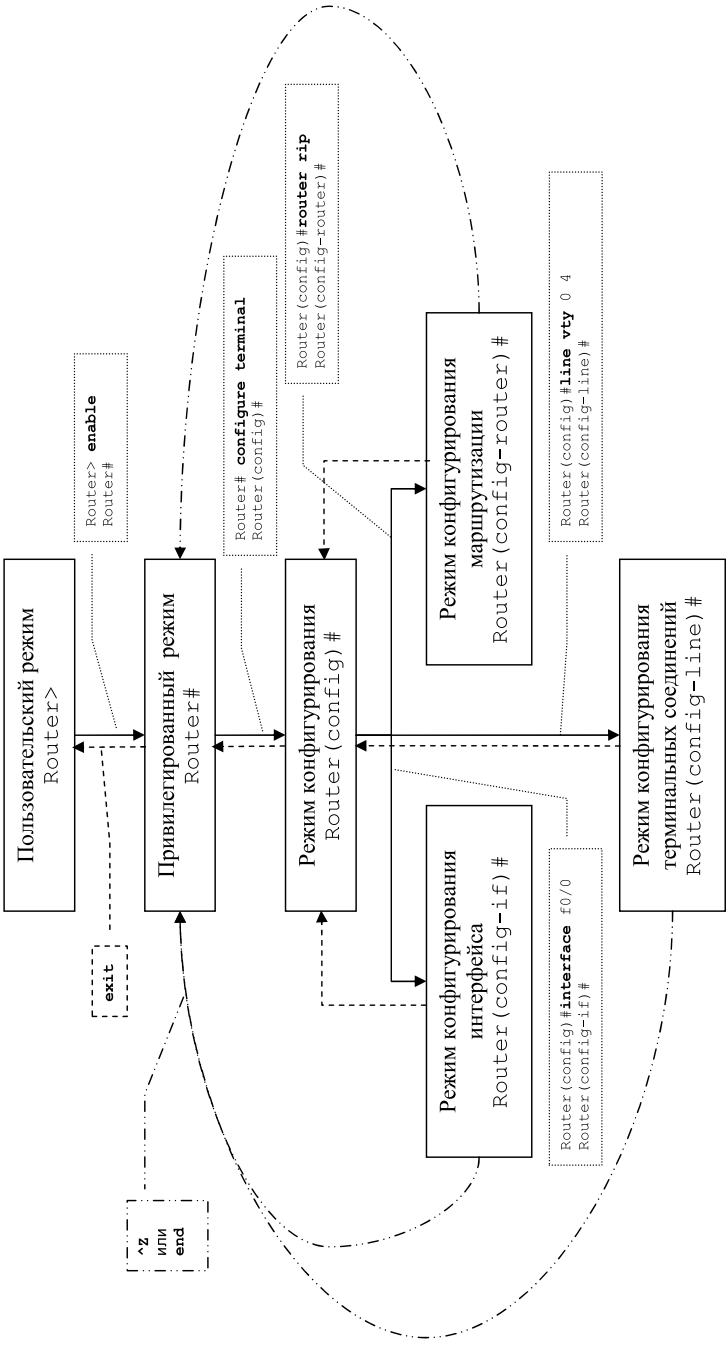


Рис. 1.4. Навигация по иерархической структуре CLI

Таблица 1.2. Наиболее часто используемые команды

Команда	**Режим**	**Описание**
?	любой	Определение параметров команды, если используется без команды, то показывает доступные в текущем режиме команды
show ip interface	#	Показывает настройки и состояние ip- интерфейсов
show	любой	Команда диагностики, показывающая различные настройки системы
show ip interface brief	#	то же самое в кратком варианте
show history	любой	Показать историю выполненных команд
show ip route	#	Показывает таблицу маршрутизации
terminal history size	(config)#	Установить размер кэша выполненных команд
show arp	#	Показывает arp-кэш
terminal no editing	(config)#	Отключает расширенные возможности редактирования
show controllers	#	Показывает состояние всех физ. контроллеров
terminal editing	(config)#	Включает расширенные возможности редактирования
show protocol	#	Показывает состояния и настройки запущенных протоколов
clock set	#	Установка времени
show running-config	#	Показывает текущую конфигурацию
enable	>	Переход в привилегированный режим
show startup-config	#	Показывает конфигурацию по умолчанию
configure terminal	#	Переход в режим конфигурирования

Продолжение на след. странице

Таблица 1.2. Наиболее часто используемые команды (окончание)

Команда	**Режим**	**Описание**
show clock	#	Показывает текущие дату и время
exit	любой	Выход из текущего режима на уровень вверх
banner motd	(config)#	Настраивает приветствие
end	любой	Выход из режима конфигурирования в привилегированный режим
show cdp neighbors	#	Показывает соседей
show version	> #	Показывает версию IOS и конфигурационный регистр
show cdp neighbors detail	#	Показывает детальную информацию о соседях
show flash	#	Показывает содержимое flash
cdp run	(config)#	Запускает протокол CDP
dir	#	Показывает содержимое указанной области памяти
ip http server	(config)#	Запускает web-сервер
show interface	(config)#	Показывает настройки и состояние интерфейсов
no	любой	Отменяет указанные команды
clock rate	(config-if)#	Устанавливает скорость передачи на DCE интерфейсе

1.2. Задания лабораторной работы №1

- **Подключение к маршрутизатору.** Постарайтесь самостоятельно подключиться к консольному порту маршрутизатора. В случае затруднений обратитесь к инструктору (преподавателю).
- **Очистка конфигурации**. Перед выполнением каждой лабораторной работы необходимо очистить файл конфигурации `startup-config` и перезагрузиться для того, чтобы конфигурации, оставшиеся от действий других групп, не влияли на выполнение текущей лабораторной работы. Для этого необходимо войти в привилегированный режим с помощью команды `enable`, ввести команду `erase startup-config`, а затем `reload`. В случае, если система предложит перед перезагрузкой сохранить настройки, следует отказаться.
- **Упражнение №1. Установка времени**. Для правильного ведения журналов событий необходимо, чтобы на маршрутизаторе были правильно установлены внутренние часы. Это можно сделать вручную или с помощью сервера времени и протокола NTP. Сам маршрутизатор также может выступать как в роли клиента, так и сервера времени[1].

  Даже если сервер времени не доступен, можно настроить внутренние часы вручную. В маршутизаторах имеется двое внутренних часов. Одни управляются с помощью команды `clock` (программные часы), а другие — с помощью `calendar` (аппаратные часы). Установите текущее время на 1 сентября 2000 года (часы clock). Результат продемонстрируйте инструктору (преподавателю). Затем установите внутреннее время маршрутизатора на текущее.
- **Упражнение №2. Установка имени хоста**. Найдите в справочной системе режим и команду установки имени маршрутизатора. Установите имя маршрутизатора в соответствии с Вашим собственным именем.
- **Упражнение №3. Описание интерфейса**. Перейдите в режим конфигурирования серийного интерфейса. Дайте описание интерфейса в виде строки `"Connection to Provider"`.

После выполнения сохраните текущую конфигурацию, перезагрузитесь и удостоверьтесь, что внесённые изменения были сохранены.

[1] Настройка протокола NTP входит в курс подготовки к сертификации CCNP. Следующие документы описывают, как это сделать на наших устройствах [9,10].

1.3. Контрольная работа №1. Сетевая модель OSI

ФИО _____ Группа _____

1. Перечислите 7 уровней модели OSI с собственным именем для каждого уровня. Перечислите номер уровня TCP/IP и его правильное название в следующих столбцах. Перечислите термины, используемые для блоков данных протоколов (PDU), а также соответствие с протоколами TCP/IP и утилиты и устройства, которые работают в каждом уровне.

№ OSI	Имя уровня OSI (Рус./Анг.)	№ TCP/IP	Имя уровня TCP/IP (Рус. / Анг.)	PDU (Название блока данных)	Протоколы TCP / IP и стандарты	Утилиты настройки и диагностики
7						
6						
5						
4						
3						
2						
1						

2. Заполните таблицу, основываясь на вашем знании модели OSI.

№ уровня OSI	Функции уровня
7	
6	
5	
4	
3	
2	
1	

Глава 2
Базовая настройка маршрутизатора

2.1. Методический материал

Маршрутизатор без дополнительных настроек выполнять свои основные функции при заводских настройках не способен. Целью лабораторной работы является обучение базовой настройке маршрутизатора.

Настройка маршрутизатора может быть выполнена с помощью мастера (диалогового режима настройки), который запускается автоматически при первом запуске[1]. Мастер может быть вызван вручную с помощью команды `setup` из привилегированного режима.

Для нас полезнее выполнить базовую настройку вручную без использования мастера. Это позволить ближе познакомиться с режимом командной строки и лучше ориентироваться в настройках.

Если после перезагрузки маршрутизатора Вы попали в диалоговый режим настройки, то можете его прервать нажатием <Ctrl+C>. Вход в привилегированный режим для маршрутизаторов осуществляется командой:

```
> enable
#
```

Если необходимо, то Вы можете перейти в режим конфигурирования:

```
# configure terminal
(config)#
```

2.1.1. Настройка времени

Настроить правильно часы на маршрутизаторе нужно для верного ведения журналов событий. Журнал событий — это важный компонент безопасности Вашей сети. Системные программные часы можно настроить вручную или с помощью протокола ntp. Второй способ предпочтительнее, так как он обеспечит синхронизацию часов всех сетевых устройств сети, что существенно упрощает разбор инцидентов.

[1] Диалоговый режим настройки запускается автоматически после перезагрузки, если размещённый в NVRAM файл `startup-config` имеет нулевой размер или отсутствует

Значение времени и даты программных часов можно установить вручную при помощи команды, выполняющейся из привилегированного EXEC режима и имеющей следующий формат:

```
# clock set <чч:мм:сс> <день> <месяц> <год>
```

Часы хранятся в формате UTC (Coordinated Universal Time). Для просмотра текущего времени и даты можно воспользоваться командой `show clock`.

На многих современных маршрутизаторах дополнительно реализованы энергонезависимые (аккумуляторные) аппаратные кварцевые часы. Аппаратное время связано с командой `calendar` и не зависит от питания маршрутизатора: после выключения питания время календаря сохраняется.

```
(config)# calendar set <чч:мм:сс> <день> <месяц> <год>
```

Для просмотра текущего времени и даты аппаратных часов можно воспользоваться командой `show calendar`.

Для задания времени при помощи `clock` существует два параметра конфигурации: `timezone` и `summer-time`. Формат этих команд следующий:

```
(config)# clock timezone
          {<имя временной зоны> |
          <часовой пояс>} [смещение]
(config)# clock summer-time
   {<имя временной зоны> |
    <часовой пояс>}
   recurring <дата-время начала>
        <дата-время конца перехода на летнее время>
```

Команда `clock timezone` используется для задания часового пояса. Команда `clock summer-time` используется для определения начальной и конечной даты перехода на летнее время. `{ }` — условное обозначение для множества парметров, `|` — означает ИЛИ, а `[ ]` — необязательный параметр.

Пример задания часового пояса Omsk: определим смещение в часах от -23 до 23, а также начало и окончание летнего времени[1].

[1] В 2011 году был отменён сезонный перевод часов. Таким образом, омское время (OMST) закрепилось в поясе UTC+7

```
(config)# clock timezone Omsk 7
(config)# clock summer-time Omsk
          recurring last Sun Mar 2:00
                    last Sun Oct 2:00
```

Заданные вручную дата и время системных программных часов сохраняют своё значение только на время непрерывной работы маршрутизатора. После его выключения или перезагрузки установленное ранее время сбрасывается. В маршрутизаторах где есть аппаратные часы (calendar), в момент загрузки маршрутизатора время из аппаратных часов считывается в программные (clock), и далее программные часы работают независимо. Время в программных часах (clock) и в календаре при длительной работе маршрутизатора может отличаться. Для периодической синхронизации аппаратных и программных часов используется команда `clock calendar-valid`.

Для приведения времени к единому значению в границах сети предприятия сети используется ntp (network time protocol). В сети задаются один или несколько мастеров времени (в качестве мастера могут выступать публичные серверы в сети Интернет). Все остальные находящиеся в этой сети маршрутизаторы и коммутаторы при включении устанавливают свои программные часы с мастером и в дальнейшем периодически синхронизируют с ним точное время.

В качестве сервера времени рекомендуется использовать маршрутизатор, имеющий аппаратные часы (calendar). Для создания сервера времени необходимо прописать в конфигурации следующую строку:

```
(config)# ntp master
```

На остальных сетевых устройствах достаточно прописать ссылку на ntp server:

```
(config)# ntp server <ip-адрес сервера времени>
```

Можно указать несколько ntp серверов и выбрать из них более предпочтительного `prefer`:

```
(config)# ntp server <ip сервера_времени1> prefer
(config)# ntp server <ip сервера_времени2>
```

Команда диагностики `show ntp status` отображает информацию о синхронизации.

Команда `show ntp associations` отображает ntp серверы, кто от кого получает время, к какому слою принадлежит маршрутизатор (stratum — чем меньше значение, тем точнее его время) и другие параметры.

По умолчанию в конфигурации маршрутизатора включены сервисы `timestamps debug` и `timestamps log`, которые отображают время события, заносимого в журнал или отображаемого при включении `debug` в формате, привязанном к правильному текущему времени. Если эти сервисы отключены, то рекомендуется их включить:

```
(config)# service timestamps debug datetime localtime
(config)# service timestamps log datetime localtime
```

При выполнении лабораторных применение этих команд необязательно.

2.1.2. Настройка имени хоста

Установка имени маршрутизатора необходима не только для правильной работы ряда сетевых протоколов, использующих его имя в процедурах аутентификации, но и для идентификации маршрутизатора при удалённом подключении. Достигается это с помощью команды конфигурационного режима `hostname`.

Пример

```
> enable
# configure terminal
(config)# hostname Lab_A
```

При вводе возможно сокращение команд и их параметров до однозначной интерпретации. Предыдущий ввод мог выглядеть следующим образом:

```
> en
# conf t
(config)# host Lab_A
(config)# ^Z
```

В дальнейшем будем активно использовать наиболее часто используемые команды в сокращениях.

2.1.3. Базовая настройка безопасности

Простейшая защита маршрутизатора от несанкционированного доступа — это парольная защита. Для ограничения доступа к привилегированному режиму используются две команды конфигурационного режима. Первая `enable password <пароль>` устанавливает пароль для входа в привилегированный режим. Пароль сохраняется в файле текущей конфигурации `running-config` в открытом виде. При хранении файла конфигурации на внешнем tftp-сервере пароль может стать известным злоумышленнику.

Для хранения пароля в файле конфигурации в виде MD5-хэша (односторонняя криптографическая функция) используется команда `enable secret <пароль>`. Так как MD5-функция практически необратима, украв MD5-хэш, злоумышленник потратит неоправданно большое время для раскрытия пароля. Такой способ хранения пароля более безопасен.

При применении обеих команд `enable password` и `enable secret` действует только `enable secret`.

Защита консольного подключения — следующий этап обеспечения парольной защиты. Для этого необходимо войти в режим конфигурирования `conf t`, затем — в режим конфигурирования подключения, указав консоль, `line con 0` (0 — это номер консольной линии, нумерация начинается с нуля; так как подключение одно, то номер единственно верный).

Затем задать пароль `password <пароль>` и дать указание проверять этот пароль при подключении к консоли `login` (без параметров). Команда `login` может применяться и с параметрами `local` или `tacacs`. Первый из параметров указывает на использование локальной базы данных пользователей для аутентификации, второй — отсылает к AAA-серверу, хранящему централизованную базу данных пользователей сетевых устройств. В обоих случаях команда `password <пароль>` при этом будет проигнорирована. В простейшем случае будем использовать команду `login` без параметров.

Пример показывает, как настроить вход на консоль с паролем `cisco`:

```
# conf t
(config)# line con 0
(config-line)# password cisco
(config-line)# login
(config-line)# end
```

Аналогично настраиваются подключения к виртуальным терминалам, только вместо команды `line con 0` нужно использовать команду

```
(config)# line vty <нач номер консоли, обычно 0>
                   <конечный номер консоли, обычно 4>
```

Работа с виртуальным терминалом осуществляется через протоколы telnet (по умолчанию) и ssh.

Пример показывает, как настроить вход на виртуальные терминалы с 0 по 4 с паролем `cisco`:

```
# conf t
(config)# line vty 0 4
(config-line)# password cisco
(config-line)# login
(config-line)# end
```

В конфигурационном файле пароли на консольный вход и виртуальные терминалы хранятся в открытом виде. Для шифрования паролей следует выполнить команду `service password-encryption`. К сожалению, это шифрование ненадёжно и обратимо[1].

2.1.4. Настройка интерфейсов FastEthernet

Ethernet-интерфейсам необходимо назначить ip-адреса в соответствии со схемой распределения и активировать их.

Сначала необходимо войти в режим конфигурирования интерфейса. Это осуществляется командой

```
(config)# interface <имя интерфейса>
```

`<имя интерфейса>` — складывается из его вида (Ethernet, Serial и т.д.), типа (для Serial), номера слота и номера порта на сетевой карте. В нашем случае — это Ethernet 0/0 или Ethernet 0/1. На старых маршрутизаторах нумерация может быть одноуровневая или двухуровневая. Можно использовать сокращения E0/0 или E0/1.

Для просмотра списка имеющихся интерфейсов и их параметров используются команды `show interface` и `show ip interface`. Последнюю можно использовать с параметром `brief`, если необходимо получить только краткую справку.

Назначение ip-адреса осуществляется командой

[1] URL:`http://users.skynet.be/glu/ciscopw.htm`

```
(config-if)#ip address <ip-адрес> <маска>
```

Последнее действие — активация интерфейса. В списке возможных команд режима конфигурирования интерфейса такой команды нет. Но есть две другие, комбинация которых даёт нужный результат, это команды `shutdown` и `no`. Первая `shutdown` — деактивирует интерфейс, а `no` — отменяет действие любой команды, следующей за ней. Следовательно, для активации интерфейса необходимо выполнить команду `no shutdown`.

Пример настройки интерфейса Ethernet 0/0 с адресом 192.168.1.1 маской 255.255.255.0:

```
#conf t
(config)#interface f0/0
(config-if)#ip address 192.168.1.1 255.255.255.0
(config-if)#no shutdown
(config-if)#end
```

2.1.5. Настройка последовательных интерфейсов

Для настройки последовательных интерфейсов используются аналогичные команды с некоторыми дополнениями. Последовательные интерфейсы могут работать в режиме DCE (Data Communication Equipment[1]) или в режиме DTE (Data Terminal Equipment[2]). Определяется режим типом подключаемого провода. Изнутри маршрутизатора тип интерфейса (DTE/DCE) можно узнать командой `show controllers`. В одном последовательном соединении одна сторона всегда DTE, а вторая DCE. DCE-интерфейсы отвечают за скорость передачи данных, и для них необходимо указать, на какой скорости будет работать канал передачи данных.

Пример настройки последовательного DCE-интерфейса Serial 0/2/1 (0 — тип интерфейса; 2 — номер слота; 1 — номер порта на сетевой карте) с адресом 172.16.1.1 маской 255.255.0.0:

```
#conf t
(config)#interface s0/2/1
(config-if)#ip address 172.16.1.1 255.255.0.0
(config-if)#clock rate 128000
(config-if)#no shutdown
```

[1] Оборудование передачи данных.

[2] Терминальное оборудование, оконечное оборудование.

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

2.1.6. Настройка динамической маршрутизации

У маршрутизатора две основные функции: маршрутизация и коммутация пакетов. Для настройки маршрутизации используются статические или динамические маршруты. Первые настраиваются системным администратором. Вторые типы маршрутов вычисляются с помощью динамических протоколов маршрутизации. Одним из таких протоколов является RIP (Route Information Protocol).

RIP работает посредством обмена таблицами маршрутов между маршрутизаторами. Для настройки RIP необходимо создать начальную таблицу обмена: указать те сети, которые непосредственно присоединены к маршрутизатору. Входим в режим настройки протокола маршрутизации `router rip`, затем командой `network <ip-адрес сети>` добавляем все присоединённые сети.

Пример. Предположим, имеется список присоединённых сетей: 192.168.0.0, 172.160.0.0 и 10.0.0.0. Тогда настройка динамической маршрутизации по протоколу RIP будет выглядеть следующим образом:

```
#conf t
(config)#router rip
(config-if)#network  192.168.1.0
(config-if)#network  172.16.0.0
(config-if)#network  10.0.0.0
(config-if)#end
```

2.1.7. Настройка разрешения имён

Разрешение имён может быть настроено вручную или динамически. Для динамической настройки достаточно выполнить следующую последовательность команд:

```
#conf t
! включить разрешение имён
(config)# ip domain-lookup
! включаем внутренний DNS сервер
(config)# ip dns server
! прописываем DNS провайдера
(config)# ip name-server 212.192.35.4
! добавляем несколько
```

```
! публичных DNS серверов для страховки
(config)# ip name-server 4.2.2.2
(config)# ip name-server 8.8.8.8
```

В лабораторных условиях без реально функционирующего dns-сервера и выхода в Интернет такая конфигурация работать не будет. В этом случае может помочь ручная настройка разрешения имён:

```
(config)# ip host <имя хоста> <ip-адрес1>
          [ip-адрес2 [ip-адрес3[...]]]
```

Пример.

```
(config)# ip host Lab_A 192.168.1.1 172.
          [ip-адрес2 [ip-адрес3[...]]]
```

2.1.8. Завершение настройки

Все выполняемые настройки сохраняются в файле `running-config`, который хранится в оперативной памяти. Все данные оперативной памяти очищаются после перезагрузки или потери питания. Файл `running-config` необходимо скопировать в файл `startup-config`, хранимый в NVRAM и используемый для настроек после перезагрузки:

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

Краткое описание базовой настройки:

```
! Входим в привилегированный режим
  >enable

! Установка времени
  # clock set 12:00:00 12 dec 2012

! Установка парольной защиты
! Входим в режим конфигурирования
    # conf t
! Установка пароля для входа в привилегированный режим
    (config)# enable secret <пароль>
! Установка пароля на консоль
! Вход в конфигурирование консоли
    (config)# line console <номер консоли, обычно 0>
! Установить пароль на консольное подключение
    (config-line)# password <пароль>
! Включить проверку паролей при входе через консольный вход
    (config-line)# login
! Вход в конфигурирование  виртуальных терминалов
    (config)# line vty <нач номер консоли, обычно 0>
                       <конечный номер консоли, обычно 4>.
! Включить проверку паролей при входе через telnet
    (config-line) # login
! Установить пароль на telnet подключение к vty
   (config-line)# password <пароль>

! Конфигурирование интерфейсов
! Войти в режим конфигурирования интерфейсов
   (config)# interface <имя интерфейса>
! Задать ip-адрес
   (config-if)# ip address <адрес> <маска>
! Если это интерфейс DCE, то установить скорость передачи
   (config-if)# clockrate <скорость>
! Поднять интерфейс
   (config-if)# no shutdown

! Конфигурирование динамической маршрутизации
! Включить маршрутизацию
   (config)# ip routing
! Войти в режим конфигурирования протокола маршрутизации
   (config)# router <имя протокола> [опции]
! Указать непосредственно подключенные к маршрутизатору сети
   (config-router)network <номер сети>
! Конфигурирование локального разрешения имен
   (config)# ip host <имя хоста> <ip-адрес1>
                      [ip-адрес2 [ip-адрес3[...]]

! Сохранение текущей конфигурации
  # copy running-config startup-config
```

2.1.9. Тестирование настроек

Для проверки правильности настроек и диагностики используйте команды из табл. 2.1.

Таблица 2.1. Основные команды проверки базовой настройки

Команда	**Описание**
`show running-config`	Отображает содержимое текущего файла настроек.
`show startup-config`	Отображает содержимое стартового файла настроек.
`show ip interface brief`	Позволяет вывести краткую справку об именах и состояниях интерфейсах[1].
`show interface`	Отображает имена физических интерфейсов, их параметры и статистику.
`show ip route`	Отображает содержимое таблицы маршрутизации.
`ping <ip-адрес>`	Проверяет качество связи до узла с указанным ip-адресом.
`traceroute <ip-адрес>`	Используется для проверки движения пакета до сети места назначения, отображает ip-адреса всех маршрутизаторов по пути следования.

[1] Данные выводятся в виде таблицы с полями Status и Protocol. Состояние up в поле Status означает, что нормально работает физический уровень модели OSI, а состояние up в поле Protocol означает нормальное функционирование канального уровня.

2.2. Задание к лабораторной работе

1. Постройте сеть по приведённой на рис. 2.1 схеме. На данной схеме пунктирной линией отмечены кроссовые соединения, а точечной — консольные подключения.
2. Распределите ip-адреса между интерфейсами маршрутизаторов и сетевыми картами компьютеров. Покажите своё распределение ip-адресов преподавателю.
3. Выполните базовую настройку. Пусть пароль на вход в привилегированный режим будет class, а все остальные пароли — cisco. Скорость на DCE-интерфейсах должна быть установлена в 56 кбит/с.
4. Протестируйте связность сети командами ping и tracert с присоединенных компьютеров.
5. При отсутствии связности с помощью команд диагностики выясните причину неисправности и устраните её.
6. Результаты выполнения работы продемонстрируйте преподавателю.

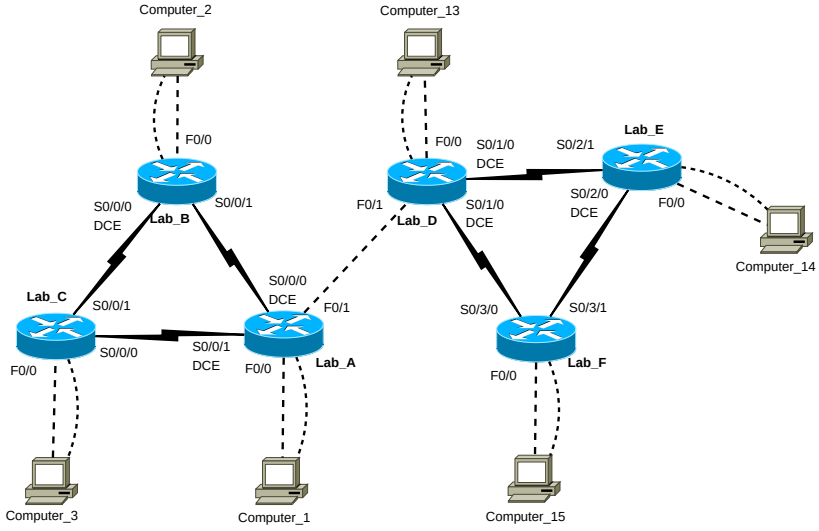


Рис. 2.1. Схема для лабораторной №2

2.3. Контрольная работа №2. Команды CLI и устройство маршрутизатора

ФИО_____ группа _____

A. Установите правильное соответствие между командами и их описаниями:

1.	sh ip route	
2.	sh ver	
3.	conf t	
4.	dir	
5.	sh int	
6.	int s0/0	
7.	en	
8.	ip routing	
9.	clock rate	
10.	sh memory	

A.	Устанавливает скорость передачи на DCE устройстве
B.	Показывает содержимое flash-памяти
C.	Показывает статистику памяти
D.	Переводит маршрутизатор в режим конфигурирования
E.	Переводит маршрутизатор в привилегированный режим
F.	Отображает информацию о памяти и конфигурационном регистре
G.	Переводит маршрутизатор в режим конфигурирования интерфейса
H.	Отображает таблицу маршрутзации
I.	Отображает состояние интерфейсов
J.	Включает маршрутизацию

B. Перечислите все виды памяти, присутствующей на маршрутизаторе. Укажите место хранения образа CIOS:

1. _____
2. _____
3. _____
4. _____
5. _____

Глава 3
Обслуживание маршрутизатора

3.1. Методический материал

При приходе на новое место работы системный администратор может столкнуться с ситуацией, когда невозможно наладить контакт с предыдущим системным администратором и узнать у него пароли входа на сетевые устройства. Пароль может быть также забыт администратором. Возникает задача войти на маршрутизатор без знания пароля. При это необходимо не только сбросить забытый пароль, но и сохранить текущие настройки. Настройки хранятся в конфигурационном файле `startup-config`, их потеря может привести к нарушению работы сети предприятия и повлиять на протекание основных-бизнес процессов, что ни в коем случае не допустимо.

Замена образа операционной системы — это вторая важная задача. Тип образа операционной системы задаёт функциональность маршрутизатора и может предъявлять дополнительные требования к аппаратному обеспечению (обычно к RAM и Flash-памяти). Основные типы образов представлены на рис. 3.1. **IPBase** обеспечивает базовую функциональность. **IPVoice** имеет поддержку VoIP, VoFR, **IP Telephony**. **Advanced Security** поддерживает Cisco IOS Firewall, IPSec, VPN, SSH. **SP Services** работает с MPLS, SSH, ATM, VoATM. **Enterprise Base** имеет мультипротокольную поддержку, работает с сервисами IBM. **Advanced IP Services** работает с IPv6, расширенным функционалом безопасности, службами провайдера. **Enterprise Services** — полная поддержка сервисов IBM и служб провайдера. **Advanced Enterprise Services** имеет полную поддержку всех служб.

3.1.1. Процедура сброса пароля на маршрутизаторе 2801

Данная процедура подходит для маршрутизаторов серий 2600, 1700, 1800, 2800 и некоторых других.

На маршрутизаторе и коммутаторе процедура сброса пароля отличается, но в обоих случаях необходим прямой физический доступ к устройствам и консольное подключение. Важно! Клиентская программа, через которую производится подключение к консоли, должна поддерживать передачу последовательности Ctrl+Break. В противном случае

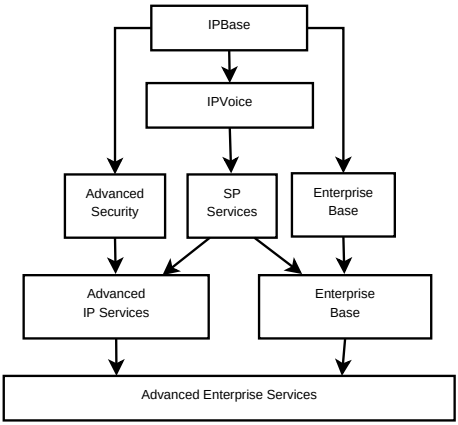


Рис. 3.1. Основные типы образов операционной системы Cisco IOS

невозможно будет попасть в режим ROMMON (ROM Monitor), который необходим для восстановления.

Восстановление забытого пароля на вход в привилегированный режим:

1. Подключитесь к маршрутизатору с помощью терминальной программы (putty или hyperterminal) через консоль.
2. Если Вы можете попасть в пользовательский режим, то введите команду `show version` и запомните значение конфигурационного регистра. Обычно это 0x2102 или 0x102[1].
3. Выключите питание маршрутизатора и снова включите.
4. Нажмите Break (Ctrl+Break) на клавиатуре и удерживайте примерно 60 секунд, чтобы попасть в режим ROMMON.
5. Каждый бит конфигурационного регистра означает какой-либо параметр. Нам необходимо установить бит "Ignore Configuration on StartUp". Можно сразу ввести необходимое значение командой `confreg 0x2142` после приглашения `rommon 1>`. А можно напечатать команду `confreg` без параметров, после чего будет запущен диалог, в котором необходимо установить данную опцию.
6. Напечатайте `reset` после `rommon 2>`, для того чтобы перезагрузить маршрутизатор.

[1]Расшифровку значений бит конфигурационного регистра можно сделать с помощью программы confregna URL: `http://skola.sssbb.sk/~badani/cisco/tools/Calculators/ConfReg122/`

7. Нажмите <Ctrl-C>, чтобы пропустить процедуру начальной установки параметров.
8. Войдите в привилегированный режим:
   ```
   Router> enable
   Router#
   ```
9. Внимание! Введите команду `configure memory` или `copy startup-config running-config`, чтобы скопировать файл `startup-config` в память.
10. Напечатайте `show running-config`. Эта команда показывает конфигурацию маршрутизатора. В частности, вы увидите все пароли или их криптографические хэши. Если пароли хранятся в открытом виде, их можно использовать. Если нет, то необходимо их заменить новыми.
11. Войдите в режим конфигурирования `configure terminal` и сделайте необходимые действия.
12. Напечатайте `enable secret <пароль>` для изменения пароля входа в привилегированный режим.
13. Поднимите все сетевые интерфейсы, которые будут использоваться. Проверьте выполнение этого действия командой `show ip interface brief` из привилегированного режима. Состояния всех выключенных интерфейсов должно быть "up up".
14. Напечатайте `config-register 0x2102`, или то значение, которое Вы получили ранее на втором шаге. После чего выйдите из режима конфигурирования.
15. Напечатайте `copy running-config startup-config` для подтверждения изменений.
16. Если есть возможность, перегрузите маршрутизатор и убедитесь, что конфигурация была применена.

3.1.2. Процедура замены образа Cisco IOS

Для замены образа IOS или файла конфигурации используется TFTP-сервер[1].

Для того чтобы сохранить или загрузить файл конфигурации или образ операционной системы на TFTP-сервер, необходимо выполнить следующие шаги:

1. Подключите сегмент сети к первому из Ethernet интерфейсов маршрутизатора (F0/0).
2. Если интерфейс не настроен, то настроить его в соответствии с подключённой к нему сети.
3. Поднимите интерфейс.
4. На компьютере запустите службу TFTP. Используйте любое приложение, например, для Windows в Интернете можно найти TFTPD32[2] или Cisco TFTP Server. Преимущество первого — не требует инсталляции. Файлы, отправляемые и принимаемые, должны находиться в папке сервера, для этого предназначенной (для TFTPD32 это папка, откуда запущен сервер).
5. На маршрутизаторе используйте команду

   ```
   #copy startup-config tftp
   ```

   или

   ```
   #copy running-config tftp
   ```

   Для образа используется аналогичная команда с указанием имени файла с расширением bin. Сохраняйте имя образа, так как оно несёт важную информацию о типе и версии IOS.

   Пример.

   ```
   #copy  c2800nm-advipservicesk9-mz.124-15.T1.bin tftp
   ```

   Если система не воспринимает такую команду, воспользуйтесь командой

   ```
   #copy  flash tftp
   ```

   После её выполнения система запросит имя копируемого файла и параметры tftp-сервера.
6. Для замены образа на маршрутизаторе достаточно выполнить обратную команду копирования `copy tftp flash`. После чего будет запрошены ip-адрес tftp-сервера, имя образа на tftp-сервере, новое имя образа на flash. Если места во flash-памяти не хватает, то текущий образ можно удалить командой `delete <имя образа>`,

[1] TFTP — Trivial File Transfer Protocol

[2] URL: `http://tftpd32.jounin.net`

предварительно уточнив имя образа, распечатав список файлов на flash командой `dir` или `show flash`.

Важно! Для коммутаторов эта процедура несколько отличается. В частности, IP-адрес назначается не интерфейсу, а управляющему VLAN'у. К портам этого VLAN'а и должен быть подключён компьютер, исполняющий роль TFTP-сервера.

3.2. Аварийное восстановление

Восстановление образа IOS может быть произведено в режиме ROMMON с помощью команды `tftpdnld` в случае повреждения образа на flash или случайного удаления.

Процедура аварийного восстановления:

1. Кроссовым кабелем подключите TFTP-сервер к интерфейсу маршрутизатора F0/0.
2. Выключите и затем включите питание маршрутизатора.
3. Во время загрузки нажмите сочетание <Ctrl+Break>[1], чтобы попасть в режим ROM Monitor (ROMMON). В этом режиме редактор командной строки усечён и не поддерживает всех функций редактирования командной строки, поэтому постарайтесь избежать нажатия лишних клавиш и редактирования строки (особенно навигационных стрелок).
4. Наберите команду `tftpdnld`. При первом запуске будет выдана инструкция по дальнейшим действиям.

```
rommon 1 > tftpdnld

Missing or illegal ip address for variable IP_ADDRESS
Illegal IP address.

usage: tftpdnld
Use this command for disaster recovery only to recover an image via TFTP.
Monitor variables are used to set up parameters for the transfer.
(Syntax: "VARIABLE_NAME=value" and use "set" to show current variables.)
"ctrl-c" or "break" stops the transfer before flash erase begins.

The following variables are REQUIRED to be set for tftpdnld:
        IP_ADDRESS: The IP address for this unit
    IP_SUBNET_MASK: The subnet mask for this unit
   DEFAULT_GATEWAY: The default gateway for this unit
       TFTP_SERVER: The IP address of the server to fetch from
         TFTP_FILE: The filename to fetch

The following variables are OPTIONAL:
    TFTP_VERBOSE: Print setting. 0=quiet, 1=progress(default), 2=verbose
TFTP_RETRY_COUNT: Retry count for ARP and TFTP (default=7)
```

[1] В симуляторе Cisco Packet Tracer можно нажать <Ctrl+C>.

```
 TFTP_TIMEOUT: Overall timeout of operation in seconds (default=7200)
TFTP_CHECKSUM: Perform checksum test on image, 0=no, 1=yes (default=1)
FE_SPEED_MODE: 0=10/hdx, 1=10/fdx, 2=100/hdx, 3=100/fdx, 4=Auto(deflt)

rommon 2 >
```

В инструкции говорится, что для работы утилиты необходимо установить переменные окружения. Первый список переменных является обязательным. IP-адрес должен быть из той же самой сети, что и TFTP-сервер. IP-адрес шлюза по умолчанию в нашей конфигурации может совпадать с TFTP-сервером.

5. После установления всех переменных окружения запустите второй раз команду `tftpdnld`.
6. Если запуск окажется неудачным, — проверьте заданные Вами параметры (переменные окружения) командой `set`, найдите неисправность, устраните её и повторите попытку.
7. Дождитесь окончания передачи, командой `reset` перезагрузите маршрутизатор.
8. Убедитесь в работоспособности маршрутизатора.

3.3. Задание к лабораторной работе

Восстановление забытого пароля

1. Перед выполнением лабораторной очистите файл стартовой конфигурации и перезагрузитесь:

```
> en
# erase startup-config
# reload
```

2. После перезагрузки войдите в режим конфигурирования и для контроля неизменности файла конфигурации после сброса пароля задайте запоминающееся имя маршрутизатору.
3. Задайте хэшированный пароль на вход в привилегированный режим, такой, чтобы Вы сами не смогли его запомнить и воспроизвести.
4. Проверьте значение конфигурационного регистра, убедитесь что оно равно 0x2102. Если это не так, — установите это значение.
5. Сохраните текущие настройки в файле `startup-config`
6. Перезагрузитесь и проверьте, что не можете попасть в привилегированный режим.
7. Проведите процедуру восстановления забытого пароля.

8. Убедитесь, что сохранилось имя маршрутизатора. Если это не так, проанализируйте, на каком этапе Вы допустили ошибку и повторите все задания с самого начала.
9. Продемонстрируйте результаты работы преподавателю, ответьте на его вопросы.

Работа с TFTP-сервером

1. Выполните резервное копирование файла стартовой конфигурации на TFTP-сервер.
2. С помощью редакторов плоских текстов[1] измените имя маршрутизатора в файле, закачанном на TFTP-сервер.
3. Залейте файл конфигурации с TFTP-сервера в текущие настройки[2].
4. Убедитесь, что конфигурация была применена верно.
5. Сохраните текущую конфигурацию в стартовую, перезагрузитесь и удостоверьтесь, что конфигурация подействовала.
6. Продемонстрируйте результаты работы преподавателю, ответьте на его вопросы.

[1] Подойдёт текстовый редактор, встроенный в файловый менеджер FAR. Можно использовать GEdit или какой-либо другой редактор, корректно обрабатывающий linux-концы строк.

[2] Обратите внимание на то, что происходит не замещение, а слияние настроек.

Аварийное восстановление

1. Перед выполнением лабораторной сделайте резервную копию образа Cisco IOS и всех файлов flash-памяти на TFTP-сервере. Для этого Вам могут понадобиться команды `show flash`, `dir`, `copy <имя образа> tftp`.
2. Зайдите в привилегированный режим.
3. Удалите файл образа командой `delete <имя образа>`.
4. Отключите все сетевые подключения из режима конфигурирования интерфейсов командой `shutdown`.
5. Перезагрузитесь с помощью команды `reload`. Так как образа нет на flash, а TFTP-сервер недоступен, то Вы должны немедленно попасть в режим ROMMON.
6. Подключите TFTP-сервер к F0/0.
7. Воспользуйтесь командой `tftpdnld` для восстановления образа Cisco IOS.
8. Перезагрузите `reset` и проверьте работоспособность маршрутизатора.
9. Скопируйте все ранее сохранённые на TFTP-сервере файлы на flash-память.
10. Продемонстрируйте результаты работы преподавателю, ответьте на его вопросы.

3.4. Контрольная работа №3. Команды базовой настройки

A. Вы находитесь в пользовательском режиме. Напишите последовательность команд, устанавливающую пароль на вход в привилегированный режим. Пароль должен храниться в конфигурационном файле в зашифрованном виде. После установки пароля необходимо вернуться в пользовательский режим.

```
>
```

B. Вы находитесь в привилегированном режиме. Напишите последовательность команд, устанавливающую пароль на консольный вход. После установки пароля необходимо вернуться в привилегированный режим.

```
#
```

C. Вы находитесь в режиме конфигурирования. Напишите последовательность команд, настраивающую и поднимающую последовательный DCE-интерфейс Serial 0/0. По завершении выйдите в привилегированный режим. Необходимые данные: IP-адрес 192.168.1.1, скорость соединения 56 КБит/сек.

```
(config)#
```

Глава 4
Статическая маршрутизация

4.1. Методический материал

Динамическая маршрутизация, использующая такие протоколы, как RIP, EIGRP, OSPF и др., создаёт записи в таблице маршрутизации и обеспечивает связность сети предприятия. В некоторых случаях необходима корректировка маршрутов. Это можно сделать вручную. Кроме того, статическая маршрутизация позволяет скрыть внутреннюю структуру сети предприятия от провайдера, что повышает безопасность Вашей сети.

Цель данной лабораторной — научить управлению статическими маршрутами.

Системный администратор может имеет дело с недокументированной или плохо документированной сетью. Разобраться в структуре такой сети поможет протокол CDP — Cisco Discovery Protocol. Знание основ этого протокола поможет выполнить лабораторную работу.

4.1.1. Формат команды настройки статического маршрута

Маршрутизация может быть настроена как вручную, тогда говорят о статической маршрутизации, так и с помощью протоколов маршрутизации, тогда говорят о динамической маршрутизации. Какой бы способ и протокол не был использован, каждый маршрут обладает одним общим для всех протоколов свойством, которое называется *административной дистанцией*.

Опр. *Административная дистанция* (АД) — это степень доверия маршруту[1], мера надёжности источника получения маршрута. Изменяется от 0 до 255 (0 — полное доверие источнику, 254 — минимальное доверие, 255 — игнорирование маршрута).

Маршрутизатор хранит базу данных всех существующих маршрутов. Когда к одной и той же сети существует несколько маршрутов, в таблицу маршрутизации попадает тот, у которого административная дистанция меньше. В табл. 4.1 приведены значения административной дистанции для различных источников. Указанные значения используются по умолчанию, но они могут быть изменены. Для динамической маршрутизации это делается с помощью команды `distance` в режиме

[1] Правильнее сказать «степень недоверия», но простим себе эту неточность.

Таблица 4.1. Таблица АД по умолчанию

Источник	**АД**
Прямое подключение	0
Статический маршрут	1
Итоговый маршрут EIGRP	5
Внешний BGP	20
EIGRP	90
IGRP	100
OSPF	110
RIP	120

конфигурирования маршрутизации. А для статического маршрута, задаваемого в режиме конфигурирования командой `ip route`, существует необязательный параметр, устанавливающий АД.

Для создания статического маршрута используется команда:

```
(config)# ip route
    <сеть места назначения> <маска подсети>
    {<имя интерфейса> | <адрес следующего шлюза>}
    [АД]
```

Имя интерфейса указывать предпочтительнее, так как при этом таблица просматривается только один раз. При указании адреса следующего шлюза происходит рекурсивный просмотр таблицы в поисках сетевого интерфейса, на который необходимо перенаправить пакет. Но в сетях множественного доступа рекомендуется указывать адрес следующего шлюза, чтобы не возникало неоднозначности при отправке пакета через эту сеть.

Наиболее часто статическая маршрутизация используется для задания маршрута по умолчанию. При задании маршрута по умолчанию в качестве параметров команды используется сеть 0.0.0.0 с маской 0.0.0.0. Алгоритм просмотра таблиц маршрутизации устроен так, что проверяет маршруты в порядке от более специфической маски к менее специфической[1]. Так как маска 0.0.0.0 самая неспецифическая, то проверяться она будет последней и наложение её на любой ip-адрес даст адрес

[1]Более специфическая означает большее количество 1 в двоичной записи маски. Самая специфическая маска 255.255.255.255, а самая неспецифическая 0.0.0.0

сети 0.0.0.0:

$$\text{ip} \ \& \ 0.0.0.0 = 0.0.0.0$$

Итак, маршрут по умолчанию создаётся командой

```
(config)#ip route 0.0.0.0 0.0.0.0
        {название интерфейса | ip следующего шлюза}
```

4.1.2. Протокол CDP

CDP (Cisco Discovery Protocol) — протокол канального уровня, разработанный компанией Cisco Systems. Позволяет обнаруживать подключённое (напрямую или через устройства первого уровня) сетевое оборудование Cisco, его название, версию IOS и IP-адреса. Поддерживается многими устройствами компании, почти не поддерживается сторонними производителями. Получаемая информация включает в себя типы подключённых устройств, интерфейсы маршрутизатора, к которым подключены соседние устройства, интерфейсы, использующиеся для создания соединений, а также модели устройств.

Устройство посылает мультикаст-уведомление (advertisement) на MAC-адрес 01-00-0c-cc-cc-cc. По умолчанию уведомления рассылаются каждые 60 с на порты Ethernet, Frame Relay и ATM. Каждое устройство, понимающее протокол, сохраняет полученную информацию в таблице и позволяет посмотреть её по команде `show cdp neighbors`. Если устройство трижды не прислало анонс (при значениях по умолчанию — 3 минуты), оно удаляется из таблицы.

В уведомлениях также содержится информация о времени жизни пакета (Time To Live — TTL) или времени удержания информации (holdtime). Последний параметр определяет время, в течение которого будет храниться CDP информация, прежде чем она будет уничтожена [3].

Команда `show cdp neighbors detail` позволит узнать не только подключения и платформу соседнего устройства, но и настройки сетевых интерфейсов (в частности IP-адреса).

Безопасность. В целях обеспечения безопасности рекомендуется работу этого протокола отключить. По умолчанию он включён. Выключение производится командой `no cdp run` — глобально, `no cdp enable` — для интерфейса. Если по какой-либо причине протокол отключён, а Вам необходимо его включить, то это осуществляется аналогично: `cdp run` — глобально, `cdp enable` — в режиме конфигурирования интерфейса.

Более подробную информацию о протоколе и его конфигурировании можно найти в [4].

4.2. Задание к лабораторной работе

Данная лабораторная работа коллективная. Выполняется в сетевом режиме Csico Packet Tracer (PT). Преподаватель создаёт в PT схему с неизвестной слушателям топологией. На каждый студенческий компьютер сбрасывается схема с облаком для консольного и Ethernet-подключения. Задачи лабораторной:

- восстановить потерянные пароли на каждом доступном маршрутизаторе (индивидуально);
- активировать все сетевые интерфейсы;
- восстановить топологию (выполняется коллективно): указать связи между устройствами, подписать типы DCE-DTE и названия интерфейсов, подписать известные уже назначенные сетевым интерфейсам ip-адреса;
- показать восстановленную схему преподавателю;
- распределить ip-адреса на интерфейсы, на которых они не не были назначены;
- с помощью статических маршрутов обеспечить связность между компьютерами по оптимальным маршрутам;
- проверить командами ping и tracert связность сети и оптимальность маршрутов;
- в случае неисправностей выявить причины и устранить их;
- результаты показать преподавателю.

4.3. Контрольная работа №4. IP-адресация

ФИО_____ группа _____

А. Заполните недостающие поля таблицы:

Адрес сети	192.168.10.0
Класс	
Число бит для нумерации сетей	3
Число единичных бит в маске	
Маска в десятичном представлении	
Максимальное число подсетей	
Максимальное число хостов на подсеть	

Выпишите номера сетей для данного разбиения на подсети:

№	Адрес подсети	Диапазон хостов	Широковещание

В. Заполните таблицу:

Адрес сети	128.192.0.0
Класс	
Число бит для нумерации сетей	
Число единичных бит в маске	
Маска в десятичном представлении	
Максимальное число подсетей	16
Максимальное число хостов на подсеть	

Выпишите номера сетей для данного разбиения на подсети:

№	Адрес подсети	Диапазон хостов	Широковещание

C. Дано предприятие, состоящее из двух подразделений: бухгалтерия и отдел продаж. В бухгалтерии 7 компьютеров, а в отделе продаж 33. Дана сеть 192.168.0.0 (классовая модель), из которой вы вправе выделять IP-адреса. Упорядочите требования и постройте разбиение этой сети на два диапазона минимальной длины для каждого подразделения с помощью VLSM.

Подсеть	
Диапазон	
Широковещание	
Маска в десятичном виде	

Подсеть	
Диапазон	
Широковещание	
Маска в десятичном виде	

Глава 5
Протокол EIGRP

5.1. Методический материал

EIGRP — относится к безклассовым протоколам внутренних шлюзов. По математическому алгоритму EIGRP — это дистанционно-векторный протокол. В то же время он имеет большое число механизмов, заимствованных из протоколов состояния канала связи. Таким образом, его можно классифицировать как модифицированный дистанционно-векторный или гибридный протокол.

Цель лабораторной — освоить базовые понятия протокола EIGRP и научиться выполнять настройку маршрутизации с использованием протокола.

5.1.1. Основы протокола EIGRP

EIGRP (Enhanced Interior Gateway Protocol) — расширенный протокол маршрутизации внутренних шлюзов. Этот протокол является результатом развития дистанционно-векторного протокола IGRP. От IGRP он унаследовал настраиваемую метрику, мгновенные обновления, распределение нагрузки между неравновесными каналами [5]. По сравнению с IGRP он имеет ряд улучшений:

1. Поддерживает работу с масками переменной длины (VLSM).
2. Не использует регулярных рассылок. Рассылки производятся только при изменении топологии сети.
3. В рассылках указывает только новые маршруты.
4. Умеет определять резервные маршруты.
5. Существенно более высокая скорость сходимости по сравнению с IGRP и RIP.

Предполагалось, что протокол будет работать в рамках *автономных систем* (Autonomous System — AS).

Опр. *Автономной системой* называется часть сети под общим административным управлением и с общей маршрутной политикой. Автономной системе присваивается уникальный 16-битный номер. Назначением номеров AS на территории Северной и Южной Америки занимается организация ARIN (American Registry for Internet Number). Для Европы, Среднего Востока и части Африки аналогичная организация называется

RIPE (Reseaux IP Europeans); для Азии и тихоокеанского региона — APNIC (Asia Pacific Network Information center). В целом назначением адресов AS руководит IANA — та же организация, которая регулирует выдачу IP-адресов.

На маршрутизаторе при настройке EIGRP требуется указать номер автономной системы. Но это просто номер процесса EIGRP, он может и не соответствовать какой-либо реальной автономной системе. На одном маршрутизаторе может быть запущено несколько процессов EIGRP, и по номеру процесса они и будут различаться.

Метрика. Напомним, что *метрика* — это величина, представляющая аналог расстояния в пространстве, на основании которой выбирается оптимальный маршрут: чем меньше метрика, тем оптимальнее маршрут. В EIGRP метрика вычисляется на основании следующей формулы [6]:

$$M = \begin{cases} \left(K_1 \cdot B + \left[\dfrac{K_2 \cdot B}{256 - L}\right] + K_3 \cdot D\right) \cdot \left[\dfrac{K_5}{R + K_4}\right], & \text{если } K_5 \neq 0 \\ \left(K_1 \cdot B + \left[\dfrac{K_2 \cdot B}{256 - L}\right] + K3 \cdot D\right), \text{иначе} \end{cases},$$

где D — задержка в десятках миллисекунд, равная сумме задержек в каналах связи вдоль маршрута и умноженная на 256 (для хранения используется 32 бита)[1]; $B = \dfrac{10^7}{bandwidth \cdot 256}$, здесь *bandwidth* — наименьшая полоса пропускания каналов вдоль маршрута в килобитах в секунду (32 бита); R — надёжность (1 байт), 0 — минимальная надёжность канала, 255 — максимальная надёжность канала; L – загруженность (1 байт), 0 — минимальная загруженность канала, 255 — максимальная.

По умолчанию значения весовых коэффициентов равны: $K_1 = K_3 = 1$, $K_2 = K_4 = K_5 = 0$. Таким образом, в большинстве случаев метрика вычисляется по формуле $M = B + D$ и зависит только от задержки и полосы пропускания. Реальная скорость передачи связана с параметром команды `clock rate` маршрутизатора на DCE-интерфейсе, но она не влияет на вычисление метрики. Для изменения метрики можно использовать команду `bandwidth` в режиме конфигурирования интерфейса или изменять весовые коэффициенты с помощью `metric weights`. На реальную скорость передачи эти настройки не влияют.

[1]Задержка, показываемая командами `ip eigrp topology` или `show interface`, указана в микросекундах, соответственно, это значение нужно поделить на 10 перед использованием в этой формуле.

Для вычисления метрики используется информация из трёх баз данных:

1. База данных о наилучших маршрутах — таблица маршрутизации `show ip route eigrp`.
2. Топологическая база данных — информация обо всех маршрутах `show ip eigrp topology all-links`.
3. Таблица соседей — информация о соседних маршрутизаторах[1] `show ip eigrp neighbors` .

Эти базы формируются в момент изменения топологии и хранятся на маршрутизаторе. Фактически EIGRP ближе к протоколам состояния канала связи, чем к дистанционно-векторным протоколам, так как для вычисления оптимального маршрута использует топологическую базу данных.

Кроме того, EIGRP при выборе оптимального маршрута с минимальной метрикой (Feasible Distance) пытается вычислить резервный маршрут, определить запасной маршрутизатор (Feasible Successor), через который будут направляться пакеты. Маршрут становится резервным, если заявленная метрика (Reported Distance) маршрута[2] оказывается меньше, чем оптимальная (Feasible Distance).

При изменении топологии резервный маршрут первым приходит на помощь. А затем после уточнения топологии, если необходимо, происходит перерасчёт оптимальных маршрутов и определяется новый резервный. Сходимость протокола очень быстрая.

5.1.2. Настройка EIGRP

Внешне настройка протокола EIGRP на маршрутизаторе Cisco мало чем отличается от настройки протокола RIP.

Пример:

```
# conf t
(config)# router eigrp 50
(config-router)# network 192.168.1.4 0.0.0.3
(config-router)# network 192.168.1.8 0.0.0.3
(config-router)# network 192.168.2.0 0.0.0.3
```

В команде `network <присоединённая сеть> <wildcard маска>` второй параметр, как правило, является инвертированной маской подсе-

[1] Отношения соседства поддерживаются с помощью протокола Hello.

[2] Эта метрика вычисляется у соседа.

ти, хотя само понятие wildcard-маски несколько шире, чем просто инвертирование маски. К этому понятию мы вернёмся в лабораторной № 7.

Если необходимо, то можно настроить административную дистанцию и веса:

```
(config-router)# distance 40
(config-router)# metric weights 0 1 1 1 1 1 exit
```

Формат второй команды следующий:

`metric weights tos k1 k2 k3 k4 k5`,

где `tos` (Type of Service) — это тип обслуживания из заголовка протокола IP.

5.1.3. Пассивные интерфейсы

С сетевых интерфейсов, присоединённых к сети конечных пользователей, не имеет смысла отправлять маршрутные обновления. Это только увеличивает количество служебного трафика и отнимает полосу пропускания у данных пользователей. В этом случае такие интерфейсы переводят в пассивный режим. В пассивном режиме сетевой интерфейс может принимать маршрутные обновления, но маршрутные обновления не рассылает.

Для перевода интерфейса в пассивный режим при конфигурировании протокола маршрутизации используется команда:

```
(config-router)# passive-interface <имя интерфейса>
```

5.1.4. Распространение маршрутов в RIP и EIGRP

Если имеется тупиковая сеть с несколькими маршрутизаторами за одним граничным, то на граничном маршрутизаторе обычно настраивается маршрут по умолчанию:

```
(config)# ip route 0.0.0.0 0.0.0.0 <интерфейс>
```

Чтобы этот маршрут был включён в таблицы обновления динамического протокола маршрутизации RIP, используется команда

```
(config-router)# ip default-information originate
```

После этого статический маршрут по умолчанию помечается * и начинает распространяться в таблицах RIP.

Аналогичного механизма в EIGRP нет. Распространение маршрута по умолчанию можно организовать с помощью распространения статических

маршрутов[1].

```
(config-router)# redistribute static
```

или с помощью задания сети по умолчанию, в направлении которой будут посылаться пакеты, если для пакета не был найден подходящий маршрут в таблице маршрутизации

```
(config)# ip default-network <ip-сети>
```

Обратите внимание, что команда выполняется в режиме глобального конфигурирования, а значит, действует на все процессы маршрутизации одновременно.

5.1.5. Автосуммирование маршрутов EIGRP

По умолчанию EIGRP автосуммирует маршруты до границ классов. Этот подход экономит размеры таблиц маршрутизации, но в случае «разорванных сетей» сходимости не будет. Пример «разорванной сети» приведён на рис. 5.1. Каждый маршрутизатор, просуммировав до границ класса, получит маршрут не к своей подсети, а к сети 192.168.1.0/24. В результате попытка отправить пакет во вторую сеть к успеху не приведёт. Для исправления этой ситуации необходимо изменить топологию сети (сделать так, чтобы обе подсети присоединены были к одному маршрутизатору) или отключить автосуммирование. В последнем случае суммирование до границ класса производиться не будет и в таблицы маршрутных обновлений будут включаться маски подсетей, что увеличит размер таблиц маршрутизации, но обеспечит связность в данной топологии.

Включается и выключается автосуммирование из режима конфигурирования протокола маршрутизации командами `auto-summary` и `no auto-summary` соответственно.

5.1.6. Диагностика EIGRP

Команды, приведённые в табл. 5.1, помогут идентифицировать ошибки в настройках или причины возникновения проблем.

В особо сложных случаях можно использовать команду
`debug ip eigrp [параметры]`.
Действие этой команды отменяется командами
`no debug all` или `undebug all`.

[1] При этом распространяется не только маршрут по умолчанию, но и все статические маршруты из таблицы маршрутизации.

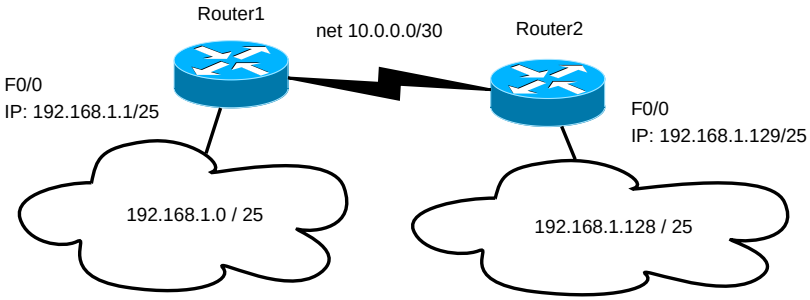


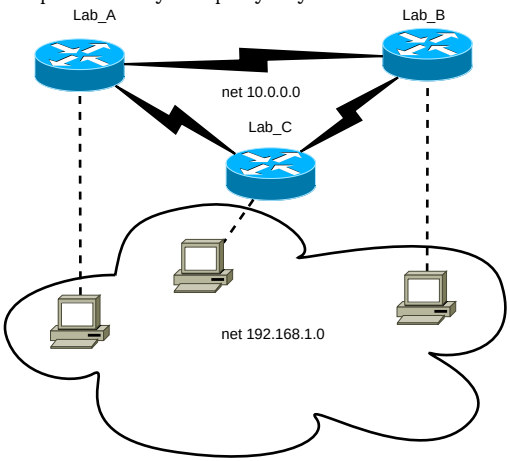
Рис. 5.1. Сеть 192.168.1.0/24 разбита на две подсети, которые для данной топологии не могут быть представлены одним маршрутом, сеть «разорвана»

Таблица 5.1. Команды диагностики EIGRP

Команда	**Описание**
show ip route eigrp	выводит записи таблицы маршрутизации, соответствующие EIGRP.
show ip eigrp neighbors	выводит базу данных EIGRP-соседей.
show ip eigrp topology [all-links]	выводит топологическую базу данных EIGRP.
show ip eigrp traffic	выводит статистику протокола (число принятых и отправленных пакетов EIGRP).
show ip protocol	информация об активных сеансах маршрутизации.
show running-config	отображает выполненные Вами настройки.

5.2. Задание к лабораторной работе

1. Собрать схему по рисунку:



2. Оптимально распределить IP-адреса исходя из требований, представленных в следующей таблице:

Сеть	**Требования**
Между маршрутизаторами	выделяем три подсети из сети 10.0.0.0/8 по два компьютера в каждой.
Локальные сети	выделяем три подсети из сети 192.168.1.0/24 по тридцать компьютеров в каждой.

3. Провести настройку маршрутизации EIGRP с номером процесс 77.
4. Провести проверку связности. В случае отсутствия связности диагностировать причину и устранить неисправность.
5. Продемонстрировать работу сети преподавателю.
6. На маршрутизаторе `Lab_A` создать петлевой интерфейс `lo0`, имитирующий подключение к сети провайдера. Назначить ему ip-адрес.
7. Создать маршрут по умолчанию на петлевой интерфейс.
8. Организовать распространение маршрута по умолчанию на остальные маршрутизаторы.
9. Продемонстрировать результаты распространения маршрута по умолчанию преподавателю.

5.3. Контрольная работа №5. Статическая маршрутизация

1. Что обозначает первый параметр в команде
`ip route 0.0.0.0 0.0.0.0 212.192.5.5 1`?
A. Сеть источника.
B. Сеть места назначения.
C. Маска источника.
D. Маска места назначения.

2. Что обозначает третий параметр в команде
`ip route 192.168.1.1 255.255.255.0 212.192.5.5 2`?
A. Адрес интерфейса, на который необходимо отправить пакет.
B. Сеть места назначения.
C. Адрес следующего маршрутизатора.
D. Адрес конечного получателя пакета.

3. Что обозначает четвёртый параметр в команде
`ip route 192.168.1.1 255.255.255.0 212.192.5.5 3`?
A. Количество переходов до сети места назначения
B. Порядковый номер в таблице маршрутизации.
C. Метрику маршрута.
D. Административную дистанцию.

4. Команда `ip route 0.0.0.0 0.0.0.0 s0/0/0` добавляет в таблицу маршрутизации маршрут, который
A. проверяется первым.
B. проверяется последним.
C. проверяется в порядке добавления.
D. не проверяется.
E. команда задана неверно.

5. Дан фрагмент вывода после ввода команды `show ip route`

```
S    10.0.0.0/8 is directly connected, FastEthernet0/0
C    172.16.0.0/16 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

Какие из этих маршрутов являются статическими? Отметить все.
A. 10.0.0.0/8
B. 172.16.0.0/16
C. 192.168.1.0/24

Глава 6
Структура таблиц маршрутизации

6.1. Методический материал

Цель лабораторной — ознакомить слушателя со структурой таблиц маршрутизации для лучшего понимания процессов, протекающих в сетевых устройствах.

6.1.1. Иерархическая структура таблиц

Таблица маршрутизации представляет собой двухуровневую иерархическую структуру.

После ввода команды `show ip route` видим:

- напрямую присоединённые сети (код C);
- статические маршруты (код S);
- маршруты, полученные посредством динамических протоколов маршрутизации.

К *маршрутам первого уровня* относятся маршруты с маской подсети меньше или равной маске класса. Следующие маршруты относятся к маршрутам первого уровня (отступ отсутствует):

- маршруты по умолчанию;
- маршруты к суперсетям (просуммированные маршруты);
- маршруты к сетям класса.

Окончательный маршрут (Ultimate Route) — это маршрут первого или второго уровня, который имеет либо IP-адрес следующего перехода (следующего шлюза[1]) или выходной интерфейс. *Родительский* маршрут — это не окончательный маршрут. Он может быть только маршрутом первого уровня. Родительский маршрут объединяет окончательные дочерние маршруты в одну запись для сокращения количества проверок при поиске оптимального маршрута.

Маршрутом второго уровня является маршрут к подсети или сети класса (имеется отступ при выводе). В маршруты второго уровня могут попасть:

- маршруты по умолчанию;
- маршруты к суперсетям (просуммированные маршруты);

[1] Шлюз, маршрутизатор и роутер — это синонимы.

- маршруты к сетям класса.

Дочерние маршруты — это всегда окончательные маршруты второго уровня.

Процесс маршрутизации можно описать следующим образом.

1. Производится поиск на наилучшее соответствие (максимально длинная маска) среди маршрутов первого уровня.
2. Если найденный маршрут окончательный:
   а) то производится отсылка на указанный интерфейс,
   б) иначе (в случае родительского маршрута) производится поиск среди маршрутов второго уровня; если соответствие найдено, то осуществляется перенаправление на указанный интерфейс.
   в) Если маршрут не найден, то проверяется тип просмотра: в случае classful поиск останавливается, а в случае classless — поиск продолжается на первом уровне.

При режиме просмотра `classless` таблицу маршрутизации для простоты можно представлять в виде плоской таблицы отсортированной от более специфической маски к менее специфической следующего вида:

Сеть места назначения	**Маска сети места назначения**	**Метрика маршрута**	**Административная дистанция**	**Источник маршрутной информации**	**От кого получена маршрутная информация**	**Собственный интерфейс или адрес следующего шлюза**

При отображении таблицы командой `show ip route` часть информации может быть опущена.

Пример. Автосуммирование отключено, режим classless.

```
     172.18.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.18.0.0/16 [90/2172416] via 209.165.202.134, 00:49:11, Serial0/0/1
C       172.18.64.0/18 is directly connected, FastEthernet0/0
     209.165.202.0/30 is subnetted, 2 subnets
C       209.165.202.128 is directly connected, Serial0/0/0
C       209.165.202.132 is directly connected, Serial0/0/1
S*   0.0.0.0/0 is directly connected, Serial0/0/0
```

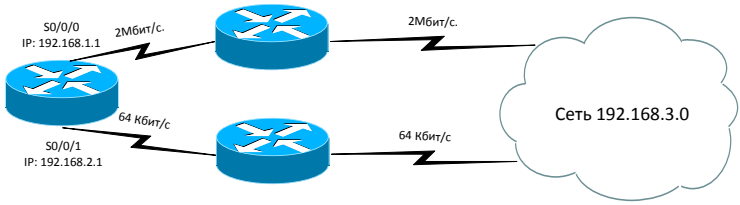


Рис. 6.1. Создание «всплывающего» маршрута

Здесь три родительских маршрута:

1. 172.18.0.0/16 — родительский маршрут, просуммированный до границы класса.
2. 209.165.202.0/30 — родительский маршрут для двух присоединённых сетей с маской на 4 адреса (2 для хостов).
3. 0.0.0.0/0 — окончательный статический маршрут с указанием собственного интерфейса S0/0/0, на который следует отправить пакеты при обнаружении соответствия.

Два дочерних для 172.18.0.0/16:

1. 172.18.0.0/16 — дочерний окончательный EIGRP-маршрут, АД=90, Метрика= 2172416, получен от 209.165.202.134, отправлять пакеты на Serial0/0/1.
2. 172.18.64.0/18 — напрямую присоединённая сеть, отправлять пакеты на FastEthernet0/0.

И два дочерних для 209.165.202.0/30:

1. 209.165.202.128 — напрямую присоединённая сеть, отправлять пакеты на Serial0/0/0, маска, как у родительского маршрута.
2. 209.165.202.132 аналогично, отправлять пакеты на Serial0/0/1.

Включение / отключение режима просмотра осуществляется командами `ip classless` / `no ip classless` из режима глобального конфигурирования. Действует на все протоколы вне зависимсоти от их принадлежности к классовому или бесклассовому типу.

6.1.2. Использование административной дистанции

Создание резервного «всплывающего» маршрута

Пусть нам даны два канала подключения к сети 192.168.3.0

(рис. 6.1). Первый канал — высокоскоростной, с низкой стоимостью трафика, подключен к интерфейсу S0/0/0. Второй — низкоскоростной, с высокой стоимостью трафика, подключён к S0/0/1. Для создания резервного маршрута необходимо сделать следующие шаги:

1. Настраиваем динамическую маршрутизацию по протоколу RIP на интерфейсе S0/0/0. Соответственно, в таблице маршрутизации появится запись:
   ```
   # show ip route
   R 192.168.3.0/24 [120/1] via 192.168.1, 11:30:05, S0
   ```
2. Настраиваем статический маршрут до сети 192.168.3.0 через S1 с АД, большей, чем 120. Например, так:
   ```
   (config)#ip route 192.168.3.0  255.255.255.0 S1 125
   (config)#exit
   ```
   Команда `show ip route` не отобразит данный статический маршрут в таблице маршрутизации, так как его АД больше, чем у протокола RIP. Но тем не менее маршрут сохранится в базе данных маршрутов и в случае поломки высокоскоростного канала немедленно будет внесён в таблицу маршрутизации, связь будет восстановлена.

6.2. Задание к лабораторной работе

1. Самостоятельно спроектировать схему, демонстрирующую «всплывающие» маршруты.
2. Обсудить схему с преподавателем. По результатам обсуждения внести изменения в схему.
3. Реализовать схему.
4. Продемонстрировать процесс «всплытия».

6.3. Контрольная работа №6. Настройки протокола EIGRP

1. Что обозначает первый параметр 24 в команде `router eigrp 24`?
   A. Номер автономной системы.
   B. Номер процесса EIGRP.
   C. Максимальное количество маршрутов в таблице маршрутизации.
   D. Общую длину маски для всех маршрутов.

2. Чему равен параметр X для первых четырёх адресов указанной сети в команде настройки протокола EIGRP
   `network 192.168.1.0 X`?
   A. 255.255.255.252
   B. 255.255.255.248
   C. 0.0.0.3
   D. 0.0.0.7

3. Какая из команд показывает таблицу соседей eigrp?
   A. show ip route eigrp
   B. show cdp neighbors
   C. show ip e n
   D. show ip eigrp topology

4. Какими кодами помечаются маршруты EIGRP в таблицах маршрутизации (указать все)?
   A. I
   B. E
   C. EX
   D. D
   E. E1

5. Известно что оптимальный маршрут к сети 10.0.0.0 имеет метрику 2172416. От соседей пришли маршруты к этой же сети с объявленными метриками, которые были пересчитаны на маршрутизаторе. Таблица объявленных (reported distance) и пересчитанных метрик представлена в следующей таблице:

№	RD	Metric
1	2283527	3283527
2	1061306	3394638
3	2283527	3173526

Какой из маршрутов станет резервным (feasible successor)?
   A. 1
   B. 2
   C. 3
   D. Нет ни одного резервного маршрута.

Глава 7
Списки управления доступом

7.1. Методический материал

Списки контроля доступа — это базовая технология обеспечения безопасности сети. Применение списков контроля доступа не только необходимо для пакетной фильтрации, но и активно используется как механизм задания условий для других команд.

Цель лабораторной — научить конфигурировать стандартные, расширенные и именованные списки доступа.

Английская аббревиатура для списков управления доступом — ACL (Access Control List). Список доступа — это набор инструкций, применяемых на интерфейсе маршрутизатора к входящему или исходящему трафику. Инструкции указывают, какие пакеты принять, а какие отвергнуть. Другое название для списка доступа — фильтр. Списки управления доступом могут создаваться для всех маршрутизируемых протоколов (IP, IPX, AppleTalk). Для каждого протокола должен существовать свой отдельный список доступа. Для чего нужны списки доступа? Перечислим основные цели их использования.

1. Ограничение потока данных в сети и повышение эффективности (в частности, установление очерёдности обработки пакетов).
2. С помощью списков доступа можно увеличить или уменьшить количество сообщений об изменениях сети.
3. Для обеспечения базового уровня защиты от несанкционированного доступа. Например, с помощью ACL можно запретить входящие пакеты из внешних сетей с адресом источника внутренней сети и исходящие пакеты с адресом источника, не принадлежащие внутренней сети.
4. Для блокировки потоков по типу данных. Например, желательно запретить принимать пакеты из внешней сети, направленные на 139 порт (протокол локальной сети), так как возможность такого доступа открывает возможность атаковать слабые места протокола NetBIOS[1], используемого операционной системой Windows. Во внутренней сети, напротив, эти порты должны быть открыты, иначе локальная сеть не сможет нормально функционировать.

[1] В настоящее время практически не используется.

Существует три типа списков ACL:
1. Стандартные списки доступа.
2. Расширенные списки доступа.
3. Именованные списки доступа.

Список доступа (или ACL) состоит из набора директив, описывающих правила фильтрации. Для всех трёх типов при создании важен порядок директив. Директивы проверяются последовательно от начала списка до конца. Если правило срабатывает, то далее список доступа не проверяется, а обрабатываемый пакет разрешается (директива permit) или запрещается (директива deny). Если ни одно правило не сработало, то пакет отбрасывается. Работает закон «Все что не разрешено, — запрещено». Новые директивы всегда записываются в конец списка. Редактирование списка на маршрутизаторе невозможно. Но возможно подготовить список на персональном компьютере с помощью редактора «плоских» текстов, а затем загрузить на маршрутизатор через TFTP-сервер. ACL создаётся на интерфейсе, при этом указывается, к какому протоколу привязан список и к какому виду трафика: входящему или исходящему. Директивы ACL проверяют заголовки 3-го уровня и просматривают заголовки 4-го в случае необходимости. Когда пакет попадает на интерфейс маршрутизатора, вначале проверяется, является ли протокол маршрутизируемым. Если да, то применяется список доступа входящего трафика. Далее пакет маршрутизируется и перенаправляется на другой интерфейс в соответствии с правилами маршрутизации. Перед отправкой в сеть применяется список для исходящего трафика (рис. 7.1).

Конфигурирование стандартного и расширенного ACL состоит из двух этапов:

1. Создание списка доступа осуществляется в режиме конфигурирования последовательностью команд вида:

```
(config-if)# access-list <номер списка>
                    {permit | deny} <условия отбора>
```

   Номера ACL зарезервированы за определёнными протоколами. В табл. 7.1 указаны наиболее часто используемые значения. Нас в первую очередь будут интересовать значения, соответствующие протоколу IP. Для именованных списков используется имя вместо номера. Синтаксис команд именованных списков будет рассмотрен далее.
2. Назначение списка доступа интерфейсу выполняется в режиме конфигурирования интерфейса.

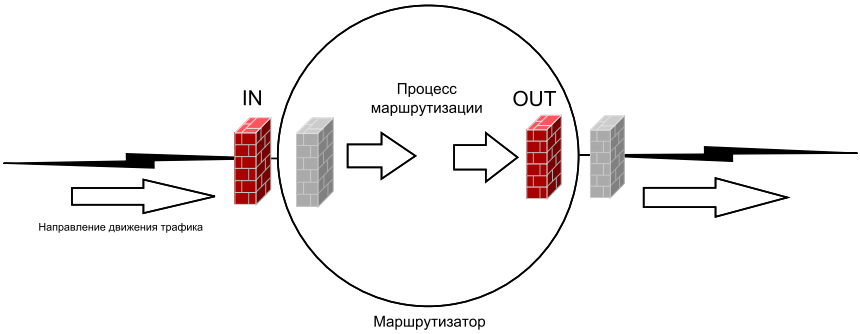


Рис. 7.1. Размещение ACL на интерфейсах маршрутизаторов. Проверяются только красные (левые) списки контроля доступа

```
(config-if)# <протокол> access-group <номер или имя ACL>
```

Таблица 7.1. Номера списков ACL

Протокол	**Диапазон**
IP, стандартный ACL	1-99
IP, расширенный ACL	100-199
AppleTalk	600-699
IPX, стандартный ACL	800-899
IPX, расширенный ACL	900-999

Для удаления всех директив из списка доступа используется команда `(config)# no access-list <номер списка>`.

7.1.1. Шаблон маски

Опр. *Шаблон маски* (Wildcard Mask) — это 32-битовая величина, разбитая на 4 октета по 8 бит[1]. Шаблон маски используется для задания правил условий отбора совместно с IP-адресом. При этом нулевой бит (0) указывает на то, что соответствующий бит IP-адреса пришедшего пакета будет проверяться на соответствие правилу, а единичный (1), — что проверяться не будет.

[1]По формату совпадает с IP-адресом.

Пример. Рассмотрим один октет шаблона маски. В следующей таблице даны пояснения значениям бит октета:

7	6	5	4	3	2	1	0	← Номер бита / Десятичное представление ↓	Пояснения
0	0	0	0	0	0	0	0	= 0	проверять все биты октета
0	0	1	1	1	1	1	1	= 63	игнорировать последние 6 бит октета
1	1	1	1	1	1	1	1	= 255	не проверять биты октета

Для упрощения записи директив в ACL используют две предопределённые пары (адрес, шаблон). Первая — `any`, заменяет пару `0.0.0.0 255.255.255.255`.

Вторая — `host <IP-адрес>`, заменяет `<IP-адрес> 0.0.0.0`.

Пример. В директиве ACL адреса и шаблоны из предыдущего примера могут быть преобразованы следующим образом:

`192.168.0.4 0.0.0.0` ⟶ `host 192.168.0.4`

`192.168.0.5 0.0.0.0` ⟶ `host 192.168.0.5`.

7.1.2. Стандартные ACL

Стандартные списки доступа характеризуются тем, что в условиях отбора у них присутствует только адрес источника. Стандартные ACL не используют информацию из заголовков 4-го уровня.

Создание стандартного ACL

Список создается в режиме конфигурирования с помощью команды

```
(config)# access-list <номер списка> { permit | deny }
                    <адрес источника> [<шаблон источника>] [log]
```

Здесь использовались следующие условные обозначения:

< > — значение параметра команды;

[ ] — необязательное значение параметра или необязательная команда;

— выбор из множества;

| — логическое «или»;

permit — разрешающее правило;

deny — запрещающее правило;

log — включает протоколирование событий фильтрации, сообщения о событиях отправляются на консоль маршрутизатора.

<номер списка> — номер ACL;

<адрес источника> — часть сетевого адреса (адрес 3 уровня) хоста, сформировавшего пакет, для диапазона номеров ACL от 1 до 99 это IP-адрес;

<шаблон-источника> — шаблон маски для адреса источника.

Пример. Создадим стандартный список, запрещающий весь поток IP-пакетов подсети сети 192.168.0.128 / 25 и разрешающий остальной поток:

```
>enable
# configure terminal
(config)#  access-list 1 deny 192.168.0.128 0.0.0.127
(config)#  access-list 1 permit any
(config)# ^z
#
```

7.1.3. Расширенные ACL

Позволяют делать фильтрацию трафика на основании информации заголовков третьего и четвёртого уровня, а также адреса места назначения. Расширенные списки создаются в режиме конфигурирования.

Создание расширенного ACL

```
(config)# access-list <номер списка> {deny | permit}
          <протокол>
          <адрес источника> <шаблон маски источника>
          <адресат> <шаблон маски адресата>
          [precedence <приоритет>]
          [tos <тип обслуживания>] [log]
```

Требуют пояснения следующие параметры:

`<протокол>` — имя или номер протокола. Может принимать одно из ключевых значений: eigrp, gre, icmp, igmp, igrp, ip, ipinip, nos, ospf, pim, tcp, udp или целое число от 0 до 255, представляющее номер протокола. Соответствие любым протоколам Интернет (таким как icmp, udp, tcp) обозначается ключевым словом ip.

`precedence <значение приоритета>` — задаёт значение приоритета из заголовка IP-пакета (0..7).

`tos <тип обслуживания>` — задаёт значение поля Type of Service из заголовка IP-пакета (0..15).

`log` — тот же смысл, что и для стандартного списка.

Для различных протоколов синтаксис команды имеет свои особенности.

Таблица 7.2. Коды ICMP-сообщений

Тип	Код	Запрос (Q) / Ошибка (E)	Описание
0	0	Q	Echo Reply (эхо – ответ)
0	0	E	Net Unreachable (сеть недоступна)
3	6	E	Destination Network Unknown (сеть места назначения неизвестна)
3	7	E	Destination Host Unknown (узел места назначе-ния неизвестен)
3	9	E	Communication with Destination Network is Administratively Prohibited (соединение с за-данной сетью запрещено)
3	10	E	Communication with Destination Host is Admin-istratively Prohibited (Соединение с заданным узлом запрещено)
8	0	Q	Echo Request (запрос на эхо)
9	0	Q	Router Advertisement (уведомление шлюза)
10	0	Q	Router Solicitation (поиск шлюза)
11	0	E	TTL Exceed in Transit (превышение времени жизни)
17	0	Q	Address Mask Request (запрос маски подсети)
18	0	Q	Address Mask Reply (ответ на запрос маски)
30	0	Q	Traceroute (трассировка маршрута)

ICMP:

```
(config)# access-list <номер списка> {deny | permit} icmp
              <адрес источника> <шаблон маски источника>
              <адресат>  <шаблон маски адресата>
              [<тип icmp-сообщения> |
              [<тип icmp-сообщения> <icmp-код>]]
              [precedence <приоритет>]
              [tos <тип об-служивания>] [log]
```

`<тип icmp-сообщения>`, `<icmp-код>` — возможные значения смотри в таблице 7.2.

TCP и UDP:

```
(config)#
   access-list <номер списка> {deny | permit} {tcp | udp}
               <адрес источника> <шаблон маски источника>
               [<оператор> <порт источника>]
               <адресат>  <шаблон маски адресата>
               [<оператор> <порт адресата>]
               [established] [precedence <приоритет>]
               [tos <тип обслуживания>] [log]
```

`<оператор>` — сравнивает порты источника или места назначения. Возможные операторы: `lt (less than)` — меньше чем, `gt (greater than)` — больше чем, `eq (equal)` — равно, `neq (not equal)` — не равно и `range` — диапазон. В случае `range` требуется указать два порта, в остальных случаях — один.

`<порт источника>` или `<порт адресата>` — TCP- или UDP-порт источника и места назначения. Наиболее часто используемые значения имеют имена, которые можно использовать вместо цифр. Имена должны соответствовать последнему RFC, описывающему систему назначенных номеров и связанных с ними протоколов (например, RFC 1700).

`established` — при наличии этого параметра правило работает только для установившегося TCP-соединения. Остальные параметры имеют тот же смысл, что в других командах.

Пример. Создадим ACL, запрещающий доступ к сети 192.168.0.0/24 по протоколу telnet:

```
>enable
# configure terminal
(config)#access-list 101 deny tcp any
                     192.168.0.128 0.0.0.255 eq telnet
(config)#  access-list 101 permit any
(config)# ^z
#
```

7.1.4. Именованные ACL

Именованные списки доступа используются в следующих случаях:

1) если необходимо интуитивно определить список, используя символьное имя;
2) если уже существует более 99 стандартных и более 100 расширенных списков доступа.

Синтаксис команды подразумевает возможность создания стандартных и расширенных списков доступа. Для создания именованного списка доступа используется команда в режиме конфигурирования:

```
#<протокол> access-list {standard | extended} <имя списка>
```

Пример.

1. Создаем стандартный список доступа с именем denyhost для протокола ip.

```
(config)# ip access-list standard denyhost
(config-ext-nacl)#
```

2. Создаем расширенный список доступа с именем denysmtp для протокола ip.

```
(config)# ip access-list extended denysmtp
(config-ext-nacl)#
```

Для задания правил в режиме конфигурирования именного ACL используются команды `permit` и `deny`. Формат этих команд повторяет соответствующие части команд создания правил стандартного и расширенного списков доступа, рассмотренных в предыдущих разделах. Примеры использования списков доступа рассмотрим в следующих разделах.

Пример. Продолжим создание списка из предыдущего примера, разрешающий отправку почты и запрещающий все остальные сообщения.

```
(config)# ip access-list extended denysmtp
(config-ext-nacl)# permit tcp any any eq smtp
```

Команду `deny any any` указывать не нужно, так как она выполняется в конце списка по умолчанию.

7.1.5. Назначение ACL

Мало создать список, — его необходимо привязать к интерфейсу и направлению трафика.

```
<протокол> access-group <номер или имя списка> [{in | out}]
```

Напомним, что данная команда выполняется в режиме конфигурирования интерфейса.

Направление `in` — это проверка входящего на интерфейс из внешней сети трафика; `out` — исходящего во внешнюю сеть трафика (см. рис. 7.1). Если явно не указано направление, то устанавливается фильтр на исходящий трафик. `<протокол>` — для нас это всегда будет ip-протокол.

При выборе интерфейса необходимо руководствоваться следующими правилами:

1. Стандартные списки доступа нужно располагать как можно ближе к источнику трафика.
2. Расширенные списки доступа нужно располагать как можно ближе к месту назначения (адресату).

Список контроля доступа можно назначить и на подключение к виртуальному терминалу:

```
# conf t
(config)# line vty 0 15
(config-line)# access-class
                    <номер или имя списка> [{in | out}]
```

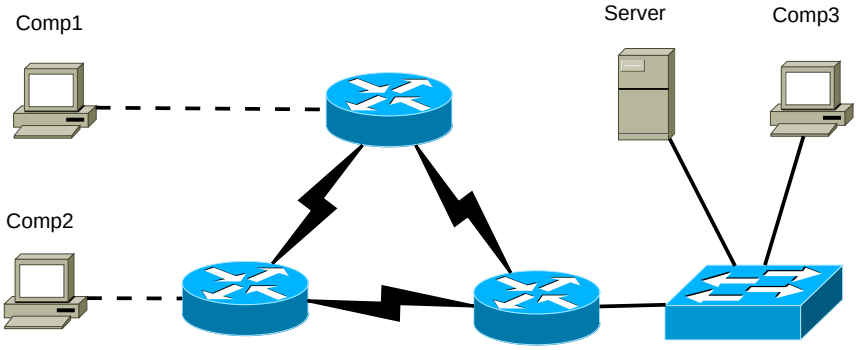
7.1.6. Команды диагностики ACL

Табл. 7.3 содержит основные команды для диагностики неисправностей.

Таблица 7.3. Команды диагностики ACL

Команда	**Описание**
`show access-list [номер списка]`	Показывает содержимое списка доступа.
`show running-config` и `show startup-config`	Показывает содержимое файлов конфигурации, в том числе и списков доступа.
`show ip interface`	Отображает параметры ip-интерфейса в том числе и назначенные на интефейс списки доступа
`clear access-list counters {access-list-number | access-list-name}`	Сбрасывает счётчики срабатывания директив ACL, которые отображаются командой `show access-list`

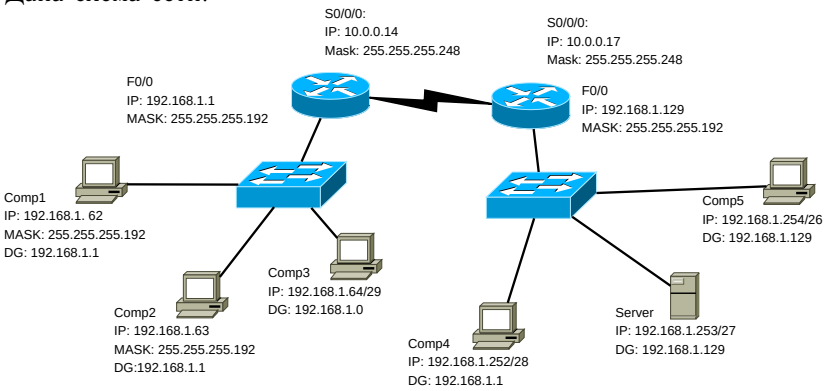
7.2. Задание к лабораторной работе



1. Создайте адресную схему и распределите IP-адреса в соответствии с топологией, представленной на рисунке.
2. Выполните настройку динамической маршрутизации.
3. Проверьте связность и в случае обнаружения неисправностей устраните их.
4. Запустите на сервере HTTP-службу.
5. Создайте ACL для запрета доступа к серверу со стороны сети компьютера Comp1.
6. Определите место для размещения списка и назначьте его на соответствующий интерфейс.
7. Проверьте работу списка доступа.
8. Продемонстрируйте результаты работы преподавателю.

7.3. Контрольная работа №7. Проектирование сетей

Дана схема сети:



Укажите все ошибки на данной схеме. Дайте объяснение, в чём именно состоит ошибка.

Глава 8
Коммутаторы и виртуальные ЛВС

8.1. Методический материал

Под *сегментацией* сети понимают разбиение сети с целью увеличения её производительности и уменьшения нагрузки.

Сегмент сети — это выделенный участок, ограниченный сетевыми устройствами. Таким образом, сегментация осуществляется с помощью коммутаторов и маршрутизаторов.

Доменом коллизий называется сегмент сети с совместно происходящими коллизиями. Если коллизия зарегистрирована в одном узле, то она происходит и во всех узлах сегмента. Концентраторы (хабы) расширяют домен коллизий. Коммутаторы и маршрутизаторы разбивают его на части.

Широковещательный домен — сегмент сети с общим широковещательным трафиком 2 уровня. Концентраторы и коммутаторы расширяют широковещательный домен, а маршрутизаторы разбивают его на части. Данные понятия иллюстрируются на рис. 8.1.

Свойства коммутаторов и маршрутизаторов ограничения циркуляции трафика в сети используют для эффективного построения коммутируемых и маршрутизируемых сетей.

Цель работы — изучить основные принципы функционирования коммутатора и научиться настраивать виртуальные локальные вычислительные сети (VLAN), позволяющие получать хорошо масштабируемые LAN.

8.1.1. Принципы работы коммутатора

Коммутатор узнает MAC-адреса путём чтения заголовков второго уровня приходящих к нему кадров. MAC-адрес запоминается и хранится в памяти коммутатора, адресуемой по содержимому (CAM — Content Addressed Memory) в связке с портом, с которого поступил кадр с данным адресом источника. При первой записи такой пары и каждом использовании запоминается время наступления этого события. Через заданный промежуток времени неиспользуемые адреса удаляются из таблицы.

Для временного хранения кадров и последующей их отправки по нужному адресу коммутатор использует буфер памяти. Существует два

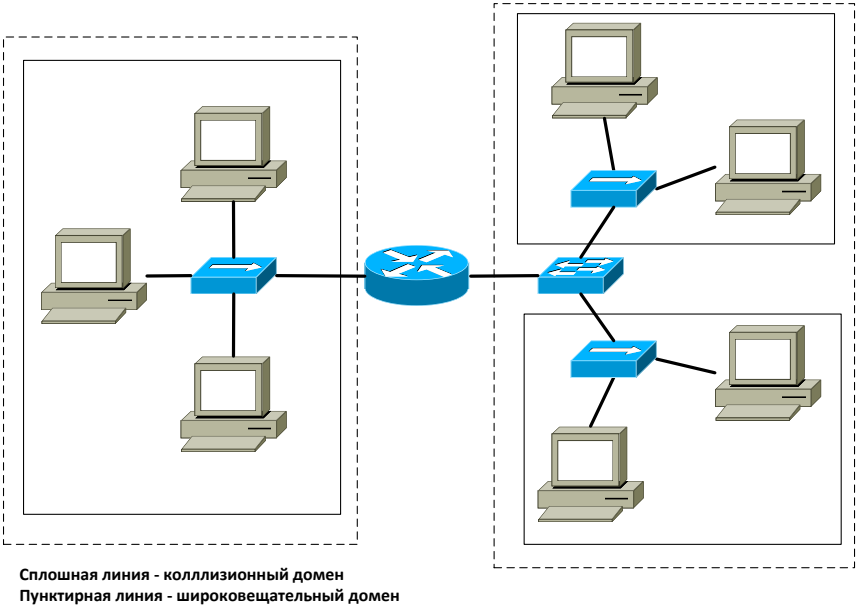


Рис. 8.1. Понятия коллизионного и широковещательного доменов

метода буферизации.

1. Буферизация по портам. Кадры хранятся в очередях, каждая из которых связана со своим портом.
2. Буферизация в общей памяти – общий буфер для всех портов.

У каждого из подходов свои недостатки и преимущества. Так, у первого нерационально используется память и, следовательно, такие устройства будут более дорогими. А у второго подхода из-за наличия общей очереди, если на одном порту идёт интенсивная передача кадров, возможны задержки на других портах.

На практике реализуются два метода коммутации:

1. Запомнить и передать (Store-and-Forward). Отправка с промежуточным хранением. Кадр должен быть получен полностью, проверена его контрольная сумма, находящаяся в конце кадра, и только после этого он может быть отправлен дальше.
2. Сквозной метод (Cut-Through). Отправка кадра начинается до его полного получения. У этого метода есть две разновидности:
    1. Коммутация с быстрой отправкой (Fast-Forward-Switching). Обладает наименьшей задержкой, отправка данных начинается сразу после получения MAC-адреса места назначения. Недостатком этого метода является возможность передачи кадра, содержащего ошибки, так как контрольная сумма находится в конце кадра.
    2. Коммутация без фрагментации (Fragment-Free Switching). В правильно работающей сети 10BASE-T или 100BASE-T обнаружить коллизию можно по первым 64 байтам. Поэтому в этом методе принимаются первые 64 байта, проверяется наличие коллизии и только затем производится пересылка кадра. Коммутаторы Cisco по умолчанию работают в режиме Fast-Forward-Switching, но если возникают проблемы, то переключаются в режим Store-and-Forward.

8.1.2. Процедура сброса пароля

Восстановление забытого пароля на коммутаторах серии 2950.

1. Подключитесь к коммутатору с помощью терминальной программы (Гипертерминал) через консоль.
2. Отключите кабель питания.

3. Нажмите кнопку режимов (mode) на панели коммутатора и удерживайте, пока не присоедините кабель питания обратно.
4. Отпустите кнопку после того, как потухнет индикатор STAT LED.
5. Напечатайте команду `load_helper`.
6. Напечатайте `dir flash:` вы должны увидеть конфигурационный файл `config.text`.
7. Переименуйте конфигурационный файл `rename flash:config.text flash:config.old`, именно этот файл содержит пароли.
8. Перезагрузите коммутатор командой `boot`.
9. Ответьте `no` на вопрос о запуске диалога конфигурирования.
10. Перейдите в привилегированный режим `enable`.
11. Переименуйте файл конфигурации обратно: `rename flash:config.old flash:config.text`.
12. Скопируйте конфигурационный файл в память: `copy flash:config.text system:running?config`
13. Измените забытые пароли.
14. Сохраните изменения командой `copy system:running?config flash:config.text`.

8.1.3. VLAN и маршрутизация VLAN

Виртуальная локальная вычислительная сеть (VLAN[1] — Virtual Local Area Network) — это способ логического группирования хостов по подключению (по портам коммутатора) или по MAC-адресам хостов. В первом случае используют термин «*статические VLAN*», а во втором — «*динамические*». Для создания VLAN можно использовать один или несколько коммутаторов, объединённых в единый блок. Применение VLAN преследует следующие цели.

1. Контроль широковещательной рассылки. Широковещание второго уровня осуществляется в пределах одного VLAN.
2. Безопасность. Трафик одного VLAN не может наблюдаться в другом VLAN. Тем самым повышается безопасность передаваемых данных.
3. Гибкость и масштабируемость. Применение технологии виртуальных сетей позволяет легко управлять членством в VLAN, а также

[1]Будем произносить эту аббревиатуру как «Вилан» и считать, что это слово мужского рода.

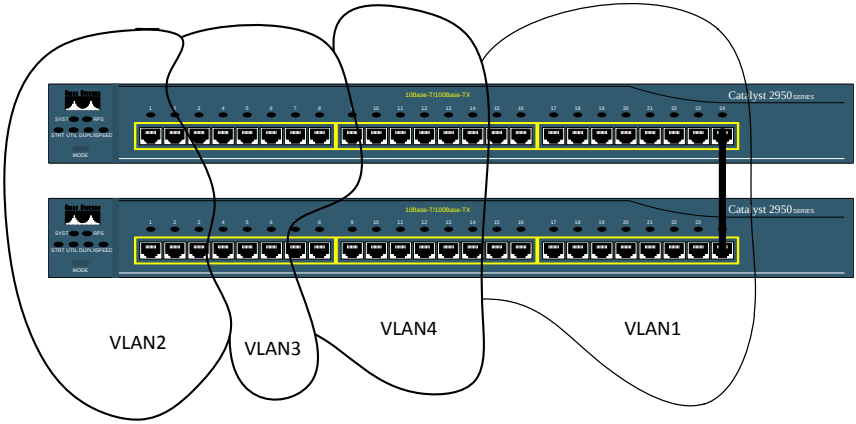


Рис. 8.2. Пример объединения портов в VLAN

легко достичь расширяемости сети за счёт добавления в блок коммутаторов дополнительных устройств.

Выделяют два типа VLAN:

1. Статический VLAN. Администратор назначает порты коммутаторов в VLAN. Таким образом, все хосты, подключенные к одному порту, находятся в одном VLAN. На представленной схеме (рис. 8.2) изображен блок из двух коммутаторов, объединённых в блок по 24-м портам. Все порты объединены в VLAN-ы. VLAN2 принадлежат 1, 2 порты первого коммутатора и 1, 2, 3 порты второго. VLAN3: 3, 4, 5, 6, 7, 8, 9 — первого коммутатора, 4, 5, 6 — второго коммутатора. VLAN4: 10, 11, 12, 13, 14 — порты первого коммутатора, 6, 7, 8, 9, 10, 11, 12, 13, 14 — второго. Остальные порты принадлежат первому VLAN.
2. Динамические VLAN характеризуются наличием выделенного коммутатора, на котором осуществляется настройка VLAN путём назначения MAC-адресов в VLAN.

Идентификация VLAN. VLAN изолируют трафик так, что кадры одного VLAN не видны другому, в том числе и широковещательные. Коммутаторы различают кадры VLAN с помощью специальных меток (tags). Иногда говорят, что кадры «окрашиваются». Соответствующий английский термин — Tagging. По сути, «окрашивание» реализуется

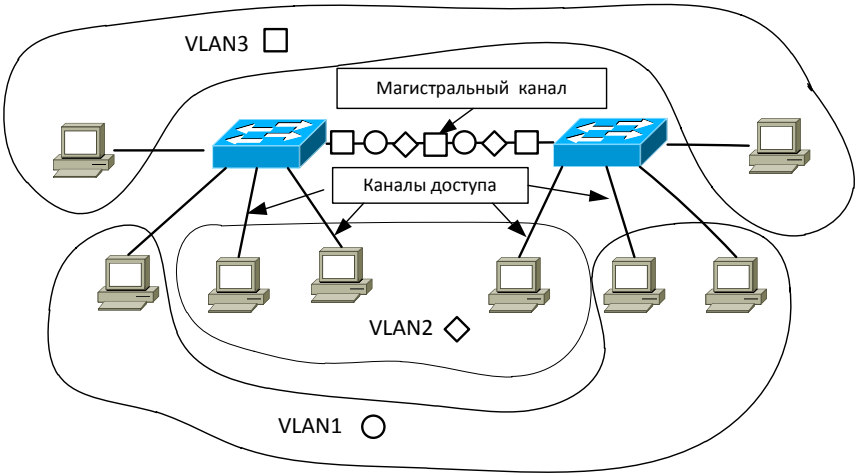


Рис. 8.3. Понятия магистрального канала и канала доступа

специальным полем в кадре, хранящем номер VLAN.

В коммутируемой среде существует два типа каналов: канал доступа и магистральный канал. *Канал доступа* — это канал, который не содержит «окрашенных» фреймов, это всегда часть одного VLAN. Порт канала доступа не знает о других VLAN.

Магистральный, или *транковый* канал (trunk link) — это канал, который служит для связи между коммутаторами и поддерживает передачу кадров различных VLAN. Концы магистрального канала называются *транковыми портами* (trunk ports). Эти понятия иллюстрируются на рис. 8.3.

В сети Ethernet для окраски кадров используют два способа идентификации. **ISL (Inter Switch Link)** — межкоммутационные каналы. Этот протокол — изобретение Cisco, поэтому поддерживается не всеми производителями. ISL применяется для каналов FastEthernet и GigabitEthernet. Может использоваться на портах коммутаторов, маршрутизаторов и сетевых картах серверов для того, чтобы трафик не пересекал устройства третьего уровня.

В этом протоколе используется внешняя инкапсуляция (внешнее тэгирование). Добавляется новый 26-байтовый заголовок ISL. Передаётся информация о VLAN и коммутаторе, с которого он поступил. Сам кадр не изменяется, только в конец добавляется ещё одна контрольная сумма.

Тэгированный кадр может существовать только в магистральном канале, при отправке его в канал доступа ISL-заголовок удаляется. Если Вы нуждаетесь в стандартном протоколе Ethernet VLAN, поддерживаемом всеми производителями, то используйте 802.1q.

IEEE 802.1q. Для окрашивания кадров использует внутренняя инкапсуляция. Формат фрейма предполагает 4-байтовое поле, вставляемое между полем адреса источника (SA) и полем длины или типа (Type или Length). Контрольная сумма пересчитывается после каждой вставки или удаления тэга.

В каналах доступа такой кадр выглядит как обычный кадр немного большей длины.

Отсутствие окраски также является окраской. VALN, чьи кадры не окрашиваются, называется native VLAN-ом. На транковом интерфейсе может существовать только один native VLAN. На концах магистрального канала номера native VLAN-ов должны быть одинаковыми, в противном случае возможно протекание трафика из одного VLAN-а в другой.

8.1.4. Маршрутизация между VLAN

Для передачи данных между VLAN необходимы устройства третьего уровня: маршрутизаторы или коммутаторы со специальными модулями маршрутизации. Когда используют модули маршрутизации на коммутаторах, говорят о внутренней маршрутизации. А когда используются маршрутизаторы, то говорят о внешней маршрутизации. Существует две основные схемы (см. рис. 8.4, 8.5), реализующие внешнюю маршрутизацию между VLAN.

Важно! Обязательным условием для взаимодействия между VLAN в обоих типах схем является правило:

«Один VLAN — одна IP-подсеть!»

Для первого типа необходимо иметь столько Ethernet-портов на маршрутизатор, сколько имеется VLAN. Это единственный выход, если маршрутизатор не поддерживает магистральных каналов (не имеет транковых портов). Для второго типа (рис. 8.5) достаточно иметь один транковый порт. В этом случае на интерфейсе маршрутизатора настраиваются подинтерфейсы, между которыми и осуществляется маршрутизация с одновременным перекрашиванием кадров. Каждому интерфейсу должен быть назначен свой адрес из соответствующей подсети, тип инкапсуляции и принадлежность VLAN.

Обе схемы фактически реализуют одну и ту же идею: «Взаимодей-

ствие между VLAN должно осуществляться через устройства третьего уровня».

Внутренняя маршрутизация осуществляется на коммутаторах, в которых присутствует модуль внутреннего процессора маршрутов. Для более детального ознакомления с вопросами внутренней маршрутизации отсылаем к [7, 8].

8.1.5. Настройка статических VLAN

Настройка статических VLAN осуществляется в два этапа:

1. Создание VLAN на коммутаторе:
   `(config)# vlan <идентификатор VLAN>` — ввод идентификатора VLAN.
2. Назначение портов в VLAN:
   `(config-if)# switchport mode access` — указать, что интерфейс является портом доступа.
   `(config-if)# switchport access vlan <номер VLAN>` — назначить порт в VLAN.

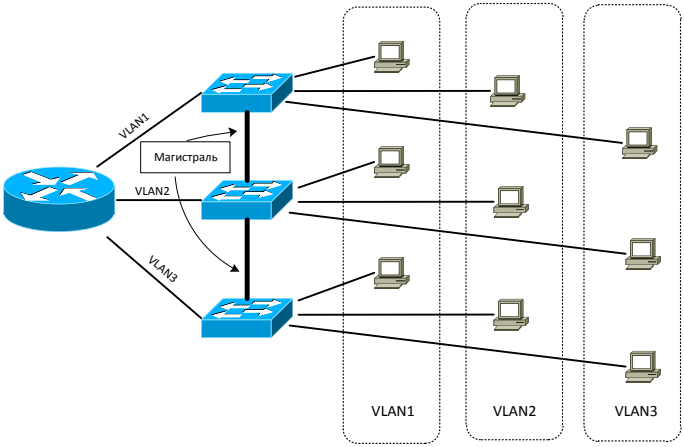


Рис. 8.4. Первый тип внешней маршрутизации между VLAN (традиционная схема)

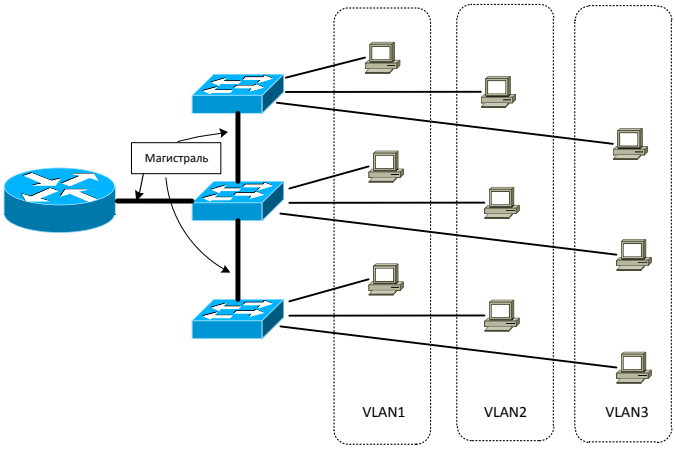


Рис. 8.5. Второй тип внешней маршрутизации между VLAN (Router-on-Stick)

Команды настройки магистрали

Для маршрутизации между VLAN дополнительно требуется настройка магистрали. Для настройки транкового (магистрального) порта на коммутаторе достаточно использовать команду

```
(config-if)# switchport mode trunk
```

Для настройки транкового (магистрального) порта на маршрутизаторе в режиме конфигурирования вводятся команды:

```
(config)# interface <имя подинтерфейса>
(config-subif)# encapsulation <тип инкапсуляции>
                              <номер VLAN>
```

Имя подинтерфейса формируется из имени основного интерфейса, точки и номера. Подинтерфейс создается в момент первого обращения к нему. Вместо `<тип инкапсуляции>` — обычно подставляется значение dot1q, соответствующее инкапсуляции 802.1q. Для того чтобы маршрутизация заработала, необходимо настроить два логических подинтерфейса (в нашем случае физический интерфейс f0/0 разбивается на два логических f0/0.1 и f0/0.2) и назначить им IP-адреса, соответствующие VLAN.

Например, так:

```
        # interface f0/0.1
(config)# encapsulation dot1q 1
(config)# ip address 192.168.1.1 255.255.255.0
(config)# interface f0/0.2
(config)# encapsulation dot1q 1
(config)# ip address 192.168.2.1 255.255.255.0
(config)# interface f0/0
(config)# no shutdown
```

Рекомендуется, чтобы номер подсети, номер подинтерфейса и номер VLAN совпадали. Это необходимо для того, чтобы в последующем было проще разобраться в существующих настройках.

Дополнительно настраивать маршрутизацию нет необходимости, так как все сети присоединённые.

8.1.6. Команды диагностики VLAN

Настройки VLAN и настройки самого коммутатора физически хранятся в разных файлах на flash-памяти. Настройки VLAN хранятся в файле `vlan.dat`, текущие настройки (`running-config`) — в оперативной памяти, а стартовые (`startup-config`) — в файле `config.text` на flash. Для полного удаления настроек VLAN необходимо физически удалить файл `valn.dat` командой `delete`:

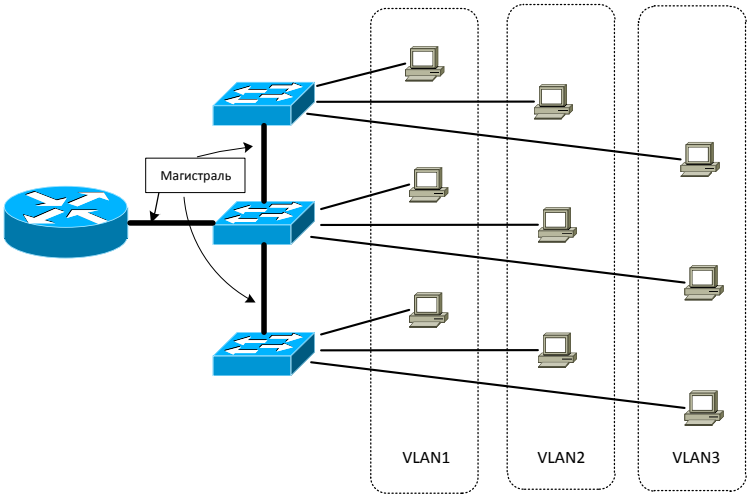
```
# delete valn.dat
```

Для диагностики используются команды из табл. 8.1.

Таблица 8.1. Команды диагностики VLAN

Команда	**Описание**
`show vlan`	Отображает список существующих VLAN и принадлежащих им портов.
`show running-config vlan`	Показывает содержимое файла конфигурации с настройками VLAN.
`show interfaces [идентификатор VLAN]`	Отображает параметры VLAN-интерфейса, в том числе назначенные на управляющий VLAN ip-адрес.
`show interfaces <имя интерфейса> switchport`	Просмотр информации о настройках интерфейса
`show interfaces trunk`	Отображает информацию о транковых интерфейсах.

8.2. Задание к лабораторной работе

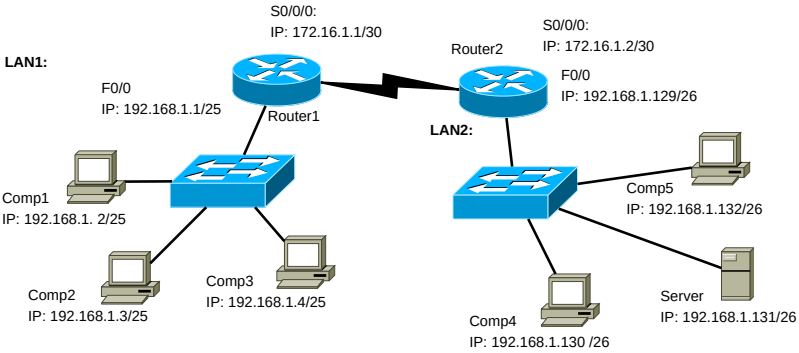


1. Реализуйте схему, представленную на рисунке.
2. Распределите IP-адреса для всех компьютеров из одного и того же диапазона. Пусть это будет 192.168.0.0/24.
3. Проверьте связность построенной схемы. В случае обнаружения неисправностей устраните их.
4. Настройте VLAN-ы.
5. Протестируйте связность.
6. Промежуточный результат продемонстрируйте преподавателю.
7. Настройте маршрутизатор в режиме Roter-on-Stick: разбейте интерфейс на подинтерфейсы, соответствующие Vlan-ам, произведите изменение схемы IP-адресации в соответствии с правилом: «Один VLAN — одна IP-подсеть».
8. Проверьте связность.
9. Продемонстрируйте результат преподавателю.
10. Создайте список контроля доступа, запрещающий обращения первого компьютера первого VLAN-а к третьему компьютеру третьего VLAN-а.
11. Назначьте список на подходящий интерфейс и протестируйте его работу.
12. Результаты продемонстрируйте преподавателю.
13. Удалите настройки VLAN. Убедитесь, что они удалены.

14. Настройте VLAN-ы и маршрутизацию между ними по следующим требованиям: первый и второй коммутаторы свои порты f0/1 объединяют в VLAN10, второй и третий коммутаторы — f0/2 объединяют в VLAN20, третий и первый — f0/3 в VLAN30; первый и второй коммутаторы свяжите между собой по f0/24, а второй и третий по f0/23; маршрутизатор подключите к f0/24 третьего.
15. Выполните настройки VLAN.
16. Добейтесь связности в такой конфигурации сети.
17. Продемонстрируйте работу сети преподавателю.

8.3. Контрольная работа №8. Настройки ACL

Дана схема сети:



Создайте список доступа для запрета http-трафика от сети LAN2 к сети LAN1. Напишите последовательность команд, размещающих данный список доступа, указав маршрутизатор, интерфейс и направление трафика.

Глава 9
Протокол DHCP. Технология NAT

9.1. Методический материал

9.1.1. Основы DHCP

DHCP (Dynamic Host Configuration Protocol) предназначен для автоматической настройки компьютеров локальной сети. DHCP — клиент-серверный протокол, в работе которого используются DHCP-серверы и DHCP-клиенты. DHCP-сервер — это хост, на котором запущена служба, способная выдавать необходимые для работы протоколов стека TCP/IP настройки любому DHCP-клиенту, который их затребовал. В список этих настроек обычно входят: IP-адрес хоста, маска подсети, шлюз по умолчанию, адрес DNS-сервера.

Запустить службу DHCP можно на любом сервере Microsoft (например, на MS Windows Server), на хостах под управлением Unix/Linux или на маршрутизаторах под управлением Cisco IOS.

DHCP-сервер имеет список (пул) IP-адресов, которые ему разрешено выдавать клиентам. Клиенты арендуют эти адреса на определённый период времени, обычно на несколько дней. Когда время аренды истекает, клиент направляет запрос на сервер для продления аренды адреса или его замены.

DHCP-клиенты — это хосты, на которых запущен DHCP-клиент для взаимодействия с DHCP-сервером[1].

DHCP-клиент получает в аренду IP-адрес, маску подсети и различные дополнительные настройки от DHCP сервера в четыре шага (рис. 9.1):

1. DHCPDISCOVER: клиент посылает широковещательный UDP-запрос в поисках DHCP-сервера.
2. DHCPOFFER: DHCP-серверы предлагают адреса клиенту.
3. DHCPREQUEST: клиент посылает широковещательный запрос на получение аренды IP-адреса от одного из DHCP-серверов.
4. DHCPACK: DHCP-сервер, к которому обратились, подтверждает назначение адреса и дополнительных настроек и обновляет свою DHCP-базу данных арендованных IP-адресов. Затем клиент

[1] В Windows-системах настройка сетевого адаптера называется «Получить IP-адрес автоматически», находится в свойствах адаптера, в настройках TCP/IP.

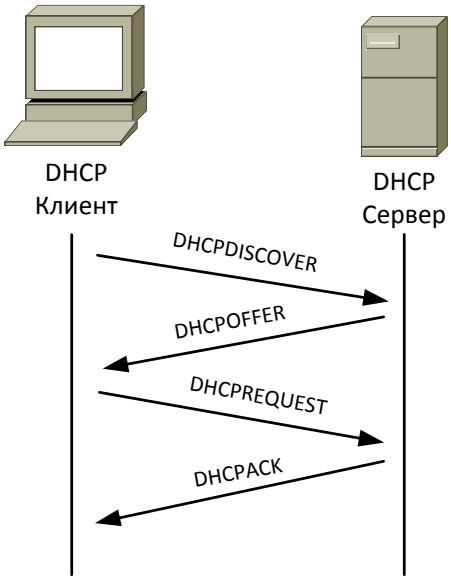


Рис. 9.1. Этапы процедуры получения настроек по DHCP

инициализирует стек протоколов TCP/IP, после чего он может участвовать в сетевых коммуникациях.

Продление аренды состоит только из третьего и четвёртого шагов. Обновление требуется, когда истекло 50% времени аренды.

Когда используется DHCP, необходимо обратить внимание на следующее:

- DHCP-серверы не имеют общей базы данных арендованных адресов, так что, если имеется более одного DHCP-сервера, необходимо убедиться, что списки адресов не перекрываются.
- Необходимо обеспечить сервер всеми DHCP-настройками, которые могут затребовать клиенты.
- Необходимо назначить статические адреса для тех хостов, которые не являются DHCP-клиентами, и исключить эти адреса из списков арендуемых адресов.
- Необходимо назначить статические адреса всем серверам локальной сети или настроить резервирование на DHCP-сервере, чтобы быть уверенным, что сервер арендует один и тот же IP-адрес. В

противном случае сетевые службы, размещённые на этих серверах, могут оказаться недоступными.

- Сконфигурировать перенаправление широковещательных DHCP-запросов (на DHCP-посреднике), если DHCP-сервер обслуживает несколько подсетей, так как маршрутизаторы не пропускают широковещательный трафик.

9.1.2. Пример настройки DHCP

Рассмотрим настройку DHCP на примере (рис. 9.2).

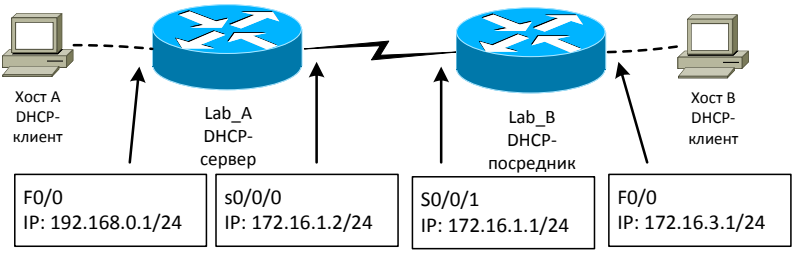


Рис. 9.2. Схема сети для разбираемого примера

0. Предварительно должна быть настроена маршрутизация, например, так:
на маршрутизаторе `Lab_A`

```
# conf t
(config)# router rip
(config-router)# network 172.16.1.0
(config-router)# network 192.168.0.0
```

на маршрутизаторе `Lab_B`

```
# conf t
(config)# router rip
(config-router)# network 172.16.1.0
(config-router)# network 172.16.3.0
```

1. Конфигурируем `Lab_A` как DHCP-сервер для клиентов на 192.168.0.0/24:

```
(config)# service dhcp
```

2. Если необходимо, то можно исключить часть адресов (например, первые десять) из ещё несозданного пула. Тогда эти адреса можно будет использовать для статических назначений для серверов и маршрутизаторов.

```
(config)# ip dhcp excluded-address
                192.168.0.1 192.168.0.10
```

Здесь в параметрах указаны начальный и конечный адреса диапазона, который DHCP выдавать не будет.

3. Далее, сконфигурируем сам адресный пул для сети 192.168.0.0:

```
(config)# ip dhcp pool NET192
(dhcp-config)# network 192.168.0.0 255.255.0.0
```

4. В режиме конфигурирования DHCP назначаем следующие IP-настройки: шлюз по умолчанию, DNS-сервер, WINS-сервер и имя домена:

```
(dhcp-config)# default-router 192.168.0.1
(dhcp-config)# dns-server 192.168.0.3
(dhcp-config)# netbios-name-server 192.168.0.5
(dhcp-config)# domain-name fcs
```

5. Так как хосту B также требуется динамическое конфигурирование, создаём второй DHCP-пул адресов с адресами и шлюзом, соответствующими сети 172.16.3.0 /24:

```
(config)# ip dhcp pool net172
(dhcp-config)# network 172.16.3.0 255.255.255.0
(dhcp-config)# default-router 172.16.3.1
(dhcp-config)# dns-server 192.168.0.3
(dhcp-config)# netbios-name-server 192.168.0.5
(dhcp-config)# domain-name fcs
```

6. Конфигурирование DHCP-сервера выполнено, но хост B использует UDP-широковещание для поиска IP-адресов, и `Lab_B` не сконфигурирован на пересылку широковещательных запросов. Для того, чтобы DHCP работал для сети хоста B, необходимо сконфигурировать FastEthernet интерфейс `Lab_B` на пересылку UDP-широковещания на `Lab_A`:

```
(config)# interface f0/0
(config)# ip helper-address 172.16.1.2
```

9.1.3. Диагностика и устранение неполадок DHCP

На хосте под управлением Windows для диагностики используется команда ipconfig с различными параметрами: `ipconfig /release` — очистить текущие IP-настройки хоста. `ipconfig /renew` — обновить IP-настройки хоста[1]. `ipconfig /all` — посмотреть все текущие настройки сетевых интерфейсов.

На маршрутизаторе для диагностики неисправностей используются команды `show ip dhcp` с опциями `conflict` или `binding`, которые показывают соответственно конфликты выданных адресов и все выданные в аренду адреса. Без параметров показывает текущие настройки сервера.

9.1.4. Основы технологии NAT

Трансляция сетевых адресов преследует три цели. Первая — экономия адресного пространства. Вторая — сокрытие внутренней структуры сети. Третья — распределение нагрузки на внутренние серверы. Трансляция адресов описана в RFC 1631. Прежде чем описывать трансляцию, необходимо ввести ряд определений.

Термины и определения

Опр. NAT (Network Address Translation) — технология трансляции адресов, позволяющая подменять IP-адреса источников пакетов, пересылаемых из внутренней сети во внешнюю и наоборот.

Опр. *Внутренняя сеть* — множество адресов локальной сети, которые транслируются вовне. Внутренние адреса обычно выбираются из так называемых приватных диапазонов, описанных в RFC 1918.

Опр. *Внешняя сеть* — все другие адреса, отличные от внутренних. Обычно это законные адреса Интернет.

Опр. *Внутренние локальные адреса* — адреса, назначенные хостам во внутренней сети, как правило, из приватного диапазона адресов.

Опр. *Внутренние глобальные адреса* — адреса, под которыми видны хосты внутренней сети из внешней, это адреса, на которые заменяются внутренние локальные адреса при трансляции SourceNAT. Обычно это реально действующие адреса Интернет, полученные от провайдера.

Опр. *Внешний локальный адрес* — адрес внешнего хоста, как он видится во внутренней сети. Не будучи обязательно легальным адресом, он берётся из адресного пространства, маршрутизируемого внутри.

[1]Указанные две команды, как правило, выполняются последовательно.

Опр. *Внешний глобальный адрес* — адрес внешнего хоста, назначенный ему.

NAT может выполнять три основные функции, перечисленные ниже:

1. Трансляция внутренних локальных адресов во внутренние глобальные (*статический* и *динамический* NAT). У пересылаемого во внешнюю сеть пакета подменяется IP-адрес источника, а когда приходит ответ, IP-адрес восстанавливается. Запись о такой замене может быть как статической, так и динамической .
2. *Совмещение внутренних глобальных адресов* (Overloading) — технический приём, использующий TCP или UDP порты источников так, что несколько хостов могут одновременно использовать один и тот же внутренний глобальный адрес. При этом подменяется не только адрес источника, но и порт.
3. *Распределение нагрузки* (Distributed NAT) – технический прием, позволяющий скрывать за одним внутренним глобальным адресом несколько локальных серверов с разными внутренними локальными адресами. Осуществляется за счёт трансляции внешнего глобального адреса во внешний локальный.

Настройка статической трансляции сетевых адресов

Статическое связывание часто необходимо для публичных серверов, находящихся во внутренней сети. Им необходим постоянный внутренний глобальный адрес. Настройка статического NAT осуществляется за три шага.

1. Создаём статическую запись в таблице трансляции:
```
(config)# ip nat inside source static
                        <внутр. лок. адрес>
                        <внут. глоб. адрес>
```
2. Определяем внутренний интерфейс:
```
(config-if)# ip nat inside
```
3. Определяем внешний интерфейс:
```
(config-if)# ip nat outside
```

Настройка динамической трансляции NAT и совмещения

Динамическая трансляция называется так потому, что запись соответствия в таблице трансляции создаётся в момент получения маршрутизатором трафика. Соответствие между локальным и глобальным адресом строится и запоминается «на лету». Через определённое время созданная запись уничтожается.

Настройка динамической трансляции осуществляется за пять шагов:

1. Создаем пул (список) глобальных адресов, в которые будет производиться трансляция.

```
(config)# ip nat pool <имя пула>
                      <стартовый ip> <конечный ip>
                      {netmask <маска подсети> |
                      prefix-length <длина маски>}
```

2. Создаём список доступа, идентифицирующий внутренние локальные адреса, которые будут транслироваться:

```
(config)# access-list <номер списка>
           permit <адрес источника> [шаблон маски]
```

3. Конфигурируем динамический NAT, основанный на адресах источников:

```
(config)# ip nat inside source
                list <номер списка доступа>
                pool <имя пула> [overload]
```

Чтобы настроить совмещение внутренних глобальных адресов с применением индивидуальных портов TCP, позволяющее многократно использовать IP-адрес, добавьте после имени пула NAT синтаксис overload. При этом будут создаваться расширенные записи таблицы NAT, содержащие информацию о портах. 4. Определяем внутренний интерфейс:

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

5. Определяем внешний интерфейс:

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

Распределение нагрузки TCP

Такой тип трансляции позволяет отобразить один глобальный адрес во множество внутренних локальных с целью распределения обращений ко многим хостам (серверам). Пусть имеется публичный web-сервер, размещённый на кластере из двух компьютеров, имеющих самостоятельные IP-адреса. Следующие шаги необходимы для конфигурирования распределения TCP нагрузки между компьютерами кластера:

1. Определяется пул адресов, между которыми распределяется нагрузка:

```
(config)# ip nat pool <имя пула>
                      <стартовый ip> <конечный ip>
                      {netmask <маска подсети> |
                      prefix-length <длина маски>}
                      type rotary
```

2. Создаётся список доступа, выбирающий адреса виртуальных хостов (обычно стандартный):
```
(config)#access-list <номер списка>
             permit <адрес источника>
             [шаблон маски]
```
3. Настраивается динамическая трансляция адресов места назначения, идентифицируемых списком доступа на предыдущем шаге:
```
(config)#ip nat inside destination
               list <номер списка доступа>
               pool <имя пула>
```
4. Определяем внутренний интерфейс:
```
(config-if)# ip nat inside
```
5. Определяем внешний интерфейс:
```
(config-if)# ip nat outside
```

9.1.5. Примеры настройки NAT

Пример. Пусть дана сеть (см. рис. 9.3). Необходимо связать локальный адрес сервера с глобальным адресом так, чтобы любой из внешней сети мог обратиться к серверу.

Конфигурируем маршрутизатор:

```
conf t
ip nat inside source static 10.1.2.25 193.168.0.55
interface f0/0
ip nat inside
int s0/0/0
ip nat outside
```

Продолжаем пример. По-прежнему дана сеть, представленная на рис. 9.3. Необходимо обеспечить выход в Интернет всем хостам внутренней сети 10.1.0.0 /16. Дан диапазон из ста внутреннних глобальных адресов от 193.168.0.1 до 193.168.0.100.

```
# ip nat pool INTERNETIPPOOL
       193.168.0.1 193.168.0.100
```

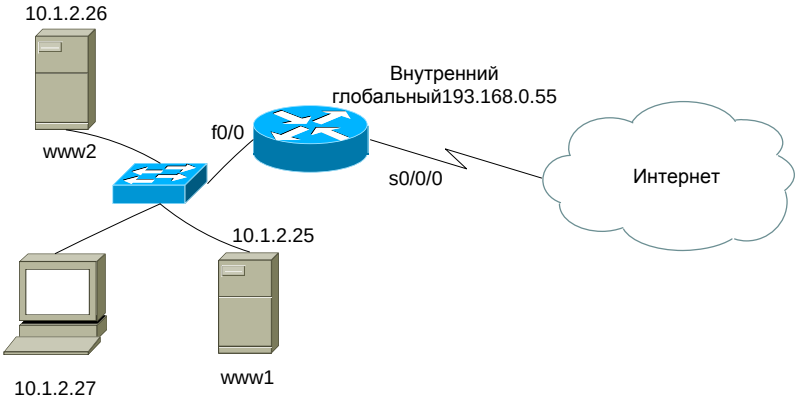


Рис. 9.3. Схема для настройки NAT

```
      netmask 255.255.255.0
# access-list 2 permit 10.1.0.0 0.0.255.255
# ip nat inside source
        list 2
        pool INTERNETIPPOOL
        overload
# interface f0/0
# ip nat inside
# interface s0/0/0
# ip nat outside
```

Вернемся к схеме на рис. 9.3. Можно распределить нагрузку Web-сервера с адресом 193.168.0.55 между www1 (10.1.2.25) и www2 (10.1.2.26).

```
# ip nat pool WEBSERVERS 10.1.2.25 10.1.2.26
            prefix-length 24 type rotary
# access-list 3 permit host 193.168.0.55
# ip nat inside destination list 3
                            pool WEBSERVERS
# interface f0/0
# ip nat inside
# interface s0/0/0
# ip nat outside
```

9.1.6. Диагностика и устранение неполадок NAT

При проверке настроек NAT помогут следующие команды. Команда `show ip nat translation` показывает трансляции в таблице NAT. Команда `show ip nat translation verbose` отображает другие сведения таблицы NAT, например, время устаревания записей в таблице NAT.

Команда `show ip nat statistics` отображает некоторые сведения о настройке, статистику трансляций и данные записей в таблице NAT.

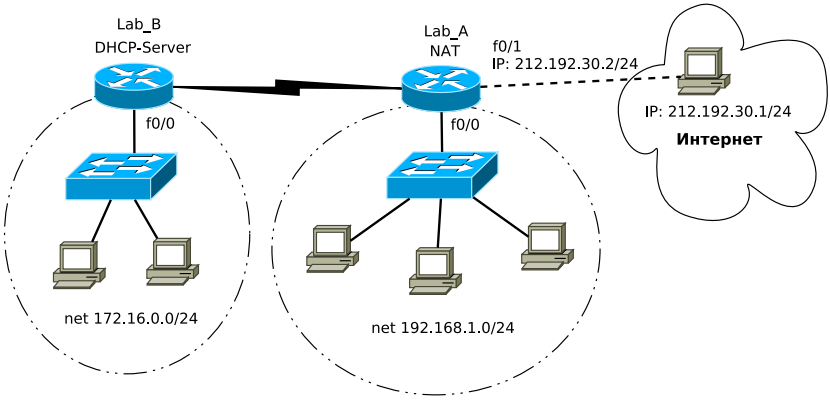
Продиагностировать проблемы с NAT помогает команда `debug ip nat`. Бывает, что протокол NAT настроен правильно, но трансляции не производятся. Как правило, проблема устраняется удалением трансляций NAT.

`clear ip nat translation *` — удаляет все записи таблицы NAT.

`clear ip nat translation protocol *` — удаляет все расширенные записи таблицы NAT.

9.2. Задание к лабораторной работе

1. Соберите схему сети:



2. Выполните базовую настройку маршрутизаторов с динамической маршрутизацией OSPF для автономной области с номером 0.
3. На граничном маршрутизаторе настройте интерфейс f0/1, который будет имитировать подключение к сети интернет через провайдера.
4. На маршрутизаторе `Lab_B` настройте DHCP-пулы для двух локальных сегментов сети. Необходимо раздавать настройки, в которые входит: ip-адрес, ip-адрес шлюза по умолчанию, dns-сервер. Реального dns-сервера в лабораторных условиях не будет, поэтому пусть этот адрес будет 192.168.1.2.
5. Компьютеры локальных сетей настройте на получение настроек автоматически.
6. Проверьте работоспособность DHCP.
7. На маршрутизаторе `Lab_A` настройте посредника для «проброса» широковещательных запросов.
8. Настройте на граничном маршрутизаторе `Lab_A` маршрут по умолчанию к Провайдеру.
9. Настройте распространение маршрута по умолчанию в таблицах OSPF[1].
10. Убедитесь в распространении маршрута по умолчанию.
11. На маршрутизаторе `Lab_A` настройте трансляцию сетевых адресов в сеть Провайдера.
12. Убедитесь, что трансляция осуществляется. При необходимости устраните обнаруженные неисправности.

[1] Команда `default-information originate`.

9.3. Контрольная работа №9. VLAN

1. Где используется инкапсуляция 802.1q? Укажите все правильные ответы.
   A. На портах доступа коммутатора.
   B. На транковых портах коммутатора.
   C. На портах доступа маршрутизатора.
   D. На подинтерфейсах маршрутизатора.

2. Какая команда отображает транковые порты на коммутаторе?
   A. show vlan
   B. show interface trunk
   C. show trunk
   D. show switchport

3. Какая из последовательностей команд правильно активирует подинтерфейсы маршрутизатора?

   A.
```
int f0/0.1
enc dot1q 1
ip add 192.168.1.1 255.255.255.128
int f0/0.2
enc dot1q 2
ip add 192.168.1.129 255.255.255.128
int f0/0
no shut
```

   B.
```
int f0/0.1
enc dot1q 1
ip add 192.168.1.1 255.255.255.128
int f0/0.2
no shut
enc dot1q 2
ip add 192.168.1.129 255.255.255.128
no shut
```

   C.
```
int f0/0
enc dot1q
no shut
int f0/0.1
ip add 192.168.1.1 255.255.255.128
int f0/0.2
ip add 192.168.1.129 255.255.255.128
```

4. Что такое native vlan?

A. Это другое название управляющего vlan.

B. Это vlan, формат кадра которого на транке не имеет полей 802.1q.

C. Это vlan, который не имеет номера.

D. Это проприетарный vlan cisco.

E. Это vlan стандарта IEEE.

5. Посмотрите вывод команды `show vlan`.

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

Укажите две наиболее вероятные причины отсутствия в списке интерфейса f0/1:

A. интерфейс стал транковым.

B. vlan, которому принадлежит интерфейс, стал native.

C. vlan, которому принадлежит интерфейс, был удалён.

D. vlan, которому принадлежит интерфейс, был удалён с транкового канала.

Список использованной литературы

1. Routers and Routing Basics CCNA 2 Companion Guide. URL: http://ptgmedia.pearsoncmg.com/images/1587131668/samplechapter/1587131668ch01.pdf (дата обращения: 25.09.2012)
2. *Johnson A.* Routing Protocols and Concepts CCNA Exploration Labs and Study GuideInstructor Edition. Cisco Press. 558 p. URL: http://www.scribd.com/doc/49995565/1/Label-the-Internal-Components-of-a-Router-Exercise (дата обращения: 25.09.2012)
3. CDP // Википедия. [2012—2012]. Дата обновления: 27.01.2012. URL: http://ru.wikipedia.org/?oldid=41193432 (дата обращения: 27.01.2012)
4. Configuring Cisco Discovery Protocol on Cisco Routers and Switches Running Cisco IOS. URL: http://www.cisco.com/en/US/tech/tk962/technologies_tech_note09186a00801aa000.shtml
5. *Лавров Д.Н.* Сети и системы телекоммуникаций: учебное пособие. Омск : Изд-во ОмГУ, 2006. 187 с.
6. *Леммл Т., Одом Ш., Уоллес К.* CCNP. Маршрутизация. М. : Лори, 2002. 444с.
7. *Одом Ш., Ноттингем О.* Коммутаторы Cisco. М. : КУДИЦ-ОБРАЗ, 2003. 523 с.
8. *Леммл Т., Хейлз К.* CCNP. Настройка коммутаторов Cisco. М. : Лори, 2002. 464 с.
9. Настройка NTP на устройствах Cisco // ciscomaster.ru. URL: http://ciscomaster.ru/node/80 (дата обращения: 6.03.13).
10. Синхронизация времени по протоколу NTP на устройствах Cisco // AdminDoc.Ru — Сайт сетевых профессионалов. URL: http://ciscomaster.ru/node/80 (дата обращения: 6.03.13).

Учебное издание

Лавров *Дмитрий Николаевич*

ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО КОММУТАЦИИ И МАРШРУТИЗАЦИИ

Редактор Л.М. Кицина
Оформление обложки З.Н. Образова

Сертификат соответствия № РОСС RU.AE88.H01449
Срок действия с 26.07.2012 г. по 25.07.2015 г.

Подписано в печать 15.05.2013. Формат бумаги 60x84 1/16. Печ. л. 6,25.
Усл.-печ. л. 5,8. Уч.-изд. л. 5. Тираж 170 экз. Заказ 88.

Издательство Омского государственного университета
644077, Омск–77, пр. Мира, 55а
Отпечатано на полиграфической базе ОмГУ