МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Институт математики и компьютерных наук
кафедра Информационной безопасности

Шабалин Андрей Михайлович

«Компьютерные сети»

Лабораторный практикум для обучающихся
по направлению подготовки
10.03.01 «Информационная безопасность» профиль
«Безопасность компьютерных систем»

для обучающихся по специальности
10.05.03 «Информационная безопасность автоматизированных систем (специалитет)»
специализация «Безопасность открытых информационных систем»
10.05.01 «Компьютерная безопасность (специалитет)» специализация
«Безопасность компьютерных систем и сетей» форма обучения очная

Тюмень 2020

Введение

Дисциплина «Компьютерные сети» имеет целью изложение истории развития мировой и отечественной мысли в области коммуникаций, а также истории защиты информации в средствах коммуникации.

Задачи курса - изучение:

- основных этапов истории развития коммуникаций терминологии;
- истории аналоговой коммуникации;
- истории и тенденции развития цифровых коммуникаций;
- основных технологий цифровых коммуникаций и их защищенность

В результате обучения студенты должны:

- знать свойства информации, подлежащие закрытию;
- знать этапы развития средств и технологий коммуникаций, историю развития информационного противоборства в России и мире
- знать основные технологии передачи цифровой информации;
- знать назначение основных устройств (маршрутизаторов, коммутаторов) обеспечивающих передачу цифровой информации.
- знать основные стандарты, используемые при передаче цифровой информации; - знать основные технологии защиты информации.
- ориентироваться в истории технологий передачи информации, методах защиты информации в контексте исторического развития.
- создавать и настраивать LAN сети.
- создавать, безопасное подключение LAN к Интернет.

Лабораторная работа 1
Packet Tracer. Навигация по IOS

Задачи

Часть 1. Создание основных подключений, доступ к интерфейсу командной строки (CLI) и изучение справки

Часть 2. Изучение режимов EXEC

Часть 3. Настройка часов

Общие сведения и сценарий

В этом упражнении вы сможете на практике отработать навыки, необходимые для навигации по операционной системе Cisco IOS, включая различные пользовательские режимы доступа, всевозможные режимы конфигурации, а также наиболее распространенные команды, используемые регулярно. Кроме того, вы поработаете с контекстной справкой при настройке команды **clock**. **Инструкции**

Часть 1. Создание основных подключений, доступ к интерфейсу командной строки (CLI) и изучение справки

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

a. Нажмите значок **Connections** (Подключения) (в виде молнии) в левом нижнем углу окна Packet Tracer.

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

c. Нажмите **PC1**. В окне будет показан вариант для подключения RS-232. Подключите кабель к порту RS-232.

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

e. Выберите порт **Console** (Консольный), чтобы завершить подключение. **Шаг 2. Установите сеанс диалога с коммутатором S1.**

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

b. Нажмите значок приложения **Terminal** (Терминал). Проверьте правильность параметров конфигурации портов, заданных по умолчанию.

Каково значение параметра в битах в секунду? с.

Нажмите **OK**.

d. В появившемся окне может отображаться несколько сообщений. В окне должно появиться сообщение **Press RETURN to get started!** (Нажмите ВОЗВРАТ, чтобы начать работу). Нажмите клавишу ввода.

Какое приглашение появляется 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 **User EXEC** (Пользовательский режим EXEC), и устройство ожидает ввода команды. Самый простой способ вызова справки — ввести вопросительный знак (?) в командной строке, 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?

В командной строке введите te с вопросительным знаком в конце (?).
S1> **te?**

Какие отображаются команды?

Справка такого вида называется контекстной. Чем подробнее вводятся команды, тем больше сведений может предоставить справка. **Часть 2. Изучение режимов EXEC**

В части 2 этого упражнения вы переключитесь в привилегированный режим EXEC и выполните дополнительные команды.

Шаг 1. Войдите в привилегированный режим EXEC.

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 завершение нажатием клавиши TAB). Введя часть команды, можно нажать клавишу **TAB** и завершить частичный ввод этой команды. Если введенных символов достаточно для уникального определения команды (например, как в случае с командой **enable**), оставшаяся часть будет введена автоматически.

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

c. Введите команду **enable** и нажмите клавишу ввода.

Как изменилась командная строка?

d. Введите в строке вопросительный знак (**?**). S1# **?**

В пользовательском режиме EXEC только одна команда начинается с буквы «c».

Сколько команд показано теперь, когда включен привилегированный режим EXEC? (**Совет**. Можно ввести «c?», чтобы отобразить только команды, начинающиеся с буквы «c».) **Шаг 2. Войдите в режим глобальной настройки.**

a. В привилегированном режиме EXEC одна из команд, начинающихся с буквы «c», — **configure**. Введите либо команду полностью, либо столько символов, сколько будет нужно для уникального определения команды. Нажмите клавишу <**Tab**>, чтобы выполнить команду, и нажмите клавишу ввода. S1# **configure**

Какое появилось сообщение?

b. Нажмите клавишу ввода, чтобы принять параметр по умолчанию, заключенный в квадратные скобки, —**[terminal]**.

Как изменилась командная строка?

c. Такой режим называется режимом глобальной конфигурации. Он будет более подробно рассмотрен в последующих упражнениях и лабораторных работах. А теперь вернитесь в

привилегированный режим EXEC, введя команду **end** или **exit** либо нажав клавиши **Ctrl+Z**. S1(config)# **exit**

S1#

Чассть3. Настройка часов

Шаг 1. Используйте команду clock.

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

S1# **show clock**

Какая информация отображена? Какой год отображается?

b. Используйте контекстную справку и команду **clock**, чтобы установить текущее время на коммутаторе. Введите команду **clock** и нажмите клавишу ввода. S1# **clock<ENTER>**

Какая информация отображена?

c. IOS вернет сообщение «% Incomplete command». Это означает, что для команды **clock** требуются дополнительные параметры. В справке можно получить дополнительные сведения, если ввести после команды пробел и вопросительный знак (?).

S1# **clock ?**

Какая информация отображена?

d. Настройте время с помощью команды **clock set**. Продолжайте выполнять команду поэтапно.

S1# **clock set ?**

Какая запрашивается информация?

Какие отобразятся сведения, если ввести только команду **clock set**, не запрашивая справку с помощью вопросительного знака?

e. Взяв за основу сведения, запрошенные при помощи команды **clock set ?**, введите время 15:00 в 24-часовом формате (15:00:00). Проверьте, нужны ли дополнительные параметры. S1#

clock set 15:00:00 ?

Система возвращает запрос на получение дополнительных сведений.

<1-31> Day of the month MONTH

Month of the year

f. Попробуйте установить дату 31 января 2035 г., используя запрошенный формат. Для этого может потребоваться запросить дополнительную информацию с помощью контекстной справки. По окончании выполните команду **show clock**, чтобы отобразить настройку часов. В результате на экране должны отобразиться следующие данные.

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. В случае ввода неправильных или неполных команд, IOS выводит на экран различные сообщения. Продолжайте работать с командой **clock**, чтобы изучить дополнительные сообщения, которые могут появиться в ходе обучения работе с IOS.

b. Введите следующую команду и запишите сообщение. S1# **cl<tab>**

Какие возвращены данные?

S1# **clock**

Какие возвращены данные?

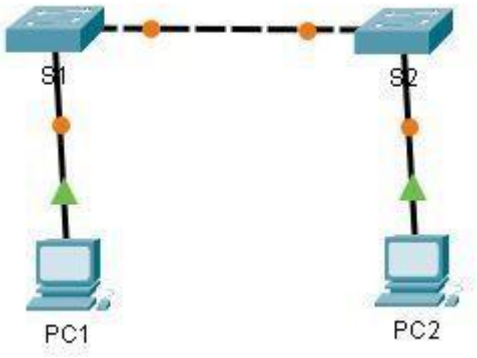
S1# **clock set 25:00:00**

Какие возвращены данные?

S1# **clock set 15:00:00 32**

Какие возвращены данные?

Лабораторная работа 2
Packet Tracer - Configure Initial Switch Settings



Задачи

Часть 1. Проверка конфигурации коммутатора по умолчанию
Часть 2. Настройка основных параметров коммутатора
Часть 3. Настройка баннера MOTD (сообщения дня)
Часть 4. Сохранение файлов конфигурации в NVRAM
Часть 5. Настройка коммутатора S2

Общие сведения и сценарий

В этом упражнении вы настроите базовые параметры коммутатора. Затем вам будет необходимо обеспечить безопасность доступа к интерфейсу командной строки (CLI) и портам консоли с помощью зашифрованных и текстовых паролей. Вы также научитесь настраивать сообщения для пользователей, выполняющих вход в систему коммутатора. Эти баннеры также предупреждают пользователей о том, что несанкционированный доступ запрещен. **Примечание. В Packet Tracer, коммутатор Catalyst 2960 использует IOS версии 12.2 по умолчанию.** При необходимости версию IOS можно обновить с файлового сервера в топологии Packet Tracer. После этого коммутатор может быть настроен на загрузку до версии IOS 15.0, если требуется эта версия.

Инструкции

Часть 1. Проверка конфигурации коммутатора по умолчанию Шаг

1. Войдите в привилегированный режим EXEC.

Привилегированный режим EXEC дает доступ ко всем командам коммутатора. Но поскольку многие привилегированные команды задают рабочие параметры, привилегированный доступ должен быть защищен паролем во избежание несанкционированного использования.

Набор привилегированных команд EXEC включает в себя команды, доступные в пользовательском режиме EXEC, множество дополнительных команд и команду **configure**, с помощью которой обеспечивается доступ к режимам конфигурации.

a. Щелкните S1 и откройте вкладку CLI. Нажмите клавишу ввода.
b. Перейдите в привилегированный режим EXEC, выполнив команду enable.

Switch> **enable**

Switch# Обратите внимание, что командная строка изменилась, указывая на привилегированный режим EXEC. **Шаг 2. Изучите текущую конфигурацию коммутатора.**

Введите команду show running-config.

Switch# **show running-config**

Ответьте на следующие вопросы:

Сколько у коммутатора интерфейсов Fast Ethernet?

Сколько у коммутатора интерфейсов Gigabit Ethernet?

Каков диапазон значений, отображаемых в vty-линиях?

Какая команда отображает текущее содержимое энергонезависимого ОЗУ (NVRAM)?
Почему коммутатор отвечает сообщением startup-config is not present? **Часть 2. Настройка основных параметров коммутатора Шаг 1. Присвойте коммутатору имя.**

Для настройки параметров коммутатора, возможно, потребуется переключаться между режимами настройки. Обратите внимание, как изменяется командная строка при переходе по разделам меню коммутатора.

Switch# **configure terminal**
Switch(config)# **hostname S1**
S1(config)# **exit**
S1#

Шаг 2. Обеспечьте безопасный доступ к консоли.

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

S1# **configure terminal**
Введите построчно команды настройки. В конце нажмите 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 защищен.

Выйдите из привилегированного режима, чтобы убедиться, что для консольного порта 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. Обеспечьте безопасный доступ к привилегированному режиму.

Установите для **enable** пароль **c1$c0**. Этот пароль ограничивает доступ к привилегированному режиму. Примечание. **Символ** 0 **в** c1$c0 **— это ноль, а не заглавная буква «O». Это пароль будет считаться неверным, пока вы не зашифруете его 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 защищен.

a. Выполните команду **exit** еще раз, чтобы выйти из коммутатора.
b. Нажмите **<клавишу ввода>**, после чего вам будет предложено ввести пароль. User Access Verification Password:
c. Первый пароль — это пароль для консоли, который был задан для **line con 0**. Введите этот пароль, чтобы вернуться в пользовательский режим EXEC.
d. Введите команду для доступа к привилегированному режиму.
e. Введите второй пароль, который был задан для ограничения доступа к привилегированному режиму EXEC.
f. Проверьте конфигурацию, изучив содержимое файла running-configuration:

S1# **show running-config**

Обратите внимание, что пароли для консоли и привилегированного режима отображаются в виде обычного текста. Это может представлять угрозу безопасности, если кто-то смотрит через ваше плечо или

получает доступ к конфигурационным файлам, хранящимся в резервной копии. **Шаг 6. Настройте зашифрованный пароль для доступа к привилегированному режиму.**

Пароль для enable нужно заменить на новый зашифрованный пароль с помощью команды **enable secret**. Установите для enable secret пароль **itsasecret**.

S1# **config t**
S1(config)# **enable secret itsasecret**
S1(config)# **exit**
S1#

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

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

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

Примечание. **Команду** show running-config **можно сократить до**

S1# **show run**

Что отображается в качестве пароля enable secret?

Почему пароль enable secret отображается не так, как было задано?

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 passwordencryption**.

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? Дайте пояснение.

Часть 3. Настройка баннера MOTD

Шаг 1. Настройте баннер MOTD (сообщения дня).

В набор команд Cisco IOS входит команда, позволяющая настроить сообщение, которое будут видеть все, кто входит в систему на коммутаторе. Это сообщение называется сообщением дня или баннером MOTD (message of the day). 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#

Когда будет отображаться этот баннер?

Зачем на всех коммутаторах должен быть баннер MOTD?

Часть 4. Сохраните и проверьте файлы конфигурации на NVRAM.

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

Сохраните файл конфигурации. Вы завершили основную настройку коммутатора. Теперь выполните резервное копирование файла конфигурации в NVRAM и убедитесь, что внесенные изменения не были потеряны при перезагрузке системы или отключении 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**?

Изучите файл загрузочной конфигурации.

Какая команда отображает содержимое NVRAM?

Все ли внесенные 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 в качестве пароля enable **c1$c0**, а в качестве пароля enable secret — **itsasecret**.
d. Настройте соответствующее сообщение для тех, кто вошел в коммутатор.
e. Зашифруйте все открытые пароли.
f. Проверьте правильность конфигурации.
g. Сохраните файл конфигурации, чтобы предотвратить его потерю в случае отключения питания коммутатора.

Лабораторная работа 3
Packet Tracer. Создание основных подключений

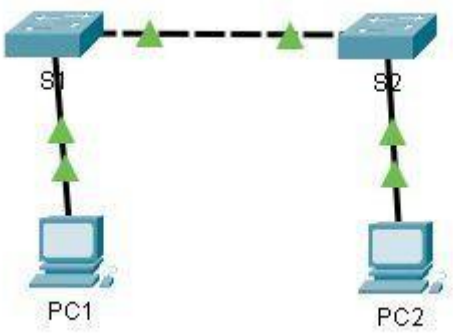


Таблица адресации

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	NIC	192.168.1.1	255.255.255.0
PC2	NIC	192.168.1.2	255.255.255.0

Цели

Часть 1. Настройка основных параметров коммутаторов S1 и S2
Часть 2. Настройка ПК
Часть 3. Настройка интерфейса управления коммутатором

Общие сведения

В этом упражнении вы сначала создадите базовую конфигурацию коммутатора. Затем вы создадите основные подключения, настроив IP-адресацию на коммутаторах и ПК. Завершив настройку IPадресации, вы будете использовать различные команды **show**, чтобы проверить настройки, а также команду **ping** для проверки основных подключений между устройствами.

Инструкции

Часть 1. Настройка основных параметров коммутаторов S1 и S2

Выполните следующие действия на коммутаторах S1 и S2. **Шаг 1.**

Настройте имя узла для коммутатора S1.

a. Щелкните S1, а затем вкладку CLI.
b. Введите нужную команду, чтобы присвоить узлу имя S1.

Шаг 2. Настройте пароли для консоли и привилегированного режима EXEC.

a. В качестве пароля консоли используйте слово **cisco**.
b. В качестве пароля привилегированного режима EXEC используйте слово **class**.

Шаг 3. Проверьте пароли, настроенные для S1.

Как можно проверить правильность настройки паролей? **Шаг 4. Настройте баннер MOTD (сообщение дня).** Введите текст 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 для обоих ПК.

a. Щелкните PC1 и откройте вкладку Desktop (Рабочий стол).
b. Щелкните IP Configuration (Настройка IP-адресов). В таблице адресации выше можно увидеть, что PC1 назначен IP-адрес 192.168.1.1 и маска подсети 255.255.255.0. Введите эти данные для PC1 в окне IP Configuration (Настройка IP-адресов).
c. Повторите шаги 1a и 1b для PC2.

Шаг 2. Проверьте связь с коммутаторами.

a. Щелкните PC1. Закройте окно IP Configuration (Настройка IP-адресов), 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**

Удалось ли создать новую папку? Дайте пояснение.

Часть 3. Настройка интерфейса управления коммутатором

Настройте IP-адрес для коммутаторов S1 и S2. **Шаг 1.**

Настройте IP-адрес для коммутатора S1.

Коммутаторы можно использовать в режиме «подключи и работай». Это значит, что их необязательно настраивать для работы. Коммутаторы пересылают данные между портами по MAC-адресам.

Для чего тогда нужно настраивать IP-адреса?

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

configure terminal
Введите построчно команды настройки. В конце нажмите 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#

Зачем вы вводите команду **no shutdown**?

Шаг 2. Настройте IP-адреса для коммутатора 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 настройки S1 и S2 в NVRAM.

Какая команда сохраняет файл конфигурации из RAM в NVRAM? **Шаг**

5. Проверьте подключение к сети.

Подключение к сети можно проверить с помощью команды **ping**. Очень важно, чтобы подключения работали во всей сети. В случае сбоя необходимо устранить неполадку. Проверьте связь коммутаторов S1 и S2 с компьютерами PC1 и PC2.

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

b. Щелкните Command Prompt (Командная строка).
c. С помощью команды ping проверьте доступность IP-адреса компьютера PC2.
d. С помощью команды ping проверьте доступность IP-адреса коммутатора S1.
e. С помощью команды ping проверьте доступность IP-адреса коммутатора S2.

Примечание. Команду **ping** можно использовать в интерфейсе командной строки коммутатора и на PC2. Все проверки должны быть пройдены успешно. Если результат первой проверки — 80 %, повторите попытку. Теперь результат должен быть 100 %. Позже вы узнаете, почему первая проверка иногда завершается неудачно. Если проверить связь с устройствами не удается, проверьте конфигурацию на наличие ошибок.

Лабораторная работа 4
Packet Tracer - Basic Switch and End Device Configuration

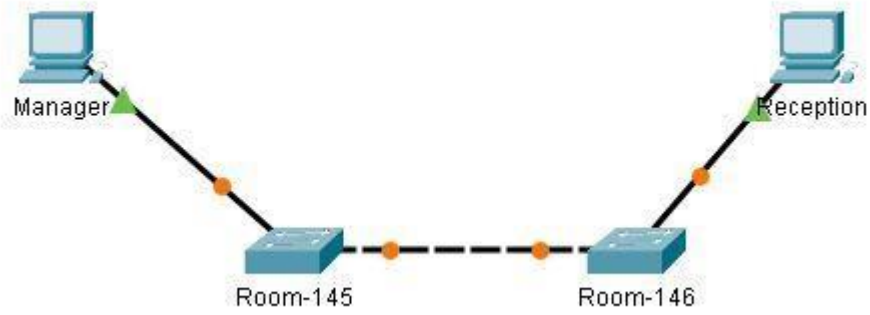


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
[[S1Name]]	VLAN 1	Коммутатор [[S1Add]]	255.255.255.0
[[S2Name]]	VLAN 1	Коммутатор [[S2Add]]	255.255.255.0
[[PC1Name]]	NIC	[[PC1Add]]	255.255.255.0
[[PC2Name]]	NIC	[[PC2Add]]	255.255.255.0

Цели

- Настроить имена узлов и IP-адреса на двух коммутаторах под управлением операционной системы Cisco IOS с помощью интерфейса командной строки (CLI).
- Используя команды Cisco IOS, задать параметры доступа или ограничьте доступ к конфигурации устройства.
- С помощью команд IOS сохранить текущую конфигурацию.
- Задать двум хост-устройствам IP-адреса.
- Проверить подключение между двумя оконечными устройствами (ПК).

Сценарий

Менеджер попросил вас, нового специалиста по обслуживанию локальных сетей, продемонстрировать навыки настройки небольшой локальной сети. Вам предстоит настроить исходные параметры на двух коммутаторах под управлением Cisco IOS, а также настроить параметры IP-адресации на узлах для создания сквозного подключения. Необходимо использовать два коммутатора и два узла (ПК) в активной сети с кабельным подключением.

Инструкции

Настройте устройства в соответствии с приведенными ниже требованиями.

Требования

- Используйте консольное подключение для доступа к каждому коммутатору. Задайте коммутаторам имена **[[S1Name]]** и **[[S2Name]]**.
- Используйте пароль **[[LinePW]]** для всех линий. Используйте скрытый пароль **[[SecretPW]]**. Зашифруйте все незашифрованные пароли.
- Настройте баннер MOTD (сообщения дня).
- Настройте адресацию для всех устройств в соответствии с таблицей адресации.
- Сохраните настройки. Убедитесь в наличии соединения между всеми устройствами.

Примечание. Нажмите **Check Results** (Проверить результаты), чтобы увидеть результаты выполненных настроек. Нажмите **Reset Activity** (Сброс упражнения), чтобы создать новый набор требований. Если вы нажмете эту кнопку до того, как завершите выполнение упражнения, все настройки будут потеряны.
ID: [[indexNames]][[indexPWs]][[indexAdds]][[indexTopos]]

Лабораторная работа 5

Packet Tracer - Изучение моделей TCP/IP и OSI в действии

Задачи

Часть 1. Изучение HTTP-трафика

Часть 2. Отображение элементов семейства протоколов TCP/IP

Общие сведения

Данное упражнение по моделированию — первый шаг на пути к пониманию принципов работы пакета проколов TCP/IP и его взаимосвязи с моделью OSI. Режим моделирования позволяет просматривать содержимое пересылаемых по сети данных на каждом из уровней.

По мере продвижения данных по сети они разбиваются на более мелкие фрагменты и идентифицируются таким образом, чтобы их можно было воссоединить по прибытию в пункт назначения. Каждый фрагмент получает собственное имя (единица данных протокола — PDU) и ассоциируется с конкретным уровнем моделей TCP/IP и OSI. Режим моделирования программы Packet Tracer позволяет просматривать все уровни и относящиеся к ним PDU. Ниже описана последовательность шагов пользователя для запроса веб-страницы с веб-сервера с помощью установленного на клиентском ПК веб-браузера.

Хотя большая часть показанной на экране информации будет подробнее рассмотрена далее, это даст вам возможность ознакомиться с возможностями программы Packet Tracer, а также наглядно рассмотреть процесс инкапсуляции.

Инструкции

Часть 1. Изучение HTTP-трафика

В части 1 данного упражнения вы будете использовать программу Packet Tracer (PT) в режиме моделирования для генерирования веб-трафика и изучения протокола HTTP.

Шаг 1. Перейдите из режима реального времени в режим моделирования.

В правом нижнем углу интерфейса Packet Tracer находятся вкладки для переключения между режимами **Realtime** (режим реального времени) и **Simulation** (режим моделирования). PT всегда запускается в режиме **реального времени**, в котором сетевые протоколы работают с реалистичными значениями времени. Однако широкие возможности Packet Tracer позволяют пользователю «остановить время», переключившись в режим моделирования. В режиме моделирования пакеты отображаются как анимированные конверты, временем управляют события и пользователи могут пошагово переходить от одного сетевого события к другому.

a. Щелкните значок режима **Simulation** для переключения из режима **реального времени** в режим **моделирования**.

b. Выберите в списке **Event List Filters** (Фильтры списка событий) пункт **HTTP**. 1) HTTP в этот момент уже может быть единственным видимым событием. При необходимости нажмите кнопку **«Редактировать фильтры** » в нижней части панели моделирования, чтобы отобразить доступные видимые события. Установите или снимите флажок **Show All/None**

(Показать все/ничего) и обратите внимание на то, как изменится состояние установленных и снятых флажков.

2) Щелкайте флажок **Show All/None** до тех пор, пока все флажки не будут сняты, а затем выберите **HTTP**. Щелкните X в правом верхнем углу окна, чтобы закрыть окно **«Редактировать фильтры»** . В разделе видимых событий теперь отображается только HTTP.

Шаг 2. Сгенерируйте веб-трафик (HTTP).

На данный момент панель моделирования пуста. В верхней части панели моделирования видны наименования шести столбцов списка событий. По мере генерации и продвижения трафика в списке будут появляться события.

Примечание. Веб-сервер и веб-клиент показаны на левой панели. Размер панели можно изменить, если навести указатель на полосу прокрутки и, когда он примет вид двунаправленной стрелки, перетащить его влево или вправо.

a. Щелкните **Web Client** (Веб-клиент) на крайней левой панели.
b. Щелкните вкладку **Desktop** (Рабочий стол), затем щелкните значок **Web Browser** (Веб-браузер), чтобы открыть веб-браузер.
c. В поле URL введите адрес **www.osi.local** и нажмите кнопку **Go**.

   Поскольку время в режиме моделирования привязано к событиям, для отображения событий в сети необходимо использовать кнопку **Capture/Forward** (Захват/вперед). Кнопка движения вперед по захваченым пакетам расположена в левой части синей полосы, которая находится под окном топологии. Из трех кнопок, эта самая правая.
d. Нажмите кнопку **Capture/Forward** четыре раза. В списке событий должны быть четыре события.

Посмотрите на страницу веб-клиента в веб-браузере. Что-нибудь изменилось?

Шаг 3. Изучите содержимое HTTP-пакета.

a. Щелкните первый цветной квадрат в столбце **Type** списка событий **Event List**. Вам может понадобиться развернуть **панель моделирования** или использовать полосу прокрутки непосредственно под списком событий **Event List**.

   Откроется окно **PDU Information at Device: Web Client** (Информация о PDU на устройстве: вебклиент). В этом окне есть только две вкладки: **OSI Model** (Модель OSI) и **Outbound PDU Details** (Сведения об исходящей PDU), поскольку это только начало передачи. По мере изучения новых событий станут видны три вкладки, включая новую вкладку **Inbound PDU Details** (Сведения о входящей PDU). Когда событие является последним в потоке трафика, отображаются только вкладки **OSI Model** и **Inbound PDU Details**.
b. Убедитесь, что выбрана вкладка **OSI Model**. В столбце **Out Layers** нажмите **Layer 7**.

   Какая информация перечислена в пронумерованных шагах непосредственно под полями **In Layers** (Входящие уровни) и **Out Layers** (Исходящие уровни)?

   Какое значение столбца **Dst Port** на **Уровне 4** в столбце **Out Layers** ?

   Какое значение имеет параметр **Dest.** Значение IP для **Layer 3** в столбце **Out Layers**?

   Какая информация отображается на слое 2 в столбце **Out Layers**?

   Заголовок Ethernet II уровня 2 и входящие и исходящие MAC-адреса.
c. Щелкните вкладку **Outbound PDU Details** (Сведения об исходящей PDU).

   Сведения на вкладке **PDU Details** (Сведения о PDU) отражают уровни модели TCP/IP.

Примечание**. Сведения в разделе** Ethernet II **представляют собой еще более подробные данные, чем показанные в разделе уровня 2 на вкладке** OSI Model. Вкладка **Outbound PDU Details** содержит более описательные и подробные сведения. Значения **DEST MAC** (MAC-адрес назначения) и **SRC MAC** (MAC-адрес источника) в разделе Ethernet II **на вкладке PDU Details** отображаются на вкладке **OSI Model** в разделе Layer 2, но не указаны в качестве таковых.

Если сравнить сведения в разделе **IP** вкладки **PDU Details** со сведениями на вкладке **OSI Model**, какая информация является для них общей? К какому уровню она относится?

Если сравнить сведения в разделе **TCP** вкладки **PDU Details**со сведениями на вкладке **OSI Model**, какая информация является для них общей и к какому уровню она относится?

Какой **Host** (узел) указан в разделе **HTTP** вкладки **PDU Details**? С каким уровнем будут связаны эти сведения на вкладке **OSI Model**?

d. Щелкните первый цветной квадрат в столбце **Type** списка событий **Event List**. Активен только уровень 1 (не отображается серым цветом). Устройство перемещает кадр из буфера и помещает его в сеть.

e. Перейдите к следующему полю HTTP **Info** в списке событий **Event List** и щелкните цветной квадрат. В этом окне есть два столбца: **In Layers** и **Out Layers**. Обратите внимание на направление стрелки непосредственно под столбцом **In Layers**. Она смотрит вверх, показывая направление перемещения данных. Пролистайте эти уровни, обращая внимание на просмотренные ранее элементы. В верхней части столбца стрелка указывает вправо. Это означает, что сервер теперь отправляет данные обратно клиенту.

Сравните данные в столбце **In Layers** с данными в столбце **Out Layers** и скажите, в чем заключается основное отличие между ними.

f. Откройте вкладку **Inbound PDU Details** (Сведения о входящей PDU). просмотр сведений о PDU.

g. Щелкните последний цветной квадрат в столбце **Info**.

Сколько вкладок отображается с этим событием и почему? Дайте пояснение.

Только две (одна — OSI Model, а вторая — Inbound PDU Details, поскольку это принимающее устройство).

Часть 2. Отображение элементов семейства протоколов TCP/IP

В части 2 данного упражнения вы будете использовать режим моделирования Packet Tracer для наблюдения и изучения работы некоторых других протоколов, входящих в семейство TCP/IP.

Шаг 1. Просмотрите дополнительные события

a. Закройте все окна со сведениями о PDU.

b. В разделе **Event List Filters** > **Visible Events (Фильтры списка событий > Видимые события)** нажмите кнопку **Show All/None**.

Какие дополнительные типы событий показаны?

Эти дополнительные записи играют различные роли в семействе протоколов TCP/IP. Протокол разрешения адресов (ARP) запрашивает MAC-адреса для узлов назначения. Протокол DNS отвечает за преобразование имен (например, **www.osi.local**) в IP-адреса. Дополнительные события TCP связаны с установлением соединений, согласованием параметров связи и разъединением сеансов связи между устройствами. Эти протоколы упоминались ранее и будут рассмотрены более подробно в ходе изучения курса. В настоящее время Packet Tracer позволяет захватывать более 35 протоколов (типов событий).

c. Щелкните первое событие DNS в столбце **Type**. Просмотрите вкладки **OSI Model** и **PDU Detail** и обратите внимание на процесс инкапсуляции. На вкладке **OSI Model** с выделенным полем **Layer 7** непосредственно под столбцами **In Layers** и **Out Layers** отображается описание того, что происходит. ("1. The DNS client sends a DNS query to the DNS server." [DNS-клиент отправляет DNSзапрос на DNS-сервер]) Это очень полезная информация, которая помогает понять, что происходит во время процесса связи.

d. Щелкните вкладку **Outbound PDU Details** (Сведения об исходящей PDU).

Какие сведения показаны в поле **NAME**: в разделе DNS QUERY?

e. Щелкните последний цветной квадрат DNS **Info** в списке событий.

На каком устройстве был захвачен PDU?

Какое значение показано рядом с полем **ADDRESS**: в разделе DNS ANSWER на вкладке **Inbound PDU Details**?

f. Найдите первое событие **HTTP** в списке и щелкните цветной квадрат события **TCP** сразу после этого события. Выделите **Layer 4** на вкладке **OSI Model**.

Какие сведения отображаются под пунктами 4 и 5 в пронумерованном списке непосредственно под столбцами **In Layers** и **Out Layers**?

TCP, наряду с другими функциями, управляет подключением и отключением канала связи. Данное конкретное событие указывает на то, что канал связи был установлен (ESTABLISHED).

g. Щелкните последнее событие TCP. Выделите Layer 4 на вкладке **OSI Model**. Проверьте действия, перечисленные непосредственно под столбцами **In Layers** и **Out Layers**.

Расскажите, для чего предназначено событие, используя информацию, предоставленную в последнем пункте списка (это должен быть пункт 4).

Сложные вопросы

В этом упражнении по моделированию рассмотрен пример сеанса веб-связи между клиентом и сервером в локальной сети (LAN). Клиент делает запросы к определенным службам, функционирующим на сервере. Сервер должен быть настроен на прослушивание определенных портов для получения запросов клиентов. (Совет. Для получения информации о порте см. Layer 4 на вкладке **OSI Model**.)

Взяв за основу сведения, которые проверялись в ходе захвата данных в Packet Tracer, ответьте: «Какой порт прослушивает **веб-сервер** для получения веб-запросов?». Какой порт прослушивает **веб-сервер** для получения DNS-запросов?

Лабораторная работа 6

Packet Tracer - Подключение проводной и беспроводной локальных сетей

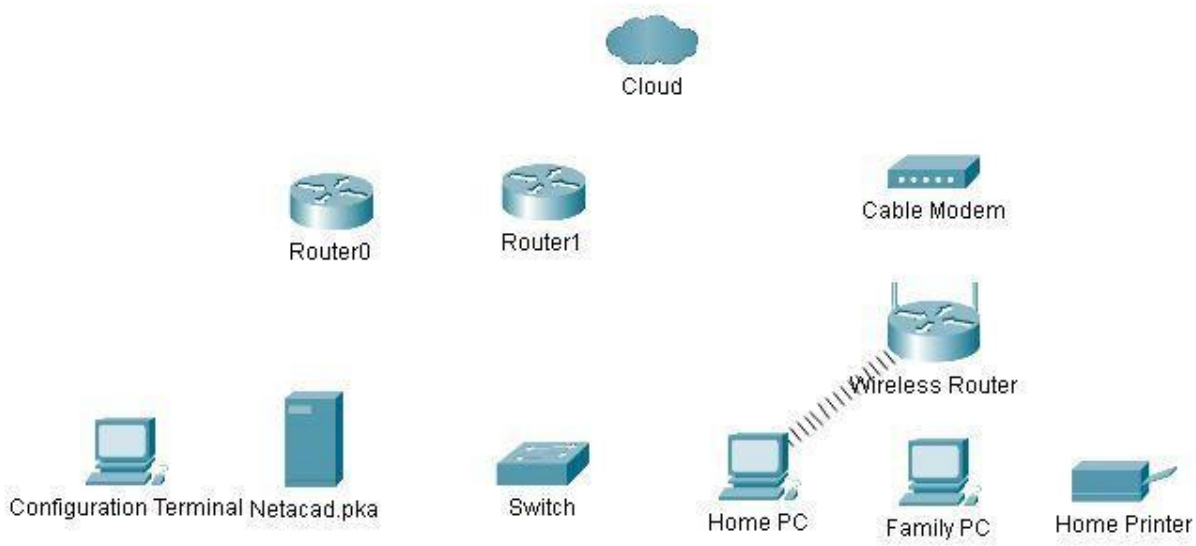


Таблица адресации

Устройство	Интерфейс	IP-адрес	Подключается к
Cloud	Eth6	—	F0/0
	Coax7	—	Port0
Cable Modem	Port0	—	Coax7
	Port1	—	Internet
Router0	Console	—	RS232
	F0/0	192.168.2.1/24	Eth6
	F0/1	10.0.0.1/24	F0
	Ser0/0/0	172.31.0.1/24	Ser0/0
Router1	Ser0/0	172.31.0.2/24	Ser0/0/0
	F1/0	172.16.0.1/24	F0/1
Wireless Router	Internet	192.168.2.2/24	Port1
	Eth1	192.168.1.1	F0
Family PC	F0	192.168.1.102	Eth1
Switch	F0/1	172.16.0.2	F1/0
Netacad.pka	F0	10.0.0.254	F0/1

Configuration Terminal	RS232	—	Console

Задачи

Часть 1. Подключение к облаку

Часть 2. Подключение маршрутизатора Router0

Часть 3. Подключение оставшихся устройств

Часть 4. Проверка подключений

Часть 5. Изучение физической топологии

Общие сведения

При работе в программе Packet Tracer (в рамках лабораторной работы или в реальных условиях) вы должны уметь выбирать необходимый кабель и надлежащим образом подключать устройства. В ходе данного упражнения будут рассмотрены: конфигурирование устройств в программе Packet Tracer, выбор кабеля в зависимости от конфигурации, а также подключение устройств. Также в этом упражнении будет подробно рассмотрено физическое представление сети в программе Packet Tracer.

Инструкции

Часть 1. Подключение к облаку

Шаг 1. Подключите Cloud (Облако) к Router0.

b. В левом нижнем углу щелкните значок в виде оранжевой молнии, чтобы открыть список доступных **подключений**.

c. Выберите правильный кабель для подключения порта **F0/0 Router0** к порту **Eth6 Cloud**. **Cloud** — это тип коммутатора, поэтому используйте подключение **Copper Straight-Through** (Медное прямое). После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом.

Шаг 2. Подключите Cloud (Облако) к Cable Modem (Кабельный модем).

Выберите правильный кабель для подключения порта **Coax7 Cloud** к порту **Port0 Modem**.

После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом. **Часть**

2. Подключение маршрутизатора Router0

Шаг 1. Подключите Router0 к Router1.

Выберите правильный кабель для подключения порта **Ser0/0/0 Router0** к порту **Ser0/0 Router1**.

Используйте один из доступных последовательных (**Serial**) кабелей.

После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом.

Шаг 2. Подключите Router0 к netacad.pka.

Выберите правильный кабель для подключения порта **F0/1 Router0** к порту **F0 netacad.pka**. Маршрутизаторы и компьютеры обычно используют одинаковые провода для отправки (1 и 2) и получения (3 и 6) данных. Кабель, который нужно выбрать, состоит из скрученных проводов. Хотя многие современные сетевые платы могут автоматически определить, какие пары используются для приема и передачи, на маршрутизаторе **Router0** и сервере **netacad.pka** нет сетевых плат с этой функцией автоопределения.

После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом. **Шаг**

3. Подключите Router0 к Configuration Terminal (Терминал настройки).

Выберите правильный кабель для подключения **консоли Router0** к **терминалу RS232** . Этот кабель не обеспечивает сетевой доступ к **Configuration Terminal**, но позволяет настроить **Router0** через терминал.

После подключения правильного кабеля индикаторы канала на кабеле станут черными. **Часть**

3. Подключение оставшихся устройств

Шаг 1. Подключите Router1 к Switch (Коммутатор).

Выберите правильный кабель для подключения порта **F1/0 Router1** к порту **F0/1 Switch**.

После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом. Подождите несколько секунд, чтобы индикатор из оранжевого стал зеленым.

Шаг 2. Подключите Cable Modem (Кабельный модем) к Wireless Router (Беспроводной маршрутизатор).

Выберите правильный **кабель для подключения порта Port1 Modem** к порту **Internet Wireless Router**.

После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом.

Шаг 3. Подключите Wireless Router (Беспроводной маршрутизатор) к Family PC (Общий ПК).

Выберите правильный кабель для подключения порта **Eth1 Wireless Router** к **Family PC**.

После подключения правильного кабеля индикатор канала на кабеле загорится зеленым цветом.

Часть 4. Проверка подключений

Шаг 1. Проверьте подключение Family PC к netacad.pka.

a. Откройте командную строку на **Family PC** и выполните команду ping для сервера **netacad.pka**.

b. Откройте **веб-браузер** и введите адрес **http://netacad.pka**. **Шаг 2. Отправьте запрос ping с Home PC (Домашний ПК) на Switch (Коммутатор).**

Откройте командную строку на **Home PC** и выполните команду ping для IP-адреса **Switch**, чтобы проверить соединение.

Шаг 3. Откройте Router0 с Configuration Terminal (Терминал настройки).

a. Откройте **Terminal** на **Configuration Terminal** и примите параметры по умолчанию.
b. Нажмите клавишу **ввода**, чтобы открыть командную строку **Router0**.
c. Введите команду **show ip interface brief**, чтобы просмотреть состояние интерфейсов.

Часть 5. Изучение физической топологии

Шаг 1. Изучите облако.

a. Откройте вкладку **Physical Workspace** (Физическая рабочая область) или используйте сочетания клавиш **Shift**+**P** и **Shift**+**L** для переключения между логической и физической рабочими областями.
b. Щелкните значок **Home City** (Родной город).
c. Щелкните значок **Cloud** (Облако).

Сколько проводов подключено к коммутатору в синей стойке?

d. Нажмите кнопку **Back** (Назад) для возврата к **Home City**. **Шаг 2. Изучите первичную сеть.**

a. Щелкните значок **Primary Network** (Первичная сеть). Удерживайте указатель мыши на разных кабелях.

Что находится в таблице справа от синей стойки?

b. Нажмите кнопку **Back** (Назад) для возврата к **Home City**. **Шаг 3. Изучите вторичную сеть.**

a. Щелкните значок **Secondary Network** (Вторичная сеть). Удерживайте указатель мыши на разных кабелях.

Почему к каждому устройству подключено по два оранжевых кабеля?

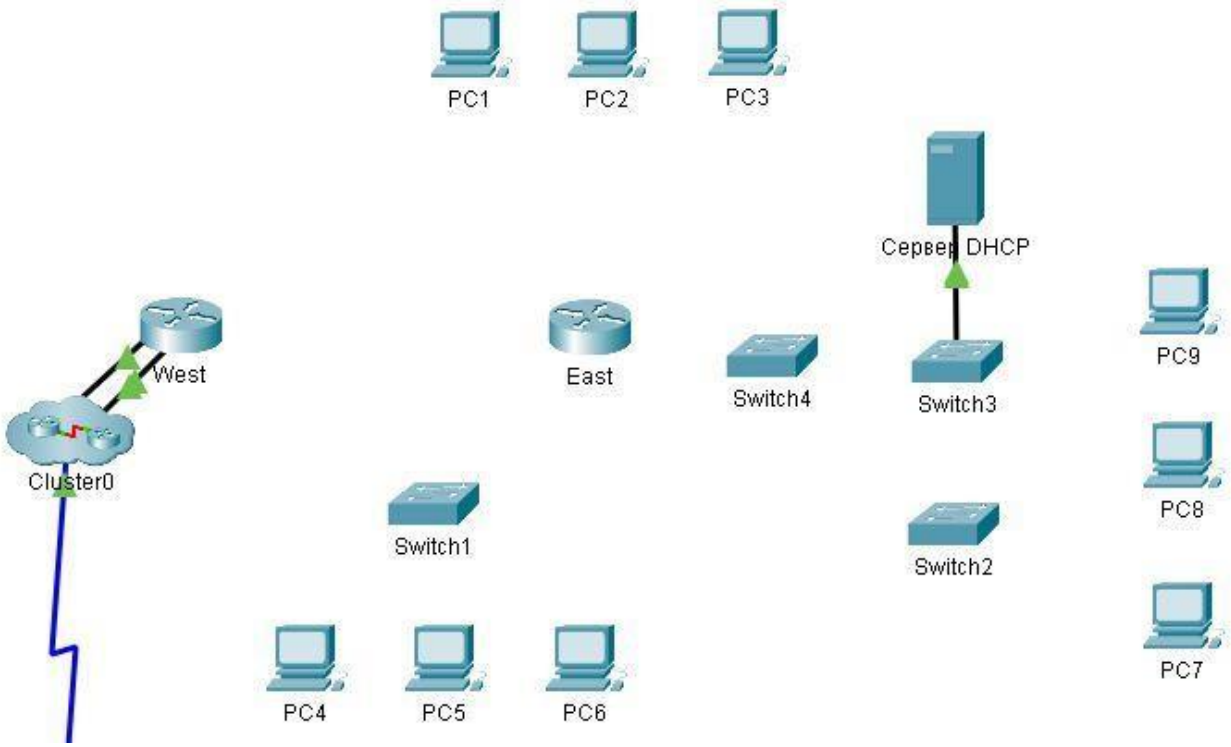
b. Нажмите кнопку **Back** (Назад) для возврата к **Home City**. **Шаг 4. Изучите домашнюю сеть.**

a. Щелкните значок **Home Network** (Домашняя сеть).

Почему нет стойки для оборудования?

b. Откройте вкладку **Logical Workspace** (Логическая рабочая область), чтобы вернуться к логической топологии.

Лабораторная работа 7
Packet Tracer - Подключение физического уровня



Цели

Часть 1. Определение физических характеристик межсетевых устройств
Часть 2. Выбор подходящих модулей для подключения
Часть 3. Подключение устройств
Часть 4. Проверка подключения

Общие сведения

В этом упражнении вы изучите различные параметры межсетевых устройств. Вам также нужно будет определить, настройка каких параметров позволяет установить надежное соединение при подключении нескольких устройств. В завершение вы добавите соответствующие модули и подключите устройства. **Примечание.** Для этого упражнения оценка составляется из автоматизированной оценки Cisco Packet Tracer и записанных вами ответов на вопросы из инструкций. См. **Ошибка! Неверная ссылка закладки.**раздел в конце этого упражнения и обратитесь за помощью к инструктору, чтобы определить свою окончательную оценку.

Часть 1. Определение физических характеристик межсетевых устройств Шаг
1. Определите порты управления маршрутизатора Cisco.

a. Нажмите маршрутизатор **East.** Вкладка **Physical** (Физический) должна быть активна.
b. Увеличьте масштаб и разверните окно, чтобы видеть весь маршрутизатор.

Какие порты управления доступны?

Шаг 2. Определите LAN- и WAN-интерфейсы на маршрутизаторе Cisco

a. Какими LAN- и WAN-интерфейсами оснащен маршрутизатор **East**? Сколько их?

b. Перейдите на вкладку **CLI**, нажмите клавишу **Enter** для доступа к подсказке пользовательского режима и введите следующие команды:
East> **show ip interface brief**
Выходные данные подтверждают правильное количество интерфейсов и их обозначение.
Интерфейс vlan1 является виртуальным и существует только в программном обеспечении.

Сколько физических интерфейсов перечислено?

c. Введите следующие команды:

East> **show interface gigabitethernet 0/0**

Какая пропускная способность задана по умолчанию для данного интерфейса?

East> **show interface serial 0/0/0**

Какая пропускная способность задана по умолчанию для данного интерфейса?

Примечание. Пропускная способность на последовательных интерфейсах используется процессами маршрутизации для определения наилучшего пути к адресу назначения. Это значение не отражает фактическую пропускную способность интерфейса. Фактическая пропускная способность согласовывается с поставщиком услуг.

Шаг 3. Определите на коммутаторах слоты расширения для модулей.

Сколько в маршрутизаторе **East** слотов расширения для установки дополнительных модулей? Нажмите коммутатор **Switch2**. Сколько у них слотов расширения?

Часть 2. Выбор подходящих модулей для подключения

Шаг 1. Определите модули, обеспечивающие необходимое подключение.

a. Нажмите маршрутизатор **East** и откройте вкладку **Physical** (Физический). Слева под меткой **Modules** (Модули) отображаются доступные варианты расширения возможностей маршрутизатора. Щелкните каждый модуль. Внизу будет показано его изображение и дано описание. Изучите эти варианты.

1) Вам нужно подключить компьютеры PC1, 2 и 3 к маршрутизатору **East**, но у вас недостаточно средств для приобретения нового коммутатора. С помощью какого модуля можно подключить три ПК к маршрутизатору **East**?
2) Сколько узлов можно подключить к маршрутизатору с помощью этого модуля?

b. Нажмите коммутатор **Switch2**.

Какой модуль можно вставить, чтобы обеспечить оптоволоконное подключение Gigabit к коммутатору **Switch3**?

Шаг 2. Добавьте подходящие модули и включите устройства.

a. Нажмите маршрутизатор **East** и попробуйте вставить соответствующий модуль из шага 1A. Модули добавляются щелчком по модулю и перетаскиванием его в пустой слот устройства.

Должно отобразиться сообщение: **Cannot add a module when the power is on** (Не удалось добавить модуль после включения питания). Интерфейсы в этой модели маршрутизатора не поддерживают горячую замену. Перед добавлением или удалением модулей устройство должно быть выключено. Щелкните выключатель питания справа от логотипа Cisco, чтобы выключить маршрутизатор **East**. Вставьте соответствующий модуль из шага 1A. Затем щелкните выключатель питания, чтобы включить маршрутизатор **East**.

Примечание. Если вы вставите неправильный модуль и вам будет нужно его удалить, перетащите модуль вниз на его изображение в правом нижнем углу и отпустите кнопку мыши.

b. Используя ту же процедуру, вставьте соответствующие модули из шага 1Б в крайний справа пустой слот на коммутаторе **Switch2**.

c. С помощью команды **show ip interface brief** определите слот на **Switch2**, в который был вставлен модуль.

В какой слот был вставлен модуль?

Часть 3. Подключение устройств

Возможно, для вас это первое упражнение, в котором вы должны подключить устройства. Вы еще можете не знать назначение различных типов кабелей. Чтобы успешно подключить все устройства, воспользуйтесь приведенной ниже таблицей и следуйте соответствующим рекомендациям. a. Выберите соответствующий тип кабеля.

b. Нажмите первое устройство и выберите указанный интерфейс.

c. Нажмите второе устройство и выберите указанный интерфейс.

d. Если устройства подключены правильно, вы увидите, что ваша оценка увеличилась.

Пример. **Чтобы подключить маршрутизатор** East **к коммутатору** Switch1**, выберите тип кабеля Copper Straight-Through** (Медный прямой). Нажмите **маршрутизатор** East **и выберите интерфейс GigabitEthernet0/0.** Затем нажмите **Switch1** и выберите **интерфейс GigabitEthernet0/1.** Теперь ваш счет должен быть 4/55.

Примечание. В данном упражнении световой индикатор сети отключен.

Устройство	Интерфейс	Тип кабеля	Устройство	Интерфейс
East	GigabitEthernet0/0	Copper Straight-Through (Медный прямой)	Switch1	GigabitEthernet0/1
East	GigabitEthernet0/1	Copper Straight-Through (Медный прямой)	Switch4	GigabitEthernet0/1
Устройство	**Интерфейс**	**Тип кабеля**	**Устройство**	**Интерфейс**
East	FastEthernet0/1/0	Copper Straight-Through (Медный прямой)	PC1	FastEthernet0
East	FastEthernet0/1/1	Copper Straight-Through (Медный прямой)	PC2	FastEthernet0
East	FastEthernet0/1/2	Copper Straight-Through (Медный прямой)	PC3	FastEthernet0
Switch1	FastEthernet0/1	Copper Straight-Through (Медный прямой)	PC4	FastEthernet0
Switch1	FastEthernet0/2	Copper Straight-Through (Медный прямой)	PC5	FastEthernet0
Switch1	FastEthernet0/3	Copper Straight-Through (Медный прямой)	PC6	FastEthernet0
Switch4	GigabitEthernet0/2	Copper Cross-Over (Медный перекрестный)	Switch3	GigabitEthernet3/1
Switch3	GigabitEthernet5/1	Fiber (Оптоволоконный)	Switch2	GigabitEthernet5/1
Switch2	FastEthernet0/1	Copper Straight-Through (Медный прямой)	PC7	FastEthernet0
Switch2	FastEthernet1/1	Copper Straight-Through (Медный прямой)	PC8	FastEthernet0
Switch2	FastEthernet2/1	Copper Straight-Through (Медный прямой)	PC9	FastEthernet0
Switch2	Gigabit3/1	Copper Straight-Through (Медный прямой)	AccessPoint	Port 0
East	Serial0/0/0	Serial DCE (Последовательный DCE) (подключается сначала к маршрутизатору East)	West	Serial0/0/0

Часть 4. Проверка подключения.

Шаг 1. Проверьте статус интерфейса на востоке.

a. Откройте вкладку **CLI** и введите следующие команды: East>

show ip interface brief

Сравните выходные данные со следующими:

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0 172.30.1.1 YES manual up up

GigabitEthernet0/1 172.31.1.1 YES manual up up

Serial0/0/0 10.10.10.1 YES manual up up

Serial0/0/1 unassigned YES unset down down

FastEthernet0/1/0 unassigned YES unset up up

FastEthernet0/1/1 unassigned YES unset up up

FastEthernet0/1/2 unassigned YES unset up up

FastEthernet0/1/3 unassigned YES unset up down Vlan1

172.29.1.1 YES manual up up

Если все кабели соединены верно, вывод должен совпадать.

Шаг 2. Подключите беспроводные устройства, ноутбук и TabletPC.

a. Щелкните ноутбук и выберите вкладку « **Конфигурация** ». Выберите интерфейс **WLAN-0.** Установите флажок в поле « **Вкл» рядом с пунктом «** Статус порта». Через несколько секунд должно появиться беспроводное соединение.

b. Перейдите на вкладку **Рабочийстол ноутбука** . Нажмите на значок **веб-браузера**, чтобы запустить веб-браузер. Введите **www.cisco.pka** в поле URL и нажмите кнопку **Перейти** . На странице должен отображаться **Cisco Packet Tracer**.

c. Щелкните ноутбук и выберите вкладку «**Конфигурация**». Выберите интерфейс **Wireless0**. Установите флажок в поле «**Вкл» рядом с пунктом «**Статус порта». Через несколько секунд должно появиться беспроводное соединение.

d. Повторите шаги, описанные в шаге 2Б, чтобы проверить отображение страницы. **Шаг 3. Измените способ доступа TabletPC.**

a. Щелкните ноутбук и выберите вкладку «**Конфигурация**». Выберите интерфейс **Wireless0**. Снимите флажок «**Вкл» рядом с пунктом «**Состояние порта». Теперь должно быть ясно, и беспроводное соединение будет разорвано.

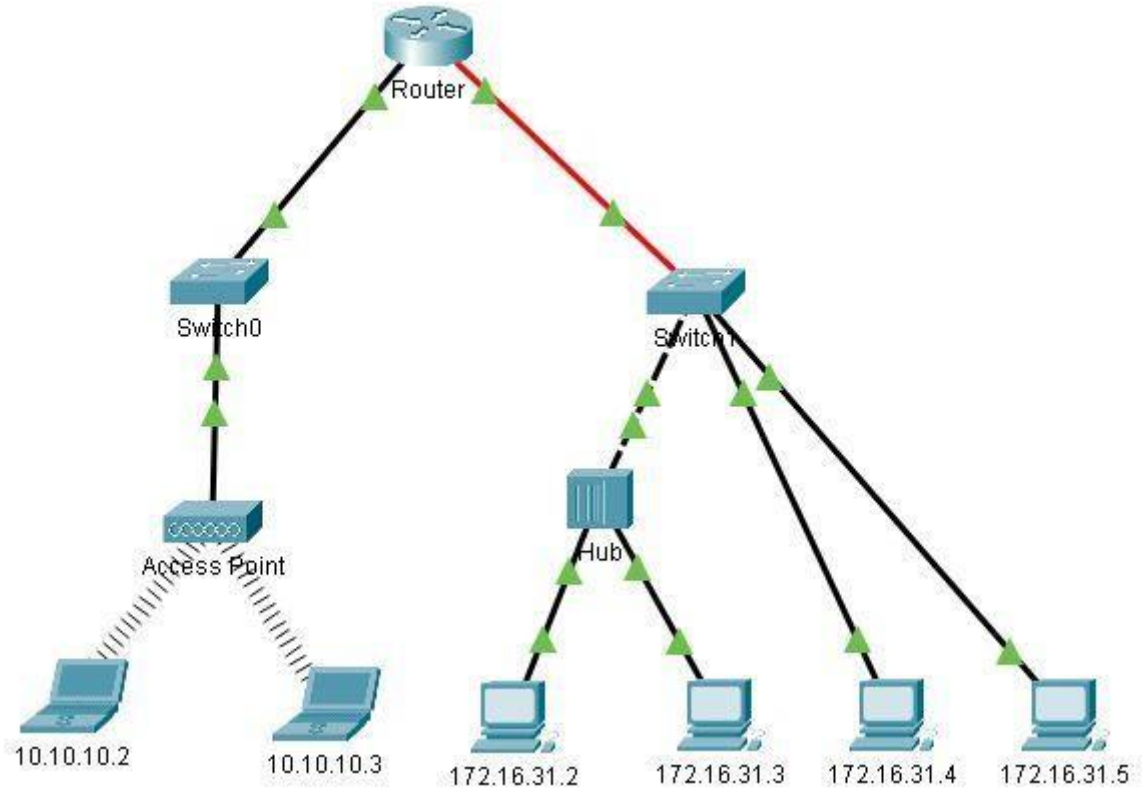
b. Нажмите на интерфейс **3G/4G Cell1** . Установите флажок в поле «**Вкл» рядом с пунктом «**Статус порта». Через несколько секунд должна появиться сотовая связь.

c. Повторите процесс проверки веб-доступа.

Примечание: Вы не должны одновременно использовать интерфейс wireless0 и интерфейс 3G/4G Cell1. Это может привести к путанице в устройстве при попытке подключения к некоторым ресурсам. **Шаг 4. Проверьте возможность подключения других ПК.**

Все компьютеры должны подключаться к веб-сайту и друг к другу. Вы научитесь использовать тестирование подключения во многих будущих лабораторных работах.

Лабораторная работа 8
Cisco Packet Tracer. Определение MAC- и IP-адресов



Задачи

Часть 1: Сбор информации PDU для локальной сети связи

Часть 2: Сбор информации PDU для удаленной сетевой связи

Общие сведения

Это упражнение оптимизировано для просмотра единиц данных протокола (PDU). Устройства уже настроены. Вам необходимо в режиме моделирования собрать сведения о единице данных протокола (PDU), а также ответить на ряд вопросов о собираемых данных.

Инструкции

Часть 1. Сбор информации PDU для локальной сети связи

Примечание. Просмотрите вопросы для повторения из части 3, прежде чем приступать к части 1. По ним вы сможете понять, какие типы данных необходимо будет собрать.

Шаг 1. Соберите сведения о единице данных протокола (PDU) по мере перемещения пакета с адреса 172.16.31.5 в адрес 172.16.31.2.

a. Нажмите **172.16.31.5** и откройте окно **Command Prompt** (Командная строка).
b. Введите команду **ping 172.16.31.2**.
c. Перейдите в режим моделирования и повторите команду **ping 172.16.31.2** . Единица данных протокола (PDU) будет показана рядом с **172.16.31.5**.
d. Нажмите единицу данных протокола (PDU) и запишите следующие данные на вкладке **OSI Model** и **Outbound PDU Layer** .
   - MAC-адрес назначения: **000C:85CC:1DA7**
   - MAC-адрес источника: **00D0:D311:C788**
   - IP-адрес источника: **172.16.31.5**
   - IP-адрес назначения: **172.16.31.2**
   - На устройстве: **172.16.31.5**
e. Нажмите **Capture / Forward** (стрелка вправо с вертикальной чертой), чтобы переместить единицу данных протокола (PDU) на следующее устройство. Соберите аналогичные сведения из шага 1Г. Повторяйте процедуру до тех пор, пока единица данных протокола (PDU) не достигнет места

назначения. Запишите полученные сведения о единице данных протокола (PDU) в электронную таблицу в формате, показанном в таблице ниже. **Пример формата электронной таблицы**

На устройстве	Адрес MAC-адрес	MAC-адрес источника	IPv4-адрес источника	IPv4-адрес назначения
172.16.31.5	000C:85CC:1DA7	00D0:D311:C788	172.16.31.5	172.16.31.2
Switch1	000C:85CC:1DA7	00D0:D311:C788	—	—
узел	—	—	—	—
172.16.31.2	00D0:D311:C788	000C:85CC:1DA7	172.16.31.2	172.16.31.5

Шаг 2. Соберите дополнительные сведения о единице данных пакета (PDU) с помощью других эхозапросов.

Повторите процедуру, описанную в шаге 1, и соберите сведения для следующих проверок.

- Эхо-запрос с 172.16.31.2 на адрес 172.16.31.3
- Эхо-запрос с 172.16.31.4 на адрес 172.16.31.5 Вернитесь в режим реального времени (Realtime).

Часть 2. Сбор информации PDU для удаленной сетевой связи

Для связи с удаленными сетями необходим шлюз. Изучите процесс, который происходит соединения устройств в удаленной сети. Обратите пристальное внимание на используемые MAC-адреса.

Шаг 1. Соберите сведения о единице данных протокола (PDU) по мере перемещения пакета с адреса 172.16.31.5 в адрес 10.10.10.2.

a. Нажмите **172.16.31.5** и откройте окно **Command Prompt** (Командная строка).
b. Введите команду **ping 10.10.10.2**.
c. Перейдите в режим моделирования и повторите команду **ping 10.10.10.2** . Единица данных протокола (PDU) будет показана рядом с **172.16.31.5**.
d. Нажмите единицу данных протокола (PDU) и запишите следующие данные на вкладке **Outbound PDU Layer** (Уровень исходящей PDU).
    - MAC-адрес назначения: 00D0:BA8E:741A
    - MAC-адрес источника: 00D0:D311:C788
    - IP-адрес источника: 172.16.31.5
    - IP-адрес назначения: 10.10.10.2
    - На устройстве: 172.16.31.5

    Какое устройство имеет этот MAC-адрес назначения?
e. Нажмите **Capture / Forward** (стрелка вправо с вертикальной чертой), чтобы переместить единицу данных протокола (PDU) на следующее устройство. Соберите аналогичные сведения из шага 1Г. Повторяйте процедуру до тех пор, пока единица данных протокола (PDU) не достигнет места назначения. Запишите полученные сведения о единице данных протокола (PDU) после пингования 172.16.31.5 в электронную таблицу в формате, показанном в таблице ниже.

На устройстве	Адрес MAC-адрес	MAC-адрес источника	IPv4-адрес источника	IPv4-адрес назначения
172.16.31.5	00D0:BA8E:741A	00D0:D311:C788	172.16.31.5	10.10.10.2
Коммутатор 1	00D0:BA8E:741A	00D0:D311:C788	—	—
Маршрутизатор	0060:2F84:4AB6	00D0:588C:2401	172.16.31.5	10.10.10.2
Switch0	0060:2F84:4AB6	00D0:588C:2401	—	—
Точка доступа	—	—	—	—
10.10.10.2	00D0:588C:2401	0060:2F84:4AB6	10.10.10.2	172.16.31.5

Вопросы для повторения

Ответьте на следующие вопросы относительно сбора данных.

1. Использовались ли для подключения устройств разные типы проводов?
2. Отразилось ли изменение проводов на обработке единицы данных протокола (PDU)?
3. Были ли на **Hub** (Концентратор) потеряны какие-либо данные?
4. Что **Hub** (Концентратор) делает с MAC- и IP-адресами?
5. Делает ли что-то **точка беспроводного доступа** с данными, которые на нее поступают?
6. Теряются ли какие-либо MAC-адреса или IP-адреса при передаче по беспроводной сети?

7. Какой самый высокий уровень модели OSI используется в **Hub** (Концентратор) и **Access Point** (Точка доступа)?
8. Копировали ли **Hub** (Концентратор) или **Access Point** (Точка доступа) единицу протокола данных (PDU), которая была отклонена с красным значком «X»?
9. Какой MAC-адрес при изучении вкладки **PDU Details** (Сведения о PDU) появился первым — адрес источника или адрес назначения?
10. Почему MAC-адреса отображаются именно в этом порядке?
11. Заметили ли вы общую структуру определения MAC-адресов при моделировании?
12. sКопировали ли коммутаторы единицу данных протокола (PDU), которая была отклонена с красным значком «X»?
13. При каждой пересылке единицы данных протокола (PDU) между сетями 10 и 172 была точка, в которой MAC-адреса неожиданно изменялись. На каком устройстве это происходило?
14. Какое устройство имеет MAC-адрес, начинающийся с 00D0:BA?
15. Каким устройствам принадлежали другие MAC-адреса?
16. Переключались ли IPv4-адреса отправки и получения на какую-либо единицу данных протокола (PDU)?
17. Если следовать эхо-ответу (который иногда называется *pong*), переключаются ли IPv4-адреса отправки и получения?
18. Заметили ли вы общую структуру определения IPv4-адресов при моделировании?
19. Почему разные IP-адреса сети необходимо присваивать разным портам маршрутизатора?
20. Если бы в данном моделировании была настроена работа с IPv6-адресами вместо IPv4-адресов, в чем состояло бы отличие?

Лабораторная работа 9
Cisco Packet Tracer. Изучение таблицы ARP

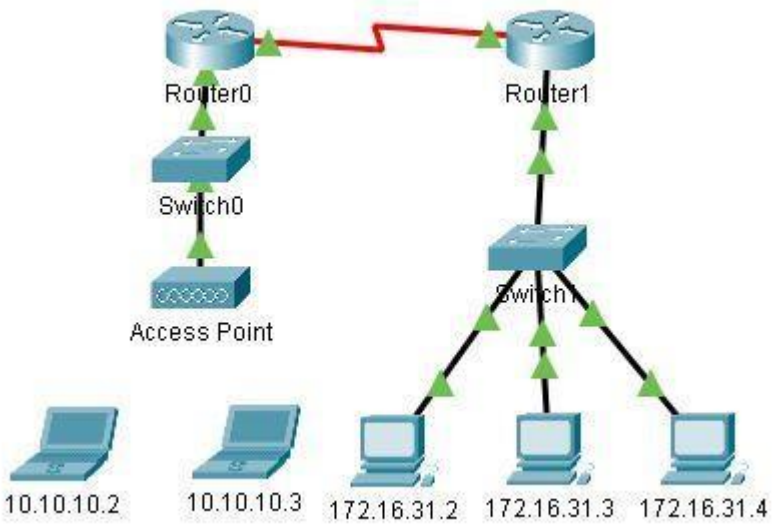


Таблица адресации

Устройство	Интерфейс	MAC-адрес	Интерфейс коммутатора
Router0	Gg0/0	0001.6458.2501	G0/1
	S0/0/0	—	—
Router1	G0/0	00E0.F7B1.8901	G0/1
	S0/0/0	—	—
10.10.10.2	Wireless	0060.2F84.4AB6	F0/2
10.10.10.3	Wireless	0060.4706.572B	F0/2
172.16.31.2	F0	000C.85CC.1DA7	F0/1
172.16.31.3	F0	0060.7036.2849	F0/2
172.16.31.4	G0	0002.1640.8D75	F0/3

Задачи

Часть 1. Анализ ARP-запроса

Часть 2. Изучение таблицы MAC-адресов коммутатора

Часть 3. Анализ процесса ARP в удаленных подключениях

Общие сведения

Часть 1. Это упражнение оптимизировано для просмотра единиц данных протокола (PDU). Устройства уже настроены. Вам необходимо в режиме моделирования собрать сведения о единице данных протокола (PDU), а также ответить на ряд вопросов о собираемых данных.

Инструкции

Часть 1. Анализ ARP-запроса

Шаг 1. Создайте ARP-запросы, отправив эхо-запросы на адрес 172.16.31.3 с 172.16.31.2.

- Нажмите **172.16.31.2** и откройте окно **Command Prompt** (Командная строка).
- Выполните команду **arp -d**, чтобы очистить таблицу ARP.

- Перейдите в режим **Simulation** (Моделирование) и выполните команду **ping 172.16.31.3**. Будет создано две единицы данных протокола PDU. Команда **ping** не может отправить ICMP-пакет, не зная MAC-адрес назначения. Поэтому компьютер отправляет широковещательный кадр ARP, чтобы найти MAC-адрес назначения.
- Нажмите кнопку **Capture/Forward** (Захватить/переадресовать) один раз. Единица данных протокола (PDU) ARP перемещается на **Switch1** (Коммутатор 1), а единица данных протокола (PDU) ICMP

исчезает, ожидая ARP-ответ. Откройте единицу данных протокола (PDU) и запишите MAC-адрес назначения. Этот адрес есть в таблице выше?

- Нажмите **Capture / Forward** (Захватить/переадресовать), чтобы переместить единицу данных протокола (PDU) на следующее устройство.

Сколько копий единицы данных протокола (PDU) создал **Switch1**?

Какой IP-адрес имеет устройство, которое приняло единицу данных протокола (PDU)? Откройте единицу данных протокола (PDU) и изучите уровень 2.

Что произошло с MAC-адресами источника и назначения?

- Нажимайте кнопку **Capture/Forward** (Захватить/переадресовать) до тех пор, пока единица данных протокола (PDU) не вернется на узел **172.16.31.2**.

Сколько копий единицы данных протокола (PDU) создал коммутатор для ответа на ARP-запрос?

Шаг 2. Изучите таблицу ARP.

- Обратите внимание, что ICMP-пакет снова появился. Откройте единицу данных протокола (PDU) и взгляните на MAC-адрес.

MAC-адреса источника и назначения соответствуют их IP-адресам?

- Вернитесь обратно в режим **реального времени**, и команда ping завершится. Нажмите **172.16.31.2** и выполните команду **arp –a**.

Какому IP-адресу соответствует запись MAC-адреса?

В общем случае, когда оконечное устройство отправляет ARP-запрос? **Часть**

2. Изучение таблицы MAC-адресов коммутатора

Шаг 1. Сгенерируйте дополнительный трафик для заполнения таблицы MAC-адресов коммутатора.

- На узле **172.16.31.2** выполните команду **ping 172.16.31.4**.
- Нажмите кнопку **10.10.10.** 2 и откройте **командную строку**. Введите команду **ping 10.10.10.3**.

Сколько ответов было отправлено и получено?

Шаг 2. Изучите таблицу MAC-адресов на коммутаторах. Нажмите **Switch1** (Коммутатор 1) и откройте вкладку **CLI** (Интерфейс командной строки).

Выполните команду **show mac-address-table**.

Совпадают ли записи с указанными в таблице выше? Нажмите **Switch0** (Коммутатор 0) и откройте вкладку **CLI** (Интерфейс командной строки).

Выполните команду **show mac-address-table**.

Совпадают ли записи с указанными в таблице выше?

Почему два MAC-адреса связаны с одним портом?

Часть 3. Анализ процесса ARP в удаленных подключениях Шаг 1. Сгенерируйте трафик ARP.

- Нажмите **172.16.31.2** и откройте окно **Command Prompt** (Командная строка).
- Введите команду **ping 10.10.10.1**.
- Введите **arp –a**.

Какой IP-адрес имеет новая запись в таблице ARP?

- Выполните команду **arp -d** , чтобы очистить таблицу ARP и перейти в режим **моделирования**.
- Повторите команду ping для адреса 10.10.10.1.

Сколько единиц данных протокола (PDU) появилось?

- Нажмите кнопку **Capture/Forward** (Захватить/переадресовать). Нажмите единицу данных протокола (PDU), которая теперь находится на **Switch1**.

Какой IP-адрес назначения ARP-запроса?

- IP-адрес назначения не 10.10.10.1.

Почему?

Шаг 2. Проанализируйте таблицу ARP на Router1.

- Перейдите в режим **реального времени**. Нажмите **Router1** (Маршрутизатор 1) и откройте вкладку **CLI** (Интерфейс командной строки).
- Войдите в привилегированный режим EXEC и выполните команду **show mac-address-table**.

Сколько MAC-адресов в таблице? Почему?

- Выполните команду **show arp**.

Есть ли запись для **172.16.31.2**?

Что происходит с первым эхо-запросом, когда маршрутизатор отвечает на ARP-запрос?

Лабораторная работа 10

Packet Tracer - Обнаружение соседних IPv6 устройств

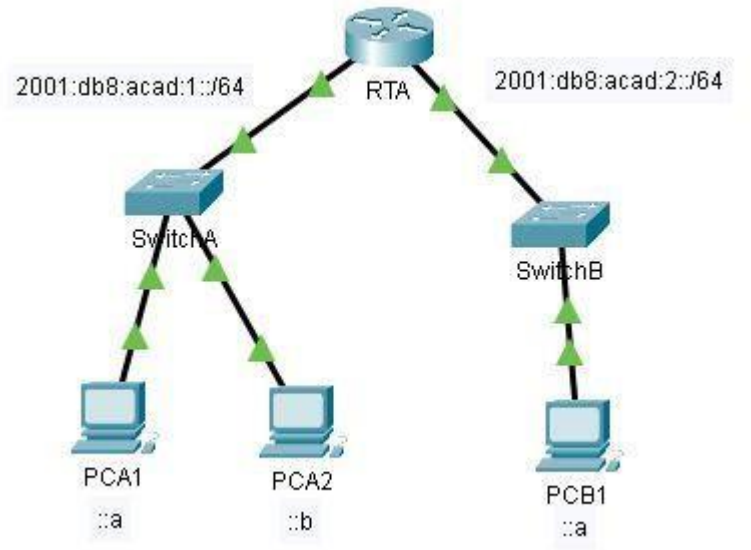


Таблица адресации

Устройство	Интерфейс	IPv6-адрес/префикс	Шлюз по умолчанию
RTA	G0/0/0	2001:db8:acad:1□1/64	Нет
	G0/0/1	2001:db8:acad:1□1/64	Нет
PCA1	NIC	2001:db8:acad:1□ A/64	fe80::1
PCA2	NIC	2001:db8:acad:1::B/64	fe80::1
PCB1	NIC	2001:db8:acad:2□ A/64	fe80::1

Цели

Часть 1. Локальная сеть обнаружения соседей IPv6

Часть 2: Удаленная сеть обнаружения соседей IPv6

Общие сведения

Чтобы устройство могло взаимодействовать с другим устройством, должен быть известен MAC-адрес устройства назначения. В IPv6 процесс, называемый Обнаружение соседей с использованием протокола NDP или ND, отвечает за определение MAC-адреса назначения. Вы будете собирать информацию PDU в режиме моделирования, чтобы лучше понять процесс.

Инструкции

Часть 1. Обнаружение соседних IPv6 устройств в локальной сети

В части 1 этого задания вы получите MAC-адрес устройства назначения в той же сети.

Шаг 1. Проверьте маршрутизатор на наличие обнаруженных соседей.

a. Нажмите маршрутизатор RTA. Выберите вкладку CLI и выполните команду **show ipv6 neighbors** из привилегированного режима exec. Если отображаются какие-либо записи, удалите их с помощью команды **clear ipv6 neighbors**.

b. Нажмите на **PCA1**, выберите вкладку Desktop и нажмите на значок **Command Prompt** (командной строки).

Шаг 2. Переключитесь в режим моделирования для захвата событий.

c. Нажмите кнопку **Моделирование** в правом нижнем углу окна Топология в Packet Tracer.

d. Нажмите кнопку « **Show All/None** » в левой нижней части панели моделирования. Убедитесь, что **Event List Filters – Visible Events** показывает **None**.

e. В командной строке на **PCA1**выполните команду **ping —n 1 2001:db8:acad:1::b**. Это приведет к запуску процесса pinging **PCA2**.

f. Нажмите кнопку **Play Capture Forward** , которая отображается в виде стрелки, указывающей вправо с вертикальной полоской в окне «Управление воспроизведением». В строке состояния над элементами управления воспроизведением должно быть указано «Captured» до 150. (Точное число может отличаться.)

g. Нажмите кнопку **Edit** (Редактировать). Выберите вкладку IPv6 вверху и установите флажки для **ICMPv6** и **NDP** . Нажмите красный значок X в правом верхнем углу окна Редактировать фильтры ACL. Теперь необходимо перечислить захваченные события. В окне должно быть около 12 записей.

Почему присутствуют ND PDU?

h. Нажмите квадрат в столбце Тип для первого события, которое должно быть **ICMPv6**.

Поскольку сообщение начинается с этого события, существует только исходящий PDU. На вкладке Модель OSI, какой тип сообщения указан для ICMPv6?

Обратите внимание, что нет адресации уровня 2. Нажмите кнопку **Next Layer >>**, чтобы получить объяснение процесса ND (Neighbor Discovery).

i. Нажмите квадрат рядом со следующим событием на панели моделирования. Он должен быть на устройстве PCA1 и тип должен быть NDP.

Что изменилось в адресации уровня 3?

Какие адреса уровня 2 отображаются?

Если узел не знает MAC-адрес назначения, специальный MAC-адрес многоадресной рассылки используется IPv6 Neighbor Discovery в качестве адреса назначения уровня 2.

j. Выберите первое событие **NDP** в SwitchA.

Есть ли разница между "In Layers" и "Out Layers" для уровня 2?

k. Выберите первое событие **NDP** на **PCA2** . Нажмите вкладку Outbound PDU Details (Сведения об исходящей PDU).

Какие адреса отображаются для следующих?

Примечание. Адреса в полях могут быть обернуты, отрегулировать размер окна PDU, чтобы сделать адресную информацию проще для чтения. Ethernet II DEST ADDR:

Ethernet II SRC ADDR:

IPv6 SRC IP:

IPv6 DST IP:

l. Выберите первое событие **NDP** в **RTA** . Почему нет Out Layers?

m. Нажмите кнопку **Next Layer >>** до конца и прочитайте шаги с 4 по 7 для получения дальнейших разъяснений.

n. Нажмите следующее событие **ICMPv6** на **PCA1** .

Имеет ли PCA1 всю необходимую информацию для связи с PCA2?

o. Нажмите последнее событие **ICMPv6** на **PCA1** . Обратите внимание, что это последнее сообщение в списке.

Что такое тип эхо-сообщения ICMPv6?

p. Нажмите **Reset Simulation** на панели «Simulation». Из командной строки PCA1 повторите **ping** на PCA2. (Подсказка: вы должны иметь возможность нажать стрелку вверх, чтобы вернуть предыдущую команду.)

q. Нажмите кнопку **Capture Forward** 5 раз, чтобы завершить процесс ping.

Почему не было событий NDP?

Часть 2. Обнаружение соседних IPv6 устройств в удаленной сети

В части 2 этого задания будут выполняться действия, аналогичные тем, которые приведены в части 1, за исключением того, что узел назначения находится в другой локальной сети. Обратите внимание, как процесс обнаружения соседей отличается от процесса, наблюдаемого в части 1. Обратите внимание на некоторые дополнительные шаги адресации, которые происходят, когда устройство взаимодействует с устройством, которое находится в другой сети.

Обязательно нажмите кнопку « **Reset Simulation** », чтобы очистить предыдущие события.

Шаг 1. Захват событий для удаленной связи.

a. Отображение и очистите все записи в таблице соседних устройств IPv6, как это было сделано в части I.
b. Перейдите в режим Simulation (Моделирование). Нажмите кнопку « **Show All/None** » в левой нижней части панели моделирования. Убедитесь, что **Event List Filters – Visible Events** показывает **None**.
c. Из командной строки на PCA1 выполните команду **ping —n 1 2001:db8:acad:2::a** на хост PCB1.
d. Нажмите кнопку **Play Capture Forward** , которая отображается в виде стрелки, указывающей вправо с вертикальной полоской в окне «Управление воспроизведением». В строке состояния над элементами управления воспроизведением должно быть указано «Captured» до 150. (Точное число может отличаться.)
e. Нажмите кнопку **Edit** (Изменить). Выберите вкладку IPv6 вверху и установите флажки для **ICMPv6** и **NDP** . Щелкните красный значок X в правом верхнем углу окна Редактировать фильтры ACL. Теперь должны быть перечислены все предыдущие события. Вы должны заметить, что на этот раз значительно больше записей.
f. Нажмите квадрат в столбце типа для первого события, которое должно быть **ICMPv6**. Поскольку сообщение начинается с этого события, существует только исходящий PDU. Обратите внимание, что в нем отсутствует информация о слое 2, как это было в предыдущем сценарии.
g. Нажмите первое событие **NDP** на устройстве **PCA1** .
   Какой адрес используется для IP-адреса Src во входящем PDU?

   Обнаружение соседей IPv6 определяет следующий пункт назначения для пересылки сообщения ICMPv6.
h. Нажмите второе событие ICMPv6 для **PCA1**. PCA1 теперь имеет достаточно информации для создания эхо-запроса ICMPv6.

   Какой MAC-адрес используется для MAC-адреса назначения?

i. Нажмите следующее событие ICMPv6 на устройстве **RTA**. Обратите внимание, что исходящий PDU от RTA не имеет адреса уровня назначения 2. Это означает, что RTA снова должен выполнить обнаружение соседей для интерфейса, который имеет сеть 2001:db8:acad:2::: потому что он не знает MAC-адреса устройств в локальной сети G0/0/1.
j. Перейдите к первому событию ICMPv6 для устройства **PCB1**.
   Что отсутствует в исходящей информации уровня 2?

k. Следующие несколько событий **NDP** связывают оставшиеся адреса IPv6 с MAC-адресами. Предыдущие события NDP связывали MAC-адреса с локальными адресами связи.
l. Перейдите к последнему набору событий ICMPv6 и обратите внимание, что все адреса были изучены. Необходимая информация теперь известна, поэтому PCB1 может отправлять эхо-ответные сообщения на PCA1.
m. Щелкните Reset Simulation на панели «Simulation». Из командной строки PCA1 повторите команду ping PCB1.
n. Нажмите кнопку Capture Forward девять раз, чтобы завершить процесс ping.

   Почему не было событий NDP?

o. Нажмите единственное событие **PCB1** в новом списке.
   Что соответствует MAC-адресу назначения?

Почему PCB1 использует MAC-адрес интерфейса маршрутизатора для создания ICMP PDU?

Шаг 2. Проверьте выходы маршрутизатора.

a. Вернитесь в режим реального времени (**Realtime**).

b. Нажмите кнопку **RTA** и выберите вкладку CLI. В командной строке маршрутизатора введите команду **show ipv6 neighbors**.

Сколько адресов в списке?

С какими устройствами связаны эти адреса?

Имеются ли какие-либо записи для PCA2 (почему или почему нет)?

c. Запустите эхо-запрос до **PCA2** с маршрутизатора.

d. Выполните команду **show lldp neighbors**.

Существуют ли записи для PCA2?

Вопросы для повторения

1. Когда устройство требует процесса обнаружения соседей IPv6?

2. Как маршрутизатор помогает минимизировать объем трафика IPv6 Neighbor Discovery в сети?
3. Как IPv6 минимизирует влияние процесса ND на сетевые узлы?

4. Чем отличается процесс обнаружения соседей, когда узел назначения находится в одной локальной сети и когда он находится в удаленной локальной сети?

Лабораторная работа 11
Cisco Packet Tracer. Настройка исходных параметров маршрутизатора.

Задачи

Часть 1. Проверка конфигурации маршрутизатора по умолчанию

Часть 2. Настройка и проверка начальной конфигурации маршрутизатора

Часть 3. Сохранение файла текущей конфигурации

Общие сведения

В этом упражнении вы выполните основные настройки маршрутизатора. Вы обеспечите безопасность доступа к интерфейсу командной строки (CLI) и порту консоли с помощью зашифрованных и открытых паролей. Также вы настроите сообщения для пользователей, входящих в систему маршрутизатора. Эти сообщения служат для предупреждения пользователей о запрете несанкционированного доступа. В завершение вы проверите и сохраните текущую конфигурацию.

Инструкции

Часть 1. Проверка конфигурации маршрутизатора по умолчанию Шаг

1. Установите подключение к консоли маршрутизатора R1.

a. Выберите кабель **Console** (Консольный) из списка доступных подключений.
b. Нажмите **PCA** и выберите разъем **RS 232**.
c. Нажмите **R1** и выберите **Console** (Консольный).
d. Нажмите **PCA**, откройте вкладку **Desktop** (Рабочий стол) и выберите **Terminal** (Терминал).
e. Нажмите кнопку **OK**, а затем клавишу **ENTER**. Теперь вы можете настроить маршрутизатор **R1**. **Шаг 2. Войдите в привилегированный режим и проверьте текущую конфигурацию.**

В привилегированном режиме EXEC доступны все команды маршрутизатора. Но поскольку многие привилегированные команды задают рабочие параметры, привилегированный доступ должен быть защищен паролем во избежание несанкционированного использования.

a. Перейдите в привилегированный режим EXEC, выполнив команду **enable**.

Router> **enable**
Router# Обратите внимание, что командная строка изменилась, указывая на привилегированный режим EXEC.

b. Введите команду **show running-config**.

Router# **show running-config**
Как называется узел маршрутизатора?
Сколько у маршрутизатора интерфейсов Fast Ethernet?

Сколько у маршрутизатора интерфейсов Gigabit Ethernet?
Сколько у маршрутизатора последовательных интерфейсов? Каков диапазон значений, отображаемых в vty-линиях?

c. Отображает текущее содержимое NVRAM.

Router# **show startup-config** startup-config is not present
Почему маршрутизатор отвечает сообщением **startup-config is not present** (startup-config отсутствует)?

Часть 2. Настройка и проверка начальной конфигурации маршрутизатора

Для настройки параметров маршрутизатора, возможно, потребуется переключаться между режимами настройки. Обратите внимание, как изменяется командная строка при перемещении через режимы конфигурации IOS.

Шаг 1. Настройте начальные параметры на маршрутизаторе R1.

Примечание. Если вы не можете запомнить команды, см. содержимое этого раздела. Команды используются те же, что и для настройки коммутатора.

a. Введите **R1** в качестве имени хоста.
b. Создайте текст сообщения текущего дня: **Unauthorized access is strictly prohibited**
(Несанкционированный доступ строго запрещен).
c. Зашифруйте все открытые пароли.
Используйте следующие пароли.
1) Привилегированный режим EXEC, незашифрованный: **cisco**
2) Привилегированный режим EXEC, зашифрованный: **itsasecret.**
3) Консольный режим: **letmein**

Шаг 2. Проверьте начальные параметры на маршрутизаторе R1.

a. Проверьте начальные параметры, просмотрев конфигурацию маршрутизатора R1.

Какую команду вы будете использовать?

b. Закройте текущий консольный сеанс. Появится сообщение:
R1 con0 is now available

Press RETURN to get started.
c. Нажмите клавишу **ENTER**. Отобразится сообщение:
Unauthorized access is strictly prohibited.

User Access Verification Password:

Зачем на всех маршрутизаторах должен быть баннер с сообщением текущего дня (MOTD)? Если вам не предлагается ввести пароль до того, как вы получите приглашение пользователя EXEC, какую команду консоли вы забыли настроить?

d. Введите пароли, необходимые для возврата в привилегированный режим EXEC.

Почему пароль **enable secret** позволяет перейти в привилегированный режим EXEC, а пароль **enable password** больше не действителен?
Если установить на маршрутизаторе другие пароли, они будут храниться в файле конфигурации в открытом или зашифрованном виде? Дайте пояснение.

Часть 3. Сохранение файла текущей конфигурации Шаг
1. Сохраните файл конфигурации в NVRAM.

a. Вы настроили исходные параметры маршрутизатора **R1**. Теперь выполните резервное копирование файла конфигурации в NVRAM и убедитесь, что внесенные изменения не были потеряны при перезагрузке системы или отключении питания.

Какую команду нужно ввести, чтобы сохранить конфигурацию в NVRAM?
Какая самая короткая и однозначная версия этой команды?
Какая команда отображает содержимое NVRAM?

d. Убедитесь, что все настроенные параметры записаны. Если нет, проанализируйте вывод и определите, какие команды не были выполнены или были введены неправильно. Вы также можете нажать кнопку **Check Results** в окне с инструкциями.

Шаг 2. Дополнительно: сохраните файл загрузочной конфигурации во флеш-память.

Работа с флеш-накопителем маршрутизатора будет подробнее рассмотрена в последующих главах, но сейчас вам будет полезно узнать, что в качестве дополнительной процедуры резервного копирования файл загрузочной конфигурации можно сохранить во флеш-память. По умолчанию маршрутизатор загружает стартовую конфигурацию из NVRAM. Но если память NVRAM будет повреждена, загрузочную конфигурацию можно будет восстановить, скопировав её из флеш-памяти.
Выполните следующие действия, чтобы сохранить загрузочную конфигурацию во флеш-память.

a. Проверьте содержимое флеш-памяти, выполнив команду **show flash**: R1# **show flash**
Сколько файлов хранится во флеш-памяти в данный момент?
Какой из этих файлов, по вашему мнению, является образом IOS? Почему вы считаете, что этот файл — образ IOS?

b. Сохраните файл загрузочной конфигурации во флеш-память, выполнив следующую команду:
R1# **copy startup-config flash**
Destination filename [startup-config]
Маршрутизатор предложит сохранить файл во флеш-памяти с названием в квадратных скобках. Если вы согласны, нажмите клавишу **ENTER**. Если нет, введите подходящее название и нажмите клавишу **ENTER**.

c. С помощью команды **show flash** убедитесь, что файл загрузочной конфигурации теперь хранится во флеш-памяти.

Лабораторная работа 12
Cisco Packet Tracer. Подключение маршрутизатора к локальной сети (LAN).

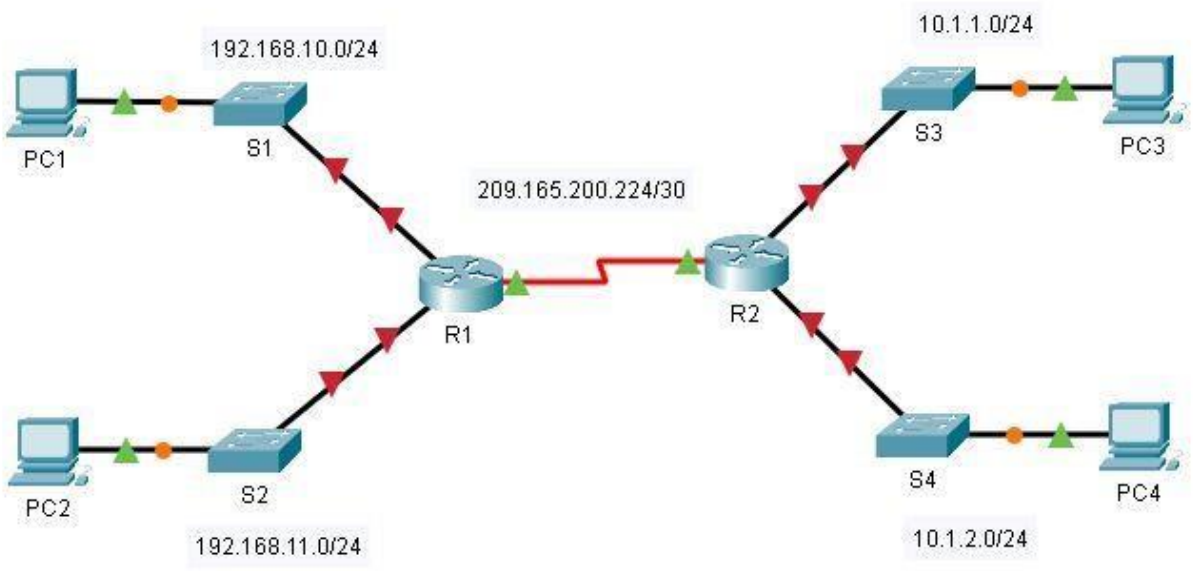


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.10.1	255.255.255.0	—
	G0/1	192.168.11.1	255.255.255.0	—
	S0/0/0 (DCE)	209.165.200.225	255.255.255.252	—
R2	G0/0	10.1.1.1	255.255.255.0	—
	G0/1	10.1.2.1	255.255.255.0	—
	S0/0/0	209.165.200.226	255.255.255.252	—
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	10.1.1.10	255.255.255.0	10.1.1.1
PC4	NIC	10.1.2.10	255.255.255.0	10.1.2.1

Задачи

Часть 1. Отображение сведений о маршрутизаторе

Часть 2. Настройка интерфейсов маршрутизатора

Часть 3. Проверка конфигурации

Общие сведения

В этом упражнении вы будете использовать различные команды **show** для отображения текущего состояния маршрутизатора. Затем вы будете использовать таблицу адресации для настройки интерфейсов Ethernet маршрутизатора. В завершение вы воспользуетесь командами для проверки и тестирования своих конфигураций.

Примечание. Маршрутизаторы в этом упражнении уже частично настроены. Некоторые из конфигураций не рассмотрены в данном курсе, но они нужны для того, чтобы помочь вам в использовании команд проверки.

Часть 1. Отображение сведений о маршрутизаторе

Шаг 1. Отобразите сведения об интерфейсе на маршрутизаторе R1.

Примечание. Чтобы получить доступ к командной строке, щелкните устройство и откройте вкладку **CLI** (Интерфейс командной строки). Пароль консоли — **cisco**. Пароль привилегированного режима EXEC — **class**.

a. Какая команда выводит статистику по всем интерфейсам, настроенным на маршрутизаторе?
b. Введите команду, чтобы отобразить статистику по интерфейсу Serial 0/0/0 на маршрутизаторе R1, и ответьте на следующие вопросы.
   1) Какой IP-адрес настроен на маршрутизаторе **R1**?
   2) Какую пропускную способность имеет интерфейс Serial 0/0/0?
c. Введите команду, чтобы отобразить статистику по интерфейсу GigabitEthernet 0/0, и ответьте на следующие вопросы.
   1) Какой IP-адрес на маршрутизаторе **R1**?
   2) Какой MAC-адрес имеет интерфейс GigabitEthernet 0/0?
   3) Какую пропускную способность (BW) имеет интерфейс GigabitEthernet 0/0? **Шаг 2. Отобразите сводный список интерфейсов маршрутизатора R1.**

a. Какая команда выводит краткую сводку по текущим интерфейсам, их состояниям и назначенным им IP-адресам?
b. Введите команду на каждом маршрутизаторе и ответьте на следующие вопросы. 1) Сколько последовательных интерфейсов на маршрутизаторах **R1** и **R2**?
   2) Сколько интерфейсов Ethernet на маршрутизаторах **R1** и **R2**?
   3) Являются ли все интерфейсы Ethernet на маршрутизаторе **R1** одинаковыми? Если ответ «Нет», объясните различия.

Шаг 3. Отобразите таблицу маршрутизации на маршрутизаторе R1.

a. Какая команда выводит на экран содержимое таблицы маршрутизации?
b. Введите команду на маршрутизаторе **R1** и ответьте на следующие вопросы.
   1) Сколько в таблице подключенных маршрутов (имеют код **C**)?
   2) Какой маршрут представлен в списке?
   3) Каким образом маршрутизатор обрабатывает пакет, предназначенный для сети, которая отсутствует в таблице маршрутизации?

Часть 2. Настройка интерфейсов маршрутизатора

Шаг 1. Настройте интерфейс GigabitEthernet 0/0 на маршрутизаторе R1.

a. Введите указанные ниже команды для задания адреса и активирования интерфейса GigabitEthernet 0/0 на маршрутизаторе **R1**.

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
```

b. Рекомендуется указать описание для каждого интерфейса, что поможет при документировании сведений о сети. Настройте описание интерфейса, указав, к какому устройству он подключен.
   R1(config-if)# **description LAN connection to S1**
c. **R1** теперь должен иметь возможность пинговать PC1.

```
R1(config-if)# end
%SYS-5-CONFIG_I: Configured from console by console
R1# ping 192.168.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/8 ms
```

Шаг 2. Настройте остальные интерфейсы Gigabit Ethernet на маршрутизаторах R1 и R2.

a. А. Используя данные из таблицы адресации, завершите настройку интерфейсов на маршрутизаторах **R1** и **R2**. Для каждого интерфейса выполните следующие действия.

1) Введите IP-адрес и активируйте интерфейс. 2)
Введите соответствующее описание.

b. Проверьте конфигурации интерфейсов.

Шаг 3. Создайте резервную копию конфигураций в NVRAM.

Сохраните файлы конфигурации на обоих маршрутизаторах в NVRAM. Какую команду вы использовали?

Часть 3. Проверка конфигурации. Шаг 1. Проверьте конфигурации интерфейсов с помощью соответствующих команд.

a. Выполните команду **show ip interface brief** на маршрутизаторах **R1** и **R2**, чтобы быстро убедиться в том, что интерфейсы имеют правильные IP-адреса и находятся в активном состоянии.

Сколько интерфейсов настроено на маршрутизаторах **R1** и **R2** с IP-адресом и находятся в активном состоянии («up»)?

Какая часть конфигурации интерфейса НЕ отображается в выходных данных команды?

С помощью каких команд можно проверить эту часть конфигурации?

b. Выполните команду **show ip route** на маршрутизаторах **R1** и **R2**, чтобы просмотреть текущие таблицы маршрутизации, и ответьте на следующие вопросы.

1) Сколько подключенных маршрутов (имеют код **C**) отображается на каждом маршрутизаторе?
2) Сколько маршрутов OSPF (имеют код **O**) отображается на каждом маршрутизаторе?
3) Если маршрутизатор содержит данные обо всех маршрутах в сети, тогда количество прямых маршрутов и динамически полученных маршрутов (OSPF) должно равняться общему количеству локальных (LAN) и глобальных (WAN) сетей. Сколько локальных (LAN) и глобальных (WAN) сетей присутствует в топологии?
4) Соответствует ли это число количеству маршрутов C и O, показанных в таблице маршрутизации?

Примечание. Если вы ответили «Нет», значит, вы настроили не все параметры. Пересмотрите шаги в части 2. **Шаг 2. Проверьте сквозное подключение через сеть.**

Теперь вы должны иметь возможность отправить эхо-запросы на любой ПК с любого ПК в сети. Кроме того, вы должны иметь возможность отправлять эхо-запросы на активные интерфейсы маршрутизаторов. Например, указанные ниже тесты должны быть успешно выполнены.

- В командной строке на компьютере PC1 отправьте эхо-запрос компьютеру PC4.
- В командной строке на маршрутизаторе R2 отправьте эхо-запрос компьютеру PC2.

Примечание. Чтобы упражнение было проще выполнять, коммутаторы в нем не настроены. Вы не сможете их пинговать.

Лабораторная работа 13

Cisco Packet Tracer. Устранение неполадок, связанных со шлюзом по умолчанию

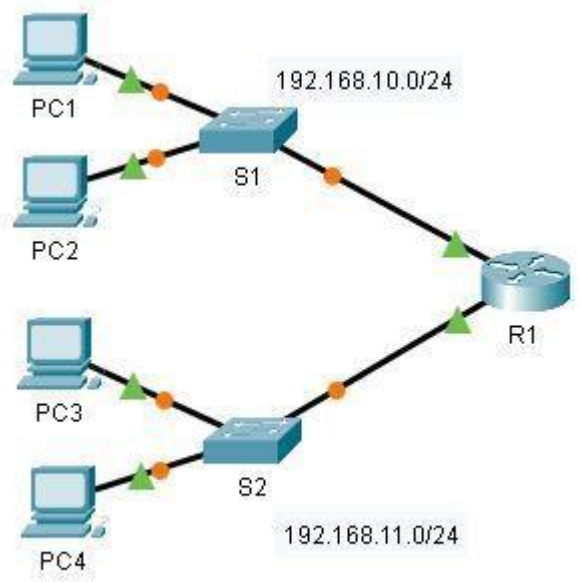


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.10.1	255.255.255.0	—
	G0/1	192.168.11.1	255.255.255.0	—
S1	VLAN 1	192.168.10.2	255.255.255.0	
S2	VLAN 1	192.168.11.2	255.255.255.0	
PC1	NIC	192.168.10.10	255.255.255.0	
PC2	NIC	192.168.10.11	255.255.255.0	
PC3	NIC	192.168.11.10	255.255.255.0	
PC4	NIC	192.168.11.11	255.255.255.0	

Задачи

Часть 1. Проверка сетевой документации и устранение проблем

Часть 2. Внедрение, проверка и документирование решений

Общие сведения

Чтобы устройство могло обмениваться данными в пределах нескольких сетей, ему должен быть присвоен IP-адрес, маска подсети и шлюз по умолчанию. Шлюз по умолчанию используется в том случае, когда узлу необходимо отправить пакет устройству, находящемуся в другой сети. Адресом шлюза по умолчанию обычно является адрес интерфейса маршрутизатора, подключенного к локальной сети, к которой подключен узел. В этом упражнении вы завершите документирование сети. После этого вы проверите сетевую документацию, протестировав сквозное подключения и устранив возникшие неполадки. Метод устранения неполадок, который вы будете использовать, включает следующие действия.

a. Проверьте сетевую документацию и выполните тестовые проверки, чтобы выявить проблемы.
b. Определите оптимальное решение для устранения конкретной проблемы.
c. Примените выбранное решение.
d. Проведите тестирование, чтобы убедиться, что проблема устранена.
e. Запишите выбранное решение.

В ходе курса CCNA вы столкнетесь с разными описаниями методов устранения неполадок, а также с другими способами тестирования и документирования проблем и решений. Это сделано намеренно. Для устранения неполадок не существует единого стандарта или шаблона. В каждой организации есть свои уникальные процессы и стандарты документирования (даже в случае, если они нормативно не утверждены). Однако все эффективные технологии устранения неполадок обычно включают в себя вышеуказанные действия.

Примечание. Если вы хорошо знакомы с конфигурацией шлюза по умолчанию, это упражнение может показаться вам сложнее, чем это нужно. Вы наверняка сможете быстрее определить и устранить возможные проблемы своими силами, чем путем выполнения этих процедур. Однако по мере изучения курса масштаб сетей и проблем, с которыми вы столкнетесь, будет становиться все сложнее. В таких ситуациях единственным эффективным способом обнаружения и устранения неполадок является использование методического подхода, аналогичного тому, который используется в данном упражнении.

Инструкции

Часть 1. Проверка сетевой документации и выявление проблем

В части 1 этого упражнения вы составите документацию и выполните проверки подключения, чтобы обнаружить проблемы. Кроме того, вы определите соответствующее решение для его последующего внедрения в части 2.

Шаг 1. Проверьте сетевую документацию и выявите проблемы.

a. Перед началом надлежащей проверки сети вам необходимо иметь полную документацию по ней. Обратите внимание, в **таблице адресации** отсутствуют некоторые данные. Заполните **таблицу адресации**, указав отсутствующие данные шлюза по умолчанию для коммутаторов и компьютеров.

b. Проверьте подключение к устройствами, принадлежащим к одной сети. Выявляя и устраняя проблемы с локальным доступом, проверить работу удаленного подключения можно быстрее, если определить работу локального подключения.

   План проверки может быть таким же простым, как список тестовых проверок связи. Используйте указанные ниже тесты для проверки локального подключения и поиска всех проблем с доступом. Первая проблема уже была задокументирована, но вы должны внедрить и проверить это решение в части 2.

Документация по тестированию и проверке

Проверка	Успешно?	Проблема	Решение	Проверено
PC1 — PC2	**Нет**	**IP-адрес на PC1**	**Изменить IP-адрес PC1**	
PC1 — S1				
PC1 — R1				

Примечание. Данная таблица является только примером. Вы должны создать свой собственный документ. Вы можете составить таблицу на листе бумаги, воспользоваться текстовым редактором или электронной таблицей. За дополнительной информацией обращайтесь к инструктору.

c. Проверьте подключение к удаленным устройствам (например, связь между компьютерами PC1 и PC4) и задокументируйте все проблемы. Зачастую такой процесс называется *сквозным подключением*. Это означает, что все устройства в сети имеют все возможности подключения, разрешаемые сетевой политикой.

Примечание. Проверку подключения к удаленным устройствам возможно еще нельзя выполнить, потому что сначала необходимо решить проблемы локальной сети. После решения этих проблем вернитесь к данному шагу и проверьте подключение между сетями. **Шаг 2. Определите оптимальное решения для устранения проблемы.**

a. Для поиска причины проблемы используйте полученные знания о принципах работы сети, а также свои навыки по настройке устройств. Например, коммутатор S1 не является причиной проблемы связи между компьютерами PC1 и PC2. Световой индикатор сети горит зеленым, а конфигурация коммутатора S1 не предусматривает передачу трафика между компьютерами PC1 и PC2. Таким образом, проблема должна быть на стороне компьютера PC1 или PC2 или обоих устройствах.

b. Проверьте параметры адресации устройства, чтобы убедиться в том, что они соответствуют сетевой документации. Например, команда **ipconfig** показывает, что компьютер PC1 имеет неправильный IP-адрес.

c. Предложите решение, которое, по вашему мнению, может решить проблему, и задокументируйте его. Например, изменить IP-адрес компьютера PC1 согласно документации.

Примечание. Зачастую решений может быть несколько. Однако оптимальным методом устранения неполадки является внедрение только одного решения. В более сложном случае внедрение нескольких решений может привести к возникновению дополнительных проблем.

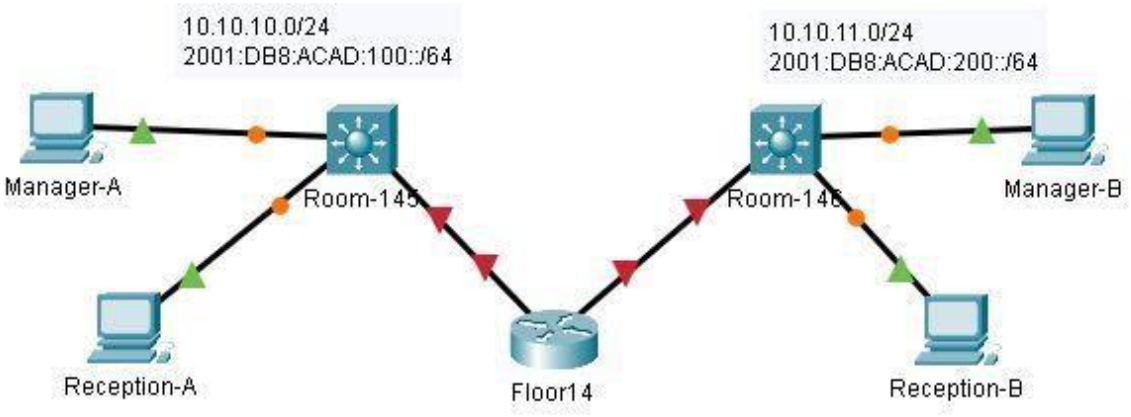
Часть 2. Внедрение, проверка и документирование решений

В части 2 этого упражнения вы внедрите решения, которые были определены в части 1. Затем вы проверите работу этих решений. Для завершения поиска всех проблем вам может понадобиться вернуться к части 1. **Шаг 1. Внедрите решения для устранения проблем подключения.**

См. данные документации в части 1. Выберите первую проблему и внедрите свое предложенное решение. Например, исправьте IP-адрес на компьютере PC1. **Шаг 2. Убедитесь, что проблема решена.**

a. Убедитесь, что ваше решение устранило проблему. Для этого выполните ту же проверку, в ходе которого была выявлена проблема. Например, можно ли теперь отправить эхо-запрос с компьютера PC1 на компьютер PC2?
b. Если проблема решена, укажите это в своей документации. Например, в приведенной выше таблице достаточно будет поставить галочку в столбце «Проверено». **Шаг 3. Убедитесь в том, что все проблемы решены.**
a. Если у вас остались проблемы, для которых решения еще не были внедрены, вернитесь к части 2, шаг 1.
b. Если все текущие проблемы устранены, решены ли проблемы с удаленными подключениями (например, можно ли отправить эхо-запрос с компьютера PC1 на компьютер PC4)? Если ответ отрицательный, вернитесь к части 1, шаг 1B, чтобы проверить удаленное подключение.

Лабораторная работа 14
Packet Tracer - базовая конфигурация устройства



Топология

Будет получена одна из трех возможных топологий.

Таблица адресации

Устройство	Интерфейс	IP-адрес	Шлюз по умолчанию
[[R1Name]]	G0/0	[[R1G0Add]]/24	Нет
		[[R1G0Addv6]]/64	
		[[R1G0Addv6LL]]	
	G0/1	[[R1G1Add]]/24	Нет
		[[R1G1Addv6]]/64	
		[[R1G1Addv6LL]]	
[[S1Name]]	VLAN 1	Коммутатор [[S1Add]]	
[[S2Name]]	VLAN 1	[[S2Add]]/24	
[[PC1Name]]	NIC	[[PC1Add]]/24	
		[[PC1Addv6]]/64	
[[PC2Name]]	NIC	[[PC2Add]]/24	
		[[PC2Addv6]]/64	
[[PC3Name]]	NIC	[[PC3Add]]/24	
		[[PC3Addv6]]/64	
[[PC4Name]]	NIC	[[PC4Add]]/24	
		[[PC4Addv6]]/64	

Цели

- Составление сетевой документации
- Настройка базовых параметров маршрутизатора и коммутатора. Проверка подключения и устранение неполадок.

Сценарий

Ваши навыки и умения специалиста по обслуживанию локальных сетей (LAN) приятно удивили вашего сетевого администратора. Теперь она предлагает, чтобы вы продемонстрировали навыки по настройке маршрутизатора, соединяющего две локальные сети (LAN). Вам необходимо будет выполнить настройку базовых параметров маршрутизатора и коммутатора с помощью операционной системы Cisco IOS. Вы также будете настраивать IPv6-адреса на сетевых устройствах и узлах. Затем вам необходимо будет проверить заданные параметры, протестировав надежность сквозного соединения. Цель состоит в том, чтобы установить связь между всеми устройствами.

Примечание. Интерфейс VLAN1 на **[[S1Name]]** не будет доступен по протоколу IPv6. В этом действии вы настроили **[[R1Name]]** маршрутизатор, **[[S2Name]]** и **хосты ПК** .

Примечание. Packet Tracer не оценивает некоторые настроенные значения, однако эти значения необходимы для полного подключения в сети.

Требования

- Внесите в таблицу адресации отсутствующие данные.
- Дайте маршрутизатору название **[[R1Name]**], а второму коммутатору — **[[S2Name]]**. Вы не сможете получить доступ к коммутатору **[[S1Name]]** .
- Во всех строках для перехода в пользовательский режим EXEC используйте пароль **cisco**.
- Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному пользовательскому режиму.
- Зашифруйте все открытые пароли.
- Настройте соответствующий баннер.
- Настройте адресацию IPv4 и IPv6 для коммутатора **[R1Name]]** в соответствии с таблицей адресации.
- Настройте адресацию IPv4 и IPv6 для коммутатора **[S2Name]]** в соответствии с таблицей адресации.
- Узлы частично настроены. Выполните адресацию IPv4 и полностью настройте адреса IPv6 в соответствии с таблицей адресации.
- Задокументируйте описания интерфейсов, включая интерфейс коммутатора **[[S2Name]]** сети VLAN 1.
- Сохраните настройки.
- Убедитесь в наличии соединения между всеми устройствами. Теперь все устройства должны успешно отправлять ping-запросы другим устройствам с адресов IPv4 и IPv6.
- Устраните все неполадки и задокументируйте их. Внедрите решения, необходимые для активации и проверки сквозных соединений.

Примечание. Чтобы проверить, как выполнено упражнение, нажмите кнопку **Check Results** (Проверить результаты). Нажмите **кнопку Reset Activity** (Сбросить упражнение), чтобы создать новый набор требований**.**

ID: [[indexNames]][[indexAdds]][[indexTopos]]

Лабораторная работа 15
Packet Tracer — Разделение IPv4-сети на подсети

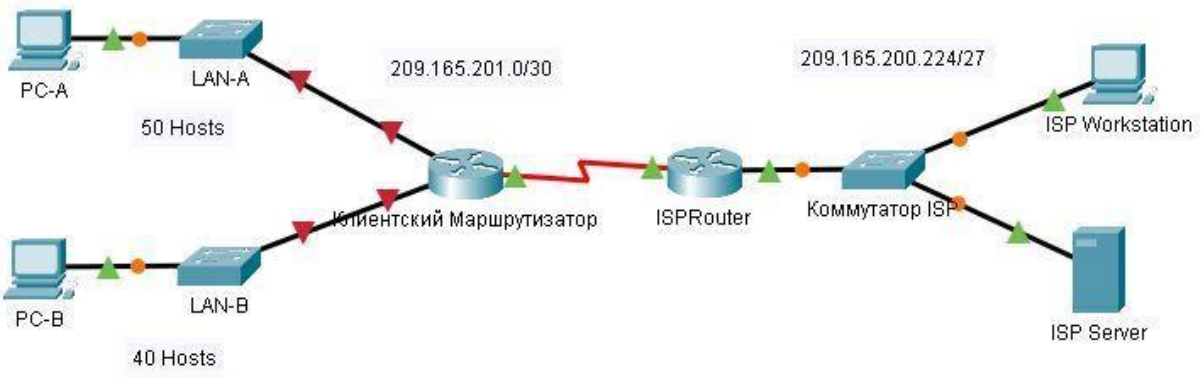


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Клиентский Маршрутизатор	G0/0			—
	G0/1			
	S0/1/0	209.165.201.2	255.255.255.252	
Коммутатор LAN-A	VLAN1			
Коммутатор LAN-B	VLAN1			
PC-A	NIC			
PC-B	NIC			
ISPRouter	G0/0	209.165.200.225	255.255.255.224	—
	S0/1/0	209.165.201.1	255.255.255.252	
ISPSwitch	VLAN1	209.165.200.226	255.255.255.224	209.165.200.225
ISP Workstation	NIC	209.165.200.235.	255.255.255.224	209.165.200.225
ISP Server	NIC	209.165.200.240	255.255.255.224	209.165.200.225

Цели

Часть 1. Разработка схемы разделения сети на подсети

Часть 2. Настройка устройств

Часть 3. Проверка сети и устранение неполадок

Общие сведения/сценарий

В этом действии сеть клиента будет подсеть на несколько подсетей. При создании схемы подсети необходимо учитывать количество компьютеров каждой подсети и другие аспекты, например дальнейшее расширение узлов в сети.

После того как вы составите схему разделения на подсети и диаграмму сети и укажите IP-адреса узлов и интерфейсов, вам нужно будет настроить компьютеры и интерфейсы маршрутизаторов и коммутаторов. После того как сетевые устройства и компьютеры будут настроены, вы проверите сетевые подключения с помощью команды **ping**.

Инструкции

Часть 1. Разделение на подсети назначенной сети

Шаг 1. Создайте схему разделения на подсети, которая соответствует необходимому количеству подсетей и адресов узлов.

В этом случае вы являетесь сетевым специалистом, назначенным для установки новой сети для клиента. Вам необходимо создать несколько подсетей в адресном пространстве сети 192.168.0.0/24 в соответствии со следующими требованиями.

a. Первая подсеть — сеть LAN-A. Необходимо не меньше 50 IP-адресов узла.
b. Вторая подсеть — сеть LAN-B. Необходимо не меньше 40 IP-адресов узла.

c. Вам также необходимы две дополнительные неиспользуемые подсети для дальнейшего расширения сети.

Примечание. Маски подсети произвольной длины использоваться не будут. Все маски подсети для устройств будут иметь одинаковую длину.

d. Составить схему разделения на подсети, отвечающую указанным условиям, помогут следующие вопросы.

Сколько адресов узлов необходимо для самой крупной подсети? Каково минимальное количество необходимых подсетей?

Сеть, которую необходимо разделить на подсети, имеет адрес 192.168.0.0/24. Как маска подсети /24 будет выглядеть в двоичном формате?

e. Маска подсети состоит из двух частей — сетевой и узловой. В двоичном формате они представлены в маске подсети единицами и нулями.

Что в маске сети представляют единицы? Что в маске сети представляют нули?

f. Чтобы разделить сеть на подсети, биты из узловой части исходной маски сети заменяются битами подсети. Количество бит подсетей определяет количество подсетей.

Если каждая из возможных масок подсети представлена в указанном двоичном формате, сколько подсетей и сколько узлов будет создано в каждом примере?

Совет. Помните, что количество бит в узловой части (во второй степени) определяет количество узлов для каждой подсети (минус 2), а количество бит в части подсети (во второй степени) определяет количество подсетей. Биты подсетей (выделены полужирным шрифтом) — это биты, заимствованные за пределами исходной маски подсети /24. /24 — префиксная запись с косой чертой, которая соответствует десятичному представлению маски 255.255.255.0.

1) (/25) 11111111111111.111111111111.**1**0000000 Эквивалент десятичного представления маски подсети с разделением точками:

   _____

   Количество подсетей? Количество узлов

2) (/26) 11111111111111.111111111111.**11**000000 Эквивалент десятичного представления маски подсети с разделением точками:

   _____

   Количество подсетей? Количество узлов

3) (/27) 11111111111111.111111111111.**111**00000 Эквивалент десятичного представления маски подсети с разделением точками:

   _____ Количество подсетей? Количество узлов

4) (/28) 11111111111111.111111111111.**1111**0000 Эквивалент десятичного представления маски подсети с разделением точками:

   _____

   Количество подсетей? Количество узлов

5) (/29) 11111111111111.111111111111.**11111**000 Эквивалент десятичного представления маски подсети с разделением точками:

   _____

   Количество подсетей? Количество узлов

6) (/30) 11111111111111.111111111111.**111111**00 Эквивалент десятичного представления маски подсети с разделением точками:

   _____ Количество подсетей? Количество узлов

   Учитывая ваши ответы, какие маски подсети соответствуют минимальному необходимому количеству адресов узлов?

   Учитывая ваши ответы, какие маски подсети соответствуют минимальному необходимому количеству подсетей?

Учитывая ваши ответы, какая маска подсети соответствует минимальному необходимому количеству как узлов, так и подсетей?

Выяснив, какая маска подсети соответствует всем указанным требованиям к сети, вы определите каждую подсеть, начиная с исходного сетевого адреса. Ниже перечислите все подсети от первой до последней. Помните, что первая подсеть — 192.168.0.0 с новой полученной маской подсети.

Адрес подсети	Префикс	Маска подсети

Шаг 2. Заполните отсутствующие IP-адреса в таблице адресации

Назначение IP-адресов на основе следующих критериев: В качестве примера используйте параметры сети ISP Network.

a. Назначьте первую подсеть LAN-A.
   1) Используйте первый адрес узла для интерфейса CustomerRouter, подключенного к коммутатору LAN-A.
   2) Используйте второй адрес узла для коммутатора LAN-A. Убедитесь, что для коммутатора назначен адрес шлюза по умолчанию.
   3) Используйте последний адрес узла для PC-A. Убедитесь, что для PC назначен адрес шлюза по умолчанию.

b. Назначьте вторую подсеть LAN-B.
   1) Используйте первый адрес узла для интерфейса CustomerRouter, подключенного к коммутатору LAN-B.
   2) Используйте второй адрес узла для коммутатора LAN-B. Убедитесь, что для коммутатора назначен адрес шлюза по умолчанию.
   3) Используйте последний адрес узла для PC-B. Убедитесь, что для PC назначен адрес шлюза по умолчанию.

Часть 2. Настройка устройств

Настройте базовые параметры на компьютерах, маршрутизаторах и коммутаторах. Имена и адреса устройств указаны в таблице адресации. **Шаг 1. Настройка CustomerRouter.**

a. Установите секретный пароль включения на CustomerRouter в **Class123**
b. Установите пароль для входа в консоль на **Cisco123**.
c. Настройте **CustomerRouter** в качестве имени узла для маршрутизатора.
d. Укажите и активируйте IP-адреса и маски подсети для интерфейсов G0/0 и G0/1.
e. Сохраните текущую конфигурацию в файл загрузочной конфигурации. **Шаг 2. Настройте два коммутатора локальной сети клиента.**

Настройте IP-адреса на интерфейсе VLAN 1 на двух коммутаторах локальной сети клиентов. На каждом коммутаторе настройте шлюз по умолчанию.

Шаг 3. Настройте интерфейсы ПК.

Настройте IP-адрес, маску подсети и настройки шлюза по умолчанию на **PC-A** и **PC-Б**.

Часть 3. Проверка сети и устранение неполадок

В части 3 вы проверите подключение сети с помощью команды **ping**.

a. Проверьте, может ли PC-A установить связь со своим шлюзом по умолчанию. Получен ли ответ?
b. Проверьте, может ли PC-A установить связь со своим шлюзом по умолчанию. Получен ли ответ?
c. Определите, может ли PC-A взаимодействовать с PC-B. Вы получили ответ?

Если вы ответили отрицательно на любой из заданных выше вопросов, вернитесь назад и проверьте введенные IP-адреса и маски подсети, а также убедитесь в том, что шлюзы по умолчанию PC-A и PC-B правильно настроены.

Лабораторная работа 16

Packet Tracer. Сценарий разделения на подсети

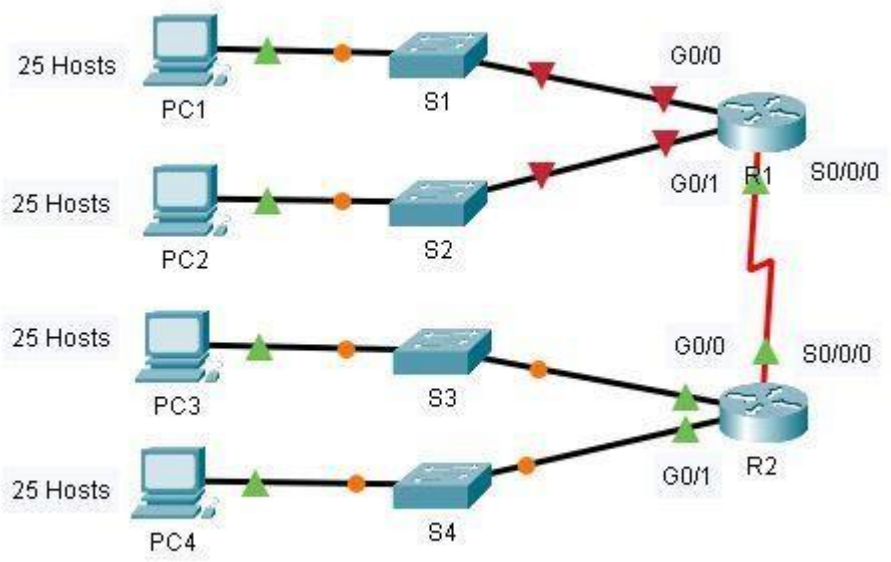


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0			
	G0/1			
	S0/0/0			
R2	G0/0			
	G0/1			
	S0/0/0			
S1	VLAN 1			
S2	VLAN 1			
S3	VLAN 1			
S4	VLAN 1			
PC1	NIC			
PC2	NIC			
PC3	NIC			
PC4	NIC			

Задачи

Часть 1. Разработка схемы IP-адресации

Часть 2. Назначение сетевым устройствам IP-адресов и проверка подключения

Сценарий

В этом упражнении вам предоставляется сетевой адрес 192.168.100.0/24 для подсети, и вы должны составить схему IP-адресации сети, изображенной в Packet Tracer. Для каждой локальной сети (LAN) в сети требуется по крайней мере, 25 адресов для оконечных устройств, коммутатора и маршрутизатора.

Для соединения между маршрутизаторами R1 и R2 потребуется по одному IP-адресу на каждом конце канала.

Инструкции

Часть 1. Разработка схемы IP-адресации

Шаг 1. Разбейте сеть 192.168.100.0/24 на нужное количество подсетей.

a. Сколько потребуется подсетей в соответствии с имеющейся топологией ?

b. Сколько бит необходимо заимствовать для поддержки нескольких подсетей в таблице топологии?

c. Сколько в результате этого создается подсетей?

d. Сколько при этом в каждой подсети будет доступно узлов?

Примечание. Если ваш ответ — менее 25 узлов, значит, вы позаимствовали слишком много бит.

e. Рассчитайте двоичное значение для первых пяти подсетей. Первые две подсети были созданы для вас.

Подсеть	Сетевой адрес	Бит 7	Бит 6	Бит 5	Бит 4	Бит 3	Бит 2	Бит 1	Бит 0
0	192.168.100.	0	0	0	0	0	0	0	0
1	192.168.100.	0	0	1	0	0	0	0	0
2	192.168.100.								
3	192.168.100.								
4	192.168.100.								

f. Рассчитайте двоичное и десятичное значение новой маски подсети.

Первый октет	Второй Октет	Третий октет	Маска бит 7	Маска бит 6	Маска бит 5	Маска бит 4	Маска бит 3	Маска бит 2	Маска бит 1	Маска бит 0
11111111	11111111	11111111								
Первый десятичный октет	**Второй десятичный октет**	**Третий десятичный октет**	**Четвертый десятичный октет**							
255.	255.	255.								

g. Заполните **Таблицу подсетей**, перечислив десятичные значения всех доступных подсетей, первый и последний используемый адрес хоста и адрес трансляции. Повторяйте эти действия до тех пор, пока все адреса не будут внесены в список.

Примечание. **Возможно, потребуется заполнить не все строки. Таблица подсетей**

Номер подсети	Адрес подсети	Первый используемый адрес узла	Последний используемый адрес узла	Широковещательный адрес
0				
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Шаг 2. Назначьте подсети для сети, показанной в топологии.

a. Назначьте подсеть 0 локальной сети (LAN), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1: **192.168.100.0 /27**

b. Назначьте подсеть 1 локальной сети (LAN), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1: **192.168.100.32 /27**

c. Назначьте подсеть 2 локальной сети (LAN), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R2: **192.168.100.64 /27**

d. Назначьте подсеть 3 локальной сети (LAN), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R2: **192.168.100.96 /27**

e. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2: **192.168.100.128 /27** **Шаг 3. Задокументируйте схему адресации.**

Заполните **таблицу адресации**, используя следующие рекомендации.

a. Назначьте первые используемые IP-адреса на каждую подсеть маршрутизатора R1 для двух каналов локальной сети (LAN) и одного канала WAN.

b. Назначьте первые используемые IP-адреса на каждую подсеть маршрутизатора R2 для каналов локальной сети (LAN). Последний из используемых IP-адресов назначьте каналу WAN.

c. Назначьте коммутаторам второй используемый IP-адрес в подключенных подсетях.

d. Назначьте последние используемые IP-адреса компьютерам в каждой подсети.

Часть 2. Назначение IP-адресов сетевым устройствам и проверка подключения

Основная часть параметров IP-адресации для данной сети уже настроена. Для завершения настройки адресации выполните следующие шаги. Динамическая маршрутизация EIGRP уже настроена между R1 и R2.

Шаг 1. Настройте интерфейсы локальной сети R1.

a. Настройте оба интерфейса локальной сети с адресами из таблицы адресации.

b. Настройте интерфейсы таким образом, чтобы узлы локальных сетей имели подключение к шлюзу по умолчанию.

Шаг 2. Настройка IP-адресацию на S3.

a. Настройте интерфейс VLAN1 коммутатора с адресацией.

b. Настройте коммутатор с адресом шлюза по умолчанию. **Шаг 3. Настройка PC4.**

Настройте на PC4 адрес узла и шлюз по умолчанию. **Шаг**

4. Проверьте подключение.

Подключение можно проверить только между маршрутизатором R1, коммутатором S3 и компьютером PC4. При этом необходимо отправлять эхо-запрос на каждый IP-адрес, перечисленный в **Таблице адресации**.

Список литературы:

1. Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 2-е изд. — Москва : ИНТУИТ, 2016. — 368 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100522 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.

2. Кияев, В. И. Безопасность информационных систем : учебное пособие / В. И. Кияев, О. Н. Граничин. — 2е изд. — Москва : ИНТУИТ, 2016. — 191 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100580 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.

3. Олифер, В. Г. Основы сетей передачи данных : учебное пособие / В. Г. Олифер, Н. А. Олифер. — 2-е изд. — Москва : ИНТУИТ, 2016. — 219 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100346 (дата обращения: 15.05.2020). — Режим доступа: для авториз. пользователей.

4. Построение коммутируемых компьютерных сетей : учебное пособие / Е. В. Смирнова, И. В. Баскаков, А. В. Пролетарский, Р. А. Федотов. — 2-е изд. — Москва : ИНТУИТ, 2016. — 428 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100370 (дата обращения:
15.05.2020). — Режим доступа: для авториз. пользователей

Интернет ресурсы: Academy Cisco Netacad.com

Используемое программное обеспечение:

- эмулятор сетей PacketTracer.версия 7.x;
- эмулятор сетей GNS3 2.*
- эмулятор сетей eNSP 1.3.*
- гипервизор Oracle Virtual Box 5.*