Министерство науки и высшего образования
Российской Федерации
Братский педагогический колледж
федерального государственного бюджетного
образовательного учреждения высшего
образования
«Братский государственный университет»

КОМПЬЮТЕРНЫЕ СЕТИ

методические рекомендации
по выполнению лабораторных работ

для студентов III курса
очной формы обучения
специальности
09.02.07 Информационные системы и программирование

Автор: Ю.Н. Войтухов

Братск, 2020

Компьютерные сети. Методические рекомендации по выполнению лабораторных работ. /Сост. Ю.Н. Войтухов.- Братск, 2020. - 58 с.

Методические рекомендации содержат указания к выполнению лабораторных работ по дисциплине «Компьютерные сети». Предназначены для студентов специальности 09.02.07 Информационные системы и программирование.

Печатается по решению научно-методического совета
Братского педагогического колледжа ФГБОУ ВО «БрГУ»
665709, г. Братск, ул. Макаренко 40

СОДЕРЖАНИЕ

Лабораторная работа №1 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 симуляции — первый шаг на пути к пониманию принципов работы пакета проколов TCP/IP и его взаимосвязи с моделью OSI. Режим симуляции позволяет просматривать содержимое пересылаемых по сети данных на каждом из уровней.

При передаче 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 симуляции 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.

Часть 1. Изучение HTTP-трафика

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

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

В правом нижнем углу интерфейса Packet Tracer находятся вкладки для переключения между режимами **Realtime** (режим реального времени) и **Simulation** (режим симуляции). 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 симуляции. В режиме симуляции пакеты отображаются как анимированные конверты, временем управляют события и пользователи могут пошагово переходить от одного сетевого события к другому.

А. Щелкните значок режима **Simulation** для переключения из режима **реального времени** в режим **симуляции**.

Б. Выберите в списке **Event List Filters** (Фильтры списка событий) пункт **HTTP**.

1. HTTP в этот момент уже может быть единственным видимым событием. Нажмите кнопку **Edit Filters** (Изменить фильтры) для отображения доступных видимых событий. 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**, пока все флажки не будут сняты, а затем выберите **HTTP**. Щелкните любое место за пределами поля **Edit Filters**, чтобы скрыть его. В разделе видимых событий теперь отображается только HTTP.

Шаг 2. Сгенерируйте веб-трафик (HTTP).

На данный момент панель симуляции пуста. В верхней части панели симуляции видны наименования шести столбцов списка событий. По мере генерации и продвижения трафика в списке будут появляться события. Столбец **Info** (Информация) содержит информацию о конкретном событии.

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.

А. Щелкните **Web Client** на крайней левой панели.

Б. Щелкните вкладку **Desktop** (Рабочий стол), затем щелкните значок **Web Browser**, чтобы открыть веб-браузер.

В. В поле URL введите адрес **www.osi.local** и нажмите кнопку **Go**.

Поскольку время в режиме симуляции привязано к событиям, для отображения событий в сети необходимо использовать кнопку **Capture/Forward** (Захват/вперед).

Г. 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.

А. Щелкните первый цветной квадрат в столбце **Info** (Информация) списка событий **Event List**. Вам может понадобиться развернуть **панель симуляции** или использовать полосу прокрутки непосредственно под списком событий **Event List**.

Откроется окно **PDU Information at Device: Web Client** (Информация о PDU на устройстве: веб-клиент). 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**.

Б. Убедитесь в том, что выбрана вкладка **OSI Model**. Убедитесь, что в столбце **Out Layers** (Исходящие уровни) выделено поле **Layer 7** (Уровень 7).

Какой текст отображается рядом с меткой **Layer 7**?

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

В. Нажмите кнопку **Next Layer** (Следующий уровень). Должен быть выделен уровень 4. Какое значение имеет параметр **Dst Port** (Порт назначения)?

Г. Нажмите кнопку **Next Layer** (Следующий уровень). Должен быть выделен уровень 3. Какое значение имеет параметр **Dest. IP** (IP-адрес назначения)?

Д. Нажмите кнопку **Next Layer** (Следующий уровень). Какая информация отображается на этом уровне?

Е. 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**?

Ж. Щелкните следующий цветной квадрат в столбце **Info** списка **Event List**. Активен только уровень 1 (не отображается серым цветом). Устройство извлекает кадр из буфера и помещает его в сеть.

З. 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.

И. Щелкните вкладку **Outbound PDU Details** (Сведения об исходящей PDU). Прокрутите вниз до раздела **HTTP**.

Какова первая строка в показанном HTTP-сообщении?

К. Щелкните последний цветной квадрат в столбце **Info**. Сколько вкладок отображается с этим событием и почему?

Часть 2. Отображение элементов семейства протоколов TCP/IP

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

Шаг 1. Просмотрите дополнительные события

А. Закройте все окна со сведениями о PDU.

Б. В разделе Event List Filters > Visible Events (Фильтры списка событий > Видимые события) нажмите кнопку **Show All** (Показать все).

Какие дополнительные типы событий показаны?

Эти дополнительные записи играют различные роли в семействе протоколов TCP/IP. Если в списке указан ARP (протокол разрешения адресов), то этот протокол осуществляет поиск MAC-адресов. 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).

В. Щелкните первое событие DNS в столбце **Info**. 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 DNS-запрос на DNS-сервер]) Это очень полезная информация, которая помогает понять, что происходит во время процесса связи.

Г. Щелкните вкладку **Outbound PDU Details** (Сведения об исходящей PDU). Какие сведения показаны в поле **NAME**: в разделе DNS QUERY?

Д. Щелкните последний цветной квадрат DNS **Info** в списке событий. Какое устройство отображено?

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

Е. 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).

Ж. 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).

Задача

В этом упражнении по симуляции 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 №2 Настройка начальных параметров коммутатора

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

В этом упражнении вы осуществите базовую настройку 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.

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 команд привилегированного режима EXEC включает команды, которые доступны в пользовательском режиме EXEC, а также команду **configure**, открывающую доступ к остальным командным режимам.

А. Щелкните **S1**, а затем вкладку **CLI**. Нажмите клавишу ввода.

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

Switch> **enable**

Switch#

Обратите внимание, что командная строка изменилась, отображая переключение в привилегированный режим EXEC.

Шаг 2. Изучите текущую конфигурацию коммутатора.

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

Switch# **show running-config**

Б. Ответьте на следующие вопросы.

1. Сколько у коммутатора интерфейсов FastEthernet?
2. Сколько у коммутатора интерфейсов Gigabit Ethernet?
3. Каков диапазон значений, отображаемых в линиях vty?
4. Какая команда отображает текущее содержимое энергонезависимого ОЗУ (NVRAM)?
5. 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 между режимами командной строки 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**
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# **line console 0**
S1(config-line)# **password letmein**
S1(config-line)# **login**
S1(config-line)# **exit**
S1(config)# **exit**
%SYS-5-CONFIG_I: Configured from console by console
S1#

Для чего нужна команда **login**?

Шаг 3. Убедитесь, что доступ к консоли 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. Защитите 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 «О». Настройка пароля будет оценена как выполненная успешно только после того как вы зашифруете его на 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.

А. Введите команду **exit** еще раз, чтобы выйти из коммутатора.

Б. Нажмите **<Enter>**, после чего вам будет предложено ввести пароль.

User Access Verification

Password:

В. Первый пароль — это пароль для консоли, который был задан для **line con 0**. Введите этот пароль, чтобы вернуться в пользовательский режим EXEC.

Г. Введите команду для доступа к привилегированному режиму.

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

Е. 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 быть небезопасно, так как пароль может увидеть любой находящийся рядом человек.

Шаг 6. Настройте зашифрованный пароль для защиты доступа к привилегированному режиму.

Пароль enable password 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** имеет приоритет перед паролем **enable** password. Если для коммутатора заданы оба пароля, для перехода в привилегированный режим EXEC нужно ввести пароль **enable secret**.

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

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

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

S1# **show run**

Б. Что отображается при выводе пароля **enable secret**?

В. Почему пароль **enable secret** отображается не так, как задан?

Шаг 8. Зашифруйте пароли enable и console.

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

S1# **config t**

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

S1(config)# **exit**

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

Часть 3. Настройка баннера MOTD (сообщения дня)

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#

1. Когда будет отображаться этот баннер?
2. Зачем на всех коммутаторах должен быть баннер MOTD?

Часть 4. Сохранение файлов конфигурации в NVRAM

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

Шаг 2. Сохраните файл конфигурации.

Вы завершили 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**?

Шаг 3. 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.

А. Имя устройства: **S2**.

Б. Защитите доступ к консоли паролем **letmein**.

В. Задайте пароль enable password **c1$c0** и пароль enable secret **itsasecret**.

Г. Введите следующее сообщение для пользователей, выполняющих вход в систему на коммутаторе:

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

Д. Зашифруйте все открытые пароли.

Е. Проверьте правильность конфигурации.

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

Лабораторная работа №3 Обеспечение базовой связности

Таблица адресации

Устройство	интерфейс	IP-адрес	Subnet Mask (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

Задачи

Часть 1. Базовая настройка коммутаторов S1 и S2

Часть 2. Настройка ПК

Часть 3. Настройка интерфейса управления коммутатором

Общие сведения

В этом упражнении вы сначала базовую настройку коммутаторов. Затем вы обеспечите базовую связность, настроив IP-адресацию на коммутаторах и ПК. Завершив настройку IP-адресации, вы будете использовать различные команды **show**, чтобы проверить настройки, а также команду **ping** для проверки базовой связности между устройствами.

Часть 1. Базовая настройка коммутаторов S1 и S2

Выполните следующие действия на коммутаторах S1 и S2.

Шаг 1. Настройте имя узла для коммутатора S1.

А. Щелкните S1 и откройте вкладку **CLI**.

Б. Введите нужную команду, чтобы присвоить узлу имя **S1**.

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

А. В качестве пароля для консоли введите **cisco**.

Б. В качестве пароля для привилегированного режима EXEC введите **class**.

Шаг 3. Проверьте пароли, настроенные для коммутатора S1.

Как можно проверить правильность настройки паролей?

Шаг 4. Настройте баннер MOTD

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-адрес для PC1 и PC2.

Шаг 1. Настройте IP-адреса для обоих ПК.

А. Щелкните PC1 и откройте вкладку **Desktop** (Рабочий стол).

Б. Выберите **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).

В. Повторите шаги 1а и 1б для компьютера PC2.

Шаг 2. Проверьте подключение к коммутаторам.

А. Щелкните PC1. Закройте окно **IP Configuration** (Настройка IP-адресов), если оно открыто. На вкладке **Desktop** (Рабочий стол) нажмите **Command Prompt** (Командная строка).

Б. Введите команду **ping** с IP-адресом коммутатора S1 и нажмите клавишу ввода.

Packet Tracer PC Command Line 1.0

PC> **ping 192.168.1.253**

Был ли эхо-запрос обработан успешно? Дайте пояснение.

Часть 3. Настройка интерфейса управления коммутатором

Настройте IP-адреса для коммутаторов S1 и S2.

Шаг 1. Настройте IP-адрес для коммутатора S1.

Коммутаторы можно использовать в режиме «plug & play». Это значит, что они могут начать работать и без предварительной настройки. Коммутаторы пересылают данные между портами, опираясь на MAC-адреса. Для чего тогда нужно настраивать IP-адреса?

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

S1# **configure terminal**

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

S1(config)# **interface vlan 1**

S1(config-if)# **ip address 192.168.1.253 255.255.255.0**

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

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

S1(config-if)#

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

S1#

Зачем вы вводите команду **no shutdown**?

Шаг 2. Настройте IP-адрес 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 конфигурации для 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.

А. Щелкните PC1 и откройте вкладку **Desktop** (Рабочий стол).

Б. Нажмите **Command Prompt** (Командная строка).

В. С помощью команды ping проверьте доступность IP-адреса компьютера PC2.

Г. С помощью команды ping проверьте доступность IP-адреса коммутатора S1.

Д. С помощью команды ping проверьте доступность IP-адреса коммутатора S2.

Примечание. Команду **ping** можно использовать в интерфейсе командной строки коммутатора и на PC2.

Все эхо-запросы должны быть обработаны 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 Подключение проводной и беспроводной локальных сетей

Таблица адресации

Устройство	**интерфейс**	**IP-адрес**	**Подключается к**
Облачная среда	Eth6	—	Fa0/0
	Coax7	—	Port0
Кабельный модем	Port0	—	Coax7
	Port1	—	Интернет
Router0	Консоль	—	RS232
	Fa0/0	192.168.2.1/24	Eth6
	Fa0/1	10.0.0.1/24	Fa0
	Ser0/0/0	172.31.0.1/24	Ser0/0
Router1	Ser0/0	172.31.0.2/24	Ser0/0/0
	Fa1/0	172.16.0.1/24	Fa0/1
WirelessRouter	Интернет	192.168.2.2/24	порт 1
	Eth1	192.168.1.1	Fa0
Family PC	Fa0	192.168.1.102	Eth1
Switch	Fa0/1	172.16.0.2	Fa1/0
Netacad.pka	Fa0	10.0.0.254	Fa0/1
Configuration Terminal	RS232	—	Консоль

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.

Часть 1. Подключение к облаку

Шаг 1. Подключите Cloud (Облако) к маршрутизатору Router0.

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

Б. Выберите правильный кабель для подключения порта **Fa0/0 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 **Fa0/1 Router0** к порту **Fa0 netacad.pka**. Маршрутизаторы и компьютеры

обычно используют одинаковые контакты для отправки (1-й и 2-й) и получения (3-й и 6-й) данных. У кабеля, который нужно выбрать, эти пары меняются местами. 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 порта **Console Router0** к порту **RS232 Configuration Terminal**. 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 **Fa1/0 Router1** к порту **Fa0/1 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.

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

Б. 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).

А. Откройте **Terminal** на **Configuration Terminal** и примите параметры по умолчанию.

Б. Нажмите клавишу **Ввод**, чтобы открыть командную строку **Router0**.

В. Введите команду **show ip interface brief**, чтобы просмотреть состояние интерфейсов.

Часть 5. Изучение физической топологии

Шаг 1. Изучите облако.

А. Откройте вкладку **Physical Workspace** (Физическая рабочая область) или используйте сочетания клавиш **Shift+P** и **Shift+L** для переключения между логической и физической рабочими областями.

Б. Щелкните значок **Home City** (Родной город).

В. Щелкните значок **Cloud** (Облако). Сколько проводов подключено к коммутатору в синей стойке? 2

Г. Нажмите кнопку **Back** (Назад) для возврата к **Home City** (Родной город).

Шаг 2. Изучите первичную сеть.

А. Щелкните значок **Primary Network** (Первичная сеть). Удерживайте указатель мыши на разных кабелях. Что находится в таблице справа от синей стойки?

Б. Нажмите кнопку **Back** (Назад) для возврата к **Home City** (Родной город).

Шаг 3. Изучите вторичную сеть.

А. Щелкните значок **Secondary Network** (Вторичная сеть). Удерживайте указатель мыши на разных кабелях. Почему к каждому устройству подключено по два оранжевых кабеля?

Б. Нажмите кнопку **Back** (Назад) для возврата к **Home City** (Родной город).

Шаг 4. Изучите домашнюю сеть.

А. Почему домашняя сеть накрыта овальной сеткой?

Б. Щелкните значок **Home Network** (Домашняя сеть). Почему нет стойки для оборудования?

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

Лабораторная работа №5 Определение MAC- и IP-адресов

Задачи

Часть 1. Сбор сведений о единице данных протокола (PDU)

Часть 2. Вопросы для повторения

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.

Часть 1. Сбор сведений о единице данных протокола (PDU)

Примечание. Просмотрите вопросы для повторения из части 2, 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 172.16.31.2 в адрес 10.10.10.3.

А. Нажмите **172.16.31.2** и откройте окно **Command Prompt** (Командная строка).

Б. Введите команду **ping 10.10.10.3**.

В. Перейдите в режим моделирования и повторите команду **ping 10.10.10.3** . Единица данных протокола (PDU) будет показана рядом с **172.16.31.2**.

Г. Нажмите единицу данных протокола (PDU) и запишите следующие данные на вкладке **Outbound PDU Layer** (Уровень исходящего PDU)

- MAC-адрес назначения: 00D0:BA8E:741A
- MAC-адрес источника: 000C:85CC:1DA7
- IP-адрес источника: 172.16.31.2

– IP-адрес назначения: 10.10.10.3
– На устройстве: компьютер.

Д. Нажмите **Capture/Forward** (Захватить/переадресовать), 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

Проверка	На устройстве	Адрес MAC	MAC-адрес источника	IPv4-адрес источника	IPv4-адрес назначения
Эхо-запрос с 172.16.31.2 на адрес 10.10.10.3	172.16.31.2	00D0:BA8E:741A	000C:85CC:1DA7	172.16.31.2	10.10.10.3
	Концентратор	--	--	--	--
	Switch1	00D0:BA8E:741A	000C:85CC:1DA7	--	--
	Router	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.3
	Switch0	0060:4706:572B	00D0:588C:2401	--	--
	Точка доступа	--	--	--	--
	10.10.10.3	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.3

Шаг 2. Соберите дополнительные сведения о единице данных протокола (PDU) из других эхо-запросов

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

– Эхо-запрос с 10.10.10.2 на адрес 10.10.10.3
– 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
– Эхо-запрос с 172.16.31.4 на адрес 10.10.10.2
– Эхо-запрос с 172.16.31.3 на адрес 10.10.10.2.

Часть 2. 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. Копировали 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?

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 №6 Изучение таблицы ARP

Таблица адресации

Устройство	**интерфейс**	**MAC Address (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	Беспроводная сеть	0060.2F84.4AB6	F0/2
10.10.10.3	Беспроводная сеть	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

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.

Часть 1. Анализ ARP-запроса

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

А. Нажмите **172.16.31.2** и откройте окно **Command Prompt** (Командная строка).

Б. Выполните команду **arp -d**, чтобы очистить таблицу ARP.

В. 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.

Г. Нажмите кнопку **Capture/Forward** (Захватить/Далее) 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?

Д. Нажмите **Capture / Forward** (Захватить/Далее), чтобы переместить единицу данных протокола (PDU) на следующее устройство. Сколько копий единицы данных протокола (PDU) создал **Switch1**?

Е. Какой IP-адрес имеет устройство, которое приняло единицу данных протокола (PDU)?

Ж. Откройте единицу данных протокола (PDU) и изучите уровень 2. Что произошло с MAC-адресами источника и назначения?

З. Нажимайте кнопку **Capture/Forward** (Захватить/Далее) 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. Проанализируйте таблицу ARP.

А. 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?

Б. Вернитесь обратно в режим **Realtime** (Реальное время), и команда ping завершится.

В. Нажмите **172.16.31.2** и выполните команду **arp –a**. Какому IP-адресу соответствует запись MAC-адреса?

Г. 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.

А. На узле **172.16.31.2** выполните команду **ping 172.16.31.4**.

Б. Нажмите **10.10.10.2** и откройте окно **Command Prompt** (Командная строка).

В. Введите команду **ping 10.10.10.3**. Сколько ответов было отправлено и получено?

Шаг 2. Изучите таблицу MAC-адресов на коммутаторах.

А. Нажмите **Switch1**и откройте вкладку **CLI** (Интерфейс командной строки). Выполните команду **show mac-address-table**. Совпадают ли записи с указанными в таблице выше?

Б. Нажмите **Switch0** и откройте вкладку **CLI** (Интерфейс командной строки). Выполните команду **show mac-address-table**. Совпадают ли записи с указанными в таблице выше?

В. Почему два MAC-адреса связаны с одним портом?

Часть 3. Анализ процесса ARP в удаленных подключениях

Шаг 1. Сгенерируйте трафик ARP.

А. Нажмите **172.16.31.2** и откройте окно **Command Prompt** (Командная строка).

Б. Введите команду **ping 10.10.10.1**.

В. Введите **arp –a**. Какой IP-адрес имеет новая запись в таблице ARP?

Г. Выполните команду **arp -d** , чтобы очистить таблицу ARP, и перейдите в режим **моделирования**.

Д. Отправьте повторный эхо-запрос на адрес 10.10.10.1. Сколько единиц данных протокола (PDU) появилось?

Е. Нажмите кнопку **Capture/Forward** (Захватить/Далее). Нажмите единицу данных протокола (PDU), которая теперь находится на **Switch1**. Какой IP-адрес назначения ARP-запроса?

Ж. IP-адрес назначения не 10.10.10.1. Почему?

Шаг 2. Проанализируйте таблицу ARP на Router1.

А. Перейдите в режим **реального времени**. Нажмите **Router1** (Маршрутизатор 1) и откройте вкладку **CLI** (Интерфейс командной строки).

Б. Войдите в привилегированный режим EXEC и выполните команду **show mac-address-table**. Сколько MAC-адресов в таблице? Почему?

В. 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 №7 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 баннеры также предупреждают неавторизованных пользователей о том, что доступ запрещен. В завершение вы проверите и сохраните текущую конфигурацию.

Часть 1. Проверка конфигурации маршрутизатора по умолчанию

Шаг 1. Установите подключение к консоли маршрутизатора R1.

А. Из списка доступных подключений выберите **Console** (Консольный) кабель.

Б. Щелкните **PCA** и выберите **RS 232**.

В. Щелкните **R1** и выберите **Console** (Консольный).

Г. Последовательно выберите **PCA** > **Desktop** (Рабочий стол) > **Terminal** (Терминал).

Д. Нажмите кнопку **ОК** и нажмите **ВВОД**. 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.

а. Войдите в привилегированный исполнительский режим с помощью команды **enable**.

Router> **enable**

Router#

Обратите внимание, что командная строка изменилась, указывая на привилегированный режим EXEC.

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

Router# **show running-config**

с. Ответьте на следующие вопросы.

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?

Г. Выведите на экран 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 по разделам маршрутизатора.

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.

А. **R1** — это имя хоста.

Б. Используйте следующие пароли:

1) консольный режим: **letmein**;

2) привилегированный режим EXEC, незашифрованный: **cisco**;

3) привилегированный режим EXEC, зашифрованный: **itsasecret**.

В. Зашифруйте все открытые пароли.

Г. Текст сообщения текущего дня: Unauthorized access is strictly prohibited (Несанкционированный доступ строго запрещен).

Шаг 2. Проверьте начальные параметры на маршрутизаторе R1.

А. Проверьте начальные параметры, просмотрев конфигурацию маршрутизатора R1. Какую команду вы будете использовать?

Б. Закройте текущий консольный сеанс. Появится следующее сообщение:

R1 con0 is now available

Press RETURN to get started.

С. Нажмите клавишу **ВВОД**. Должно появиться следующее сообщение:

Unauthorized access is strictly prohibited.
User Access Verification
Password:

Зачем на всех маршрутизаторах должен быть баннер с сообщением текущего дня (MOTD)?

Если окно с запросом на ввод пароля не появилось, какую консольную команду вы забыли настроить?

Г. 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.

А. Теперь начальные параметры для маршрутизатора **R1** настроены. 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?

Б. Убедитесь, что все настроенные параметры записаны. Если это не так, проанализируйте выходные данные и определите, какие команды не были выполнены или не были правильно введены. Вы также можете нажать кнопку **Check Results** в окне с инструкциями.

Шаг 2. Дополнительный бонус: 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 загрузочную 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.

А. 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?

Б. Сохраните файл загрузочной конфигурации во флеш-память, выполнив следующие команды:

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**.

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

Лабораторная работа №8 Подключение маршрутизатора к локальной сети (LAN)

Таблица адресации

Устройство	**интерфейс**	**IP-адрес**	**Subnet Mask (Маска подсети)**	**Основной шлюз**
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**.

А. Какая команда выводит статистику по всем интерфейсам, настроенным на маршрутизаторе?

Б. Какая команда выводит сведения только об интерфейсе Serial 0/0/0?

В. 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?

Г. Введите команду, чтобы отобразить статистику по интерфейсу GigabitEthernet 0/0, и ответьте на следующие вопросы.

1) Какой IP-адрес настроен на маршрутизаторе **R1**?

2) Какой MAC-адрес имеет интерфейс GigabitEthernet 0/0?

3) Какую пропускную способность имеет интерфейс GigabitEthernet 0/0?

Шаг 2. Отобразите сводный список интерфейсов маршрутизатора R1.

А. Какая команда выводит краткую сводку по текущим интерфейсам, их состояниям и назначенным им IP-адресам?

Б. 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.

А. Какая команда выводит на экран содержимое таблицы маршрутизации?

Б. Введите команду на маршрутизаторе **R1** и ответьте на следующие вопросы.

1) Сколько в таблице подключенных маршрутов (имеют код «C»)?

Какой маршрут представлен в списке?

2) 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.

А. 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

Б. 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**

В. Маршрутизатор **R1** должен теперь иметь возможность отправить эхо-запрос на компьютер 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.

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.

Б. Проверьте конфигурации интерфейсов.

Шаг 3. Сделайте 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.

А. 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?

Б. 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 EIGRP (имеют код **D**) отображается на каждом маршрутизаторе?
3) Если маршрутизатор содержит данные обо всех маршрутах в сети, тогда количество прямых маршрутов и динамически полученных маршрутов (EIGRP) должно равняться общему количеству локальных (LAN) и глобальных сетей (WAN). Сколько локальных (LAN) и глобальных (WAN) сетей присутствует в топологии?

4) Соответствует ли это число количеству маршрутов C и D, 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 отправить им эхо-запрос.

Лабораторная работа №9 Настройка IPv6-адресации

Таблица адресации

Устройство	**интерфейс**	**IPv6-адрес/префикс**	**Основной шлюз**
R1	G0/0	2001:DB8:1:1::1/64	—
	G0/1	2001:DB8:1:2::1/64	—
	S0/0/0	2001:DB8:1:A001::2/64	—
	Link-local	FE80::1	—
Sales	NIC	2001:DB8:1:1::2/64	FE80::1
Урегулирование	NIC	2001:DB8:1:1::3/64	FE80::1
Бухгалтерия	NIC	2001:DB8:1:1::4/64	FE80::1
физической структуры	NIC	2001:DB8:1:2::2/64	FE80::1
Конструкторский отдел	NIC	2001:DB8:1:2::3/64	FE80::1
САПР	NIC	2001:DB8:1:2::4/64	FE80::1

Задачи

Часть 1. Настройка IPv6-адресации на маршрутизаторе

Часть 2. Настройка IPv6-адресации на серверах

Часть 3. Настройка IPv6-адресации на клиентских узлах

Часть 4. Тестирование и проверка подключения к сети

Общие сведения

В этом упражнении вам предстоит отработать настройку IPv6-адресов на маршрутизаторе, серверах и клиентских узлах. Кроме того, вы проверите выполнение IPv6-адресации.

Часть 1. Настройка IPv6-адресации на маршрутизаторе

Шаг 1. Включите пересылку IPv6-пакетов на маршрутизаторе.

А. Введите команду глобальной настройки маршрутизации одноадресной рассылки IPv6. Данная команда нужна для включения пересылки IPv6-пакетов на маршрутизаторе. Вы изучите эту команду позднее в этом семестре.

R1(config)# ipv6 unicast-routing

Шаг 2. Настройте IPv6-адресацию на GigabitEthernet0/0.

А. Нажмите на **R1** и откройте вкладку **CLI** (Интерфейс командной строки). Нажмите **Enter**.

Б. Войдите в привилегированный режим EXEC.

В. Введите команды, необходимые для перехода в режим настройки интерфейса GigabitEthernet0/0.

Г. Настройте IPv6-адрес с помощью следующей команды:

R1(config-if)# **ipv6 address 2001:DB8:1:1::1/64**

Д. Настройте локальный IPv6-адрес канала с помощью следующей команды:

R1(config-if)# **ipv6 address FE80::1 link-local**

Е. Активируйте интерфейс.

Шаг 3. Настройте IPv6-адресацию на GigabitEthernet0/1.

А. Введите команды, необходимые для перехода в режим настройки интерфейса GigabitEthernet0/1.

Б. Нужные IPv6-адреса см. в **таблице адресации**.

В. Настройте IPv6-адрес, локальный адрес канала и активируйте интерфейс.

Шаг 4. Настройте IPv6-адресацию на Serial0/0/0.

А. Введите команды, необходимые для перехода в режим настройки интерфейса Serial0/0/0.

Б. Нужные IPv6-адреса см. в **таблице адресации**.

В. Настройте IPv6-адрес, локальный адрес канала и активируйте интерфейс.

Часть 2. Настройка IPv6-адресации на серверах

Шаг 1: Настройте IPv6-адресацию на сервере Accounting (Бухгалтерия).

А. Нажмите на **Accounting** (Бухгалтерия), откройте вкладку **Desktop** (Рабочий стол) и выберите **IP Configuration** (Конфигурация IP).

Б. Установите для **IPv6-адреса** значение **2001:DB8:1:1::4** с префиксом **/64**.

В. Установите для **IPv6-шлюза** локальный адрес канала **FE80::1**.

Шаг 2: Настройте IPv6-адресацию на сервере CAD (Отдел автоматизации).

Повторите шаги от 1A до 1B для сервера **CAD** (Отдел автоматизации). IPv6-адреса см. в **таблице адресации**.

Часть 3. Настройка IPv6-адресации на клиентских узлах

Шаг 1. Настройте IPv6-адресацию на клиентских узлах Sales (Отдел продаж) и Billing (Отдел выписки счетов).

А. Нажмите на **Billing** (Отдел выписки счетов), откройте вкладку **Desktop** (Рабочий стол) и выберите **IP Configuration** (Конфигурация IP).

Б. Установите для **IPv6-адреса** значение **2001:DB8:1:1::3** с префиксом **/64**.

В. Установите для **IPv6-шлюза** локальный адрес канала **FE80::1**.

Г. Повторите шаги с 1A по 1B для узла **Sales**. IPv6-адреса см. в **таблице адресации**.

Шаг 2. Настройте IPv6-адресацию на клиентских узлах Engineering (Технический отдел) и Design (Проектный отдел).

А. Нажмите **Engineering** (Технический отдел), откройте вкладку **Desktop** (Рабочий стол) и выберите **IP Configuration** (Конфигурация IP).

Б. Установите для **IPv6-адреса** значение **2001:DB8:1:2::3** с префиксом **/64**.

В. Установите для **IPv6-шлюза** локальный адрес канала **FE80::1**.

Г. Повторите шаги с 1A по 1B для узла **Design** (Проектный отдел). IPv6-адреса см. в **таблице адресации**.

Часть 4. Тестирование и проверка подключения к сети

Шаг 1. Откройте веб-страницы с сервера на клиентских узлах.

А. Нажмите **Sales** (Отдел продаж) и откройте вкладку **Desktop** (Рабочий стол). При необходимости закройте окно **IP Configuration** (Конфигурация IP).

Б. Нажмите **Web Browser** (Веб-браузер). Введите **2001:DB8:1:1::4** в строке адреса и нажмите **Go** (вперед). Должен открыться веб-сайт **Accounting** (Бухгалтерия).

В. Введите **2001:DB8:1:2::4** в строке адреса и нажмите **Go** (Вперед). Должен открыться веб-сайт **CAD**.

Г. Повторите шаги с 1А по 1Г для других клиентских узлов.

Шаг 2. Проверьте связь с провайдером.

А. Откройте окно настройки любого клиентского ПК, нажав на его значок.

Б. На вкладке **Desktop** (Рабочий стол) нажмите **Command Prompt** (Командная строка).

В. Проверьте подключение к интернет-провайдеру с помощью следующей команды:

PC> **ping 2001:DB8:1:A001::1**

Г. Выполняйте команду **ping** на других клиентских узлах, пока не убедитесь, что у всех есть связь с провайдером.

Лабораторная работа №10 Проверка адресации IPv4 и IPv6

Таблица адресации

Устройство	**интерфейс**	**IPv4-адрес**	**Subnet Mask (Маска подсети)**	**Основной шлюз**
		IPv6-адрес/префикс		
R1	G0/0	10.10.1.97	255.255.255.224	—
		2001:DB8:1:1::1/64		—
	S0/0/1	10.10.1.6	255.255.255.252	—
		2001:DB8:1:2::2/64		—
	Link-local	FE80::1		—
R2	S0/0/0	10.10.1.5	255.255.255.252	—
		2001:DB8:1:2::1/64		—
	S0/0/1	10.10.1.9	255.255.255.252	—

		2001:DB8:1:3::1/64		—
	Link-local	FE80::2		—
R3	G0/0	10.10.1.17	255.255.255.240	—
		2001:DB8:1:4::1/64		—
	S0/0/1	10.10.1.10	255.255.255.252	—
		2001:DB8:1:3::2/64		—
	Link-local	FE80::3		—
PC1	NIC			
PC2	NIC			

Задачи

Часть 1. Заполнение таблицы адресации

Часть 2. Проверка подключения с помощью команды ping

Часть 3. Определение пути с помощью трассировки маршрута

Общие сведения

Двойной стек позволяет сосуществовать адресам IPv4 и IPv6 одной и той же сети. В этом упражнении вы изучите внедрение двойного стека, включая документирование конфигурации IPv4 и IPv6 для оконечных устройств, проверку связи по IPv4- и IPv6-протоколам с помощью команды **ping** и трассировку пути по IPv4 и IPv6.

Часть 1. Заполнение таблицы адресации

Шаг 1. Проверьте IPv4-адресацию с помощью команды ipconfig.

А. Нажмите **PC1**, откройте вкладку **Desktop** (Рабочий стол) и выберите **Command Prompt** (Командная строка).

Б. Введите команду **ipconfig /all** для сбора данных об IPv4-адресе. Заполните **таблицу адресации**, указав IPv4-адрес, маску подсети и шлюз по умолчанию.

В. Нажмите **PC2**, откройте вкладку **Desktop** (Рабочий стол) и выберите **Command Prompt** (Командная строка).

Г. Введите команду **ipconfig /all** для сбора данных об IPv4-адресе. Заполните **таблицу адресации**, указав IPv4-адрес, маску подсети и шлюз по умолчанию.

Шаг 2. Проверьте IPv6-адресацию с помощью команды ipv6config.

А. На **PC1** введите команду **ipv6config /all** для сбора данных об IPv6-адресе. Заполните **таблицу адресации**, указав IPv6-адрес, префикс подсети и шлюз по умолчанию.

Б. На **PC2** введите команду **ipv6config /all** для сбора данных об IPv6-адресе. Заполните **таблицу адресации**, указав IPv6-адрес, префикс подсети и шлюз по умолчанию.

Часть 2. Проверка подключения с помощью команды ping

Шаг 1. Проверьте IPv4-соединение с помощью команды ping.

А. С узла **PC1** отправьте эхо-запрос на IPv4-адрес узла **PC2**. Получилось?

Б. С узла **PC2** отправьте эхо-запрос на IPv4-адрес узла **PC1**. Получилось?

Шаг 2. Проверьте IPv6-соединение с помощью команды ping.

А. С узла **PC1** отправьте эхо-запрос на IPv6-адрес узла **PC2**. Получилось?

Б. С узла **PC2** отправьте эхо-запрос на IPv6-адрес узла **PC1**. Получилось?

Часть 3. Определение пути с помощью трассировки маршрута

Шаг 1. Используйте команду tracert для трассировки IPv4-пути.

А. На **PC1** выполните трассировку маршрута до **PC2**.

PC> **tracert 10.10.1.20**

Какие адреса встретились на пути?

С какими интерфейсами связаны эти четыре адреса?

Б. На **PC2** выполните трассировку маршрута до **PC1**.

Какие адреса встретились на пути?

С какими интерфейсами связаны эти четыре адреса?

Шаг 2. Используйте команду tracert для трассировки IPv6-пути.

А. На **PC1** выполните трассировку маршрута до IPv6-адреса **PC2**.

PC> **tracert 2001:DB8:1:4::A**

Какие адреса встретились на пути?

С какими интерфейсами связаны эти четыре адреса?

Б. На **PC2** выполните трассировку маршрута до IPv6-адреса **PC1**.

Какие адреса встретились на пути?

С какими интерфейсами связаны эти четыре адреса?

Лабораторная работа №11 Выполнение команды ping и трассировка маршрута для проверки пути

Таблица адресации

Устройство	**Интерфейс**	**IPv4-адрес**	**Маска подсети**	**Шлюз по умолчанию**
		IPv6-адрес/префикс		
R1	G0/0	2001:DB8:1:1::1/64		—
	G0/1	10.10.1.97	255.255.255.224	—
	S0/0/1	10.10.1.6	255.255.255.252	—
		2001:DB8:1:2::2/64		—
	Link-local	FE80::1		—
R2	S0/0/0	10.10.1.5	255.255.255.252	—
		2001:DB8:1:2::1/64		—
	S0/0/1	10.10.1.9	255.255.255.252	—
		2001:DB8:1:3::1/64		—
	Link-local	FE80::2		—
R3	G0/0	2001:DB8:1:4::1/64		—
	G0/1	10.10.1.17	255.255.255.240	—
	S0/0/1	10.10.1.10	255.255.255.252	—
		2001:DB8:1:3::2/64		—
	Link-local	FE80::3		—
PC1	NIC			
PC2	NIC			
PC3	NIC			
PC4	NIC			

Задачи

Часть 1. Проверка и восстановление IPv4-подключения

Часть 2. Проверка и восстановление IPv6-подключения

Сценарий

Это упражнение посвящено проблемам соединения между узлами. Помимо получения и документирования сетевых параметров,

вы будете находить проблемы и принимать меры для восстановления соединения.

Примечание. Пароль пользовательского режима EXEC — **cisco**. Пароль привилегированного режима EXEC — **class**.

Часть 1. Проверка и восстановление IPv4-подключения

Шаг 1. Используйте команды ipconfig и ping-запроса для проверки подключения.

А. Щелкните **PC1**, откройте вкладку **Desktop** (Рабочий стол) и выберите **Command Prompt** (Приглашение к вводу команды).

Б. Введите команду **ipconfig /all** для сбора данных об IPv4-адресе. Заполните **таблицу адресации**, указав IPv4-адрес, маску подсети и шлюз по умолчанию.

В. Щелкните **PC3**, откройте вкладку **Desktop** (Рабочий стол) и выберите **Command Prompt** (Приглашение к вводу команды).

Г. Введите команду **ipconfig /all** для сбора данных об IPv4-адресе. Заполните **таблицу адресации**, указав IPv4-адрес, маску подсети и шлюз по умолчанию.

Д. Проверьте подключение между **PC1** и **PC3**. Команда ping не должна быть успешно выполнена.

Шаг 2. Определите причину сбоя подключения.

А. На **PC1** введите команду для отслеживания маршрута к **PC3**. Какой последний IPv4-адрес успешно ответил на запрос?

Б. Отслеживание прекратится после 30 попыток. Чтобы остановить трассировку преждевременно, нажмите **Ctrl**+**C**.

В. На **PC3** введите команду для отслеживания маршрута к **PC1**. Какой последний IPv4-адрес успешно ответил на запрос?

Г. Для того чтобы остановить отслеживание, нажмите **Ctrl** +**C**.

Д. Щелкните **R1** и откройте вкладку **CLI** (Интерфейс командной строки). Нажмите **ENTER** и войдите в систему маршрутизатора.

Е. Введите команду **show ip interface brief**, чтобы вывести список интерфейсов и их состояний. У этого маршрутизатора есть два IPv4-адреса. Один из них должен был быть записан в шаге 2A. А какой второй адрес?

Ж. Введите команду **show ip route**, чтобы вывести список сетей, к которым подключен маршрутизатор. Обратите внимание, что к интерфейсу **Serial0/0/1** подключено две сети. Что это за сети?

З. Повторите шаги с 2Д по 2Ж на маршрутизаторе **R3** и укажите ответы здесь.

Обратите внимание, что последовательный интерфейс на маршрутизаторе R3 изменился.

И. Выполните дополнительные проверки, если это позволит выявить проблему. Доступен режим моделирования.

Шаг 3. Предложите решение проблемы.

А. Сравните свои ответы на шаге 2 с имеющейся у вас документацией о сети. В чем заключается ошибка?

Б. Как можно устранить проблему?

Шаг 4. Внедрите решение.

Выполните действие, предложенное в шаге 3Б.

Шаг 5. Убедитесь, что подключение восстановлено.

А. На **PC1** проверьте подключение к **PC3**.

Б. На **PC3** проверьте подключение к **PC1**. Удалось ли устранить проблему?

Шаг 6. Задокументируйте выбранное решение.

Часть 2. Проверка и восстановление IPv6-подключения

Шаг 1. Используйте команды ipv6config и ping-запроса для проверки подключения.

А. Щелкните **PC2**, откройте вкладку **Desktop** (Рабочий стол) и выберите **Command Prompt** (Приглашение к вводу команды).

Б. Введите команду **ipv6config /all** для сбора данных об IPv6-адресе. Заполните **таблицу адресации**, указав IPv6-адрес, префикс подсети и шлюз по умолчанию.

В. Щелкните **PC4**, откройте вкладку **Desktop** (Рабочий стол) и выберите **Command Prompt** (Приглашение к вводу команды).

Г. Введите команду **ipv6config /all** для сбора данных об IPv6-адресе. Заполните **таблицу адресации**, указав IPv6-адрес, префикс подсети и шлюз по умолчанию.

Д. Проверьте подключение между **PC2** и **PC4**. Команда ping не должна быть успешно выполнена.

Шаг 2. Определите причину сбоя подключения.

А. На **PC2** введите команду для отслеживания маршрута к **PC4**. Какой последний IPv6-адрес успешно ответил на запрос?

Б. Отслеживание прекратится после 30 попыток. Чтобы остановить трассировку преждевременно, нажмите **Ctrl+C**.

В. На **PC4** введите команду для отслеживания маршрута к **PC2**. Какой последний IPv6-адрес успешно ответил на запрос?

Г. Для того чтобы остановить отслеживание, нажмите **Ctrl +C**.

Д. Щелкните **R3** и откройте вкладку **CLI** (Интерфейс командной строки). Нажмите **ENTER** и войдите в систему маршрутизатора.

Е. Введите команду **show ipv6 interface brief**, чтобы вывести список интерфейсов и их состояний. У этого маршрутизатора есть два IPv6-адреса. Один из них должен соответствовать адресу шлюза, записанному в шаге 1Г. Имеется ли несоответствие этих адресов?

Ж. Выполните дополнительные проверки, если это позволит выявить проблему. Доступен режим моделирования.

Шаг 3. Предложите решение проблемы.

А. Сравните свои ответы на шаге 2 с имеющейся у вас документацией о сети. В чем заключается ошибка?

Б. Как можно устранить проблему?

Шаг 4. Внедрите решение.

Выполните действие, предложенное в шаге 3Б.

Шаг 5. Убедитесь, что подключение восстановлено.

А. На **PC2** проверьте подключение к **PC4**.

Б. На **PC4** проверьте подключение к **PC2**. Удалось ли устранить проблему?

Шаг 6. Задокументируйте выбранное решение.

Лабораторная работа №12 Устранение проблем с адресацией IPv4 и IPv6

Таблица адресации

Устройство	**интерфейс**	**IPv4-адрес**	**Subnet Mask (Маска подсети)**	**Основной шлюз**
		IPv6-адрес/префикс		
R1	G0/0	10.10.1.1	255.255.255.0	—
	G0/1	192.168.0.1	255.255.255.0	—
		2001:DB8:1:1::1/64		—
	G0/2	2001:DB8:1:2::1/64		—
	S0/0/0	209.165.201.2	255.255.255.252	—
		2001:DB8:1:A001::2/64		—
	Link-local	FE80::1		—
Dual Stack Server	NIC	64.100.1.254	255.255.255.0	64.100.1.1
		2001:DB8:CAFE:1::10/64		FE80::A

DNS-сервер	NIC	64.100.1.254	255.255.255.0	64.100.1.1
		2001:DB8:CAFE:1::10/64		FE80::A
PC1	NIC	10.10.1.2	255.255.255.0	10.10.1.1
PC2	NIC	192.168.0.2	255.255.255.0	192.168.0.1
		2001:DB8:1:1::2/64		FE80::1
PC3	NIC	2001:DB8:1:2::2/64		FE80::1

Задачи

Часть 1. Устранение первой проблемы

Часть 2. Устранение второй проблемы

Часть 3. Устранение третьей проблемы

Сценарий

Вы - сетевой инженер в компании, которая решила сменить протокол IPv4 на протокол IPv6. Но пока необходима поддержка обоих протоколов (двойной стек). Три сотрудника обратились в справочную службу, но решить их проблемы там не удалось. Справочная служба переадресовала вопросы вам, специалисту 2-го уровня технической поддержки. Ваша задача: найти причину проблем и устранить их.

Часть 1. Устранение первой проблемы

Пользователь **PC1** жалуется, что не может открыть веб-страницу **dualstackserver.pka**.

Шаг 1. Проверьте подробный запрос службы поддержки.

Служба поддержки получила от пользователя следующую информацию по телефону. Проверьте правильность информации.

Запрос службы поддержки	
Идентификатор пользователя: PC1	
Проблема: не удается открыть веб-страницу dualstackserver.pka.	
Подробная информация о проблеме	
Проверка. Показывает ли команда **ipconfig** IP-адрес компьютера?	Да
Проверка. Может ли компьютер установить связь со шлюзом с помощью команды **ping**?	Да
Проверка. Может ли компьютер установить связь с сервером с помощью команды **tracert**?	Да
Проверка. Может ли компьютер получить информацию о сервере с помощью команды **nslookup**?	Нет
Решение. Передать проблему в поддержку 2-го уровня.	

Шаг 2. Подумайте о возможных причинах сбоя.

А. Изучите результаты проведенных проверок. Если возможно, обсудите возможные сценарии, которые могли привести к этой ситуации, с другими сетевыми инженерами (одногруппниками).

Б. Выполните дополнительные проверки, если это позволит выявить проблему. Доступен режим моделирования.

Шаг 3. Предложите решение проблемы.

Составьте список того, что можно было бы изменить для решения этой проблемы. Начните с решения, которое поможет с наибольшей вероятностью.

Шаг 4. Внедрите решение.

Выберите и примените наиболее подходящее решение из списка. В случае неудачи переходите к следующему решению.

Шаг 5. Проверьте, что решение позволило устранить проблему.

А. Повторите проверки, указанные в запросе службы поддержки. Позволило ли это решить проблему?

Б. Если проблема не решена, отмените изменения, если вы не уверены, что они правильны, и вернитесь к шагу 4.

Шаг 6. Запишите выбранное решение.

Зафиксируйте решение проблемы. Эти записи пригодятся для решения аналогичной проблемы в будущем.

Часть 2. Устранение второй проблемы

Пользователь PC2 жалуется, что он не может получить доступ к файлам **DualStackServer.pka** по адресу: 2001:DB8:CAFE:1::10

Шаг 1. Проверьте подробный запрос службы поддержки.

Служба поддержки получила от пользователя следующую информацию по телефону. Проверьте правильность информации.

Шаг 2. Для устранения проблемы выполните шаги 2–5 части 1.

Шаг 3. Запишите выбранное решение.

Зафиксируйте решение проблемы. Эти записи пригодятся для решения аналогичной проблемы в будущем.

Запрос службы поддержки	
Идентификатор пользователя: PC2	
Проблема: не удается получить доступ к FTP-службе по адресу 2001:DB8:CAFE:1:10.	
Подробная информация о проблеме	
Проверка. Показывает ли команда **ipv6config** IPv6-адрес компьютера?	Да
Проверка. Может ли компьютер установить связь со шлюзом с помощью команды **ping**?	Да
Проверка. Может ли компьютер установить связь с сервером с помощью команды **tracert**?	Нет
Решение. Передать проблему в поддержку 2-го уровня.	

Часть 3. Устранение третьей проблемы

Пользователь **PC3** сообщает об отсутствии связи с **PC2**.

Шаг 1. Проверьте подробный запрос службы поддержки.

Справочная служба получила от пользователя следующую информацию по телефону. Проверьте правильность информации.

Запрос службы поддержки	
Идентификатор пользователя: PC3	
Проблема: отсутствие связи с PC2.	
Подробная информация о проблеме	
Проверка. Показывает ли команда **ipconfig** IP-адрес компьютера?	Да
Проверка. Показывает ли команда **ipv6config** IPv6-адрес компьютера?	Да
Проверка. Может ли компьютер установить связь с IPv4-шлюзом при выполнении команды **ping**?	Нет
Проверка. Может ли компьютер установить связь с IPv6-шлюзом при выполнении команды **ping**?	Да
Проверка. Поступает ли запрос с компьютера на клиентский узел IPv4 при отправке команды **tracert**?	Нет
Проверка. Поступает ли запрос с компьютера на клиентский узел IPv6 при отправке команды **tracert**?	Да
Решение. Передать проблему в поддержку 2-го уровня.	

Шаг 2. Для устранения проблемы выполните шаги 2–5 части 1.

Шаг 3. Запишите выбранное решение.

Зафиксируйте решение проблемы. Эти записи пригодятся для решения аналогичной проблемы в будущем.

Лабораторная работа №13 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 топологии. Для каждой локальной сети (LAN) в сети требуется достаточно пространства для, 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.

Часть 1. Разработка схемы IP-адресации

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

А. Сколько потребуется подсетей в соответствии с имеющейся топологией?

Б. Сколько битов необходимо заимствовать для поддержки нескольких подсетей в таблице топологии?

В. Сколько в результате этого создается подсетей?

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

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

Д. Рассчитайте двоичное значение для первых пяти подсетей. Первая подсеть уже показана.

Сеть 0: 192 . 168 . 100 . 0 0 0 0 0 0 0 0

Сеть 1: 192 . 168 . 100 . ___ ___ ___ ___ ___ ___ ___ ___

Сеть 2: 192 . 168 . 100 . ___ ___ ___ ___ ___ ___ ___ ___

Сеть 3: 192 . 168 . 100 . ___ ___ ___ ___ ___ ___ ___ ___

Сеть 4: 192 . 168 . 100 . ___ ___ ___ ___ ___ ___ ___ ___

Е. Рассчитайте двоичное и десятичное значение новой маски подсети.

11111111.11111111.11111111. ___ ___ ___ ___ ___ ___ ___ ___

255 . 255 . 255 . _____

Ж. 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.

А. Назначьте подсеть 0 локальной сети (LAN), подключенной к гигабитному интерфейсу Ethernet 0/0 маршрутизатора R1.

Б. Назначьте подсеть 1 локальной сети (LAN), подключенной к гигабитному интерфейсу Ethernet 0/1 маршрутизатора R1.

В. Назначьте подсеть 2 локальной сети (LAN), подключенной к гигабитному интерфейсу Ethernet 0/0 маршрутизатора R2.

Г. Назначьте подсеть 3 локальной сети (LAN), подключенной к гигабитному интерфейсу Ethernet 0/1 маршрутизатора R2.

Д. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

Шаг 3. Задокументируйте схему адресации.

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

А. Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала глобальной сети (WAN).

Б. Назначьте первые используемые IP-адреса маршрутизатору R2 для каналов локальной сети (LAN). Последний из используемых IP-адресов назначьте каналу WAN.

с. Второй из используемых IP-адресов назначьте коммутаторам.

d. Последний из используемых IP-адресов назначьте узлам.

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

Основная часть параметров IP-адресации для данной сети уже настроена. Для завершения настройки адресации выполните следующие шаги.

Шаг 1. Настройте IP-адресацию на интерфейсах LAN маршрутизатора R1.

Шаг 2. Настройте IP-адресацию на коммутаторе S3, включая шлюз по умолчанию.

Шаг 3. Настройте IP-адресацию на PC4, в том числе 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**.

Лабораторная работа №14 Изучение работы сети

Задачи

Часть 1. Анализ межсетевого трафика в филиале

Часть 2. Анализ межсетевого трафика к центральному офису

Часть 3. Анализ межсетевого трафика из филиала

Общие сведения

Цель этого упражнения по моделированию — помочь вам понять процессы движения трафика и изучить содержимое пакетов данных, передаваемых в сложной сети. Сообщения будут изучены в трех различных местоположениях, смоделированных по аналогии с обычными коммерческими и домашними сетями.

Изучите представленную топологию. Сеть Central (центральный офис) имеет три маршрутизатора и несколько сетей, которые могут представлять различные здания в пределах комплекса зданий. Сеть Branch (филиал) имеет только один маршрутизатор с доступом к Интернету и выделенным подключением к глобальной сети (WAN) для связи с центральным офисом. Сеть Home Office (домашний офис) имеет широкополосное подключение через кабельный модем для доступа к Интернету и корпоративной сети через Интернет.

Для устройств в каждой из сетей используются статические и динамические адреса. На устройствах настроены шлюзы по умолчанию и DNS-серверы там, где это нужно.

Часть 1. Анализ межсетевого трафика в филиале

В части 1 данного упражнения вы будете в режиме моделирования генерировать веб-трафик и изучать протокол HTTP вместе с другими протоколами, необходимыми для обмена данными.

Шаг 1. Переключитесь из режима реального времени (Realtime) в режим моделирования (Simulation).

А. Щелкните значок режима **Simulation** (Моделирование), чтобы переключиться из режима **Realtime** (Режим реального времени) в режим **Simulation** (Моделирование).

Б. Убедитесь, что в списке **Event List Filters** (Фильтр списка событий) выбраны **ARP, DNS, HTTP** и **TCP**.

В. Переместите ползунок под кнопками **Play Controls** (Кнопки управления) (**Back**, **Auto Capture/Play**, **Capture/Forward**) вправо.

Шаг 2. Сгенерируйте трафик с помощью веб-браузера.

На данный момент панель моделирования пуста. В списке событий в верхней части панели моделирования есть шесть столбцов, расположенных вдоль заголовка. По мере генерации и движения трафика в списке будут появляться события. Столбец **Info** (Информация) содержит информацию о конкретном событии.

Примечание. На панели слева от панели моделирования отображается топология сети. При необходимости используйте полосы прокрутки для просмотра данных филиала. Размер панелей можно изменить, если навести указатель на полосу прокрутки и перетащить его влево и вправо.

А. Щелкните **Sales PC** (ПК отдела продаж) на крайней левой панели.

Б. Откройте вкладку **Desktop** (Рабочий стол) и щелкните значок **Web Browser** (Веб-браузер), чтобы открыть веб-браузер.

В. В поле URL введите адрес **http://branchserver.pt.pta** и нажмите кнопку**Go** (Перейти). Посмотрите на список событий на панели моделирования. Какой тип события отображен в списке первым?

Г. Щелкните поле **DNS**. В разделе **Out Layers** (Исходящие уровни) DNS показан на уровне 7. На уровне 4 используется протокол UDP для связи с DNS-сервером через порт назначения 53 (**Dst Port:**). Показаны IP-адреса источника и места назначения. Какие данные для связи с DNS-сервером отсутствуют?

Д. Нажмите кнопку **Auto Capture/Play** (Автоматический захват/воспроизведение). Примерно через 30–40 секунд откроется окно, показывающее текущее состояние моделирования. (Может открыться окно с сообщением о переполнении буфера). Нажмите кнопку **View Previous Events** (Просмотр предыдущих событий). Вернитесь в начало списка и обратите внимание на количество событий протокола **ARP**. Посмотрите на столбец Device (Устройство) в списке событий и скажите, сколько устройств в сети филиала Branch получили **ARP**-запросы.

Е. Перейдите в нижнюю часть списка событий к событиям **DNS**. Выберите событие **DNS**, у которого свойство At Device (На устройстве) имеет значение **BranchServer**. Щелкните квадрат в столбце **Info**(Информация). Что можно определить, выбрав 7-й уровень в **модели OSI**? (Посмотрите на результат, отобразившийся сразу под **In Layers**(Входящие уровни))

Ж. Щелкните вкладку **Outbound PDU Details** (Сведения об исходящей PDU). Прокрутите страницу вниз и найдите раздел DNS Answer (DNS-ответ). Какой показан адрес?

З. Следующие несколько событий — это события **TCP**, позволяющие установить канал связи. Выберите последнее событие **TCP** на устройстве **Sales** (Отдел продаж) прямо перед событием **HTTP**. Щелкните цветной квадрат Info, чтобы отобразить сведения о PDU. Выделите уровень 4 в столбце **In Layers** (Входящие уровни). Посмотрите на 6-й элемент списка сразу под столбцом **In Layers**(Входящие уровни) и назовите состояние подключения.

И. Следующие несколько событий — это события **HTTP**. Выберите любое событие **HTTP** на промежуточном устройстве (IP Phone (IP-телефон) или Switch (Коммутатор)). Сколько активных уровней на одном из этих устройств и почему?

К. Выберите последнее событие **HTTP** на узле Sales PC. Выберите самый верхний уровень на вкладке **OSI Model** (Модель OSI). Какой результат показан под столбцом **In Layers** (Входящие уровни)?

Часть 2. Анализ межсетевого трафика к центральному офису

В части 2 этого упражнения вы будете в режиме моделирования Packet Tracer просматривать и изучать, как обрабатывается трафик, покидающий локальную сеть.

Шаг 1. Подготовьтесь к захвату трафика, идущего к веб-серверу сети Central (Центрального офиса).

А. Закройте все окна со сведениями о PDU.

Б. Нажмите кнопку **Reset Simulation** (Сброс моделирования), которая находится примерно в центре панели моделирования.

В. Введите адрес **http://centralserver.pt.pta** в веб-браузере узла Sales PC.

Г. Нажмите кнопку **Auto Capture/Play** (Автоматический захват/воспроизведение). Примерно через 75 секунд откроется окно, показывающее текущее состояние моделирования. Нажмите кнопку**View Previous Events** (Просмотр предыдущих событий). Перейдите в начало списка. Обратите внимание, что первыми событиями являются**DNS**, а записей **ARP** нет до установки связи с сервером филиала**BranchServer**. Почему это происходит? Дайте ответ на основании полученных знаний.

Д. Щелкните последнее событие DNS в столбце **Info** (Информация). Выделите **Layer 7** (Уровень 7) на вкладке **OSI Model** (Модель OSI).

На основе представленной информации скажите, что можно определить по результатам DNS?

Е. Щелкните вкладку **Inbound PDU Details** (Сведения о входящей PDU). Прокрутите страницу вниз до раздела **DNS ANSWER** (DNS-ответ). Какой адрес показан для centralserver.pt.pta?

Ж. Следующие несколько событий — это события **ARP**. Щелкните цветной квадрат Info последнего события **ARP**. Откройте вкладку **Inbound PDU Details** (Сведения о входящей PDU) и обратите внимание на MAC-адрес. На основе сведений из раздела ARP скажите, какое устройство предоставляет ответ ARP?

З. Следующие несколько событий являются событиями **TCP**, которые опять подготавливают установку канала связи. Найдите первое событие**HTTP** в списке событий. Щелкните цветной квадрат события **HTTP**. Выделите Уровень 2 на вкладке **OSI Model** (Модель OSI). Что можно определить по MAC-адресу назначения?

И. Щелкните событие **HTTP** на устройстве **R4**. Обратите внимание, что уровень 2 содержит заголовок Ethernet II. Щелкните

событие **HTTP** на устройстве **Intranet**. Что показано на уровне 2 этого устройства?

Обратите внимание, что активны только два уровня, а не три, как на маршрутизаторе. Это подключение к сети WAN, которое будет описано далее в курсе.

Часть 3. Анализ межсетевого трафика из филиала

В 3-й части этого упражнения вы удалите все события и сделаете новый веб-запрос, для которого понадобится Интернет.

Шаг 1. Подготовьтесь к захвату трафика, идущего к веб-серверу в Интернете.

А. Закройте все окна со сведениями о PDU.

Б. Нажмите кнопку **Reset Simulation** (Сброс моделирования), которая находится примерно в центре панели моделирования. Введите адрес**http://www.netacad.pta** в веб-браузере узла Sales PC.

В. Нажмите кнопку **Auto Capture/Play** (Автоматический захват/воспроизведение). Примерно через 75 секунд откроется окно, показывающее текущее состояние моделирования. Нажмите кнопку**View Previous Events** (Просмотр предыдущих событий). Вернитесь в начало списка и обратите внимание, что первыми событиями являются события **DNS**. Что можно сказать о количестве событий **DNS**?

Г. Взгляните на некоторые из устройств, через которые проходят события**DNS** на пути к DNS-серверу. Где находятся эти устройства?

Д. Щелкните последнее событие **DNS**. Откройте вкладку **Inbound PDU Details** (Сведения о входящей PDU) и перейдите вниз к последнему разделу DNS Answer (DNS-ответ). Какой IP-адрес показан для**www.netacad.pta**?

Е. Во время передачи события **HTTP** по сети маршрутизаторами на вкладке **OSI Model** (Модель OSI) активны три уровня в столбцах **In Layers** (Входящие уровни) и **Out Layers** (Исходящие уровни). На основе этой информации скажите, через сколько маршрутизаторов происходит передача?

Ж. Щелкните событие **TCP** перед последним событием **HTTP**. На основе показанной информации скажите, какова цель данного события?

З. В списке есть еще несколько событий **TCP**. Найдите событие **TCP**, где свойство *Last Device* (Последнее устройство) имеет значение **IP Phone**(IP-телефон), а свойство *Device At* (На устройство)

— значение **Sales**(Отдел продаж). Щелкните цветной квадрат Info и выберите **Layer 4**(Уровень 4) на вкладке **OSI Model** (Модель OSI). На основе выходных данных скажите, каково состояние установленного подключения?

Лабораторная работа №15 Настройка безопасного пароля и протокола SSH

Таблица адресации

Устройство	интерфейс	IP-адрес	Subnet Mask (Маска подсети)	Основной шлюз
RTA	G0/0	172.16.31.1	255.255.255.0	—
PCA	NIC	172.16.31.2	255.255.255.0	172.16.31.1

Сценарий

Сетевой администратор попросил подготовить маршрутизатор **RTA** для развертывания. Перед его подключением к сети необходимо активировать функции безопасности.

Требования

- Настройте IP-адресацию на компьютере **PCA** в соответствии с таблицей адресации.
- С помощью консоли подключитесь к маршрутизатору **RTA** из терминала на PC-A.
- Настройте IP-адресацию на **RTA** и активируйте интерфейс.
- Укажите имя узла **RTA**.
- Зашифруйте все открытые пароли.
- RTA(config)# **service password-encryption**
- Установите надежный пароль (пароль придумайте сами).
- Установите доменное имя **RTA.com** (Указывайте имя с учетом регистра для правильного расчета баллов программой Packet Tracer).
- RTA(config)# **ip domain-name RTA.com**
- Создайте произвольного пользователя с надежным паролем.
- RTA(config)# **username** ***any_user*** **password** ***any_password***
- Создайте ключи RSA длиной 1024 бита.

Примечание. В программе Packet Tracer введите команду **crypto key generate rsa** и нажмите клавишу Enter для продолжения.

RTA(config)# **crypto key generate rsa**

- Заблокируйте на три минуты всех, кто не смог войти в систему, выполнив четыре попытки в течение двух минут.

RTA(config)# **login block-for 180 attempts 4 within 120**

- Настройте линии VTY для доступа по SSH и используйте профили локальных пользователей для аутентификации.

RTA(config)# **line vty 0 4**
RTA(config-line)# **transport input ssh**
RTA(config-line)# **login local**

- Сохраните конфигурацию в NVRAM.