**ЛАБА 1**

* *Показать конфигурацию коммутатора и объяснить что обозначает параметр, который настраивался в рамках лабороторной работы*
* *Как происходит коммутация и при чём тут CAM Table (mac address table)?*

Коммутация — это процесс соединения различных абонентов коммуникационной сети через транзитные узлы.

<https://pc.ru/docs/network/switching-methods>

* *Теоретический вопрос на понимание технологий VLAN, DHCP, VTP, Sub-Interface:*
  + *Что такое VLAN*

VLAN (Virtual Local Area Network) — технология, логически разделяющая и изолирующая одну или несколько физических локальных сетей на несколько виртуальных широковещательных доменов. При создании VLAN’а хосты физической сети, объединенные общей функцией, выделяются в логическую виртуальную сеть, при этом их физическое местонахождение не имеет значения.

* + *Сколько VLAN бывает*

Внутрь фрейма после Source MAC-адреса добавляется ещё одно поле, очень грубо говоря, содержащее номер VLAN’а. Длина, выделенная для номера влана равна 12 битам, это означает, что максимальное число вланов 4096.

* + *Для чего используется VLAN?*

Расширить или уменьшить диапазон IP-адресов в локальной сети. Если у нас очень большая сеть, мы можем уменьшить количество доступных IP-адресов, чтобы упростить управление ими.

Оптимизация сети: очень большая сеть может иметь много широковещательного трафика, это значительно замедляет работу сети.

Улучшить организацию всей сети: мы можем разделить очень большую сеть на более мелкие подсети, чтобы использовать каждую подсеть для определенной аудитории. Например, мы могли бы создать подсеть для управления, администрирования, отделов продаж, подсеть для гостей и т. Д.

Повышенная безопасность и контроль дорожного движения: разделив на небольшие подсети, мы можем адекватно сегментировать нашу сеть на VLAN (уровень 2) и использовать различную IP-адресацию (уровень 3), чтобы разрешить или запретить трафик между разными компьютерами. Благодаря разделению на подсети или подсети сетевые администраторы могут более легко управлять всем входящим и исходящим трафиком.

* + *Какие версии протокола VTP существуют? Их различия. Аналоги VTP других произволителей*

VTP - проприетарный протокол Cisco применяемый для обмена информацией о vlan между коммутаторами. Упрощает работу системного администратора тем, что помогает согласовывать vlan-ы на коммутаторах тем самым предотвращая ошибки конфигурации "вручную", и динамически оповещать все коммутаторы управляемого домена об изменениях в конфигурации.

Альтернативный протокол, используемый другими вендорами - GVRP.

Существует три версии протокола VTP - 1, 2, 3. Для успешного обмена информацией все коммутаторы должны использовать одинаковую версию VTP. Сообщения VTP инкапсулируются во фреймы 802.1Q. Для указания версии vtp используется команда vtp version number.

VTP имеет три версии:  **VTPv1, VTPv2 и VTPv3** . Позвольте мне поделиться некоторыми идеями, которые покажут вам функции и возможности версий VTP.

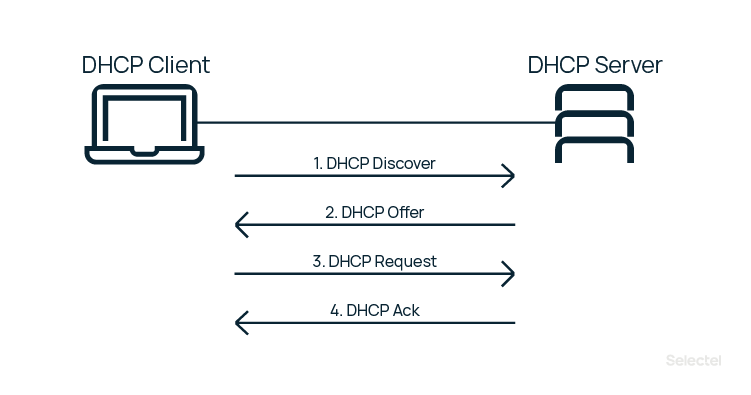
* VTPv1 и VTPv2 поддерживают VLAN от 1 до 1000, тогда как VTPv3 поддерживает от VLAN 1 до 4096.
* VLAN расширенного диапазона поддерживаются только в VTP версии 3. При преобразовании VTP версии 3 в VTP версии 2 VLAN в диапазоне от 1006 до 4094 удаляются из-под контроля VTP.
* VTP версии 3 поддерживает распространение любой базы данных в домене, позволяя настроить первичный и вторичный серверы.
* VTP версии 3 не поддерживается на портах частной сети VLAN (PVLAN).
* Перед настройкой VTP версии 3 необходимо убедиться, что команда spanning-tree extend system-id включена.
* Если для использования VTP недостаточно DRAM, режим VTP меняется на прозрачный.

В версии 3 VTP добавился новый режим работы и изменились некоторые режимы работы, по сравнению с предыдущими версиями

* + *Что такое VTP Prunning?*

VPT pruning - режим используемый для фильтрации фреймов. При его включении, коммутатор получая фреймы для какого то конкретного vlan-а, будет отправлять их только на те trunk-интерфейсы которые ведут к нужному vlan-у. На все остальные фрейм отправлятся не будет.

* + *Виды сообщений DHCP (DORA и остальные)*



* *Назовите любые 7 параметров, передаваемых DHCP сервером*

DHCP — протокол автоматизации назначения IP-адреса клиенту. Передаёт также маску подсети, GW, DNS. (Время аренды IP-адреса, в секундах; Часовой пояс; Имя домена)

* *Что такое широковещательный трафик? Механизм широковещания.*

В компьютерных сетях широковещательный трафик - это тип данных, отправляемых на все компьютеры и устройства в сети или подсети. Он используется в ситуациях, когда необходимо достичь всех возможных сетевых назначений или, когда адрес определенного компьютера неизвестен.

* *Что такое широковещательный домен?*

Широковещательный домен — группа доменов коллизий, соединенных с помощью устройств второго уровня. Это - логический участок компьютерной сети, в котором каждое устройство может передавать данные любому другому устройству непосредственно, без использования маршрутизатора.

* *Что такое MTU?*

В компьютерных сетях термин maximum transmission unit означает максимальный размер полезного блока данных одного пакета, который может быть передан протоколом без фрагментации.

* *Практика VLAN:*
  + *Как добавить еще один VLAN?*
  + *Как удалить VLAN*
  + *Как изменить сервер VTP на другой коммутатор*
  + *Как добавить и настроить новый sub-interface*
  + *Как изменить tag VLAN*
* *Практика DHCP:*
  + *Как добавить область DHCP*
  + *Как изменить область раздаваемых DHCP адресов*
* *Показать сетевые настройки (стека TCP/IP) VPC*

VLAN Trunk Protocol – протокол компании Cisco (работает только на cisco-устройствах), предназначенный для динамического распространения базы VLAN-ов на сетевых устройствах.

На коммутаторе VTP может работать в трёх режимах:

* **Server** (режим по умолчанию):
  + Можно создавать, изменять и удалять VLAN из командной строки коммутатора,
  + Генерирует объявления VTP и передает объявления от других коммутаторов,
  + Может обновлять свою базу данных VLAN при получении информации не только от других VTP серверов, но и от других VTP клиентов в одном домене, с более высоким номером ревизии.
  + Сохраняет информацию о настройках VLAN в файле vlan.dat во flash.
* **Client**:
  + Нельзя создавать, изменять и удалять VLAN из командной строки коммутатора,
  + Передает объявления от других коммутаторов,
  + Синхронизирует свою базу данных VLAN при получении информации VTP,
  + Сохраняет информацию о настройках VLAN в файле vlan.dat во flash.
* **Transparent**:
  + Можно создавать, изменять и удалять VLAN из командной строки коммутатора, но только для локального коммутатора,
  + Не генерирует объявления VTP,
  + Передает объявления от других коммутаторов,
  + Не обновляет свою базу данных VLAN при получении информации по VTP,
  + Сохраняет информацию о настройках VLAN в NVRAM,
  + Всегда использует configuration revision number 0.

**В версии 3 VTP** добавился новый режим работы и изменились некоторые режимы работы, по сравнению с предыдущими версиями:

* **Server**:
  + Добавилась поддержка Private VLAN
  + Могут анонсироваться VLAN из расширенного диапазона
* **Client**:
  + Настройки VLAN сохраняются в NVRAM и в режиме клиента
  + Добавилась поддержка Private VLAN
  + Могут анонсироваться VLAN из расширенного диапазона
* **Transparent**:
  + без изменений
* **Off**:
  + Новый режим работы VTP, который добавился в 3 версии.
  + Не передает объявления VTP.
  + В остальном аналогичен режиму Transparent

Единица передачи информации на уровне л2 – фрэйм у л3 – ип пакет

**ЛАБА 2**

1. *Объяснить принципы статической маршрутизации.*

Статическая маршрутизация осуществляется на основе таблиц маршрутизации, задаваемых администратором.

1. *Команда ip route. Что делает, какие варианты задания маршрута существуют.*
2. *Таблица маршрутов. Записи и типы маршрутов (S/L/C).*
3. *Чем коммутатор отличается от роутера?*

коммутатор осуществляет связь между устройствами только одной сети, в то время как маршрутизатор может связывать несколько сетей;

для маршрутизатора можно настроить правила передачи данных;

коммутатор не получится подключить к интернету;

коммутатор использует только LAN-порты, а в маршрутизаторе присутствует как минимум один WAN-порт, обеспечивающий связь с глобальной сетью.

1. *Какие аргументы принимает команда ip route?*

Router(config)#ip route <distanation-network> <mask> <next-hop>

* distanation-network - IP-адрес, до которой прописывается маршрут.
* mask - маска хоста или подсети, до которой прописывается маршрут.
* next-hop - IP-адрес шлюза, через который прописывается маршрут

1. *Что такое дефолтный маршрут?*

Чтобы направить пакеты, адресованные в сети, которые явно не указаны в таблице маршрутизации используется маршрут по умолчанию (Default route). Маршруты по умолчанию доступны в топологиях, где не желательно изучение более специфичных сетей, как в случае, конечных тупиковых сетей (stub network) или когда количество системных ресурсов ограничено, например нет достаточно оперативной памяти, чтобы принять все маршруты, которые существуют в мире.

1. *Для чего нужна маска подсети?*

Маска подсети играет фундаментальную роль при разбиении на подсети, потому что она сообщает нам, какие биты принадлежат части сети, а какие - части хостов. Маска подсети определяет сетевой IP-адрес, диапазон IP адресов для хостов, а также широковещательный IP-адрес. Маска подсети может быть выражена в двоичном формате, в десятичном формате с точками в виде IP-адреса, а также в нотации CIDR. Обозначение CIDR - это в основном число 1, которое мы имеем слева направо в маске подсети в двоичной записи

1. *Как узнать Network и Broadcast адрес в подсети?*
2. *Что такое ARP?*

ARP (англ. Address Resolution Protocol — протокол определения адреса) — протокол в компьютерных сетях, предназначенный для определения MAC-адреса по IP-адресу другого компьютера. На каждом интерфейсе есть своя арп таблица!

1. *Покажи Таблицу маршрутизации*

Show ip route

1. *Принцип работы трассировки*

Так вот, суть трассировки в том, что отправляется один пакет с временем жизни (TTL), установленным на единицу — первый шлюз уменьшает значение на единицу, смотрит, что счётчик стал равен нулю, никуда не отправляет этот пакет, зато нам отправляет ответ, что пакет «умер». Мы и так знаем, что пакет умер — из этого ответа нас интересует только IP адрес шлюза, где с пакетом случилось это несчастье. Затем отправляется пакет со счётчиком установленным на 2 — пакет проходит первый шлюз (его IP мы уже знаем), но несчастье (счётчик достигает нуля) с ним случается уже на втором шлюзе — мы получаем ICMP ответ с IP этого шлюза. Затем отправляется следующий пакет и т. д., пока не будут определены все узлы до нужного нам сетевого хоста.

1. *Что такое TTL?*

Пересылаемые сетевые пакеты состоят из двух областей: заголовки и данные. В заголовках находится разная информация, например, IP адреса пункта отправки и пункта назначения, порты отправки и назначения, тип пакета, контрольная сумма пакета и прочее. Среди полей заголовка, у IP протокола есть такое поле как time to live (TTL) — время жизни пакета. Это счётчик с числом, которое уменьшается на единицу каждый раз, когда пакет проходит новый узел. Этот счётчик сделан для того, чтобы проблемный пакет (например, при ошибке, повлекшей закольцованный маршрут) не путешествовал по сети бесконечно. То есть любой пакет пройдя определённое количество узлов в конце-концов достигнет точки назначения или будет отброшен одним из узлов сети, когда закончится «время жизни».

Когда счётчик TTL становится равным нулю, очередной шлюз просто не пересылает этот пакет дальше. Но при этом шлюз на тот IP адрес, откуда пришёл пакет с истёкшим временем жизни, отправляет по протоколу ICMP ответ TIME\_EXCEEDED (время жизни кончилось). И этот ответ содержит IP адрес шлюза, где пакет закончил своё существование.

1. *В чем измеряется TTL?*

Определяет максимальное количество хопов (hop, то есть прыжок, участок между маршрутизаторами), которые пакет может пройти.

1. *Как работает Traceroute?*

Так вот, суть трассировки в том, что отправляется один пакет с временем жизни (TTL) установленным на единицу — первый шлюз уменьшает значение на единицу, смотрит, что счётчик стал равен нулю, никуда не отправляет этот пакет, зато нам отправляет ответ, что пакет «умер». Мы и так знаем, что пакет умер — из этого ответа нас интересует только IP адрес шлюза, где с пакетом случилось это несчастье. Затем отправляется пакет со счётчиком установленным на 2 — пакет проходит первый шлюз (его IP мы уже знаем), но несчастье (счётчик достигает нуля) с ним случается уже на втором шлюзе — мы получаем ICMP ответ с IP этого шлюза. Затем отправляется следующий пакет и т. д., пока не будут определены все узлы до нужного нам сетевого хоста.

Когда счётчик TTL становится равным нулю, очередной шлюз просто не пересылает этот пакет дальше. Но при этом шлюз на тот IP адрес, откуда пришёл пакет с истёкшим временем жизни, отправляет по протоколу ICMP ответ TIME\_EXCEEDED (время жизни кончилось). И этот ответ содержит IP адрес шлюза, где пакет закончил своё существование.

**ЛАБА 3**

В Distance-Vector протоколах (RIP), маршрутизатор узнает информацию о маршрутах посредством маршрутизаторов, непосредственно подключенных в один с ним сегмент сети. То есть, маршрутизатор имеет информацию о топологии только в границах его соседних маршрутизаторов и понятия не имеет как устроена топология за этими маршрутизаторами, ориентируясь только по метрикам.

В Link-state протоколах (OSPF) каждый маршрутизатор должен непросто знать самые лучшие маршруты во все удалённые сети, но и иметь в памяти полную карту сети со всеми существующими связями между другими маршрутизаторами в том числе. Это достигается за счет построения специальной базы LSDB.

* *Что такое RIP*

Протокол RIP является дистанционно-векторным протоколом маршрутизации. Протоколы динамической маршрутизации определяют оптимальный путь к необходимой сети на основании значения, которое называется метрикой. В качестве метрики в протоколе RIP используется количество транзитных устройств или переходов (hop count – прыжок пакета) из одной сетевой структуры в другую.

* + *Что такое Hello интервал RIP и чему он равен*

Hello-протокол (hello protocol) — протокол, использующийся для установки и поддержания соседских отношений.

HelloInterval — Интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет с интерфейса (частота отправки сообщений Hello). По умолчанию равен 30 секундам.

* + *Через сколько секунд роутер удаляет маршрут, если информации о нем не была получена*

Когда устройство получает откорректированный маршрут (с максимальной метрикой), свидетельствующий о том, что этот маршрут недоступен, запускается таймер для такого маршрута. Стандартное значение таймера хранения информации равно 180 с. До тех пор, пока не истечет таймер, новая информация о маршруте не принимается устройством, но информация от соседнего маршрутизатора, который ранее анонсировал исчезнувший маршрут, принимается и обрабатывается до истечения таймера хранения информации (Invalid timer).

* + *Как протокол RIP помечает недостижимые сети*

Протокол RIP помечает недостижимые сети метрикой 16 (бесконечно большая метрика).

* + *Почему RIP не используется в современных инфраструктурах*
* Медленная сходимость. Одна из проблем RIP — медленная сходимость, то есть изменения, произошедшие на одном из участков Интернета, распространяются очень медленно через остальной Интернет.
* Нестабильность. Гораздо более важная проблема RIP — нестабильность, которая означает, что сеть Интернет, работающая по протоколу RIP, может стать нестабильной. Это случается, когда пакет от одного маршрутизатора к другому может идти по петле. Ограничение участков в 15 будет увеличивать стабильность, но не снимет все проблемы.
* RIP не работает с адресами субсетей.
* Число шагов важный, но не единственный параметр маршрута, да и 15 шагов не предел для современных сетей..
  + *Вид и тип протокола RIP*

RIP является дистанционно-векторным протоколом внутренней маршрутизации.

ОСНОВНЫЕ РАЗЛИЧИЯ МЕЖДУ RIPV1 И RIPV2

|  |  |
| --- | --- |
| ***RIPv1*** | ***RIPv2*** |
| Он использует широковещательную передачу для обновления маршрутизации. | Он использует многоадресную рассылку для обновления маршрутизации. |
| Он посылает широковещательный пакет по адресу назначения 255.255.255.255. | Он отправляет многоадресную рассылку по адресу назначения 224.0.0.9. |
| Он не поддерживает VLSM. | Он поддерживает VLSM. |
| Он не поддерживает никакой аутентификации. | Он поддерживает аутентификацию MD5 |
| Он поддерживает только классовую маршрутизацию. | Он поддерживает как классовую, так и бесклассовую маршрутизацию. |
| Он не поддерживает непрерывную сеть. | Он поддерживает непрерывную сеть. |
|  | Появилась split horizons. |
|  | Более быстрая сходимость маршрутов. |

* + *Что такое технология разделения горизонтов (split horizon)?*

Правило расщеплённого горизонта говорит, что маршрутизатор не должен распространять информацию о сети через интерфейс, на который прибыло обновление. Другими словами, маршрутизатор не будет информировать о достижимости получателя своего соседа, от которого информация о маршруте к получателю была получена.

* *Что такое OSPF*

Open Shortest Path First (OSPF) является протоколом состояния канала Link-state, который быстро реагирует на изменения в сети, рассылая модификации при изменениях в сетевой топологии всем маршрутизаторам в пределах некоторой области сети. OSPF предназначен для работы в больших гибких составных сетях и может работать с оборудованием разных фирмпроизводителей, поэтому получил широкое распространение.

Протокол OSPF не проводит периодический обмен объемными обновлениями (update) маршрутной информации и характеризуется быстрой сходимостью. Обмен маршрутной информацией производится только при возникновении изменений в сети.

* + *Что такое Hello интервал OSPF и чему он равен*

HelloInterval — интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет с интерфейса. Для широковещательных сетей и сетей точка-точка значение по умолчанию, как правило, равно 10 секундам. Для не широковещательных сетей со множественным доступом значение по умолчанию — 30 секунд.

Hello-пакеты используются, чтобы устанавливать и поддерживать отношения смежности (adjacency) между соседними устройствами.

В OSPF-терминологии соединение называется связь (link). Определены четыре типа связи: "точка-точка", транзит, ответвление и виртуальная.

В сетях первых двух типов период рассылки Hello-пакетов составляет 10 секунд, а в сетях NBMA – 30 с. Период Dead Interval – в четыре раза больше. Обмен Hello-пакетами производится с использованием адресов 224.0.0.5 или 224.0.0.6 многоадресного режима (multicast) без подтверждения доставки

* + *Вид и тип протокола OSPF*
  + *Что такое DR, BDR*

Процесс соседства формируется между соседними маршрутизаторами через DR и BDR, используя LSA. LSA (Link State Advertisement) – сообщение о состоянии канала между маршрутизаторами.

В рамках канала связи выделяют три роли маршрутизаторов:

* DR (designated router — выделенный маршрутизатор) — роль маршрутизатора в рамках канала связи, обязывающая его контролировать рассылку LSA. Все маршрутизаторы сегмента устанавливают отношения соседства с DR и совершают синхронизацию LSDB исключительно с ним. В случае изменений в сети, маршрутизаторы делают рассылку служебных сообщений на DR, который распространяет их остальным устройствам. Маршрутизатор, являющийся DR в одном сегменте связи, не обязательно является DR в другом. Например, маршрутизатор R3 может быть DR в канале связи с R4 и являться BDR в канале связи с R2. Процесс выбора DR и BDR рассмотрен ниже. В случае каких либо изменений в сети, маршрутизатор, который зарегистрировал эти изменения, отправляет анонсы не всем маршрутизаторам, а только DR на мультикастный адрес 224.0.0.6, тем самым сокращается количество информации, передаваемой по сети. А вот DR уже информирует всех остальных об этих изменениях, рассылая Network LSA.
* BDR (backup designated router — резервный выделенный маршрутизатор) — роль маршрутизатора сегмента связи, обязывающая его контролировать работоспособность DR и, в случае выхода его из строя, брать на себя роль DR. BDR, аналогично DR, устанавливает отношения соседства со всеми устройствами и получает уведомления об изменениях, однако не производит рассылку служебных сообщений для синхронизации LSDB.
* DRother (designated router other — маршрутизаторы не являющиеся выделенными) — роли маршрутизаторов, которые не были выбраны DR и BDR в данном сегменте связи. В случае выхода из строя DR, среди DROther проводятся выборы на роль BDR.

Выбор DR и BDR

* Для того чтобы выбрать для сети DR и BDR, маршрутизаторы просматривают значение приоритета в hello-сообщениях и следуют таким условиям для того, чтобы определить какой маршрутизатор выбрать:
* Маршрутизатор с наивысшим значением приоритета становится DR.
* Маршрутизатор со вторым наивысшим значением приоритета становится BDR.
* По умолчанию приоритет интерфейса равен 1. Если у маршрутизаторов одинаковые приоритеты, то DR и BDR выбираются по значению Router ID. Маршрутизатор с наивысшим Router ID становится DR, а маршрутизатор со вторым наивысшим Router ID — BDR.
* Маршрутизатор с приоритетом равным 0 не может стать DR или BDR. Маршрутизатор, не ставший DR или BDR называется DROTHER.
* Если в сети появляется новый маршрутизатор с более высоким приоритетом чем у текущего DR, то это не влияет на выбранных DR и BDR, переизбрание их не происходит. DR и BDR меняются только тогда, когда один из них вышел из строя. Если из строя вышел DR, то его заменяет BDR и происходят выборы нового BDR. Если из строя выходит BDR, то выбирается новый BDR.

Для того чтобы определить, что DR вышел из строя BDR использует Wait Timer. Если в течение этого таймера BDR не получает подтверждения того, что DR отправляет LSA, то он считает, что DR вышел из строя.

Преимущества использования DR и BDR в широковещательной сети:

* Уменьшение служебного трафика: DR и BDR исполняют роль коммуникационного центра в процедуре обмена топологической информацией по широковещательной сети с множественным доступом. Это снижает поток информации, так как DR принимая обновление, сам распространяет его по сети, если это необходимо. Такой способ распространения весьма значительно уменьшает количество служебной информации в сети.
* Управление синхронизацией топологии: DR и BDR являются гарантами того, что топологическая информация на всех маршрутизаторах сегмента будет совпадать. Таким образом, DR и DR уменьшают количество ошибок маршрутизации.
  + *Что такое LSDB*

В эту структуру данных маршрутизатора сохраняются полученные маршрутизатором от других маршрутизаторов состояния ликов (LSA). Когда маршрутизатор получает все LSA, на основании LSDB строится карта сети, по которой, в свою очередь, определяются маршруты (кратчайшие пути) в удалённые сети.

База данных состояния каналов (link state database, LSDB) — список всех записей о состоянии каналов (LSA).

Объявление о состоянии канала (link-state advertisement, LSA) — единица данных, которая описывает локальное состояние маршрутизатора или сети. Например, для маршрутизатора LSA включает описание состояния каналов и отношений соседства. Множество всех LSA, описывающих маршрутизаторы и сети, образуют базу данных состояния каналов (LSDB).

DBD — пакеты, которые описывают содержание LSDB. DBD (Database Description) -- пакет, который описывает содержание LSDB маршрутизатора. Эти пакеты позволяют маршрутизаторам обменятся информацией о том, что они знают и чего недостает в их LSDB.

* + *Метрики*

Протокол маршрутизации OSPF использует метрику cost. Метрика протокола OSPF базируется на полосе пропускания bandwidth (пропускная способность). Алгоритм протокола рассчитывает суммарное значение метрики всех соединений через сеть. Меньшее число указывает лучший маршрут.

* + *Мультикаст*

Мультивещание, многоадресное вещание ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *multicast* — групповая передача) — форма [широковещания](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%80%D0%BE%D0%BA%D0%BE%D0%B2%D0%B5%D1%89%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB), при которой адресом назначения сетевого пакета является мультикастная группа (один ко многим). Существует мультивещание на [канальном](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%83%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C), [сетевом](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D1%8B_%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B3%D0%BE_%D1%83%D1%80%D0%BE%D0%B2%D0%BD%D1%8F) и [прикладном](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D1%8B_%D0%BF%D1%80%D0%B8%D0%BA%D0%BB%D0%B0%D0%B4%D0%BD%D0%BE%D0%B3%D0%BE_%D1%83%D1%80%D0%BE%D0%B2%D0%BD%D1%8F) уровнях. Мультивещание не следует путать с технологией передачи на физическом уровне [точка-многоточка](https://ru.wikipedia.org/wiki/%D0%A2%D0%BE%D1%87%D0%BA%D0%B0-%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE%D1%82%D0%BE%D1%87%D0%BA%D0%B0).

* *Что за параметры указаны в квадратных скобках при просмотре информации о маршрутах?*

*Важные понятия:*

* Что такое Redistributing?

Пока не создан единый протокол маршрутизации, управляющий остальными, существует необходимость в том, чтобы несколько протоколов маршрутизации мирно сосуществовали в одной сети. К примеру, одна компания работает с OSPF, а другая компания работает с EIGRP, и эти две компании слились в одно целое предприятие. Пока вновь образованный ИТ-персонал не перейдет для использования на единый протокол маршрутизации (возможно они когда-нибудь это сделают), маршруты, известные протоколу OSPF, необходимо объявить в часть сети, работающей под [управлением EIGRP](https://wiki.merionet.ru/seti/11/nastrojka-protokola-eigrp-na-oborudovanii-cisco/), и наоборот.

Упомянутый выше сценарий возможен благодаря Route redistribution, и именно этому посвящена данная статья. Другие причины, по которым вам потребуется выполнить Route redistribution, это: различные части сети конкретной компании находятся под различным административным контролем; если необходимо [объявить маршруты своему поставщику услуг через BGP](https://wiki.merionet.ru/seti/35/osnovy-protokola-border-gateway-protocol-bgp/), или, возможно, необходимо подключиться к сети делового партнера.

* Area (область) — логическая единица деления OSPF-домена, применяемая для уменьшения пересылаемой маршрутной информации и снижения числа пересчётов SPT при изменениях на сети. Для работы OSPF обязательно наличие backbone-area (area c area-id=0). Все области должны присоединяться к backbone-area, как «ромашка», где в центре находится backbone-area, а «лепестки» — остальные области. Строгие ограничения по числу устройств в area отсутствуют и к делению домена на области необходимо подходить творчески, учитывая производительность маршрутизаторов, загрузку каналов связи и проект сети.
* Distance (дистанция) — степень доверия к источнику маршрутной информации. Поскольку на маршрутизаторе могут одновременно работать несколько протоколов маршрутизации, как на R1, где работает OSPF и BGP, то необходимо ввести параметр, который будет указывать на то, какому из источников маршрутной информации доверять больше. Чем меньше величина distance, тем более доверительным является источник маршрутной информации. В контексте статьи будут интересны следующие значения distance:

connected-маршруты — 0;  
static-маршруты — 1;  
OSPF-маршруты — 110.

* Neighbors (соседи) — два маршрутизатора с запущенным процессом OSPF, имеющие общий канал связи, ассоциированный с одной и той же area. На рисунке 1, например, маршрутизаторы R2 и R1 являются соседями, т.к. соединены напрямую и их интерфейсы eth2 и eth1 ассоциированы с backbone-area.
* Adjacency (отношения соседства) — логическое соединение двух маршрутизаторов, являющихся соседями. Для отношений соседства необходимо выполнение ряда параметров, рассмотренных ниже. Два маршрутизатора, являющиеся соседями, устанавливают отношения соседства после полной синхронизации базы данных маршрутной информации LSDB.
* RID (router identificator — идентификатор маршрутизатора) — условный идентификатор маршрутизатора в домене OSPF, записываемый в форме ip-адреса. Рекомендуется, для упрощения диагностики, назначать RID вручную, однако, в случае если идентификатор не задан, RID будет выбран автоматически из списка ip-адресов.

**ЛАБА 4**

* **Что такое BGP?**

BGP ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Border Gateway Protocol*, протокол граничного шлюза) — протокол динамической маршрутизации.

Относится к классу протоколов маршрутизации внешнего шлюза ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *EGP — Exterior Gateway Protocol*).

На текущий момент является основным [протоколом](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%BC%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D0%B8) динамической [маршрутизации](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F) в сети [Интернет](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82).

Протокол BGP предназначен для обмена информацией о достижимости подсетей между [автономными системами](https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D0%BD%D0%BE%D0%BC%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_(%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82)) (АС, англ. AS — autonomous system), то есть группами маршрутизаторов под единым техническим и административным управлением, использующими [протокол внутридоменной маршрутизации](https://ru.wikipedia.org/wiki/IGP) для определения маршрутов внутри себя и протокол междоменной маршрутизации для определения маршрутов доставки пакетов в другие АС.

BGP - это протокол внешнего шлюза. В отличие от протоколов внутреннего шлюза, таких как OSPF и RIP, его внимание сосредоточено не на автоматическом обнаружении топологии сети, а на выборе наилучшего маршрута и управлении распространением маршрутов между ASs.

* **Какие виды BGP вы знаете?**

BGP бывает двух типов: внутренний или iBGP и внешний eBGP. Внутренним он называется когда он работает в одной автономной системе (AS), а внешним когда в он работает в различных автономных системах.

iBGP и eBGP также различаются тем, как маршруты, полученные от одного соседа, распространяются на других соседей. К примеру, новые маршруты, полученные от eBGP, обычно перераспределяются между всеми iBGP узлами, а также всеми другими eBGP соседями. Но если новые маршруты объявляются на iBGP пиринге, то повторно они объявляются только всем одноранговым узлам eBGP. Это означает, что все iBGP соседи должны быть соединены в одну сеть.

Внутренний BGP (Internal BGP, iBGP) — BGP работающий внутри автономной системы. iBGP-соседи не обязательно должны быть непосредственно соединены.

Внешний BGP (External BGP, eBGP) — BGP работающий между автономными системами. По умолчанию, eBGP-соседи должны быть непосредственно соединены.

* **В чем особенность построения маршрута в eBGP?**

Внешний BGP (External BGP, eBGP) — BGP работающий между автономными системами. По умолчанию, eBGP-соседи должны быть непосредственно соединены. Если iBGP-маршрутизаторы работают в нетранзитной AS, то соединение между ними должно быть full mesh. Это следствие принципов работы протокола — если маршрутизатор, находящийся на границе AS, получил обновление, то он передает его всем соседям; соседи, которые находятся внутри автономной системы, больше это обновление не распространяют, так как считают, что все соседи внутри AS уже его получили.

* **Что такое Redistributing?**

Перераспределение маршрутов (route redistribution) — передача маршрутов, выученных с помощью одного протокола маршрутизации, в другой протокол маршрутизации. Кроме того, статические маршруты или непосредственно присоединенные сети, также могут быть перераспределены и, после этого, будут передаваться с помощью соответствующего протокола маршрутизации.

Перераспределение маршрутов возможно только между протоколами которые поддерживают один и тот же стек протоколов.

Для того чтобы перераспределить маршруты из одного источника в другой, должна быть как минимум одна точка где они перераспределяются. То есть, должен быть маршрутизатор, который это выполняет. Например, если перераспределяются маршруты протокола OSPF в маршруты EIGRP, то на таком маршрутизаторе должны быть настроены оба протокола, а затем правила перераспределения маршрутов из одного протокола в другой.

* **Как работает BGP?**

Процесс выбора запускается после обновления информации и служит для отбора маршрутов, предназначенных для использования локально и передачи другим маршрутизаторам, использующим BGP. Процесс использует атрибуты полученных маршрутов для оценки степени предпочтения маршрута или информации о том, что маршрут является неподходящим для занесения в базу маршрутов и должен быть исключён из процесса отбора. Процесс делится на три фазы:

* Вычисление степени предпочтения каждого полученного маршрута;
* Выбор наилучшего маршрута для каждого места назначения и занесение его в базу маршрутов;
* Передача маршрутов на другие маршрутизаторы, при этом может производиться суммирование маршрутов.

Этапы:

1. Первое что проверяется, это достижимость NEXT\_HOP, если он не достижим, маршрут сразу отбрасывается (помним о next\_hop\_self)

2. Смотрится атрибут weight (напомню что это Cisco атрибут), и используется для определения интерфейса, через который осуществляется выход из нашей AS

3. Далее смотрится атрибут LOCAL\_PREF, выбирается наибольший

4. Роутер, который сам генерирует маршрут, имеет наибольший вес — 32768 и NEXT\_HOP равен 0.0.0.0

5. Далее смотрим на атрибут AS-PATH, выбирается маршрут с наименьшей длиной.

6. Если AS-PATH имеет одинаковую длину, используется сравнение по ORIGIN\_TYPE, таким образом:

IGP = 0, EGP = 1, INCOMPLEETE = 2 (маршрут пришедший через редистрибьюцию, имеет наименьшее значение, так как нет никакой уверенности в том, откуда этот маршрут пришел).

7. Если и на этом участке еще не удается выбрать лучший маршрут, то сравнивается MED, чем он меньше, тем выше приоритет (напоминаю, что по умолчанию MED работает только тогда, когда мы подключены несколькими линками к одной AS).

По умолчанию BGP маршрут выбирается один, но мы на это можем повлиять, используя:

— maximum-paths ibgp указав здесь количество маршрутов (для балансировки). Это для ibgp маршрутов,

— maximum-paths — тоже самое, только для ebgp маршрута.

Так же на этом этапе мы можем повлиять на процедуру выбора, а именно, сделать проверку по MED раньше, чем проверку по ORIGIN, делается это с помощью команды **bgp deterministic-med**, теперь сначала проверяется пункт 7, а затем 6.

Так же помним, из прошлой заметки, что есть команда, которая дает нам возможность использовать MED с разными AS: **bgp always-compare-med**

Так же здесь есть еще одна полезная команда, которая позволяет работать MED в конфедерациях ( о которых мы будем говорить еще не скоро  ). Если мы хотим чтоб MED сравнивался между пирами конфедерации, нам нужна команда **bgp bestpath med confed**

8. Если значение MED одинаковы, то далее смотрится административная дистанция, EBGP = 20, IBGP = 200, выбирается конечно же меньшая дистанция, то есть выигрывает EBGP маршрут.

9.  Выбираем ближайший IBGP. Выбирается старейший EBGP маршрут

Здесь стоит сказать о такой фичи как Synchronization, сейчас она отключена по умолчанию во всех роутерах, но что она значит?

Когда синхронизация была включена, это нам говорила о том, что, роутер не может отсылать маршрут в EBGP до тех пор, пока этот маршрут не получен по IGP (например )

10. Если и здесь все одинаково, тогда ничего не остается как сделать выбор по наименьшему RID (мы его можем устанавливать с помощью bgp router-id {IP})

11. Если по 10-му пункту мы тоже не смогли выбрать лучший маршрут, тогда смотрим на длинну cluster list, с минимальной длиной маршрут выигрывает.

12. Если ни на одном из этапов не был выведен лучший маршрут, то смотрится на IP адрес соседа, от кого пришел данный маршрут,

у кого адрес меньше, тот и побеждает в выборах. Но думаю редко когда дойдет до этого пункта.

* **Что такое AS?**

Автономная система (autonomous system, AS) — набор маршрутизаторов, имеющих единые правила маршрутизации, управляемых одной технической администрацией и работающих на одном из протоколов IGP (для внутренней маршрутизации AS может использовать и несколько IGP).

* **Какой минимальной размерности подсеть можно арендовать у IANA,** **чтобы считаться AS?**

Номера AS выделяются [Internet Assigned Numbers Authority](https://ru.wikipedia.org/wiki/IANA), которая также выделяет [IP-адреса](https://ru.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81) [региональным интернет-регистраторам](https://ru.wikipedia.org/wiki/RIR) (Regional Internet Registry) блоками. RIR затем присваивают организации номер AS из блока, полученного от IANA. Организации, желающие получить ASN, должны пройти процесс регистрации в [RIR](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B3%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D1%80%D0%B5%D0%B3%D0%B8%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80) или в [LIR](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D1%80%D0%B5%D0%B3%D0%B8%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80) и получить одобрение. Текущий список присвоенных ASN можно увидеть на веб-сайте IANA: более подробную информацию о владельце автономной системы можно запросить у RIR, выдавшего этот ASN.

Ранее (до 2007 года) использовались только 16-битные номера AS, что позволяло сделать максимум 65536 присвоений, часть из которых (номера от 64512 до 65534) была зарезервирована как приватные номера AS, которые могут использоваться только локально, по аналогии с [частными IP-адресами](https://ru.wikipedia.org/wiki/%D0%A7%D0%B0%D1%81%D1%82%D0%BD%D1%8B%D0%B9_IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81). Кроме того, номера 0 и 65535 являются зарезервированными IANA и не могут использоваться для маршрутизации, а диапазон 64496-64511 зарезервирован для использования в документации и примерах. В связи со скорым исчерпанием доступного диапазона в 2007-м году был разработан и предложен стандарт на 32-битные номера AS [RFC 4893](https://tools.ietf.org/html/rfc4893), что позволило адресовать 232 автономных систем (за вычетом некоторых зарезервированных диапазонов), не теряя совместимости с уже имеющимися 16-битными ASN.

IANA — Администрация адресного пространства Интернета. Занимается распределением номеров AS и IP-адресов в глобальном масштабе. Назначает RIR, подчиняется напрямую ICANN. Она такая одна и в этой статье она нас не интересует.

RIR — Региональная регистратура Интернета. Занимается выделением крупных блоков адресов, регистрацией LIR и распределением AS. Россия находится в юрисдикции [RIPE NCC](http://www.ripe.net/), расположенной в Амстердаме.

LIR — Локальная Регистратура Интернета. Занимается поддержкой работы сети, распределением PI (о них — дальше) и номеров AS. Как правило, это — ISP. Минимальный блок адресного пространства для LIR — 4096 IP-адресов.

AS — Автономная система. Содержит в себе адресное пространство (IP-адреса), имеет уникальный ASN — номер, позволяющий однозначно идентифицировать AS в Интернете. Номер AS — ключевая часть маршрутизации.

PI — Provider Independent. Провайдеро-независимые IP адреса. Находятся в определенной AS, маршрут к ним зависит только от политики маршрутизации. Принадлежат конечному пользователю [компании или LIR], а не его вышестоящему провайдеру. Следственно, сохраняются при смене ISP\подключении дополнительного ISP.

Для регистрации локальной регистратуре LIR необходимо предоставить следующую информацию: описать причину запроса того количества блоков IP-адресов (кратно 256, подсети класса C, минимально выдаваемого адресного пространства), который собираетесь использовать сейчас и динамику использования в течение ближайших 2 лет.

Сколько можно заказать адресов? Минимум 256, 512 или 1024.

Что такое блок РА адресов? Это блок адресов, выделяемый клиенту в рамках договора на IP адреса. Минимальный размер блока 256 адресов.

* **Что делает команда route-reflector?**

При настройке атрибута route reflection маршруты, полученные по данному подключению, будут анонсированы остальным соседям кроме источника. Если настроить протокол BGP без route-reflect, то все маршрутизаторы не будут видеть сети дальше чем 2 hop, данная настройка позволяет решить эту проблему.

* **Как работает фильтрация BGP?**

В BGP существует достаточно много возможностей фильтрации, таких как access-list, prefix-list, as-path access list.

Каждая из них применяется в разных случаях.

Нарпимер Prefix-list предназначен для фильтрации маршрутов (ip адреса), as-path access-list для фильтрации по атрибуту AS-PATH и так далее.

Но давайте теоретически разберемся как маршрутизатор работает с получаемыми маршрутами.

Маршрутизатор на каждый свой сосед отводит определенную часть памяти, как для входящих маршрутов так и исходящих. Маршрутизатор создает таблицу, которая у Cisco называется: AdjRib-in и ADjRIB-out.

После того, как маршрутизатор получил update, он положил его в таблицу соседа, от которого он получил это обновление, далее идет механизм фильтрации, после фильтрации выжившие маршруты попадают в BGP Table (где содержатся абсолютно все маршруты BGP, кроме тех которые были порезаны фильтром). Далее запускается механизм выбора лучшего маршрута BGP, после выбора лучшего маршрута, эти маршруты попадают в Local RIB, и в дальнейшем только эти маршруты могут рассылаться своим соседям.

Сначала маршрут попадает в фильтр (который уже вешается на out), затем в таблицу соседа AdjRib-out и после из этих таблиц и начинается рассылка информации соседям.

Этот принцип работы достаточно прост, но его необходимо понимать, где что когда работает. Дальше мы углубимся в эту тему.

* **Что такое target scope?**

target-scope - используется в механизме поиска следующего хопа, т.е. решения какой же хоп станет следующим. Это максимальное значение параметра scope для маршрута, посредством которого может быть найден следующий хоп. Для iBGP значение установлено в 30 по умолчанию.

scope - используется в механизме поиска следующего хопа, т.е. решения какой же хоп станет следующим. Нужный маршрут может быть выбран только среди маршрутов, значения scope которых меньше либо равно значению target-scope. Значения по умолчанию зависят от протокола.

* **Конфигурация cisco и mikrotik (понимать конфиги)**
* **Чем iBGP отличается от RIP и OSPF**

Оcновным отличием BGP от других протоколов маршрутизации является то, что он использует TCP в качестве транспортного протокола.

RIP: для передачи служебной информации используются UDP-датаграммы, за протоколом закреплён порт 520.

BGP - это протокол внешнего шлюза. В отличие от протоколов внутреннего шлюза, таких как OSPF и RIP, его внимание сосредоточено не на автоматическом обнаружении топологии сети, а на выборе наилучшего маршрута и управлении распространением маршрутов между ASs.

* **Чем отличается построение маршрутов в iBGP от таковых в RIP и OSPF**
* **Что такое route-reflection?**
* **Чем отличается принцип работы Route-reflection в маршрутизаторах cisco и mikrotik**