ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Методические указания для проведения практических занятий
по дисциплине

Системное администрирование инфокоммуникационных систем

(направление подготовки 11.03.02
Инфокоммуникационные технологии и системы связи)

Ростов-на-Дону
2019

Методические указания для проведения практических занятий
по дисциплине

Системное администрирование инфокоммуникационных систем

(направление подготовки 11.03.02
Инфокоммуникационные технологии и системы связи)

Составил: И.А. Сосновский, доцент кафедры ИТСС

Рассмотрено и одобрено
на заседании кафедры
Протокол от «26» августа 2019 г. № 1

Практическое занятие №1. Введение в межсетевую операционную систему IOS компании Cisco Знакомство со средой моделирования.

1. Порядок выполнения и сдачи работы.

1.1. Изучить теоретическую и практическую часть.

1.2. Сдать преподавателю теорию работы путём ответа на контрольные вопросы.

1.3. Выполнить в PacketTracer практическую часть.

1.4. Получите вариант и выполните в PacketTracer задание для самостоятельной работы

1.5. Предъявите преподавателю результат выполнения задания для самостоятельной работы. Продемонстрируйте свои файлы с конфигурациями роутеров. Продемонстрируйте ему, что компьютеры пингуются согласно таблице 4.

1.6. Продемонстрируйте работу telnet.

1.7. Оформите отчёт. Содержание отчёта смотри ниже.

1.8. Защитите отчёт.

2 Теоретическая часть.

При первом входе в сетевое устройство пользователь видит командную строку пользовательского режима вида:

Switch>

Команды, доступные на пользовательском уровне являются подмножеством команд, доступных в привилегированном режиме. Эти команды позволяют выводить на экран информацию без смены установок сетевого устройства.

Чтобы получить доступ к полному набору команд, необходимо сначала активизировать привилегированный режим.

Press ENTER to start.

Switch>

Switch> enable

Switch#

Switch# disable

Switch>

Здесь и далее вывод сетевого устройства будет даваться обычным шрифтом, а ввод пользователя жирным шрифтом.

О переходе в этот режим будет свидетельствовать появление в командной строке приглашения в виде знака #. Из привилегированного уровня можно получать информацию о настройках системы и получить доступ к режиму глобального конфигурирования и других специальных режимов конфигурирования, включая режимы конфигурирования интерфейса, подъинтерфейса, линии, сетевого устройства, карты маршрутов и т.п. Для выхода из системы IOS необходимо набрать на клавиатуре команду exit (выход).

Switch> exit

Независимо от того, как обращаются к сетевому устройству: через консоль терминальной программы, подсоединённой через ноль-модем к COM-порту сетевого устройства, либо в рамках сеанса протокола Telnet, устройство можно перевести в один из режимов. Нас интересуют следующие режимы.

Пользовательский режим — это режим просмотра, в котором пользователь может только просматривать определённую информацию о сетевом устройстве, но не может ничего менять. В этом режиме приглашение имеет вид типа Switch>.

Привилегированный режим— поддерживает команды настройки и тестирования, детальную проверку сетевого устройства, манипуляцию с конфигурационными файлами и доступ в режим конфигурирования. В этом режиме приглашение имеет вид типа Switch#.

Режим глобального конфигурирования — реализует мощные однострочные команды, которые решают задачи конфигурирования. В этом режиме приглашение имеет вид типа Switch (config) # .

Команды в любом режиме IOS распознаёт по первым уникальным символам. При нажатии табуляции IOS сам дополнит команду до полного имени.

При вводе в командной строке любого режима имени команды и знака вопроса (?) на экран выводятся комментарии к команде. При вводе одного знака результатом будет список всех команд режима. На экран может выводиться много экранов строк, поэтому иногда внизу экрана будет появляться подсказка - More -. Для продолжения следует нажать enter или пробел [1-3].

Команды режима глобального конфигурирования определяют поведение системы в целом. Кроме этого, команды режима глобального конфигурирования включают команды переходу в другие режимы конфигурирования, которые используются для создания конфигураций, требующих многострочных команд. Для входа в режим глобального конфигурирования используется команда привилегированного режима configure. При вводе этой команды следует указать источник команд конфигурирования: terminal (терминал), memory (энергонезависимая память или файл), network (сервер tftp (Trivial ftp -упрощённый ftp) в сети). По умолчанию команды вводятся с терминала консоли. Например [1-3]

Switch# configure terminal

Switch(config)#(commands)

Switch(config)# exit

Switch#

Команды для активизации частного вида конфигурации должны предваряться командами глобального конфигурирования. Так для конфигурации интерфейса, на возможность которой указывает приглашение Switch(config-if)#, сначала вводится глобальная команда для определения типа интерфейса и номера его порта:

Switch# conf t

Switch(config)# interface *type port*

Switch(config-if)# *(commands)*

Switch(config-if)# exit

Switch(config)# exit

Для ограничения доступа к системе используются пароли. Команда line console устанавливает пароль на вход на терминал консоли:

Switch (config)# line console 0

Switch (config-line)# login

Switch (config-line)# password Cisco

Команда line vty 0 4 устанавливает парольную защиту на вход по протоколу Telnet [1-3]:

Switch (config)# line vty 0 4

Switch (config-line)# login

Switch (config-line)# password cisco

Команда enable password ограничивает доступ к привилегированному режиму:

Switch#conf t

Switch(config)# enable password пароль

Далее

Ctrl-Z

Switch#ex

…

Press RETURN to get started

Switch>en

Password: пароль

Switch#

Здесь пароль пароль – последовательность латинских символов.

Для установки на сетевом интерфейсе IP адреса используется команда:

Router(config-if)#ip address [ip-address] [subnet-mask],

Router(config-if)#no shut

Команда no shut (сокращение no shutdown) используется для того, чтобы бы интерфейс был активным (без этой команды возможно произвольное временное отключение интерфейса). Обратная команда – shut, выключит интерфейс.

Важно иметь возможность контроля правильности функционирования и состояния сетевого устройства в любой момент времени. Для этого служат команды [1-3]:

Команда	Описание
show version	Выводит на экран данные о конфигурации аппаратной части системы, версии программного обеспечения, именах и источниках конфигурационных файлов и загруженных образах
show running-conf ig	Показывает содержание активной конфигурации
show interfaces	Показывает данные обо всех интерфейсах на устройстве
show protocols	Выводит данные о протоколах третьего сетевого уровня.

2.1 Cisco Discovery Protocol (CDP)

CDP позволяет устройствам обмениваться основной конфигурационной информацией. CDP будет работать без настройки какого ни будь протокола. По умолчанию, CDP включен на всех интерфейсах. CDP работает на втором (канальном) уровне модели OSI. Поэтому CDP не является маршрутизируемым протоколом и работает только с непосредственно подключенными устройствами. Протокол CDP связывает физическую среду передачи данных более низкого уровня с протоколами более высокого сетевого уровня. Поэтому устройства, поддерживающие разные протоколы третьего уровня, могут узнавать друг друга.

При запуске устройства протокол CDP запускается автоматически. Поле этого он может автоматически определить соседние устройства, на которых

также выполняется протокол CDP. Среди найденных устройств будут не только те, которые работают с протоколом IP.

CDP позволяет администраторам иметь доступ к данным о другом сетевом устройстве, к которому есть непосредственное соединение.

Для вывода информации о соседних устройствах, обнаруженных по протоколу CDP, используется семейство команд show cdp. Оно выводит следующие данные по каждому порту и каждому подсоединённому к нему устройству: Идентификаторы устройства, список адресов, идентификатор порта, перечень функциональных возможностей, аппаратная платформа устройства [1-3].

2.2 Команды ping и traceroute

Для диагностики возможности установления связи в сетях используются протоколы тип запрос-ответ или протокол эхо-пакетов. Результаты роботы такого протокола могут помочь в оценке надёжности пути к другому устройству, величин задержек в целом и между промежуточными устройствами. Для того чтобы такая команда работала, необходимо, чтобы не только локальное сетевое устройство знало, как попасть в пункт назначения, но и чтобы устройство в пункте назначения знало, как добраться до источника.

Команда ping посылает ICMP(Internet Control Message Protocol) эхо-пакеты для верификации соединения. В приведённом ниже примере время прохождения одного эхо-пакета превысило заданное, о чём свидетельствует точка (.) в выведенной информации, а четыре пакета прошли успешно, о чём говорит восклицательный знак (!)[1-3].

Switch> ping 172.16.101.1

Type escape sequence to abort.

Sending 5 100-byte ICMP echoes to 172.16.10.1 timeout is 2 seconds:

.!!!!

Success rate is 80 percent, round-trip min/avg/max = 6/6/6 ms

Символ	Значение
!	Успешный приём эхо-ответа
.	Превышено время ожидания
U	Пункт назначения недосягаем
C	Перегрузка сети
I	Выполнение команды прервано администратором
?	Неизвестный тип пакета
&	Пакет превысил значение параметра времени жизни TTL пакета

Команды traceroute показывает адреса промежуточных интерфейсов (хопов) на пути пакетов в пункт назначения [1-3].

Switch> traceroute 172.16.101.1

Расширенная версия команды ping поддерживается только в привилегированном режиме. Для того, чтобы войти в расширенный режим, необходимо в строке подсказки Extended commands ввести букву "y"(Yes)

Команда в режиме диалога опрашивает значения параметров. Важно отметить, что эта команда позволяет, находясь на одном устройстве, проверять связь между сетевыми интерфейсами на других устройствах.

Router# ping

Protocol [ip]:

Target IP address: 2.2.2.2

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Source address:1.1.1.1

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data [no]:

Data pattern [OxABCD]:

Loose, Strict, Record, Timestamp, Verbose [none]:

Sweep range of sizes [n]:

2.3 Команда telnet

Протокол виртуального терминала telnet, входящий в состав протоколов TCP/IP, позволяет установить соединение между сетевым устройством telnet клиента и сетевым устройством telnet сервера, что обеспечивает возможность работы в режиме виртуального терминала. Telnet используется для удалённого управления сетевым устройством либо для проверки связи на уровне приложений. Успешное установление Telnet-соединения позволяет вам управлять удалённым устройством так, как будто вы находитесь за его консолью. Сетевые устройства Cisco способны поддерживать одновременно до пяти входных сеансов протокола Telnet [1-3].

3 Практическая часть.

3.1 Соединение с сетевым устройством Cisco

Создайте в Packet Tracer топологию, изображённую на рисунке с использованием модели маршрутизатора по умолчанию - Generic. Назовите устройства так, как вы видите на рисунке 1: Router1, Router2 и Router4.

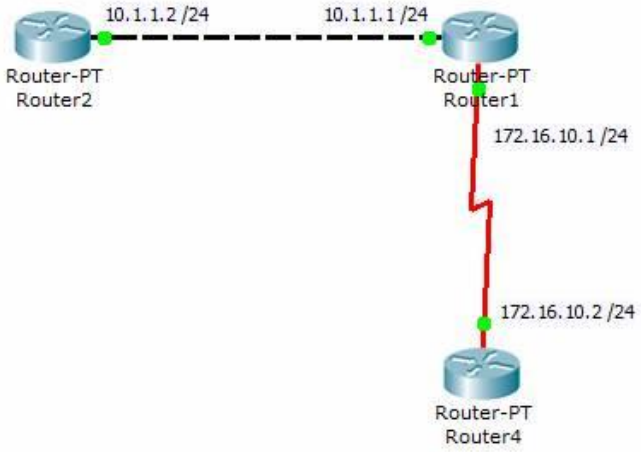


Рис.1

Черная линия означает Ethernet соединение. Красная означает последовательное соединение. Для создании последовательного соединения выбираем последовательное соединение точка-точка (serial cable). Выбираем второе устройство. Определяемся, какой маршрутизатор будет выполнять

функции DCE устройства. Это устройство задаёт синхронизацию. В симуляторе для него будет необходимо определить частоту синхронизации [3].

Сохраните топологию.

3.2 Ознакомление с сетевым устройством Cisco.

1. Для выбора сетевого устройства Router1 нажмите в рабочей области программы на изображение нужного. Откроется окно настроек сетевого устройства. Здесь выберем вкладку CLI для управления устройством.

2. В середине экрана Сетевого устройства Router1 вы увидите

Continue with configuration dialog? [yes/no]:

Введите: “no” и нажмите клавишу <Enter>.

Вы увидите

Router>

Теперь вы подключены к сетевому устройству и находитесь в командной строке режима пользователя. Здесь "Router" – это имя Сетевого устройства, а ">" означает, что вы находитесь в режиме пользователя.

3. Тепер введите команду enable, чтобы попасть в привилегированный режим.

Router>enable

Router#

4. Чтобы вернуться в режим пользователя, просто напечатайте disable. Из режима пользователя введіте logout или exit, чтобы покинуть сетевое устройство.

Router#disable

Router>

Router>exit

Router con0 is now available

Press RETURN to get started

3.3 Основные команды сетевого устройства

1. Войдите сетевое устройство Router1

Router>

2. Мы хотим увидеть список всех доступных команд в этом режиме. Введите команду, которая используется для просмотра всех доступных команд:

Router>?

Клавишу Enter нажимать не надо.

3. Теперь войдите в привилегированный режим

Router>enable

Router#

4. Просмотрите список доступных команд в привилегированном режиме

Router#?

5. Перейдём в режим конфигурации

Router#config terminal

Router(config)#

6. *Имя хоста* сетевого устройства используется для локальной идентификации. Когда вы входите в сетевое устройство, вы видите *Имя хоста* перед символом режима (">" или "#"). Это имя может быть использовано для определения места нахождения. Установите "Router1" как имя вашег сетевого устройства.

Router(config)#hostname Router1

Router1(config)#

7. Пароль доступа позволяет вам контролировать доступ в привилегированный режим. Это очень важный пароль, потому что в привилегированном режиме можно вносить конфигурационные изменения. Установите пароль доступу "parol".

Router1(config)#enable password parol

8. Давайте испытаем этот пароль. Выйдите из сетевого устройства и попытайтесь зайти в привилегированный режим.

Router1>en

Password:*****

Router1#

Здесь знаки: ***** - это ваш ввод пароля. Эти знаки на экране не видны.

3.4 Основные Show команды.

Перейдите в пользовательский режим командой disable. Введите команду для просмотра всех доступных show команд.

Router1>show ?

1. Команда show version используется для получения типа платформы сетевого устройства, версии операционной системы, имени файла образа операционной системы, время работы системы, объём памяти, количество интерфейсов и конфигурационный регистр.

2. Можно увидеть часы

Router1>show clock

3. Во флеш-памяти сетевого устройства сохраняется файл-образ операционной системы Cisco IOS. В отличие от оперативной памяти, в реальных устройствах флеш память сохраняет файл-образ даже при сбое питания.

Router1>show flash

4. ИКС сетевого устройства по умолчанию сохраняет 10 последних введенных команд

Router1>show history

5. Две команды позволят вам вернуться к командам, введённым ранее. Нажмите на стрелку вверх или <ctrl> P.

6. Две команды позволят вам перейти к следующей команде, сохранённой в буфере. Нажмите на стрелку вниз или <ctrl> N

7. Можно увидеть список хостов и IP-Адреса всех их интерфейсов

Router1>show hosts

8. Следующая команда выведет детальную информацию о каждом интерфейсе

Route1r>show interfaces

9. Команда

Router1>show sessions

выведет информацию о каждой telnet сессии.

10. Команда

Router1>show terminal

показывает конфигурационные параметры терминала.

11. Можно увидеть список всех пользователей, подсоединённых к устройству по терминальным линиям

Router1>show users

12. Команда

Router1>show controllers

показывает состояние контроллеров интерфейсов.

13. Перейдём в привилегированный режим.

Router1>en

14. Введите команду для просмотра всех доступных show команд.

Router1#show ?

Привилегированный режим включает в себя все show команды пользовательского режима и ряд новых.

15. Посмотрим активную конфигурацию в памяти сетевого устройства. Необходим привилегированный режим. Активная конфигурация автоматически не сохраняется и будет потеряна в случае сбоя электропитания.

Router1#show running-config

В строке more, нажмите на клавишу пробел для просмотра следующей страницы информации.

16. Следующая команда позволит вам увидеть текущее состояние протоколов третьего уровня.

Router#show protocols

3.5 Введение в конфигурацию интерфейсов.

Постараемся понять, как включать (поднимать) интерфейсы сетевого устройства и что надо, чтобы перевести интерфейс в состояние UP.

1. На сетевом устройстве Router1 войдём в режим конфигурации

Router1#conf t

Router1(config)#

2. Теперь ми хотим настроить Ethernet интерфейс. Для этого мы должны зайти в режим конфигурации интерфейса.

Router1(config)#interface FastEthernet0/0

Router1(config-if)#

3. Посмотрим все доступные в этом режиме команды

Router1(config-if)#?

Для выхода в режим глобальной конфигурации наберите exit. Снова войдите в режим конфигурации интерфейса

Router1(config)#int fa0/0

Мы использовали сокращенное имя интерфейса.

4. Для каждой команды мы можем выполнить противоположную команду, поставивши перед ней слово no. Так команда

Router1(config-if)#no shutdown

включает этот интерфейс.

5. Добавим к интерфейсу описание

Router1(config-if)#description Ethernet interface on Router 1

Чтобы увидеть описание этого интерфейса, перейдите в привилегированный режим и выполните команду show interface .

Router1(config-if)#end

Router1#show interface

6. Теперь присоединитесь к сетевому устройству Router 2 и поменяйте имя его хоста на Router2

Router#conf t

Router(config)#hostname Router2

Войдём на интерфейс FastEthernet 0.

Router2(config)#interface fa0/0

Включите интерфейс.

Router2(config-if)#no shutdown

Теперь, когда интерфейсы на двух концах нашего Ethernet соединения включены на экране появится сообщение о смене состояния интерфейса на активное.

7. Перейдём к конфигурации последовательных интерфейсов. Зайдём на Router1. Проверим, каким устройством выступает наш маршрутизатор для последовательной линии связи: оконечным устройством DTE (data terminal equipment) либо устройством связи DCE (data circuit)

Router1#show controllers S2/0

Если видим - ..... DCE cable.....- ,то наш маршрутизатор является устройством связи и он должен задавать частоту синхронизации тактовых импульсов, используемых при передаче данных. Частота берётся из определённого ряда частот.

Router1#conf t

Router1(config)#int s2/0

Router1(config-if)#clock rate ?

Выберем частоту 64000

Router1(config-if)#clock rate 64000

и подымаем интерфейс

Router1(config-if)#no shut

8. Переходим к маршрутизатору router4 и дадим одноимённое имя. Подымаем на нём интерфейс serial2/0.

Теперь, когда интерфейсы на двух концах нашего последовательного соединения включены на экране появится сообщение о смене состояния интерфейса на активное.

9. Проверим на каждом устройстве, что сконфигурированные нами интерфейсы находятся в состоянии UP.

Router1#sh int s2/0

Router1#sh int e0/0

Router2#sh int e0/0

Router4#sh int s2/0

3.6 CDP

1. На маршрутизаторе router1, введём команду для вывода состояния всех интерфейсов, на которых работает CDP.

router1#show cdp interface

Мы должны увидеть, что оба интерфейса подняты и посылают CDP пакеты.

```
FastEthernet0/0 is up, line protocol is up
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial2/0 is up, line protocol is up
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

2. Убедившись, что сетевое устройство посылает и принимает CDP-обновления, мы можем использовать CDP для получения информации о непосредственно подключенных устройствах. Введите команду

router1#show cdp neighbors

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Router4      Ser 2/0          138            R       PT1000      Ser 2/0
Router2      Fas 0/0          142            R       PT1000      Fas 0/0
```

Мы сделали всё правильно. Видим, что наш маршрутизатор router1 соединён с интерфейсом Fas 0/0 (Port ID) маршрутизатора (Capability) router2 (Device ID) серии 1000 (Platform) через интерфейс Fas 0/0 (Local Intrfce) и с интерфейсом Ser 2/0 маршрутизатора router4 серии 1000 через интерфейс Ser 2/0.

3. На router1, введите команду для более детальной информации о соседях router1#show cdp neighbors detail

Эта команда показывает по одному устройству за раз. Она используется для отображения адресной информации сетевого уровня. На данный момент этот уровень у нас не настроен поэтому поле Entry address(es) пустое. Команда также выводит информацию о версии IOS.

4. На router1, введите команду, чтобы узнать информацию об устройстве " router4"

router1#show cdp entry Router4

Эта команда даёт ту же информацию, как и show cdp neighbor detail, но для одного конкретного устройства. Помните, что имена хостов чувствительны к регистру.

5. На устройстве router1 введите команду, чтобы увидеть, как часто router1 посылает соседям обновления CDP и как долго у соседей они должны храниться.

router1#show cdp

```
Global CDP information:
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is enabled
```

Для экономии полосы пропускания низкоскоростных устройств CDP можно отключить

router1 (config)#no cdp run

и снова включить для всего устройства

router1 (config)#cdp run

6. Иногда необходимо отключить CDP для определённого интерфейса, например при его узкой полосе пропускания или в целях безопасности. На устройстве router1, отключите CDP на интерфейсе FastEthernet 0/0.

router1 (config)#interface fa0/0

router1 (config-if)#no cdp enable

router1 (config)#Ctrl-Z

router1#show cdp interface

В полученном выводе вы не увидите сведений об FastEthernet 0/0.

3.7 Настройка IP адресов интерфейсов

1. Подключимся к устройству Router1 и установим IP адрес Ethernet интерфейса

Router1(config)#interface fa0/0

Router1(config-if)#ip address 10.1.1.1 255.255.255.0

2. Теперь назначим интерфейсу S0/0 IP адрес 172.16.10.1 255.255.255.0, не выходя из конфигурации интерфейса

Router1(config-if)#in s0

Router1(config-if)#ip ad 172.16.10.1 255.255.255.0

Отметим, что на последовательное соединение точка точка всегда выделяется целая подсеть.

3. Переключимся к устройству Router2 и назначим интерфейсу FastEthernet 0/0 IP адрес 10.1.1.2 255.255.255.0

Router2(config)#interface fa0/0

Router2(config-if)#ip address 10.1.1.2 255.255.255.0

4. Подключимся к устройству Router4 и установим IP адрес Ethernet интерфейса Serial 2/0.

Router4(config-if)#ip address 172.16.10.2 255.255.255.0

5. На каждом устройстве посмотрите вашу активную конфигурацию и убедитесь, что там появились назначенные IP адреса.

Router1#show running-config

Router2#show running-config

Router3#show running-config

6. Посмотрите детальную IP информацию о каждом интерфейсе и убедитесь, что отконфигурированные интерфейсы перешли в состояние UP

Router1#show ip interface

Router2#show ip interface

Router4#show ip interface

7. Краткую информацию можно получить командой show ip interface brief, например

Router1#show ip in bri

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	10.1.1.1	YES	manual	up	up
FastEthernet1/0	unassigned	YES	manual	up	down
Serial2/0	172.16.10.1	YES	manual	up	up

Router2#show ip in bri

```
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        10.1.1.2        YES manual up                    up

FastEthernet1/0        unassigned      YES manual up                    down

Serial2/0              unassigned      YES manual administratively down down
```

Router4#show ip in bri

```
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        unassigned      YES manual administratively down down

FastEthernet1/0        unassigned      YES manual administratively down down

Serial2/0              172.16.10.2     YES manual up                    up
```

8. Подключимся к устройству Router1. Вы должны успешно пропинговать непосредственно подсоединённый FastEthernet 0/0 интерфейс на устройстве Router2.

Router1#ping 10.1.1.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/7 ms
```

Попробуем пропинговать интерфейс Serial 2/0 на устройстве Router4

Router1#ping 172.16.10.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/7 ms
```

Успешно.

9. Вернёмся на Router2. Вы должны успешно пропинговать адрес 10.1.1.1 непосредственно подсоединённого FastEthernet 0/0 интерфейса на устройстве Router1. Вернёмся на Router4. Вы должны успешно пропінговати адрес 172.16.10.1 непосредственно подсоединённого інтерфейса Serial 2/0 на устройстве Router1. Попробуем пропинговать интерфейс FastEthernet 0/0 на устройстве Router1.

Router4#ping 10.1.1.1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Неудача. Попробуем пропинговать адрес 10.1.1.2 FastEthernet 0/0 интерфейса на устройстве Router2. Неудача.

10. Вернёмся на Router2. Попробуем пропинговать адрес 172.16.10.1 интерфейса Serial 2/0 на устройстве Router1. Неудача. Попробуем пропинговать адрес 172.16.10.2 інтерфейса Serial 2/0 на устройстве Router4. Неудача.

Неудачи нас постигли потому, что мы не настроили на маршрутизаторах маршрутизацию.

11. Зайдите на устройство Router1. Определите пути прохождения пакетов на Router2

Router1#traceroute 10.1.1.2

и Router4

Router1# traceroute 172.16.10.2

Вы должны увидеть по одному хопу.

12. Выполните команду расширенного пинга от адреса 10.1.1.2 к адресу 172.16.10.2

Router1#ping

…

Target IP address: 172.16.10.2

…

Extended commands [n]: y

Source address: 10.1.1.2

3.8 Telnet

Будьте внимательны: симулятор имеет ограниченную поддержку telnet.

1. Войдите на устройство Router1. Нам необходимо, чтобы сетевое устройство принимало telnet-сессии и было защищено паролем. Каждая так называемая линия в сетевом устройстве потенциально представляет активную telnet-сессию, которую устройство может поддерживать. Наши сетевые

устройства поддерживают до 5 линий, назначенные на виртуальные терминалы vty. Мы используем все 5 линий

Router1(config)#line vty 0 4

Router1(config-line)#

2. Теперь сообщим сетевому устройству, что нам понадобится пароль входу в систему.

Router1(config-line)#login

Router1(config-line)#password parol

3. Войдите на устройство Router2 и установим telnet-соединение с устройством Router1. Для этого мы используем IP адресу его интерфейсу FastEthernet 0/0

Router2#telnet 10.1.1.1

4. Мы увидим просьбу ввести пароль. Введите пароль parol и нажмите <enter>. Заметьте, что имя сетевого устройства поменялось на “Router1”, потому, что мы установили telnet-соединение с Router1. Команда

Router1>show user

```
* 67 vty 0                idle                00:00:00 10.1.1.2
```

покажет, что соединение осуществлено от адреса 10.1.1.2 устройства router2 .

Теперь на секунду нажмите одновременно клавиши control-shift-6, потом отпустите и сразу нажмите клавишу x. Заметьте, что имя сетевого устройства поменялось назад на “Router2”. Теперь вы опять устройстве Router2.

Router1><Control> + <Shift> + <6> потом <x>

Router2#

6. Введите команду show sessions. Это позволит вам увидеть все активные telnet- сессии. Чтобы возобновить telnet-сессию, определите номер сессии, которую вы хотите возобновить (в нашем случае есть только одна с номером 1) и введите команду resume 1.

Router2#Show sessions

```
Conn Host              Address            Byte  Idle Conn Name
*  1 10.1.1.1          10.1.1.1              0     1 10.1.1.1
```

Router2#resume 1

Router1#

7. Теперь имя хоста снова поменялось на Router1. Нажмите комбинацию control-shift-6 и клавишу x, чтобы вернуться назад на Router2.

Router1#<Control> + <Shift> + <6> потом <x>

Router2#

8. Закройте сессию

Router2#disconnect 1

```
Closing connection to 10.1.1.1 [confirm]
```

Сохраните проект в целом и конфигурацию каждого роутера в отдельности (в текстовый файл).

4 Контрольные вопросы.

4.1 Какие есть режимы ввода команд в командной строке?

4.2 Как переключаться между режимами ввода команд в командной строке?

4.3 Какую роль играет клавиша табуляции при вводе команд?

4.4 Как войти в режимы глобальной конфигурации, активизировать частный вид конфигурации и выйти из этих режимов?

4.5 Как ориентироваться в ранее введенных командах и повторять их?

4.6 Что такое CDP, для чего он служит и как им пользоваться?.

4.7 Какую информацию возвращает команда ping?

4.8 Можно ли находясь на одном устройстве попарно пропинговать все устройства в сети?

4.9 Для чего служит команда traceroute?

4.10 Для чего служит команда протокол telnet?

4.11 Как задать имя хоста?

4.12 Какую информацию можно посмотреть командами show в

пользовательском режиме?

4.13 Какую информацию можно посмотреть командами show в привилегированном режиме, но нельзя посмотреть в пользовательском режиме?

4.14 Каким устройством может выступать маршрутизатор для последовательной линии связи?

4.15 На каком устройстве при последовательном соединении можно устанавливать частоту синхронизации?

4.16 Как поднять интерфейс и определить его состояние?

4.17 Как назначить IP адрес на интерфейс и убедиться, что он назначен?

4.18 Почему могут не проходить пинги между устройсвами?

4.19 Как приостановить и возобновить telnet-сессию?

4.20 Как закрыть telnet соединение?

5 Задание для самостоятельной работы

5.1. Варианты заданий

Вариант	i11-i31	i12-i21	i22-i32
1, 9	serial	Serial	serial
2, 10	serial	Serial	ethernet
3, 11	serial	Ethernet	serial
4, 12	serial	Ethernet	ethernet
5, 13	ethernet	Serial	serial
6, 14	ethernet	Serial	ethernet
7, 15	ethernet	Ethernet	serial
8, 16	ethernet	Ethernet	ethernet

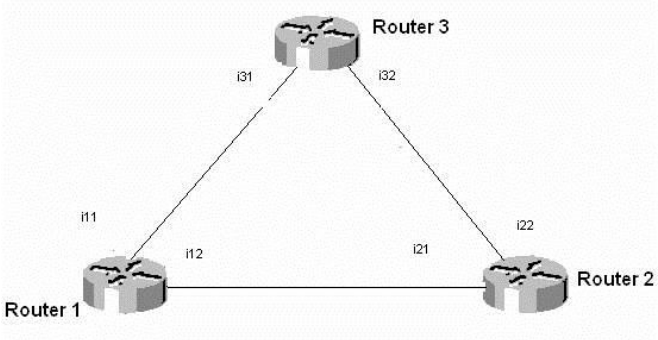
Выберите в дизайнере подходящие устройства и создайте топологию, изображённую на рисунке 2. Сами назначте устройствам имена. Поднимите на каждом устройстве используемые интерфейсы. Проверьте их состояния. На каждом устройстве, используя команды CDP show cdp neighbors, получите информацию о соседних устройствах. Сохраните скриншоты команд CDP.

5.2. Назначьте интерфейсам адреса, согласно варианту (v=1-16) из таблицы

3. Все маски равны 255.255.255.0. Например, для варианта 7 (v=7) имеем

Устройство	Интерфейс	Адрес
Router1	i11	7.1.1.2
Router3	i31	7.1.1.2
Router1	i12	7.1.2.1
Router2	i21	7.1.2.2
Router2	i22	7.1.3.1
Router3	i32	7.1.3.2

Вариант	i11, i31	i12, i21	i22, i32
1	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
2	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
3	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
4	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
5	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
6	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
7	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
8	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
9	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.2.1, v.1.2.2
10	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
11	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
12	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
13	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
14	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
15	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2
16	v.1.1.1, v.1.1.2	v.1.2.1, v.1.2.2	v.1.3.1, v.1.3.2



5.3. Проверьте, что адреса назначены. На каждом устройстве выполните команду show ip interface brief . Сохраните скриншоты.

5.4. Если сделано всё правильно вы сможете пропинговать из любого компьютера определённые (но не все) адреса интерфейсов других компьютеров.

Из\На	I11	I12	I21	I22	I31	I32
Router1	Да	Да	Да *	Нет	Да *	Нет
Router2	Нет	Да	Да	Да	Нет	Да *
Router3	Да	Нет	Нет	Да	Да	Да

Сделайте это. Сохраните скриншоты для пингов соединений, отмеченных в таблице 4 знаком *.

5.5. Выполните на Router1 расширенный пинг. Сохраните 3 скриншота для пингов: от i12 к i21, от i11 к i31 и от i22 к i32.

5.6. Настройте на Router1 Telnet. Задайте пароль.

5.7. Перейдите на Router2. Зайдите по Telnet на Router1. Выполните команду show user. Приостановите сессию. Возобновите сессию. Убейте сессии. Сохраните скриншот консоли Router2.

5.8. Сохраните топологию.

Практическое занятие №2. Статическая маршрутизация.

1 Порядок выполнения и сдачи работы

1.1 Изучить теоретическую и практическую часть.

1.2 Сдать преподавателю теорию работы путём ответа на контрольные вопросы.

1.3 Выполнить в Packet Tracer практическую часть.

1.4 Получите вариант и выполните в Packet Tracer задание для самостоятельной работы.

1.5 Предъявите преподавателю результат выполнения пунктов 8 и 9 задания для самостоятельной работы.

1.6 Оформите отчёт. Содержание отчёта смотри ниже.

1.7 Защитите отчёт.

2. Теоретическая часть.

2.1 ARP (Address Resolution Protocol).

Когда отправитель определил IP адрес приёмника, он смотрит в свою ARP таблицу чтобы узнать MAC адрес приёмника. Если источник обнаруживает, что MAC и IP адреса приёмника присутствуют в ARP таблице, он устанавливает между ними соответствие и использует его в ходе инкапсуляции IP пакетов во фреймы канального уровня. MAC адреса фреймов канального уровня берутся из ARP таблиц. После этого фрейм по физическому каналу отправляется от отправителя к адресату.

Если отправитель имеет IP пакет для получателя с IP-адресом АДР и этот адрес отсутствует в ARP таблице, то отправитель отправляет по сети широковещательный ARP запрос следующего содержания: сообщите MAC адрес сетевого интерфейса с IP-адресом АДР. Запрос принимают все сетевые устройства в сегменте сети, и только устройство, имеющее IP-адрес АДР, реагирует на него, посылая отправителю информацию о MAC адресе своего

сетевого интерфейса с IP адресом АДР. Отправитель записывает пару <MAC адрес, IP-адрес АДР > в свою ARP таблицу [1-3].

2.2 Маршрутизация

Протоколы маршрутизации - это правила, по которым осуществляется обмен информации о путях передачи пакетов между маршрутизаторами. Протоколы характеризуются временем сходимости, потерями и масштабируемостью. В настоящее время используется несколько протоколов маршрутизации. Каждый протокол имеет сильные и слабые стороны.

Одна из главных задач маршрутизатора состоит в определении наилучшего пути к заданному адресату. Маршрутизатор определяет пути (маршруты) к адресатам или из статической конфигурации, введённой администратором, или динамически на основании маршрутной информации, полученной от других маршрутизаторов. Маршрутизаторы обмениваются маршрутной информацией с помощью протоколов маршрутизации. Маршрутизатор хранит таблицы маршрутов в оперативной памяти. Таблица маршрутов это список наилучших известных доступных маршрутов. Маршрутизатор использует эту таблицу для принятия решения куда направлять пакет. Для просмотра таблицы маршрутов следует использовать команду show ip route. Даже, если на некотором маршрутизаторе X не задавались никакие команды маршрутизации, тогда он всё равно строит таблицу маршрутов для непосредственно подсоединённых к нему сетей, например [1-3]:

. . .

C 192.168.4.0/24 is directly connected, Ethernet0

10.0.0.0/16 is subnetted, 3 subnets

C 10.3.0.0 is directly connected, Serial0

C 10.4.0.0 is directly connected, Serial1

C 10.5.0.0 is directly connected, Ethernet1

Маршрут на непосредственно подсоединённые сети отображается на интерфейс маршрутизатора, к которому они присоединены. Здесь /24 обозначает маску 255.255. 255.0, а /16 - 255.255.0.0.

Таблица маршрутов отображает сетевые префиксы (адреса сетей) на выходные интерфейсы. Когда X получает пакет, предназначенный для 192.168.4.46, он ищет префикс 192.168.4.0/24 в таблице маршрутов. Согласно таблице пакет будет направлен на интерфейс Ethernet0. Если X получит пакет для 10.3.21.5, он направит его на Serial0.

Эта таблица показывает четыре маршрута для непосредственно подсоединённых сетей. Они имеют метку C. Маршрутизатор X отбрасывает все пакеты, направляемые к сетям, не указанным в таблице маршрутов. Для направления пакетам к другим адресатам необходимо в таблицу включить дополнительные маршруты. Новые маршруты могут быть добавлены двумя методами [1-3]:

Статическая маршрутизация – администратор вручную определяет маршруты к сетям назначения.

Динамическая маршрутизация – маршрутизаторы следуют правилам, определяемым протоколами маршрутизации для обмена информацией о маршрутах и выбора лучшего пути.

Статические маршруты не меняются самим маршрутизатором. Динамические маршруты изменяются самим маршрутизатором автоматически при получении информации о смене маршрутов от соседних маршрутизаторов. Статическая маршрутизация потребляет мало вычислительных ресурсов и полезна в сетях, которые не имеют нескольких путей к адресату назначения. Если от маршрутизатора к маршрутизатору есть только один путь, то часто используют статическую маршрутизацию.

Для конфигурации статической маршрутизации в маршрутизаторах Cisco используют две версии команды ip route

Первая версия

ip route АдресСетиНазначения МаскаСетиНазначения Интерфейс

Команда указывает маршрутизатору, что все пакеты, предназначенные для АдресСетиНазначения-МаскаСетиНазначения следует направлять на свой интерфейс Интерфейс. Если интерфейс Интерфейс - типа Ethernet, то

физические (MAC) адреса исходящих пакетов будут широковещательными (почему?).

Вторая версия

ip route АдресСетиНазначения МаскаСетиНазначения Адрес

Команда указывает маршрутизатору, что все пакеты, предназначенные для АдресСетиНазначения-МаскаСетиНазначения, следует направлять на тот свой интерфейс, из которого достижим IP адрес Адрес. Как правило, Адрес это адрес следующего хопа по пути к АдресСетиНазначения. Выходной интерфейс и физические адреса исходящих пакетов определяются маршрутизатором по своим ARP таблицам на основании IP адреса Адрес [1-3]. Например

ip route 10.6.0.0 255.255.0.0 Serial1 (1)

ip route 10.7.0.0 255.255.0.0 10.4.0.2 (2)

Первый пример отображает сетевой префикс 10.6.0.0/16 на локальный интерфейс маршрутизатора Serial1. Следующий пример отображает сетевой префикс 10.7.0.0/16 на IP адрес 10.4.0.2 следующего хопа по пути к 10.7.0.0/16. Обе эти команды добавят статические маршруты в таблицу маршрутизации (метка S):

S 10.6.0.0 via Serial1

S 10.7.0.0 [1/0] via 10.4.0.2

Когда интерфейс падает, все статические маршруты, отображаемые на этот интерфейс, удаляются из таблицы маршрутов. Если маршрутизатор не может больше найти адрес следующего хопа по пути к адресу, указанному в статическом маршруте, то маршрут исключается из таблицы.

Заметим, что для сетей типа Ethernet рекомендуется всегда использовать форму (2) команды ip route. Ethernet интерфейс на маршрутизаторе, как правило, соединён с несколькими Ethernet интерфейсами других устройств в сети. Указание в команде ip route IP адреса позволит маршрутизатору правильно сформировать физический адрес выходного пакета по своим ARP таблицам.

2.3 Маршрутизация по умолчанию.

Совсем не обязательно, чтобы каждый маршрутизатор обслуживал маршруты ко всем возможным сетям назначения. Вместо этого маршрутизатор хранит маршрут по умолчанию или шлюз последнего пристанища (last resort). Маршруты по умолчанию используются, когда маршрутизатор не может поставить в соответствие сети назначения строку в таблице маршрутов. Маршрутизатор должен использовать маршрут по умолчанию для отсылки пакетов другому маршрутизатору. Следующий маршрутизатор будет иметь маршрут к этой сети назначения или иметь свой маршрут по умолчанию к третьему маршрутизатору и т.д. В конечном счёте, пакет будет маршрутизирован на маршрутизатор, имеющий маршрут к сети назначения.

Маршрут по умолчанию может быть статически введен администратором или динамически получен из протокола маршрутизации [1-3].

Так как все IP адреса принадлежат сети 0.0.0.0 с маской 0.0.0.0, то в простейшем случае надо использовать команду

ip route 0.0.0.0 0.0.0.0 [адрес следующего хопа | выходной интерфейс]

Ручное задание маршрута по умолчанию на каждом маршрутизаторе подходит для простых сетей. В сложных сетях необходимо организовать динамический обмен маршрутами по умолчанию.

2.4 Интерфейс петля

На сетевых устройствах можно создавать сетевые интерфейсы не связанные с реальными каналами для передачи данных и назначать на них IP адреса с масками. Такие интерфейсы называют петлями (loopback). Петли полезны при поэтапном проектировании сетей. Если к какому-то реальному сетевому интерфейсу маршрутизатора в дальнейшем будет подсоединена подсеть, то в начале на маршрутизаторе создаётся loopback, настраивается в плане взаимодействия с остальными участками сети и лишь затем заменяется на реальный интерфейс. Интерфейс петля появляется после команды interface loopbackN или сокращённо int lN, где N целое неотрицательное число – номер петли. Например

Router(conf)>int l0 1.1.1.1 255.0.0.0

2.5 Команда trace

Команда trace является идеальным способом для выяснения того, куда отправляются данные в сети. Эта команда использует ту же технологию протокола ICMP, что и команда ping, только вместо проверки сквозной связи между отправителем и получателем, она проверяет каждый шаг на пути. Команда trace использует способность маршрутизаторов генерировать сообщения об ошибке при превышении пакетом своего установленного времени жизни (Time To Live, TTL). Эта команда посылает несколько пакетов и выводит на экран данные про время прохождения туда и назад для каждого из них. Преимущество команды trace заключается в том, что она показывает очередной достигнутый маршрутизатор на пути к пункту назначения. Это очень мощное средство для локализации отказов на пути от отправителя к получателю [1-3]. Варианты ответов утилиты trace

Символ	Значение
!H	Зондирующий пакет был принят маршрутизатором, но не переадресован, что обычно бывает из-за списка доступа
P	Протокол недосягаем
N	Сеть недосягаема
U	Порт недосягаем
*	Превышение границы ожидания

3 Практическая часть

3.1 ARP

1. Присоединитесь к маршрутизатору Router1 с и посмотрите его ARP таблицу

Router1#show arp

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.1               -   00D0.58B7.80A1  ARPA   FastEthernet0/0
```

Она содержит только одну строку о MAC адресе своего Ethernet интерфейса с IP адресом 10.1.1.1.

2. Присоединитесь к маршрутизатору router2 и посмотрите его ARP таблицу. Она содержит только одну строку о MAC адресе своего Ethernet интерфейса с IP адресом 10.1.1.2

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.2                -   00D0.BA88.005C  ARPA   FastEthernet0/0
```

3. Пропингуйте Ethernet интерфейс маршрутизатора Router1

Router2#ping 10.1.1.1

4. Снова посмотрите вашу ARP таблицу. Она содержит уже две строки. Появилась запись о MAC адресе Ethernet интерфейса Router1 с IP адресом 10.1.1.1.

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.1                0   00D0.58B7.80A1  ARPA   FastEthernet0/0
Internet  10.1.1.2                -   00D0.BA88.005C  ARPA   FastEthernet0/0
```

5. Присоединитесь к маршрутизатору router1 и посмотрите его ARP таблицу. Она содержит уже две строки

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.1                -   00D0.58B7.80A1  ARPA   FastEthernet0/0
Internet  10.1.1.2                2   00D0.BA88.005C  ARPA   FastEthernet0/0
```

Появилась запись о MAC адресе Ethernet интерфейса маршрутизатора Router2 с IP адресом 10.1.1.2. Почему, ведь мы не слали от Router1 никаких IP пакетов? Потому, что Router1 для ответа на пинг от Router2 должен был знать о MAC адресе Ethernet интерфейса Router2 с IP адресом 10.1.1.2, и он сформировал ARP пакет для его получения.

3.2 Статические маршруты

В прошлой работе мы не могли из маршрутизаторов Router2 и Router4 пропинговать некоторые интерфейсы из-за отсутствия маршрутизации. Исправим положение.

1. Присоединитесь к маршрутизатору router2. Мы не могли пинговать адреса 172.16.10.1 и 172.16.10.2. Посмотрите таблицу маршрутов

Router2# show ip route

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

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
```

Видим непосредственно присоединённые сети. Нет маршрута к сети 172.16.10.0/24. Добавим маршрут к сети 172.16.10.0/24 через адрес 10.1.1.1 ближайшего хода на пути к этой сети:

Router2(config)#ip route 172.16.10.0 255.255.255.0 10.1.1.1

Здесь и далее 172.16.10.0/24 – это сокращённая запись - определение подсети 172.16.10.0 с маской 255.255.255.0. В маске 255.255.255.0 содержится 24 единицы, что и обозначается /24.

2. Успешно пропингуем serial интерфейс Router1

Router2#ping 172.16.10.1

Снова посмотрите таблицу маршрутов

```
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
     172.16.0.0/24 is subnetted, 1 subnets
S       172.16.10.0 [1/0] via 10.1.1.1
```

3. Но нам не удастся пропинговать serial интерфейс Router4.

Router2#ping 172.16.10.2

Почему? Потому, что ICMP пакеты пингов не знают, как им вернуться обратно от Router4, так как на Router4 не прописаны маршруты.

4. Присоединитесь к маршрутизатору router4. Посмотрите таблицу маршрутов

Router4# show ip route

```
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.10.0 is directly connected, Serial2/0
```

Нет маршрута к сети 10.1.1.0/24. Добавим маршрут к сети 10.1.1.0/24 через адрес 172.16.10.1 ближайшего хопа на пути к этой сети:

Router4(config)#ip route 10.1.1.0 255.255.255.0 172.16.10.1

```
     10.0.0.0/24 is subnetted, 1 subnets
S       10.1.1.0 [1/0] via 172.16.10.1
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.10.0 is directly connected, Serial2/0
```

5. Теперь все сетевые интерфейсы в сети пингуются из каждого сетевого устройства. Проверьте это.

3.3 Маршрутизация по умолчанию.

Сетевые устройства Router2 и Router4 имеют только по одному выходу во внешний мир: через интерфейсы с адресами 10.1.1.1 и 172.16.10.1, соответственно. Поэтому, можно не определять на какие подсети мы маршрутизируем пакеты и использовать маршрутизацию по умолчанию.

1. Вначале удалим старые маршруты.

Router2(config)#no ip route 172.16.10.0 255.255.255.0 10.1.1.1

Router4(config)#no ip route 10.1.1.0 255.255.255.0 172.16.10.1

2. И назначим маршруты по умолчанию.

Router2(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.1

Router4(config)#ip route 0.0.0.0 0.0.0.0 172.16.10.1

3. Посмотрите таблицу маршрутов на всех устройствах.

Router2#sh ip route

```
Gateway of last resort is 10.1.1.1 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.1.1.1
```

Router4#sh ip route

```
Gateway of last resort is 172.16.10.1 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.10.0 is directly connected, Serial2/0
S*   0.0.0.0/0 [1/0] via 172.16.10.1
```

4. Все сетевые интерфейсы в сети пингуются из каждого сетевого устройства. Проверьте это.

3.4 Loopback

1. Определим интерфейс петлю на устройстве Router4

Router4(conf)#int loopback 0 1.1.1.1 255.255.255.0

2. Пропишем на устройстве Router1 маршрут на сеть петли

Router1(conf)# ip route 1.1.1.0 255.255.255.0 172.16.10.2

3. Присоединимся к устройству Router2 и пропингуем созданную петлю

Router2#ping 1.1.1.1

Сохраните проект в целом и конфигурацию каждого маршрутизатора в отдельный файл.

4 Контрольные вопросы

4.1. Как отправитель узнаёт MAC адрес получателя?

4.2. Как посмотреть ARP таблицу?

4.3. Когда в ARP таблице появляются новые строки?

4.4. Что такое таблица маршрутов?

4.5. Если администратор не настраивал никаких маршрутов, то что она будет содержать?

4.6. Чем статическая маршрутизация отличается от динамической?

4.7. Какие две формы задания статической маршрутизации вы знаете?

4.8. Как в команде маршрутизации определяется сеть назначения?

4.9. Почему для сетей типа Ethernet рекомендуется всегда использовать форму (2) команды маршрутизации?

4.10. Объясните значения полей в командах маршрутизации.

4.11. Почему в качестве поля Адрес рекомендуют использовать адрес следующего хопа по пути к сети назначения.

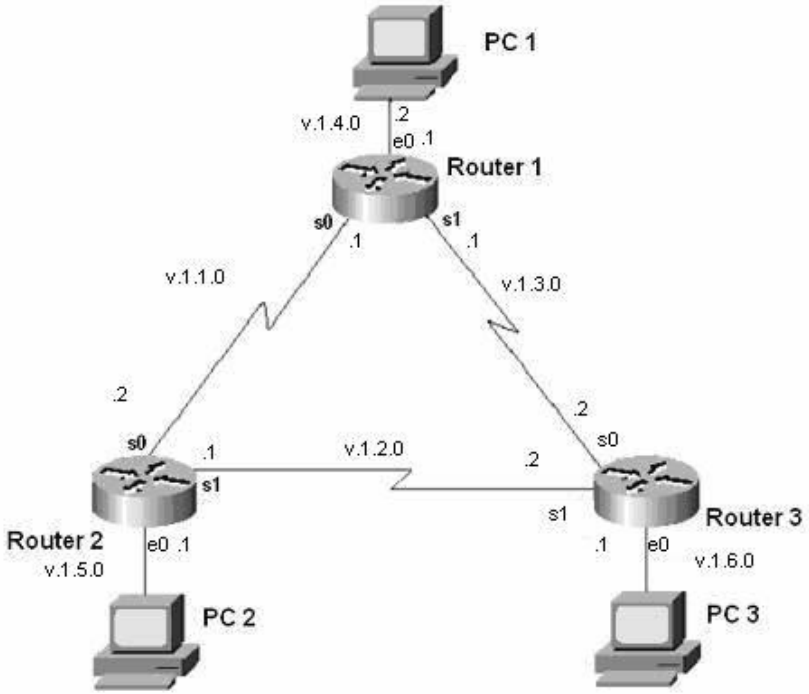
4.12. Когда используется маршрутизация по умолчанию?

4.13. Когда используют интерфейс петля?

4.14. Как работает команда трасировки?

5 Задание для самостоятельной работы

5.1. Построить в Packet Tracer топологию, представленую на рисунке. Использовать необходимые маршрутизаторы.



В нашей сети шесть подсетей. Вы видите, что каждый маршрутизатор подключён к трём подсетям.

5.2. На каждом маршрутизаторе поднять используемые интерфейсы и посмотреть соседей командой show cdp neighbors. Сделать скриншоты.

5.3. Назначить интерфейсам сети адреса согласно рисунку 1 и таблице 1 в которых v – это номер варианта. Все маски 255.255.255.0. Не забудьте назначить шлюзы по умолчанию для компьютеров согласно таблицы.

	v.1.1.0	v.1.2.0	v.1.3.0	v.1.4.0	v.1.5.0	v.1.6.0
Router1	S0:v.1.1.1		S1:v.1.3.1	E0:v.1.4.1		
Router2	S0:v.1.1.2	S1:v.1.2.1			E0:v.1.5.1	
Router3		S0:v.1.2.2	S1:v.1.3.2			E0:v.1.6.1
PC1				E0:v.1.4.2		
PC2					E0:v.1.5.2	
PC3						E0:v.1.6.2

5.4. Проверьте факт назначения адресов путём выполнения на каждом маршрутизаторе команд show running-config и show ip interface brief. Для компьютеров используйте команду ipconfig.

5.5. Проверьте правильность назначения адресов путём выполнения на каждом маршрутизаторе команд ping к непосредственным соседям. Например, на маршрутизаторе Router1 выполните

Router1#ping v.1.1.2

Router1#ping v.1.3.2

Router1#ping v.1.4.2

5.6. Поставим перед собой задачу связать между собой компьютеры PC1, PC2 и PC3. Для этого осуществим на маршрутизаторах настройку статической маршрутизации. В каждом маршрутизаторе пропишем маршруты на удалённые Ethernet сети. Для решения поставленной задачи маршрутизировать пакеты на удалённые сети последовательных соединений не надо.

У каждого маршрутизатора есть по две на удалённые Ethernet сети. Всего надо прописать шесть статических маршрутов.

Чтобы из маршрутизатора router1 достичь удалённую Ethernet сеть v.1.5.0/24, пакеты можно направить на IP адрес 1.1.1.2 ближайшего внешнего интерфейса на пути в эту сеть. Это сделает команда

router1(config)#ip route 1.1.5.0 255.255.255.0 1.1.1.2

Задайте остальные пять команд маршрутизации.

5.7. На каждом маршрутизаторе посмотреть таблицу маршрутизации командой show ip route. Сделать скриншоты.

5.8. На каждом маршрутизаторе сделайте скриншоты расширенных пингов

а) на маршрутизаторе router1 от PC2 к PC3

б) на маршрутизаторе router2 от PC1 к PC3

в) на маршрутизаторе router3 от PC1 к PC2

Например, результат расширенного пинга на маршрутизаторе router1 от PC2 к PC3 для для варианта 1 (v=1) имеет вид

```
router1#ping
Protocol [ip]:
Target IP address: 1.1.6.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:y
Source address or interface:1.1.5.2
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.6.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

5.9. На каждом компьютере сделайте о скриншоты выполнения команд трасировки tracert других компьютеров. Всего шесть скриншотов. Например, трасировка из PC1 на PC2 для варианта 1 (v=1)

```
PC1:#tracert 1.1.5.2


"Type escape sequence to abort."
Tracing the route to 1.1.5.2

 1 1.1.4.1 0 msec 16 msec 0 msec
 2 1.1.1.2 20 msec 16 msec 16 msec
 3 1.1.5.2 20 msec 16 msec *
```

5.10. Сохраните проект.

Практическое занятие №3. Динамическая маршрутизация.

Порядок выполнения и сдачи работы

1.1 Изучить теоретическую и практическую часть.

1.2 Сдать преподавателю теорию работы путём ответа на контрольные вопросы.

1.3 Выполнить в Packet Tracer практическую часть.

1.4 Используя вариант из предыдущей лабораторной работы, выполните в Boson задание для самостоятельной работы.

1.5 Предъявите преподавателю результат выполнения пунктов 7, 10, 14 и 18 задания для самостоятельной работы.

1.6 Оформите отчёт. Содержание отчёта смотри ниже.

1.7 Защитите отчёт.

2. Теоретическая часть.

Статическая маршрутизация не подходит для больших, сложных сетей потому, что обычно сети включают избыточные связи, многие протоколы и смешанные топологии. Маршрутизаторы в сложных сетях должны быстро адаптироваться к изменениям топологии и выбирать лучший маршрут из многих кандидатов.

IP сети имеют иерархическую структуру. С точки зрения маршрутизации сеть рассматривается как совокупность автономных систем. В автономных подсистемах больших сетей для маршрутизации на остальные автономные системы широко используются маршруты по умолчанию.

Динамическая маршрутизация может быть осуществлена с использованием одного и более протоколов. Эти протоколы часто группируются согласно того, где они используются. Протоколы для работы внутри автономных систем называют внутренними протоколами шлюзов (interior gateway protocols (IGP)), а протоколы для работы между автономными системами называют внешними протоколами шлюзов (exterior gateway protocols

(EGP)). К протоколам IGP относятся RIP, RIP v2, IGRP, EIGRP, OSPF и IS-IS. Протоколы EGP3 и BGP4 относятся к EGP. Все эти протоколы могут быть разделены на два класса: дистанционно-векторные протоколы и протоколы состояния связи [1-3].

Маршрутизаторы используют метрики для оценки или измерения маршрутов. Когда от маршрутизатора к сети назначения существует много маршрутов, и все они используют один протокол маршрутизации, то маршрут с наименьшей метрикой рассматривается как лучший. Если используются разные протоколы маршрутизации, то для выбора маршрута используется административные расстояния, которые назначаются маршрутам операционной системой маршрутизатора.

RIP использует в качестве метрики количество переходов (хопов). EIGRP использует сложную комбинацию факторов, включающую полосу пропускания канала и его надёжность.

Результаты работы маршрутизирующих протоколов заносятся в таблицу маршрутов, которая постоянно изменяется при смене ситуации в сети. Рассмотрим типичную строку в таблице маршрутов, относящуюся к динамической маршрутизации [1-3].

R 192.168.14.0/24 [120/3] via 10.3.0.1 00:00:06 Serial0

Здесь R определяет протокол маршрутизации. Так R означает RIP, а O – OSPF и т.д. Запись [120/3] означает, этот маршрут имеет административное расстояние 120 и метрику 3. Эти числа маршрутизатор использует для выбора маршрута. Элемент 00:00:06 определяет время, когда обновилась данная строка. Serial0 это локальный интерфейс, через который маршрутизатор будет направлять пакеты к сети 192.168.14.0/24 через адрес 10.3.0.1.

Для того чтобы динамические протоколы маршрутизации обменивались информацией о статических маршрутах, следует осуществлять дополнительное конфигурирование.

2.1 Дистанционно-векторная маршрутизация

Эта маршрутизация базируется на алгоритме Белмана-Форда. Через определённые моменты времени маршрутизатор передаёт соседним маршрутизаторам всю свою таблицу маршрутизации. Такие простые протоколы как RIP и IGRP просто распространяют информацию о таблицах маршрутов через все интерфейсы маршрутизатора в широковещательном режиме без уточнения точного адреса конкретного соседнего маршрутизатора.

Соседний маршрутизатор, получая широковещание, сравнивает информацию со своей текущей таблицей маршрутов. В неё добавляются маршруты к новым сетям или маршруты к известным сетям с лучшей метрикой. Происходит удаление несуществующих маршрутов. Маршрутизатор добавляет свои собственные значения к метрикам полученных маршрутов. Новая таблица маршрутизации снова распространяется по соседним маршрутизаторам (см. рис.1) [1-3].

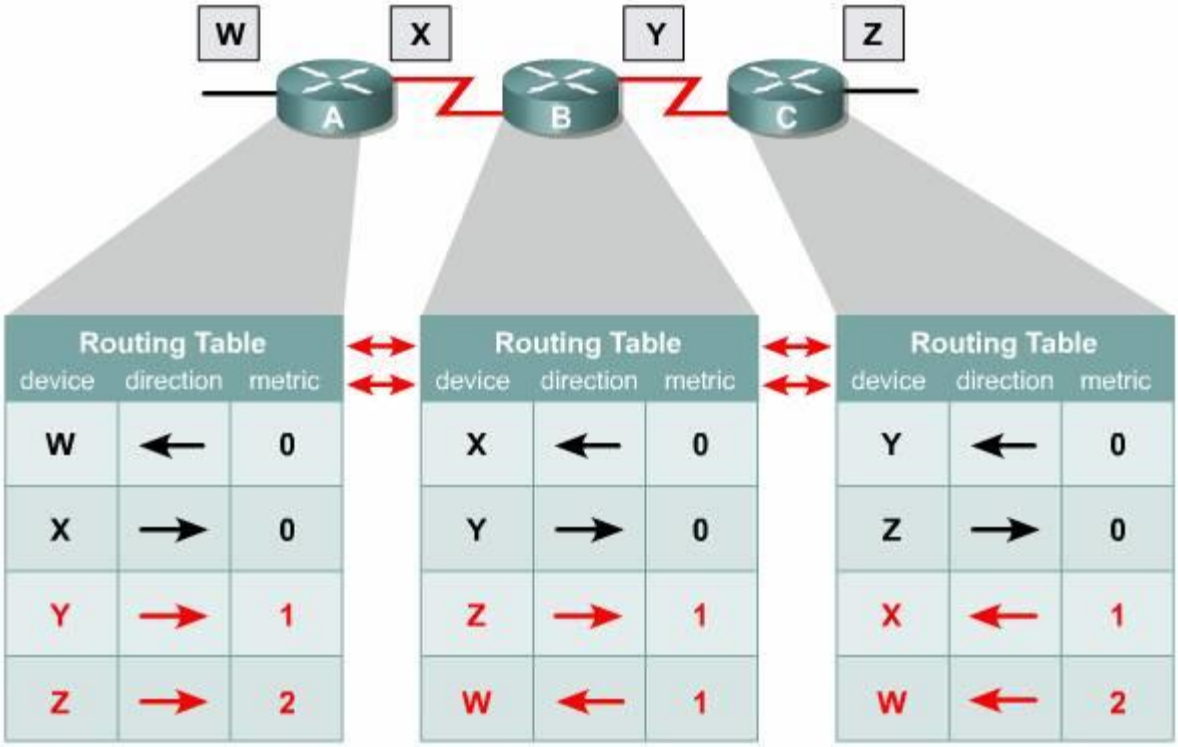


Рис.1. Дистанционно-векторная маршрутизация

2.2 Протоколы состояния связи

Эти протоколы предлагают лучшую масштабируемость и сходимость по сравнению с дистанционно-векторными протоколами. Протокол базируется на алгоритме Дейкстры, который часто называют алгоритмом «кратчайший путь – первым» (shortest path first (SPF)). Наиболее типичным представителем является протокол OSPF (Open Shortest Path First).

Маршрутизатор берёт в рассмотрение состояние связи интерфейсов других маршрутизаторов в сети. Маршрутизатор строит полную базу данных всех состояний связи в своей области, то есть имеет достаточно информации для создания своего отображения сети. Каждый маршрутизатор затем самостоятельно выполняет SPF-алгоритм на своём собственном отображении сети или базе данных состояний связи для определения лучшего пути, который заносится в таблицу маршрутов. Эти пути к другим сетям формируют дерево с вершиной в виде локального маршрутизатора.

Маршрутизаторы извещают о состоянии своих связей всем маршрутизаторам в области. Такое извещение называют LSA (link-state advertisements) [1-3].

В отличие от дистанционно-векторных маршрутизаторов, маршрутизаторы состояния связи могут формировать специальные отношения со своими соседями.

Имеет место начальный наплыв LSA пакетов для построения базы данных состояний связи. Далее обновление маршрутов производится только при смене состояний связи или, если состояние не изменилось в течение определённого интервала времени. Если состояние связи изменилось, то частичное обновление пересылается немедленно. Оно содержит только состояния связей, которые изменились, а не всю таблицу маршрутов.

Администратор, заботящийся об использовании линий связи, находит эти частичные и редкие обновления эффективной альтернативой дистанционно-векторной маршрутизации, которая передаёт всю таблицу маршрутов через регулярные промежутки времени.

Протоколы состояния связи имеют более быструю сходимость и лучшее использование полосы пропускания по сравнению с дистанционно-векторными протоколами. Они превосходят дистанционно-векторные протоколы для сетей любых размеров, однако имеют два главных недостатка: повышенные требования к вычислительной мощности маршрутизаторов и сложное администрирование [1-3].

2.3 Сходимость.

Этот процесс одновременно и совместный, и индивидуальный. Маршрутизаторы разделяют между собой информацию, но самостоятельно пересчитывают свои таблицы маршрутизации. Для того чтобы индивидуальные таблицы маршрутизации были точными, все маршрутизаторы должны иметь одинаковое представление о топологии сети. Если маршрутизаторы договорились о топологии сети, то имеет место их сходимость. Быстрая сходимость означает быстрое восстановление после обрыва связей и других изменений в сети. О протоколах маршрутизации и о качестве проектирования сети судят главным образом по сходимости.

Когда маршрутизаторы находятся в процессе сходимости, сеть восприимчива к проблемам маршрутизации. Если некоторые маршрутизаторы определили, что некоторая связь отсутствует, то другие ошибочно считают эту связь присутствующей. Если это случится, то отдельная таблица маршрутов будет противоречива, что может привести к отбрасыванию пакетов и петлям маршрутизации [1-3].

Невозможно, чтобы все маршрутизаторы в сети одновременно обнаружили изменения в топологии. В зависимости от использованного протокола, может пройти много времени пока все процессы маршрутизации в сети сойдутся. На это влияют следующие факторы:

Расстояние в хопах до точки изменения топологии.

Число маршрутизаторов, использующих динамические протоколы.

Полоса пропускания и загрузка каналов связи.

Загрузка маршрутизаторов .

Эффект некоторых факторов может быть уменьшен при тщательном проектировании сети.

2.4 Конфигурирование динамической маршрутизации

Для конфигурирования динамической маршрутизации используются две основные команды: router i network. Команда router запускает процесс маршрутизации и имеет форму:

Router(config)# router protocol [keyword]

где Protocol - любой из протоколов маршрутизации: RIP, IGRP, OSPF и т.п., keyword –дополнительные параметры.

Затем необходимы команды network:

Router (config-router)# network network-number [keyword]

где network-number - идентифицирует непосредственно подключенную сеть, добавляемую в процесс маршрутизации, keyword –дополнительные параметры. network-number позволяет процессу маршрутизации определить интерфейсы, которые будут брать участие в отсылке и приёме пакетов актуализации маршрутной информации [1-3].

Для просмотра информации о протоколах маршрутизации используется команда show ip protocol., которая выводит значения таймеров процессов маршрутизации и сетевую информацию, имеющую отношение к маршрутизации. Эта информация может использоваться для идентификации маршрутизатора, подозреваемого в поставке плохой маршрутной информации

Содержимое таблицы IP маршрутизации выводится командой show ip route. Она содержит записи про все известные маршрутизатору сети и подсети и указывает на способ получения этой информации.

2.5 Протокол RIP

Ключевые характеристики протокола RIP [1-3]:

- маршрутизация на основании вектора расстояния;
- метрика при выборе пути в виде количества переходов (хопов);
- максимально допустимое количества хопов- 15;

- по умолчанию пакеты актуализации маршрутной информации посылаются в режиме широковещания каждые 30 секунд.

Выбор протокола RIP як протокола маршрутизации осуществляется командой:

Router(config)# router rip

Команда network назначает IP адрес сети с которой маршрутизатор имеет непосредственное соединение.

Router(config-router)# network network-number

Процесс маршрутизации связывает интерфейсы с соответствующими адресами и начинает обработку пакетов в заданных сетях.

В показанном на рис.2 примере команды network 1.0.0.0 и network 2.0.0.0 задают непосредственно подключенные к маршрутизатора Cisco A сети.

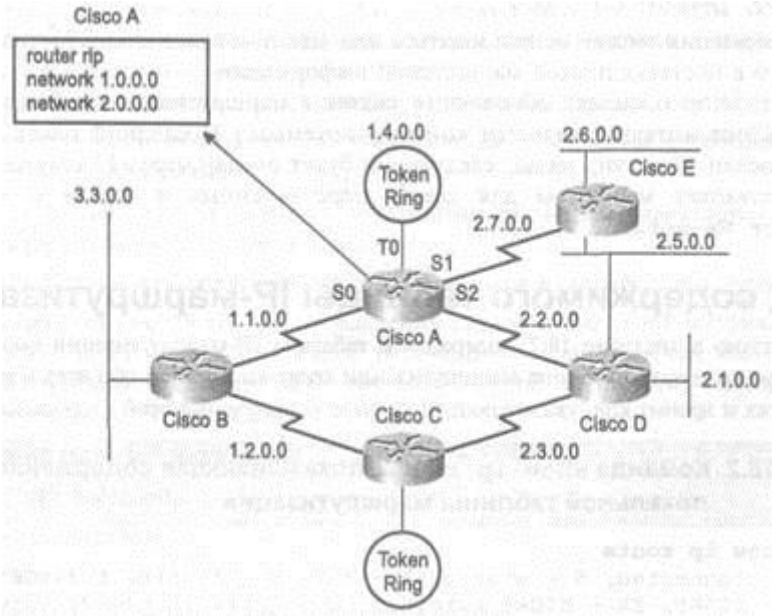


Рис.2.

Команда debug ip rip выводит содержание пакетов актуализации маршрутной информации протокола RIP в том виде, в котором эти данные посылаются и принимаются.

2.6 Протокол IGRP

IGRP представляет собою протокол маршрутизации по вектору расстояния разработанный компанией Cisco. Этот протокол посылает пакеты

актуализации маршрутной информации с 90-секундным интервалом, в которых содержатся сведения о сетях для конкретной автономной системы. Этот протокол характеризует универсальность, позволяющую автоматически справляться со сложными топологиями, и гибкость в работе с сегментами, имеющими разные характеристики по полосе пропускания и величины задержки. Используемая им метрика не имеет свойственных протоколу RIP ограничений по количеству переходов. Она включает следующие составляющие: Ширина полосы пропускания; Величина задержки; Уровень загрузки; Надёжность канала; Размер максимального блока передачи в канале.

Выбор протоколу IGRP в качестве протокола маршрутизации осуществляется с помощью команды [1-3]:

Router (config)# router igrp autonomous-system

где параметр Autonomous-system называют номером автономной системы и он идентифицирует вычислительный процесс IGRP- маршрутизации. Процессы в маршрутизаторах сети с одинаковым номером autonomous-system будут коллективно использовать маршрутную информацию.

Команда network задаёт непосредственно присоединённые сети, которые подлежат включению в данный процесс маршрутизации:

Router(config-router)#network network-number

В показанном примере на рис.3 на маршрутизаторе Cisco A запущен маршрутизирующий процесс, организующий IGRP маршрутизацию в автономной системе с номером 109. В маршрутизции будут участвовать сети 1.0.0.0 и 2.0.0.0.

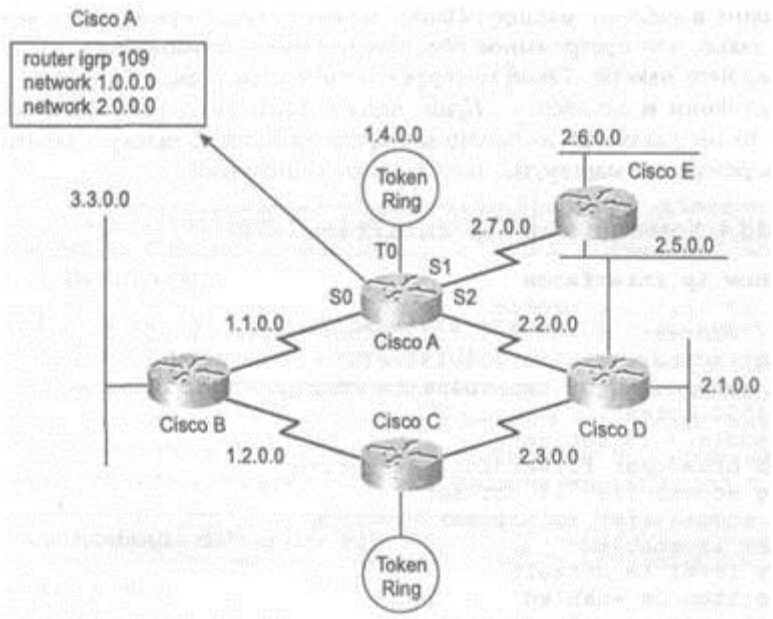


Рис.3.

Команда debug ip igrp transactions и debug ip igrp events выводят содержание пакетов актуализации маршрутной информации протокола IGRP в том виде, в котором эти данные посылаются и принимаются

2.7 Протокол OSPF

OSPF это динамический, иерархический протокол состояния связи, используемый для маршрутизации внутри автономных систем. Он базируется на открытых стандартах и был спроектирован как замена протоколу RIP. Он является развитием ранних версий протокола маршрутизации IS-IS. OSPF - устойчивый протокол, поддерживающий маршрутизацию с наименьшим весом и балансировку загрузки. Кратчайший путь в сети вычисляется по алгоритму Дейкстры. Cisco поддерживает свою версию стандарта OSPF [1-3].

Как только маршрутизатор настроен на работу с OSPF, он начинает процесс изучения окружения, проходя несколько фаз инициализации. В начале маршрутизатор использует Hello для определения своих соседей и создания отношений для обмена обновлением маршрутной информацией с ними. Затем маршрутизатор начинает фазу ExStart начального обмена между базами маршрутов. Следующей является фаза обмена, в которой назначеный маршрутизатор отсылает маршрутную информацию и получает подтверждения

от нашего нового маршрутизатора. В течение стадии загрузки, новый маршрутизатор компилирует таблицу маршрутов. По окончании вычислений маршрутизатор переходит в полное состояние, в котором он является активным членом сети.

Для запуска OSPF маршрутизации служит команда

Router(config)#router ospf N,

где N-номер вычислительного процесса OSPF. В отличие от IGRP он может быть различным для разных маршрутизаторов автономной системы. OSPF область Area организуется командой

Router(config-router)# network network-number area Area

и определяет автономную систему.

В OSPF network-number имеет особый формат. Для подключаемой в процесс маршрутизации сети используетя инверсная маска. Так, чтобы сеть 212.34.0.0 255.255.0.0 поместить в область 7 OSPF маршрутизации следует дать команду

Router(config-router)# network 212.34.0.0 0.0.255.255 area 7

Команда show ip ospf interface для каждого интерфейса выводит всю OSPF информацию: IP адрес, область, номер процесса, идентификатор маршрутизатора, стоимость, приоритет, тип сети, интервалы таймера.

Команда show ip ospf neighbor показывает важную информацию, касающуюся состояния соседей.

3 Практическая часть.

3.1 Загрузите в симулятор топологию и конфигурацию, использованную практической части лабораторной работы №2.

3.2 Если сделано всё правильно вы сможете пропинговать из любого маршрутизаторы адреса непосредственно соединённых интерфейсов других маршрутизаторов. На каждом устройстве, используя команды CDP show cdp neighbors detail, получите IP адреса соседних устройств и пропингуйте их.

3.3 В лабораторной работе №2 мы не смогли пинговать дальние интерфейсы. Из Router2 была недоступна сеть 172.16.10.0/24, а из Router4 была недоступна сеть 10.1.1.0/24. В лабораторной работе №3 с помощью статической маршрутизации мы решили проблему. В этой работе для решения проблемы используем разные формы динамической маршрутизации.

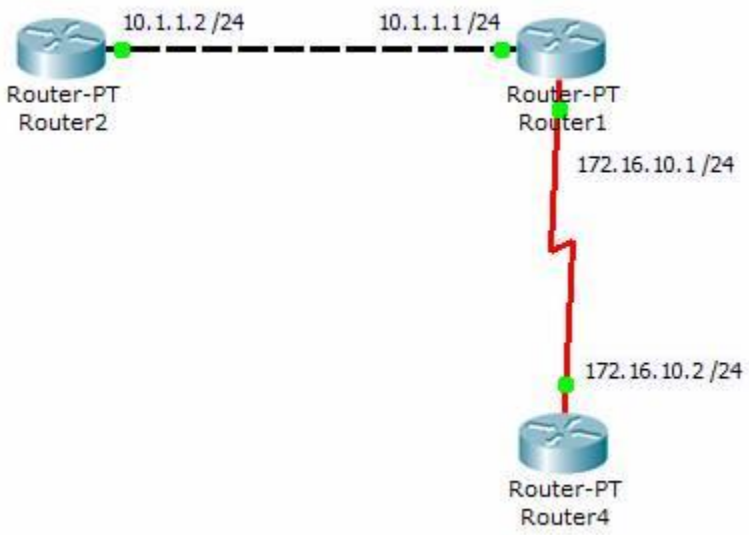


Рис. 4.

3.4. Посмотрим таблицы маршрутов

Router2# sh ip route

Нет маршрута на сеть 172.16.10.0/24.

Поэтому в эту сеть из Router2 не идут пинги.

Router4# sh ip route

Нет маршрута на сеть 10.1.1.0/24.

Поэтому в эту сеть из Router4 не идут пинги.

3.1 RIP

1. Включим RIP на всех маршрутизаторах

Router1(config)# router rip

Router1(config-router)# network 172.16.10.0

Router1(config-router)# network 10.1.1.0

Router2(config)# router rip

Router2 (config-router)# network 10.1.1.0

Router4(config)# router rip

Router4 (config-router)# network 172.16.10.0

2. На каждом роутере командой show running-config посмотрим как маршрутизаторы поняли наши команды. Видим, что сеть 10.1.1.0/24 воспринята как сеть 10.0.0.0/8, а сеть 172.16.10.0/24 воспринята как сеть 172.16.0.0/16. Это связано с классами IP адресов.

3. Командой show ip protocols посмотрим с какими параметрами работает протокол RIP. Например, для Router1 имеем

```
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 6 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial2/0             1     2 1
  FastEthernet0/0       1     2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
        10.0.0.0
        172.16.0.0
Passive Interface(s):
Routing Information Sources:
        Gateway         Distance      Last Update
Distance: (default is 120)
```

Переведите сообщение.

4. Посмотрим таблицы маршрутов

Router2# sh ip route

```
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
R    172.16.0.0/16 [120/1] via 10.1.1.1, 00:00:15, FastEthernet0/0
```

Есть маршрут на сеть 172.16.10.0/24 через интерфейс Ethernet на адрес 10.1.1.1.

Пинги в эту сеть из Router2 пойдут. Проверьте

Router2#ping 172.16.10.1

Router2# ping 172.16.10.2

5. Перейдём на другой маршрутизатор

Router4# sh ip route

```
R    10.0.0.0/8 [120/1] via 172.16.10.1, 00:00:22, Serial2/0
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.10.0 is directly connected, Serial2/0
```

Есть маршрут на сеть 10.1.1.0/24 через интерфейс Serial на адрес 172.16.10.1.

Пинги в эту сеть из Router4 пойдут. Проверьте

Router4#ping 10.1.1.1

Router4# ping 10.1.1.2.

Командой debug ip rip посмотрим как маршрутизаторы обмениваются маршрутной информацией. Например, для Router1 имеем повторяющиеся каждые 30 секунд сообщения

Router1# debug ip rip

```
RIP: sending update to 255.255.255.255 via Serial0 (172.16.10.1)
 subnet 10.1.1.0, metric 1

RIP: sending update to 255.255.255.255 via Ethernet0 (10.1.1.1)
 subnet 172.16.10.0, metric 1

RIP: received update from 172.16.10.2 on Serial0

RIP: received update from 10.1.1.2 on Ethernet0
```

Выключим трассировку

Router1# no debug ip rip

Сохраните конфигурацию.

3.2 EIGRP

Остановим на всех маршрутизаторах RIP командой

Router(config)#no router rip.

1. Включим EIGRP на всех маршрутизаторах, образуя автономную систему с номером 100

Router1(config)# router eigrp 100

Router1(config-router)# network 172.16.10.0

Router1(config-router)# network 10.1.1.0

Router2(config)# router eigrp 100

Router2 (config-router)# network 10.1.1.0

Router4(config)# router eigrp 100

Router4 (config-router)# network 172.16.10.0

2. На каждом маршрутизаторе командой show running-config посмотрим как маршрутизаторы поняли наши команды. Видим, что сеть 10.1.1.0/24 воспринята как сеть 10.0.0.0/8, а сеть 172.16.10.0/24 воспринята как сеть 172.16.0.0/16. Это связано с классами IP адресов.

3. Командой show ip protocols посмотрим с какими параметрами работает протокол EIGRP. Например, для Router1 имеем

```
Routing Protocol is "eigrp  100 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 100
  Automatic network summarization is in effect
  Automatic address summarization:
    172.16.0.0/16 for FastEthernet0/0
      Summarizing with metric 20512000
    10.0.0.0/8 for Serial2/0
      Summarizing with metric 28160
  Maximum path: 4
  Routing for Networks:
     172.16.0.0
     10.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.10.2     90            8321604
    10.1.1.2        90            8350639
  Distance: internal 90 external 170
```

Переведите сообщение.

4. Посмотрим таблицы маршрутов

Router2# sh ip route

```
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
D    172.16.0.0/16 [90/20514560] via 10.1.1.1, 00:08:37, FastEthernet0/0
```

Есть маршрут на сеть 172.16.10.0/24 через интерфейс Ethernet на адрес 10.1.1.1.

Пинги в эту сеть из Router2 пойдут. Проверьте

Router2#ping 172.16.10.1

Router2# ping 172.16.10.2

5. Перейдём на другой маршрутизатор

Router4# sh ip route

```
D    10.0.0.0/8 [90/20514560] via 172.16.10.1, 00:12:30, Serial2/0
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.10.0 is directly connected, Serial2/0
```

Есть маршрут на сеть 10.1.1.0/24 через интерфейс Serial на адрес 172.16.10.1.

Пинги в эту сеть из Router4 пойдут. Проверьте

Router4#ping 10.1.1.1

Router4# ping 10.1.1.2.

6. Командами debug ip eigrp transactions и debug ip eigrp events посмотрите как маршрутизаторы обмениваются маршрутной информацией.

Сохраните конфигурацию.

3.3 OSPF

Остановим на всех маршрутизаторах EIGRP командой

Router(config)#no router eigrp 100

1. Включим OSPF на всех маршрутизаторах. Дадим процессу OSPF номер 100. Образуем OSPF область 0

Router1(config)#router ospf 100

Router1(config-router)# network 172.16.10.0 0.0.0.255 area 0

Router1(config-router)# network 10.1.1.0 0.0.0.255 area 0

Router2(config)#router ospf 100

Router2(config-router)# network 10.1.1.0 0.0.0.255 area 0

Router4(config)# router ospf 100

Router4(config-router)# network 172.16.10.0 0.0.0.255 area 0

2. Команда show running-config показывает, что маршрутизаторы поняли наши команды в том же виде, как мы их и задавали.

3. Командой show ip protocols посмотрим с какими параметрами работает протокол OSPF. Например, для Router1 имеем

```
Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.16.10.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.10.0 0.0.0.255 area 0
    10.1.1.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.1.2             110      00:01:40
    172.16.10.2          110      00:01:45
  Distance: (default is 110)
```

Переведите сообщение.

4. Посмотрим таблицы маршрутов

Router2# sh ip route

```
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
     172.16.0.0/24 is subnetted, 1 subnets
O       172.16.10.0 [110/782] via 10.1.1.1, 00:08:26, FastEthernet0/0
```

Есть маршрут на сеть 172.16.10.0/24 через интерфейс Ethernet на адрес 10.1.1.1.

Пинги в эту сеть из Router2 пойдут. Проверьте

Router2# ping 172.16.10.1

Router2# ping 172.16.10.2

5. Перейдём на другой маршрутизатор

Router4# sh ip route

```
     10.0.0.0/24 is subnetted, 1 subnets
O       10.1.1.0 [110/782] via 172.16.10.1, 00:03:26, Serial2/0
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.10.0 is directly connected, Serial2/0
```

Есть маршрут на сеть 10.1.1.0/24 через интерфейс Serial на адрес 172.16.10.1.

Пинги в эту сеть из Router4 пойдут. Проверьте

Router4# ping 10.1.1.1

Router4# ping 10.1.1.2.

6. Команды show ip ospf interface, show ip ospf database и debug ip igrp neighbor покажут вам всю информацию о параметрах протокола OSPF.

Сохраните конфигурацию.

5. Контрольные вопросы.

5.1 Что такое автономная система.

5.2 Что такое метрика?

5.3 Какие существуют два класса протоколов динамической маршрутизации.

5.4 Объясните работу дистанционно-векторных протоколов.

5.5 Объясните работу протоколов состояния связи.

5.6 Как узнать, какие протоколы маршрутизации запущены на маршрутизаторе?

5.7 В чём преимущества и недостатки дистанционно-векторных протоколов и протоколов состояния связи?

5.8 Что такое сходимость протоколов маршрутизации?

5.9 Какие параметры влияют на скорость сходимости?

5.10 Как на маршрутизаторе запустить и настроить протокол маршрутизации RIP?

5.11 Как на маршрутизаторе запустить и настроить протокол маршрутизации EIGRP?

5.12 Как на маршрутизаторе запустить и настроить протокол маршрутизации OSPF?

5.13 Как посмотреть содержание пакетов актуализации маршрутной информации протокола RIP?

5.14 Как посмотреть содержание пакетов актуализации маршрутной информации протокола EIGRP?

5.15 Уточните, что в EIGRP понимается под автономной системой?

5.16 В чём различие в формате команды router для EIGRP и OSPF?

5.17 В чём различие в формате команд network для RIP, EIGRP и OSPF?

6. Задание для самостоятельной работы.

6.1. Используйте топологию своего варианта из предыдущей лабораторной работы, представленную на рисунке 5.

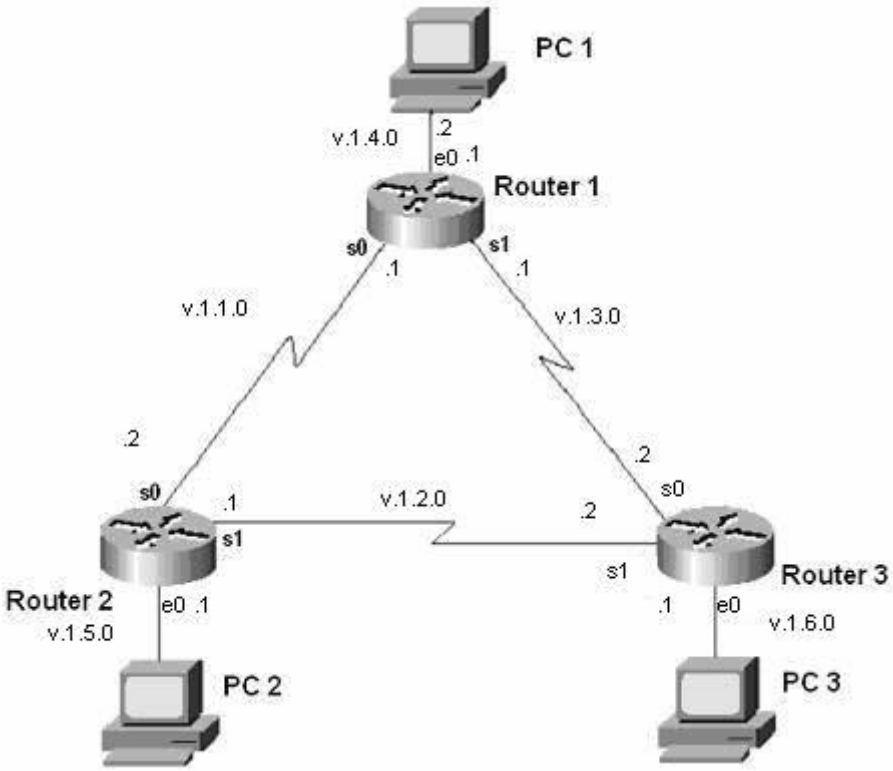


Рис. 5.

В нашей сети шесть подсетей. Вы видите, что каждый маршрутизатор подключён к трём подсетям.

6.2. Отредактируйте вручную сохранённую конфигурацию предыдущей успешно выполненной лабораторной работы: уберите в rtr файлах маршрутизаторов команды статической маршрутизации.

6.3. Загрузите отредактированную конфигурацию в симулятор.

6.4. На каждом маршрутизаторе проверьте правильность загрузки конфигурации командами show cdp neighbors и show ip interface brief.

Если последовательный интерфейс не поднялся, проверьте командой show running-config, что на интерфейсе DCE

стороны последовательной связи задана команда clock rate! Если не задана, то задайте её.

6.5. Настройте на каждом маршрутизаторе динамическую маршрутизацию по протоколу RIP.

6.6. На каждом маршрутизаторе посмотреть таблицу маршрутизации командой show ip route. Сделать скриншоты. Например, для маршрутизатора router1 для варианта 1 (v=1) имеем

```
C       1.1.4.0/24 is directly connected, Ethernet0
C       1.1.1.0/24 is directly connected, Serial0
C       1.1.3.0/24 is directly connected, Serial1
R       1.1.6.0/24 [120/1] via 1.1.3.2, 00:01:43, Serial1
R       1.1.5.0/24 [120/1] via 1.1.1.2, 00:06:30, Serial0
R       1.1.2.0/24 [120/1] via 1.1.1.2, 00:03:35, Serial0
```

6.7. На каждом компьютере выполните команды трассировки tracert других компьютеров. Сделайте скриншоты. Всего шесть скриншотов. Например, трассировка из PC1 на PC2 для варианта 1 (v=1) имеет вид

```
PC1:#tracert 1.1.5.2


"Type escape sequence to abort."
Tracing the route to 1.1.5.2

 1 1.1.4.1 0 msec 16 msec 0 msec
 2 1.1.1.2 20 msec 16 msec 16 msec
 3 1.1.5.2 20 msec 16 msec *
```

Видим, что путь для пакетов из PC1 на PC2 (1.1.5.2) лежит последовательно через Router1 (Ethernet 1.1.4.1) и затем через Router2 (serial0 1.1.1.2)

6.8. Отключим на маршрутизаторе router1 последовательный интерфейс serial 0

Router1(config)#interface serial 0

Router1(config-if)#shutdown

6.9. Через пару минут, когда в сети пройдут обновления маршрутной информации, на каждом маршрутизаторе посмотреть таблицу маршрутизации командой show ip route. Сделать скриншоты. Например, для маршрутизатора router1 для варианта 1 (v=1) имеем

```
C       1.1.4.0/24 is directly connected, Ethernet0
C       1.1.3.0/24 is directly connected, Serial1
R       1.1.2.0/24 [120/1] via 1.1.3.2, 00:07:26, Serial1
R       1.1.6.0/24 [120/1] via 1.1.3.2, 00:08:41, Serial1
R       1.1.5.0/24 [120/2] via 1.1.3.2, 00:07:44, Serial1
```

Видим, что таблица изменилась: пропала сеть 1.1.1.0/24 и все пакеты теперь маршрутизируются на адрес 1.1.3.2 через интерфейс Serial1.

6.10. На каждом компьютере выполните команды трассировки tracert других компьютеров. Сделайте скриншоты. Всего шесть скриншотов. Например, трассировка из PC1 на PC2 для варианта 1 (v=1) имеет вид

```
PC1:#tracert 1.1.5.2


"Type escape sequence to abort."
Tracing the route to 1.1.5.2

 1 1.1.4.1 0 msec 16 msec 0 msec
 2 1.1.3.2 20 msec 16 msec 16 msec
 3 1.1.2.1 20 msec 16 msec 16 msec
 4 1.1.5.2 20 msec 16 msec *
```

Видим, что теперь путь для пакетов из PC1 на PC2 (1.1.5.2) лежит последовательно через Router1 (Ethernet 1.1.4.1) , затем через Router3 (serial0 1.1.3.2) и затем через Router2 (serial1 1.1.2.1).

6.11. Сохраните конфигурацию.

6.12. Отключите RIP и настройте на каждом маршрутизаторе динамическую маршрутизацию по протоколу IGRP.

6.13. На каждом маршрутизаторе посмотреть таблицу маршрутизации командой show ip route. Сделать скриншоты. Например, для маршрутизатора router1 для варианта 1 (v=1) имеем

```
C       1.1.4.0/24 is directly connected, Ethernet0
C       1.1.1.0/24 is directly connected, Serial0
C       1.1.3.0/24 is directly connected, Serial1
I       1.1.6.0/24 [100/651] via 1.1.3.2, 00:02:38, Serial1
I       1.1.5.0/24 [100/651] via 1.1.1.2, 00:04:26, Serial0
I       1.1.2.0/24 [100/651] via 1.1.1.2, 00:08:28, Serial0
```

6.14. Проверьте, что вы всё сделали правильно. На каждом компьютере выполните команд трассировки tracert других компьютеров.

6.15. Сохраните конфигурацию.

6.16. Отключите IGRP и настройте на каждом маршрутизаторе динамическую маршрутизацию по протоколу OSPF.

6.17. На каждом маршрутизаторе посмотреть таблицу маршрутизации командой show ip route. Сделать скриншоты. Например, для маршрутизатора router1 для варианта 1 (v=1) имеем

```
C       1.1.4.0/24 is directly connected, Ethernet0
C       1.1.1.0/24 is directly connected, Serial0
C       1.1.3.0/24 is directly connected, Serial1
O       1.1.5.0/24 [110/65] via 1.1.1.2, 00:00:39, Serial0
O       1.1.2.0/24 [110/65] via 1.1.3.2, 00:00:22, Serial1
O       1.1.6.0/24 [110/65] via 1.1.3.2, 00:00:26, Serial1
```

6.18. Проверьте, что вы всё сделали правильно. На каждом компьютере выполнените команд трассировки tracert других компьютеров.

6.19. Сохраните конфигурацию.

Список используемых источников:

1. Манин А.А, Сосновский И.А. Системы коммутации. Принципы и технологии пакетной коммутации. Уч. пособие. 3е изд. Ростов-на-дону: СКФ МТУСИ, 2019. -245 с.

2. Тодд Лэммл, Шон Одом, Кевин Уоллес. CCNP. Маршрутизация. Учебное руководство. Издательство: Лори 2015 г .500 с.

2. http://linuxlearning.ooi.ru/mod/book/view.php?id=151&chapterid=192 – сайт системного администратора. Дата обращения 1.09.2019 г.