Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ

Э. Р. Абанеев

СЕТИ ПЕРЕДАЧИ ДАННЫХ

Методические указания
по выполнению лабораторных работ

Томск 2017

Корректор: А. Н. Миронова

Абанеев Э. Р.

Сети передачи данных : методические указания по выполнению лабораторных работ / Э. Р. Абанеев. – Томск : ФДО, ТУСУР, 2017. – 49 с.

Методические указания содержат краткое изложение теоретического материала, описание последовательности выполнения работ и правила оформления отчетов. Лабораторные работы посвящены коммутации второго уровня модели OSI, использованию коммутаторов и их базовой настройке. Для студентов всех форм обучения, в том числе с применением дистанционных образовательных технологий.

© Абанеев Э. Р., 2017
© Оформление.
ФДО, ТУСУР, 2017

СОДЕРЖАНИЕ

1 Теоретические положения 4
2 Лабораторная работа № 1 «Подключение к коммутатору, изучение сетевой операционной системы коммутатора» 28
2.1 Задание 28
2.2 Порядок выполнения работы 28
3 Лабораторная работа № 2 «Изучение текущей конфигурации коммутатора и настройка базовых параметров коммутатора» 34
3.1 Задание 34
3.2 Порядок выполнения работы 34
4 Лабораторная работа № 3 «Реализация базовой схемы подключения» 41
4.1 Задание 41
4.2 Порядок выполнения работы 41
5 Требования к оформления отчета по работе 46
Литература 47
Приложение А Формы отчетов по лабораторным работам 48

1 ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

Изучение сети

Маршрут, по которому сообщение идет от источника к месту назначения, может быть простым (например, один кабель, соединяющий два компьютера) или сложным (например, сети, буквально охватывающие весь мир). Такая сетевая инфраструктура обеспечивает стабильный и надежный канал для передачи данных.

Компоненты сети

Сетевая инфраструктура включает в себя три категории компонентов сети (рис. 1.1):

1. Устройства.
2. Среда передачи.
3. Сервисы.

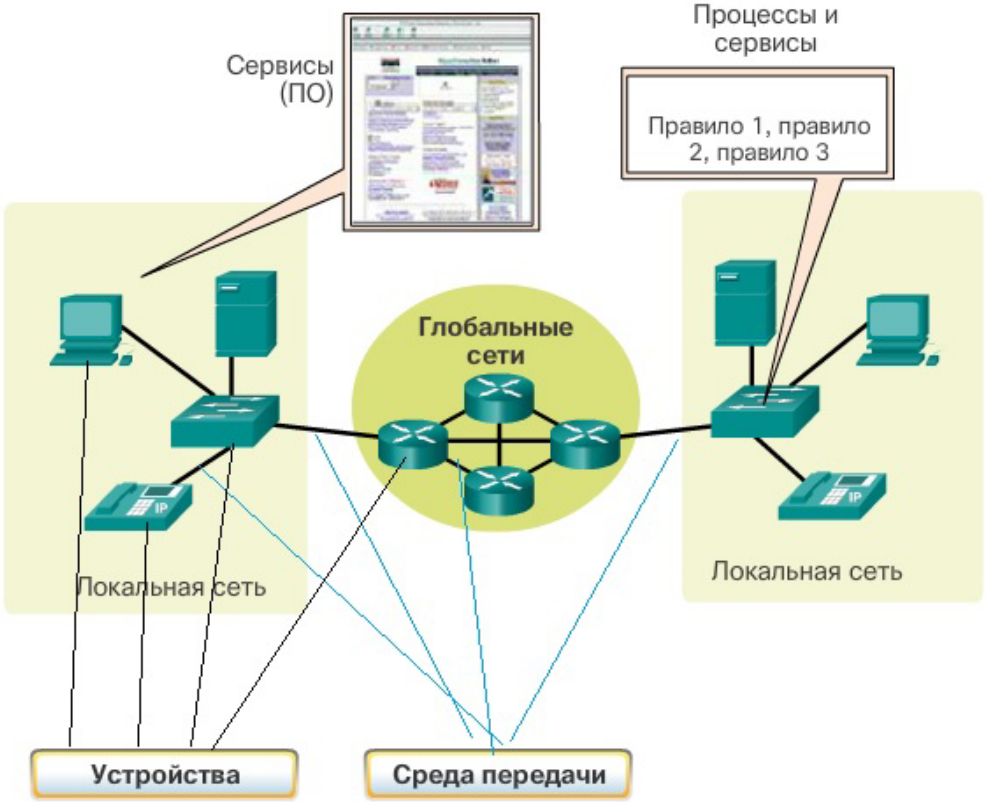


Рис. 1.1 – Компоненты сети

Устройства и среды передачи – это физические элементы или аппаратное обеспечение сети. Аппаратное обеспечение зачастую является видимой частью сетевой платформы: ноутбук, ПК, коммутатор, маршрутизатор, беспроводная точка доступа или кабели, используемые для соединения устройств.

Сервисы включают в себя множество сетевых приложений, которые люди используют ежедневно, например сервисы электронной почты и веб-хостинга. Процессы обеспечивают функциональность, посредством которой сообщения направляются и перемещаются в пределах сети. Процессы менее очевидны для нас, но критически важны для работы сетей.

Сетевые устройства

Сетевые устройства, с которыми пользователи знакомы лучше всего, называются оконечными устройствами. Примеры оконечных устройств представлены на рис. 1.2.



Рис. 1.2 – Примеры оконечных устройств

Оконечное устройство является либо отправителем (источником), либо получателем (адресатом) сообщения, передаваемого по сети.

Промежуточные устройства соединяют отдельные оконечные устройства с сетью и могут соединять несколько отдельных сетей для создания глобальных сетей. Такие устройства обеспечивают подключение и прохождение потоков данных по сети.

Для определения пути передачи сообщения промежуточные устройства используют адрес оконечного устройства назначения в сочетании с информацией о связях в сети. Примеры распространенных промежуточных устройств и перечень их функций показаны на рисунке 1.3.



Промежуточные сетевые устройства выполняют некоторые из этих функций или сразу все.

- Восстановление и ретрансляция сигналов.
- Сбор и поддержка в актуальном состоянии информации о существующих путях в сети и между сетями.
- Уведомление других устройств об ошибках и сбоях в процессе коммуникации.
- Перенаправление данных по альтернативному маршруту в случае сбоя одного из каналов связи.
- Классификация и направление сообщений согласно приоритетам.
- Разрешение или запрет передачи данных в зависимости от настроек безопасности.

Рис. 1.3 – Примеры промежуточных устройств

Среды передачи данных

Связь в сетях осуществляется по средам передачи данных. Среда передачи данных предоставляет собой физический канал, по которому сообщение передается от источника к адресату.

В современных сетях для соединения устройств и создания между ними каналов в основном используются три типа сред передачи данных (см. рис. 1.4).

Металлические провода в кабелях – данные кодируются в электрические импульсы.

Стеклянные или пластиковые волокна (оптоволоконный кабель) – данные кодируются в световые импульсы.

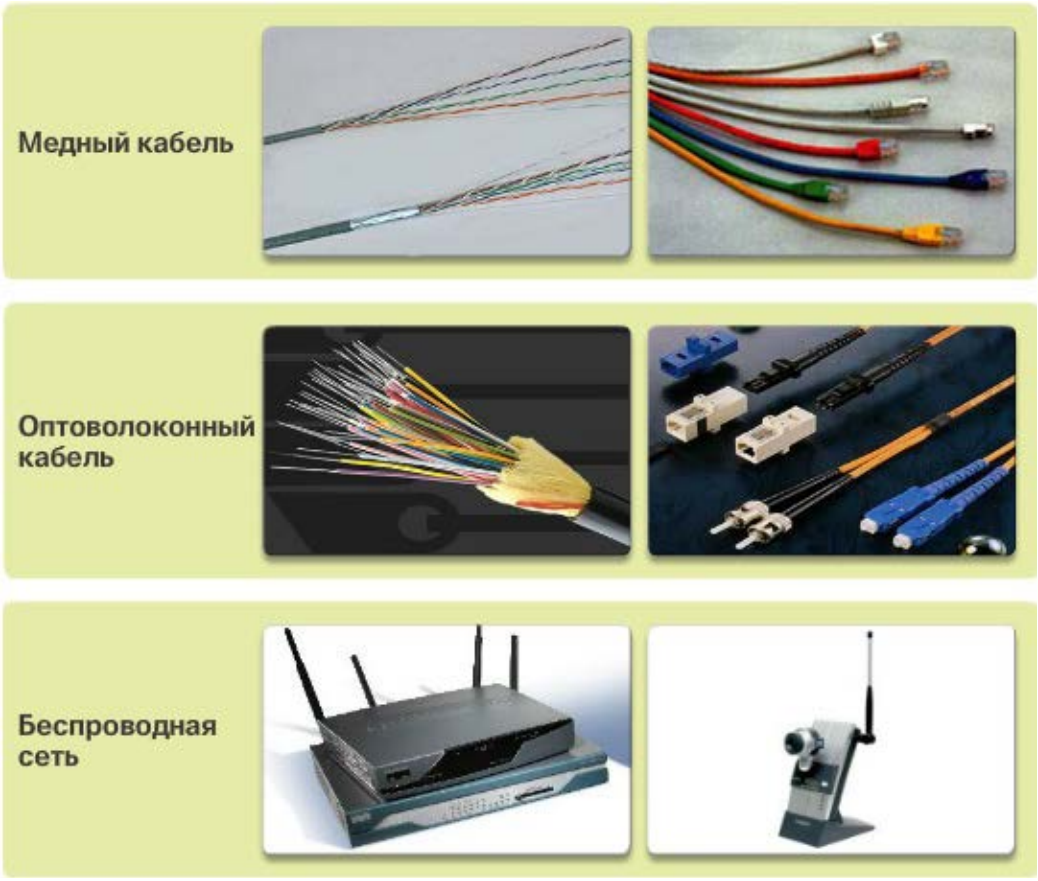


Рис. 1.4 – Типы сред передачи данных

Беспроводная передача – данные кодируются при помощи электромагнитных волн радиочастотного диапазона.

У разных сред передачи свои преимущества и особенности. Среды передачи данных имеют разные характеристики и различное применение.

Сетевые обозначения

Для обозначения различных устройств и соединений, из которых состоит сеть, на схемах сетей часто используются символы, такие как на рис. 1.5.

Схема обеспечивает наглядный способ понимания, каким образом устройства в большой сети связаны между собой. Этот тип изображения сети называется схемой топологии. Чтобы представлять устройство и работу сети, крайне важно понимать подобные логические схемы и сопоставлять их с реальными устройствами.



Рис. 1.5 – Сетевые обозначения

Кроме этих обозначений существуют также специальные термины, которые используются при описании устройств и соединений между ними. Важные термины, которые следует запомнить:

Сетевая карта (Network Interface Card, NIC) – интерфейсная плата или сетевой адаптер для локальной сети, который обеспечивает физическое подключение к сети на настольном компьютере или другом устройстве. Кабель, соединяющий компьютер с сетевым устройством, подключается непосредственно к сетевой карте (рис. 1.2).

Физический порт – разъем на сетевом устройстве, через который кабели подключены к компьютеру или другому сетевому устройству.

Интерфейс – специализированные порты в сетевом устройстве, которые подключаются к отдельным сетям. Поскольку маршрутизаторы соединяют между собой сети, порты маршрутизатора называются сетевыми интерфейсами.

Примечание. Термины «порт» и «интерфейс» часто взаимозаменяемы.

Типы сетей

Сетевые инфраструктуры могут значительно отличаться по следующим критериям:

– площадь покрытия;

– количество подключенных пользователей;

– количество и типы доступных услуг;

– область ответственности.

На рисунке 1.6 представлены два наиболее распространенных типа сетевой инфраструктуры.

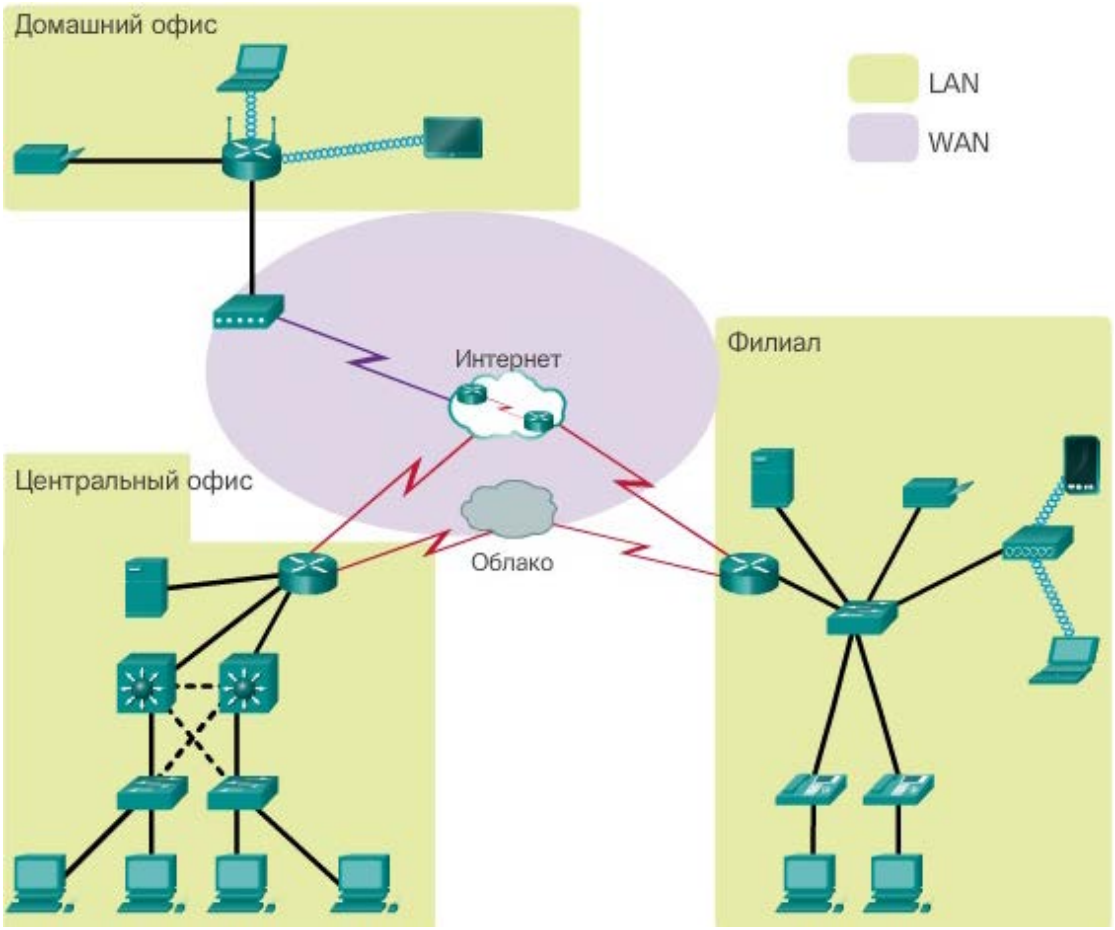


Рис. 1.6 – Типы сетевой инфраструктуры

Локальная сеть (LAN) – сетевая инфраструктура, предоставляющая доступ пользователям и оконечным устройствам на небольшой территории; обычно является домашней сетью, сетью малого или крупного предприятия, управляется одним лицом или ИТ-отделом и принадлежит им.

Глобальная сеть (WAN) – сетевая инфраструктура, предоставляющая доступ к другим сетям на большой территории; обычно принадлежит провайдерам телекоммуникационных услуг и находится под их управлением.

Другие типы сетей

- Городская сеть (Metropolitan Area Network, MAN) – сетевая инфраструктура, которая охватывает территорию больше, чем локальная сеть, но меньше глобальной сети (например, город). Как правило, управляет городскими сетями одна организация, например крупный сетевой оператор.
- Беспроводные локальные сети (WLAN) аналогичны локальным сетям, но соединяют пользователей и оконечные устройства на небольшой территории с помощью беспроводной связи.
- Сеть хранения данных (SAN) – сетевая инфраструктура, разработанная для поддержки файловых серверов, хранения данных, их получения из хранилища и репликации.

Локальные сети

Локальная сеть (ЛВС, LAN) – сетевая инфраструктура, которая охватывает небольшую территорию (см. рис. 1.7).

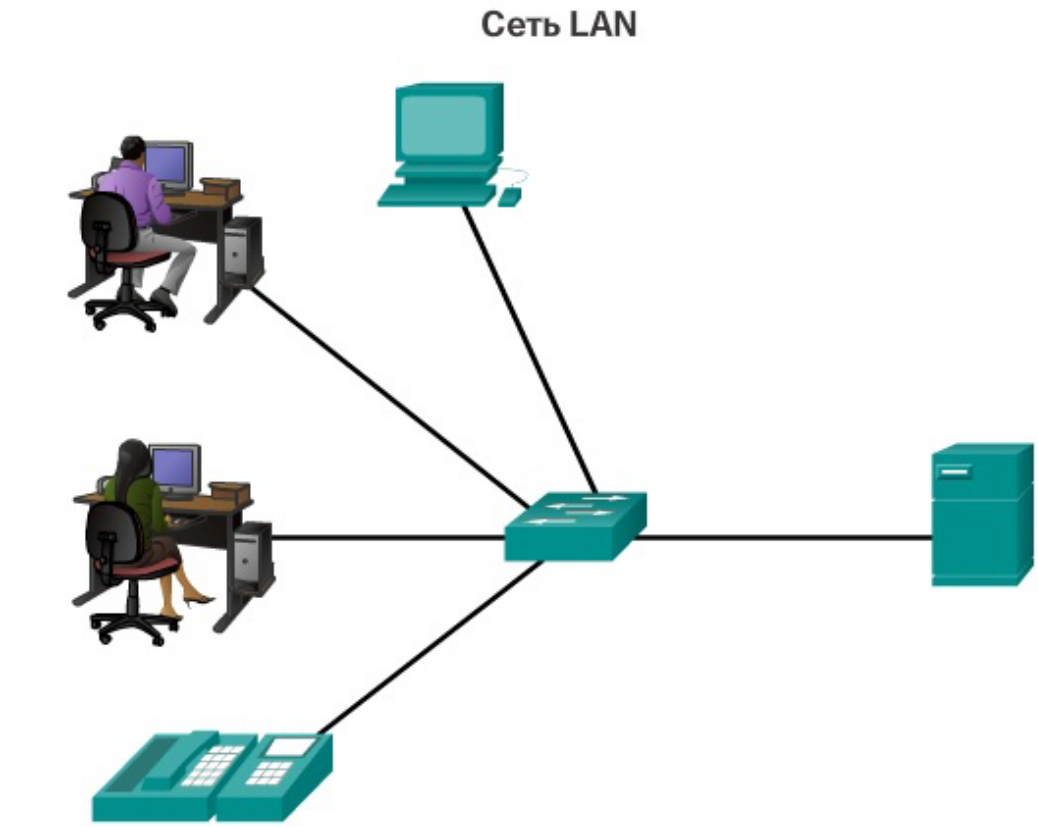


Рис. 1.7 – Пример локальной сети

Особенности локальных сетей

Локальные сети связывают оконечные устройства в ограниченной области, например в доме, школе, офисном здании или комплексе зданий.

Локальные сети обычно администрирует одна организация или частное лицо. Администратор управляет политикой безопасности и контролем доступа на сетевом уровне.

Локальные сети предоставляют высокоскоростной доступ к внутренним оконечным и промежуточным устройствам.

Технологии доступа в Интернет

Существует множество способов подключения пользователей и организаций к Интернету.

Домашние пользователи, удаленные сотрудники компаний и малые офисы, как правило, для доступа в Интернет нуждаются в подключении к поставщикам услуг Интернета. Варианты подключения существенно меняются в зависимости от интернет-провайдера и географического местоположения. Однако популярные варианты включают в себя широкополосную кабельную сеть, широкополосную цифровую абонентскую линию (DSL), беспроводные глобальные сети и мобильные сервисы.

Организациям обычно нужен доступ к другим корпоративным узлам и Интернету. Для бизнес-сервисов, в том числе веб-конференций, IP-телефонов, центров обработки и хранения данных требуются быстрые соединения.

Каналы для бизнеса обычно предоставляются операторами связи. Популярные услуги бизнес-класса включают DSL, арендуемые линии (выделенные линии) и прочие сетевые услуги.

Подключение к Интернет для дома и небольшого офиса

На рисунке 1.8 показаны стандартные варианты подключения малых и домашних офисов.

Кабельное подключение обычно предлагают поставщики услуг кабельного телевидения. Данные передаются по тому же кабелю, который используется для передачи сигналов кабельного телевидения. Этот способ обеспечивает подключения к Интернету с высокой пропускной способностью и постоянным доступом к сети.

DSL – цифровая абонентская линия, обеспечивает подключение к Интернету с высокой пропускной способностью и постоянным доступом к сети. DSL использует телефонные линии связи. Обычно небольшие и домашние офисы используют асимметричные линии DSL (ADSL), в которых данные пользователю передаются с большей скоростью, чем от пользователя.



Рис. 1.8 – Варианты подключения малых и домашних офисов

Сотовая связь. Для доступа в Интернет используется мобильная телефонная сеть. В любой точке, где доступен сигнал сотовой сети, можно получить доступ в Интернет. Производительность будет ограничена возможностями телефона и базовой станции, к которой он подключен.

Спутниковая связь. Спутниковые интернет-каналы можно использовать в районах, где нет других способов подключения. Для использования спутниковых антенн необходимо, чтобы спутник находился в зоне прямой видимости.

Телефонный коммутируемый доступ – это экономичный вариант подключения с использованием любой телефонной линии и модема. Низкая пропускная способность коммутируемой линии обычно недостаточна

для передачи большого объема данных. Однако такая линия может быть полезна для мобильного доступа в пути.

Для подключения домов и небольших офисов все чаще используются *оптоволоконные кабели*. Это позволяет интернет-провайдерам обеспечивать более высокие скорости передачи данных, а также предоставлять больше услуг, например Интернет, телефон и телевидение.

Способ подключения зависит от географического местоположения пользователей и наличия в регионе оператора связи.

Подключение к Интернету для предприятий

Корпоративные варианты подключения отличаются от вариантов для домашнего пользователя. Компании может требоваться более высокая пропускная способность, выделенная линия и управляемые услуги. Доступные варианты подключения зависят от технологий, которые используют операторы связи, находящиеся рядом.

На рисунке 1.9 показаны стандартные варианты подключения для предприятий.

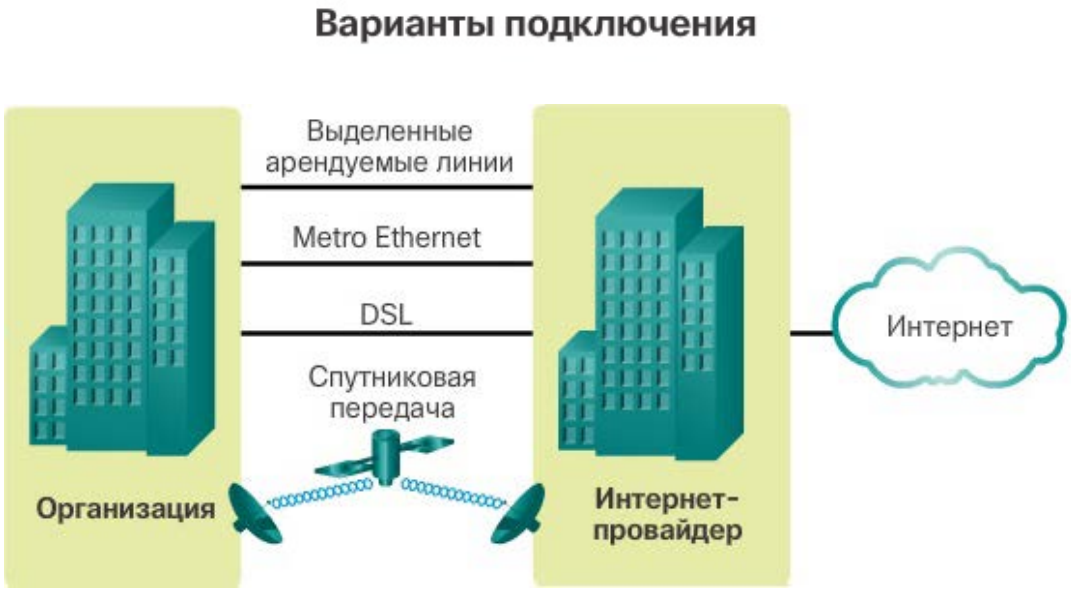


Рис. 1.9 – Варианты подключения для предприятий

Выделенная арендованная линия – арендованные линии представляют собой зарезервированные каналы в сети оператора связи, обеспечивающие связь между географически удаленными офисами для передачи голоса и данных в частной сети. Плата за аренду таких каналов связи обычно взимается ежемесячно или ежегодно. Они могут быть дорогими.

Глобальная сеть Ethernet – глобальные сети Ethernet позволяют расширить сети LAN до WAN. Преимущества технологии Ethernet теперь доступны и в глобальных сетях.

DSL – корпоративное DSL-подключение доступно в различных форматах. Популярностью пользуются симметричные цифровые абонентские линии (Symmetric Digital Subscriber Lines, SDSL), аналогичные абонентской версии DSL, но обеспечивающие одинаковую скорость при получении и отправке данных.

Спутниковая связь. Как и в случае небольших и домашних офисов, спутниковые услуги обеспечивают подключение там, где проводная связь недоступна.

Способ подключения зависит от географического местоположения пользователей и наличия в регионе оператора связи.

Цель лабораторных работ

Наша цель – в освоении основных принципов управления небольшой локальной сетью. В центре такой сети, как мы выяснили, находится *сетевое устройство*, называемое *коммутатором*. Коммутатор может быть *управляемым* и *неуправляемым*. Неуправляемый коммутатор предоставляет только доступ к локальной сети (Ethernet), все подключаемые к такому коммутатору устройства будут находиться в одном локальном сегменте сети Ethernet (если оперировать терминологией VLAN, то все будут в VLAN1). В случае использования управляемого коммутатора есть много

возможностей по разделению локальной сети на сегменты (различные VLANы), а также использование функций сетевой безопасности.

В наших лабораторных мы будем настраивать управляемый коммутатор, используя программу моделирования Cisco Packet Tracer.

Что такое коммутатор

Сетевой коммутатор (от англ. switch – переключатель) – устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети (рис. 1.10, 1.11). *Коммутатор работает на канальном (втором) уровне модели OSI*. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты. Для соединения нескольких сетей на основе сетевого уровня служат маршрутизаторы (3-й уровень OSI).



Рис. 1.10 – Вид коммутатора спереди



Рис. 1.11 – Вид коммутатора сзади

В отличие от концентратора (1-й уровень OSI), который распространяет трафик от одного подключённого устройства ко всем остальным, коммутатор передаёт данные только непосредственно получателю (исключение составляет широковещательный трафик всем узлам сети и трафик для устройств, для которых неизвестен исходящий порт коммутатора). Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

Как и любому оконечному устройству, сетевому устройству тоже необходима операционная система (ОС) (рис. 1.12).

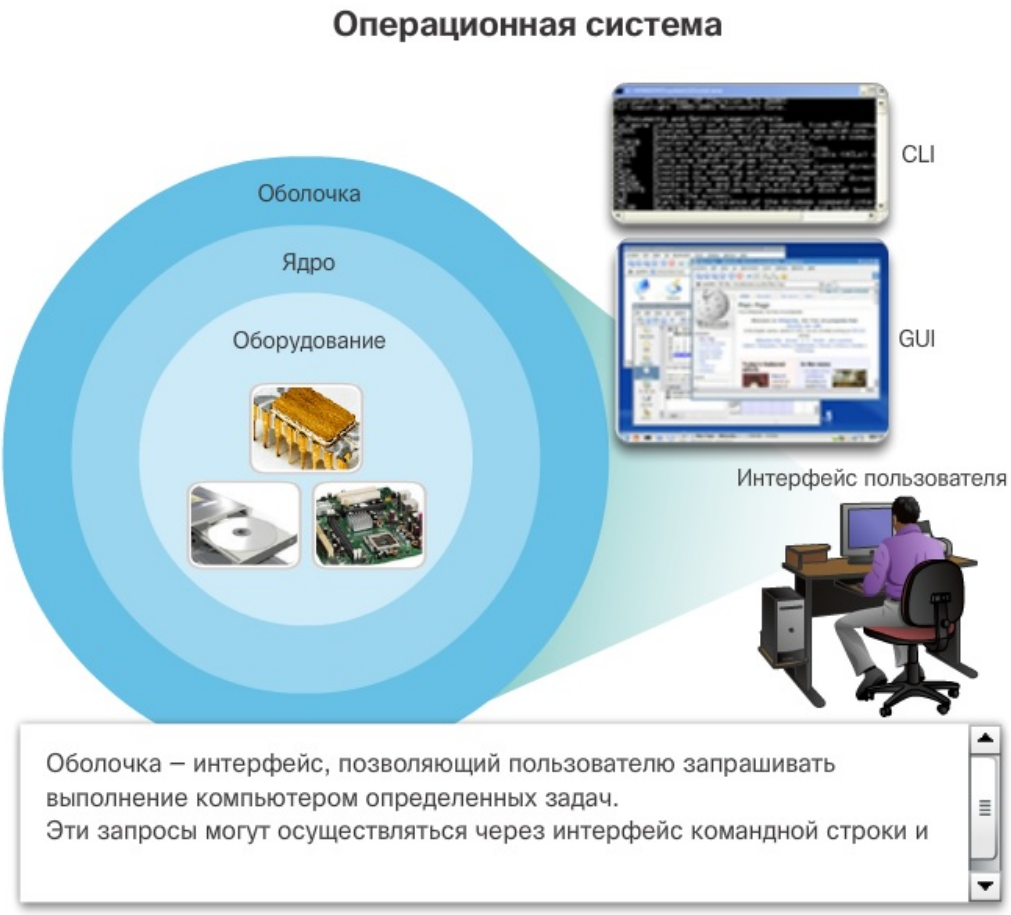


Рис. 1.12 – Схема взаимодействия операционной системы с оборудованием

Как показано на рисунке 1.12, часть ОС, которая непосредственно взаимодействует с аппаратным обеспечением компьютера, называется ядром. Часть, которая обеспечивает связь между приложениями и пользователем, называется оболочкой. Пользователь взаимодействует с оболочкой посредством интерфейса командной строки *(command-line interface, CLI)* или графического интерфейса пользователя *(graphical user interface, GUI).*

При использовании ***CLI*** происходит непосредственное обращение к системе в текстовом режиме путем ввода команд с клавиатуры в командной строке. Система выполняет команду, часто выводя выходные данные в текстовом формате. Для работы с CLI требуется передавать минимальное количество данных. Однако пользователь должен знать базовую структуру команд для управления системой.

Интерфейс GUI, такой как в ОС Windows, OS X, Apple iOS или Android, позволяет пользователю взаимодействовать с системой при помощи графических значков, меню и окон.

Однако GUI не всегда предоставляет все те возможности, что доступны при использовании CLI. Кроме того, в GUI может произойти сбой, он может быть недоступен или просто работать не так, как надо. Поэтому для обращения к сетевым устройствам обычно используется CLI. CLI – менее ресурсоемкий интерфейс, он работает гораздо устойчивее, чем GUI.

Сетевая операционная система, используемая на устройствах Cisco, называется операционной системой сетевого взаимодействия Cisco (IOS). Cisco IOS используется на большинстве устройств Cisco, независимо от их типа и размеров.

Примечание. Операционная система на домашних маршрутизаторах обычно называется микропрограммным обеспечением (прошивкой, firmware). Самый распространенный способ настройки домашнего маршрутизатора – использование GUI на основе веб-браузера.

Настройка сетевого оборудования корпоративного уровня, как правило, осуществляется с помощью командной строки CLI операционной системы устройства.

Способы доступа к коммутатору

Коммутатор с Cisco IOS может не иметь конфигурации, но при этом осуществлять передачу данных между двумя соединенными устройствами. После подключения двух ПК к коммутатору между этими компьютерами сразу будет установлено соединение.

Хотя коммутатор Cisco начнет работать немедленно, обычно рекомендуется настраивать начальные параметры. Существует несколько способов получить доступ к командной строке устройства для его настройки. Ниже приведены наиболее распространенные из них.

Консоль – это физический порт управления, обеспечивающий внеполосный доступ к устройству Cisco. Под внеполосным (Out-of-band, OOB) доступом понимается доступ по отдельному каналу, используемому исключительно в целях управления устройством. Преимущество использования консольного порта состоит в том, что *доступ к устройству возможен даже без настройки сетевых служб, например, во время первоначальной настройки сетевого устройства*. При выполнении начальной настройки к консольному порту устройства с помощью специального кабеля подключается компьютер с запущенной программой эмуляции терминала. С этого компьютера можно вводить команды для настройки коммутатора или маршрутизатора.

Secure Shell (SSH) – метод, позволяющий удаленно установить защищенное подключение CLI через виртуальный интерфейс по сети. В отличие от консольного подключения, для SSH-подключений на устройстве должны быть активны сетевые службы, включая активный интерфейс с настроенным адресом.

Telnet – это незащищенный протокол, позволяющий удаленно начать сеанс CLI через виртуальный интерфейс по сети. В отличие от SSH, Telnet не обеспечивает защищенное зашифрованное соединение. Данные для аутентификации пользователя, пароли и команды передаются по сети в виде простого текста.

Примечание. Некоторые устройства, такие как маршрутизаторы, также могут поддерживать устаревший вспомогательный порт (AUX), который раньше использовался, чтобы удаленно начать сеанс CLI с помощью модема. Аналогично консольному подключению порт AUX обеспечивает внеполосное подключение и не требует наличия работающих сетевых служб.

Существует несколько программ эмуляции терминала, используемых для подключения к сетевым устройствам при помощи последовательного подключения через консольный порт либо посредством подключения по протоколам SSH/Telnet. Вот несколько примеров таких программ:

- PuTTY;
- Tera Term;
- SecureCRT;
- OS X Terminal.

Эти программы позволяют работать эффективнее за счет регулировки размера окон, изменения размера шрифтов и цветовых схем.

Консольный порт коммутатора

Как уже было сказано выше, коммутатор в начальном своем состоянии (из коробки) не имеет конфигурации, и соответственно подключиться к нему используя сетевые службы (SSH или Telnet) невозможно. Поэтому первичная настройка осуществляется через консольный порт коммутатора (рис. 1.13).



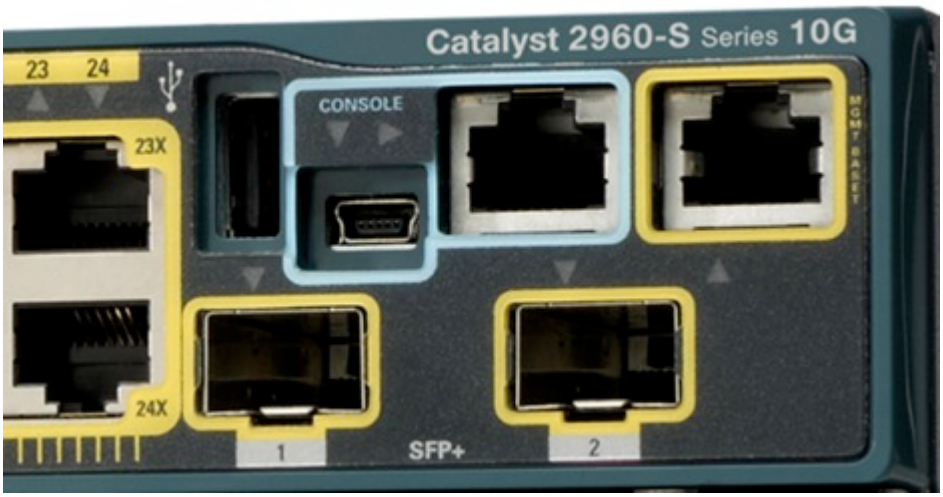


Рис. 1.13 – Консольный порт коммутатора
на разных устройствах

Подключение к консольному порту осуществляется с помощью специального консольного кабеля (рис. 1.14, 1.15).



Рис. 1.14 – Консольный кабель



Рис. 1.15 – Консольный кабель с адаптером COM-USB

В первом случае сторона консольного кабеля, которая подключается к ПК, имеет интерфейс RS232 (COM-порт). Поскольку на современных ПК данный порт за ненадобностью часто отсутствует, то производители стали делать консольные кабели сразу с адаптером COM-USB, такой адаптер можно купить отдельно (рис. 1.16).



Рис. 1.16 – Консольный кабель и адаптер COM-USB

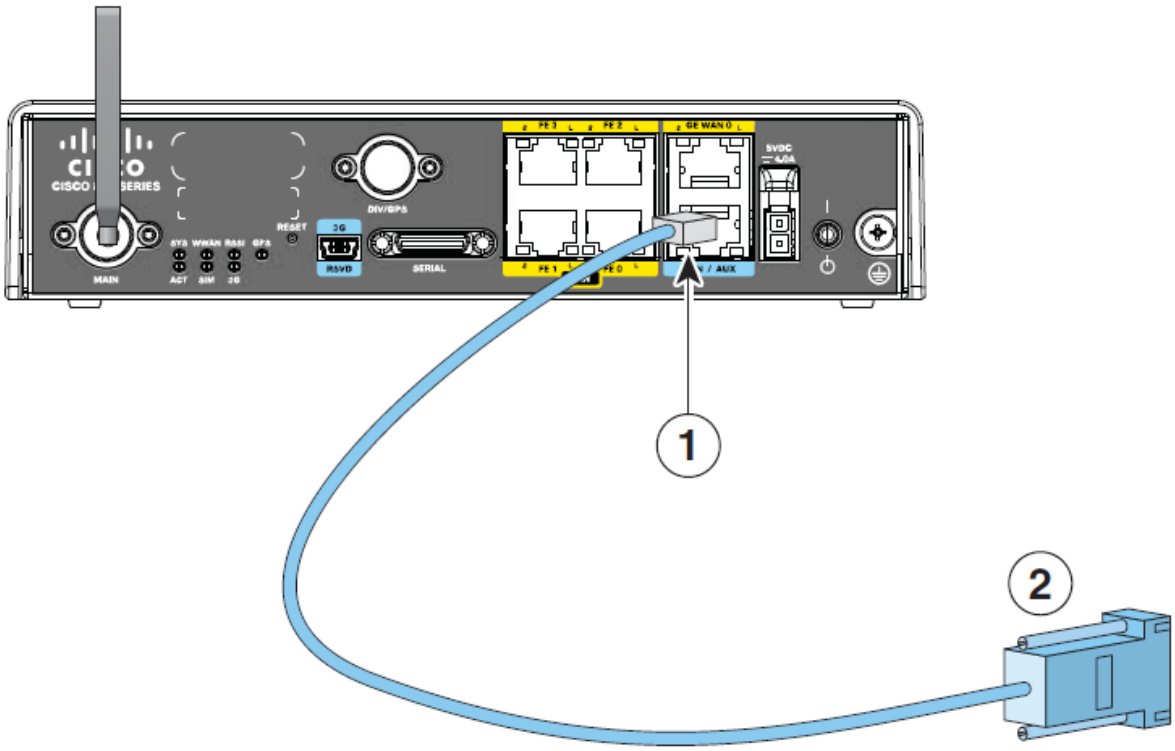


Рис. 1.17 – Схема подключения консольного кабеля к ПК

Packet Tracer. Советы по использованию справки и навигации

Packet Tracer – простая, универсальная программа для домашнего использования, которая поможет вам в освоении учебного курса CCNA компании Cisco. С помощью Packet Tracer можно экспериментировать с сетевым поведением, создавать сетевые модели и проводить анализ типа «что, если». В этом упражнении Вы подробно ознакомитесь с принципом работы относительно сложной сети с помощью некоторых функций Packet Tracer. При этом Вы узнаете, как пользоваться справкой и учебными руководствами. Вы также научитесь переключаться между различными режимами и рабочими областями.

Чтобы загрузить данную программу, вам необходимо перейти по ссылке: https://cloud.tusur.ru/index.php/s/iYi6iHfzZaPRLLw

Пройдите регистрацию на курс использования Packet Tracer и получите данную программу бесплатно для использования в учебных целях.

Packet Tracer – ключевой учебный инструмент, применяемый в следующих курсах Сетевой академии Cisco: IT Essentials, CCNA Routing and Switching, CCNA Security, Intro to Internet of Things (IoT) и Mobility Fundamentals. Инструкция по загрузке и запуску программы находится в электронном курсе (модуль «Контрольные и лабораторные работы»).

Packet Tracer: создание консольного соединения между ПК и коммутатором Cisco 2960

Процесс настройки коммутатора Cisco можно смоделировать в симуляторе Packet Tracer.

Сначала нажмем кнопку Switches, затем выберем коммутатор серии 2960 и поместим его в главное окно.

Теперь нам нужен компьютер. Нажмем на значок End Devices (Конечные устройства) и первое устройство – PC, то есть компьютер. Выберем его и тоже добавим в главное окно – простым щелчком.

Теперь у нас есть компьютер и коммутатор. Для моделирования начальной настройки коммутатора Cisco нам потребуется подходящий кабель. Нажмем на значок Connections (Подключения) и выберем консольный кабель, второй слева. Итак, мы выбираем консольный кабель. Затем на настольном компьютере выберем последовательный порт RS 232 и перетащим соединение на коммутатор 2960.

Щелкнем на коммутаторе и выберем консольный порт. Теперь мы соединили компьютер с коммутатором серии 2960, используя консольный кабель (он же rollover).

Итак, мы подключили последовательный кабель от компьютера к консольному порту. Теперь для начальной настройки коммутатора Cisco нам потребуется программа эмуляции терминала. Чтобы открыть ее, мы щелкнем на компьютере, затем выберем вкладку Desktop (Рабочий стол). Здесь показаны доступные приложения. Программа эмуляции терминалов

называется Terminal. Щелкнув по этому значку, Вы увидите те же параметры конфигурации терминала, которые используются в реальных программах эмуляции терминала, например в PuTTY или Tera Term. Как видите, скорость передачи данных, биты данных, контроль четности, стоповые биты и управление потоком уже настроены. Все, что нужно сделать, это нажать «ОК».

Теперь у нас есть терминальное подключение к коммутатору. Нажмем клавишу «Ввод». Как видите, теперь открылось окно ввода команд для управления коммутатором. Этот способ консольного доступа к коммутаторам и маршрутизаторам можно использовать при проверке навыков работы с Packet Tracer и подготовке к экзаменам в Packet Tracer. Есть и другой, более быстрый способ доступа к интерфейсу командной строки: щелкните по значку коммутатора или маршрутизатора, выберите вкладку CLI (Интерфейс командной строки). Как видите, при этом тоже открывается окно ввода команд.

Установка программы Packet Tracer

1. Скачайте программу Cisco Packet Tracer: https://cloud.tusur.ru/index.php/s/iYi6iHfzZaPRLLw

2. Установка программы (инструкция по загрузке и запуску программы находится в электронном курсе). Согласитесь с лицензионным соглашением (I agree the agreement).

3. Оставьте пути установки, размещения ярлыков программы и создание ярлыка на рабочем столе по умолчанию (Next, Next и Next) (рис. 1.19).

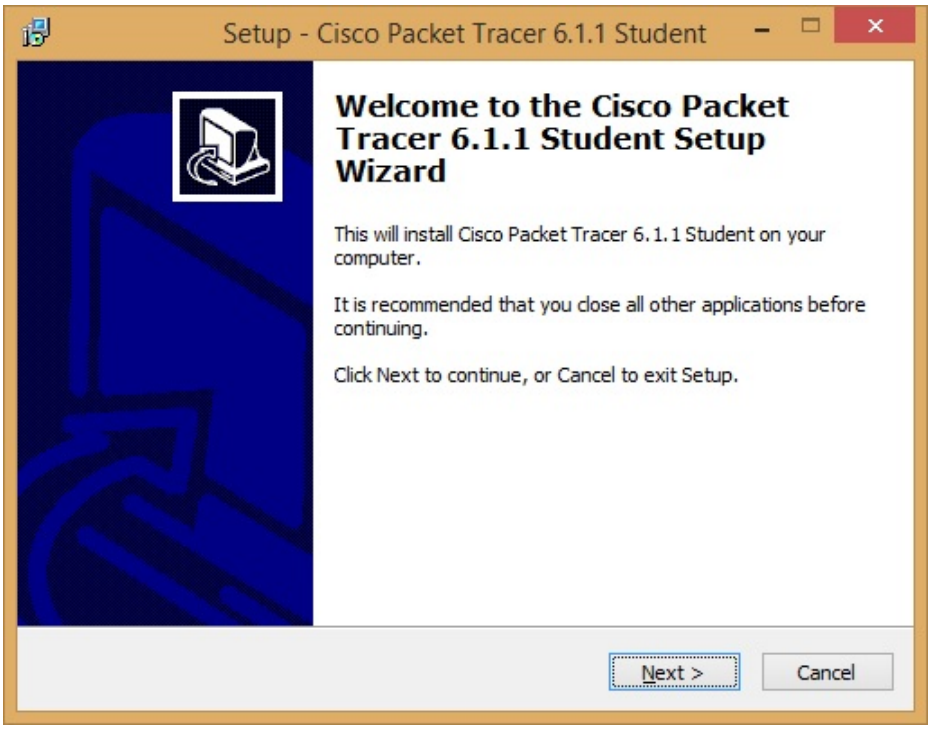


Рис. 1.19 – Начало установки программы Packet Tracer

4. Для установки программы нажмите Install (рис. 1.20).

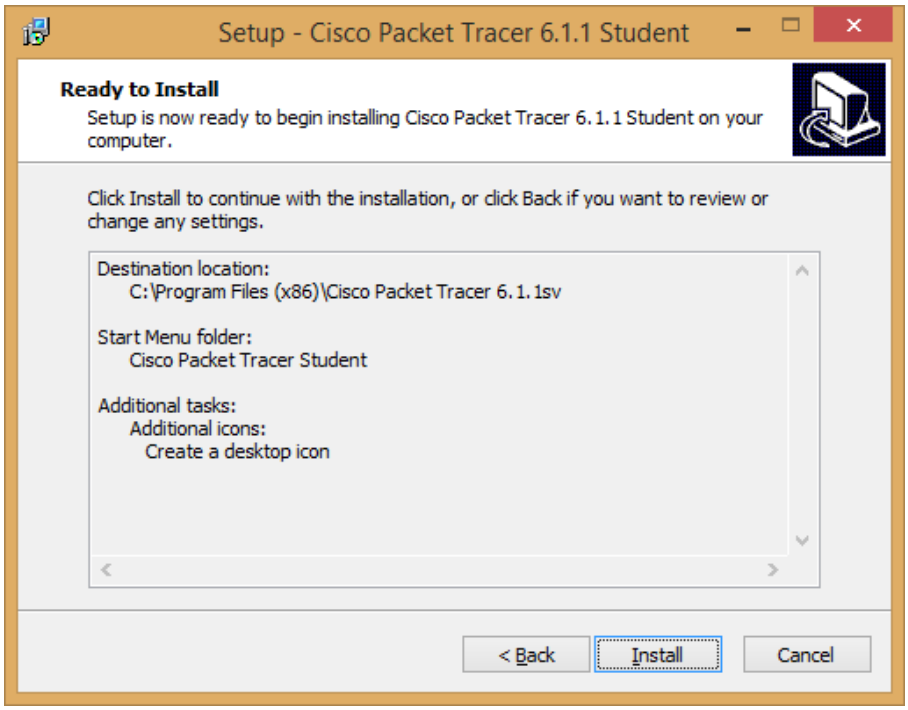


Рис. 1.20 – Установка программы Packet Tracer

5. После установки программы перезагрузите свой компьютер.

6. Сохранение результатов работы. Результаты работы в программе Packet Tracer необходимо сохранять в специальном формате pkz. Для этого, после завершения выполнения заданий зайдите в меню File – Save As PKZ (рис. 1.21).

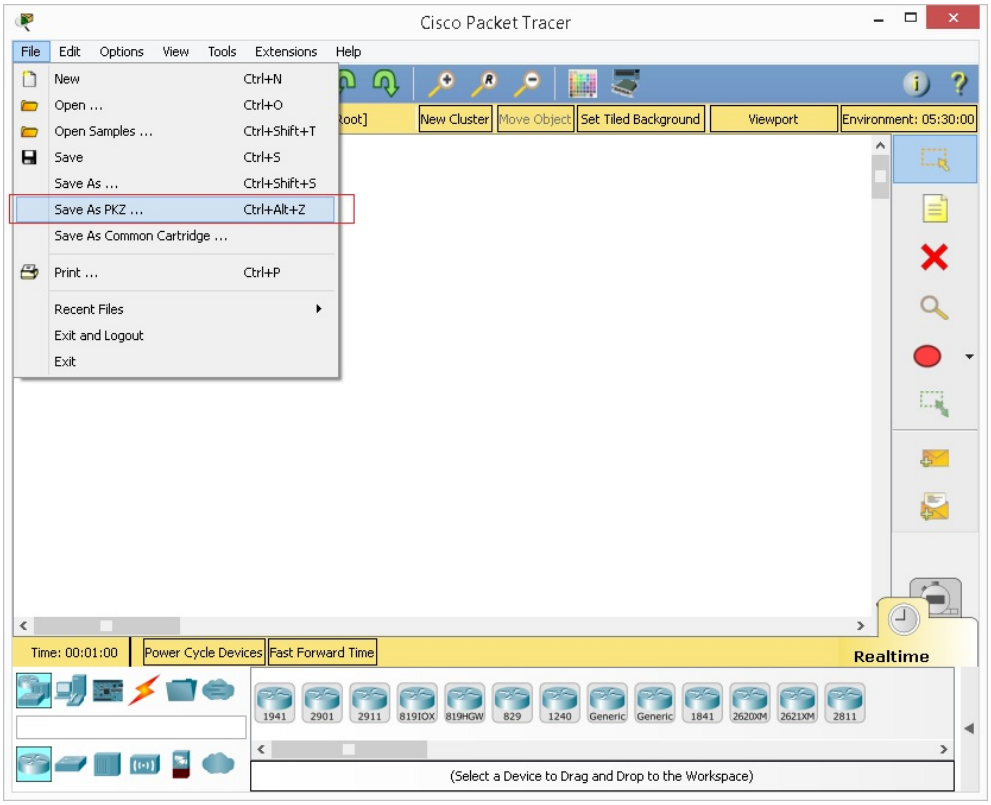


Рис. 1.21 – Сохранение результатов работы в формате pkz

Выберите место сохранения файла и нажмите Save. Данный файл необходимо будет отправить на проверку преподавателю вместе с отчетом по лабораторной работе.

2 ЛАБОРАТОРНАЯ РАБОТА № 1 «ПОДКЛЮЧЕНИЕ К КОММУТАТОРУ, ИЗУЧЕНИЕ СЕТЕВОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ КОММУТАТОРА»

В лабораторной работе № 1 Вы сможете на практике отработать навыки, необходимые для использования IOS, включая различные пользовательские режимы доступа, всевозможные режимы конфигурации, а также наиболее распространённые команды, которые Вы регулярно используете. Кроме того, Вы поработаете с контекстной справкой при настройке команды clock.

2.1 Задание

1. Подключение к коммутатору, доступ к командной строке и изучение справки.

2. Изучение режимов ввода.

3. Настройка часов.

2.2 Порядок выполнения работы

Часть 1. Базовые подключения, доступ к командной строке (CLI) и изучение справки (Help)

В части 1 этого задания Вам необходимо будет подключить ПК к коммутатору через консольное соединение и изучить функции справки, различные режимы ввода команд.

Шаг 1. Подключите PC1 к S1 с помощью консольного кабеля.

a. Щёлкните значок Connections (Соединения) (в виде молнии) в левом нижнем углу окна Packet Tracer.

b. Выберите светло-голубой консольный кабель, щёлкнув по нему. Указатель мыши примет вид разъёма со свисающим концом кабеля.

c. Щёлкните PC1. В окне будет показан вариант для подключения RS-232.

d. Перетащите другой конец консольного подключения к коммутатору S1 и щёлкните коммутатор, чтобы открыть список подключений.

e. Выберите консольный порт, чтобы завершить подключение.

Шаг 2. Установите сеанс диалога с коммутатором S1.

a. Щёлкните PC1 и откройте вкладку Desktop (Рабочий стол).

b. Щёлкните значок приложения Terminal. Проверьте правильность параметров по умолчанию, установленных для порта.

Каково значение параметра в битах в секунду?

c. Нажмите кнопку «OK».

d. В появившемся окне может быть показано несколько сообщений. В какой-либо части окна должно появиться сообщение Press RETURN to get started! (Нажмите клавишу «ВВОД», чтобы начать работу!) Нажмите клавишу «ВВОД».

Какое приглашение показано на экране?

Шаг 3. Изучите справку по IOS.

a. В IOS доступна справка по командам в зависимости от уровня работы. В данный момент отображается приглашение, называемое «пользовательским режимом», и устройство ожидает ввода команд. Самый простой способ вызова справки – ввести вопросительный знак (?) в приглашении, чтобы получить список команд.

S1> ?

Какая команда начинается с буквы «c»?

b. В командной строке введите t с вопросительным знаком в конце (?).

S1> t?

Какие отображаются команды?

c. В командной строке введите te с вопросительным знаком в конце (?).

S1> te?

Какие отображаются команды?

Такой тип справки называется контекстной; в ней предоставляются дополнительные сведения при расширении команд.

Часть 2. Изучение режимов ввода

В части 2 этого задания Вы переключитесь в привилегированный режим и выполните дополнительные команды.

Шаг 1. Войдите в привилегированный режим.

a. В командной строке введите вопросительный знак (?).

S1> ?

Какие из показанных данных описывают команду enable?

b. Введите en и нажмите клавишу TAB.

S1> en<Tab>

Что отображается после нажатия клавиши TAB?

Это называется завершением команды или завершением клавишей TAB. После ввода части команды с помощью клавиши TAB можно завершить ввод этой команды. Если введённых символов достаточно для уникального определения команды (например, как в случае с командой enable), оставшаяся часть будет введена автоматически.

Что произойдёт, если ввести te<Tab> в командной строке?

c. Введите команду enable и нажмите клавишу «ВВОД». Как изменилась строка приглашения?

d. Введите в строке вопросительный знак (?).

S1# ?

Ранее уже использовалась одна команда, которая началась с буквы «c» в пользовательском режиме. Сколько команд показано теперь, когда включён привилегированный режим? (Подсказка. Можно было ввести «c?» для вывода только команд, начинающихся с «c».)

Шаг 2. Войдите в режим глобальной конфигурации.

a. Одной из команд, доступных в привилегированном режиме и начинающихся с буквы «c», является configure. Введите команду полностью или только её часть, достаточную для завершения, клавишей «TAB», а затем нажмите «ВВОД».

S1# configure

Какое отобразилось сообщение?

b. Нажмите «ВВОД», чтобы принять параметр по умолчанию, заключённый в квадратные скобки [terminal].

Как изменилась строка приглашения?

c. Такой режим называется режимом глобальной конфигурации. Он будет более подробно рассмотрен в последующих интерактивных заданиях и лабораторных работах. А теперь вернитесь в привилегированный режим, введя команду exit или end либо нажав сочетание клавиш Ctrl + Z.

S1(config)# exit

S1#

Часть 3. Настройка часов

Шаг 1. Используйте команду clock.

a. Используйте команду clock, чтобы подробнее изучить справку и синтаксис команды. Введите show clock в привилегированном режиме.

S1# show clock

Какая информация отображается? Какой год отображается?

b. Используйте контекстную справку и команду clock, чтобы установить текущее время на коммутаторе. Введите команду clock и нажмите клавишу «ВВОД».

S1# clock<ВВОД>

Какая информация отображается?

c. IOS выдала сообщение % Incomplete command, которое означает, что для команды clock требуются дополнительные параметры. В справке можно получить дополнительные сведения о времени, если ввести после команды пробел и вопросительный знак (?).

S1# clock ?

Какая информация отображается?

d. Настройте время с помощью команды clock. Продолжайте изучение команды, выполняя по одному действию за один раз.

S1# clock set ?

Какая запрашивается информация?

Какие отобразятся сведения, если ввести только команду clock, не выполняя запрос справки с помощью вопросительного знака?

e. На основе данных, запрошенных с помощью команды clock set ?, введите время 15:00, используя 24-часовой формат. Проверьте, нужны ли дополнительные параметры.

S1# clock set 15:00:00 ?

Выходные данные содержат запрос на получение дополнительных сведений:

<1-31> Day of the month

MONTH Month of the year

f. Попробуйте установить дату 01/31/2035, используя запрошенный формат. Для этого может потребоваться запросить дополнительную справку. По окончании выполните команду show clock, чтобы отобразить параметры часов. Вывод команды должен иметь следующий вид:

S1# show clock

*15:0:4.869 UTC Tue Jan 31 2035

g. Если ваши выходные данные отличаются, попробуйте выполнить следующую команду:

S1# clock set 15:00:00 31 Jan 2035

Шаг 2. Изучите дополнительные командные сообщения.

a. IOS выводит различные данные для неправильных или неполных команд, в чём можно было убедиться в предыдущих разделах. Продолжайте работать с командой clock, чтобы изучить дополнительные сообщения, которые могут появиться в ходе обучения работы с IOS.

b. Введите следующую команду и запишите сообщение:

S1# cl

Какие возвращены данные?

S1# clock

Какие возвращены данные?

S1# clock set 25:00:00

Какие возвращены данные?

S1# clock set 15:00:00 32

Какие возвращены данные?

Результат сохраняется в формате pkz

3 ЛАБОРАТОРНАЯ РАБОТА № 2 «ИЗУЧЕНИЕ ТЕКУЩЕЙ КОНФИГУРАЦИИ КОММУТАТОРА И НАСТРОЙКА БАЗОВЫХ ПАРАМЕТРОВ КОММУТАТОРА»

В лабораторной работе № 2 необходимо настроить основные параметры коммутатора. Необходимо обеспечить безопасность доступа к интерфейсу командной строки (CLI) и портам консоли с помощью зашифрованных и текстовых паролей. Также изучите способы конфигурации сообщений, которые будут адресованы пользователям, выполняющим вход в систему коммутатора. Эти баннерные сообщения предупреждают пользователей о том, что несанкционированный доступ запрещён.

3.1 Задание

1. Проверка конфигурации коммутатора по умолчанию.
2. Настройка основных параметров коммутатора.
3. Настройка баннера MOTD.
4. Сохранение файлов конфигурации в NVRAM.
5. Настройка второго коммутатора.

3.2 Порядок выполнения работы

Часть 1. Проверка конфигурации коммутатора по умолчанию

Шаг 1. Войдите в привилегированный режим.

В привилегированном режиме доступны все команды коммутатора. Но в связи с тем, что многими из привилегированных команд задаются рабочие параметры, привилегированный доступ должен быть защищён паролем во избежание несанкционированного использования.

К привилегированному набору команд относятся те команды, которые содержатся в пользовательском режиме, а также команда configure, при помощи которой выполняется доступ к остальным командным режимам.

a. Нажмите S1 и откройте вкладку CLI. Нажмите «ВВОД».

b. Перейдите в привилегированный режим, выполнив команду enable.

Switch> enable

Switch#

Обратите внимание, что изменённая в конфигурации строка будет отражать привилегированный режим.

Шаг 2. Изучите текущую конфигурацию коммутатора.

a. Выполните команду show running-config.

Switch# show running-config

b. Ответьте на следующие вопросы.

Сколько у маршрутизатора интерфейсов FastEthernet?

Сколько у маршрутизатора интерфейсов Gigabit Ethernet?

Каков диапазон значений, отображаемых в vty-линиях?

Какая команда отображает текущее содержимое NVRAM?

Почему коммутатор отвечает сообщением startup-config is not present?

Часть 2. Настройка основных параметров коммутатора

Шаг 1. Задайте коммутатору имя.

Для настройки параметров коммутатора может потребоваться переключение между режимами настройки. Обратите внимание, как изменяется строка приглашения при переходе по разделам коммутатора.

Switch# configure terminal

Switch(config)# hostname S1

S1(config)# exit

S1#

Шаг 2. Защитите доступ к консоли.

Для обеспечения безопасного доступа к консоли перейдите в режим config-line и установите для консоли пароль letmein.

S1# configure terminal

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

S1(config)# line console 0

S1(config-line)# password letmein

S1(config-line)# login

S1(config-line)# exit

S1(config)# exit

%SYS-5-CONFIG_I: Configured from console by console

S1#

Для чего нужна команда login?

Шаг 3. Убедитесь, что доступ к консоли защищён.

Выйдите из привилегированного режима, чтобы убедиться, что для порта консоли установлен пароль.

S1# exit

Switch con0 is now available

Press RETURN to get started.

User Access Verification

Password:

S1>

Примечание. Если коммутатор не выводит запрос на ввод пароля, значит, Вы не настроили параметр login в шаге 2.

Шаг 4. Защитите доступ в привилегированный режим.

Установите для enable пароль c1$c0. Этот пароль ограничивает доступ к привилегированному режиму.

Примечание. Символ 0 в c1$c0 – это цифра ноль, а не буква «O». Этот пароль не будет действительным, пока Вы его не зашифруете в шаге 8.

S1> enable

S1# configure terminal

S1(config)# enable password c1$c0

S1(config)# exit

%SYS-5-CONFIG_I: Configured from console by console

S1#

Шаг 5. Убедитесь, что доступ к привилегированному режиму защищён.

a. Выполните команду exit ещё раз, чтобы выйти из коммутатора.

b. Нажмите «ВВОД», после чего вам будет предложено ввести пароль.

User Access Verification

Password:

c. Первый пароль относится к паролю консоли, который был задан для line con 0. Введите этот пароль, чтобы вернуться в пользовательский режим.

d. Введите команду для доступа к привилегированному режиму.

e. Введите второй пароль, который был задан для ограничения доступа к привилегированному режиму.

f. Проверьте конфигурацию, изучив содержимое файла running-configuration:

S1# show running-configuration

Обратите внимание, что пароли для консоли и привилегированного режима отображаются в виде обычного текста. Это может представлять собой угрозу безопасности, если за вашими действиями наблюдают со стороны.

Шаг 6. Настройте зашифрованный пароль для обеспечения безопасности доступа к привилегированному режиму.

Пароль для enable нужно заменить на новый зашифрованный пароль с помощью команды enable secret. Настройте для enable secret пароль itsa-secret.

S1# config t

S1(config)# enable secret itsasecret

S1(config)# exit

S1#

Примечание. Пароль enable secret переопределяет пароль enable. Если для коммутатора заданы оба пароля, для перехода в привилегированный режим нужно ввести пароль enable secret.

Шаг 7. Убедитесь, что в файл конфигурации добавлен пароль enable secret.

a. Введите команду show running-config ещё раз, чтобы проверить новый пароль enable secret.

Примечание. Команду show running-config можно сократить до

S1# show run

b. Что отображается при выводе пароля enable secret?

c. Почему пароль enable secret отображается не так, как он был настроен?

Шаг 8. Зашифруйте пароли enable и console.

Как было видно в шаге 7, пароль enable secret зашифрован, а пароли enable и console хранятся в виде обычного текста. Сейчас мы зашифруем эти открытые пароли с помощью команды service password-encryption.

S1# config t

S1(config)# service password-encryption

S1(config)# exit

Если установить на коммутаторе другие пароли, они будут храниться в файле конфигурации в виде обычного текста или в зашифрованном виде? Укажите причины.

Часть 3. Настройка баннера MOTD

Шаг 1. Настройте сообщение дня (MOTD).

В набор команд Cisco IOS входит команда, которая позволяет настроить сообщение, которое будет отображаться при входе в систему на коммутаторе. Это сообщение называется сообщением дня (MOTD). Текст баннера нужно заключить в двойные кавычки или использовать разделитель, отличный от любого символа в строке MOTD.

S1# config t

S1(config)# banner motd "This is a secure system. Authorized Access Only!"

S1(config)# exit

%SYS-5-CONFIG_I: Configured from console by console

S1#

В каких случаях будет отображаться этот баннер?

Для чего на всех коммутаторах настраивается баннер MOTD?

Часть 4. Сохранение файлов конфигурации в NVRAM

Шаг 1. Проверьте правильность конфигурации с помощью команды show run.

Шаг 2. Сохраните файл конфигурации.

Вы завершили настройку базовых параметров коммутатора. Теперь необходимо выполнить резервное копирование файла конфигурации в NVRAM и убедиться, что внесённые изменения не потерялись после перезагрузки системы и отключения питания.

S1# copy running-config startup-config

Destination filename [startup-config]?[Enter]

Building configuration...

[OK]

Какова самая короткая версия команды copy running-config startup-config?

Шаг 3. Изучите файл загрузочной конфигурации.

Какая команда отображает содержимое NVRAM?

Все ли внесённые изменения были записаны в файл?

Часть 5. Настройка коммутатора S2

Вы завершили настройку коммутатора S1. Теперь настройте коммутатор S2. Если Вы не можете вспомнить команды, вернитесь к частям 1–4.

Настройте для коммутатора S2 следующие параметры.

a. Имя устройства: S2.

b. Защитите доступ к консоли паролем letmein.

c. Установите для привилегированного режима пароль c1$c0, а в качестве enable secret – пароль itsasecret.

d. Настройте следующее сообщение для пользователей, выполняющих вход в систему на коммутаторе:

Authorized access only. Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law.

e. Зашифруйте все открытые пароли.

f. Проверьте правильность конфигурации.

g. Сохраните файл конфигурации, чтобы предотвратить его потерю в случае отключения питания коммутатора.

Результат сохраняется в формате pkz.

4 ЛАБОРАТОРНАЯ РАБОТА № 3 «РЕАЛИЗАЦИЯ БАЗОВОЙ СХЕМЫ ПОДКЛЮЧЕНИЯ»

В рамках лабораторной работы № 3 необходимо выполнить настройку основных параметров коммутатора. Затем необходимо настроить связность между устройствами, выполнив конфигурацию IP-адресации на коммутаторах и ПК. По завершении настройки IP-адресации вам необходимо будет выполнить различные команды show, чтобы проверить настройки, а также команду ping для проверки основных параметров подключения между устройствами.

4.1 Задание

1. Настройка основных параметров на коммутаторах.
2. Настройка ПК.
3. Настройка интерфейса управления коммутатором.
4. Проверка подключения к сети.

Таблица 4.1 – Исходные данные (таблица адресации)

Устройство	Интерфейс	IP-адрес	Маска подсети
S1	VLAN 1	192.168.1.253	255.255.255.0
S2	VLAN 1	192.168.1.254	255.255.255.0
PC1	Сетевой адаптер	192.168.1.1	255.255.255.0
PC2	Сетевой адаптер	192.168.1.2	255.255.255.0

4.2 Порядок выполнения работы

Часть 1. Настройка основных параметров на коммутаторах S1 и S2

Шаг 0. Соедините сетевые устройства.

a. Соедините коммутаторы S1 и S2 кроссоверным кабелем.

b. Подключите PC1 к S1, а PC2 к S2 прямым кабелем.

Выполните следующие действия на коммутаторах S1 и S2.

Шаг 1. Задайте коммутатору S1 имя узла.

a. Нажмите S1 и откройте вкладку CLI.

b. Введите соответствующую команду для настройки имени узла S1.

Шаг 2. Настройте пароли для консоли и привилегированного режима.

a. В качестве пароля консоли введите cisco.

b. В качестве пароля привилегированного режима введите class.

Шаг 3. Проверьте настройки паролей для коммутатора S1.

Как можно проверить правильность настройки паролей?

Шаг 4. Настройте сообщение дня (MOTD).

Введите соответствующий текст для предупреждения о несанкционированном доступе. Ниже представлен пример текста.

Authorized access only. Violators will be prosecuted to the full extent of the law.

Шаг 5. Сохраните файл конфигурации в NVRAM.

Какую команду необходимо для этого выполнить?

Шаг 6. Повторите шаги 1–5 для коммутатора S2.

Часть 2. Настройка ПК

Настройте IP-адреса для PC1 и PC2.

Шаг 1. Настройте IP-адреса на обоих ПК.

a. Нажмите PC1 и откройте вкладку Desktop (Рабочий стол).

b. Нажмите кнопку IP Configuration (Настройка IP). В верхней части таблицы адресации (Addressing Table) можно увидеть, что компьютер PC1

имеет IP-адрес 192.168.1.1 и маску подсети 255.255.255.0. Введите эти данные для PC1 в окне IP Configuration.

c. Повторите шаги 1a и 1b для компьютера PC2.

Шаг 2. Проверьте подключение к коммутаторам.

a. Нажмите PC1. Закройте окно IP Configuration, если оно открыто. На вкладке Desktop (Рабочий стол) нажмите Command Prompt (Командная строка).

b. Введите команду ping с IP-адресом коммутатора S1 и нажмите клавишу «ВВОД».

Packet Tracer PC Command Line 1.0

PC> ping 192.168.1.253

Успешно ли был обработан эхо-запрос? Поясните свой ответ.

Часть 3. Настройка интерфейса управления коммутатором

Настройте IP-адреса для коммутаторов S1 и S2.

Шаг 1. Настройте IP-адрес на коммутаторе S1.

Коммутаторы представляют собой устройства, соответствующие стандарту plug-and-play, то есть нет необходимости в выполнении дополнительных настроек перед их вводом в эксплуатацию. Коммутаторы пересылают данные между портами, используя MAC-адреса. Для чего тогда нужно настраивать IP-адреса?

Чтобы настроить IP-адрес на коммутаторе S1, используйте следующие команды:

S1 #configure terminal

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

S1(config)# interface vlan 1

S1(config-if)# ip address 192.168.1.253 255.255.255.0

S1(config-if)# no shutdown

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

S1(config-if)#

S1(config-if)# exit

S1#

Почему необходимо ввести команду no shutdown?

Шаг 2. Настройте IP-адреса на коммутаторе S2.

Используя данные из таблицы адресации, настройте IP-адрес для S2.

Шаг 3. Проверьте настройки IP-адресов на коммутаторах S1 и S2.

Команда show ip interface brief выводит сведения об IP-адресе, а также о состоянии всех портов и интерфейсов коммутатора. Для этого можно также использовать команду show running-config.

Шаг 4. Сохраните конфигурации для S1 и S2 в NVRAM.

С помощью какой команды можно сохранить файл конфигурации из ОЗУ в NVRAM?

Шаг 5. Проверьте подключение к сети.

Подключение к сети можно проверить с помощью команды ping. Очень важно, чтобы связность работала по всей сети. В случае сбоя необходимо предпринять соответствующее действие по устранению неполадок. Отправьте эхо-запросы на IP-адреса коммутаторов S1 и S2 с компьютеров PC1 и PC2.

a. Нажмите PC1 и откройте вкладку Desktop (Рабочий стол).

b. Нажмите Command Prompt (Командная строка).

c. Отправьте эхо-запрос на IP-адрес компьютера PC2.

d. Отправьте эхо-запрос на IP-адрес коммутатора S1.

e. Отправьте эхо-запрос на IP-адрес коммутатора S2.

Примечание. Аналогичную команду ping можно использовать в интерфейсе командной строки коммутатора и на компьютере PC2.

Все эхо-запросы должны быть успешными. Если для первого эхо-запроса было получено 80% ответов, повторите попытку. Теперь результат должен быть 100%. Позже Вы узнаете, почему первый запрос может показать сбой. Если проверить связь с устройствами не удаётся, проверьте конфигурацию на наличие ошибок.

Результат сохраняется в формате pkz.

5 ТРЕБОВАНИЯ К ОФОРМЛЕНИЯ ОТЧЕТА ПО РАБОТЕ

Оформление лабораторной работы должно соответствовать требованиям образовательного стандарта вуза ОС ТУСУР 01–2013 Работы студенческие по направлениям подготовки и специальностям технического профиля. Общие требования и правила оформления. Текст стандарта можно найти по ссылке: https://regulations.tusur.ru/documents/70

Рекомендуется следующее содержание отчета:

1) титульный лист;
2) задание на лабораторную работу;
3) введение;
4) основная часть;
5) заключение;
6) список использованных источников.

Введение должно содержать цель работы, описание ее значения.

Подготовка отчета о проделанной работе

На проверку присылается отчет по форме, указанной в приложении А для каждой лабораторной работы и файл выполненной работы в программе Packet Tracer в формате pkz.

ЛИТЕРАТУРА

Основная литература

1. Пуговкин, А. В. Сети передачи данных : учеб. пособие / А. В. Пуговкин. – Томск : Факультет дистанционного обучения ТУСУРа, 2015. – 138 с.

2. Пятибратов, А. П. Вычислительные системы, сети и телекоммуникации : учебник для вузов / А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко ; ред. А. П. Пятибратов. – 3-е изд., перераб. и доп. – М. : Финансы и статистика, 2006. – 558 с.

Дополнительная литература

1. Телекоммуникационные системы и сети : учеб. пособие для вузов : в 3 т. Т. 2 : Радиосвязь, радиовещание, телевидение / Г. П. Катунин [и др.] ; под общ. ред. В. П. Шувалова. – 2-е изд., испр. и доп. – М. : Горячая линия-Телеком, 2005. – 672 с.

2. Тепляков, И. М. Основы построения телекоммуникационных систем и сетей : учеб. пособие / И. М. Тепляков. – М. : Радио и связь, 2004. – 326 с.

Базы данных, информационно-справочные и поисковые системы

1. Сайт компании Cisco Systems [Электронный ресурс]. – Режим доступа: http://www.cisco.com (дата обращения: 13.03.2017).

2. Издательство «Открытые системы» [Электронный ресурс]. – Режим доступа: http://www.osp.ru (дата обращения: 13.03.2017).

3. CNews: интернет-издание о высоких технологиях [Электронный ресурс]. – Режим доступа: http://www.cnews.ru (дата обращения: 13.03.2017).

ПРИЛОЖЕНИЕ А

Формы отчетов по лабораторным работам

Отчет по лабораторной работе № 1

Вопрос	Ответ
Установите сеанс диалога с коммутатором S1. Каково значение параметра в битах в секунду при подключении по терминалу?	
Какое приглашение командной строки будет выведено на экран после установления терминального соединения и нажатия клавиши «ВВОД»? (Напишите слово и символ.)	
Изучите справку по IOS. Какая команда начинается с буквы «c»? Какие отображаются команды, если в командной сроке ввести **S1>te?** ?	
Изучение режимов ввода. S1> ? Какие из показанных данных описывают команду enable?	
b. Введите en и нажмите клавишу «TAB». S1> en<Tab> Что отображается после нажатия клавиши «TAB»?	
S1# ? Сколько команд показано теперь, когда включён привилегированный режим?	
Режим глобальной конфигурации. Как изменилась строка приглашения?	
Введите show clock в привилегированном режиме. S1# show clock Какая информация отображается? Какой год отображается?	

Отчет по лабораторной работе № 2

Вопрос	Ответ
Какой командной можно посмотреть текущую конфигурацию коммутатора?	
Изучите текущую конфигурацию коммутатора. Сколько у коммутатора интерфейсов FastEthernet? Сколько у коммутатора интерфейсов Gigabit Ethernet?	
Какими командами настраивается пароль для входа в привилегированный режим?	
Почему пароль enable secret отображается в конфигурации не так, как он был настроен?	
Какой командой зашифровываются все пароли в конфигурации коммутатора?	
Какова самая короткая версия команды copy running-config startup-config?	
Какая команда отображает содержимое NVRAM?	

Отчет по лабораторной работе № 3

Вопрос	Ответ
Как можно проверить правильность настройки паролей?	
Какой командой сохраняется конфигурация коммутатора?	
Поясните, почему после настройки ip-адресации на ПК успешно проходит эхо-запрос от PC1 до PC2?	
Почему после настройки виртуального интерфейса необходимо ввести команду no shutdown?	
Какими двумя командами можно проверить настройки IP-адресов на коммутаторах S1 и S2?	