

Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет инфокоммуникаций

Кафедра инфокоммуникационных технологий

В. Ю. Бунас, А. С. Зеленин

**ОСНОВЫ ПОСТРОЕНИЯ
ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ.
ЛАБОРАТОРНЫЙ ПРАКТИКУМ**

*Рекомендовано УМО по образованию в области информатики
и радиоэлектроники для специальности
1-45 01 01 «Инфокоммуникационные технологии (по направлениям)»
и направления специальности
1-45 01 02-01 «Инфокоммуникационные системы (стандартизация,
сертификация и контроль параметров)»
в качестве учебно-методического пособия*

Минск БГУИР 2017

УДК 654(076.5)
ББК 32.88я73
Б91

Рецензенты:

кафедра телекоммуникаций и информационных технологий
Белорусского государственного университета
(протокол №9 от 01.03.2016);

декан факультета повышения квалификации и переподготовки кадров
учреждения образования
«Белорусская государственная академия связи»,
кандидат технических наук, доцент О. Р. Ходасевич

Бунас, В. Ю.

Б91 Основы построения инфокоммуникационных систем и сетей. Лабораторный практикум : учеб.-метод. пособие / В. Ю. Бунас, А. С. Зеленин. – Минск : БГУИР, 2017. – 102 с. : ил.
ISBN 978-985-543-320-1.

Содержит описание четырёх лабораторных работ, в которых предлагается изучить основы построения, функционирования и администрирования современных устройств распределения информации: коммутаторы и маршрутизаторы. В них также исследуются базовые принципы маршрутизации и коммутации пакетных данных, отдельно рассматриваются вопросы конфигурирования сетевых устройств, защиты доступа, планирования адресного пространства, организации локальных и корпоративных сетей.

УДК 654(076.5)
ББК 32.88я73

ISBN 978-985-543-320-1

© Бунас В. Ю., Зеленин А. С., 2017
© УО «Белорусский государственный университет информатики и радиоэлектроники», 2017

СОДЕРЖАНИЕ

ЛАБОРАТОРНАЯ РАБОТА №1

Сетевые устройства распределения информации: коммутаторы, маршрутизаторы. Внутренняя организация и конструктивное исполнение. Командный интерфейс. Режимы конфигурирования и просмотр конфигурации..... 4

ЛАБОРАТОРНАЯ РАБОТА №2

Сетевые устройства распределения информации: коммутаторы, маршрутизаторы. Первичное конфигурирование и сохранение конфигурации. Защита от несанкционированного доступа..... 26

ЛАБОРАТОРНАЯ РАБОТА №3

Коммутаторы. Таблица коммутации. Способы формирования таблицы коммутации. Подключение компьютера к коммутатору и формирование таблицы коммутации..... 51

ЛАБОРАТОРНАЯ РАБОТА №4

Маршрутизаторы. Таблица маршрутизации. Способы формирования таблицы маршрутизации. Статическое заполнение таблицы маршрутизации. Соединение компьютеров через маршрутизаторы..... 71

ПРИЛОЖЕНИЕ А

Классификация сетевых устройств распределения информации..... 84

ПРИЛОЖЕНИЕ Б

Учебно-лабораторный стенд..... 88

ПРИЛОЖЕНИЕ В

Процедура сброса пароля на сетевых устройствах Cisco..... 91

ПРИЛОЖЕНИЕ Г

Варианты обжима витой пары..... 92

ПРИЛОЖЕНИЕ Д

Список наиболее часто используемых команд в ОС Cisco IOS..... 95

ЛАБОРАТОРНАЯ РАБОТА №1

СЕТЕВЫЕ УСТРОЙСТВА РАСПРЕДЕЛЕНИЯ ИНФОРМАЦИИ: КОММУТАТОРЫ, МАРШРУТИЗАТОРЫ. ВНУТРЕННЯЯ ОРГАНИЗАЦИЯ И КОНСТРУКТИВНОЕ ИСПОЛНЕНИЕ. КОМАНДНЫЙ ИНТЕРФЕЙС. РЕЖИМЫ КОНФИГУРИРОВАНИЯ И ПРОСМОТР КОНФИГУРАЦИИ

1.1 ЦЕЛЬ РАБОТЫ

1.1.1 Изучение принципов функционирования сетевых устройств.

1.1.2 Изучение устройства и конструктивного исполнения коммутаторов и маршрутизаторов.

1.1.3 Изучение базовых принципов управления сетевыми устройствами.

1.2 ЗАДАНИЕ К РАБОТЕ

1.2.1 Ознакомиться с многообразием сетевых устройств и областью их применения в компьютерных сетях.

1.2.2 Изучить внутреннее устройство коммутатора и маршрутизатора.

1.2.3 Познакомиться с процессом подключения к сетевым устройствам через консольный порт и научиться работать с ними через терминальный клиент.

1.2.4 Научиться работать с интерфейсом командной строки (CLI) и просматривать основную информацию о сетевом устройстве.

1.3 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

1.3.1 Назначение коммутатора и маршрутизатора

В современных компьютерных сетях применяются разнообразные сетевые устройства (приложение А). Каждое устройство выполняет определенные функции, которые строго зависят от уровня обработки информации в сетевой иерархии. В общем случае под *сетевым устройством* понимается аппаратное и (или) программное средство, которое осуществляет прием, обработку и продвижение информации между отдельными устройствами в компьютерной сети.

Среди всех сетевых устройств отдельно следует выделить коммутатор и маршрутизатор.

В соответствии с общепринятой классификацией в терминологии модели взаимодействия открытых систем (ВОС¹) *коммутатор (switch)* в общем случае

¹ В англ. литературе более известно под названием сетевой модели Open Systems Interconnection – OSI.

относится к устройствам канального уровня L2 и используется для соединения нескольких устройств в одной сети. В локальной сети коммутаторы отвечают за направление потока данных и управление им на уровне доступа к сетевым ресурсам.

Внимание! В настоящее время в малых и корпоративных сетях передачи данных широко распространены коммутаторы уровня L3, отличающиеся от традиционных коммутаторов наличием усечённых функций маршрутизации, а также возможностью поддержки механизма коммутации между виртуальными сетями (VLAN).

Маршрутизатор (router) представляет собой устройство сетевого уровня (L3 по модели ВОС) и предназначен для объединения различных сегментов сетей, осуществляет передачу пакетов между сетями на основе адресов третьего уровня. Маршрутизаторы способны выбирать наилучший путь в сети для передаваемых данных.

Коммутаторы выполняют большую часть работы на канальном уровне. Для них сеть представляется набором MAC-адресов устройств. Они извлекают эти адреса из заголовков, добавленных к пакетам на канальном уровне, и используют их во время обработки пакетов для принятия решения о том, на какой порт отправить тот или иной пакет.

Маршрутизаторы работают на сетевом уровне модели ВОС. Для маршрутизаторов сеть – это набор сетевых адресов устройств и множество сетевых путей. Маршрутизаторы анализируют все возможные пути между любыми двумя узлами сети и выбирают самый короткий из них. При выборе могут приниматься во внимание и другие факторы, например, состояние промежуточных узлов и линий связи, пропускная способность линий или стоимость передачи данных. Благодаря использованию данной информации, маршрутизатор может осуществлять больше операций с пакетами, чем коммутатор. Поэтому программное обеспечение, необходимое для работы маршрутизатора, является более сложным.

1.3.2 Внутренняя организация и конструктивное исполнение коммутаторов и маршрутизаторов

Поскольку внутренняя организация коммутаторов и маршрутизаторов практически схожа, то далее для удобства изучения материала будет рассмотрено внутреннее устройство только лишь маршрутизатора на примере маршрутизатора производства компании Cisco. Коммутаторы организованы аналогичным образом. Отличия между ними в первую очередь связаны с количеством интерфейсов и особенностями операционной системы.

Все модели коммутаторов и маршрутизаторов содержат следующие компоненты:

- центральный процессор (ЦП);
- оперативное запоминающее устройство (ОЗУ);

- постоянное запоминающее устройство (ПЗУ);
- операционная система (ОС).

Кроме того, маршрутизаторы также могут оснащаться специальной памятью, которая включает в себя флеш-память и энергонезависимое запоминающее устройство (NVRAM).

Как и всем компьютерам, планшетам и интеллектуальным устройствам, сетевым устройствам уровня L2 и L3 требуется центральный процессор, обрабатывающий команды операционной системы, такие как инициализация системы, функции маршрутизации и коммутации.

ЦП необходима операционная система для выполнения маршрутизации и коммутации. Операционная система сетевого взаимодействия, используемая в продуктах компании Cisco (IOS), – это системное программное обеспечение, которое используется для большинства устройств Cisco независимо от их размера и типа.

Маршрутизатор имеет доступ к четырём типам памяти: ОЗУ, ПЗУ, энергонезависимой памяти (NVRAM) и флеш-памяти (таблица 1.1).

Таблица 1.1 – Типы памяти сетевых устройств и их назначение

Память	Энергозависимый / энергонезависимый	Место хранения
ОЗУ	Энергозависимый	– Текущая выполняемая копия IOS. – Файл текущей конфигурации: running-config . – IP-маршрутизация и таблицы ARP. – Буфер пакета
ПЗУ	Энергонезависимый	– Инструкции по загрузке. – Основное программное обеспечение для диагностики. – Ограниченная версия IOS
NVRAM	Энергонезависимый	– Файл загрузочной конфигурации: startup-config
Флеш-память	Энергонезависимый	– IOS. – Прочие системные файлы

1.3.2.1 ОЗУ

ОЗУ используется для хранения различных приложений и процессов, к которым относятся следующие.

1) *Cisco IOS*: при загрузке IOS распаковывается в ОЗУ.

2) *Файл текущей конфигурации*: файл, в котором хранятся команды конфигурации, используемые в настоящий момент системой IOS маршрутизатора. Он также называется **running-config**.

3) *Таблица IP-маршрутизации*: файл, в котором хранится информация о сетях с прямым подключением и об удалённых сетях. Эта таблица используется, чтобы определить наилучший путь для пересылки пакетов.

4) *ARP-кэш*: содержит сопоставления адресов IPv4 с MAC-адресами подобно кэш-памяти ARP (протокола разрешения адресов) на компьютерах.

ARP-кэш используется на маршрутизаторах, которые имеют интерфейсы LAN, такие как Ethernet.

5) *Буфер пакетов*: временно сохраняет пакеты после их поступления на интерфейс или перед их отправкой из него.

Как и компьютеры, маршрутизаторы Cisco используют динамическое оперативное запоминающее устройство (динамическое ОЗУ или DRAM). Динамическое ОЗУ – тип ОЗУ, в котором хранятся инструкции и данные, необходимые для выполнения ЦП. В отличие от ПЗУ ОЗУ является энергозависимой памятью и требует постоянного питания для сохранения своей информации. После отключения питания или перезагрузки маршрутизатора ОЗУ теряет всё своё содержимое.

По умолчанию маршрутизаторы модели Cisco 2901 имеют 512 МБ встроенной памяти DRAM с возможностью расширения до 2 ГБ.

1.3.2.2 ПЗУ

Маршрутизаторы Cisco используют ПЗУ для хранения следующих данных.

- 1) *Указания по загрузке* – информация для запуска устройства.
- 2) *Основное программное обеспечение для диагностики* – самотестирование при включении питания (POST) для всех компонентов.
- 3) *Ограниченная версия IOS* – неполная резервная версия операционной системы на случай, если маршрутизатору не удастся загрузить полноценную IOS.

1.3.2.3 Энергонезависимая память NVRAM

Память NVRAM используется системой Cisco IOS в качестве постоянного хранилища для файла загрузочной конфигурации (файла **startup-config**). Как и ПЗУ, память NVRAM сохраняет своё содержимое после отключения питания.

1.3.2.4 Флеш-память

Флеш-память – энергонезависимая компьютерная память, используемая в качестве постоянного хранилища для IOS и других системных файлов. Во время загрузки IOS копируется из флеш-памяти в ОЗУ.

Флеш-память также функционирует как сервер упрощённого протокола передачи файлов (TFTP), чтобы позволить другим серверам загружаться удалённо от сохранённых образов или копировать их в свою собственную флеш-память.

Маршрутизаторы Cisco серии 1941 имеют два внешних разъёма Compact Flash. Каждый разъём поддерживает высокоскоростные носители ёмкостью до 4 ГБ.

На рисунке 1.1 показан вид внутреннего устройства маршрутизатора Cisco серии 1941 первого поколения маршрутизаторов ISR.

Блок питания

Интерфейсные платы

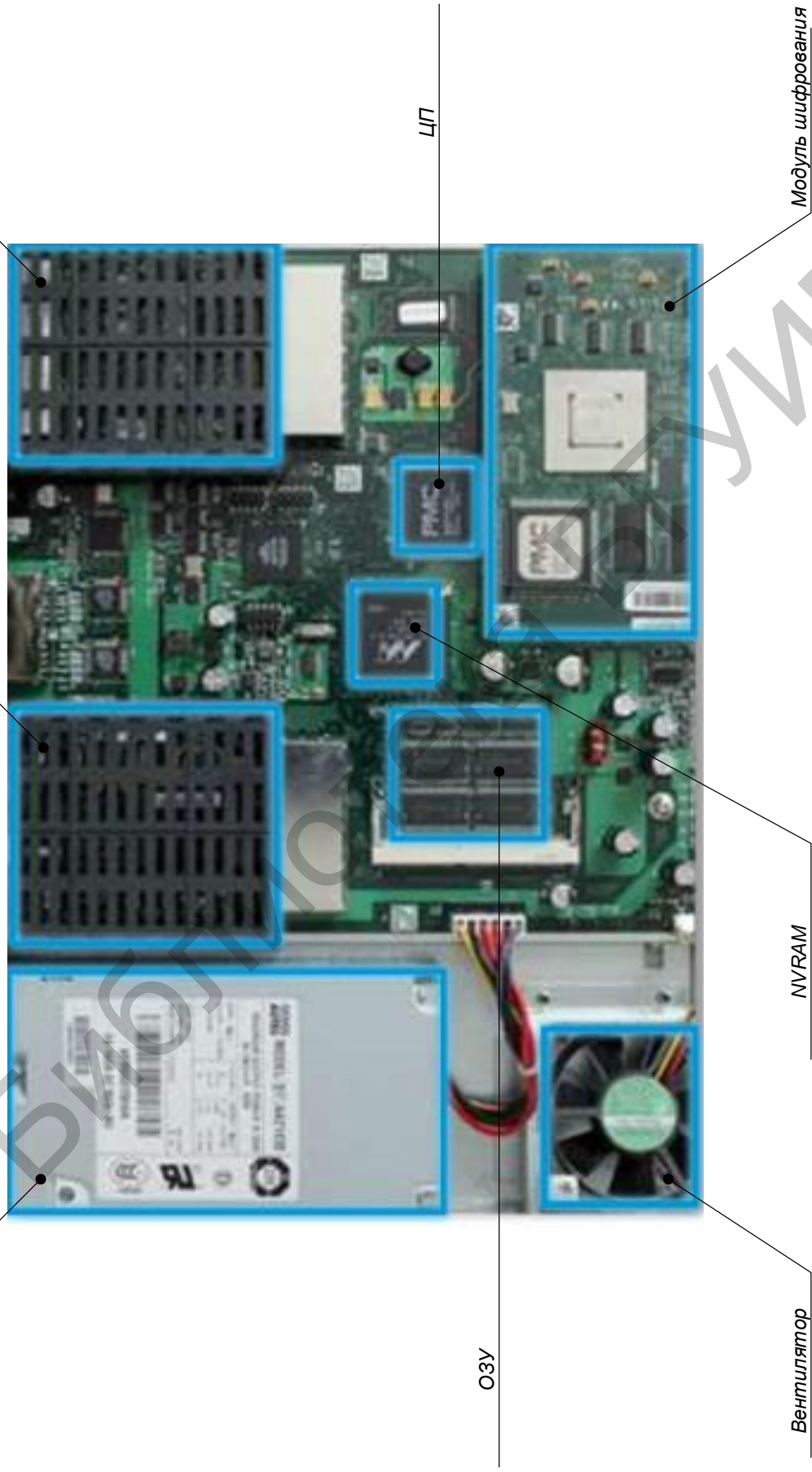


Рисунок 1.1 – Внутреннее устройство маршрутизатора Cisco серии 1941

Маршрутизатор Cisco 1941 предлагает следующие возможности подключения.

1) *Порты консоли*: два порта консоли для начальной настройки и административного доступа к интерфейсу командной строки (CLI) с использованием стандартного порта RJ-45 и USB-разъёма типа B (mini-B USB).

2) *Порт AUX*: порт RJ-45 для удалённого административного доступа; аналогичен порту консоли.

3) *Два интерфейса LAN*: два интерфейса Gigabit Ethernet для подключения локальной сети.

4) *Разъёмы расширенной высокопроизводительной интерфейсной платы WAN (EHWIC)*: два разъёма, обеспечивающие модульность и гибкость маршрутизатора благодаря поддержке различных типов интерфейсных модулей, включая последовательный интерфейс, интерфейс DSL, порт коммутации и беспроводное подключение.

Маршрутизатор Cisco 1941 ISR также имеет разъёмы хранения: два разъёма флеш-памяти Dual-compact могут быть использованы для установки карты флеш-памяти 4 ГБ в каждый из них, что позволит увеличить объём запоминающего устройства. Также имеются два USB-порта для подключения дополнительных запоминающих устройств.

На рисунке 1.2 показано расположение этих разъёмов.

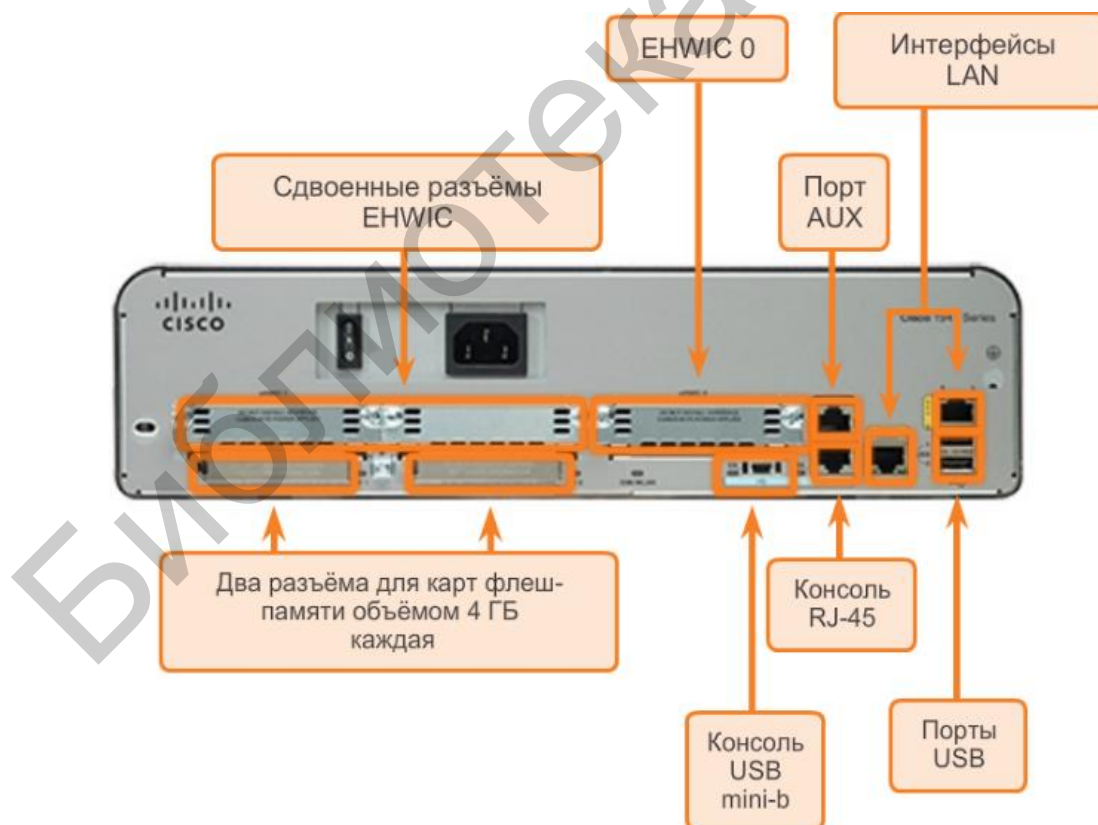


Рисунок 1.2 – Расположение портов маршрутизатора Cisco серии 1941

Подключения на маршрутизаторе Cisco можно разделить на две категории.

1) *Внеполосные интерфейсы (порты управления)* – порты консоли и вспомогательные порты, которые используются для настройки, управления и устранения неполадок маршрутизатора. В отличие от интерфейсов LAN и WAN, порты управления не используются для пересылки пакетов.

2) *Внутриполосные интерфейсы* – это интерфейсы LAN и WAN с настроенной IP-адресацией для передачи пользовательского трафика. Интерфейс Ethernet – наиболее широко используемый тип подключения к локальной сети, в то время как для WAN-подключений часто используются последовательный интерфейс и интерфейс типа DSL.

Как и во многих других сетевых устройствах, в устройствах Cisco используются светодиодные индикаторы, которые предоставляют информацию об их текущем состоянии. Светодиодный индикатор обозначает активность соответствующего интерфейса. Если при активном правильно подключённом интерфейсе индикатор не горит, это может означать, что с этим интерфейсом возникла проблема. Если интерфейс выполняет какие-либо операции, его индикатор горит постоянно.

Как и в случае с коммутатором Cisco, существует несколько способов доступа к среде интерфейса командной строки (CLI) на маршрутизаторе Cisco. Ниже приведены наиболее распространённые методы.

1) *Консоль*: использует низкоскоростные последовательные или USB-подключения для обеспечения прямого подключения и внеполосного административного доступа к устройству Cisco.

2) *Telnet* или *SSH*: два способа удалённого доступа к сеансу использования интерфейса командной строки (CLI) через активный сетевой интерфейс.

3) *Порт AUX*: используется для удалённого управления маршрутизатором с помощью телефонной линии коммутируемого доступа и модема.

В дополнение к этим портам маршрутизаторы также имеют сетевые интерфейсы для получения и пересылки IP-пакетов. Маршрутизаторы имеют несколько интерфейсов, которые используются для подключения к нескольким сетям. Как правило, интерфейсы подключаются к разным типам сетей, что требует наличия различных средств передачи данных и разъёмов.

Каждый интерфейс на маршрутизаторе является участником или узлом в разной IP-сети. Для каждого интерфейса необходимо настроить IP-адрес и маску подсети другой сети. Система Cisco IOS не допускает, чтобы два активных интерфейса на одном маршрутизаторе принадлежали одной и той же сети.

Интерфейсы маршрутизатора можно разделить на следующие две категории.

1) *Ethernet-интерфейсы LAN*: используются для подключения кабелей, которые присоединены к устройствам локальной сети, таким как компьютеры и коммутаторы. Этот интерфейс также можно использовать для соединения маршрутизаторов друг с другом. Широко используются несколько типов ин-

терфейсов Ethernet: более старый Ethernet, Fast Ethernet и Gigabit Ethernet. Используемое название зависит от модели и типа устройства.

2) *Последовательные интерфейсы WAN*: используются для подключения маршрутизаторов к внешним сетям, обычно на больших расстояниях. Как и у интерфейсов LAN, у каждого последовательного интерфейса WAN есть собственные IP-адрес и маска подсети, что указывает на его принадлежность к определённой сети.

Внимание! Следует отметить, что одним из принципиальных отличий коммутатора от маршрутизатора является наличие большого количества Ethernet-интерфейсов, в принципе этим и объясняется способность коммутаторов в объединении множества оконечных и сетевых устройств в сегмент локальной сети.

На рисунке 1.3 приведена лицевая панель коммутатора Cisco 2960.

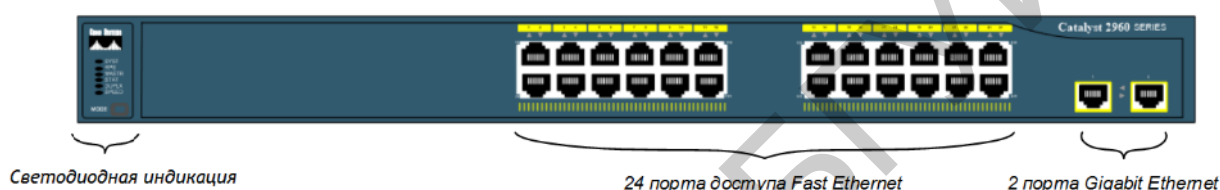


Рисунок 1.3 – Лицевая панель коммутатора Cisco 2960

1.3.3 Командный интерфейс. Режимы конфигурирования и просмотр конфигурации

Сетевые устройства работают на основе сетевой операционной системы. Сетевая операционная система, используемая на устройствах Cisco, называется операционной системой сетевого взаимодействия Cisco (IOS). Операционная система сетевого взаимодействия Cisco (IOS) – это общий термин для группы сетевых операционных систем, используемых на сетевых устройствах Cisco. Операционная система Cisco IOS используется в большинстве устройств Cisco, независимо от их типа и размеров. Наиболее распространённый способ доступа к этим устройствам – использование интерфейса командной строки (CLI).

Далее будет рассмотрена базовая конфигурация маршрутизатора на основе CLI IOS (режимы конфигурации коммутатора практически идентичны).

После включения маршрутизатора в первый раз он осуществляет тест самопроверки POST, который запускает диагностические утилиты с целью проверки внутренних цепей маршрутизатора. Если тест завершён успешно, начинается поиск и загрузка Cisco IOS из флеш-памяти при условии её наличия. Затем IOS загружает конфигурацию, которая находится в NVRAM (файл **startup-config**). Это позволяет загрузить настройки конфигурации Cisco IOS, и интерфейс пользователя Cisco становится доступным.

Для первичной настройки маршрутизатора необходимо подключиться к

нему с использованием консольного кабеля от COM-порта компьютера к консольному порту маршрутизатора. Запустить терминальное ПО (например, Hyper Terminal или PuTTY) и ввести следующие параметры конфигурации COM-порта компьютера:

COM Port COM1 (Выбор COM-порта компьютера)
Bits per second 9600 (Скорость цифрового потока, бит/с)
Data bits 8 (Количество информационных бит в одном пакете)
Parity None (Выбор режима проверки на чётность)
Stop Bits 1 (Количество стартовых и стоповых бит)

Таким образом, согласно приведенным выше настройкам, структура одного пакета, передаваемого через консольное соединение, представлена на рисунке 1.4

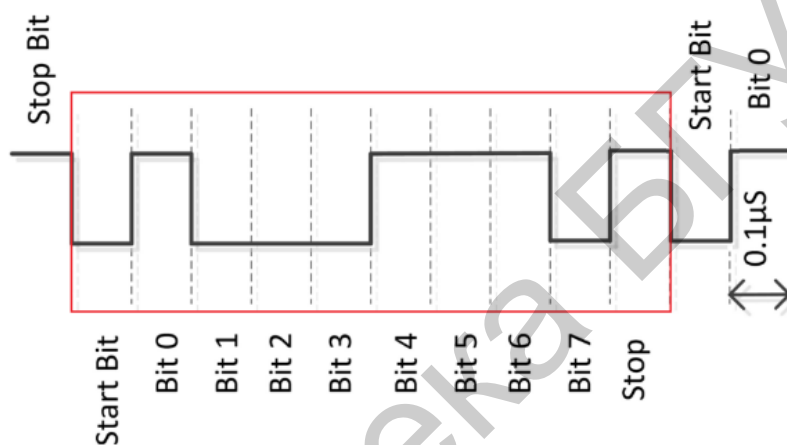


Рисунок 1.4 – Пример структуры пакета для консольного соединения

Внимание! Бит чётности (в случае его выставления в настройках структуры пакета) располагается перед стоповым битом.

Интерфейс пользователя Cisco IOS разделён на несколько различных режимов, а команды, доступные в каждом из режимов, определяют его. Когда начинается сеанс связи с маршрутизатором, он начинается с режима USER EXEC, который зачастую называется просто режимом EXEC. Список команд, доступных в режиме EXEC, весьма ограничен. Для того чтобы иметь доступ ко всем командам, необходимо войти в режим привилегированного EXEC с помощью команды **enable**. Из режима привилегированного EXEC можно ввести любую из команд EXEC, или войти в режим глобальной конфигурации, которая предлагает ещё более широкий выбор команд и опций. Вход в глобальный режим из привилегированного осуществляется с использованием команды **configure terminal**. Из режима глобальной конфигурации можно выйти в режим конфигурации любого из интерфейсов, для того чтобы сконфигурировать этот интерфейс (порт или подинтерфейс).

Основные командные состояния маршрутизатора или коммутатора, его режимы, приведены в таблице 1.2.

Таблица 1.2 – Отображение команд в режимах конфигурации в IOS

<u>1 - USER EXEC</u>	<u>3 - Global Configuration Mode</u>
Switch> Router>	Switch(config)# Router(config)#
<u>2 - Privileged EXEC</u>	<u>4 - Specialized Configuration Mode</u>
Switch# Router#	Switch(config-mode)# Router(config-mode)#

Основными режимами являются пользовательский и привилегированный. Осуществляя функции защиты, ПО CISCO IOS разделяет сессии режимов на два уровня доступа. Привилегированный режим обладает более высоким уровнем прав в возможностях использования устройства.

1.3.3.1 Пользовательский режим (USER EXEC)

Функциональные возможности *пользовательского режима* ограничены, при этом он эффективно выполняет некоторые базовые операции. Пользовательский режим находится на базовом уровне иерархической структуры режимов. Это первый режим, в котором пользователь начинает работу при входе в интерфейс командной строки (CLI) устройства IOS.

Пользовательский режим позволяет выполнять ограниченное количество базовых команд. Этот режим часто называют «режимом для просмотра». В пользовательском режиме запрещается выполнять команды, которые могут изменить параметры устройства.

По умолчанию для входа в пользовательский режим из консоли аутентификация не требуется. Однако во время начальной конфигурации рекомендуется настроить процедуру аутентификации.

Пользовательский режим определяется с помощью команды интерфейса командной строки, оканчивающейся символом «>». Следующий пример демонстрирует символ «>» в командной строке маршрутизатора:

```
Router>
```

1.3.3.2 Привилегированный режим (Privileged EXEC)

Для выполнения команд конфигурации и управления сетевой администратор должен использовать *привилегированный режим* или более специализированный режим в иерархии. Это означает, что сначала пользователю нужно войти в пользовательский режим, а из него – в привилегированный режим. Это можно осуществить с помощью команды **enable**.

Привилегированный режим можно определить по командной строке, оканчивающейся символом «#».

```
Router#
```

Привилегированный режим открывает доступ к режиму глобальной конфигурации и ко всем другим более конкретным режимам настройки.

1.3.3.3 Режим глобальной конфигурации (Global Configuration Mode)

Основной режим конфигурации называется *глобальным режимом конфигурации*. В режиме глобальной конфигурации выполняются изменения конфигурации интерфейса командной строки (CLI), влияющие на работу устройства в целом. Перед доступом к специализированным режимам конфигурации нужно войти в режим глобальной конфигурации.

Чтобы перевести устройство из привилегированного режима в режим глобальной конфигурации и выполнить ввод команд конфигурации из терминала, используется следующая команда интерфейса командной строки:

```
Router#configure terminal
```

После ввода команды командная строка изменяется таким образом, чтобы показать, что он находится в режиме глобальной конфигурации.

```
Router(config)#
```

1.3.3.4 Специальные режимы конфигурации (Specialized Configuration Modes)

Из режима глобальной конфигурации пользователь может перейти в *различные режимы конфигурации* для подкоманд. Каждый из этих режимов позволяет выполнить настройку параметров конкретной области или функции устройства с операционной системой IOS. Ниже приведены некоторые из них:

- *режим конфигурации интерфейса* предназначен для настройки одного из сетевых интерфейсов (например, Fa0/0, G0/1 или S0/1/0);
- *режим конфигурации линии* предназначен для настройки одной из физических или виртуальных линий (консоль, AUX, VTY).

Чтобы вернуться в режим глобальной конфигурации из конкретного режима, введите **exit** в командной строке. Чтобы окончательно выйти из режима конфигурации и вернуться в привилегированный режим, введите **end** или воспользуйтесь комбинацией клавиш **Ctrl + Z**.

1.3.3.5 Командные строки

При использовании интерфейса командной строки (CLI) режим определяется по командной строке, которая является уникальной для каждого режима. По умолчанию каждая командная строка начинается с имени устройства. После имени следует остаток командной строки, который определяет режим. Например, запрос по умолчанию для режима глобальной конфигурации на маршрутизаторе выглядит так:

```
Router(config)#
```

Внимание! Список основных команд для различных режимов конфигурации сетевых устройств приводится в приложении Д.

Отдельное внимание следует уделить различным вариантам базовой команды для проверки – **show**.

Типичная команда **show** предоставляет сведения о конфигурации, эксплуатации и состоянии компонентов коммутатора или маршрутизатора Cisco.

Довольно распространена команда группы **show – show interfaces**. Эта команда служит для отображения статистических сведений по всем интерфей-

сам устройства. Для отображения статистики по определённому интерфейсу введите команду **show interfaces** с указанием типа интерфейса и номера порта (слота). Например:

```
Router# show interfaces gigabitEthernet 0/1
```

К дополнительным командам **show** относят:

– **show startup-config**, которая отображает сохранённую конфигурацию, расположенную в NVRAM;

– **show running-config**, которая отображает содержимое файла текущей конфигурации.

Команда **show version** позволяет проверить некоторые основные средства программно-аппаратного обеспечения маршрутизатора (коммутатора), а также устранить связанные с ними неполадки. Эта команда отображает версию системы Cisco IOS, которая используется в настоящий момент на устройстве, а также версию программы начальной загрузки и информацию о конфигурации оборудования, включая количество системной памяти.

После выполнения команды **show version** выводятся следующие выходные данные:

1) *Версия IOS* – версия операционной системы Cisco в ОЗУ, используемой маршрутизатором (коммутатором).

2) *Программа начальной загрузки ПЗУ*: отображает версию программы начальной загрузки системы, хранящейся в ПЗУ, которая первоначально использовалась для загрузки маршрутизатора (коммутатора).

3) *Расположение системы IOS*: отображает место расположения и загрузки программы начальной загрузки системы Cisco IOS, а также полное имя файла образа IOS.

4) *ЦП и количество ОЗУ*: в первой части этой строки указывается тип центрального процессора, установленного на сетевом устройстве. Последняя часть этой строки отображает количество динамической оперативной памяти (DRAM). Маршрутизаторы некоторых серий, например Cisco 1941 ISR, используют часть памяти DRAM в качестве памяти пакетов. Память пакетов используется для их буферизации. Чтобы определить общее количество памяти DRAM на маршрутизаторе, необходимо сложить оба значения.

5) *Интерфейсы* – информация о физических интерфейсах маршрутизатора.

6) *Количество памяти NVRAM и флеш-памяти* – это количество памяти NVRAM и флеш-памяти, доступной на маршрутизаторе. Память NVRAM используется для хранения файла startup-config, а флеш-память используется для постоянного хранения системы Cisco IOS.

В последней строке команды **show version** отображается текущее настроенное значение конфигурационного регистра программы в шестнадцатеричном формате. Если в скобках отображается второе значение, оно указывает на значение конфигурационного регистра, которое используется во время следующей загрузки.

1.4 ОПИСАНИЕ ЛАБОРАТОРНОГО СТЕНДА

Лабораторная работа проводится в специализированном компьютерном классе с использованием стенда с активным сетевым оборудованием (приложение Б). Доступ к оборудованию осуществляется с использованием специально оборудованной кабельной сети. К каждому рабочему месту студента подведены три патчкорда, которые выведены на сетевую розетку. На рисунке 1.5 приведены варианты подключения персонального компьютера к сети класса.

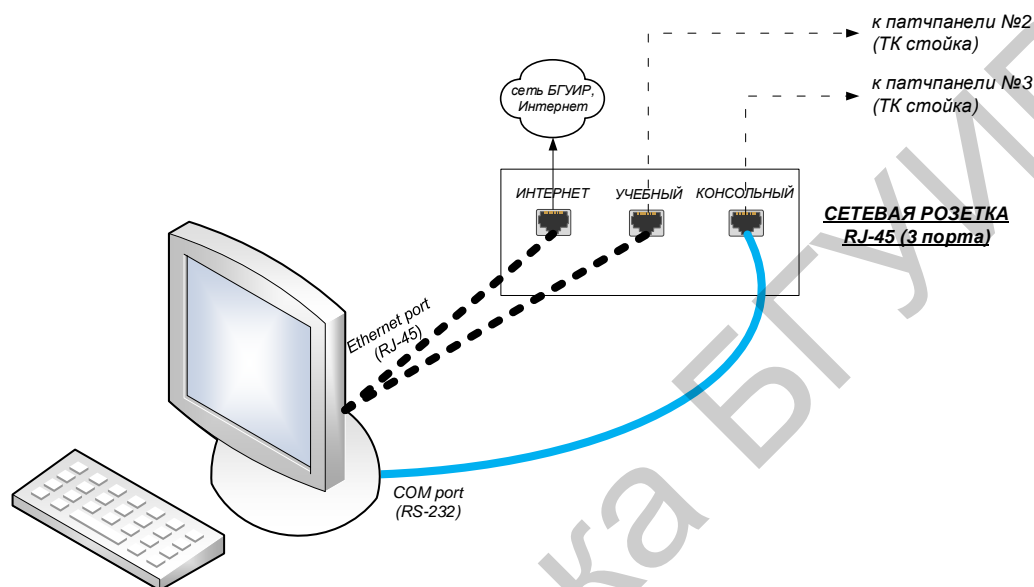


Рисунок 1.5 – Варианты подключения компьютера к сети класса

С помощью персональных компьютеров осуществляется непосредственное и дистанционное управление сетевыми устройствами. В распоряжении студента также находятся патчкорды для подключения персональных компьютеров к сетевым розеткам. Кроме того, на каждом рабочем месте студента должно быть установлено программное обеспечение для терминального доступа (например, PuTTY). Правила безопасности на рабочем месте должны позволять студенту изменять параметры сетевого окружения.

В состав лабораторного стенда также входит телекоммуникационная стойка с коммутаторами Cisco Catalyst 2960, маршрутизаторами Cisco 2901 ISR и патчпанелями. На рисунке 1.6 приведен общий вид стенда с сетевыми устройствами и патчпанелями (ПП).

Внимание! Нумерация на патчпанелях №2 и №3 совпадает с нумерацией компьютеров и сетевых розеток (от 1 до 12). Патчпанель №4 предназначена для подключения к консольным портам сетевых устройств. Здесь принята следующая нумерация: порты с 1 по 3 предназначены для подключения к соответствующим маршрутизаторам, порты с 4 по 6 – для подключения к коммутаторам.

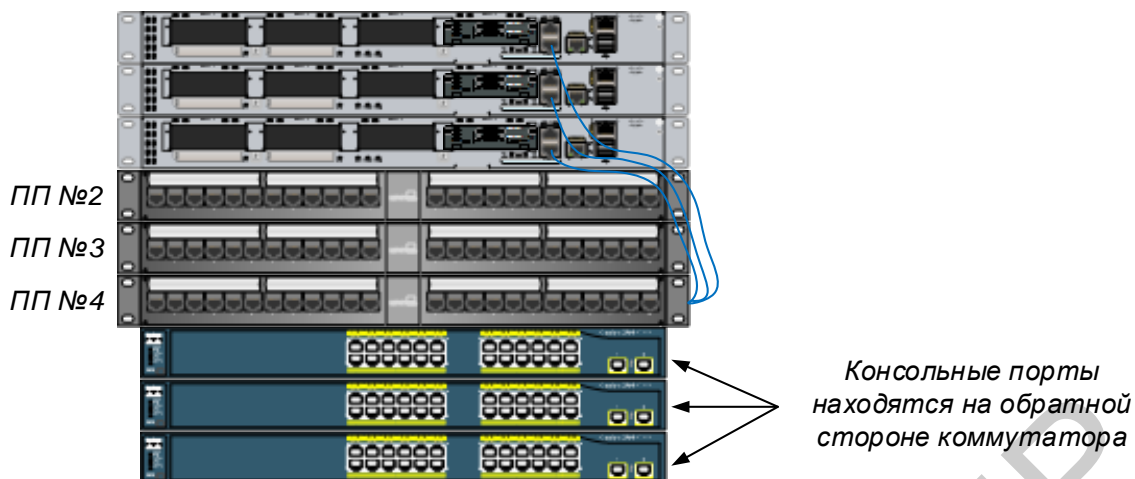
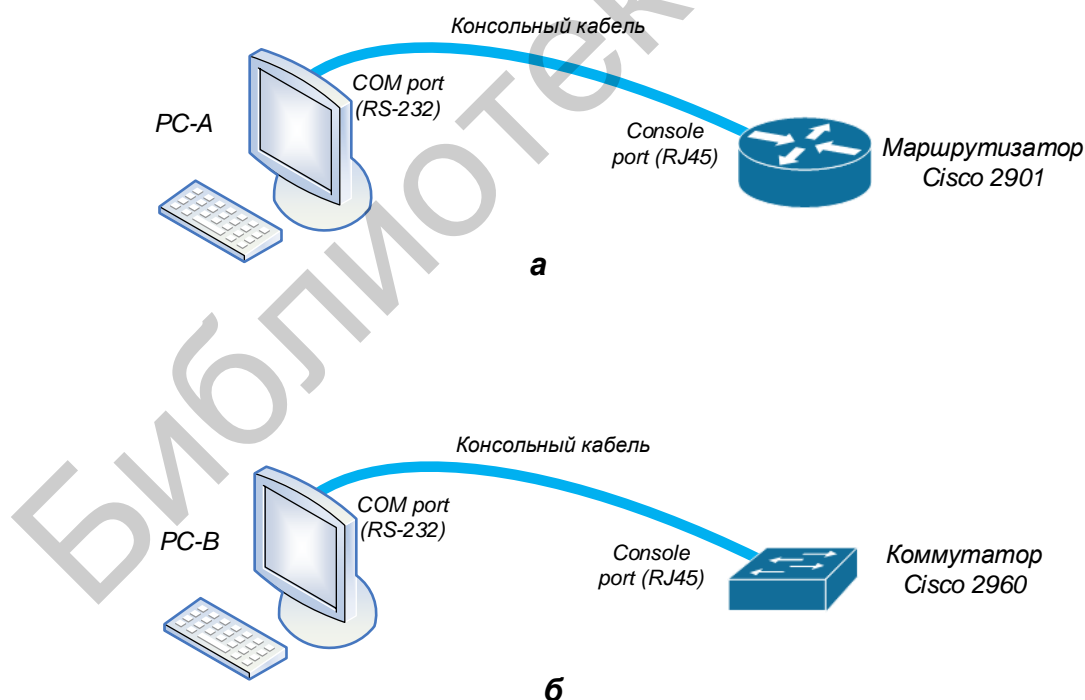


Рисунок 1.6 – Общий вид учебного стенда

Работа выполняется бригадами из трех-четырех человек. В порядке выполнения работы каждой бригаде выделяется комплект сетевого оборудования, который включает в себя коммутатор (Cisco Catalyst 2960) и маршрутизатор (Cisco 2901 ISR). Для подключения к устройствам студентам необходимо производить коммутацию на соответствующих патчпанелях и сетевых розетках.

В данной работе предусматривается изучение следующих двух топологий (рисунок 1.7).



а – подключение к маршрутизатору; б – подключение к коммутатору

Рисунок 1.7 – Топологии консольного подключения ПК к сетевым устройствам

1.5 ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1.5.1 Изучение физических характеристик маршрутизатора

Зарисуйте панель маршрутизатора Cisco 2901 ISR и обозначьте компоненты и интерфейсы в соответствии с приведёнными ниже вопросами. В качестве примера используйте рисунок 1.2.

1.5.1.1 Обведите и отметьте выключатель питания маршрутизатора.

1.5.1.2 Обведите и обозначьте порты управления. Какие порты управления встроены?

1.5.1.3 Обведите и обозначьте интерфейсы локальной сети. Сколько интерфейсов локальной сети имеет изображённый маршрутизатор? Какой тип интерфейса используется?

1.5.1.4 Обведите и обозначьте интерфейсы глобальной сети. Сколько интерфейсов глобальной сети имеет изображённый маршрутизатор? Какой тип интерфейса используется?

1.5.1.5 Оснащён ли ваш маршрутизатор слотами расширения для различных модулей подключения к сети? Обведите и обозначьте слоты для модулей. Сколько здесь слотов для модулей? Сколько из них используется? Какого типа эти слоты?

1.5.1.6 Маршрутизатор Cisco 2901 ISR оснащён слотами памяти CompactFlash для высокоскоростного хранения данных. Обведите и обозначьте слоты памяти CompactFlash. Сколько здесь слотов памяти? Сколько из них используется?

1.5.1.7 Маршрутизатор Cisco 2901 ISR оснащён портами USB 2.0. Встроенные порты USB поддерживают устройства eToken и карты флеш-памяти USB. USB-устройство eToken обеспечивает аутентификацию устройств и безопасную конфигурацию маршрутизаторов Cisco. Функция USB-накопителя позволяет использовать его как дополнительную внешнюю память и дополнительное загрузочное устройство. Обведите и обозначьте порты USB. Сколько здесь портов USB?

1.5.1.8 Маршрутизатор Cisco 2910 также оснащён консольным портом мини-USB типа B. Обведите и обозначьте консольный порт мини-USB типа B.

1.5.2 Изучение физических характеристик коммутатора

Зарисуйте панель коммутатора Cisco 2960 и обозначьте компоненты и интерфейсы, отвечая на вопросы по аналогии с пунктом 1.5.1.

1.5.3 Изучение командной строки маршрутизатора

1.5.3.1 Подсоедините консольные кабели к маршрутизатору Cisco 2901 ISR, как указано на схеме топологии (рисунок 1.7, а). Такое подключение обес-

печивает доступ к интерфейсу командной строки (CLI), а также позволяет просматривать и изменять настройки устройства. Для этого подключите инверсный консольный кабель (рисунок 1.8) к консольному порту сетевой розетки (см. рисунок 1.5), другой конец кабеля подключите к последовательному СОМ-порту компьютера.

Внимание! Большинство современных компьютеров выпускаются без последовательных СОМ-портов. Для подключения устройства Cisco к компьютеру с помощью инверсного консольного кабеля можно использовать адаптер с USB на DB9. Возможно, что при подключении к последовательному СОМ-порту через адаптер с USB на DB9 на компьютер нужно будет установить специальный драйвер, предоставленный производителем.



Рисунок 1.8 – Консольный кабель Cisco

1.5.3.2 Произведите соответствующую коммутацию между патчпанелями №3 и №4, чтобы обеспечить консольное соединение между компьютером и устройством.

1.5.3.3 Запустите на компьютере терминальное ПО, для этого используйте свободно распространяемую программу PuTTY. Эта программа позволяет передавать по консольному кабелю на маршрутизатор команды, набранные на клавиатуре, и отображать на экране монитора информацию, поступающую от маршрутизатора.

Запустите программу PuTTY (рисунок 1.9). В секции Session установите режим Serial. В поле Serial-line укажите название СОМ-порта, к которому подключен маршрутизатор (как правило, СОМ1). В поле Speed укажите скорость 9600.

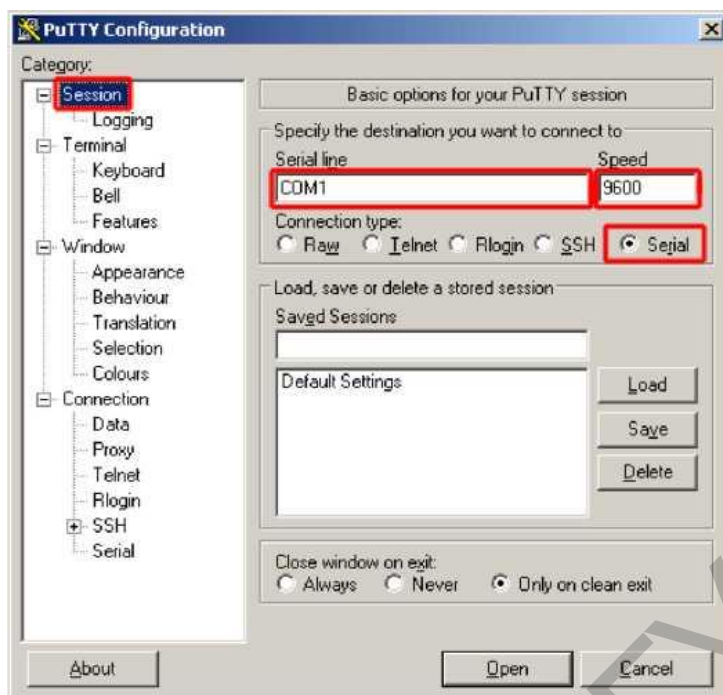


Рисунок 1.9 – PuTTY: выбор типа подключения

Перейдите в раздел Serial. Заполните поля, как показано на рисунке 1.10. Эти настройки необходимы для согласования последовательного интерфейса компьютера и сетевых устройств Cisco. Как правило, данные параметры указаны в документации к оборудованию.

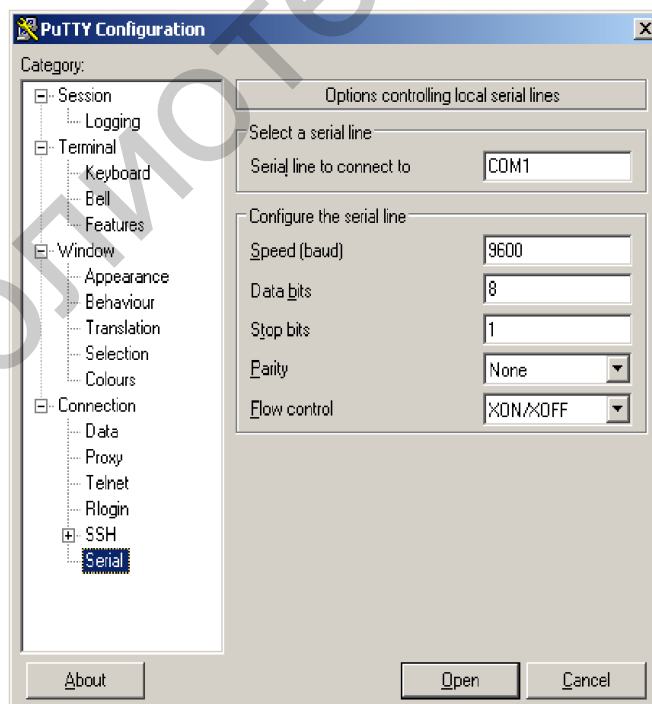


Рисунок 1.10 – PuTTY: настройка параметров серийного порта

Нажмите кнопку **Open**.

Если на маршрутизатор подано питание и все было сделано правильно, на экране терминала отобразится сначала процесс загрузки операционной системы маршрутизатора – Cisco IOS, а затем появится приглашение к диалогу.

```
Cisco CISCO2901/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]:
```

Рисунок 1.11 – Приглашение выбора режима настройки маршрутизатора

Внимание! Все команды, необходимые для ввода в командную строку, выделены полужирным шрифтом.

Введите **no** и нажмите **Enter** на клавиатуре компьютера.

1.5.3.4 Войдите в привилегированный режим с помощью команды **enable**

```
Router> enable
```

```
Router#
```

1.5.3.5 Удалите файл загрузочной конфигурации из NVRAM.

Введите команду **erase startup-config**, чтобы удалить загрузочную конфигурацию из энергонезависимого ОЗУ (NVRAM).

```
Router# erase startup-config
```

```
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK]
```

```
Erase of nvram: complete
```

```
Router#
```

1.5.3.6 Перезагрузите маршрутизатор.

Запустите команду **reload**, чтобы удалить из памяти предыдущую конфигурацию. По запросу перезагрузки нажмите клавишу ВВОД, чтобы подтвердить перезагрузку. Чтобы прервать перезагрузку, нажмите любую клавишу.

```
Router# reload
```

```
Proceed with reload? [confirm]
```

```
*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console.
```

```
Reload Reason:
```

```
Reload Command.
```

Внимание! Возможно, появится запрос о сохранении текущей конфигурации перед перезагрузкой маршрутизатора. Чтобы ответить, введите **no и нажмите клавишу ВВОД.**

```
System configuration has been modified. Save? [yes/no]: no
```

1.5.3.7 Пропустите диалоговое окно начальной конфигурации.

После перезагрузки маршрутизатора появится запрос о входе в диалоговое окно начальной конфигурации. Введите **no** и нажмите клавишу ВВОД.

Would you like to enter the initial configuration dialog? [yes/no]: **no**

1.5.3.8 Завершите программу автоустановки.

Программа предложит прекратить процесс автоустановки. Ответьте **yes** и нажмите клавишу ВВОД.

Would you like to terminate autoinstall? [yes]: **yes**

Router>

1.5.4 Изучение командной строки и просмотр конфигурации коммутатора

1.5.4.1 Подключите консоль к коммутатору Cisco 2960 и войдите в привилегированный режим, для этого по аналогии повторите операции, которые описаны в подпунктах 1.5.3.1 – 1.5.3.3.

Switch> **enable**

Switch#

1.5.4.2 Определите, были ли созданы виртуальные локальные сети (VLAN).

Воспользуйтесь командой **show flash**, чтобы определить, были ли созданы сети VLAN на коммутаторе (рисунок 1.12).

Switch# **show flash**

Switch#

```
Switch#show flash:
Directory of flash:/

 1 -rw-     4414921    <no date>  c2960-lanbase-mz.122-25.FX.bin
 3 -rw-       1070    <no date>  config.text
 2 -rw-        616    <no date>  vlan.dat

64016384 bytes total (59599777 bytes free)
Switch#
```

Рисунок 1.12 – Содержимое флеш-памяти

1.5.4.3 Удалите файл виртуальной локальной сети (VLAN).

Если файл **vlan.dat** обнаружен во флеш-памяти, удалите этот файл.

Switch# **delete vlan.dat**

Delete filename [vlan.dat]?

Будет предложено проверить имя файла. На данном этапе можно изменить имя файла или нажать клавишу ВВОД, если имя введено верно.

При запросе удаления этого файла нажмите клавишу ВВОД, чтобы подтвердить удаление. (Чтобы отменить удаление, нажмите любую другую клавишу).

```
Delete flash:/vlan.dat? [confirm]
```

```
Switch#
```

1.5.4.4 Удалите файл загрузочной конфигурации.

Введите команду **erase startup-config**, чтобы удалить файл загрузочной конфигурации из NVRAM. При необходимости удаления файла конфигурации нажмите клавишу ВВОД, чтобы подтвердить удаление. (Чтобы отменить операцию, нажмите любую другую клавишу.)

```
Switch# erase startup-config
```

```
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
```

```
[OK]
```

```
Erase of nvram: complete
```

1.5.4.5 Перезагрузите коммутатор, чтобы удалить из памяти всю информацию о предыдущей конфигурации. При необходимости перезагрузки коммутатора нажмите клавишу ВВОД, чтобы продолжить перезагрузку. (Чтобы отменить перезагрузку, нажмите любую другую клавишу.)

```
Switch# reload
```

```
Proceed with reload? [confirm]
```

Примечание – Возможно, появится запрос о сохранении текущей конфигурации перед перезагрузкой коммутатора. Введите **no** и нажмите клавишу ВВОД.

```
System configuration has been modified. Save? [yes/no]: no
```

1.5.4.6 Пропустите диалоговое окно начальной конфигурации.

После перезагрузки коммутатора появится запрос о входе в диалоговое окно начальной конфигурации. Введите **no** в окне запроса и нажмите клавишу ВВОД.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

```
Switch>
```

Примечание – Если указанное выше сообщение не отображается, попросите преподавателя восстановить на коммутаторе начальную конфигурацию.

1.5.4.7 В пользовательском режиме отобразите версию IOS своего коммутатора.

```
Switch> show version
```

```
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE SOFTWARE (fc1)
```

```
Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2012 by Cisco Systems, Inc.
```

```
Compiled Sat 28-Jul-12 00:29 by prod_rel_team
```

```
ROM: Bootstrap program is C2960 boot loader
```

```
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE (fc1)
```

```
Switch uptime is 2 minutes System returned to ROM by power-on
```

```
System image file is "flash://c2960-lanbasek9-mz.15 0-2.SE.bin"
```

Какая версия IOS установлена на коммутаторе в настоящее время?

1.5.4.8 Выполните настройку часов.

Важную роль в процессе поиска и устранения неисправностей на сетевых устройствах играет настройка времени. Перечисленные ниже действия позволяют вручную настроить внутренние часы коммутатора.

а) Отобразите текущие настройки часов.

```
Switch> show clock
```

```
*00:30:05.261 UTC Mon Mar 1 1993
```

б) Настройки часов изменяются в привилегированном режиме. Войдите в привилегированный режим, набрав команду **enable** в командной строке пользовательского режима.

```
Switch> enable
```

в) Выполните настройку часов. Вопросительный знак («?») открывает справку и позволяет определить необходимые настройки текущего времени, даты и года. Нажмите клавишу ВВОД, чтобы завершить настройку часов.

```
Switch# clock set ?
```

```
hh:mm:ss Current Time
```

```
Switch# clock set 15:38:00 ?
```

```
<1-31> Day of the month MONTH Month of the year
```

```
Switch# clock set 15:38:00 Apr 15 ?
```

```
<1993-2035> Year
```

```
Switch# clock set 15:38:00 Apr 15 2016
```

```
Switch#
```

```
*Apr 15 15:38:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 00:31:43 UTC Mon Mar 1 1993 to 15:38:00 UTC Fri Apr 15 2016, configured from console by console.
```

г) Введите команду **show clock** и проверьте, обновлены ли настройки часов.

```
Switch# show clock
```

```
15:38:27.205 UTC Fri Apr 15 2016
```

1.6 СОДЕРЖАНИЕ ОТЧЁТА

1.6.1 Цель работы.

1.6.2 Общий вид (лицевые панели) маршрутизатора Cisco 2901 ISR и коммутатора Cisco Catalyst 2960 с отмеченными на них всеми интерфейсами, модулями и слотами, а также светодиодной индикацией.

1.6.3 Схемы подключения ПК к сетевым устройствам, а также настройки параметров серийного порта при подключении к консолям сетевых устройств с пояснениями по каждому из параметров (см. рисунок 1.10).

1.6.4 Команды для просмотра текущей версии операционной системы сетевого устройства. Запишите номер версии операционной системы IOS, которая применяется на коммутаторе.

1.6.5 Выводы по работе.

1.7 КОНТРОЛЬНЫЕ ВОПРОСЫ

1.7.1 Дайте определение сетевому устройству. Каково назначение коммутатора и маршрутизатора? Почему маршрутизатор относят к устройствам сетевого уровня? Какие типы памяти применяются в сетевых устройствах? Каково их предназначение?

1.7.2 Какое из сетевых устройств и почему целесообразнее использовать при построении локальной сети с большим количеством персональных компьютеров (хостов²)? Каково внутреннее устройство коммутатора? В чем принципиальное отличие между коммутатором и маршрутизатором?

1.7.3 В каком типе памяти хранится файл текущей конфигурации? В каком типе памяти хранится файл загрузочной конфигурации? Где хранится образ операционной системы Cisco IOS? В чем смысл процедуры POST?

1.7.4 Перечислите типы внутрисетевых и внеполосных интерфейсов. Для чего они предназначены? Какие типы портов управления применяются для управления сетевыми устройствами? Какие методы применяются для удаленного управления сетевыми устройствами?

1.7.5 С какой целью применяются последовательные интерфейсы WAN? Для чего применяется интерфейс командной строки (CLI)? Какие параметры следует вводить при настройке консольного соединения?

1.7.6 Почему перед перезагрузкой маршрутизатора необходимо удалить файл загрузочной конфигурации (startup configuration)? Для чего может понадобиться слот расширения EHWIC?

1.7.7 Каким образом можно трактовать полученный ответ (результаты вывода) сетевого устройства на команду **show version**? Для чего может быть использован порт мини-USB? Каким образом настроить системное время на сетевых устройствах и в чем заключается важность данной процедуры?

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Цикл методических материалов и контрольно-обучающих программ сетевой академии Cisco Systems [Электронный ресурс]. – 2016. – Режим доступа : <http://netacad.com/>.

2 Компьютерные сети / В. Г. Олифер [и др.]. – 4-е изд. – СПб. : ПИТЕР, 2012.

3 Хабракен, Джо. Как работать с маршрутизаторами Cisco / Джо Хабракен ; пер. с англ. – М. : ДМК Пресс, 2005.

² Хост (от англ. *host* – «хозяин, принимающий гостей»), или узел – любое устройство, предоставляющее сервисы формата «клиент – сервер» в режиме сервера по каким-либо интерфейсам и уникально определенное на этих интерфейсах. В более частном случае под хостом могут понимать любой компьютер, сервер, подключенный к локальной или глобальной сети.

ЛАБОРАТОРНАЯ РАБОТА №2

СЕТЕВЫЕ УСТРОЙСТВА РАСПРЕДЕЛЕНИЯ ИНФОРМАЦИИ: КОММУТАТОРЫ, МАРШРУТИЗАТОРЫ. ПЕРВИЧНОЕ КОНФИГУРИРОВАНИЕ И СОХРАНЕНИЕ КОНФИГУРАЦИИ. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

2.1 ЦЕЛЬ РАБОТЫ

- 2.1.1 Изучение принципов IP-адресации в компьютерных сетях.
- 2.1.2 Изучение базовых принципов конфигурирования сетевых устройств.
- 2.1.2 Изучение методов защиты сетевых устройств.

2.2 ЗАДАНИЕ К РАБОТЕ

- 2.2.1 Ознакомиться с основами планирования адресного пространства.
- 2.2.2 Изучить принципы базовой конфигурации на сетевых устройствах.
- 2.2.3 Познакомиться с процессом настройки внутрисетевых интерфейсов.
- 2.2.4 Научиться настраивать различные режимы безопасности на сетевых устройствах.

2.3 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

2.3.1 IP-адресация на основе классов

Структура адреса IPv4 – это точечно-десятичное представление в виде четырёх десятичных чисел в диапазоне от 0 до 255. Адреса IPv4 – это номера, присвоенные отдельным устройствам, подключённым к сети. Они имеют логическую природу, поскольку предоставляют информацию о местоположении устройства.

Помимо IP-адреса необходима маска подсети. *Маска подсети* – это особый тип адреса IPv4, который совместно с IP-адресом определяет, к какой именно подсети подключено данное устройство.

IP-адреса могут быть присвоены физическим портам и виртуальным интерфейсам на всех устройствах. *Виртуальный интерфейс* означает, что с данным устройством не связано дополнительное физическое оборудование.

При появлении Internet адресное пространство было разделено на три основных класса сетей: класс А, класс В и класс С. Особенность сети класса А заключалась в том, что первый октет (8 бит) IP-адреса определял собственно сеть, а оставшиеся биты использовались организацией, которая управляла сетью, для того чтобы различать узлы сети. В сетях класса В два первых октета использо-

вались для определения сети, а оставшиеся два – для определения отдельных узлов, в сетях класса С для определения сети отводилось три октета и лишь один для определения узлов. Разделение на классы производилось путем анализа первых битов IP-адреса.

Таблица 2.1 – Классы IP-адресов

Класс	IP	1 байт	2 байт	3 байт	4 байт
A	1-127	0NNNNNNN	Хост		
B	128-191	10NNNNNN	Сеть	Хост	
C	192-223	110NNNNN	Сеть		Хост
D	224-239	1110NNNN	Группа		
E	240-255	11110NNN	Резерв		

В адресах класса А старший бит первого октета всегда имеет значение 0. Это означает, что наименьший номер сети при использовании адреса такого класса равен 00000000 (0), а наибольший равен 01111111 (127). Но в этом случае необходимо учитывать некоторые ограничения. Во-первых, адрес сети класса А, равный 0, используется для обозначения так называемой «данной сети», или сети, к которой фактически подключен передающий хост. Во-вторых, адрес сети класса А, равный 127, применяется для создания петли обратной связи. В связи с этим практически применимые адреса класса А сводятся к тем, которые содержат в первом октете число от 1 до 126.

Адреса класса В всегда начинаются с двоичных цифр 10 (например, 10101100.00010000.00000001.00000001, или 172.16.1.1). Это означает, что первый октет должен находиться в пределах от 128 (10000000) до 191 (10111111). Адрес сети класса С должен начинаться с двоичных цифр 110 (например, 11000000.10101000.00000001.00000001, или 192.168.1.1).

В дополнение к этим трем классам адресов существуют еще два класса. В классе D старшие четыре бита установлены в 1110. Этот класс используется для поддержки групповой передачи данных. В классе Е старшие четыре бита установлены в 1111, и этот класс является зарезервированным для экспериментальных целей.

2.3.2 Бесклассовая адресация (CIDR)

С ростом сети Internet возникла проблема нехватки IP-адресов. И не столько адресов, сколько подсетей для различных организаций. Причиной было то, что многие организации были достаточно велики, чтобы выйти за пределы сети класса С, которая могла содержать максимум 254 узла, но недостаточно велики, чтобы занять целый класс В, сеть которого могла вместить 65 534 узла.

В долгосрочной перспективе решением этой проблемы назвали внедрение протокола IPv6 (длина адреса 128 бит, а не 32). Как временное быстрое решение была разработана *бесклассовая междоменная маршрутизация* (Classless Inter-Domain Routing, или CIDR). Как видно из названия, CIDR избавляется от

классов А, В и С. В системе CIDR для идентификации сети может использоваться не фиксированное число октетов (один, два или три), но любое число битов IP-адреса. Так, к примеру, если организации нужно адресное пространство, примерно в четыре раза большее чем адресное пространство сети класса В, для этого необходимо определить длину идентификатора сети в 14 бит, таким образом оставляя 18 бит (в четыре раза больше узлов, чем в сети класса В) на используемое адресное пространство.

Итак, чтобы обозначить конкретную CIDR-сеть, следует указать конкретное значение старших битов, присваиваемое организации в записи через точку, а также число битов, определяющих сеть – так называемую маску подсети. Она так же, как и IP-адрес, занимает 4 байта, но имеет строго определенный вид: первая часть этой последовательности – единицы, вторая – нули. Таким образом, IP-адрес разбивается на две части: адрес сети, который используется при маршрутизации между сетями, и адрес отдельной хост-машины. Позиции битов, которые соответствовали «1» маски, отвечают за адрес сети, те, что соответствуют «0», – за адрес конкретного устройства. Маска подсети обычно записывается, как и IP-адрес, пооктетно через точки либо после IP-адреса через слеш указывается число единиц (длина сетевой части IP-адреса).

Пример задачи

По указанной записи IP-адреса и маски 62.76.34.36 255.255.255.224 (таблица 2.2):

- определить вторую форму записи адреса, указав через слеш маску подсети;
- рассчитать адрес подсети;
- рассчитать широковещательный адрес подсети;
- определить диапазон доступных адресов для хостов.

Таблица 2.2 – Разложение IP-адреса на сетевую и хостовую части на основании сетевой маски

62								76								34								36							
0	0	1	1	1	1	1	0	0	1	0	0	1	1	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	1	0	0
255								255								255								224							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	
27 бит в сетевой части																								5 бит в хостовой части							

Для определения второй формы записи адреса представим маску подсети в двоичной форме. Таким образом, маска 255.255.255.224 представляет собой три октета всех единиц и четвертый октет 11100000. Подсчитав количество всех единиц, мы получаем маску в другой форме /27. Следовательно, указанный адрес можно также представить в компактной форме как 62.76.34.36/27.

Адрес сети узнаем наложением маски на IP-адрес (логическая операция «И» между битовыми последовательностями). Для последнего октета получит-

ся 00100000. В привычном виде: 62.76.34.32/27. В этой сети может быть 2^5 адресов (для хостов): от 0 до 32. Адрес, в котором все 0, – это адрес сети, а в котором все 1, – широковещательный (broadcast). То есть в нашем случае 62.76.34.32/27 – это адрес сети, а 62.76.34.63/27 – широковещательный адрес. Все, что между ними, – и есть свободный диапазон адресов, которые могут применяться для хостов. Формула для расчетов количества хостов $N = 2^m - 2$, где m – количество битов в хостовой части. В данном примере $m = 5$, получаем $N = 2^5 - 2$, таким образом, в этой сети может быть 30 устройств с адресами (диапазоном) 62.76.34.33 – 62.76.34.62/27.

2.3.3 Адресация оконечных устройств

Для обеспечения связи оконечного устройства со всей сетью его нужно правильно настроить с IP-данными. Для этого оконечному устройству нужно присвоить IP-адрес, маску подсети, а в некоторых случаях и шлюз по умолчанию. Эти данные настраиваются в параметрах сетевого адаптера ПК.

Чтобы оконечное устройство было правильно подключено к сети, на нём нужно настроить все эти параметры. Эта информация настраивается в области параметров сети ПК. Кроме IP-адреса, данных о маске подсети и основного шлюза, можно настроить данные сервера DNS, как показано на рисунке 2.1.

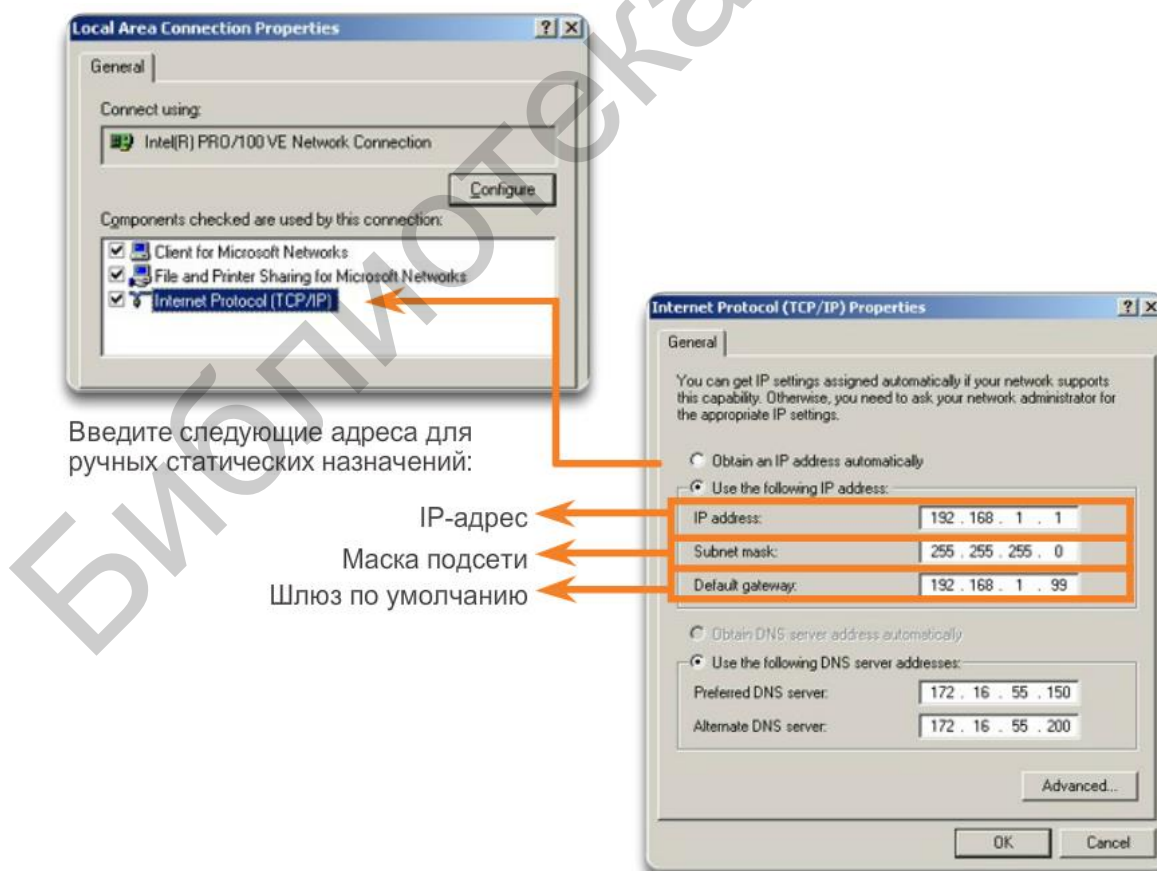


Рисунок 2.1 – Адресация оконечных устройств

Адрес шлюза по умолчанию – это IP-адрес интерфейса маршрутизатора, используемого для выхода сетевого трафика из локальной сети. Его используют, когда трафик нужно направить в другую сеть. Если в сети используется коммутатор, то для удаленного управления коммутатором, а также для передачи трафика в другую сеть на коммутаторе производится настройка шлюза по умолчанию.

Пример конфигурации шлюза по умолчанию на коммутаторе Cisco:

```
Switch(config)#ip default-gateway 192.168.1.99
```

Здесь 192.168.1.99 – IP-адрес сетевого интерфейса маршрутизатора, к которому подключен коммутатор.

Адрес сервера DNS – это IP-адрес сервера службы доменных имен (англ. Domain Name System, DNS), который используется для преобразования IP-адресов в веб-адреса, например www.cisco.com. Доступ к устройствам в Интернете осуществляется с помощью IP-адреса. Однако пользователям легче запомнить имена, а не цифры. Поэтому для простоты веб-сайтам присваиваются имена. Сервер DNS используется для поддержания сопоставления между IP-адресами и различными устройствами.

Информацию об IP-адресе (см. рисунок 2.1) можно ввести в ПК вручную или получить автоматически с помощью протокола динамической конфигурации сетевого узла (DHCP).

Внимание! Возможности DHCP в данной работе не рассматриваются.

2.3.4 Проверка параметров подключения оконечных и сетевых устройств

Для проверки внутренней IP-конфигурации на локальном узле используется команда **ping** на зарезервированном виртуальном loopback-адресе (127.0.0.1). Loopback-адрес, 127.0.0.1, определяется протоколом TCP/IP как зарезервированный адрес, который направляет пакеты обратно к узлу, таким образом можно определить актуальное состояние сетевой интерфейсной платы узла (рисунок 2.2).

Пример команды **ping**, которая вводится в командной строке на локальном узле:

```
C:\> ping 127.0.0.1
```

Ответ данной команды будет выглядеть примерно следующим образом:

```
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

```
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

```
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

```
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 127.0.0.1:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

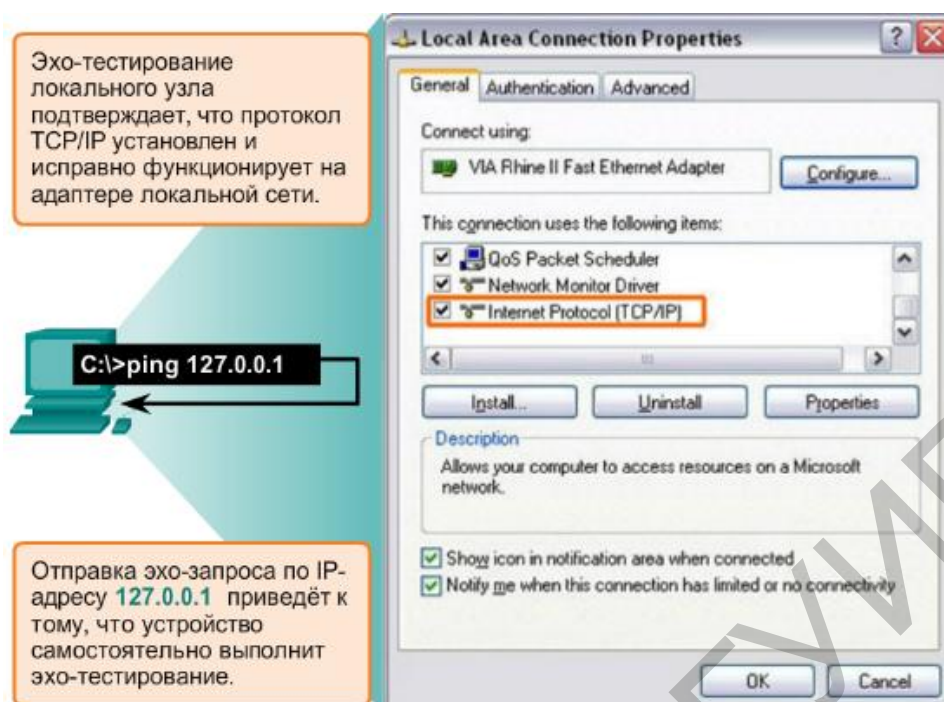


Рисунок 2.2 – Проверка локального TCP/IP-стека оконечного устройства

Результат показывает, что четыре тестовых пакета каждый по 32 байта были отправлены и возвращены от узла 127.0.0.1 быстрее чем за 1 мс. Этот успешный эхо-запрос доказывает, что сетевая интерфейсная плата, драйверы и реализация TCP/IP функционируют правильно.

Команду **ping** можно использовать как для проверки конфигурации оконечного узла, так и для проверки интерфейсов сетевых устройств, таких как коммутатор и маршрутизатор.

Пример тестирования оконечного узла на маршрутизаторе Cisco с помощью команды **ping** представлен ниже. Обратите внимание, что ввод команды осуществляется в привилегированном режиме.

```
Router#ping 192.168.1.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
```

```
..!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/2 ms
```

Команда **tracert** применяется для тестирования задержек на каждом транзитном узле, через который проходит пакет.

```
Router#tracert 192.168.1.1
```

```
Type escape sequence to abort.
```

```
Tracing the route to 192.168.1.1
```

```
1 192.168.1.1 1 msec 0 msec 0 msec
```

Чтобы просмотреть настройки IP для ПК с ОС Windows, в командной строке введите команду **ipconfig**. В выходных данных команды вы увидите

IP-адрес, маску подсети и шлюз, которые ПК получил либо в результате ручного ввода или автоматического с сервера DHCP.

2.3.5 Базовая конфигурация сетевых устройств

Как было упомянуто ранее, коммутаторы и маршрутизаторы Cisco во многом похожи. Они работают на аналогичной операционной системе, поддерживают схожие структуры команд. Кроме того, при внедрении этих двух устройств в сеть потребуется выполнить одинаковые настройки. В этом случае говорят, что необходимо произвести базовую конфигурацию сетевых устройств.

Под *базовой конфигурацией* понимают назначение имени сетевому устройству, ограничение доступа к конфигурации устройства, отключение поиска DNS, настройку баннерных сообщений и сохранение конфигурации. Все остальные расширенные настройки специфичны и зависят от типа устройства, его назначения в сети. Более подробно расширенные настройки для коммутатора и маршрутизатора будут рассмотрены в следующих лабораторных работах.

2.3.5.1 Изменение имени устройства

Один из первых шагов при настройке сетевого устройства – это назначение уникального *имени устройства* или узла. Сетевые администраторы распознают устройства по сети или через Интернет именно с помощью имен узлов.

В соответствии с общими требованиями по обозначению имени должны:

- начинаться с буквы;
- не содержать пробелов;
- оканчиваться на букву или цифру;
- содержать только латинские буквы, цифры и тире;
- содержать не более 64 символов.

Внимание! В именах узлов, используемых в устройствах IOS, сохраняются различия между прописными и строчными символами.

Настройка имени узла с помощью интерфейса командной строки (CLI) в IOS производится в режиме глобальной конфигурации. Для этого необходимо из привилегированного режима перейти в режим глобальной конфигурации с помощью команды **configure terminal**. Ниже приведены настройки для коммутатора, настройка маршрутизатора производится аналогичным образом.

Switch#configure terminal

После ввода команды командная строка будет содержать следующее:

Switch(config)#

Далее в режиме глобальной конфигурации введите имя узла (например, в данном случае это имя **Sw-Floor-1**):

Switch(config)#**hostname Sw-Floor-1**

После ввода команды командная строка будет содержать следующее:

Sw-Floor-1(config)#

Обратите внимание, что узел изменил свое имя. Для выхода из режима глобальной конфигурации используйте команду **exit**.

Внимание! Чтобы отменить действие любой команды в IOS, введите перед ней ключевое слово «no».

Например, чтобы удалить имя устройства, потребуется следующая команда:

```
Sw-Floor-1(config)#no hostname  
Switch(config)#
```

Обратите внимание, что команда **no hostname** вернула имя коммутатора по умолчанию.

2.3.5.2 Ограничение доступа к конфигурации устройств

Рекомендуется физически ограничивать доступ к сетевым устройствам, размещая их в отдельных помещениях или в закрытых шкафах. Тем не менее пароли остаются основным средством защиты от несанкционированного доступа к сетевым устройствам. Для обеспечения безопасности устройство IOS использует иерархические режимы. Для усиления защиты IOS может потребовать несколько паролей, чтобы разрешать доступ к разным уровням иерархии.

К приведённым здесь типам паролей относятся:

- *пароль привилегированного режима* – ограничивает доступ в привилегированный режим;
- *секретный пароль* – зашифрованный пароль, ограничивающий доступ в привилегированный режим;
- *пароль консоли* – ограничивает доступ к устройствам через консольное подключение;
- *пароль для VTU* – ограничивает доступ к устройствам через Telnet.

Рекомендуется использовать различные пароли аутентификации для каждого из уровней доступа. Кроме того, рекомендуется использовать надёжные пароли, которые сложно подобрать.

При выборе пароля примите во внимание следующие основные моменты:

- используйте пароли длиной более 8 символов;
- используйте сочетание прописных и заглавных латинских букв, чисел, специальных знаков и/или числовых последовательностей;
- на разных устройствах рекомендуется использовать разные пароли;
- не следует использовать общеупотребительные слова, такие как «password» или «admin», так как их легко подобрать.

Для защиты доступа к привилегированному режиму используйте команду **enable secret password**, где слово «password» – прописанное курсивом, означает парольное слово. Устаревшая, менее безопасная версия этой команды – **enable password password**. Команда **enable password** использует шифрование type-7, алгоритмы которого известны и которое достаточно легко раскрываемо. Хотя для настройки аутентификации перед доступом в привилегированный режим подходят обе эти команды, рекомендуется использовать **enable secret**. Команда **enable secret** обеспечивает более высокий уровень безопасности, поскольку ис-

пользует шифрование type-5, которое является односторонним – для его взлома потребуется полный перебор всех возможных вариантов.

Пример команды для установления пароля **class**:

```
Switch(config)#enable secret class
```

Консольный порт сетевых устройств необходимо защитить как минимум надёжным паролем. Это снижает вероятность доступа неавторизованных сотрудников, которые могут подключиться через консольный порт устройства и попытаться получить доступ.

Чтобы установить пароль для консоли в режиме глобальной конфигурации, нужно ввести следующие команды:

```
Switch(config)#line console 0
```

```
Switch(config-line)#password cisco
```

```
Switch(config-line)#login
```

Первая команда **line console 0** предназначена для входа в специфический режим конфигурации линии. Нуль в обозначении линии используется для обозначения первого (а в большинстве случаев – единственного) интерфейса консоли. Вторая команда – **password cisco** определяет пароль для консоли строки, в данном случае паролем будет являться слово «*cisco*». Команда **login** настраивает коммутатор для аутентификации при входе в систему. Если включена процедура входа и настроен пароль, пользователь консоли должен будет ввести пароль, чтобы получить доступ к интерфейсу командной строки (CLI).

Каналы VTY обеспечивают доступ к устройствам Cisco по протоколу Telnet (или SSH). По умолчанию многие коммутаторы Cisco поддерживают до 16 каналов VTY, пронумерованных от 0 до 15. Количество каналов VTY, поддерживаемых на маршрутизаторе Cisco, зависит от типа маршрутизатора и версии IOS. Пароль нужно установить для всех доступных каналов VTY. Для всех соединений можно установить один пароль. При этом часто возникает необходимость задать уникальный пароль для одного канала, чтобы обеспечить администратору резервный доступ в том случае, если все остальные соединения заняты.

Команды, используемые для назначения пароля каналов VTY:

```
Switch(config)#line vty 0 15
```

```
Switch(config-line)#password cisco
```

```
Switch(config-line)#login
```

По умолчанию в IOS встроена команда **login** на каналах VTY. Это предотвращает доступ по протоколу Telnet к устройству без аутентификации. Если по ошибке была введена команда **no login**, из-за чего была снята аутентификация, по протоколу Telnet к сети могут присоединиться неавторизованные пользователи. Это представляет определённую угрозу безопасности.

Ещё одна важная команда, которая защищает пароль во время просмотра файлов конфигурации, – это **service password-encryption**. Данная команда шифрует все незашифрованные пароли во время их настройки. Шифрование применяется только к паролям в файле конфигурации, но не к паролям, кото-

рые отправлены по среде передачи данных. Эта команда не позволяет неавторизованным пользователям прочитать пароль.

2.3.5.3 Запрет на нежелательные поиски в DNS

Очень часто при неверно введенной команде в IOS сетевое устройство идентифицирует эту команду как вероятностное имя сетевого устройства и пытается произвести его поиск через DNS. Для этого рекомендуется отключить поиск в DNS, чтобы предотвратить попытки устройства преобразовывать введенные команды так, будто бы они являются именами узлов:

```
Switch(config)#no ip domain-lookup
```

Внимание! Прервать выполнение текущего процесса также можно с использованием сочетания клавиш Ctrl + Shift + 6.

2.3.5.4 Баннерные сообщения сетевых устройств

Несмотря на то что пароли защищают сеть от неавторизованных пользователей, необходимо использовать уведомления о том, что лишь авторизованным пользователям можно получить доступ к устройству. Для этого нужно добавить баннер в выходные данные устройства.

IOS предоставляет множество типов баннеров. Сообщение текущего дня – достаточно распространенный баннер.

Для настройки сообщения текущего дня в режиме глобальной конфигурации используется следующий синтаксис:

```
Switch(config)#banner motd #message#
```

После выполнения команды баннер будет показан при всех последующих попытках доступа к устройству. Следует отметить, что само содержание сообщения в данном примере помещено в логические скобки из двух решеток.

2.3.5.5 Файл текущей конфигурации

Файл *текущей конфигурации* **running-config** отражает текущую конфигурацию, функционирующую на устройстве (рисунок 2.3). Изменения текущей конфигурации незамедлительно влияют на работу устройства Cisco.

Файл текущей конфигурации хранится в рабочей памяти устройства или в оперативном запоминающем устройстве (ОЗУ). Это означает, что файл текущей конфигурации временно активен, когда работает устройство Cisco (подключено к питанию). Однако при отключении питания устройства или перезапуске устройства все несохраненные изменения конфигурации будут потеряны.

После внесения изменений в файл текущей конфигурации следует рассмотреть следующие варианты действий:

- вернуть устройство к исходной конфигурации;
- удалить все внесённые изменения;
- сделать изменённую конфигурацию новой начальной конфигурацией.

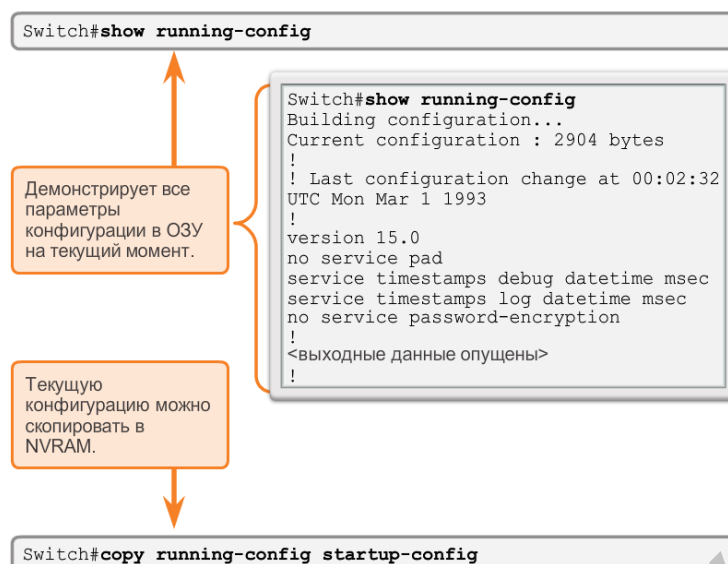


Рисунок 2.3 – Отображение и сохранение текущей конфигурации

2.3.5.6 Файл загрузочной конфигурации

Файл *загрузочной конфигурации* **startup-config** отображает конфигурацию, которая будет применена на устройстве после перезагрузки. Файл загрузочной конфигурации хранится в энергонезависимой памяти (NVRAM). После настройки сетевого устройства и изменения текущей конфигурации важно сохранить эти изменения в файл загрузочной конфигурации (см. рисунок 2.3). Это предотвращает потери изменений вследствие сбоя питания или случайной перезагрузки. Осуществить это можно с помощью следующей команды:

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

После выполнения команды файл текущей конфигурации обновляет файл загрузочной конфигурации.

Если изменения, внесённые в ходе конфигурации, не принесли желаемого результата, возможно, понадобится восстановить предыдущую конфигурацию устройства. Для этого осуществляется перезапуск устройства путем ввода команды **reload** в командной строке привилегированного режима.

Выполняя перезагрузку, IOS определит, что изменённая конфигурация не была сохранена в файл начальной конфигурации. IOS запросит, нужно ли сохранить изменения. Для отмены изменений введите **no**.

Если нежелательные изменения сохранены в файл начальной конфигурации, возможно, понадобится очистить все конфигурации. Для этого нужно удалить начальную конфигурацию и перезапустить устройство.

Начальную конфигурацию можно удалить с помощью команды **erase startup-config**.

Чтобы удалить файл загрузочной конфигурации, введите команды **erase startup-config** в командную строку привилегированного режима:

```
Switch#erase startup-config
```

После ввода команды появится запрос о подтверждении:

Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]

Ответ по умолчанию – «Подтверждаю». Для подтверждения и удаления файла загрузочной конфигурации нажмите клавишу **Enter**. Нажатие любой другой клавиши приведёт к преждевременному завершению данного процесса.

Внимание! Будьте внимательны при использовании команды «erase». Эту команду можно использовать для удаления любого файла в устройстве. Неправильное использование этой команды может привести к удалению самой IOS или других важных файлов.

2.3.5.7 Резервная конфигурация с захватом текста

В дополнение к сохранению текущей конфигурации в начальную файлы конфигурации можно сохранить также в текстовый документ. Эта последовательность действий позволит в дальнейшем редактировать или использовать рабочую копию файлов конфигурации.

На рисунке 2.4 показано, как файлы можно сохранять в текстовый документ с помощью программы HyperTerminal. Аналогичную операцию можно сделать с помощью терминального клиента PuTTY.

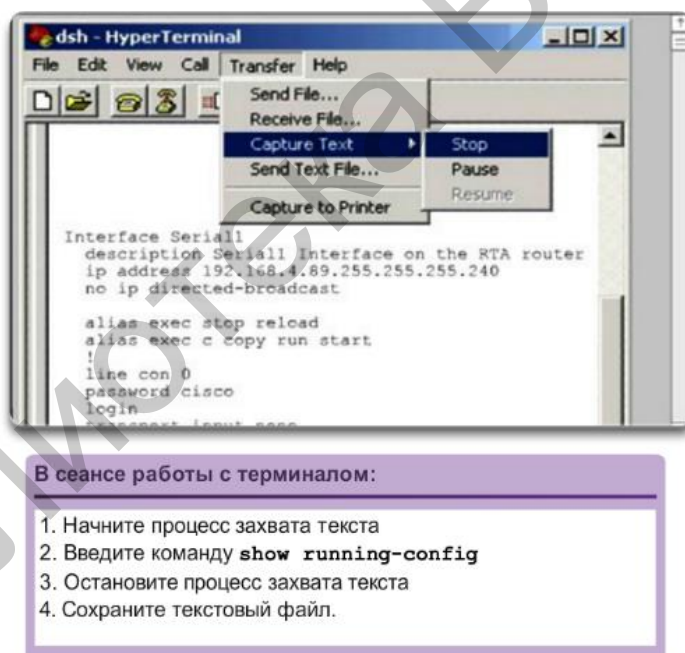


Рисунок 2.4 – HyperTerminal: Сохранение конфигурации в текстовый файл

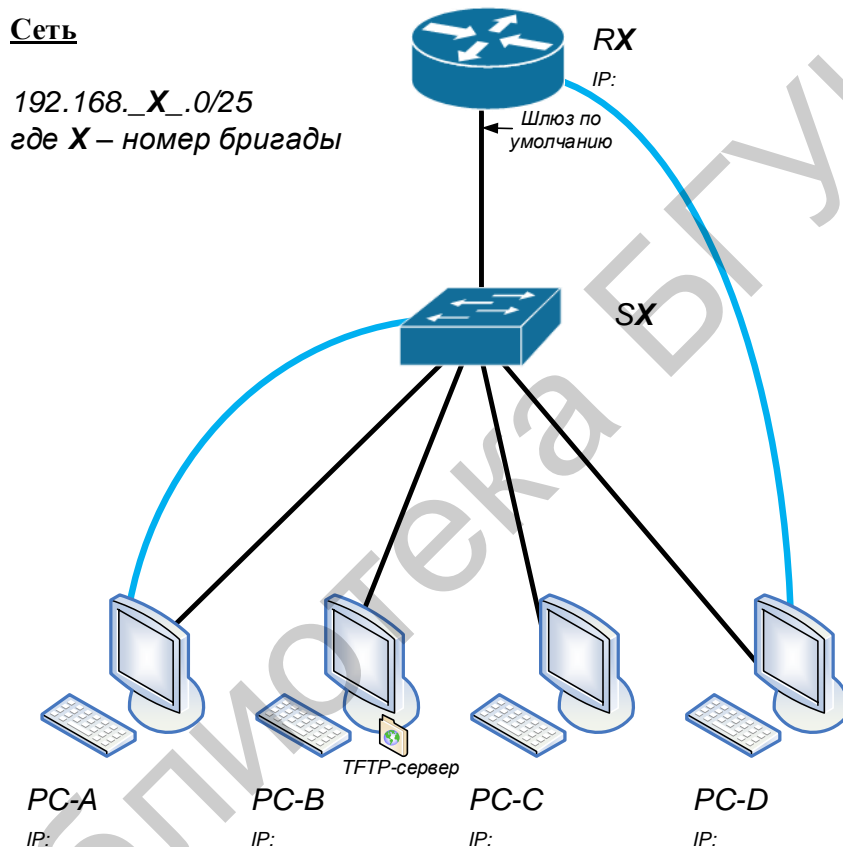
2.4 ОПИСАНИЕ ЛАБОРАТОРНОГО СТЕНДА

Работа выполняется бригадами из трёх-четырёх человек. В процессе выполнения работы каждой бригаде выделяется комплект сетевого оборудования, который включает в себя коммутатор Cisco Catalyst 2960 и маршрутизатор Cisco 2901 ISR. Для подключения к устройствам студентам необходимо произвести коммутацию на соответствующих патчпанелях и сетевых розетках. Для вы-

полнения работы студентам понадобится программное обеспечение для терминального доступа (например, PuTTY), а также приложение для эмуляции файлового сервера (например, TFTP32).

Внимание! Для подключения компьютеров к Ethernet-портам коммутатора используйте второй «УЧЕБНЫЙ» порт сетевой розетки (см. рисунок 1.5) и не забывайте при этом производить соответствующие коммутации на патчпанели №2 и коммутаторе. Порядок подключения к консольным портам оборудования описан в лабораторной работе №1.

В данной работе предусматривается изучение следующей топологии сети (рисунок 2.5).



2.5 ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

2.5.1 Исследование изучаемой топологии

2.5.1.1 К Ethernet-интерфейсам коммутатора SX (где X – номер бригады) подключите компьютеры PC-A, PC-B, PC-C, PC-D (буквы А, В, С и D соответствуют 1, 2, 3 и 4 компьютеру первой бригады; 5, 6, 7 и 8 компьютеру второй бригады и т. д.). Последний интерфейс коммутатора используйте для подключения к маршрутизатору RX (где X – номер бригады).

2.5.1.2 Для всех компьютеров используйте IP-адресацию из диапазона 192.168.X.0/25 (где X – номер бригады). Для адресации Ethernet-интерфейса маршрутизатора используйте последний доступный адрес в указанном диапазоне. Рассчитайте и распределите все необходимые адреса по работе.

2.5.1.3 Компьютеры PC-A и PC-D, помимо подключения к Ethernet-линиям, используются для внеполосной настройки сетевых устройств посредством подключения консольных линий согласно схеме.

2.5.1.4 После проверки преподавателем правильности сборки схемы, включите все устройства.

2.5.2 Настройка статических IP-адресов компьютеров

2.5.2.1 Назначьте компьютерам соответствующие статические IP-адреса, для этого в ОС Windows нажмите кнопку **Пуск** и зайдите в **Панель управления** (рисунок 2.6).

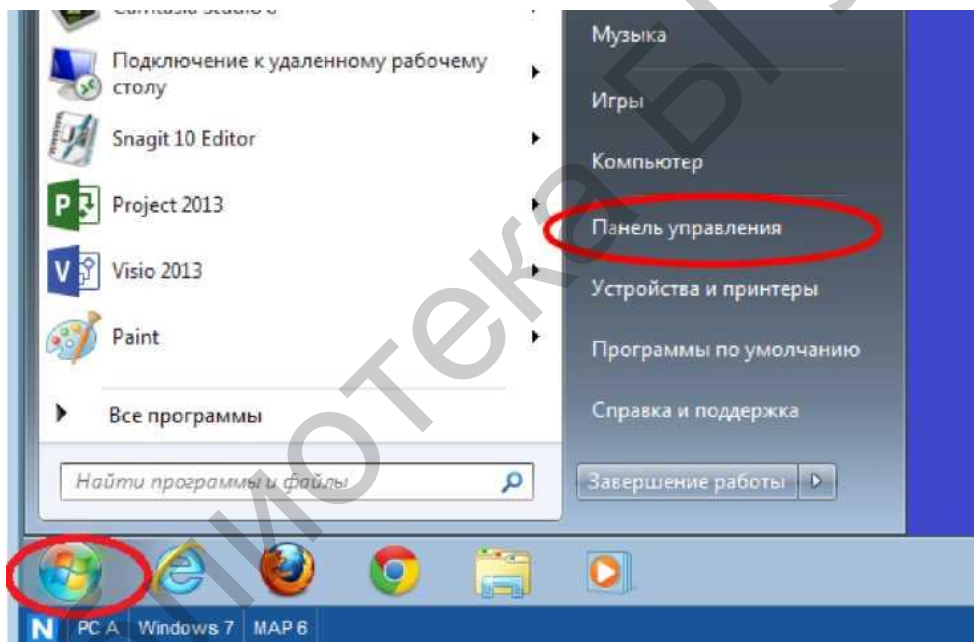


Рисунок 2.6 – Меню пуск

2.5.2.2 В разделе «Сеть и Интернет» выберите ссылку **Просмотр состояния сети и задач**.

Если в **Панели управления** отображается список значков, из раскрывающегося меню **Просмотр** выберите параметр **Категория** (рисунок 2.7).

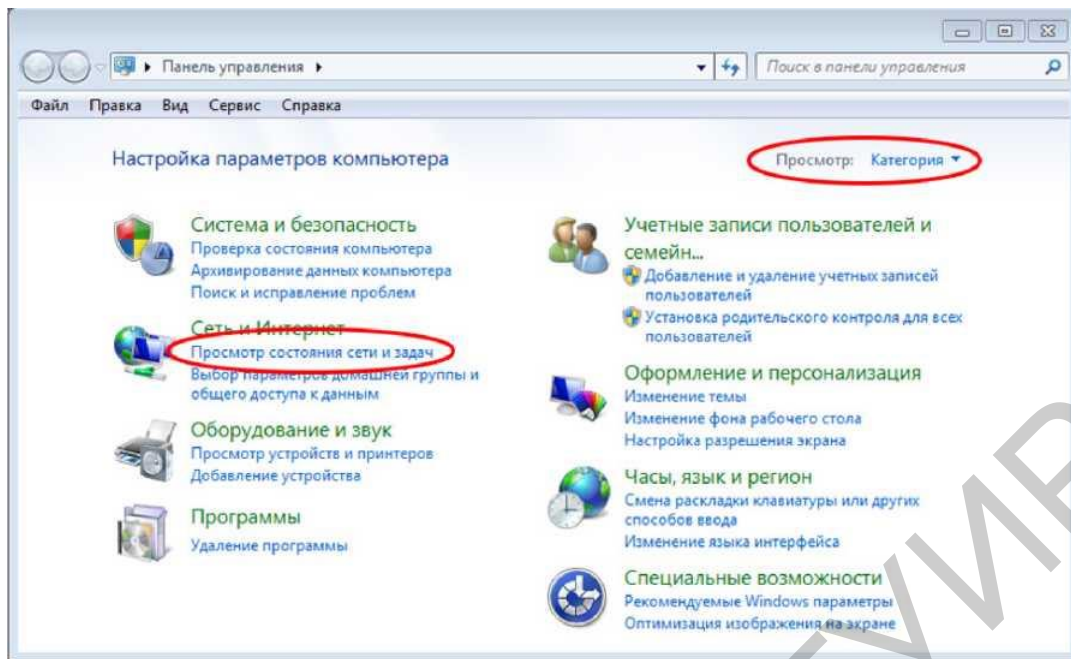


Рисунок 2.7 – Панель управления

2.5.2.3 В левой части окна **Центр управления сетями и общим доступом** выберите ссылку **Изменение параметров адаптера** (рисунок 2.8).

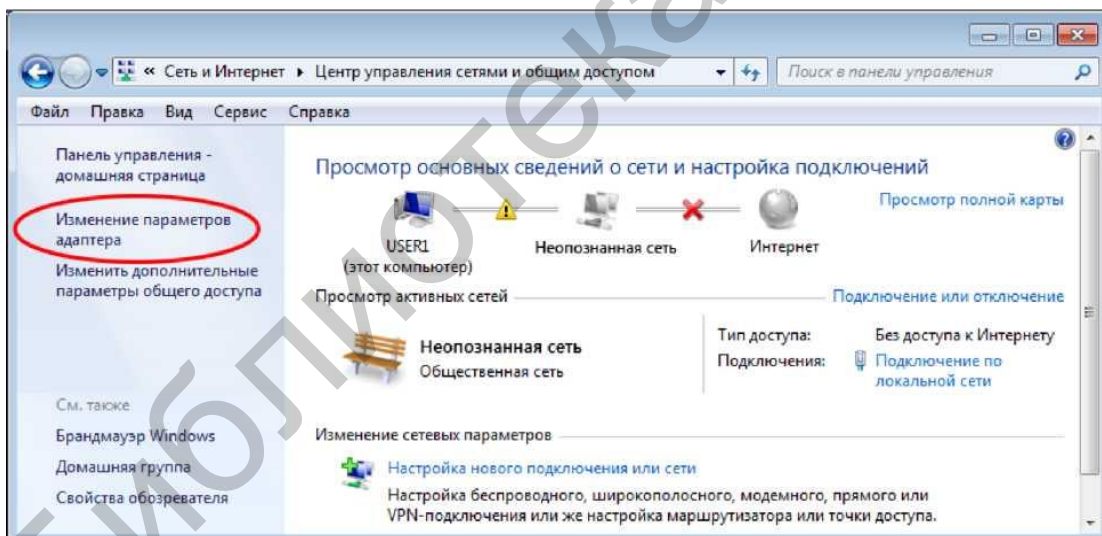


Рисунок 2.8 – Центр управления сетями и общим доступом

2.5.2.4 В окне **Сетевые подключения** отображаются доступные интерфейсы ПК. Щёлкните правой кнопкой мыши на значке **LAN** и выберите пункт **Свойства** (рисунок 2.9).

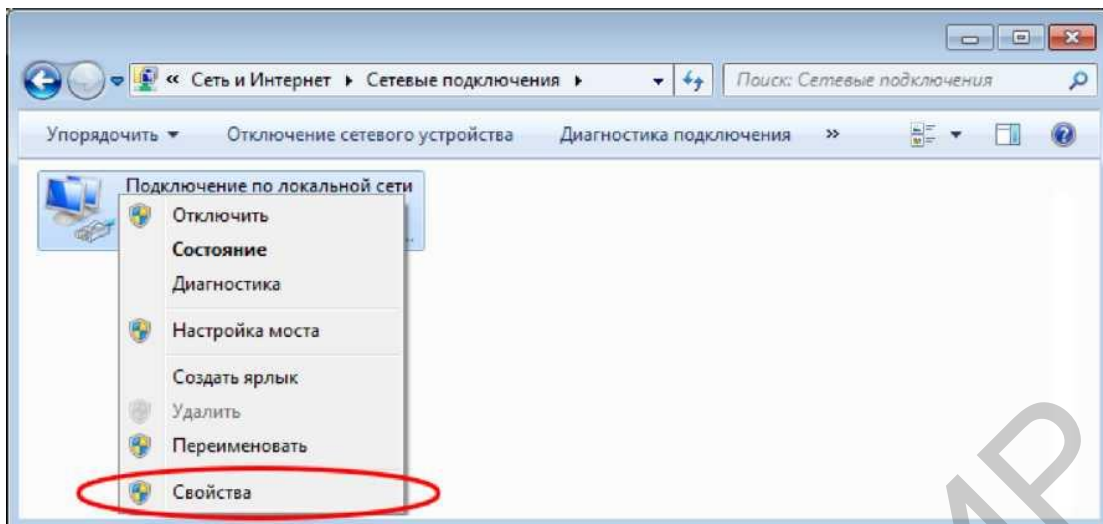


Рисунок 2.9 – Сетевые подключения

2.5.2.5 Выберите опцию **Протокол Интернета версии 4 (TCP/IPv4)** и нажмите кнопку **Свойства** (рисунок 2.10).

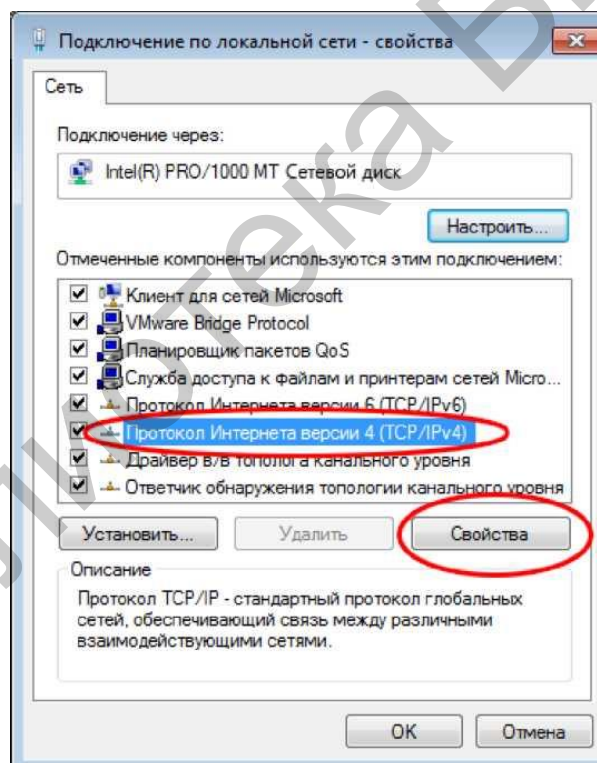


Рисунок 2.10 – Свойства подключения по локальной сети

Чтобы открыть окно **Свойства**, можно также дважды щёлкнуть кнопкой мыши на **Протокол Интернета версии 4 (TCP/IPv4)**.

2.5.2.6 Чтобы настроить IP-адрес, маску подсети и шлюз по умолчанию вручную, установите переключатель **Использовать следующий IP-адрес** (рисунок 2.11).

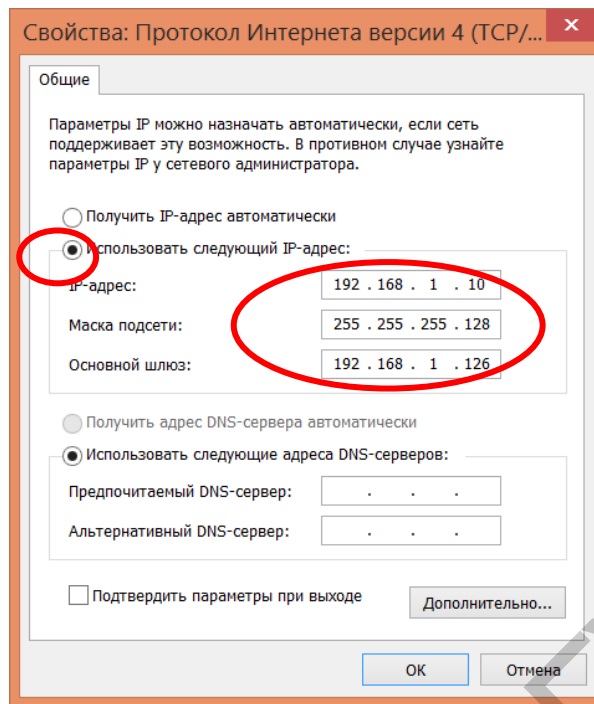


Рисунок 2.11 – Общие свойства протокола Интернета версии 4

В рассмотренном выше примере введены IP-адрес и маска подсети для одного из компьютеров. Кроме того, указан шлюз по умолчанию, поскольку к сети подключён один маршрутизатор.

2.5.2.7 Указав все данные IP, нажмите кнопку ОК. Нажмите кнопку ОК в окне «Свойства подключения по локальной сети», чтобы присвоить IP-адрес адаптеру локальной сети.

2.5.2.8 Повторите перечисленные выше действия на остальных компьютерах.

2.5.2.9 Проверьте настройки и соединение ПК. Для этого на каждом компьютере запустите окно командной строки (**cmd.exe**). Это можно сделать путем нажатия кнопки **Пуск**. Введите **cmd** в строке **Найти программы и файлы** и нажмите клавишу ВВОД (рисунок 2.12).



Рисунок 2.12 – Поиск cmd

2.5.2.10 В окне **cmd.exe** с помощью команды **ipconfig /all** проверьте настройки ПК. Эта команда отображает имя ПК и сведения об IPv4-адресе, маске и шлюзе по умолчанию, а также другую техническую информацию (рисунок 2.13).

```
C:\Windows\system32\cmd.exe
C:\Users\NetAcad>ipconfig /all

Windows IP Configuration

Host Name . . . . . : PC-A
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-50-56-BE-6C-89
Dhcp Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80-d428-7de2-997c-b05a%11(Preferred)
IPv4 Address. . . . . : 192.168.1.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Dhcpv6 Iaid . . . . . : 234884137
Dhcpv6 Client Duid. . . . . : 00-01-00-01-17-F6-72-3D-00-0C-29-8D-54-44
```

Рисунок 2.13 – Окно cmd.exe с результатами вывода информации

2.5.2.11 Введите **ping 192.168.1.11** (например, если второй компьютер настроен с адресом 192.168.1.11) и нажмите клавишу ВВОД (рисунок 2.14).

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:
Reply from 192.168.1.11: bytes=32 time=1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\NetAcad>
```

Рисунок 2.14 – Окно cmd.exe с результатами эхо-запроса

Проверьте, успешно ли выполнен эхо-запрос с помощью команды ping. Если нет, попытайтесь найти и устранить неполадку.

Внимание! Если вы не получили ответ от любого настроенного удаленного компьютера в вашей бригаде, попробуйте отправить эхо-запрос на данный компьютер ещё раз. Если ответ от удалённого ПК не поступает, обратитесь за помощью к инструктору.

2.5.2.12 Компьютер PC-B будет являться TFTP-сервером для данной топологии сети. Для этого на рабочем столе PC-B запустите приложение

TFTPД32. Настройте рабочую папку, предварительно создав ее, для приложения укажите следующий путь:

D:\work\номер вашей группы\фамилия_или_логин

2.5.3 Базовая настройка коммутатора

Внимание! Базовая настройка маршрутизатора производится аналогичным образом, более подробно см. пункт 2.5.4.

2.5.3.1 На компьютере РС-А запустите приложение PuTTY, указав все необходимые по умолчанию параметры связи для непосредственной настройки и управления устройствами через внеполосное подключение (см. порядок подключения через PuTTY в лабораторной работе №1). Убедитесь, что подключение реализовано, для этого на экране должна быть выведена информация или появиться приглашение от подключенного устройства.

Внимание! Если устройство не реагирует и не отображается какая-либо активность на вашем экране, попробуйте нажать несколько раз клавишу «Enter».

По умолчанию устройство должно находиться в стартовом режиме (Setup Mode) с предложением воспользоваться мастером начальной конфигурации. Откажитесь от помощи мастера, набрав **no** в командной строке. В противном случае воспользуйтесь командами очистки загружаемой конфигурации и перезапустите устройство. Если на устройстве стоит пароль, воспользуйтесь механизмом сброса пароля (приложение В).

2.5.3.2 Войдите в привилегированный режим.

Привилегированный режим даёт доступ ко всем командам коммутатора. К привилегированному набору команд относятся те, которые содержатся в пользовательском режиме, а также команда **configure**, при помощи которой выполняется доступ к остальным командным режимам. Перейдите в привилегированный режим, введя команду **enable**.

```
Switch>enable
```

```
Switch#
```

Приглашение в командной строке изменится с **Switch>** на **Switch#**, что указывает на привилегированный режим.

2.5.3.3 Войдите в режим конфигурации.

Для входа в режим конфигурации используйте команду **configuration terminal**.

```
Switch#configure terminal
```

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

```
Switch(config)#
```

Приглашение в командной строке изменится в соответствии с режимом глобальной конфигурации.

Внимание! Если вы не знаете, как полностью пишется та или иная команда в CLI, используйте клавишу «Tab» на клавиатуре, например, в

указанном выше примере для входа в глобальный режим вместо полного ввода «**configure terminal**» достаточно набрать «**conf t**» и нажать клавишу «**Enter**».

2.5.3.4 Установите соответствующее имя на коммутатор.

С помощью команды **hostname** измените имя коммутатора на **S1** (для второй и третьей бригады соответственно **S2** и **S3**).

```
Switch(config)#hostname S1  
S1(config)#
```

2.5.3.5 Запретите нежелательные поиски в DNS.

Отключите поиск в DNS, чтобы предотвратить попытки коммутатора преобразовывать введённые команды таким образом, как будто они являются именами узлов.

```
S1(config)#no ip domain-lookup  
S1(config)#
```

2.5.3.6 Установите секретный доступ по паролю **ciscoenapa** к привилегированному режиму доступа.

Для предотвращения несанкционированного доступа к коммутатору необходимо настроить пароли, для этого в режиме конфигурации введите команду **enable secret** и *парольное слово*:

```
S1(config)#enable secret ciscoenapa  
S1(config)#
```

2.5.3.7 Установите доступ по паролю **ciscovty** к Telnet-линиям vty.

Настройте каналы виртуального соединения для удалённого управления (vty), чтобы коммутатор разрешил доступ через Telnet. Если вы не настроите пароли vty, то не сможете получить доступ к устройству через Telnet.

```
S1(config)#line vty 0 15  
S1(config-line)#password ciscovty  
S1(config-line)#login  
S1(config-line)#exit  
S1(config)#
```

2.5.3.8 Установите доступ по паролю **ciscocon** к консольной линии. Обеспечьте синхронизацию командной строки и вывода информации на линии управления.

Доступ через порт консоли также следует ограничить. Согласно конфигурации по умолчанию все консольные подключения должны быть настроены без паролей. Чтобы консольные сообщения не прерывали выполнение команд, используйте параметр **logging synchronous**.

```
S1(config)#line console 0  
S1(config-line)#password ciscocon  
S1(config-line)#login  
S1(config-line)#logging synchronous  
S1(config-line)#exit  
S1(config)#
```

2.5.3.9 Все пароли должны храниться в зашифрованном виде.

Команда **service password-encryption** защищает все введенные ранее пароли во время просмотра файлов конфигурации.

```
S1(config)#service password-encryption
```

```
S1(config)#
```

2.5.3.10 Установите актуальное время на коммутаторе (см. лабораторную работу №1).

2.5.3.11 Введите сообщение дня (MOTD). Сконфигурируйте **message-of-the-day banner** “Unauthorized access is strictly prohibited and prosecuted to the full extent of the law!”

Баннер входа в систему, называемый также сообщением дня (MOTD), предупреждает о том, что любые попытки несанкционированного доступа к коммутатору запрещены.

Для использования команды **banner motd** необходимы разграничители, чтобы можно было распознать содержимое баннерного сообщения. Разграничительным символом может быть любой символ, которого нет в данном сообщении. По этой причине часто используются такие символы, как #.

```
S1(config)#banner motd #
```

```
Enter TEXT message. End with the character '#'
```

Unauthorized access is strictly prohibited and prosecuted to the full extent of the law. #

```
S1(config)#
```

2.5.3.12 Настройте IP-шлюз по умолчанию для коммутатора SX (где X – номер бригады). Данным шлюзом будет являться Ethernet-интерфейс маршрутизатора RX (где X – номер бригады).

Если не настроен ни один шлюз по умолчанию, коммутатором нельзя управлять из удаленной сети и компьютеры не смогут получать доступ во внешнюю сеть. В качестве IP-адреса шлюза по умолчанию используйте IP-адрес маршрутизатора, который был определен в подпункте 2.5.1.2.

```
S1(config)#ip default-gateway 192.168.X.Y
```

```
S1(config)#exit
```

```
S1#
```

Внимание! В данном примере вместо X и Y подставьте свои значения, где X – номер бригады, Y – IP-адрес вашего шлюза по умолчанию.

2.5.3.13 Сохраните конфигурацию.

С помощью команды **copy** сохраните текущую конфигурацию в файл загрузочной конфигурации, который хранится в энергонезависимой памяти (NVRAM).

```
S1#copy running-config startup-config
```

```
Destination filename [startup-config]? [Enter]
```

```
Building configuration...
```

```
[OK]
```

```
S1#
```

2.5.3.14 Отобразите текущую конфигурацию.

Команда **show running-config** отображает всю текущую конфигурацию постранично. Для пролистывания страниц используйте клавишу **ПРОБЕЛ**. Команды, выполненные в подпунктах 2.5.3.1 – 2.5.3.12, выделены ниже.

```
S1#show running-config
```

```
Building configuration...
```

```
Current configuration : 1364 bytes
```

```
!
```

```
version 12.2
```

```
no service timestamps log datetime msec
```

```
no service timestamps debug datetime msec
```

```
service password-encryption
```

```
!
```

```
hostname S1
```

```
!
```

```
enable secret 5 $1$mERr$AC4/4pjw9OcfjbNW6dVXO0
```

```
!
```

```
no ip domain-lookup
```

```
!
```

```
spanning-tree mode pvst
```

```
!
```

```
interface FastEthernet0/1
```

```
... Внимание! Часть вывода информации пропущена...
```

```
interface GigabitEthernet0/2
```

```
!
```

```
interface Vlan1
```

```
no ip address
```

```
shutdown
```

```
!
```

```
ip default-gateway 192.168.X.Y <-Внимание! Здесь изменены значения.
```

```
!
```

```
banner motd ^CUnauthorized access is strictly prohibited and prosecuted to the  
full extent of the law!^C
```

```
!
```

```
line con 0
```

```
password 7 0822455D0A1606181C
```

```
logging synchronous
```

```
login
```

```
!
```

```
line vty 0 4
```

```
password 7 0822455D0A1613030B
```

```
login
```

```
line vty 5 15
```

```
password 7 0822455D0A1613030B
login
!
end
S1#
```

2.5.4 Базовая настройка маршрутизатора

По аналогии с базовой настройкой коммутатора осуществите базовую конфигурацию маршрутизатора (выполните подпункты с 2.5.3.1 по 2.5.3.11).

Внимание! Для маршрутизатора подпункт 2.5.3.12 не выполнять! Кроме того, для конфигурации маршрутизатора используйте консольное соединение компьютера РС-D. В качестве сетевого имени маршрутизатора (hostname) используйте RX, где X-номер бригады. Пароли доступа использовать те же, что и для коммутатора.

2.5.5 Дополнительная настройка интерфейсов маршрутизатора

2.5.5.1 Определите, к какому интерфейсу маршрутизатора подключён ваш коммутатор. Запишите имя интерфейса (например, GE 0/0 или GE 0/1).

2.5.5.2 Войдите в режим глобальной конфигурации маршрутизатора (см. подпункты 2.5.3.2 и 2.5.3.3).

2.5.5.3 Настройте интерфейс маршрутизатора для подключения его к локальной сети и дайте ему описание. Ниже приведён пример для случая подключения коммутатора к порту GE 0/0, по аналогии сделаете для GE 0/1.

```
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip address 192.168.X.Y 255.255.255.128
R1(config-if)#description Connection to LAN_X
R1(config-if)#no shutdown
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
R1(config-if)#exit
R1(config)#
```

Внимание! В данном примере вместо X и Y подставьте свои значения, где X – номер бригады, Y – IP-адрес вашего шлюза по умолчанию.

2.5.5.4 Сохраните и просмотрите конфигурацию маршрутизатора по аналогии, как это было сделано с коммутатором (см. пункт 2.5.3, подпункты 2.5.3.13 и 2.5.3.14).

2.5.6 Проверка работоспособности физических линий

Просмотрите состояние линий, статистические данные.

Проверьте работоспособность всей сети через утилиту **ping** и **tracert**. Все ли устройства «видят» друг друга? Если нет, то произведите настройку всех устройств так, чтобы все оконечные станции «видели друг друга». Объясните результат.

2.5.7 Выполнение резервного копирования конфигурации

Выполните резервное копирование конфигурации на TFTP-сервер. Выполните также резервное копирование конфигураций посредством выделения текстовой части в PuTTY и сохраните выделенные части в текстовые файлы. Сохраните текущую конфигурацию.

Удалите сохраненную конфигурацию и выполните перезагрузку устройства. Восстановите конфигурацию устройств из резервных копий. Проверьте работоспособность.

2.5.8 Завершающие этапы настройки сетевых устройств

После проверки выполнения лабораторной работы удалите все сохраненные настройки в файле **startup-config** на маршрутизаторе и коммутаторе, если она имеется. Перезапустите устройства. Убедитесь, что файл конфигурации был удалён и устройства находятся в стартовом режиме (Setup Mode).

2.6 СОДЕРЖАНИЕ ОТЧЁТА

2.6.1 Цель работы.

2.6.2 Расчёт сетевого диапазона для бригады (см. подпункт 2.5.1.2): адрес сети, маска подсети, широковещательный адрес, доступный диапазон адресов для хостов, адреса для компьютеров в бригаде, IP-адрес шлюза по умолчанию.

2.6.3 Схема изучаемой сетевой топологии с указанием IP-адресов компьютеров и IP-адрес шлюза по умолчанию.

2.6.4 Все сведения о конфигурации из IOS CLI на коммутаторе и маршрутизаторе.

2.6.5 Выводы по работе.

2.7 КОНТРОЛЬНЫЕ ВОПРОСЫ

2.7.1 Для чего применяются IP-адреса? Для чего предназначена маска сети? Какова структура адреса по протоколу IPv4? В чем суть классовой адресации? Назовите достоинства и недостатки.

2.7.2 Для чего применяются классы D и E? В чем суть бесклассовой адресации? Назовите достоинства и недостатки.

2.7.3 Для IP-адреса 192.168.1.78/26 определите: полную форму записи маски, адрес сети, широковещательный адрес, диапазон доступных адресов.

2.7.4 Для IP-адреса 200.54.18.6 255.255.255.0 определите: компактную форму записи маски, адрес сети, широковещательный адрес, диапазон доступных адресов.

2.7.5 Определите, каким по счету является IP-адрес 100.17.24.10/30 в диапазоне доступных адресов.

2.7.6 Широковещательный адрес сети 172.16.1.255, маска 255.255.255.0. Определите вторую форму записи маски, адрес сети, диапазон доступных адресов.

2.7.7 Как настроить IP-адрес на оконечном устройстве? Что такое шлюз по умолчанию и для чего он применяется? Как настроить шлюз по умолчанию на компьютере и коммутаторе? Для чего применяется DNS? Для чего рекомендуется отключать поиск DNS в процессе конфигурации сетевого устройства?

2.7.8 С помощью каких команд можно произвести тестирование сетевых адаптеров оконечных устройств? В чем суть тестирования loopback-интерфейса ПК? Как на ПК запустить командную строку? Для чего применяется команда **tracerout** на сетевых устройствах?

2.7.9 Что такое базовая конфигурация сетевого устройства? Какие выделяют основные этапы базовой конфигурации сетевого устройства? Чем отличается базовая конфигурация коммутатора от конфигурации маршрутизатора? Можно ли назначить нескольким сетевым устройствам в сети одно и то же имя **hostname**?

2.7.10 Расскажите о режимах ограничения доступа к конфигурации сетевого устройства? В чем смысл баннерных сообщений, как их настроить на сетевых устройствах? В чем отличие команды **enable secret** от **enable password**? Что происходит с открытыми ключами в тексте конфигурации после ввода команды **service password-encryption**? Как осуществить ограничение доступа по консольной и VTY линиям?

2.7.11 Для чего предназначены файлы текущей и загрузочной конфигурации? Как осуществить перезагрузку и удаление начальной конфигурации? Какие существуют варианты резервного сохранения конфигурации?

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Цикл методических материалов и контрольно-обучающих программ сетевой академии Cisco Systems [Электронный ресурс]. – 2016. – Режим доступа : <http://netacad.com/>.

2 Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2012. – 864 с.

3 Боллапрагада, В. Структура операционной системы Cisco IOS / В. Боллапрагада, К. Мэрфи, Р. Уайт. – М. : Вильямс, 2002. – 208 с.

4 Димарцио, Д. Ф. Маршрутизаторы Cisco. Пособие для самостоятельного изучения / Д. Ф. Димарцио. – СПб. : Символ-Плюс, 2003. – 512 с.

ЛАБОРАТОРНАЯ РАБОТА №3

КОММУТАТОРЫ. ТАБЛИЦА КОММУТАЦИИ. СПОСОБЫ ФОРМИРОВАНИЯ ТАБЛИЦЫ КОММУТАЦИИ. ПОДКЛЮЧЕНИЕ КОМПЬЮТЕРА К КОММУТАТОРУ И ФОРМИРОВАНИЕ ТАБЛИЦЫ КОММУТАЦИИ

3.1 ЦЕЛЬ РАБОТЫ

3.1.1 Изучение особенностей функционирования коммутаторов.

3.1.2 Изучение основ конфигурации интерфейсов коммутатора.

3.1.3 Изучение способов формирования таблицы коммутации.

3.2 ЗАДАНИЕ К РАБОТЕ

3.2.1 Изучить особенности технологии Ethernet.

3.2.2 Ознакомиться с функциональным назначением коммутатора.

3.2.3 Изучить основные возможности конфигурирования сетевых интерфейсов.

3.2.4 Исследовать процесс формирования таблицы коммутации.

3.2.5 Познакомиться с процессом удаленного управления коммутатором.

3.3 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

3.3.1 Технология Ethernet

В настоящее время Ethernet является основной технологией для построения пакетных сетей передачи данных. Ethernet функционирует на канальном и физическом уровнях. Стандарты протоколов Ethernet определяют формат и размер кадра³, интервал отправки и кодирование.

Технология Ethernet регламентируется стандартами IEEE 802.2, 802.3 и поддерживает передачу данных на скоростях:

- 10 Мбит/с;
- 100 Мбит/с;
- 1000 Мбит/с (1 Гбит/с);
- 10 000 Мбит/с (10 Гбит/с);
- 40 000 Мбит/с (40 Гбит/с);
- 100 000 Мбит/с (100 Гбит/с).

Как показано на рисунке 3.1, стандарты Ethernet регламентируют как протоколы уровня 2, так и технологии уровня 1. Для протоколов второго уровня

³ Кадры также называются протокольными блоками данных (от англ. Protocol Data Unit, PDU).

технология Ethernet полагается на работу двух отдельных подуровней канального уровня, а также на подуровни управления логическим каналом LLC и MAC.

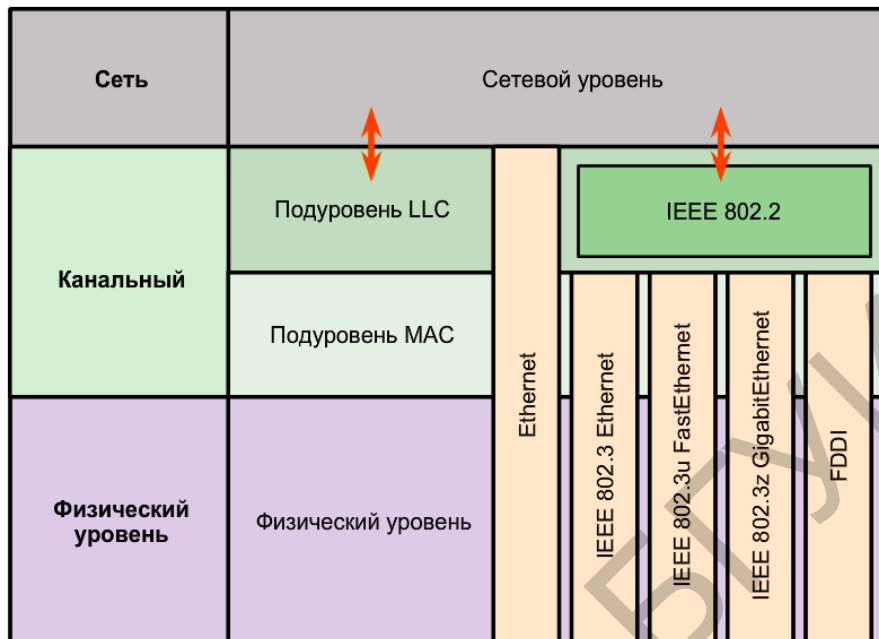


Рисунок 3.1 – Уровневая структура семейства технологий Ethernet

Подуровень LLC (от англ. Logical Link Control) технологии Ethernet обеспечивает связь между верхними и нижними уровнями. Как правило, это происходит между сетевым программным обеспечением (например, драйвер сетевой платы компьютера NIC) и аппаратным обеспечением устройства. Подуровень LLC использует данные сетевых протоколов, которые обычно представлены в виде пакета IPv4, и добавляет управляющую информацию, чтобы помочь доставить пакет к узлу назначения.

Подуровень MAC (от англ. Media Access Control) технологии Ethernet обеспечивает инкапсуляцию данных, в процессе чего формируется кадр заданной структуры перед его отправкой. При формировании кадра на уровне MAC к PDU сетевого уровня добавляются заголовок и концевик. Кроме того, подуровень MAC обеспечивает управление доступом к среде передачи данных.

В процессе инкапсуляции происходит синхронизация данных между передающими и получающими узлами с помощью специальных указателей в составе кадра. Процесс инкапсуляции также обеспечивает адресацию канального уровня. Каждый заголовок Ethernet, добавляемый в кадр, содержит физический адрес (MAC-адрес), посредством которого кадр доставляется к узлу назначения. Кроме того, каждый кадр Ethernet содержит концевик с циклическим контролем по избыточности (CRC), предназначенный для косвенного анализа ошибок.

Для предотвращения чрезмерных нагрузок, возникающих при обработке каждого кадра, был создан уникальный идентификатор – MAC-адрес, который

используется для определения фактических узлов источника и назначения в пределах сети Ethernet. Независимо от типа используемой сети Ethernet MAC-адресация обеспечила метод идентификации устройств на более низком уровне модели OSI.

MAC-адрес Ethernet – это 48-битное двоичное значение, выраженное в виде 12 шестнадцатеричных чисел (4 бита для каждой шестнадцатеричной цифры), является уникальным значением адреса в глобальном масштабе для конкретного сетевого адаптера (от англ. Network Interface Controller, NIC). Значение MAC-адреса – это непосредственный результат применения правил, которые разработаны институтом IEEE для поставщиков, чтобы обеспечить глобальные уникальные адреса для каждого устройства Ethernet. В соответствии с этими правилами каждый поставщик, который занимается реализацией Ethernet-устройств, должен быть зарегистрирован в IEEE. IEEE присваивает поставщику 3-байтный (24-битный) код, который называется уникальным идентификатором организации (от англ. Organizationally Unique Identifier, OUI).

Институт IEEE требует от поставщиков соблюдения двух простых правил, как показано на рисунке 3.2:

1) Все MAC-адреса, назначаемые сетевой интерфейсной плате или другому устройству Ethernet, должны в обязательном порядке использовать этот идентификатор OUI поставщика в виде первых 3 байт.

2) Всем MAC-адресам с одним и тем же идентификатором OUI должно быть присвоено уникальное значение (код производителя, или серийный номер), которое указывается в виде последних 3 байт.

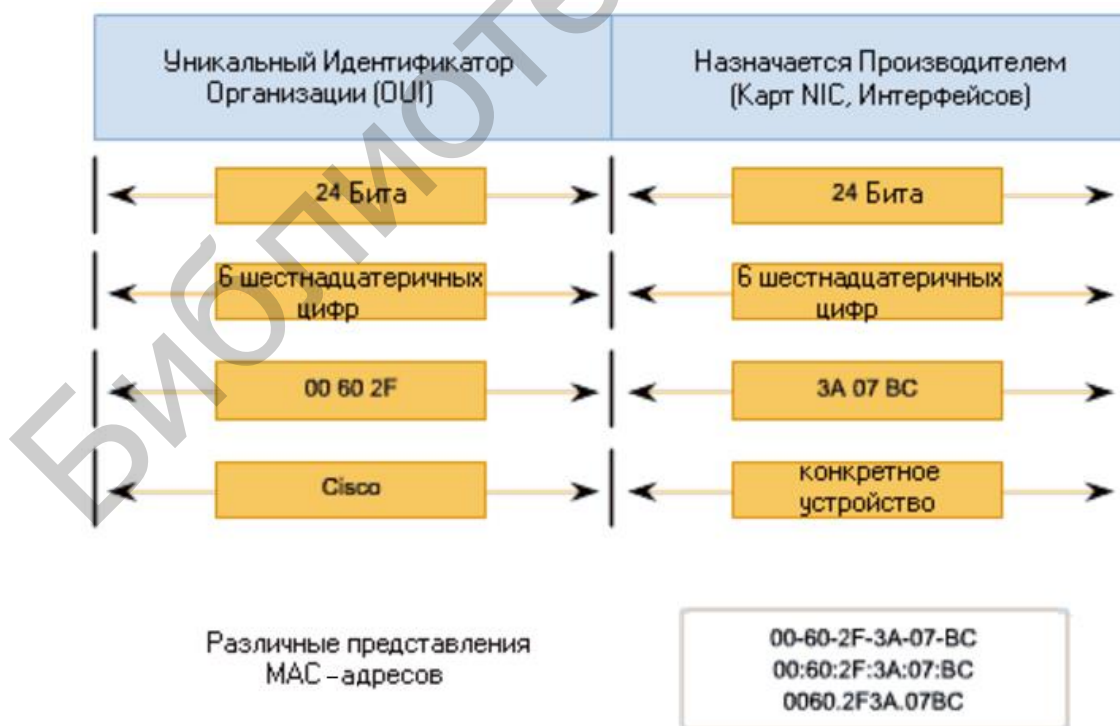


Рисунок 3.2 – Структура MAC-адреса

Основными полями кадра Ethernet (таблица 3.1) являются:

1) Поля «Преамбула» (7 байт) и «Начало разделителя кадра (SFD)», которое также называется «Начало кадра» (1 байт), используются для синхронизации приёмников.

2) Поле «MAC-адрес назначения» (6 байт) является идентификатором для предполагаемого получателя. Адрес в кадре сравнивается с MAC-адресом в устройстве. В случае совпадения устройство принимает кадр.

3) Поле «MAC-адрес источника» (6 байт), с его помощью определяется сетевая плата или интерфейс, отправившие кадр.

4) Поле «Длина» (2 байта). В любом стандарте IEEE 802.3, используемом до 1997 года, поле «Длина» определяет точную длину поля данных кадра. Позже оно используется как часть контрольной последовательности кадра (FCS), чтобы обеспечить правильность получения сообщения. В других случаях это поле используется, чтобы описывать, какой протокол более высокого уровня присутствует. Если 2-октетное значение равно или превышает шестнадцатеричный формат 0x0600 или десятичное число 1536, то содержимое поля «Данные» декодируется в соответствии с указанным протоколом EtherType. Если же значение равно или менее шестнадцатеричного формата 0x05DC или десятичного числа 1500, то поле «Длина» позволяет обозначить использование формата кадра IEEE 802.3. Вот таким образом различаются кадры Ethernet II и 802.3.

5) Поле «Данные» (46–1500 байт) содержит инкапсулированные данные из более высокого уровня, который является универсальным PDU уровня 3, или, что используется чаще, – пакетом IPv4. Длина всех кадров должна быть не менее 64 байт. В случае инкапсуляции небольшого пакета используются дополнительные биты, которые называются символами-заполнителями, для увеличения размера кадра до этого минимального значения.

6) Поле «Контрольная последовательность кадра» (4 байта) использует циклический контроль избыточности (CRC) для обнаружения ошибок в кадре. Передающее устройство перед отправкой кадра включает в данное поле результаты расчета CRC. Получающее устройство принимает кадр и пересчитывает CRC. Если расчёты совпадают со значением полученного поля с CRC, ошибки отсутствуют. Несовпадение расчётов означает изменение данных, следовательно, кадр отбрасывается. Причиной изменения данных может являться межсимвольная интерференция электрических сигналов либо неисправность сетевого устройства.

Таблица 3.1 – Структура кадра Ethernet (IEEE 802.3)

7 байт	1 байт	6 байт	6 байт	2 байта	46–1500 байт	4 байта
Преамбула	Начало разделителя кадра	MAC-адрес назначения	MAC-адрес источника	Длина (тип протокола)	Данные	Контрольная последовательность кадра

3.3.2 Функциональное назначение коммутатора, таблица коммутации, способы формирования

Коммутаторы локальных сетей обрабатывают кадры на основе алгоритма прозрачного моста (transparent bridge), который определен стандартом IEEE 802.1D. Процесс работы алгоритма прозрачного моста начинается с построения таблицы коммутации (Forwarding DataBase, FDB).

Изначально *таблица коммутации* пуста. При включении питания одновременно с передачей данных коммутатор начинает изучать расположение подключенных к нему сетевых устройств путём анализа MAC-адресов источников получаемых кадров. Например, если на порт 1 коммутатора, показанного на рисунке 3.3, поступает кадр от узла А, то он создаёт в таблице коммутации запись, ассоциирующую MAC-адрес узла А с номером входного порта. Записи в таблице коммутации создаются динамически. Это означает, что, как только коммутатором будет прочитан новый MAC-адрес, то он сразу будет занесён в таблицу коммутации. Дополнительно к MAC-адресу и ассоциированному с ним порту в таблицу коммутации для каждой записи заносится время старения (aging time). Время старения позволяет коммутатору автоматически реагировать на перемещение, добавление или удаление сетевых устройств.

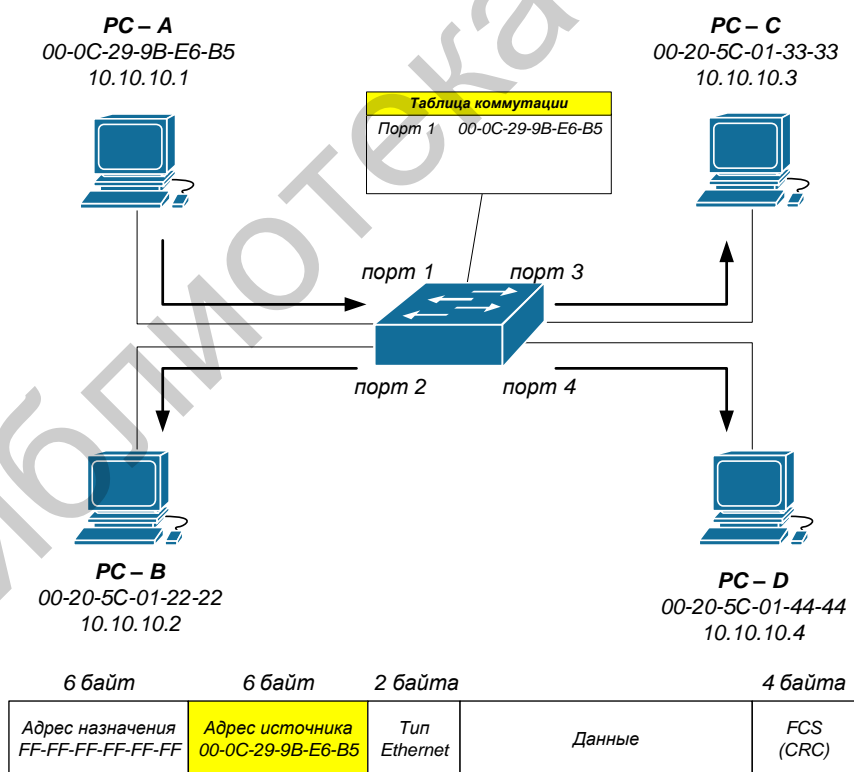


Рисунок 3.3 – Построение таблицы коммутации

Каждый раз, когда идёт обращение по какому-либо MAC-адресу, соответствующая запись получает новое время старения. Записи, к которым не обращались долгое время, из таблицы удаляются. Это позволяет хранить в таблице коммутации только актуальные MAC-адреса, что уменьшает время поиска соответствующей записи в ней и гарантирует, что она не будет использовать слишком много системной памяти.

Помимо динамического создания записей, в таблице коммутации в процессе самообучения коммутатора существует возможность создания статических записей вручную. Статическим записям, в отличие от динамических, не присваивается время старения, поэтому время их жизни не ограничено.

Статическую таблицу коммутации удобно использовать с целью повышения сетевой безопасности, когда необходимо гарантировать, что только устройства с определенными MAC-адресами могут подключаться к сети. В этом случае необходимо отключить автоизучение MAC-адресов на портах коммутатора.

Внимание! Как правило, размер статической таблицы коммутации меньше размера динамической таблицы коммутации. Размеры обеих таблиц также зависят от модели коммутатора. Обычно производители указывают размеры таблиц коммутации в спецификациях устройств.

Как только в таблице коммутации появляется хотя бы одна запись, коммутатор начинает использовать её для пересылки кадров. Рассмотрим пример, показанный на рисунке 3.4, описывающий процесс пересылки кадров между портами коммутатора.

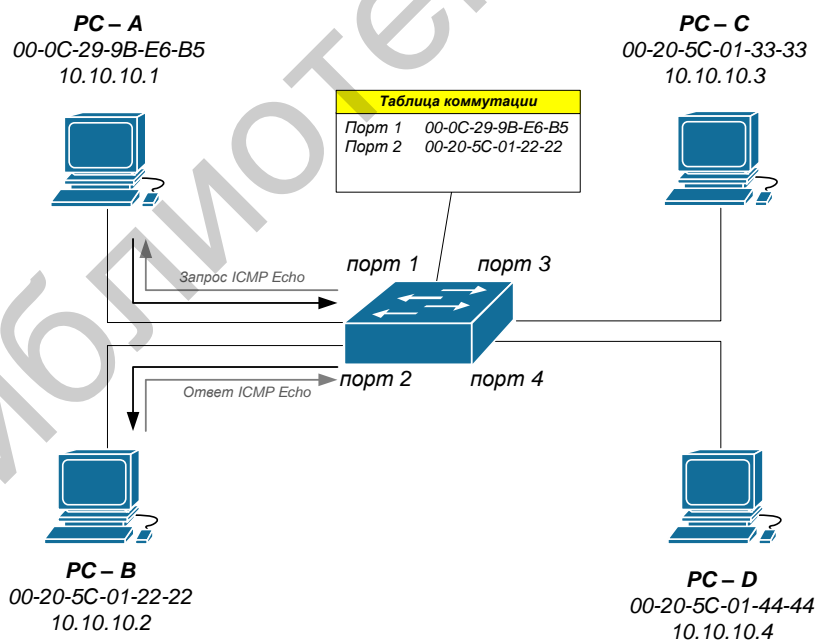


Рисунок 3.4 – Передача кадра с порта на порт коммутатора

Когда коммутатор получает кадр, отправленный компьютером А компьютеру В, он извлекает из него MAC-адрес приёмника и ищет этот MAC-адрес в

своей таблице коммутации. Как только в таблице коммутации будет найдена запись, ассоциирующая MAC-адрес приёмника (компьютера В) с одним из портов коммутатора, за исключением порта-источника, кадр будет передан через соответствующий выходной порт (в приведённом примере – порт 2). Этот процесс называется продвижением (forwarding) кадра.

Если бы оказалось, что выходной порт и порт-источник совпадают, то передаваемый кадр был бы отброшен коммутатором. Этот процесс называется фильтрацией (filtering).

В том случае, если MAC-адрес приёмника в поступившем кадре неизвестен (в таблице коммутации отсутствует соответствующая запись), коммутатор создаёт множество копий этого кадра и передаёт их через все свои порты, за исключением того, на который он поступил. Этот процесс называется лавинной передачей (flooding). Несмотря на то что процесс лавинной передачи занимает полосу пропускания, он позволяет коммутатору избежать потери кадров, когда MAC-адрес приёмника неизвестен, и осуществлять процесс самообучения.

Помимо лавинной передачи одноадресных кадров, коммутаторы также выполняют лавинную передачу многоадресных и широковещательных кадров, которые генерируются сетевыми мультимедийными приложениями.

3.3.3 Основы управления состоянием таблицы коммутации

На коммутаторах Cisco в режиме командной строки (CLI) существует набор команд для контроля за состоянием и управления содержимым таблицы коммутации.

Для того чтобы определить MAC-адрес, полученный коммутатором, необходимо использовать команду **show mac address-table** в привилегированном режиме:

```
S1#show mac address-table
```

В ответ на эту команду коммутатор ответит списком изученных физических адресов сетевых устройств, которые подключены к коммутатору:

```
S1#show mac address-table
```

```
Mac Address Table
```

```
-----  
Vlan Mac Address  Type  Ports  
-----  -  
1    0060.5cc3.01ca DYNAMIC Fa0/1  
1    0090.2132.7ca1 DYNAMIC Fa0/2  
1    00d0.bad3.c165 DYNAMIC Fa0/3  
1    0002.1635.4d26 DYNAMIC Fa0/4
```

```
S1#
```

По полученному ответу можно судить, что коммутатор динамически изучил (DYNAMIC) подключённые сетевые устройства, которые присоединены интерфейсами FastEthernet (Fa) с номерами портов с 0/1 по 0/4. Их MAC-адреса

приведены в соответствующем столбце – это физические адреса сетевых устройств.

Даже если сетевая коммуникация в сети не происходила (т. е. не использовался эхо-запрос с помощью команды **ping**), коммутатор может узнать MAC-адреса при подключении к ПК и другим коммутаторам.

Для очистки таблицы MAC-адресов коммутатора S1 можно использовать в привилегированном режиме команду **clear mac address-table**. Пример конфигурации:

```
S1#clear mac address-table
```

В результате действия данной команды всё содержимое таблицы коммутации обнулится и, если теперь попытаться отобразить таблицу, в ней не будет записей о подключённых устройствах.

Для того чтобы коммутатор вновь изучил подключённые к нему устройства, необходимо на оконечных устройствах произвести **ping** запросы, например, на IP-адреса соседних устройств. В результате данной операции таблица коммутации будет наполняться записями физических интерфейсов (MAC-адресами) сетевых устройств.

Для того чтобы определить MAC-адрес сетевого адаптера (NIC) компьютера, в командной строке компьютера выполните команду **ipconfig/all**.

```
PC>ipconfig/all
```

```
FastEthernet0 Connection:(default port)
```

```
Connection-specific DNS Suffix..:
```

```
Physical Address.....: 0060.5CC3.01CA
```

```
Link-local IPv6 Address.....: FE80::260:5CFF:FEC3:1CA
```

```
IP Address.....: 10.10.10.1
```

```
Subnet Mask.....: 255.0.0.0
```

```
Default Gateway.....: 0.0.0.0
```

```
DNS Servers.....: 0.0.0.0
```

```
DHCP Servers.....: 0.0.0.0
```

```
DHCPv6 Client DUID.....: 00-01-00-01-C3-E1-53-35-00-60-5C-C3-01-CA
```

3.3.4 Основы конфигурации сетевых интерфейсов коммутатора

Порядок конфигурации сетевых интерфейсов на коммутаторе предусматривает следующие операции:

- выбор порта интерфейса (вход в режим конфигурации интерфейса);
- настройка режима дуплекса;
- настройка скорости порта интерфейса;
- настройка автоматического определения типа кабеля (auto-MDIX);
- настройка описания интерфейса;

- включение/отключение порта;
- команды проверки состояния интерфейса.

3.3.4.1 Вход в режим конфигурации интерфейса

Вход в режим конфигурации интерфейса на коммутаторах Cisco 2960 выполняется следующим образом:

1) Необходимо войти в режиме глобальной конфигурации с помощью команды **configure terminal**.

2) Определить номер порта коммутатора, на котором будут производиться настройки.

Примечание – Коммутатор Cisco 2960 содержит 24 низкоскоростных порта FastEthernet со скоростью передачи 100 Мбит/с и два GigabitEthernet со скоростью 1000 Мбит/с (см. приложение Б). Пример обозначения порта коммутатора Cisco 2960 с номером 12: **FastEthernet 0/12**, где цифра **0/** – обозначает номер слота (модуля) коммутатора, а **12** – порядковый номер порта в составе слота. Cisco 2960 содержит только один модуль, поэтому его нумерация всегда начинается с **0/**. Для многомодульных коммутаторов типа Cisco Catalyst 6509 обращение к модулю осуществляется именно по первой части нумерации, т. е. запись **1/**, **2/**... соответствует обращению к первому, второму и последующим модулям коммутатора Cisco 6509.

3) Войти в режим конфигурации Ethernet-интерфейса.

Ниже приведен пример входа в режим конфигурации интерфейса:

```
S1#configure terminal
```

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

```
S1(config)#interface fastEthernet 0/12
```

```
S1(config-if)#
```

Отличительной особенностью того, что был выполнен вход в режим конфигурации интерфейса, является запись config-if в скобках. Соответственно все последующие операции будут применимы только к **0/12** Ethernet-порту коммутатора.

Примечание – Для того чтобы произвести идентичные настройки на группе портов коммутатора, можно использовать следующую запись:

```
S1(config)#interface range fastEthernet 0/1-8
```

```
S1(config-if-range)#
```

В данном случае используется команда **range**, а далее выбирается требуемый диапазон. Запись config-if-range в скобках соответствует нахождению в режиме конфигурации группы интерфейсов.

3.3.4.2 Настройка режима дуплекса и скорости интерфейса

Полнодуплексная связь позволяет передавать и получать данные одновременно в обоих направлениях, за счет чего повышается эффективность полосы пропускания линии связи.

Полудуплексная связь является однонаправленной, т. е. отправка и приём данных не происходят одновременно. Полудуплексная связь плохо сказывается на производительности, т. к. одновременно данные могут передаваться только

в одном направлении (рисунок 3.5). На данный момент практически не используется.

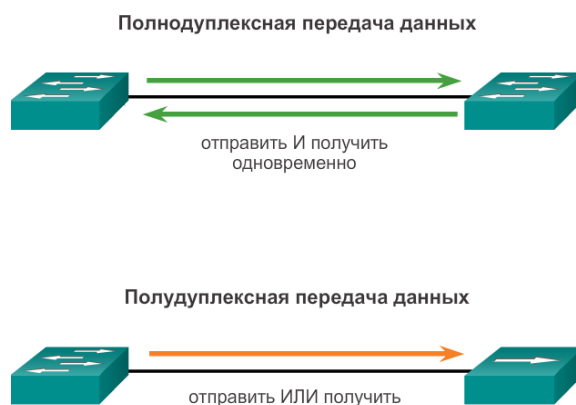


Рисунок 3.5 – Режимы дуплексной связи

Команды режима конфигурации интерфейса **duplex** и **speed** позволяют вручную установить дуплексный режим и скорость для порта коммутатора.

Автосогласование параметров дуплекса и скорости полезно, когда настройки этих параметров для устройства, подключенного к порту, неизвестны или могут меняться. При подключении к известным устройствам, таким как серверы, выделенные рабочие станции или сетевые устройства, рекомендуется вручную задавать параметры скорости и дуплекса.

3.3.4.3 Настройка автоматического определения типа кабеля (auto-MDIX)

До недавнего времени при соединении устройств требовались определённые типы кабелей (прямые или кроссовые). Для соединения двух коммутаторов или коммутатора и маршрутизатора требовались разные кабели стандарта Ethernet. Более подробно о различных схемах коммутации и применении различных типов кабелей смотрите в приложении Г.

Использование функции автоматического определения кабеля (auto-MDIX) позволяет решить проблему выбора коммутации пар между сетевыми устройствами. При включенной функции auto-MDIX интерфейс распознаёт требуемый тип кабельного соединения (прямое или кроссовое) и настраивает подключение соответствующим образом.

На новых маршрутизаторах и коммутаторах Cisco эту функцию включает команда режима конфигурации интерфейса **mdix auto**. При использовании функции auto-MDIX на интерфейсе скорость интерфейса и дуплексный режим должны быть настроены в режим **auto**, чтобы функция работала должным образом.

Команды для включения функции auto-MDIX показаны на рисунке 3.6.

Примечание – Функция auto-MDIX по умолчанию включена на коммутаторах Catalyst 2960 и Catalyst 3560, но недоступна на коммутаторах прежних версий Catalyst 2950 и Catalyst 3550.

Чтобы просмотреть настройки функции auto-MDIX для конкретного интерфейса, следует использовать команду **show controllers ethernet-controller** с ключевым словом **phy**. Для отображения выходных данных, имеющих отношение к функции auto-MDIX, используйте фильтр **include Auto-MDIX**.

На рисунке 3.6 приведён пример настройки интерфейса Ethernet с заданным типом дуплекса, скорости и функции auto-MDIX.

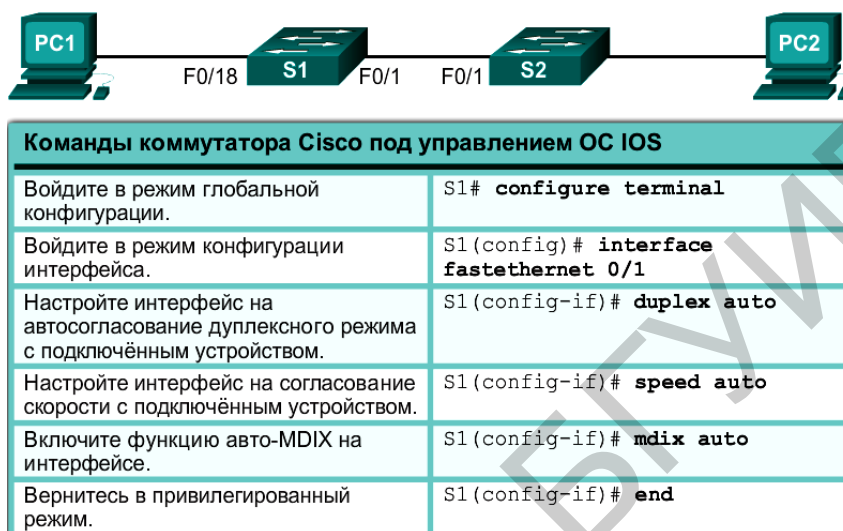


Рисунок 3.6 – Пример настройки интерфейса Ethernet

3.3.4.4 Настройка описания интерфейса

Очень часто для последующих конфигураций и мониторинга состояний сетевых устройств каждому соединению вводят краткое описание с целью косвенного анализа, к какому устройству подключён данный порт.

На всех сетевых устройствах Cisco под управлением IOS данное описание вводится с помощью команды **description**. Пример конфигурации описания на порту **0/1** коммутатора **S1**, к которому подключен коммутатор **S2**:

```
S1(config)#interface fa0/1
S1(config-if)#description connect to S2
S1(config-if)#exit
S1(config)#
```

3.3.4.5 Включение/отключение портов коммутатора

В отличие от маршрутизаторов на коммутаторах Cisco по умолчанию все порты включены и готовы для передачи кадров Ethernet. Тем не менее с целью обеспечения безопасности рекомендуется выключать неиспользуемые порты. Для этого в режиме конфигурации интерфейса используется команда **shutdown**. Последующее включение данного порта возможно с помощью команды **no shutdown**. Ниже приведен пример отключения порта **0/1** на коммутаторе:

```
S1(config)#interface fa0/1
S1(config-if)#shutdown
```

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

```
S1(config-if)#exit
```

```
S1(config)#
```

Внимание! Отключение порта сопровождается командой административного отключения «%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down».

3.3.4.6 Команды проверки состояния интерфейса

Команда **show interfaces** является распространённой командой, которая выводит данные о состоянии и статистике сетевых интерфейсов коммутатора. Команда **show interfaces** часто используется при настройке и мониторинге сетевых устройств.

Ниже показаны выходные данные команды **show interfaces fastEthernet 0/18**. Первая строка указывает, что интерфейс FastEthernet 0/18 находится в состоянии up/up, т. е. в рабочем состоянии, кроме того, отмечено, что включён полнодуплексный режим, а скорость настроена на 100 Мбит/с.

```
S1#show interfaces fa0/18
```

```
FastEthernet0/18 is up, line protocol is up (connected)
```

```
Hardware is Lance, address is 0090.0c1c.db12 (bia 0090.0c1c.db12)
```

```
BW 100000 Kbit, DLY 1000 usec,
```

```
reliability 255/255, txload 1/255, rxload 1/255
```

```
Encapsulation ARPA, loopback not set
```

```
Keepalive set (10 sec)
```

```
Full-duplex, 100Mb/s
```

```
input flow-control is off, output flow-control is off
```

```
ARP type: ARPA, ARP Timeout 04:00:00
```

```
Last input 00:00:08, output 00:00:05, output hang never
```

```
Last clearing of "show interface" counters never
```

```
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
```

```
Queueing strategy: fifo
```

```
Output queue :0/40 (size/max)
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
```

```
5 minute output rate 0 bits/sec, 0 packets/sec
```

```
956 packets input, 193351 bytes, 0 no buffer
```

```
Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
```

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
0 watchdog, 0 multicast, 0 pause input
```

```
0 input packets with dribble condition detected
```

```
2357 packets output, 263570 bytes, 0 underruns
```

```
0 output errors, 0 collisions, 10 interface resets
```

```
0 babbles, 0 late collision, 0 deferred
```

```
0 lost carrier, 0 no carrier
```

```
0 output buffer failures, 0 output buffers swapped out
```

3.3.5 Удалённое управление коммутатором

3.3.5.1 Понятия SVI и VLAN

На коммутаторах Cisco можно настроить особый IP-адрес, который называют виртуальным интерфейсом коммутатора (SVI – Switch Virtual Interface). SVI или адрес управления можно использовать для удалённого доступа к коммутатору в целях отображения или настройки параметров. Если для SVI сети VLAN 1 назначен IP-адрес, то по умолчанию все порты в сети VLAN 1 имеют доступ к IP-адресу управления SVI.

Для удалённого доступа к коммутатору на виртуальном интерфейсе коммутатора нужно настроить IP-адрес и маску подсети:

- **interface vlan 1** – применяется для перехода в режим настройки виртуального интерфейса из режима глобальной конфигурации;

- **ip address 192.168.1.2 255.255.255.0** – настраивает IP-адрес и маску подсети для коммутатора (здесь указан в качестве примера IP-адрес и маска 192.168.1.2 255.255.255.0);

- **no shutdown** – активизирует интерфейс.

После настройки этих команд все IP-элементы в коммутаторе будут готовы для передачи данных по сети.

Примечание – Для удалённого управления коммутатором необходима настройка одного или нескольких физических портов, а также каналов VTY.

Согласно конфигурации коммутатора по умолчанию управление коммутатором должно осуществляться через VLAN 1. Однако в базовой конфигурации коммутатора не рекомендуется назначать VLAN 1 в качестве административной VLAN. Для административных целей рекомендуется использовать другой номер, например VLAN 99.

Интерфейс SVI не будет отображаться как up/up, пока не будет создана VLAN и не появится устройство, подключённое к порту коммутатора, связанному с этим VLAN. Для того чтобы создать сеть VLAN с идентификатором *vlan_id* и привязать её к интерфейсу, используйте следующие команды:

```
S1(config)#vlan vlan_id
```

```
S1(config-vlan)#name vlan_name
```

```
S1(config-vlan)#exit
```

```
S1(config)#interface interface_id
```

```
S1(config-if)#switchport access vlan vlan_id
```

3.3.5.2 Процедура настройки SVI и осуществление удаленного управления

Шаг 1. Настройка интерфейса управления

Войдите в режим глобальной конфигурации, чтобы назначить коммутатору IP-адрес SVI (см. ниже).

Для настройки IP-адреса и маски подсети используется команда **interface vlan 99**. Для настройки IP-адреса используется команда **ip address**. Команда **no**

shutdown активирует интерфейс. В данном примере сеть VLAN 99 настроена с IP-адресом 192.168.1.2/24.

```
S1#configure terminal
```

```
S1(config)#vlan 99
```

```
S1(config-vlan)#exit
```

```
S1(config)#interface vlan 99
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
```

```
S1(config-if)#ip address 192.168.1.2 255.255.255.0
```

```
S1(config-if)#no shutdown
```

```
S1(config-if)#exit
```

```
S1(config)#
```

Обратите внимание, что интерфейс VLAN 99 выключен, несмотря на то что введена команда **no shutdown** (выделено). В настоящее время интерфейс выключен, поскольку сети VLAN 99 не назначены порты коммутатора.

Шаг 2. Ассоциирование портов коммутатора с виртуальной сетью

Для ассоциирования (привязки) всех пользовательских портов, для которых разрешен удаленный доступ к коммутатору, используется следующая настройка.

```
S1(config)#interface range f0/1 - 24,g0/1 - 2
```

```
S1(config-if-range)#switchport access vlan 99
```

```
S1(config-if-range)#exit
```

```
S1(config)#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

Чтобы установить подключение между узлом и коммутатором, порты, используемые узлом, должны находиться в той же VLAN, что и коммутатор. Обратите внимание, что в выходных данных, представленных выше, интерфейс VLAN 1 выключился, поскольку теперь ни один из портов не назначен сети VLAN 1.

Шаг 3. Настройка шлюза по умолчанию

В случае если требуется управлять коммутатором удаленно из сетей без прямого подключения, на коммутаторе следует настроить шлюз по умолчанию. Шлюз по умолчанию – это IP-адрес интерфейса маршрутизатора, к которому подключен коммутатор. Коммутатор пересылает IP-пакеты с IP-адресами назначения за пределы локальной сети на шлюз по умолчанию. Например, если интерфейс маршрутизатора R1, подключенный к коммутатору, имеет IP-адрес 192.168.1.1. Указанный адрес является адресом шлюза по умолчанию для коммутатора S1.

Для того чтобы настроить шлюз по умолчанию для коммутатора, используйте команду **ip default-gateway**. Введите IP-адрес шлюза по умолчанию (ниже пример):

```
S1#configure terminal
```

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

```
S1(config)#ip default-gateway 192.168.1.1
```

```
S1(config)#exit
```

Шаг 4. Проверка конфигурации

Чтобы убедиться, что все пользовательские порты находятся в сети VLAN 99, выполните команду **show vlan brief**:

```
S1#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	
99 VLAN0099	active	Fa0/1, Fa0/2, 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 Gig0/1, Gig0/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
S1#
```

Шаг 5. Настройка удалённого соединения по Telnet

В производственной сети коммутатор может находиться в коммутационном шкафу или в другой сети, в то время как административный компьютер не имеет прямого подключения по консольной линии. Очень часто в подобных случаях для удалённого управления используется протокол Telnet или его более безопасный аналог SSH⁴.

Telnet (от англ. TErminal NETwork) – сетевой протокол для реализации текстового интерфейса по сети при помощи транспорта TCP. В основном при-

⁴ SSH (от англ. Secure Shell – безопасная оболочка) – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов). Схож по функциональности с протоколом Telnet, но, в отличие от него, шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования. SSH-клиенты и SSH-серверы доступны для большинства сетевых операционных систем.

меняется для удалённого управления сетевыми устройствами в сети. Современный стандарт протокола описан в RFC 854.

Telnet – это небезопасный протокол, но его можно использовать для проверки удалённого доступа. В случае с Telnet вся информация, включая пароли и команды, отправляется через сеанс в незашифрованном виде. Для более безопасного удалённого доступа к сетевым устройствам рекомендуется использовать SSH.

Примечание – При использовании Windows 7 может потребоваться включение протокола Telnet от имени администратора. Чтобы установить клиент Telnet, откройте окно **cmd** и введите **pkgmgr /iu:«TelnetCNent»**. Ниже приведён пример.

```
C:\Users\User1> pkgmgr /iu:"TelnetClient"
```

В том же окне **cmd** на компьютере PC-A выполните команду Telnet для подключения к коммутатору S1 через административный адрес SVI. В качестве пароля используйте пароль, который настроен для линий VTY.

```
C:\Users\User1> telnet 192.168.1.2
```

После ввода пароля появится командная строка пользовательского режима. Войдите в привилегированный режим.

Чтобы завершить сеанс Telnet, используйте команду **exit**.

Шаг 6. Сохранение текущей конфигурации на удалённый файловый сервер

Существует несколько вариантов сохранения текущей конфигурации коммутатора, ниже приведён пример сохранения на TFTP-сервер:

```
S1#copy running-config tftp:  
Address or name of remote host []? 192.168.1.170  
Destination filename [S1-config]?  
Writing running-config....!!  
[OK - 1825 bytes]  
1825 bytes copied in 3.015 secs (0 bytes/sec)
```

Здесь применяется следующий порядок: после ввода команды сохранения на tftp-сервер **copy running-config tftp:** указывается IP-адрес данного сервера, затем имя файла конфигурации, под которым будет осуществляться сохранение. Успешным сохранением принято считать появление сообщения ОК и объём записанной информации.

3.4 ОПИСАНИЕ ЛАБОРАТОРНОГО СТЕНДА

Работа выполняется бригадами из трёх-четырёх человек. В процессе выполнения работы каждой бригаде выделяется коммутатор Cisco Catalyst 2960. Для подключения к устройству студентам необходимо произвести коммутацию на соответствующих патчпанелях и сетевых розетках. Для выполнения работы студентам также понадобится программное обеспечение для терминального до-

стуга (например, PuTTY), а также приложение для эмуляции файлового сервера (например, TFTPД32).

Внимание! Для подключения компьютеров к Ethernet-портам коммутатора используйте второй «УЧЕБНЫЙ» порт сетевой розетки (см. рисунок 1.5) и не забывайте при этом производить соответствующие коммутации на патчпанели №2 и коммутаторе. Порядок подключения к консольным портам оборудования описан в лабораторной работе №1.

В данной работе предусматривается изучение следующей топологии сети (рисунок 3.7).

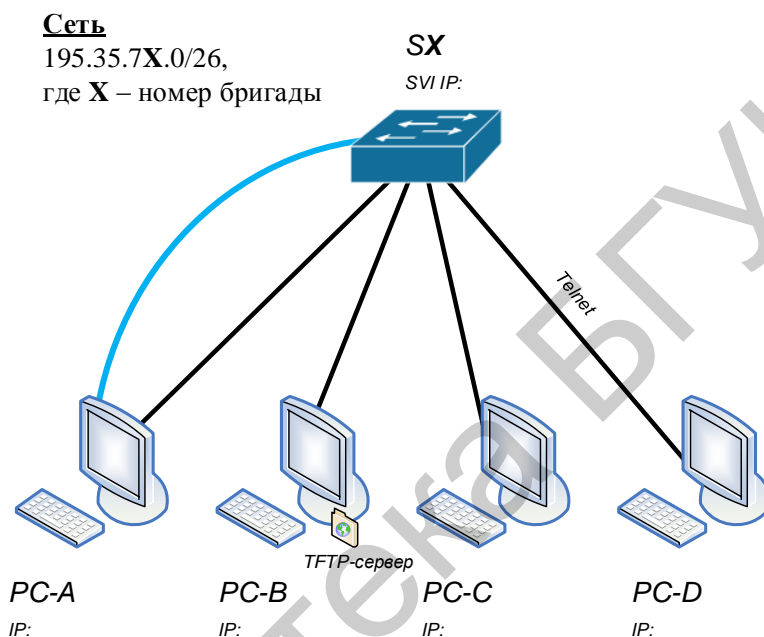


Рисунок 3.7 – Схема подключения сетевого оборудования

3.5 ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

3.5.1 Исследование изучаемой топологии

3.5.1.1 К интерфейсам коммутатора SX (где X – номер бригады) подключите компьютеры согласно схеме и назначьте им IP-адреса из диапазона 195.35.7X.0/26 (где X – номер бригады). Используйте первые доступные IP-адреса из подсетей для компьютеров, а последний доступный – для удалённого управления коммутатором по SVI. Какие типы кабелей будете использовать при реализации подключения (см. приложение Г)?

3.5.1.2 К интерфейсам коммутатора, начиная с номера 1 и по порядку, подключите компьютеры и назначьте им адреса, начиная с первого доступного и по порядку, из диапазонов согласно номеру бригады.

3.5.1.3 Компьютер PC-B будет являться TFTP-сервером для данной топологии сети. Для этого на рабочем столе PC-B запустите приложение TFTPД32.

Настройте рабочую папку, предварительно создав её, для приложения указав следующий путь:

D:\work\номер вашей группы\фамилия_или_логин

3.5.1.4 Компьютер PC-A используется для внеполосной настройки посредством консольных линий согласно схеме.

3.5.2 Настройка параметров коммутатора

3.5.2.1 Начните с базовой настройки коммутатора через PuTTY на PC-A:

- установите соответствующее имя на устройство;
- установите доступ по паролю **ciscoenapa** к привилегированному режиму;
- установите доступ по паролю **ciscovty** к Telnet-линиям vty;
- установите доступ по паролю **ciscocon** к консольной линии;
- все пароли должны храниться в зашифрованном виде;
- установите актуальное время на устройствах;
- сконфигурируйте сообщение дня **“Unauthorized access strictly prohibited and prosecuted to the full extent of the law!”**;
- отключите поиск DNS-серверов;
- обеспечьте синхронизацию командной строки на линии управления.

3.5.2.2 Проведите дополнительные настройки на коммутаторе:

- установите все интерфейсы на полный дуплекс с максимально поддерживаемой скоростью работы порта и включением функции auto-MDIX;
- установите описание интерфейсов, все неиспользуемые интерфейсы переведите в состояние administratively down;
- создайте интерфейс управления SVI 99 на коммутаторе и назначьте ему последний IP-адрес из соответствующего диапазона адресов, к которым относятся компьютеры, обеспечьте доступность интерфейсов управления по протоколу Telnet для всех портов, к которым подключены компьютеры.

3.5.3 Изучение таблицы MAC-адресов коммутатора

3.5.3.1 Запишите MAC-адреса сетевых устройств с помощью соответствующих команд отображения информации о работе интерфейсов: на всех внутрисетевых интерфейсах компьютеров, по которым они подключены к коммутатору и на всех внутрисетевых интерфейсах коммутатора, к которому подключены компьютеры.

3.5.3.2 По всем полученным MAC-адресам определите уникальный идентификатор OUI и серийный номер адаптера.

3.5.3.3 Отобразите таблицу MAC-адресов коммутатора. Какие MAC-адреса записаны в таблице? С какими портами коммутатора они сопоставлены и каким устройствам принадлежат?

3.5.3.4 Очистите таблицу MAC-адресов коммутатора и снова отобразите таблицу MAC-адресов. Появились ли в таблице MAC-адресов новые адреса?

3.5.3.5 С компьютера PC-D отправьте эхо-запросы на все устройства в сети и просмотрите таблицу MAC-адресов коммутатора. Как она изменяется?

3.5.3.6 Произведите отключение компьютера PC-A от коммутатора по внутрисполосному интерфейсу (произведите соответствующее отключение на патчпанели №2). Как изменилась таблица MAC-адресов коммутатора?

3.5.3.7 Подключите компьютер PC-A к коммутатору по внутрисполосному интерфейсу. Что необходимо сделать, чтобы в таблицу MAC-адресов была внесена запись о компьютере PC-A?

3.5.4 Доступ к коммутатору через Telnet. Работа с конфигурацией

3.5.4.1 На компьютере PC-D запустите клиентское приложение PuTTY.

3.5.4.2 Через Telnet получите доступ к коммутатору. Какой пароль требуется для входа в управление устройством?

3.5.4.3 Отобразите текущую конфигурацию устройства через Telnet.

3.5.4.4 Сохраните все файлы конфигурации устройств на TFTP-сервер, а также через функцию запись протокола в файл через PuTTY. Просмотрите сохраненные файлы. Какое имя имеет файл, который сохранен на TFTP-сервер?

3.5.5 Завершающие этапы настройки коммутатора

После проверки выполнения лабораторной работы удалите всю сохраненную настройку в файле **startup-config** на коммутаторе, если она имеется. Учтите, что данные о VLAN на коммутаторе хранятся в отдельном файле под названием **vlan.dat**. Удалите этот файл. Перезапустите устройство. Убедитесь, что файл конфигурации был удален и устройство находится в стартовом режиме (Setup Mode).

3.6 СОДЕРЖАНИЕ ОТЧЁТА

3.6.1 Цель работы.

3.6.2 Расчёт выделенного бригаде сетевого диапазона: адрес сети, маски подсети, широковещательный адрес, доступный диапазон адресов для хостов, адресов, предназначенных для компьютеров, IP-адрес для доступа к коммутатору по SVI.

3.6.3 Схема изучаемой сетевой топологии с указанием IP-адресов сетевых устройств и SVI IP для доступа к коммутатору.

3.6.4 Запишите ответы на вопросы, которые приведены в пунктах 3.5.1, 3.5.3, 3.5.4.

3.6.5 Приведите всю конфигурацию из IOS CLI на коммутаторе, а также всю информацию о содержании таблицы коммутации на коммутаторе.

3.6.6 Выводы по работе.

3.7 КОНТРОЛЬНЫЕ ВОПРОСЫ

3.7.1 На каких уровнях функционирует технология Ethernet? Какие скорости передачи и в каких режимах может обеспечить технология Ethernet? Поясните назначение полей в структуре кадра Ethernet.

3.7.2 Какие функции выполняет подуровень LLC? Что такое подуровень MAC и для чего он применяется? Какова структура MAC-адреса?

3.7.3 Поясните процесс формирования записей в таблице коммутации.

3.7.4 Какие команды в IOS используются для управления состоянием таблицы коммутации? Может ли в таблице коммутации для заданного порта присутствовать более чем одна запись MAC-адреса?

3.7.5 Как заставить коммутатор изучить MAC-адреса подключённых к нему сетевых устройств? Расскажите о порядке конфигурации сетевых интерфейсов на коммутаторе.

3.7.6 Что такое дуплекс и какие режимы дуплекса существуют? Приведите примеры его использования. Для чего применяется технология auto-MDIX?

3.7.7 Каким типом кабеля соединяются между собой сетевые устройства? Перечислите все возможные комбинации соединений и применяемых типов кабелей для: ПК, концентраторов, коммутаторов, маршрутизаторов.

3.7.8 С помощью каких команд в IOS можно выключить группу сетевых интерфейсов? Для чего может понадобиться настройка SVI? Расскажите о порядке настройки SVI на коммутаторе.

3.7.9 Выделите в MAC-адресе 0060.5c3.01ca часть идентификатора производителя OUI и серийный номер адаптера порта Ethernet.

3.7.10 Выявите достоинства и недостатки VLAN.

3.7.11 Проведите сравнительный анализ протоколов Telnet и SSH.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Цикл методических материалов и контрольно-обучающих программ сетевой академии Cisco Systems [Электронный ресурс]. – 2016. – Режим доступа : <http://netacad.com/>.

2 Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2012. – 864 с.

3 Пахомов, С. Возможности современных коммутаторов по организации виртуальных сетей. КомпьютерПресс 4 / С. Пахомов [Электронный ресурс]. – 2005. – Режим доступа : <http://www.cpress.ru/>.

ЛАБОРАТОРНАЯ РАБОТА №4

МАРШРУТИЗАТОРЫ. ТАБЛИЦА МАРШРУТИЗАЦИИ. СПОСОБЫ ФОРМИРОВАНИЯ ТАБЛИЦЫ МАРШРУТИЗАЦИИ. СТАТИЧЕСКОЕ ЗАПОЛНЕНИЕ ТАБЛИЦЫ МАРШРУТИЗАЦИИ. СОЕДИНЕНИЕ КОМПЬЮТЕРОВ ЧЕРЕЗ МАРШРУТИЗАТОРЫ

4.1 ЦЕЛЬ РАБОТЫ

4.1.1 Изучение принципов маршрутизации.

4.1.2 Знакомство с построением статических таблиц маршрутизации.

4.2 ЗАДАНИЕ К РАБОТЕ

4.2.1 Ознакомиться с функциональным назначением маршрутизатора.

4.2.2 Исследовать процесс формирования таблицы маршрутизации.

4.2.3 Изучить особенности конфигурирования сетевых интерфейсов на маршрутизаторах.

4.2.4 Познакомиться с процессом конфигурации статических маршрутов и их оптимизацией.

4.3 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

4.3.1 О маршрутизации и таблицах маршрутизации

Транспортировка пакетов в IP-сетях осуществляется на основе информации о текущей конфигурации сети, имеющейся у маршрутизаторов и конечных сетевых устройств.

Рациональный маршрут следования пакета выбирается путём анализа данных, содержащихся в *таблицах маршрутизации*. По результатам анализа IP-пакет, принятый маршрутизатором или сформированный в компьютере пользователя, продвигается в направлении узла – получателя сообщения.

Таблицы маршрутизации могут различаться в зависимости от фирмы-производителя и принятой операционной системы, однако в любом случае должны содержать следующую информацию:

- адрес сети назначения с указанием маски;
- сетевой адрес следующего маршрутизатора;
- выходной порт маршрутизатора, на который должен быть подан пакет;
- метрика маршрута, характеризующая меру предпочтения данного

маршрута в соответствии с заданным критерием⁵.

В зависимости от способа ввода информации в таблицу маршрутизации различают статическую и динамическую маршрутизацию.

При *статической* маршрутизации все записи в таблице имеют неизменный, статический характер и вносятся администратором сети.

При *динамической* маршрутизации все данные вносятся в таблицы маршрутизации с помощью специальных сетевых протоколов. Протоколы маршрутизации позволяют собирать информацию о топологии связей в сети и оперативно вносить в таблицы данные об изменениях связей, возникающих в сети. Результатом работы протоколов является согласование содержания таблиц маршрутизации у взаимодействующих маршрутизаторов.

4.3.2 Статическая маршрутизация

Статическая маршрутизация – вид маршрутизации, при котором записи в таблице маршрутизации создаются и удаляются вручную сетевым администратором.

Содержание записей таблиц маршрутизации различается в зависимости от размещения сети назначения и требований конкретных пользователей. Так, в маршрутах к сетям, непосредственно подключённым к портам данного маршрутизатора, указывается адрес выходного порта и отсутствуют ссылки на какой-либо другой маршрутизатор.

Для отдельного пользователя возможно назначение специфического маршрута, отличающегося от типового маршрута к данной сети; при этом в таблицу заносится полный IP-адрес узла назначения.

Пакеты, адресованные пользователям сетей, данные о которых отсутствуют в графе «сеть назначения», направляются к одному из соседних маршрутизаторов, через который обеспечивается доступ к этим сетям. Такой маршрутизатор называется *маршрутизатором по умолчанию*.

Все записи в таблице имеют статус «статических» с условно бесконечным сроком действия. При возникновении изменений в сети администратор должен оперативно скорректировать таблицы маршрутизации для тех маршрутизаторов, у которых произошедшие изменения требуют смены маршрутов следования пакетов.

Статическая маршрутизация осуществляется администратором сети без участия каких-либо протоколов маршрутизации и обычно применяется в сетях с простой топологией, объединяющих небольшое (1-3) число подсетей и имеющих доступ к сети Интернет через шлюз, являющийся шлюзом по умолчанию.

Статическая маршрутизируемая среда может применяться для:

⁵ Наиболее часто применяется критерий, учитывающий количество промежуточных маршрутизаторов (хопов) в данном маршруте. Кроме того, используются метрики, соответствующие признакам В, Т и R в поле сервиса IP-пакета (В – пропускная способность, Т – вносимая задержка, R – надёжность маршрута).

- сети малого предприятия;
- сети домашнего офиса;
- филиала с одной сетью.

Достоинства статической маршрутизации:

- простота отладки и конфигурирования в малых компьютерных сетях;
- экономия аппаратных ресурсов маршрутизатора;
- отсутствие динамической нагрузки на сеть.

Основным *недостатком* статической маршрутизации является чувствительность к повреждениям линий связи. Если маршрутизатор выходит из строя или канал связи становится недоступным, маршрутизатор не реагирует на неисправность, статический маршрут остаётся активным, при этом другие маршрутизаторы в сети будут продолжать передавать данные по недоступному маршруту.

В малых сетях (например, с тремя локальными сетями, соединёнными между собой маршрутизаторами) подобные ситуации могут оперативно решаться администратором. Однако при масштабировании сети существенно возрастает трудоёмкость коррекции таблиц маршрутизации. Поэтому в крупных сетях более предпочтительным оказывается использование специальных динамических протоколов маршрутизации.

Маршруты статической маршрутизации вводятся командой **ip route**.

Задание порта по умолчанию производится командой **ip route 0.0.0.0 0.0.0.0 interface/next hop ip address**.

Просмотр текущего состояния таблицы маршрутизации осуществляется при помощи команды **show ip route**.

Данные таблиц статической и динамической маршрутизации объединяются в одной таблице, в которую попадают лучшие из сформированных маршрутов.

4.3.3 Основы конфигурации сетевых интерфейсов маршрутизатора

Настройка Ethernet-интерфейсов на маршрутизаторе в целом не отличается от настроек интерфейсов для коммутатора. Единственное – на каждый интерфейс необходимо прописать адрес и маску сетевого соединения, в котором участвует маршрутизатор. Это реализуется с использованием команды **ip address ip_host mask**. Ниже приведён пример настройки для интерфейса FastEthernet 0/0 на маршрутизаторе R1:

```
R1(config)#interface fa0/0
R1(config-if)#description connection to PC1
R1(config-if)#ip address 172.16.1.17 255.255.255.240
R1(config-if)#no shutdown
```

Внимание! В отличие от коммутаторов все интерфейсы маршрутизаторов по умолчанию выключены, поэтому после проведения соответствующих

ющих настроек на интерфейсе его включают с помощью команды **shutdown**.

Для соединения маршрутизаторов между собой могут применяться отличные от Ethernet технологии. Так, например, маршрутизаторы Cisco 2901 ISR могут дополнительно доукомплектовываться платами расширения, которые поддерживают протокол V.35 и снабжаются серийными интерфейсами (рисунок 4.1). Данная технология с серийными интерфейсами применяется для организации глобальных сетей типа WAN. В настройках данных интерфейсов имеются отличия от уже известных Fast Ethernet. Так, например, на серийном интерфейсе S0/0/0 можно задать скорость канала в битах. Скорость задаётся на интерфейсе только с одной стороны канала связи, на DCE-устройстве (Data Circuit-terminating Equipment – аппаратура передачи данных). DCE-устройство конвертирует сигналы от DTE (Data Terminal Equipment – оконечное оборудование данных) и преобразует их в форму, приемлемую для передачи по линии WAN.

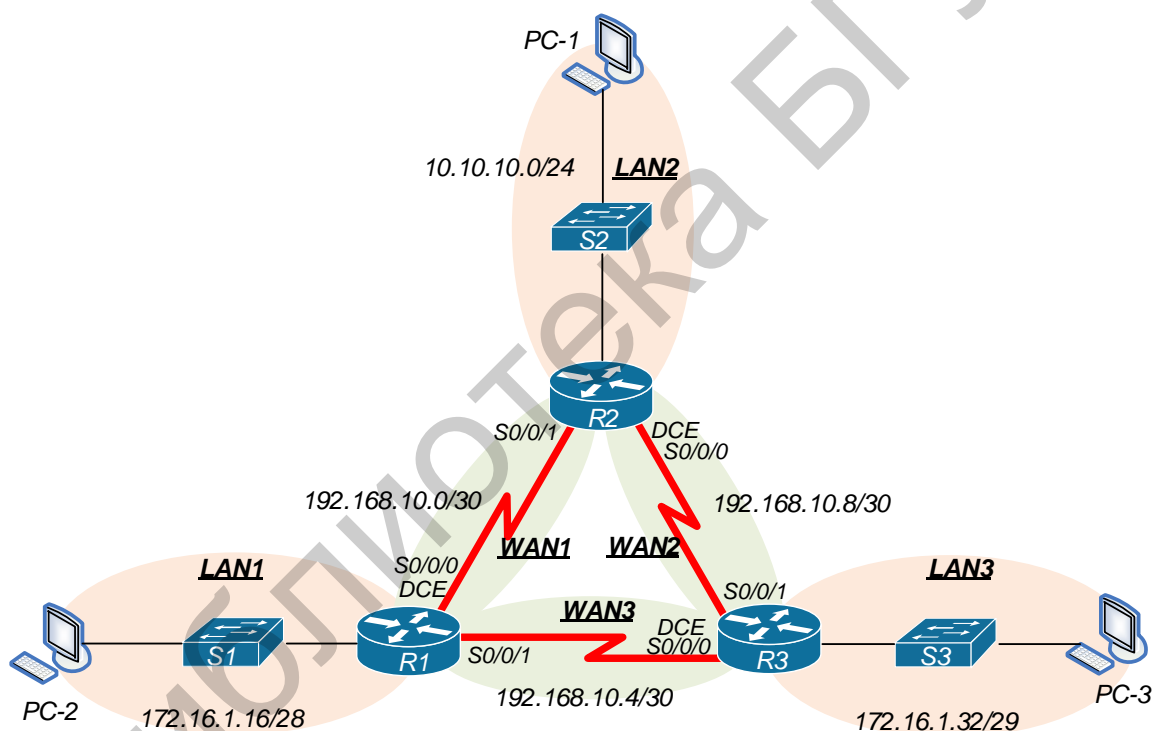


Рисунок 4.1 – Сетевая структура с тремя локальными сетями, объединёнными маршрутизаторами

Поэтому, чтобы произвести настройку серийного интерфейса, необходимо узнать тип устройства на каждой стороне. Эту информацию можно получить при помощи команды **show controllers serial**. В примере ниже вывод команды сильно сокращён. Интересующая нас информация находится в начале:

```
R1#show controllers serial 0/0/0
Interface Serial0/0/0
```

```
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 2000000
idb at 0x81081AC4, driver data structure at 0x81084AC0
<вывод команды сокращён >
```

По выводу данной команды определяем, что интерфейс **serial 0/0/0** включается в маршрутизатор, как в DCE-устройство.

Следующим шагом является настройка интерфейса на маршрутизаторах (предполагается, что R1 – DCE, R2 – DTE):

```
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.252
R1(config-if)#clock rate 2000000
R1(config-if)#no shutdown
```

```
R2(config)#interface serial 0/0/1
R2(config-if)#ip address 192.168.10.2 255.255.255.252
R2(config-if)#no shutdown
```

Внимание! Команда **clock rate** доступна только со стороны DCE-устройства, задающего тактовую частоту работы приёмопередатчиков на линии связи между маршрутизаторами.

Для проверки доступности соседних маршрутизаторов, имеющих непосредственное подключение друг к другу, можно использовать уже известную команду **ping**:

```
R2 #ping 192.168.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 21/21/22 ms
```

Либо применив проприетарный протокол Cisco CDP (от англ. Cisco Discovery Protocol), пример использования приведен ниже:

```
R1#show cdp neighbors
```

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

DeviceID	Local Intrfce	Holdtime	Capability	Platform	Port ID
R2	Ser 0/0/0	178	R	C2900	Ser 0/0/1

```
R1#
```

Выделенная строка говорит о том, что к маршрутизатору R1 подключено сетевое устройство с именем хоста R2 через локальный интерфейс Serial 0/0/0. Столбец *Holdtime* оповещает о времени обновления записей (счётчик). В столбце *Capability* можно узнать о типе устройства (S – соответствует коммутатору, R – маршрутизатору). В нашем случае это устройство – маршрутизатор, на базе платформы C2900 (столбец *Platform*), который подключён через удалённый интерфейс Serial 0/0/1 (столбец *Port ID*).

4.3.4 Настройка статической маршрутизации на маршрутизаторах Cisco

Для продвижения пакетов из одной сети в другую маршрутизаторам необходимо знать, куда направлять входящие пакеты. Один из вариантов данного продвижения – статическая маршрутизация. В оборудовании компании Cisco добавление статических маршрутов осуществляется в режиме глобальной конфигурации. Команда имеет следующий синтаксис:

```
ip route destination_ip_network_address mask {interface/next hop ip address} {metric}
```

Здесь *destination_ip_network_address* – ip-адрес сети назначения; *mask* – маска сети назначения; *interface/next hop ip address* – выходной интерфейс текущего маршрутизатора или ip-адрес следующего маршрутизатора, соответственно; *metric* – метрика или приоритет маршрута (при существовании одинаковых маршрутов до одной и той же сети выбирается маршрут с меньшей метрикой). По умолчанию используется значение метрики, равное 1, и не является обязательным параметром.

Так, для того чтобы на маршрутизаторе R1 добавить маршрут до локальной сети LAN_2, в режиме глобальной конфигурации выполните команду:

```
R1(config)#ip route 10.10.10.0 255.255.255.0 192.168.10.2
```

Чтобы просмотреть текущую таблицу маршрутизации, выполните в привилегированном режиме команду **show ip route**:

```
R1#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
10.0.0.0/24 is subnetted, 1 subnets
```

```
S 10.10.10.0 [1/0] via 172.16.1.17
```

```
172.16.0.0/28 is subnetted, 1 subnets
```

```
C 172.16.1.16 is directly connected, FastEthernet0/0
```

```
192.168.10.0/30 is subnetted, 2 subnets
```

```
C 192.168.10.0 is directly connected, Serial0/0/0
```

```
C 192.168.10.4 is directly connected, Serial0/0/1
```

В выводе команды символом **C** отмечены сети, непосредственно подключённые к маршрутизатору, символ **S** используется для обозначения статических маршрутов. Расшифровка символов приводится в самом начале вывода команды.

Обратите внимание, что интерфейс **fa0/0** маршрутизатора R1 имеет адрес, принадлежащий сети LAN1, интерфейс **Serial0/0/0** относится к сети WAN1, а

Serial0/0/1 – к сети WAN3. Поэтому маршрутизатор изначально знает о существовании этих сетей, что и промаркировано в таблице маршрутизации символом **C**. Поэтому сети LAN1, WAN1, WAN3 для маршрутизатора R1 прописывать не нужно.

Настройка статических маршрутов на маршрутизаторе R1 заключается в добавлении всех сетей, к которым маршрутизатор не подключён (LAN2, LAN3 и WAN2). Правильность указания статических маршрутов можно изучить с помощью команды **show ip route**.

Внимание! Важной особенностью настройки статической маршрутизации является тот факт, что необходимо настраивать маршруты в двух направлениях. Это необходимо для того, чтобы передаваемые пакеты достигали узла назначения, а пакеты от узла назначения могли вернуться к узлу-источнику.

Статическая маршрутизация, помимо своих преимуществ – простоты настройки и отсутствия вычислительной нагрузки на ЦП, имеет один очень важный недостаток – неспособность автоматически реагировать на изменения топологии, происходящие в результате сбоя или модернизации сети.

Для удаления старых статических маршрутов необходимо использовать команду **no ip route**, например:

```
R1(config)#no ip route 172.16.1.32 255.255.255.248 192.168.10.6
```

Одним из способов повышения отказоустойчивости сети является задание альтернативных маршрутов. В основе этого метода лежит использование параметра **metric** в команде **ip route static**. На каждом маршрутизаторе можно продублировать все существующие маршруты, заменив на них **next hop** ip-адресом интерфейса другого маршрутизатора и указав **metric**, равный двум. Ниже приведен пример для R1 для сети LAN_2 (10.10.10.0/24):

```
R1#show running-config
```

```
Building configuration...
```

```
< вывод команды сокращён >
```

```
ip classless
```

```
ip route 10.10.10.0 255.255.255.0 192.168.10.2
```

```
< вывод команды сокращён >
```

```
Запись альтернативного маршрута через шлюз R3:
```

```
R1(config)#ip route 10.10.10.0 255.255.255.0 192.168.10.6 2
```

```
В этом случае при просмотре таблицы маршрутизации:
```

```
R1#show ip route
```

```
< вывод команды сокращён >
```

```
10.0.0.0/24 is subnetted, 1 subnets
```

```
S    10.10.10.0 [1/0] via 192.168.10.2
```

```
172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
```

```
C    172.16.1.16/28 is directly connected, FastEthernet0/0
```

```
S    172.16.1.32/28 [1/0] via 192.168.10.6
```

```
S    172.16.1.32/29 [1/0] via 192.168.10.6
```

```
192.168.10.0/30 is subnetted, 3 subnets
C    192.168.10.0 is directly connected, Serial0/0/0
C    192.168.10.4 is directly connected, Serial0/0/1
S    192.168.10.8 [1/0] via 192.168.10.2
```

Обратите внимание, что в таблице маршрутизации новые маршруты отсутствуют, т. к. их метрика меньше маршрутов, созданных раньше.

4.3.5 Формирование маршрута «по умолчанию»

Часто возникают ситуации, когда указанный в пакете адрес сети назначения отсутствует в зафиксированных маршрутах. В этом случае пакеты направляются на интерфейс соседнего маршрутизатора, имеющего выходы в общую сеть. Для этого формируется так называемый маршрут «по умолчанию». Синтаксис такой команды:

```
ip route 0.0.0.0 0.0.0.0 {interface/ next hop ip address}
```

В маршруте «по умолчанию» ip-адрес сети назначения указан как 0.0.0.0 и маска сети назначения как 0.0.0.0.

Пример команды: **ip route 0.0.0.0 0.0.0.0 192.168.10.1**

Команда означает, что все пакеты, имеющие неизвестные адреса назначения, следует отправлять на адрес 192.168.10.1.

В случае наличия нескольких маршрутов со статической маршрутизацией выбирается более специфичный, т. е. тот, в котором указана более точно сеть назначения. Таким образом, получается, что маршрут по умолчанию имеет самый низкий приоритет. Это удобно, т. к. позволяет значительно сократить количество записей в таблице маршрутизации: можно создавать только те маршруты, у которых next-hop отличается от маршрута «по умолчанию».

При просмотре таблицы маршрутизации маршрут по умолчанию будет отмечаться звездочкой (*).

Статические маршруты по умолчанию используются в следующих случаях:

- при отсутствии других маршрутов в таблице маршрутизации, совпадающих с IP-адресом назначения пакета, иными словами, при отсутствии более точного совпадения (статические маршруты часто используются при подключении пограничного маршрутизатора компании к сети интернет-провайдера);
- если маршрутизатор подключён только к одному маршрутизатору, в таком случае используется термин «тупиковый маршрутизатор».

4.3.6 Суммарный статический маршрут

Для уменьшения числа записей в таблице маршрутизации можно объединить несколько статических маршрутов в один статический маршрут. Это возможно при следующих условиях:

– сети назначения являются смежными и могут быть объединены в один сетевой адрес;

– все статические маршруты используют один и тот же выходной интерфейс или один IP-адрес следующего перехода.

Как видно из рисунка 4.2, маршрутизатору R1 требуется четыре отдельных статических маршрута для подключения к сетям в диапазоне 172.20.0.0/16 – 172.23.0.0/16. Вместо этого можно настроить один суммарный статический маршрут 172.20.0.0/14, который будет обеспечивать подключение к этим сетям.

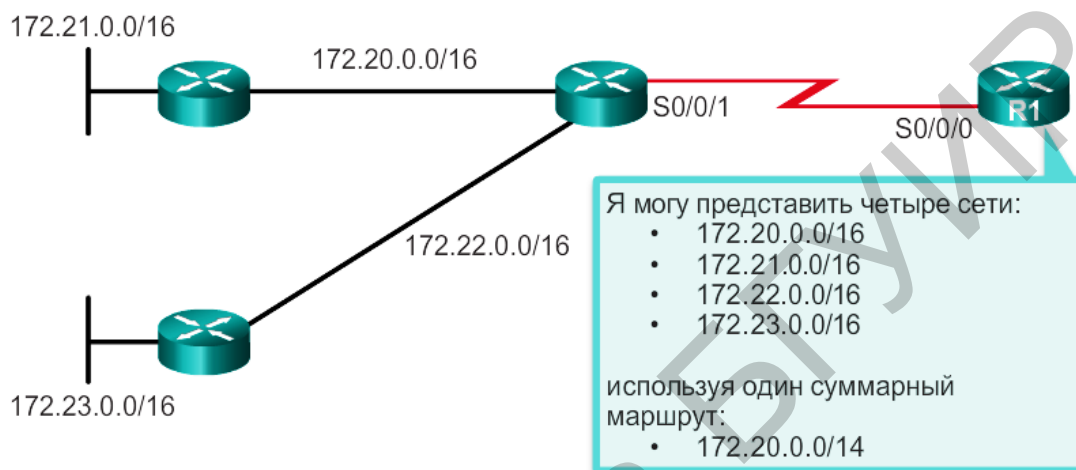


Рисунок 4.2 – Использование суммарного статического маршрута

Объединение сетей в один адрес и маску можно выполнить в три этапа:

- записать сети в двоичном формате;
- подсчитать количество крайних слева совпадающих битов для определения маски суммарного маршрута;
- скопировать совпадающие биты и дополнить их нулевыми битами для определения суммарного сетевого адреса.

После определения суммарного маршрута следует заменить существующие маршруты одним суммарным маршрутом.

4.4 ОПИСАНИЕ ЛАБОРАТОРНОГО СТЕНДА

Работа выполняется бригадами из трёх-четырёх человек. В процессе выполнения работы каждой бригаде выделяется комплект сетевого оборудования, который включает в себя коммутатор Cisco Catalyst 2960 и маршрутизатор Cisco 2901 ISR. Для подключения к устройствам необходимо произвести коммутацию на соответствующих патчпанелях и сетевых розетках. Для выполнения работы также понадобится программное обеспечение для терминального доступа (например, PuTTY), а также приложение для эмуляции файлового сервера (например, TFTP32).

Внимание! Для подключения компьютеров к Ethernet-портам коммутатора используйте второй «УЧЕБНЫЙ» порт сетевой розетки (см. рисунок 1.5) и не забывайте при этом производить соответствующие коммутации на патчпанели №2 и коммутаторе. Порядок подключения к консольным портам оборудования описан в лабораторной работе №1.

В данной работе предусматривается изучение следующей топологии сети (рисунок 4.3).

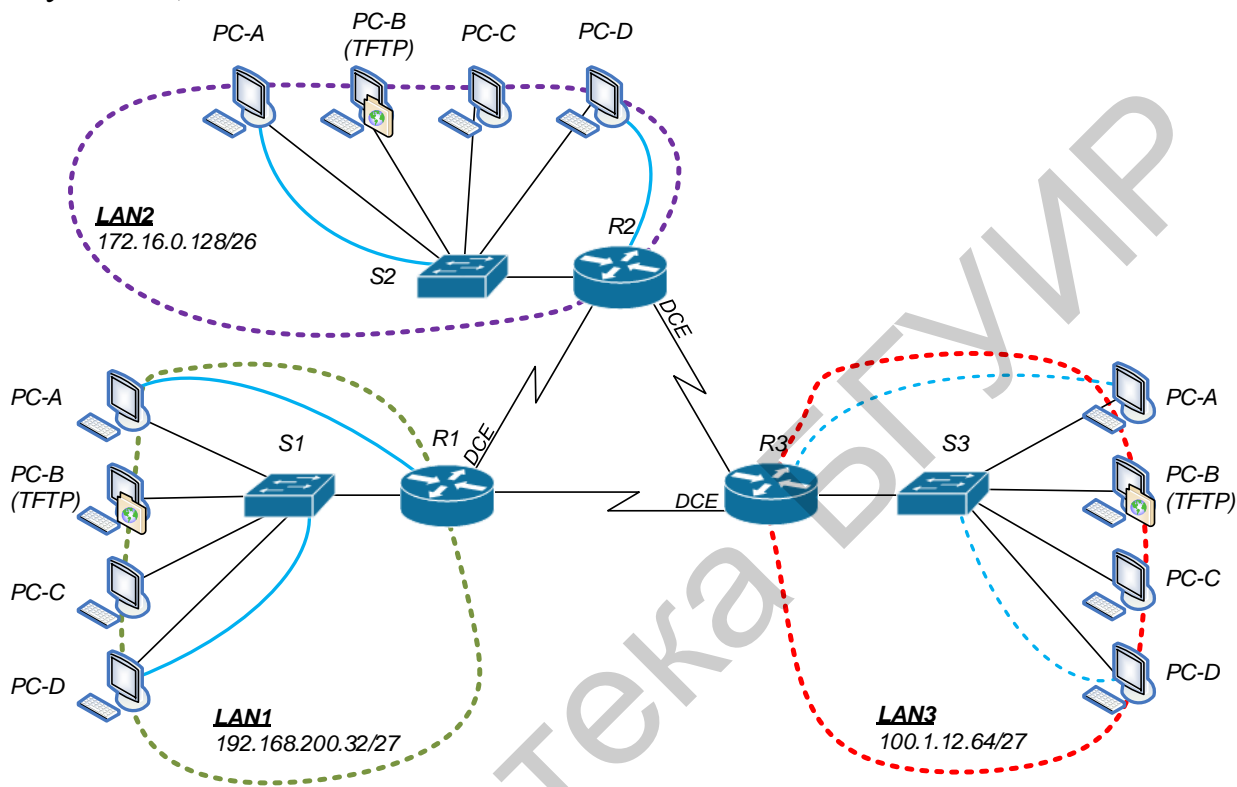


Рисунок 4.3 – Схема взаимодействия оборудования

4.5 ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

4.5.1 Исследование изучаемой топологии

4.5.1.1 Соберите вышеприведенную схему с учетом того, что к одному из интерфейсов маршрутизатора будет подключён коммутатор. Каждый коммутатор образует самостоятельный сегмент локальной сети (LAN). Каждой LAN (бригаде) для сетевых устройств выделяются следующие подсети:

- LAN1 – 192.168.200.32/27;
- LAN2 – 172.16.0.128/26;
- LAN3 – 100.1.12.64/27.

4.5.1.2 Осуществите распределение адресов в соответствующих LAN следующим образом: первые четыре адреса назначить соответствующим компьютерам из LAN, предпоследний адрес использовать для удалённого управления

коммутатором, последний доступный адрес использовать для интерфейса маршрутизатора, который соединяет маршрутизатор с коммутатором.

4.5.1.3 Подключите компьютеры к соответствующим консольным линиям сетевых устройств.

4.5.1.4 Все компьютеры PC-B в своих сегментах сетей будут являться локальными TFTP-серверами.

4.5.2 Базовая настройка коммутатора и маршрутизатора

Выполнение базовой настройки предполагает выполнение следующих действий:

- назначьте имя устройству в соответствии с топологией;
- доступ к привилегированному режиму по паролю **ciscoenapa**;
- доступ по консольному кабелю по паролю **ciscocon**;
- доступ через vty по паролю **ciscovty**;
- все пароли должны храниться в зашифрованном виде;
- настройте актуальное время на коммутаторах и маршрутизаторах;
- отключите поиск DNS;
- обеспечьте синхронизацию командной строки и вывода информации на линии управления;
- на всех сетевых устройствах сконфигурируйте сообщение дня **“Unauthorized access strictly prohibited and prosecuted to the full extent of the law!”**;
- отдельно для коммутатора настройте SVI в VLAN 99 и пропишите шлюз по умолчанию.

4.5.3 Дополнительная настройка параметров на маршрутизаторе, проверка таблицы маршрутизации, проверка соединений с другими LAN

4.5.3.1 Настройте все интерфейсы на маршрутизаторах согласно их сетям. Определите протоколом CDP интерфейсы подключения. Отключите протокол CDP. Для адресации сетей между маршрутизаторами используйте диапазон 192.168.0.0/24. Разбейте этот диапазон на подсети с необходимым количеством хостов в каждой.

4.5.3.2 Настройте описание всех интерфейсов.

4.5.3.3 На всех маршрутизаторах настройте статическую маршрутизацию.

4.5.3.4 Произведите анализ таблиц маршрутизации.

4.5.3.5 Проверьте доступ к удалённым LAN с помощью эхо-запроса.

4.5.3.6 По возможности оптимизируйте таблицы маршрутизации.

4.5.3.7 Предусмотрите вариант резервных путей доступа к другим LAN при падении одной из линий, соединяющих маршрутизаторы между собой.

4.5.3.8 Поэкспериментируйте с программным отключением одного из WAN-интерфейсов на произвольном маршрутизаторе. Проверьте доступность удаленных LAN с помощью эхо-запроса.

4.5.3.9 Произведите анализ таблиц маршрутизации при падении линий.

4.5.3.10 Сохраните все файлы конфигурации сетевых устройств в своем сегменте на TFTP-сервере, при этом для доступа к файлу конфигурации коммутатора используйте организованное Telnet-соединение.

4.5.4 Завершающие этапы настройки сетевых устройств

После проверки выполнения лабораторной работы удалите все сохранённые файлы **startup-config**. Перезапустите устройства. Убедитесь, что файл конфигурации был удалён и устройства находятся в стартовом режиме (Setup Mode).

4.6 СОДЕРЖАНИЕ ОТЧЁТА

4.6.1 Цель работы.

4.6.2 Расчёт сетевых диапазонов для соответствующих локальных сетей (бригад): адрес сети, маски подсети, широковещательный адрес, доступный диапазон адресов для хостов, адресов, предназначенных для компьютеров, IP-адрес для доступа к коммутатору по SVI, адрес шлюза по умолчанию.

4.6.3 Расчёт сетевых диапазонов для соединений между маршрутизаторами.

4.6.4 Схема изучаемой сетевой топологии с указанием IP-адресов всех сетевых устройств и соединений между ними.

4.6.5 Приведите всю конфигурацию из IOS CLI на коммутаторе и маршрутизаторе, а также всю информацию о содержании таблицы маршрутизации на маршрутизаторе.

4.6.6 Выводы по работе.

4.7 КОНТРОЛЬНЫЕ ВОПРОСЫ

4.7.1 Дайте определение таблице маршрутизации. Какую информацию содержит таблица маршрутизации?

4.7.2 Дайте определение статической маршрутизации. В чём отличие статической маршрутизации от динамической? В каких случаях рекомендуется применять статическую маршрутизацию?

4.7.3 Где хранятся записи статических и динамических маршрутов, каковы особенности маркировки данных записей? Назовите достоинства и недостатки статической маршрутизации.

4.7.4 В чём заключаются основные отличия настройки интерфейсов на маршрутизаторе по сравнению с коммутатором? Каковы особенности конфигурации интерфейсов WAN?

4.7.5 С помощью каких команд можно настроить статические маршруты на маршрутизаторе Cisco? С помощью каких команд в IOS можно осуществить просмотр таблицы маршрутизации?

4.7.6 Какой указатель в таблице маршрутизации соответствует: а) непосредственно присоединенной сети; б) статическому маршруту к удаленной сети?

4.7.7 С какой целью применяется маршрут «по умолчанию»? В чём заключается особенность конфигурации статического маршрута «по умолчанию»?

4.7.8 Каким образом можно осуществить оптимизацию таблицы маршрутизации, которая содержит статические маршруты? Расскажите о процедуре суммирования (объединения) статических маршрутов.

4.7.9 Определите суммарный маршрут, если в таблице маршрутизации даны следующие записи (для всех сетей маска – /24):

```
S 172.16.0.0 [1/0] via 192.168.1.2
S 172.16.1.0 [1/0] via 192.168.1.2
S 172.16.2.0 [1/0] via 192.168.1.2
S 172.16.3.0 [1/0] via 192.168.1.2.
```

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Цикл методических материалов и контрольно-обучающих программ сетевой академии Cisco Systems [Электронный ресурс]. – 2016. – Режим доступа : <http://netacad.com/>.

2 Компьютерные сети / В. Г. Олифер [и др.]. – 4-е изд. – СПб. : ПИТЕР, 2012.

3 Димарцио, Д. Ф. Маршрутизаторы Cisco. Пособие для самостоятельного изучения / Д. Ф. Димарцио. – СПб. : Символ-Плюс, 2003. – 512 с.

4 Хабракен, Джо. Как работать с маршрутизаторами Cisco / Джо Хабракен ; пер. с англ. – М. : ДМК Пресс, 2005.

5 Интернет-ресурс linkmeup. Сети для самых маленьких. Часть третья. Статическая маршрутизация [Электронный ресурс]. – 2013. – Режим доступа : <http://linkmeup.ru/blog/14.html>.

ПРИЛОЖЕНИЕ А (обязательное)

Классификация сетевых устройств распределения информации

Устройства, применяемые в компьютерных сетях, принято классифицировать по ряду признаков.

А.1 По уровню обработки информации в терминологии модели взаимодействия открытых систем (ВОС) можно выделить:

– устройства первого физического уровня (L1) – предназначены для формирования, усиления и регенерации сигналов, передаваемых между узлами сети;

– устройства второго канального уровня (L2) – предназначены для управления потоком информации, поступающей на порты оборудования с её последующим распределением между портами в соответствии с адресной информацией физического уровня;

– устройства третьего сетевого уровня (L3) – предназначены для маршрутизации данных между компьютерными сетями в соответствии с метриками и адресной информацией логического уровня;

– устройства более высоких уровней⁶ с четвертого по седьмой (L4-L7) – предназначены для осуществления соответствующих функций транспортного, сеансового, представления и прикладного уровней модели ВОС.

На рисунке А.1 приведён пример классификации некоторых сетевых устройств по модели ВОС. Подробное описание приведённых устройств дано в таблице А.1.

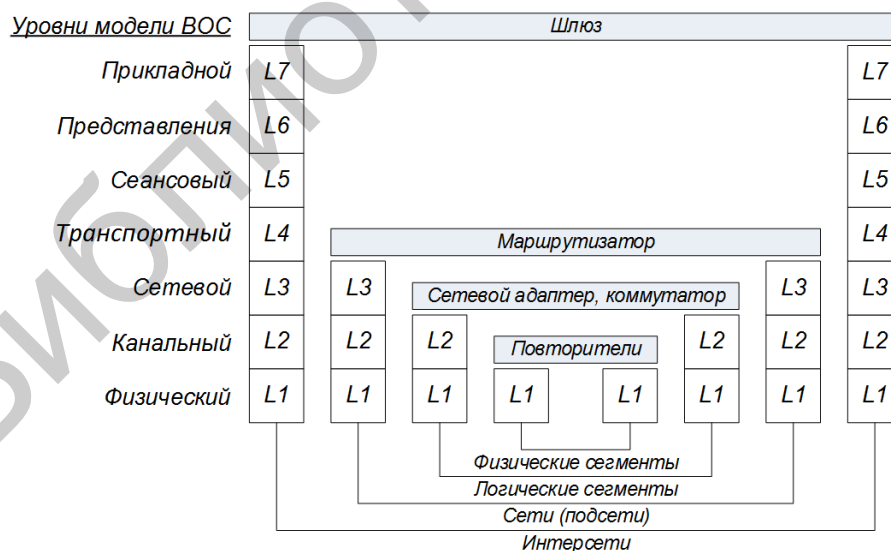


Рисунок А.1 – Соответствие функций сетевых устройств модели ВОС

⁶ Как правило, это обычные оконечные устройства, такие как компьютеры, планшеты, принтеры и др., или специфические устройства, наподобие шлюзов, межсетевых экранов, шифраторов потоков данных и пр.

А.2 По области применения устройства:

1) *Оконечные устройства пользователя.* В эту группу входят компьютеры, планшеты, принтеры, сканеры и другие устройства, которые выполняют функции, необходимые непосредственно пользователю сети.

2) *Сетевые устройства.* Эти устройства позволяют осуществлять связь с другими сетевыми устройствами или устройствами конечного пользователя. В сети они выполняют распределительные или иные специфические функции.

А.3 По масштабам построения сетей с помощью сетевых устройств:

1) Локальная (LAN – Local Area Network) и кампусная (CAN – Campus Area Network) – сеть передачи данных, охватывающая ограниченную территорию, обычно в пределах здания(й) и использующая короткие линии связи между узлами сети (до 1...2 км).

2) Городская сеть мегаполиса (MAN – Metropolitan Area Network) – предназначена для обслуживания территорий крупных городов или регионов.

3) Глобальная, или территориальная (WAN – Wide Area Network) – территориально распределенная сеть, которая охватывает значительное географическое пространство, не имеет единой сетевой архитектуры. На рисунке А.2 приведён пример обобщённой структуры сети Интернет.

А.4 В зависимости от используемых способов коммутации:

1) С коммутацией каналов – использует способ организации связи без буферизации данных, когда при необходимости обмена информацией между узлами сети устанавливается физическое соединение на всё время сеанса связи до тех пор, пока соединение не будет разомкнуто.

2) С коммутацией сообщений – здесь пересылка сообщений осуществляется без нарушения их целостности по виртуальному каналу без создания физического соединения между конечными устройствами.

3) С коммутацией пакетов – использует передачу пакетов с буферизацией данных. Сообщение разбивается на пакеты и передается по каналу. Канал передачи данных занят только на время передачи пакета. Обеспечивает эффективную передачу неравномерного трафика.

А.5 По потреблению электроэнергии выделяют:

1) Активное сетевое устройство – это средство, которое содержит электронные или оптические схемы и получающее питание от электрической сети или других источников питания. Как правило, активные устройства сопровождаются операционной системой, которая предназначена для управления и контроля состояний основных функций устройства.

2) Пассивное сетевое устройство – это средство, не получающее питание от электрической сети или других источников и выполняющее функции распределения или снижения уровня сигналов. Например, кабельная система: кабель (коаксиальный и витая пара), вилка/розетка (RJ45, RS232), патчпанель, оргайзер и т. д.

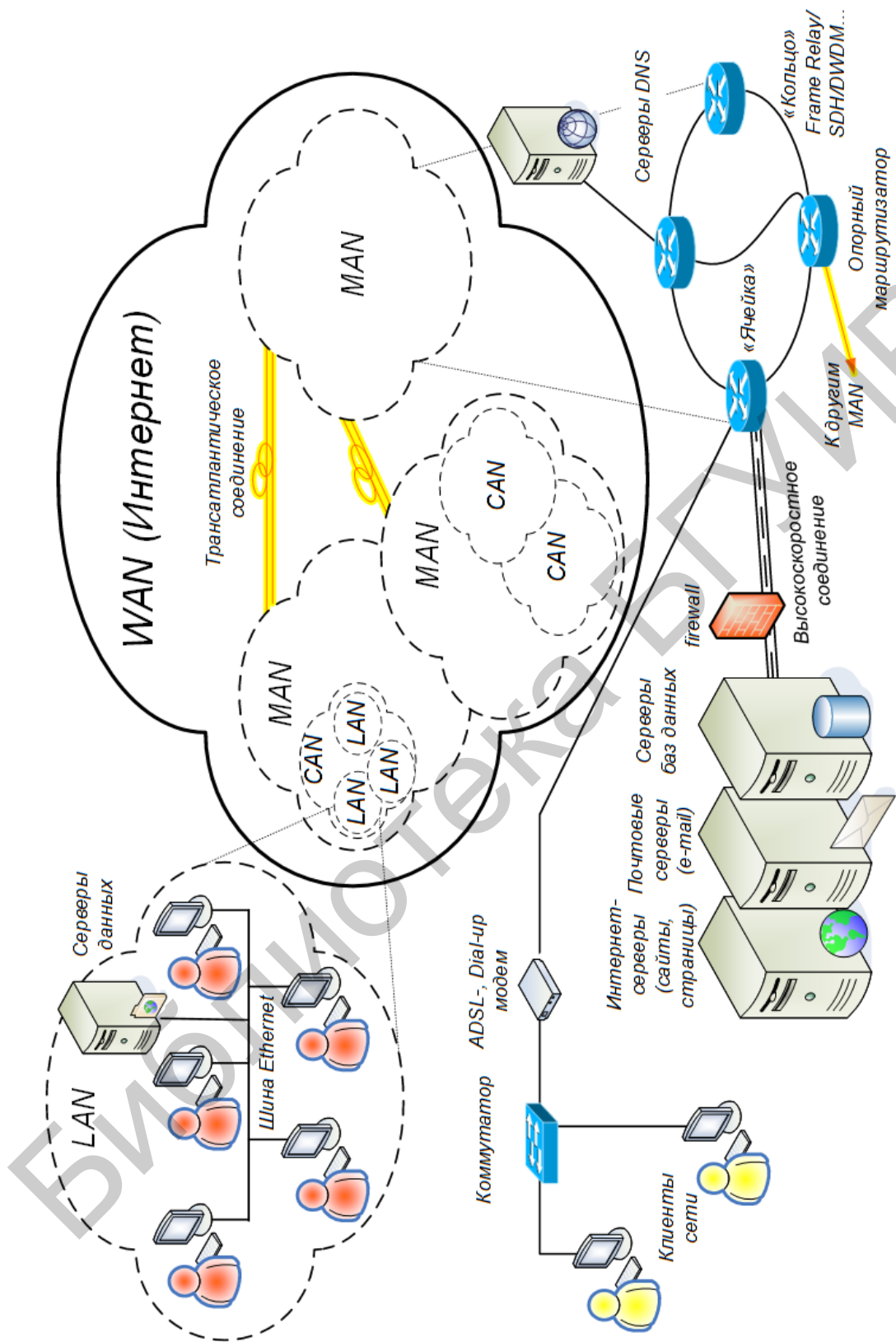


Рисунок А.2 – Обобщённая структура сети Интернет

Таблица А.1 – Классификация сетевых устройств

Устройство	Уровень модели ВОС	По масштабам сети	Назначение
1 Концентратор (hub)	L1	LAN, CAN	Предназначен для ретрансляции сигналов с одного порта на все остальные
2 Модем (modem)	L1	LAN	Предназначен для согласования параметров линии с направляющей средой, зависит от протокола реализации (Dial-up, xDSL, PON, др.)
3 Коммутатор (switch)	L2	LAN, CAN, MAN	Предназначен для коммутации кадров между активными портами в малых сетях, сетях предприятий, транспортных сетях
4 Сетевой адаптер (NIC)	L2	LAN	Предназначен для распознавания MAC-адреса сервера, компьютера или другого оконечного устройства пользователя
5 Беспроводная точка доступа (AP wireless)	L2	LAN	Предназначен для организации беспроводного доступа по протоколам 802.11
6 Маршрутизатор (router)	L3	CAN, MAN, WAN	Предназначен для маршрутизации пакетов между сетями, основываясь на данных таблицы маршрутизации, метрик, работает с логическими адресами IP
7 Беспроводной маршрутизатор (wireless router)	L3	LAN, CAN	Предназначен для маршрутизации пакетов между беспроводными сетями
8 Межсетевой экран (firewall – FW)	L4-L7	LAN, CAN, MAN	Предназначен для защиты ресурсов частной сети от несанкционированного доступа пользователей из других сетей
9 Шлюз (gateway – GW)	L7	MAN, WAN	Предназначен для трансляции протоколов, размещается между взаимодействующими сетями и служит посредником, переводящим сообщения в формат другой сети

ПРИЛОЖЕНИЕ Б
(обязательное)
Учебно-лабораторный стенд

Учебно-лабораторный стенд представляет собой шкаф с телекоммуникационным оборудованием, как показано на рисунке Б.1 (вид спереди) и Б.2 (вид сзади).

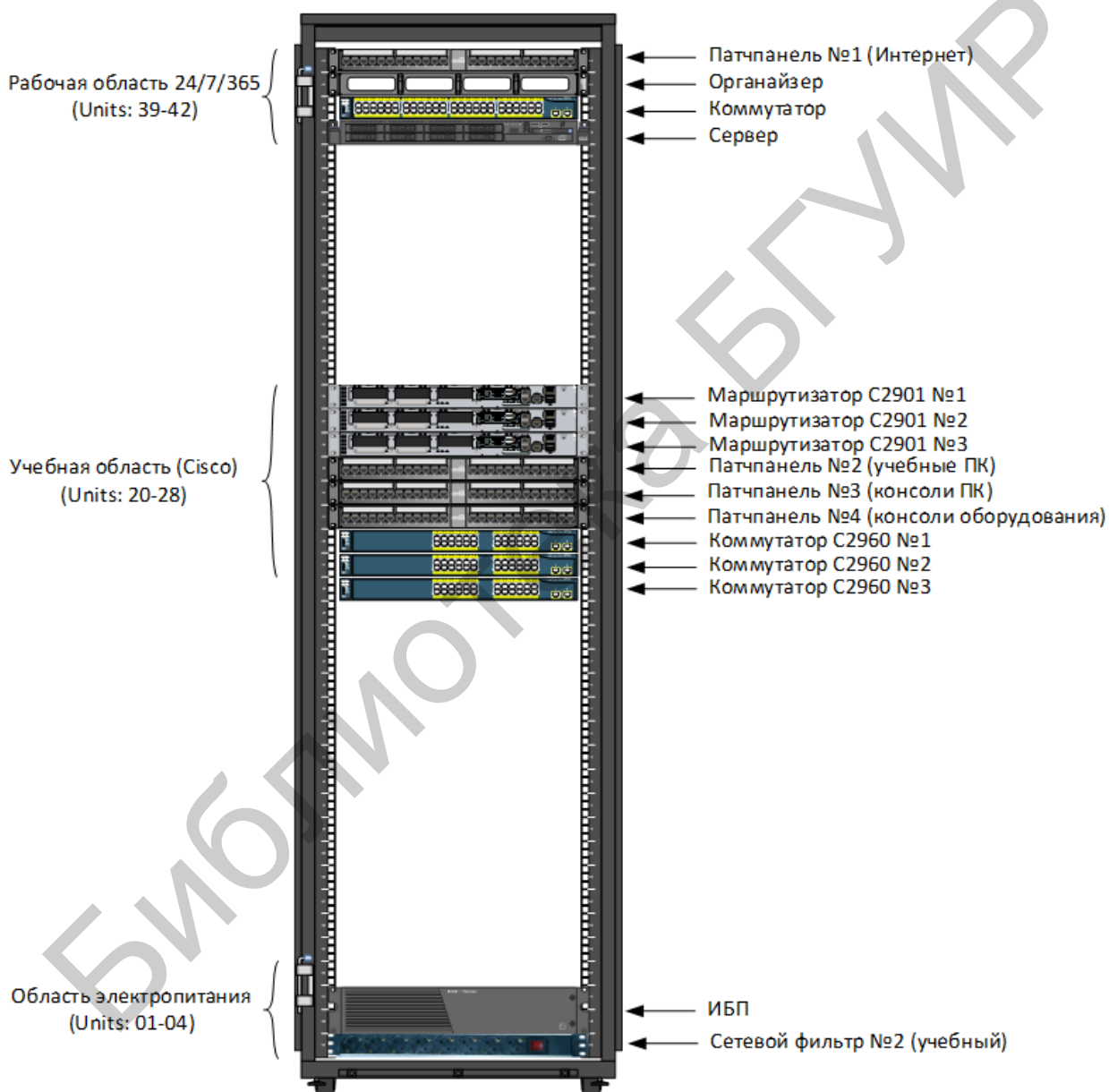


Рисунок Б.1 – Размещение сетевых устройств в телекоммуникационной стойке (вид спереди)

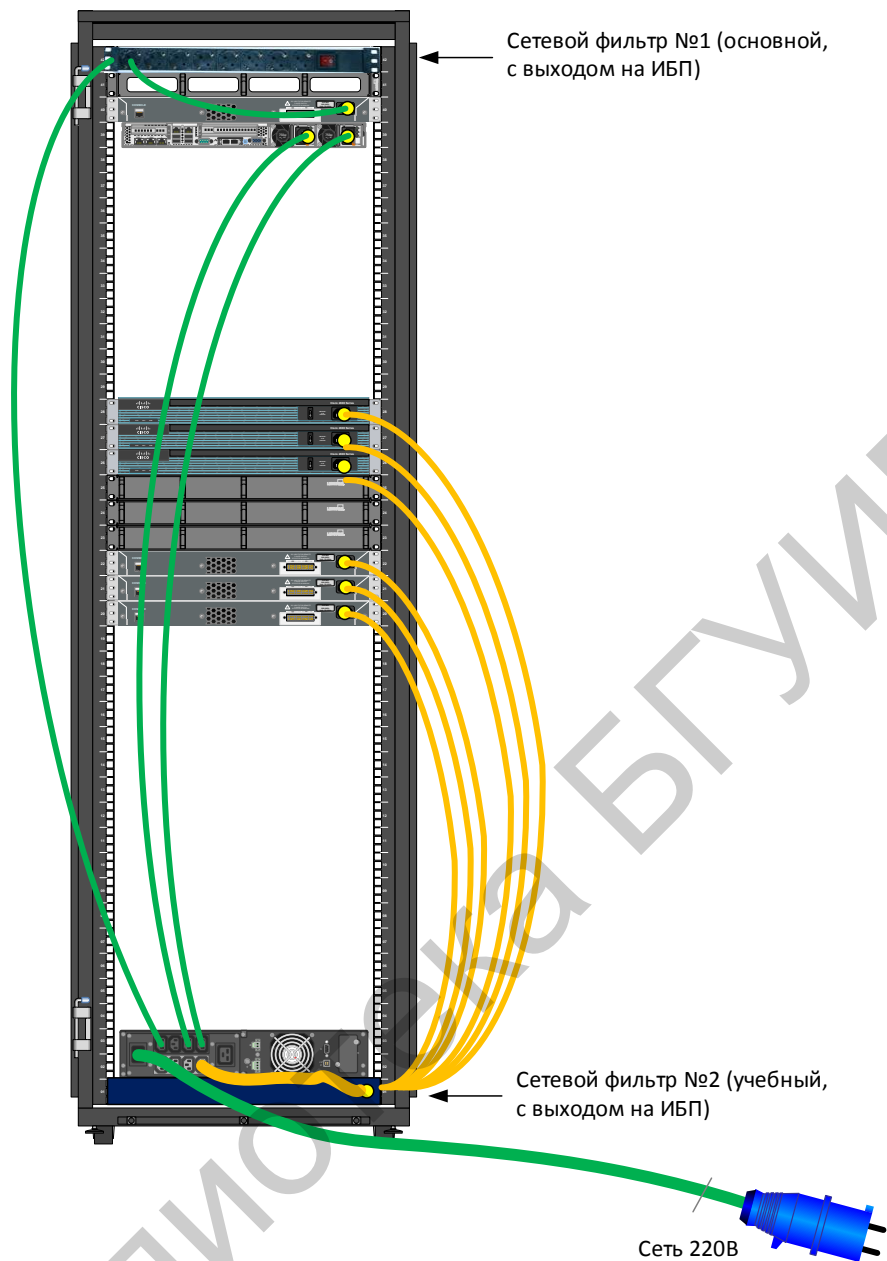


Рисунок Б.2 – Размещение сетевых устройств в телекоммуникационной стойке (вид сзади)

В учебной области шкафа (units 20-28) установлено три коммутатора Cisco Catalyst 2960 series и три маршрутизатора Cisco 2901 Integrated Services Router. Кроме этого, в стойку установлено несколько патчпанелей, позволяющих производить коммутацию как между портами коммутаторов и маршрутизаторов, так и внешним оборудованием, таким, как, например, персональные компьютеры и прочие оконечные устройства.

Коммутатор Catalyst 2960 series относится к управляемым коммутаторам 2 уровня.

Все коммутаторы имеют по 24 порта Ethernet для подключения устройств со скоростью работы 10/100 Мбит/с и два порта со скоростью работы в 1 Гбит/с.

На рисунке Б.3 приведена передняя панель коммутатора Cisco 2960.

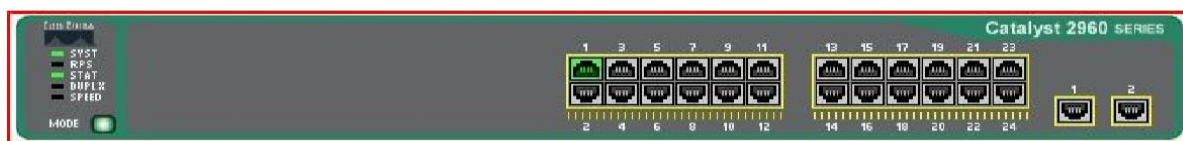


Рисунок Б.3 – Передняя панель коммутатора Catalyst 2960 series

Маршрутизаторы Cisco 2901 ISR относятся к серии маршрутизаторов с интеграцией сервисов, таких, как передача потокового видео, VoIP, система обработки вызовов, средства голосовой почты и прочие, добавленные к телефонии, функции, POE, поддержка беспроводных сетей, ускоренного аппаратного шифрования, функции межсетевое экрана, система предотвращения вторжений и др.

На рисунке Б.4 приведена передняя панель маршрутизатора Cisco 2901 ISR.



Рисунок Б.4 – Передняя панель маршрутизатора Cisco 2901 ISR

Стандартная комплектация маршрутизатора Cisco 2901 ISR содержит два порта со скоростью работы в 1 Гбит/с, 4 слота для сервисных модулей гибкого расширения (EMVIC), консольные RJ-45 и мини-USB порты, порт Aux. Кроме того, содержит два стандартных USB 2.0 порта для различного применения.

В сетевых устройствах Cisco низкого уровня консольный порт представляет собой разъём RJ-45 на задней панели. В сетевых устройствах высокого уровня консольные порты находятся на картах, таких как модуль Supervisor Engine. По умолчанию доступ к консольному порту не предусматривает наличие пароля.

Другим способом подключения к устройству является подключение через вспомогательный (Aux) порт. Процедура подключения аналогична таковой через консольный порт, но позволяет осуществить удалённое подключение при помощи модема. Это означает, что можно позвонить на удаленное сетевое устройство, осуществить изменение и проверку конфигурации, просмотреть статистику использования устройства.

Третьим способом соединения с устройством Cisco является использование программы Telnet. Можно использовать Telnet для соединения с любым активным портом сетевого устройства.

ПРИЛОЖЕНИЕ В

(справочное)

Процедура сброса пароля на сетевых устройствах Cisco

Практически на любом сетевом устройстве есть возможность сбросить пароль, имея физический доступ (консольное соединение).

В.1 Восстановление доступа к маршрутизатору Cisco 2901 ISR

В.1.1 Подключитесь к консольному порту маршрутизатора.

В.1.2 Произведите перезагрузку устройства с помощью команды **#reload**, если это невозможно сделать, то выключите и включите питание сетевого устройства.

В.1.3 Когда на экране побежит строка **#####...###**, означающая загрузку образа операционной системы IOS (40–60 с после включения), необходимо нажать клавиши **Ctrl + C** или **Ctrl + Break**. Этим мы приостановим загрузку маршрутизатора и теперь будем находиться в режиме ROM Monitor (**rommon**). Режим **rommon** по сути является усеченной версией IOS с поддержкой основных команд управления.

В.1.4 В этом режиме введите команду: **confreg 0x2142** – она заставит устройство игнорировать **startup-config** при загрузке.

В.1.5 Введите **reset** для перезагрузки.

В.1.6 После загрузки **running-config** образ системы будет чистым, а **startup-config** содержит по-прежнему последнюю сохранённую конфигурацию. Сейчас самое время поменять пароль или скопировать заранее подготовленный образ в систему.

В.1.7 В конце необходимо вернуть состояние регистров обратно, для этого необходимо изменить регистр на номер **0x2102**. Ниже приведён пример.

Router(config)#**config-register 0x2102**

Если этого не сделать, то вся конфигурация будет актуальна до первой перезагрузки.

В.2 Восстановление доступа к коммутатору Cisco Catalyst 2960

В.2.1 При нажатой кнопке выбора режима (**mode**) на корпусе коммутатора вставьте шнур питания (не отпускать кнопку до тех пор, пока индикатор над портом 1 не будет гореть как минимум 2 с).

В.2.2 Введите команду: **flash_init**.

В.2.3 Введите команду: **delete flash:config.text**.

В.2.4 Продолжите процесс загрузки: **boot**.

При необходимости поменяйте пароль или скопируйте заранее подготовленный образ в систему.

ПРИЛОЖЕНИЕ Г (обязательное) Варианты обжима витой пары

Существует три варианта обжима витой пары: прямой, перекрестный и инверсный. Ниже более подробно рассматривается каждый вариант, а также их применение.

Г.1 Прямой (Straight-through) порядок обжима витой пары. Ниже на рисунке Г.1 представлен вариант прямого кабеля 568В – 568В, существует также вариант 568А – 568А.

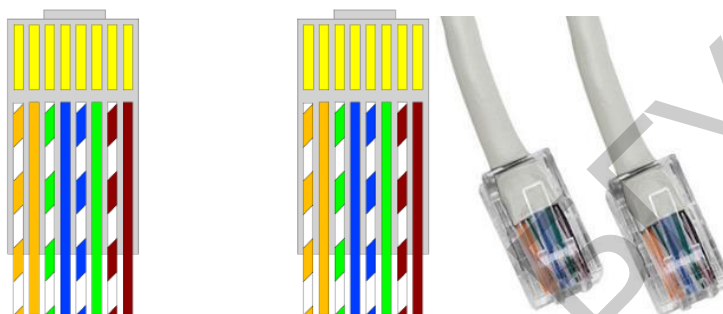


Рисунок Г.1 – Обжим прямого кабеля

Для стандарта Ethernet 100Base-T используются четыре жилы (оранжевая и зеленая пара), а оставшиеся четыре зарезервированы для стандарта Gigabit Ethernet (1000Base-T). Есть два варианта разводки 568А или 568В. Чаще используется вариант 568В, как было отмечено ранее.

Нумерация разъемов коннектора RJ-45 представлена на рисунке Г.2.

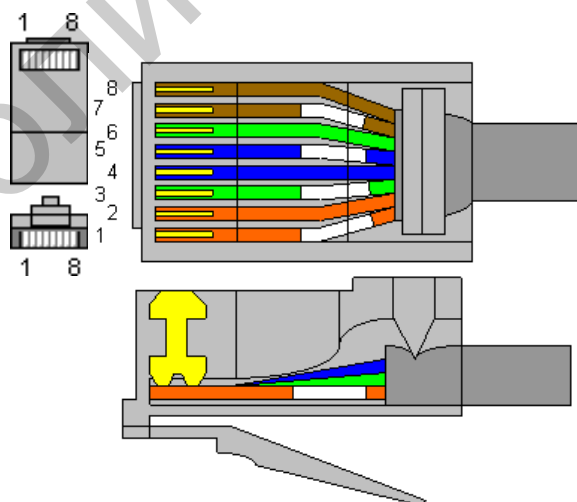
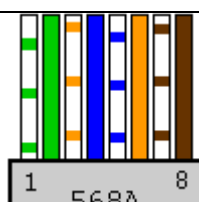
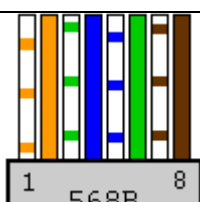


Рисунок Г.2 – Внешний вид коннектора RJ-45 с нумерацией разъемов

Разводка кабеля для соединения компьютера с сетевым оборудованием (патчкорда) представлена в таблице Г.1, на рисунках изображен внешний вид кабеля, подготовленного к вставке в коннектор (оба коннектора обжимаются одинаково).

Таблица Г.1 – Варианты распиновки прямого кабеля

EIA/TIA-568A	Пер- вый	Цвет провода	Вто- рой	EIA/TIA-568B	Пер- вый	Цвет провода	Вто- рой
 1 568A 8	1	бело-зеленый (TX+)	1	 1 568B 8	1	бело-оранжевый (TX+)	1
	2	зеленый (TX-)	2		2	оранжевый (TX-)	2
	3	бело-оранжевый (RX+)	3		3	бело-зеленый (RX+)	3
	4	синий	4		4	синий	4
	5	бело-синий	5		5	бело-синий	5
	6	оранжевый (RX-)	6		6	зеленый (RX-)	6
	7	бело-коричневый	7		7	бело-коричневый	7
	8	коричневый	8		8	коричневый	8

Г.2 Перекрестный (crossover) порядок обжима витой пары. Применяется в случае, когда требуется соединить между собой два концентратора или два маршрутизатора, не имеющих переключения uplink/normal, а также для прямого соединения двух компьютеров. На рисунке Г.3 и в таблице Г.2 представлены варианты обжимки перекрестного кабеля: первый коннектор обжат как 568B, второй как 568A.

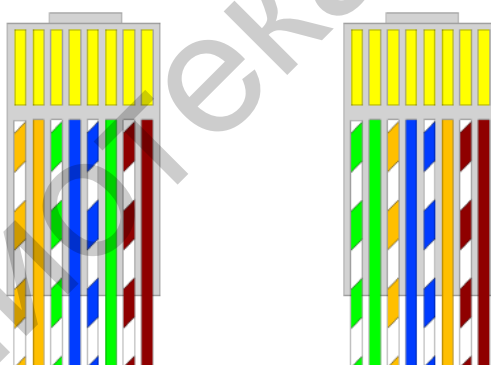


Рисунок Г.3 – Обжим перекрестного кабеля

Таблица Г.2 – Варианты распиновки перекрестного кабеля

EIA/TIA-568B	Первый	Цвет провода	Второй	Цвет провода	EIA/TIA-568A
Первый коннектор  1 568B 8	1	бело-оранжевый (TX+)	3	бело-зеленый (RX+)	Второй коннектор  1 568A 8
	2	оранжевый (TX-)	6	зеленый (RX-)	
	3	бело-зеленый (RX+)	1	бело-оранжевый (TX+)	
	4	синий	4	синий	
	5	бело-синий	5	бело-синий	
	6	зеленый (RX-)	2	оранжевый (TX-)	
	7	бело-коричневый	7	бело-коричневый	
	8	коричневый	8	коричневый	

Г.3 Инверсный (rollover) – кабель с инверсным расположением проводников, «перевертыш», где провода скрещиваны в обратном порядке (рисунок Г.4). В основном используется в оборудовании Cisco для соединения компьютера с портом AUX или консольный портом (наряду с кабелем RG-45 – DB9).

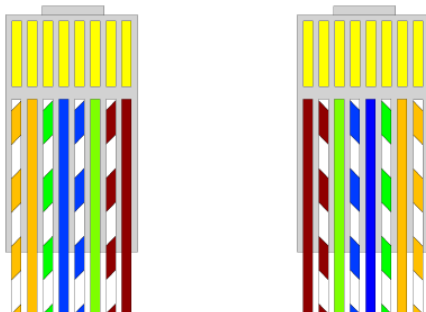


Рисунок Г.4 – Обжим инверсного кабеля

Таким образом, обобщая возможные варианты применения перечисленных типов кабеля, получаем, что:

1) Прямой кабель применяется для соединений разнотипного оборудования:

- компьютер (NIC) – коммутатор/концентратор;
- коммутатор/концентратор – маршрутизатор.

2) Перекрёстный кабель применяется в основном для соединений однотипного оборудования:

- компьютер (NIC) – компьютер (NIC);
- коммутатор/концентратор – коммутатор/концентратор;
- маршрутизатор – маршрутизатор;
- компьютер (NIC) – маршрутизатор.

3) Инверсный кабель в основном применяется для консольных или AUX-соединений с целью управления сетевым устройством.

ПРИЛОЖЕНИЕ Д (справочное)

Список наиболее часто используемых команд в ОС Cisco IOS

Общие настройки

R1#**clock set** – установка времени

R1(config)#**hostname** – установка имени устройства

R1#**configure terminal** – переход в конфигурационный режим

R1(config)#[no] **banner** [motd, login] – установка приветственного [login] баннера

R1(config)#**service timestamp** – включение генерирования отображения временных меток в системном журнале и сообщениях отладки

R1(config)#[no] **ip classless** – глобальная команда, которая включает и выключает бесклассовую маршрутизацию

R1(config)#[no] **ip subnet-zero** – глобальная команда, которая разрешает или запрещает настройку конфигурации IP-интерфейса в нулевой сети

R1(config)#[no] **ip domain-lookup** – глобальная команда, которая разрешает или запрещает разрешение имён в DNS

R1(config)#[no] **ip domain-name** [domain name] – определение имени домена

R1#**copy** running-config tftp:[[[//location]/directory]/filename] или

R1#**copy** startup-config tftp:[[[//location]/directory]/filename] – копирование конфигурации на TFTP-сервер

R1#**copy** tftp:[[[//location]/directory]/filename] running-config или

R1#**copy** tftp:[[[//location]/directory]/filename] startup-config – восстановление конфигурации с TFTP-сервера

R1#**erase** nvram: or

R1#**erase** startup-config – удаление загрузочной конфигурации

R1#**delete** flash:filename – удаление файла из флеш-памяти

Полезные команды просмотра

R1#**show version** – показ версии IOS

R1#**show running-config**, или **startup-config** – просмотр текущего и стартового конфигурационного файла

R1#**show controllers** s0/0/0 – просмотр информации о физическом оборудовании

R1#**show interface** fa0/1 – просмотр информации об интерфейсе

R1#**show ip interfaces brief** – краткая сводка по всем интерфейсам оборудования

R1#**show arp** – просмотр таблицы ARP

R1#**show processes** – информация о процессах, запущенных в системе и загрузка процессора устройства

SW1#**show dhcp lease** – просмотр полученных адресов по протоколу DHCP

R1#**show protocols** – информация по протоколам маршрутизации и интерфейсам на маршрутизаторе

R1#**show history** – просмотр истории команд

SW1#**show mac-address-table** – просмотр таблицы MAC-адресов

SW1#**show port-security** {interface interface-id} – просмотр режима безопасности на порте

SW1#**show port-security** {interface interface-id} **address** – просмотр сконфигурированных MAC-адресов

Команды терминала

R1#**terminal ip netmask-format decimal** – установка десятичного формата маски вместо префиксного

R1#**terminal history size** {size} – установка размера истории введенных команд в строках, 256 max

R1#**terminal no history size** – сброс размера истории по умолчанию

R1#**terminal no history** – отключение истории терминала

R1#**terminal monitor** – просмотр отладочной информации в Telnet- и SSH-сеансах

Настройка линий и паролей

ОБЩИЕ

R1(config)#[no] **enable password** – установка пароля привилегированного режима

R1(config)#[no] **enable secret** – установка зашифрованного пароля привилегированного режима

R1(config)#[no] **service password-encryption** – шифрование паролей в конфигурационных файлах (не имеет обратной силы)

КОНСОЛЬНАЯ ЛИНИЯ

R1(config)#**line console 0** – переход в режим настройки консольного порта

R1(config-line)#[no] **password** {password} – установка пароля на интерфейс

R1(config-line)#[no] **login** – включение пароля

R1(config-line)#**logging synchronous** – подавление вывода технической информации во время набора команд

R1(config-line)#**exec-timeout** {minutes} – установка времени «тайм-аута»

TELNET и SSH подключение

R1(config)#**crypto key generate rsa** – генерация RSA ключа для шифрования связи, нужен для SSH-соединения

R1(config)#**line vty 0 15** – переход в режим настройки терминалов

R1(config-line)#[no] **password**, [no] **Login**, **logging synchronous**, **exec-timeout** – см. выше по аналогии с «консольная линия»

R1(config-line)#**transport** {input/output} {all/none/ssh/telnet} – определяет, какой протокол будет использоваться для подключения к терминальному серверу (для исходящих соединений)

R1(config-line)#**login local** – выдавать запрос на ввод логина и пароля, которые проверяются в локальной базе данных

R1(config)#**ip ssh version** {1/2} – версия протокола

R1(config)#**ip ssh time-out** – «тайм-аут» интервал SSH

R1(config)#**ip ssh authentication-retries** – количество попыток аутентификации

Настройки сетевых интерфейсов

R1(config)#**interface FastEthernet 0/0 (fa0/0), Serial 0/0/0 (s0/0/0), LoopBack 0-2³¹ (lo1-...)** – выбор интерфейса

R1(config)#**interface fa0/0.10** – создание сабинтерфейса на физическом интерфейсе. Номер может быть любой, обычно отображает номер VLAN, связанного с этим сабинтерфейсом

R1(config-subif)#**encapsulation dot1q** {vlan_id} – привязка сабинтерфейса к соответствующему VLAN с номером *vlan_id*

SW1(config)#**interface range** {interface interface-id} – режим работы с диапазоном интерфейсов

R1(config-if)#**ip address** {address/dhcp} {mask} – задание адреса и маски либо получение с сервера DHCP

R1(config-if)#**no shutdown** – включение интерфейса
R1(config-if)#**shutdown** – выключение интерфейса
R1(config-if)#**clock rate** {rate} – установка тактовой частоты для порта serial, применимо только на DCE-стороне оборудования
R1(config-if)#[no] **bandwidth** {band} – ширина канала (в килобитах); [no] – восстановление значения по умолчанию
R1(config-if)#**delay** {delay} – указывает задержку на канале (в десятках микросекунд)
R1(config-if)#**duplex** – настройка направленности интерфейса
R1(config-if)#**speed** – скорость интерфейса
R1(config-if)#**description** – описание интерфейса
R1(config-if)#**ip nat** {inside/outside} – задание внутреннего и внешнего интерфейса для NAT-трансляции
R1(config-if)#**ip summary-address** {rip, eigrp ASN} {IP суммарной сети} {маска} – суммирование адресов

WAN

R1(config-if)#**encapsulation** {hdlc/ppp} – выбор протокола на последовательном канале (hdlc, ppp...)
R1(config-if)#**compress** {predictor | stac} – включение компрессии (разные алгоритмы)
R1(config-if)#**ppp quality** {percentage} – мониторинг качества связи (качество должно быть не менее указанного значения)
R1(config-if)#**ppp authentication** {chap | chap pap | pap chap | pap} – включение аутентификации протокола ppp
R1(config-if)#**ppp pap sent-username** {username} **password** {password} – данные, выслаемые в pap-аутентификации
R1#**debug ppp** {.....} – просмотр отладочной информации
R1(config)#**username** {name} **password** {password} – имя пользователя и пароль, используемый в аутентификации

НА SWITCH

SW1(config)#**ip default-gateway** {ip address} – установка шлюза по умолчанию
SW1(config-if)#**ip address** {address} {mask} – задание адреса и маски на интерфейсе
SW1(config-if)#**duplex** {auto, full, half} – установка режима передачи на интерфейсе
SW1(config-if)#**speed** {10, 100, ..., auto} – установка скорости передачи на интерфейсе
SW1(config-if)#[no] **mac-address-table static** {MAC address} **vlan** {1-4096, ALL} – [снятие] установка статического MAC-адреса на порт

VLAN

SW1(config)#[no] **vlan** {vlan_id} – удаление/создание VLAN с номером vlan_id
SW1(config-vlan)#**name** {имя} – задает имя VLAN
SW1(config)#**interface vlan** {номер} – переход в режим настройки интерфейса VLAN
SW1(config-if)#**switchport access vlan** {номер} – привязывает порт к конкретному VLAN
SW1(config-if)#**no switchport access vlan** – удаление порта из VLAN и возврат в дефолтный vlan
SW1(config-if)#**mls qos trust cos** – приоритет voice трафика
SW1(config-if)#**switchport voice vlan** {номер} – создание VLAN для голосового трафика
SW1(config-if)#**switchport mode** {access/dynamic {auto/desirable}}/trunk} – установка режима доступа к порту
SW1(config-if)#**switchport trunk allowed vlan** {...} – установка разрешенных/исключенных VLAN на транковом интерфейсе
SW1(config-if)#**no switchport trunk allowed vlan** – сброс всех сконфигурированных VLAN на транковом интерфейсе
SW1(config-if)#**switchport trunk native** {vlan номер} – установка родного (native) VLAN

SW1(config-if)#**no switchport trunk native vlan** – сброс родного VLAN назад к VLAN 1
 SW1(config-if)#**switchport nonegotiate** – отключение DTP-протокола на порте
 SW1#**show vlan brief** – просмотр краткой информации о VLAN
 SW1#**show vlan summary** – выводит информацию об общем количестве сконфигурированных VLAN
 SW1#**show vlan name {vlan-name}** – просмотр информации о VLAN с именем *vlan-name*
 SW1#**show interfaces vlan {vlan}** – подробная информация об интерфейсе
 SW1#**show interfaces trunk** – информация о транковом канале на интерфейсах
 SW1#**show interface fa0/18 switchport** – информация о режиме работы интерфейса относительно VLAN
 SW1#**delete flash:vlan.dat** – удаление всей информации о VLAN
КОНФИГУРИРОВАНИЕ БЕЗОПАСНОСТИ НА ПОРТЕ
 SW1(config-if)#**switchport port-security** – включение безопасности на порте
 SW1(config-if)#**switchport port-security mac-address {H.H.H/sticky}** – привязка MAC-адреса к порту либо обучение его динамически
 SW1(config-if)#**switchport port-security maximum {1..132}** – количество MAC адресов, привязанных к порту
 SW1(config-if)#**switchport port-security violation {protect | restrict | shutdown}** – режим работы порта после попытки доступа с запрещенного MAC-адреса
КОНФИГУРИРОВАНИЕ ВЕБ-ИНТЕРФЕЙСА
 SW1(config)#**ip http authentication enable** – конфигурирование метода аутентификации
 SW1(config)#**ip http server** – включение сервера

Создание канала

SW1(config-if)#**channel-group {1..6} mode {режим работы: auto/on/desirable}** – создание канала на нескольких линиях

STP– Spanning Tree Protocol

SW1(config)#**spanning-tree mode {rapid-pvst/mst/pvst}** – включение различных режимов работы протокола
 SW1(config-if)#**[no] spanning-tree vlan {vlan-id} cost {число}** – устанавливает стоимость линии на интерфейсе; [no] – возврат к значению по умолчанию
 SW1(config-if)#**[no] spanning-tree vlan {vlan-id} port-priority {число}** – устанавливает приоритет интерфейса; [no] – возврат к значению по умолчанию
 SW1(config-if)#**spanning-tree bpduguard {enable/disable}** – включение/отключение режима BPDU guard (заперт на получение BPDU-пакетов на порте)
 SW1(config-if)#**[no] spanning-tree portfast** – перевод порта коммутатора в режим пересылки пакетов (форвардинга) сразу после подключения оконечного устройства
 SW1 (config-if)#**spanning-tree link-type point-to-point** – указание типа соединения на порте
 SW1(config)#**spanning-tree vlan {vlan-id} root primary|secondary** – определяет данный коммутатор во VLAN первичным или корневым (id 24576) или вторичным (запасным) (id 28672)
 SW1(config)#**spanning-tree vlan {vlan-id} root primary diameter {1..7}** – установка диаметра сети для STP-таймингов
 SW1(config)#**spanning-tree vlan {vlan-id} priority {value = (0..65536 inc 4096)}** – установка приоритета вручную
 SW1#**clear spanning-tree detected-protocols** – очистка всех обнаруженных STP
 SW1#**show spanning-tree** – отображение информации касательно STP

VTP – VLAN Trunking Protocol

SW1#**show vtp status** – просмотр информации о vtp

SW1(config)#**vtp mode** {client/server/transparent} – выбор режима работы VTP-протокола

SW1(config)#**vtp domain** {имя домена} – установка имени VTP-домена

SW1(config)#**vtp password** {пароль} – установка пароля VTP-домена

SW1(config)#**vtp version** {1-3} – установка версии протокола VTP

SW1#**show vtp** {counters/password/status} – вывод VTP-статистики, пароля, статуса домена

Cisco Discovery Protocol

R1#**show cdp neighbors** – показ соседних устройств фирмы Cisco

R1#**show cdp neighbors detail** – показ соседних устройств фирмы Cisco в деталях

R1(config)#**no cdp run** – отключение протокола CDP

R1(config-if)#**no cdp enable** – прекратить оповещения по CDP на отдельном интерфейсе

Цепочки ключей

R1(config)#**key chain** {имя цепочки} – конфигурация цепочки ключей

R1(config-keychain)#**key** {номер цепочки} – номер ключа в цепочке

R1(config-keychain-key)#**key-string** {пароль} – указание пароля

R1(config-keychain-key)#**accept-lifetime** {начальное время} [duration | Time to stop | infinite] – время существования ключа для входящих сообщений

R1(config-keychain-key)#**send-lifetime** {начальное время} [duration | Time to stop | infinite] – время существования ключа для исходящих сообщений

Маршрутизация

R1#[no] **debug ip routing** – показ отладочной информации о маршрутизации

R1#**clear ip route** – очистка таблицы маршрутизации

R1#**show ip route** [static/rip/connected/eigrp/ospf] | [ip address] – просмотр таблицы маршрутизации, протокол, IP-адрес

R1#**show ip protocols** – параметры и статистика протокола маршрутизации

Маршрутизация статическая

R1(config)#**ip route prefix mask** {ip-address | interface-type interface-number [ip-address]} [distance] [name] [permanent] [tag tag] – полный формат записи маршрута

R1(config)#**ip route** network-address subnet-mask {ip-address | exit-interface }

R1(config)#**ip route** network-address subnet-mask {ip-address | exit-interface } **null 0** – удалять все пакеты на маршрут сеть/маска

Маршрутизация динамическая RIP/RIP v2

R1(config)# [no] **router rip** – режим настройки протокола RIP; [no] ... – отключение протокола маршрутизации

R1(config-router)#[no] **network** {сеть} – удаление/добавление сети в маршрутизацию

R1(config-router)#**default-information originate** – распространение маршрута по умолчанию

R1(config-router)#**redistribute static** – принудительная раздача статических маршрутов

R1(config-router)#[no] **passive-interface** {interfaces/default} – интерфейс, по которому не распространяется информация об обновлениях маршрута. Default – включение для всех интерфейсов запрета на распространение маршрутной информации

R1(config-router)#**distance** {1-255} – установка административной дистанции маршрутизирующего протокола

R1(config-if)#**ip rip authentication mode** {md5, text} – включение на интерфейсе аутентификации

R1(config-if)#**ip rip authentication key-chain** {имя цепочки} – включение на интерфейсе аутентификации

Маршрутизация динамическая EIGRP

R1(config)# [no] **router eigrp** {ASN} – режим настройки протокола EIGRP; [no] ... – отключение протокола маршрутизации. ASN – номер автономной системы, номер процесса eigrp, запущенного на роутере

R1(config-router)#[no] **network** {network-address} [wildcard-mask] – удаление/добавление сети в маршрутизацию. Wildcard-mask – дикая/обратная маска для включения только подсети классовой сети.

R1#**show ip eigrp** **interfaces** – IP-EIGRP-интерфейсы, на которых работает протокол

neighbors – IP-EIGRP-соседи, с которых получает информацию

topology [ip сети] – IP-EIGRP таблица топологии сети

traffic – IP-EIGRP-статистика трафика

R1(config-router)#**metric weights** {tos} {k1 k2 k3 k4 k5} – изменение коэффициентов расчёта метрики; k1-k5 – 0-255 – величина коэффициентов; tos – type of service – тип сервиса

R1(config)#[no] **auto-summary** – отключение/включение автоматического суммирования маршрутов

R1(config-if)#**ip summary-address eigrp** {as-number} {network-address} {subnet-mask} – ручная суммаризация маршрутов на интерфейсе

R1(config-router)#**redistribute static** – распространение статических маршрутов

R1(config-if)#**ip bandwidth-percent eigrp** {as-number} {percent} – использование протоколом полосы пропускания в процентах

R1(config-if)#**ip hello-interval eigrp** {as-number} {seconds} – установка времени периодичности рассылки HELLO-пакетов

R1(config-if)#**ip hold-time eigrp** {as-number} {seconds} – установка времени удержания маршрута до его удаления в случае неполучения HELLO-пакета

R1(config-if)#**ip authentication mode eigrp** {as-номер} **md5** – включение режима MD5-аутентификации на интерфейсе

R1(config-if)#**ip authentication key-chain eigrp** {as-номер} {название цепочки} – указание, какую цепочку ключей использовать для MD5-утентификации

R1#**debug eigrp packets** – отладочная информация для каждого пакета EIGRP

R1#**debug eigrp fsm** – в динамике информация об оптимальных и резервных маршрутах

R1#**debug ip eigrp** – то же, что и debug eigrp packets, только для протокола IP

Маршрутизация динамическая OSPF

R1(config)#[no] **router ospf** {process} – режим настройки протокола OSPF; [no] ... – отключение

R1(config-router)#[no] **network** {network-address} {wildcard-mask} **area** {идентификатор} – задает сети и интерфейсы, участвующие в OSPF-маршрутизации, а также указывает, в какую зону входит интерфейс

R1(config-router)#**auto-cost reference-bandwidth** {значение} – задает исходную полосу пропускания, используемую для расчёта стоимости интерфейсов (метрики)

R1(config-router)#**router-id** {ID роутера} – команда задания ID роутера (A.B.C.D)

R1(config-router)#**maximum-paths** {значение} – задает максимальное значение количества маршрутов с одинаковой метрикой в таблице маршрутизации (для балансировки нагрузки)

R1(config-if)#**ip ospf** {process} **area** {идентификатор} – запуск OSPF на каком-либо интерфейсе, минуя команду router ospf

R1(config-if)#**ip ospf cost** {значение} – задает стоимость интерфейса в протоколе OSPF

R1(config-if)#**ip ospf hello-interval** {значение} – задает значение hello-интервала

R1(config-if)#**ip ospf dead-interval** {значение} – задает значение dead-интервала

R1(config-if)#**ip ospf network** {значение} – задает тип сети

R1(config-if)#**ip ospf priority** {значение} – задание приоритета интерфейса

R1(config-if)#**ip ospf authentication** [пароль | message-digest | null] – команда включения аутентификации на интерфейсе. Открытый пароль, пароль зашифрован MD5, отключение аутентификации

R1(config-if)#**ip ospf message-digest-key** {номер ключа} **md5** {пароль} – задает пароль для MD5-аутентификации

R1(config-router)#**area** {зона} **authentication** [message-digest | null] – включение аутентификации для всей зоны

R1#**clear ip ospf process** – перезапуск OSPF-процессов

R1#**show ip route ospf** – показывает маршруты протокола OSPF в таблице маршрутизации

R1# **show ip protocols** – параметры протокола маршрутизации и текущее значение таймеров

R1#**show ip ospf interface** – номер зон интерфейса, соседние маршрутизаторы, доступные через указанный интерфейс, значения hello- и dead-таймеров

R1#**show ip ospf neighbor** [RID соседнего маршрутизатора] – список соседних маршрутизаторов и коды их состояния

R1#**show ip ospf** – подробная информация о протоколе OSPF

R1#**debug ip ospf events** – генерирует отладочное сообщение для каждого OSPF-пакета

R1#**debug ip ospf packet** – генерирует отладочное сообщение для каждого OSPF-пакета, а также выводит описание пакета

R1#**debug ip ospf hello** – генерирует отладочное сообщение для каждого hello-пакета

Учебное издание

Бунас Виталий Юрьевич
Зеленин Александр Сергеевич

***ОСНОВЫ ПОСТРОЕНИЯ
ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ.
ЛАБОРАТОРНЫЙ ПРАКТИКУМ***

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редактор *Е. И. Герман*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *В. М. Задоя*

Подписано в печать 14.09.2017. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 6,16. Уч.-изд. л. 6,3. Тираж 130 экз. Заказ 386.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
ЛП №02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6