**Лабораторная работа No3  
НАСТРОЙКА АЛГОРИТМОВ МАРШРУТИЗАЦИИ В ЛОКАЛЬНЫХ ПОДСЕТЯХ**

1. **Цель работы**: обеспечить возможность выбора и настройки статических и динамических алгоритмов маршрутизации, оптимизировать сетевой трафик за счет конфигурирования эффективных маршрутов, а также проверить корректность передачи данных из разных подсетей.
2. **Общие теоретические понятия**
3. ***Динамическая маршрутизация***

Недостатком статической маршрутизации является необходимость большого объема ручной работы. Кроме того, изменения в топологии сети требуют ручной корректировки настроек. Использование протоколов динамической маршрутизации позволяет автоматически настраивать каждый маршрутизатор в соответствии с текущими маршрутами.

Для создания отношений соседства между маршрутизаторами протоколы маршрутизации позволяют обмениваться напрямую подключенными маршрутами и другими (поддерживаемыми) маршрутами. Таким образом, все маршрутизаторы обмениваются данными об обновлениях друг с другом. Кроме того, маршрутизаторы передают обновления при изменении топологии, что позволяет обнаружить потерю маршрута.

1. ***Настройка протокола маршрутизации RIP с помощью протокола RIP***

Packet Tracer предоставляет графический интерфейс, который позволяет настраивать протокол динамической маршрутизации, известный как протокол маршрутной информации (RIP). Настройка статической маршрутизации аналогична этому варианту. Кроме того, существует только одно текстовое поле, которое можно использовать для ввода сетевого адреса непосредственно подключенной сети.

Хотя можно предположить, что эта настройка похожа на настройку статических маршрутов, но не в этом случае. Настройка статического маршрута требует ввода маршрута к другим сетям, но для RIP необходимо ввести IP-адреса вашего собственного сетевого интерфейса. Вводим IP-адреса предложенных интерфейсов. Соответственно, выполняются две функции: на указанный интерфейс вводится протокол маршрутизации и разрешается распространять сетевые данные.

Ниже приведены шаги по настройке динамической маршрутизации RIP.

1. Создается топология, идентичная той, что приведена в предыдущем примере. С помощью вкладки «Конфигурация» интерфейсам роутера назначаются идентичные IP-адреса.
2. Доступ к разделу RIP можно получить с той же вкладки. Настроить динамическую маршрутизацию очень просто. Каждому маршрутизатору нужно только ввести IP-адрес своего сетевого интерфейса (рис. 3.1.).



***Рисунок 3.1. Настройка динамической маршрутизации с помощью графического интерфейса пользователя***

1. Для каждого роутера вводятся следующие сетевые IP-адреса:

**Таблица 3.1. Сетевые IP-адреса интерфейсов маршрутизаторов**

|  |  |
| --- | --- |
| ***Маршрутизатор*** | ***Сеть RIP*** |
| Р1 | 192.168.10.0 |
| 192.168.20.0 |
| Р2 | 192.168.10.0 |
| 192.168.30.0 |
| Р3 | 192.168.20.0 |
| 192.168.40.0 |
| Р4 | 192.168.30.0 |
| 192.168.40.0 |

1. После настройки топологии выполняется проверка связности с помощью обычного инструмента PDU. Тестируются два маршрутизатора с непрямым соединением, например, R1 и R4 или R2 и R3. Успешный проход указывает на то, что на каждом маршрутизаторе правильно настроена динамическая маршрутизация.
2. На следующем шаге проверяется, как ведут себя протоколы динамической маршрутизации при изменении топологии. Для этого выберите инструмент «Удалить» на общей панели инструментов и удалите связь между роутерами R1 и R2, или R1 и R3. Для выполнения теста на связность используется режим моделирования и инструмент Simple PDU. Посылки будут путешествовать по другому маршруту, что будет свидетельствовать об успешности испытания. Посылки будут путешествовать более длинным путем.

Если был выполнен шаг 5 статической маршрутизации, будет наблюдаться ошибка, так как альтернативные маршруты для каждой сети не были вручную введены в каждый маршрутизатор, чтобы предотвратить потерю соединения между маршрутизаторами. Это важная особенность динамических маршрутов.

1. ***Настройка протокола маршрутизации RIP с помощью интерфейса командной строки***

Та же топология будет настроена с помощью интерфейса командной строки. Конфигурационные команды очень просты, что можно увидеть при использовании графического интерфейса пользователя в окне Эквивалентные команды IOS. Для настройки динамической маршрутизации будет открыта вкладка CLI, в которой будут выполнены следующие шаги:

1. Для назначения IP-адресов интерфейса маршрутизатора используются те же команды, что и в примере настройки статической маршрутизации командной строки.
2. Затем вернитесь в режим глобальной конфигурации и используйте следующую команду для переключения в режим маршрутизатора RIP:

R1(config)#router rip

1. Чтобы узнать IP-адрес сети, воспользуйтесь *командой network.* Выполните следующие команды для маршрутизатора R1:

R1(config-router)#network 192.168.10.0

R1(config-router)#network 192.168.20.0

1. Настройте все маршрутизаторы одинаково. Затем для выполнения теста на связность используется обычный инструмент PDU.

Далее вы можете подробно изучить таблицу маршрутизации.

1. ***Таблица маршрутизации***

Таблица маршрутизации включает в себя список всех предпочтительных маршрутов, известных маршрутизаторам. Таблицу маршрутизации можно просмотреть двумя способами. Для одного из них используется кнопка Inspect Tool, а для другого — команда Cisco IOS *show ip route*. В них появляется таблица, состоящая из нескольких столбцов и информации. Далее вы увидите, что включено в таблицу:

R1#показать ip маршрут

C 192.168.10.0/24 подключен напрямую, FastEthernet0/0

C 192.168.20.0/24 подключен напрямую, FastEthernet0/1

R 192.168.30.0/24 [120/1] через 192.168.10.2, 00:00:13,

FastEthernet0/0

R 192.168.40.0/24 [120/1] через 192.168.20.2, 00:00:22,

FastEthernet0/1

В первом столбце описана причина, по которой он был введен в таблицу маршрутизации C - напрямую подключенная сеть, R - протокол динамической маршрутизации RIP.

Во втором столбце указана сеть назначения.

В квадратных скобках первое значение указывает на административное расстояние, показывающее приоритет протокола маршрутизации, а второе значение представляет метрическое значение протокола динамической маршрутизации. Значение метрики протокола динамической маршрутизации — это количество переходов и количество маршрутизаторов, направляющихся в сеть назначения для протокола RIP. В этом случае административное расстояние для протокола RIP равно 120, а для статического маршрута — 1.

Если маршрутизатор имеет два маршрута к одной и той же сети, статический или RIP, будет использоваться статический маршрут, поскольку административное расстояние меньше.

Адрес шлюза, который является следующим маршрутизатором, направляющимся к сети назначения, представляет собой IP-адрес, записанный после слова «via». Таймер удержания — это временная метка, записываемая в конце динамического маршрута. Кроме того, любой протокол маршрутизации отправляет сообщения с определенным интервалом, например «Таймер приветствия». Если говорить о протоколе RIP, то это 30 секунд. Если маршрутизатор не получает сообщений о маршруте в течение трех интервалов приветствия (180 с или таймер удержания), этот маршрут удаляется из таблицы маршрутизации и выполняется поиск альтернативного маршрута.

Выходной интерфейс маршрутизатора, к которому шлюз может получить доступ, находится в последнем столбце.

1. ***Распределение нагрузки***

В топологии, которая будет рассмотрена далее, возможно, что каждый маршрутизатор имеет два разных способа подключения к каждой сети назначения. Когда трафик проходит мимо маршрутизаторов, было бы полезно изучить, как они используют альтернативные пути и выполняют балансировку нагрузки.

1. **Балансировка нагрузки в протоколе RIP**

Так как в данном случае ничего менять не нужно, то сначала рассмотрим протокол RIP. Нет необходимости предпринимать какие-либо действия. RIP автоматически распределяет нагрузки, если альтернативные пути для доступа к сетям назначения имеют одинаковые метрики. В этом примере мы будем использовать тип интерфейса loopback в качестве сети назначения. Виртуальный интерфейс loopback использует IP-адрес и ведет себя как реальный интерфейс. Добавьте этот интерфейс в маршрутизатор R4, выполнив следующие действия в той же топологии:

1. К сожалению, графический интерфейс не может этого сделать, поэтому вы будете использовать интерфейс командной строки для добавления этого интерфейса в свой маршрутизатор (CLI) и введите следующие команды:

R4(config)#interface loopback 0

R4(config-if)#ip адрес 192.168.100.1 255.255.255.0

1. Процесс маршрутизации должен быть запущен на интерфейсе обратной связи на том же маршрутизаторе. Введите сетевой IP-адрес интерфейса обратной связи после переключения в режим глобальной конфигурации. Информация о маршруте будет отправлена автоматически:

R4(config)#router rip  
 R4(router-if)#network 192.168.100.0

1. Используйте для тестирования "Комплекс", БРП, договоритесь о временном интервале в 2 с.



***Рисунок 3.2. Использование инструмента Advanced PDU***

1. В режиме симуляции определяется, что первый пакет будет следовать по маршруту R1-R2-R4, а второй пакет — по маршруту R1-R3-R4.

Кроме того, изучив таблицу маршрутизации, проверяется корректность работы механизма распределения трафика:

Router>show ip route

R 192.168.30.0/24 [120/1] через 192.168.10.2, 00:00:12,FastEthernet0/0

R 192.168.40.0/24 [120/1] через 192.168.20.2, 00:00:14,FastEthernet0/1

Р 192.168.100.0/24

[120/2] через 192.168.20.2, 00:00:08, FastEthernet0/1

[120/2] через 192.168.10.2, 00:00:08, FastEthernet0/0

Для лучшего понимания отображаемая таблица маршрутов содержит только маршруты RIP. Поскольку 192.168.100.0/24 имеет два входящих порта, трафик будет распределяться между ними.

1. **Балансировка нагрузки для статических маршрутов**

Статическая маршрутизация требует дополнительных корректировок для балансировки нагрузки. Распределение IP-адресов всех физических интерфейсов, а также интерфейсов обратной связи происходит, как было указано ранее. Чтобы настроить балансировку нагрузки, необходимо выполнить следующие действия:

1. Настройте маршрут для маршрутизаторов R2 и R3 для доступа к интерфейсу orbaskin маршрутизатора R4:

R2(config)#ip маршрут 192.168.100.0 255.255.255.0 192.168.30.2R3(config)#ip маршрут 192.168.100.0 255.255.0 192.168.40.2

1. На маршрутизаторе R1 настроены два маршрута к 192.168.100.0/24. Маршрутизатору необходимо объяснить, что есть два способа получить доступ к интерфейсу обратной связи маршрутизатора R4. Для этого используются следующие команды:

R1(config)#ip road 192.168.100.0 255.255.255.0 192.168.10.2R1(config)#ip road 192.168.100.0 255.255.0 192.168.20.2

1. Включите "Complex PDU" как в статической маршрутизации и "Complex PDU", как в предыдущем разделе, чтобы проверить эффективность механизма распределения для статической маршрутизации.

После того, как эта конфигурация была сделана, в таблице маршрутизации мы можем наблюдать два маршрута к 192.168.100.0/24, аналогичные маршрутам RIP.

1. ***Протокол шлюза extern BGP (протокол пограничного шлюза)***

Интернет – это большая сеть, состоящая из множества других сетей. Каждая сеть использует протоколы маршрутизации для определения маршрутов к другим сетям. Такие протоколы , как Enhanced Interior Gateway Routing Protocol (EIGRP), RIP (Routing Information Protocol) и OSPF (Open Shortest Path First), хорошо работают для большинства сетей. Однако из-за своего небольшого размера они не подходят для составных сетей, таких как Интернет, из-за недостаточной масштабируемости и отсутствия достаточного административного разделения. Интернет-провайдеры (ISP) и крупные предприятия используют протокол пограничного шлюза (BGP) для информирования о маршрутах между ними.

Протокол BGP и его характеристики будут рассмотрены в сравнении с другими протоколами. Кроме того, мы рассмотрим команды Cisco IOS, используемые при настройке BGP, и способы их настройки.

1. **Что такое BGP?**

При использовании обмена маршрутной информацией между несколькими автономными системами (AS) BGP является высокоэффективным протоколом маршрутизации. Это определение поднимает еще один вопрос: что значит быть автономной областью? Автономная зона — это набор префиксов IP-адресов или IP-сетей, которые контролируются одним администратором. Компании или интернет-провайдеры могут быть сетевыми операторами, которые осуществляют надзор за автономной областью.

Каждая автономная зона имеет номер, который называется ASN (номер автономной системы). Публичные номера автономных территорий присваиваются региональными интернет-реестрами (RIRs), которым это право делегировано Администрацией адресного пространства Интернет (IANA).

Конфигурация BGP в значительной степени основана на том, как организация подключается к поставщику услуг Интернета. Существует четыре возможных типа подключения:

1. Единый вход – самый простой вариант конструкции, обеспечивающий единый канал связи с одним поставщиком услуг Интернета (ISP) (рис. 3.3). Нет никакой гарантии, что это соединение обеспечивает резервирование или отказоустойчивость.
2. Двойное соединение или две части. Кроме того, в данной схеме подключения используется один провайдер, но допускается использование для него двух и более каналов (рисунок 3.4). Это повышает доверие в случае проблем с каналом.



***Рисунок 3.3. Однокомнатный***



***Рисунок 3.4. Опции с двойным домом***

1. Единое многосетевое соединение. В этом случае есть несколько интернет-провайдеров, и каждый из них имеет подключенный канал (рисунок 3.5).
2. Двойное многогнездное соединение. Схемы подключения обеспечивают высочайший уровень доступности и надежности. В этом случае имеется два и более провайдера, и к каждому из них подключаются два и более канала связи (рисунок 3.6).



***Рисунок 3.5. Варианты подключения с одним многосетевым подключением***



***Рисунок 3.6. Двойные многоквартирные опции***

BGP может не соответствовать предложенным параметрам топологии. В некоторых случаях с одним подключением лучше иметь только один статический маршрут по умолчанию к провайдеру и еще один статический маршрут от провайдера к сети компании. Но реализация BGP в варианте с многосетевым подключением обеспечивает более эффективную маршрутизацию.

Существует два типа BGP:

1. Внешние BGP (eBGP);

2. Внутренний BGP (iBGP).

1. **Внешний BGP**

Для обмена маршрутами между автономными зонами используется тип протокола BGP. eBGP, который имеет административное расстояние 20. По умолчанию TTL (Time-to-Live) имеет значение 1 при отправке пакетов обновления в eBGP. Это означает, что пакеты будут получать только напрямую подключенный маршрутизатор BGP. С помощью правильной команды это поведение можно изменить. Маршрутизатор eBGP уведомляет обо всех маршрутах, поддерживаемых маршрутизаторами eBGP и iBGP. Сосед eBGP указывает маршрут в следующем поле маршрутизатора объявленного маршрута.

1. **Внутренний BGP**

Для обмена маршрутами в пределах автономной зоны используется тип протокола BGP. iBGP, который имеет административное расстояние 200. Обновления iBGP не ограничивают значение TTL. Маршруты iBGP не обмениваются данными, которые были изучены другими маршрутизаторами iBGP. Этот механизм предотвращает образование петель маршрута в пределах отдельной области. Маршрутизатор iBGP оставляет адрес следующего маршрутизатора без изменений в поле адреса в объявлениях о маршруте. С помощью соответствующих команд это поведение также можно изменить. Cisco Packet Tracer не поддерживает iBGP.

1. ***BGP как протокол динамической маршрутизации***

Несмотря на то, что BGP и другие протоколы динамической маршрутизации работают одинаково, между протоколами динамической маршрутизации есть некоторые различия. Протоколы IGP (Interior Gateway Protocols), такие как RIP, OSPF и EIGRP, имеют расширенные протоколы маршрутизации. IP-адрес сети определяется сетевым объявлением, которое создается путем настройки протокола маршрутизации. В процессе объявления о маршрутизации участвуют интерфейсы, IP-адреса которых находятся в пределах диапазона рекламируемой сети. Через эти интерфейсы показываются или распространяются рекламные объявления. Чтобы это работало, два соседних маршрутизатора должны иметь прямое соединение друг с другом и на них должны выполняться процессы протокола Internal Gateway Protocol (IGP). Количество переходов, пропускная способность, время задержки и другие параметры используются протоколами интерфейса внутреннего протокола (IGP) для выбора оптимального пути.

В отличие от этого, BGP не использует идею интерфейсов. Весь маршрутизатор работает в автономной зоне. Соседи BGP должны быть назначены вручную с помощью команды neighborhood, так как они не обнаруживаются автоматически. Далее сообщения BGP передаются в виде набора односторонних пакетов. BGP основан на протоколе TCP и прослушивает порт 179. Соседей можно найти в нескольких шагах от них, и они не обязательно должны быть рядом. Значение времени жизни по умолчанию для сообщения GP равно 1. Это значение необходимо корректировать в сторону увеличения, если точка обмена не подключена напрямую. Принципы, определяющие выбор наилучшего маршрута BGP, отличаются от принципов протоколов Inside Gateway Protocol (IGP). Атрибуты точки доступа или атрибуты пути включают достижимость следующего прыжка, вес маршрута и путь к автономной зоне (AS\_PATH — это количество автономных зон, которые являются частью пути к сети назначения).

Кроме того, при работе по протоколам Inside Gateway (IGP) BGP предназначен для обработки сотен тысяч IP-маршрутов, что требует большого количества ресурсов.

1. ***Настройка BGP в трассировщике пакетов***

Во-первых, в нем рассматриваются команды, используемые в BGP:

Маршрутизатор BGP <ASN>

Например:

R1(config)# маршрутизатор bgp 120

Эта команда запускает BGP-процесс маршрутизатора и переводит его в режим настройки маршрута. Номер автономного округа ASN может быть от 1 до 65535.

Процесс BGP запрашивает назначение идентификатора маршрутизатора. Методы выбора идентификатора маршрутизатора по умолчанию используются BGP в следующем порядке приоритета:

1. Он был установлен вручную. В режиме настройки маршрута для настройки идентификатора используется функция bgp router-id.
2. Максимальное значение интерфейса обратной связи. Когда в этом сценарии инициируется процесс BGP, идентификатор маршрутизатора становится самым большим IP-адресом любого доступного интерфейса обратной связи. Интерфейс замыкания на себя становится доступным, когда процесс BGP уже начался.
3. Максимальное значение другого интерфейса. Когда начинается процесс BGP, идентификатор маршрутизатора выбирается как самый большой IP-адрес, настроенный на любом доступном интерфейсе, кроме интерфейса обратной связи.

Идентификатор маршрутизатора может быть задан явно с помощью следующей команды:

bgp router-id X.X.X.X

В качестве примера для присвоения идентификатора маршрутизатора используется следующая команда:

R1(config-router)#bgp router-id 1.1.1.1

Для настройки объединенного BGP используется следующая команда:

R1(config-router)#neighbor X.X.X.X remote-as <asn>

Например:

R1(config-router)#neighbor 10.0.0.2 remote-as 130

Здесь значение номера автономной зоны, введенное после опции remote-as, должно соответствовать автономной зоне, подключенной к соседнему маршрутизатору. Таким образом, существует различие между внешним протоколом (eBGP) и внутренним протоколом (iBGP).

Для внешнего протокола BGP будут использоваться следующие команды:

R1(конфигурация)#router BGP 120

R1(config-router)#neighbor 10.0.0.2 remote-as 130

Для внутреннего протокола BGP будет использоваться следующая форма:

R1(конфигурация)#router BGP 120

R1(config-router)#neighbor 192.168.1.20 remote-as 120

Как уже упоминалось, внутренний протокол BGP не изменяет поле следующего маршрутизатора при изменении маршрутной информации в пределах автономной зоны. Это может быть проблемой, так как перераспределение может быть недоступно через протоколы PGI. Это происходит потому, что протоколы IGP отклоняют такие маршруты из-за неверного адреса следующего маршрутизатора. IP-адрес следующего роутера определяется командой:

R1(config-router)#neighbor X.X.X.X next-hop-self

Протокол BGP также имеет сетевую команду. Это используется для указания конкретного маршрута, который должен быть объявлен через протокол BGP, и такой маршрут должен существовать в таблице маршрутизации:

R1(config-router)#network 10.20.20.0 маска 255.255.255.0

Если выбран только один маршрут класса, опцию маски можно пропустить.

Трассировщик пакетов не может принимать все команды протокола BGP. Таким образом, в последующих примерах будут использоваться только ранее упомянутые команды.

В примере на рисунке 3.7 будет использоваться только одна многосетевая топология, поскольку Packet Tracer несовместим с iBGP.



***Рисунок 3.7. Пример конфигурации BGP в трассировщике пакетов***

В этой сети есть четыре маршрутизатора, два из которых принадлежат отдельной компании, а два других — разным интернет-провайдерам. Маршрутизаторы компании имеют интерфейсы обратной связи, настроенные с помощью IP-адресов. Это проиллюстрирует, как таблица маршрутизации включает маршруты, полученные по протоколу BGP (таблица 3.2).

**Таблица 3.2. IP-адреса интерфейсов маршрутизатора**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Устройство*** | ***Интерфейс*** | ***IP-адрес*** | ***Маска*** |
| Предприятие 1 | Loopback0 | 20.30.0.1 | 255.255.0.0 |
| FastEthernet0/0 | 10.0.0.1 | 255.255.255.255 |
| Технология FastEthernet1/0 | 10.0.0.9 | 255.255.255.255 |
| Предприятие 2 | Loopback0 | 40.30.0.1 | 255.255.0.0 |
| FastEthernet0/0 | 10.0.0.5 | 255.255.255.255 |
| Технология FastEthernet1/0 | 10.0.0.13 | 255.255.255.255 |
| ИСП1 | FastEthernet0/0 | 10.0.0.2 | 255.255.255.255 |
| Технология FastEthernet1/0 | 10.0.0.6 | 255.255.255.255 |
| ИСП2 | FastEthernet0/0 | 10.0.0.10 | 255.255.255.255 |
| Технология FastEthernet1/0 | 10.0.0.14 | 255.255.255.255 |

Чтобы настроить протокол BGP в этой топологии, необходимо выполнить следующие действия:

1. Настройка начинается с производственных маршрутизаторов:

Enterprise1(config)#router bgp 10200

Enterprise1(config-router)#bgp router-id 0.0.0.1

Enterprise1(config-router)#neighbor 10.0.0.2 remote-as 30200

Enterprise1(config-router)#neighbor 10.0.0.10 remote-as 50300

Enterprise1(config-router)#network маска 20.30.0.0 255.0.0

Enterprise2(config)#router bgp 3400

Enterprise2(config-router)#bgp router-id 0.0.0.2

Enterprise2(config-router)#neighbor 10.0.0.6 remote-as 30200

Enterprise2(config-router)#neighbor 10.0.0.14 remote-as 50300

Enterprise2(config-router)#network маска 40.30.0.0

255.255.0.0

1. Далее настройте маршрутизаторы провайдера:

ISP1(config)#router bgp 30200ISP1(config-router)#bgp router-id 1.1.1ISP1(config-router)#neighbor 10.0.0.1 remote-as 10200ISP1(config-router)#neighbor 10.0.0.5 remote-as 3400ISP2(config)#router bgp 50300ISP2(config-router)#bgp router-id 2.2.2ISP2(config-router)#neighbor 10.0.0.9 remote-as 10200ISP2(config-router)#neighbor 10.0.0.13 remote-as 3400

1. Когда конфигурация выполнена правильно, в консоли появятся сообщения о настройке окрестности:

%BGP-5-ADJCHANGE: сосед 10.0.0.9 вверх

%BGP-5-ADJCHANGE: сосед 10.0.0.13 вверх

1. Проверьте связь с интерфейсом обратной связи маршрутизатора Enterprise2 от маршрутизатора Enterprise1:

Enterprise1>ping 40.30.0.1

Введите escape-последовательность для прерывания.

Отправка 5 100-байтовых ICMP Echos на 40.30.0.1, тайм-аут равен 2

товары второго сорта:

.....

Вероятность успеха составляет 0 процентов (0/5)

1. Отмечается, что попытка тестирования связности не удалась.

Это связано с тем, что пакет запроса ICMP использует адрес 10.0.0.1 в качестве отправителя, поэтому когда пакет получен маршрутизатором Enterprise2, он не может отправить ответ ICMP, потому что у него нет адреса, маршрута к сети 10.0.0.0.0/30. Для выхода в сеть, указанную на Enterprise1, будет использоваться расширенная версия утилиты ping, в которой интерфейс вывода может быть указан явно:

Enterprise1#ping

Протокол [ip]:

Целевой IP-адрес: 40.30.0.1

Количество повторов [5]:

Размер дейтаграммы [100]:

Таймаут в секундах [2]:

Расширенные команды [n]: y

Адрес источника или интерфейса: 20.30.0.1

Тип услуги [0]:

Установить бит DF в заголовке IP? [нет]:

Проверить данные ответов? [нет]:

Шаблон данных [0xABCD]:

Свободный, Строгий, Запись, Временная метка, Подробный[none]:

Диапазон размеров развертки [n]:

Введите escape-последовательность для прерывания.

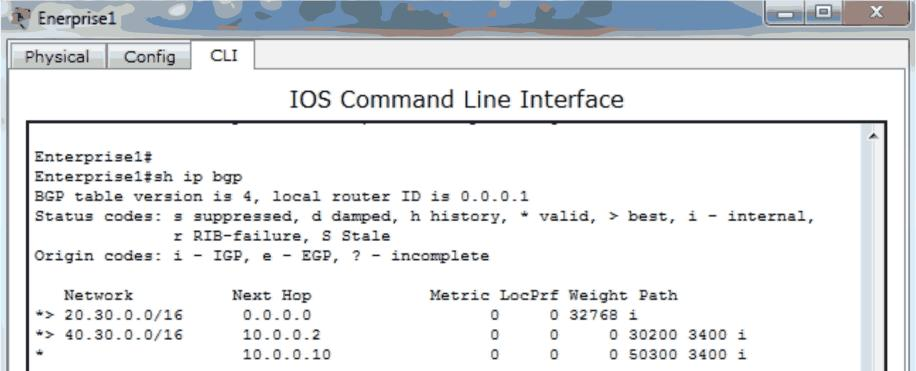
При отправке 5 100-байтовых ICMP Echos на 40.30.0.1, время ожидания составляет 2 секунды:

Пакет отправлен с исходным адресом 20.30.0.1

!!!!!

Вероятность успеха составляет 100 процентов (5/5), минимальное/среднее/максимальное время приема-передачи = 0/0/1 мс

1. Таким образом, eBGP был успешно настроен. Затем изучите маршруты BGP в таблице маршрутизации.



***Рисунок 3.8. Результат использования команды sh ip bgp***

1. **Порядок выполнения лабораторных работ**
2. Спроектируйте подсети, показанные на рисунке 3.9.
3. Назначьте IP-адрес и маску подсети для каждой подсети.
4. Проверьте соединения между хостами с помощью *команды ping.*
5. Используя алгоритмы динамической маршрутизации, задайте необходимые команды.
6. Использование команды *show ip route* для проверки *ip-сетей*, назначенных каждому порту.
7. Проверьте соединение между подсетями с помощью команды *ping*.
8. **Проведение лабораторных работ**

Требуется проектирование подсетки на основе топологии, показанной на рисунке 3.9. Локальная сеть будет сегментирована на подсети для оптимизации трафика и повышения безопасности. Каждый маршрутизатор будет отвечать за управление определенными подсетями в сети. Коммутаторы будут подключать компьютеры к соответствующим подсетям, обеспечивая эффективное подключение и связь. При проектировании подсетей будет учитываться количество компьютеров, тип трафика и требования к безопасности, характерные для каждой подсети.

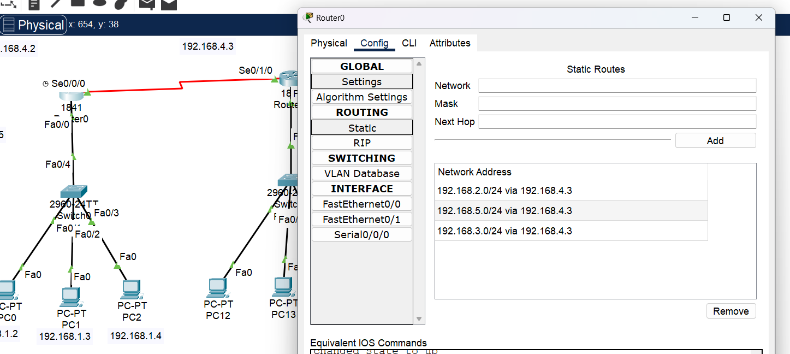


***Рисунок 3.9. Локальная сеть, состоящая из 3 маршрутизаторов, 3 коммутаторов и 9 компьютеров***

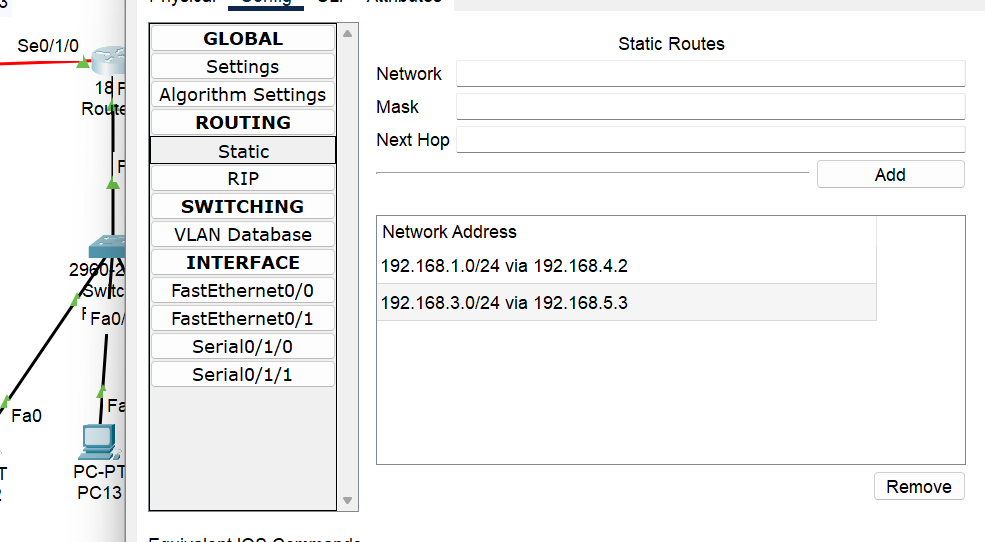
Сеть будет разделена на 3 отдельные подсети с определенной IP-адресацией и настройками масок. Подсеть 1 будет использовать диапазон 192.168.1.0/24 с маской 255.255.255.0, подсеть 2 будет определена как 192.168.2.0/24 и маска 255.255.0, а подсеть 3 будет включать адреса из 192.168.3.0/24 с маской 255.255.255.0.

Чтобы облегчить связь между подсетями, на 3 маршрутизаторах будут настроены статические маршруты. Первый маршрутизатор будет содержать статические маршруты к подсетям 2, 3 и 4, используя исходящий интерфейс 192.168.4.3. Второй маршрутизатор будет настроен на статические маршруты к подсетям 1 и 3, имея в качестве исходящего интерфейса 192.168.4.2. Третий маршрутизатор завершит схему настройкой статических маршрутов в подсети 1, 2 и 4, с исходящим интерфейсом 192.168.5.2.

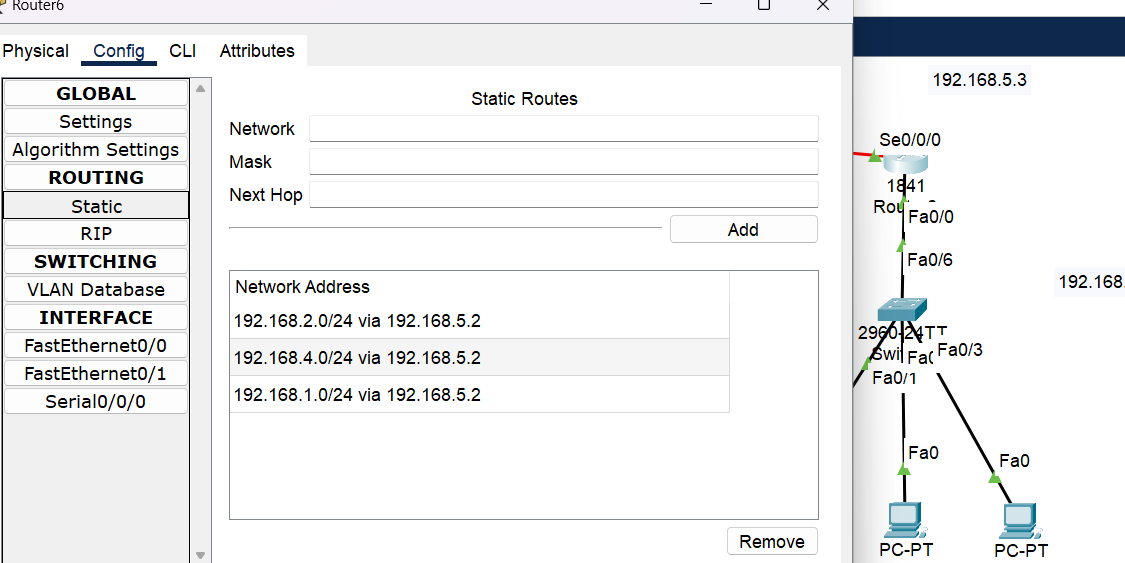
Коммутаторы будут играть ключевую роль в подключении компьютеров к соответствующим подсетям, обеспечивая эффективную связь между устройствами в сети. Сегментация сети на подсети позволит оптимизировать трафик и значительно повысить уровень безопасности за счет ограничения доступа к определенным сегментам.



***Рисунок 3.10. Настройка статической маршрутизации на первом маршрутизаторе***



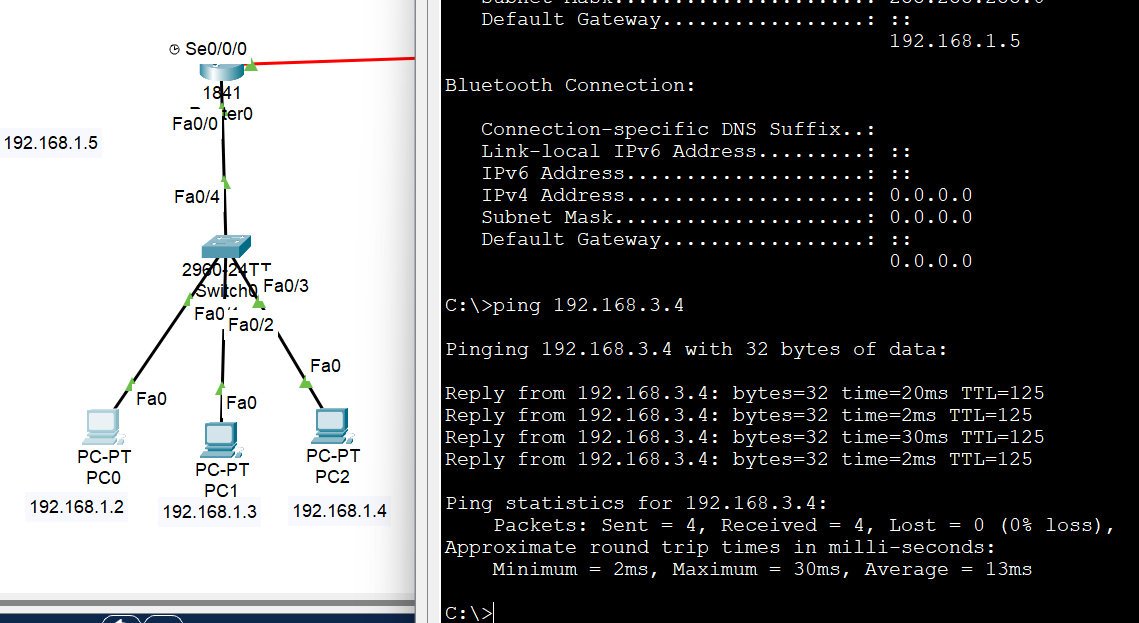
***Рисунок 3.11. Настройка статической маршрутизации на второй маршрутизатор***



***Рисунок 3.12. Настройка статической маршрутизации на третий маршрутизатор***

После того, как сеть настроена, команда ping используется для проверки наличия соединения между устройствами. Пакеты данных отправляются на маршрутизаторы и компьютеры для проверки их доступности. Команда show ip route отображает таблицу маршрутизации маршрутизатора, предоставляющую информацию об известных IP-сетях и маршрутах к ним. Предварительно настроенные статические маршруты проверяются на корректность.

Пакеты ping отправляются между компьютерами в разных подсетях, чтобы проверить, могут ли они взаимодействовать. Это подтверждает правильность сегментации сети. Проверьте соединение между первым компьютером (подсеть 1) и последним компьютером (подсеть 3). Пинг отправляется с первого компьютера на IP-адрес последнего. Успешное *выполнение пинга* демонстрирует правильное функционирование сети. Совместное использование вышеуказанных методов позволяет получить полную картину состояния сети, что позволяет оперативно выявлять и устранять проблемы с подключением или маршрутизацией.



***Рисунок 3.13. Соединение первого компьютера с последним по***

***Команда Ping***

1. **Содержание отчета**
2. Знакомство:
3. Цель и задачи лабораторной работы.
4. Общее описание локальной сети и необходимость использования алгоритмов маршрутизации.
5. Описание локальной сети:
6. Представление топологии сети: маршрутизаторы, коммутаторы, компьютеры и т.д.
7. Первичная настройка сетевых устройств: настройка IP-адресов, настройка сетевых интерфейсов и т.д.
8. Используемые алгоритмы маршрутизации:
9. Объяснение основных понятий и принципов алгоритмов маршрутизации: статический, RIP, OSPF и т.д.
10. Описание того, как работает каждый алгоритм в рамках проектируемой локальной сети.
11. Настройка алгоритмов маршрутизации:
12. Настройка и настройка алгоритмов маршрутизации на устройствах в сети.
13. Описание конкретных шагов, необходимых для каждого алгоритма.
14. Проверка работы алгоритмов маршрутизации:
15. Использование определенных команд для проверки состояния и работы алгоритмов маршрутизации на устройствах в сети.
16. Тестирование связности между разными подсетями с использованием настроенных алгоритмов маршрутизации.
17. Заключение:
18. Результаты, полученные в ходе лабораторных работ.
19. Наблюдения и выводы относительно эффективности и производительности используемых алгоритмов маршрутизации.
20. Библиография:
21. Библиографические источники, используемые для понимания концепций и принципов алгоритмов маршрутизации.
22. Приложения:
23. При необходимости сделайте скриншоты настроек и взаимодействий в лаборатории.

**Контрольные вопросы**

1. Определите концепцию динамической маршрутизации и объясните ее преимущества по сравнению со статической маршрутизацией.
2. Представьте два распространенных протокола динамической маршрутизации и упомяните основные различия между ними.
3. Приведем пример настройки RIP через CLI (Command Line Interface) на реальном или виртуальном роутере, указав используемые команды и настраиваемые параметры.
4. Объясните, что такое таблица маршрутизации и каковы ее ключевые элементы.
5. Опишите, как маршрутизатор использует таблицу маршрутизации для маршрутизации сетевого трафика.
6. Определите концепцию балансировки нагрузки в контексте протокола RIP и объясните ее преимущества.
7. Приведите пример настройки балансировки нагрузки с помощью RIP на виртуальном маршрутизаторе, упомянув доступные варианты и их влияние.
8. Определите протокол BGP (Border Gateway Protocol) и упомяните его роль в Интернете.
9. Объясните различия между внешним и внутренним BGP, приведя примеры применимости для каждого из них.
10. Представьте BGP как протокол динамической маршрутизации и сравните его с RIP, выделив такие аспекты, как масштабируемость и конвергенция.

**Библиография**

1. Дойл, Д., и Кэрролл, Д. (2016). Маршрутизация TCP/IP. Пресса Cisco.
2. Куросе, Д. Ф., и Росс, К. В. (2017). Компьютерные сети: нисходящий подход. Пирсон.
3. Эггерт, Л., и Фриче, У. (2014). BGP: Полное руководство. О'Рейли Медиа.
4. Ламмле, Тодд. Протоколы и концепции маршрутизации. CCIE Routing & Switching Certification Guide, 2-е изд., John Wiley & Sons, 2016.
5. Сетевая академия Cisco. https://www.netacad.com/
6. Microsoft Learn. https://docs.microsoft.com/en-us/learn/
7. Уроки по очкам. https://www.tutorialspoint.com/