HCIE-R&S

Технологии LAN

www.huawei.com

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

HUAWEI

Введение

- Ethernet - одна из самых распространенных технологий, используемых для локальных вычислительных сетей (LAN), которая определяет их типы кабелей и методы вычисления. Технология для локальных вычислительных сетей Ethernet получила широкое распространение в отрасли благодаря простоте, малозатратности и простоте внедрения. Появление технологий Gigabit Ethernet и Ethernet 10G позволили Ethernet стать самой перспективной сетевой технологией.
- Данный документ описывает следующие понятия LAN: таблица MAC-адресов, основы ARP, MSTP, умное стекирование iStack, CSS и агрегация каналов.

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

Цели

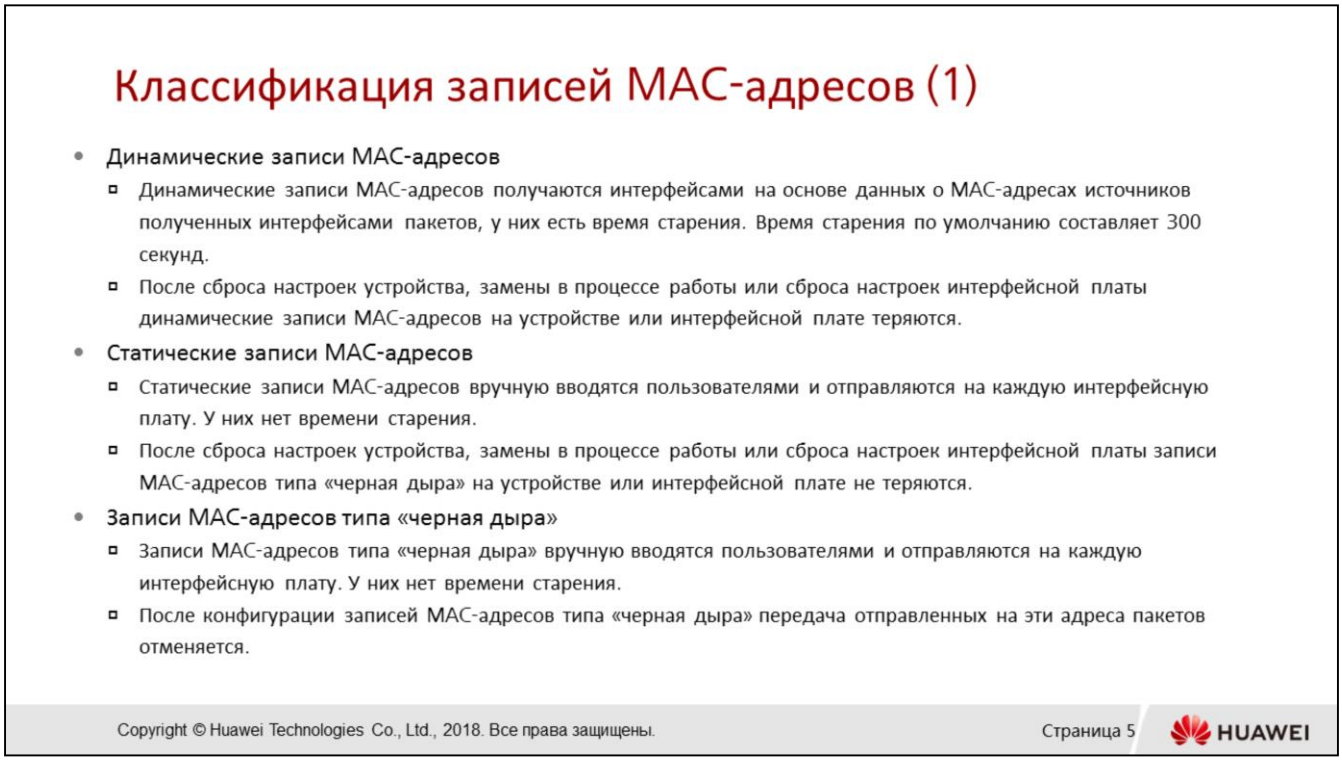
- По завершении данного курсы вы узнаете:
  - Классификацию записей MAC-адресов и о нестабильности (флаппинге) MAC-адресов.
  - Основы и сценарии применения самообращенного запроса ARP.
  - Основы MSTP.
  - О системах iStack и системе переключения кластеров (CSS).
  - Об агрегации каналов и принципах ее работы.

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

Содержание

1. **Таблица MAC-адресов**
   - Классификация записей MAC-адресов
   - Защита портов
   - Нестабильность (флаппинг) MAC-адресов
2. Самообращенный запрос ARP
3. MSTP
4. Умное стекирование iStack
5. CSS
6. Eth-Trunk

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.



- **Определение таблицы MAC-адресов**
  - Таблица MAC-адресов - это таблица адресов, используемая коммутатором для записи карт распределения между известными MAC-адресами других устройств и интерфейсами с получаемыми MAC-адресами, а также виртуальными локальными сетями (VLAN), которым принадлежат интерфейсы. По получении пакета данных коммутатор ищет MAC-адрес назначения в таблице MAC-адресов. Если коммутатор находит MAC-адрес, он направляет пакет от соответствующего отправляющего интерфейса на записанный MAC-адрес. В противном случае коммутатор рассылает пакет на все интерфейсы (кроме интерфейса, с которого получен пакет) в связанной виртуальной локальной сети (VLAN).
- **Записи MAC-адресов делятся на динамические, статические и адреса типа «черная дыра»..**
  - Динамические записи MAC-адресов

Динамические записи MAC-адресов получаются интерфейсами на основе данных о MAC-адресах источников полученных интерфейсами пакетов, у них есть время старения. После сброса настроек устройства, замены в процессе работы или сброса настроек интерфейсной платы динамические записи MAC-адресов на устройстве или интерфейсной плате теряются. Для проверки передачи данных между двумя соединенными устройствами можно проверить динамические записи MAC-адресов. Для получения информации о количестве обменивающихся данными пользователей, подключенных к интерфейсу, можно проверить количество отдельных записей динамических MAC-адресов.

  - Статические записи MAC-адресов

Статические записи MAC-адресов вручную вводятся пользователями и отправляются на каждую интерфейсную плату. У них нет времени старения. После сброса настроек устройства, замены в процессе работы или сброса настроек интерфейсной платы статические записи MAC-адресов на устройстве или интерфейсной плате не теряются. У статических записей MAC-адресов может быть только один исходящий интерфейс. Статическая привязка интерфейса к MAC-адресу не не влияет на получение динамической записи MAC-адреса интерфейсом. Статические записи MAC-адресов могут быть настроены таким образом, чтобы позволить

авторизованному пользователю получить доступ к сетевым ресурсам и предотвратить использование MAC-адреса другими пользователями для атаки.

- Записи MAC-адресов типа «черная дыра»

Записи MAC-адресов типа «черная дыра» вручную вводятся пользователями и отправляются на каждую интерфейсную плату. У них нет времени старения. После сброса настроек устройства, замены в процессе работы или сброса настроек интерфейсной платы записи MAC-адресов типа «черная дыра» на устройстве или интерфейсной плате не теряются. Записи MAC-адресов типа «черная дыра» могут быть настроены для отфильтровки неавторизованных пользователей.

Классификация записей MAC-адресов (2)

```
[Huawei]dis mac-address
MAC address table of slot 0:
-------------------------------------------------------------------------------
MAC Address    VLAN/       PEVLAN CEVLAN Port            Type       LSP/LSR-ID
               VSI/SI                                               MAC-Tunnel
-------------------------------------------------------------------------------
00aa-bbcc-ddee -           -      -      -               blackhole  -
0011-2233-4455 1           -      -      GE0/0/2         static     -
-------------------------------------------------------------------------------
Total matching items on slot 0 displayed = 2

MAC address table of slot 0:
-------------------------------------------------------------------------------
MAC Address    VLAN/       PEVLAN CEVLAN Port            Type       LSP/LSR-ID
               VSI/SI                                               MAC-Tunnel
-------------------------------------------------------------------------------
5489-986d-53e0 1           -      -      GE0/0/16        dynamic    0/-
5489-98fc-608b 1           -      -      GE0/0/1         dynamic    0/-
-------------------------------------------------------------------------------
Total matching items on slot 0 displayed = 2
```

- По умолчанию время старения динамических записей MAC-адресов составляет 300 секунд.

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

HUAWEI

- Записи MAC-адресов на устройстве можно проверить при помощи команды **display mac-address**. Как указано в пердыдущем слайде, записи MAC-адресов можно разделить на динамические, статические и типа «черная дыра». Записи также включают данные о VLAN и VSI каждого MAC-адреса.

Конфигурация записей MAC-адресов

- Конфигурация статических записей MAC-адресов.

```
[Huawei]mac-address static 0011-2233-4455 GigabitEthernet 0/0/2 vlan 1
```

- Конфигурация записей MAC-адресов типа «черная дыра»

```
[Huawei]mac-address blackhole 00aa-bbcc-ddee
```

- Настройка времени старения динамических записей MAC-адресов.

```
[Huawei]mac-address aging-time 400
```

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

Содержание

1. **Таблица MAC-адресов**
   - Классификация записей MAC-адресов
   - Защита портов
   - Нестабильность (флаппинг) MAC-адресов
2. Самообращенный запрос ARP
3. MSTP
4. Умное стекирование iStack
5. CSS
6. Eth-Trunk

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

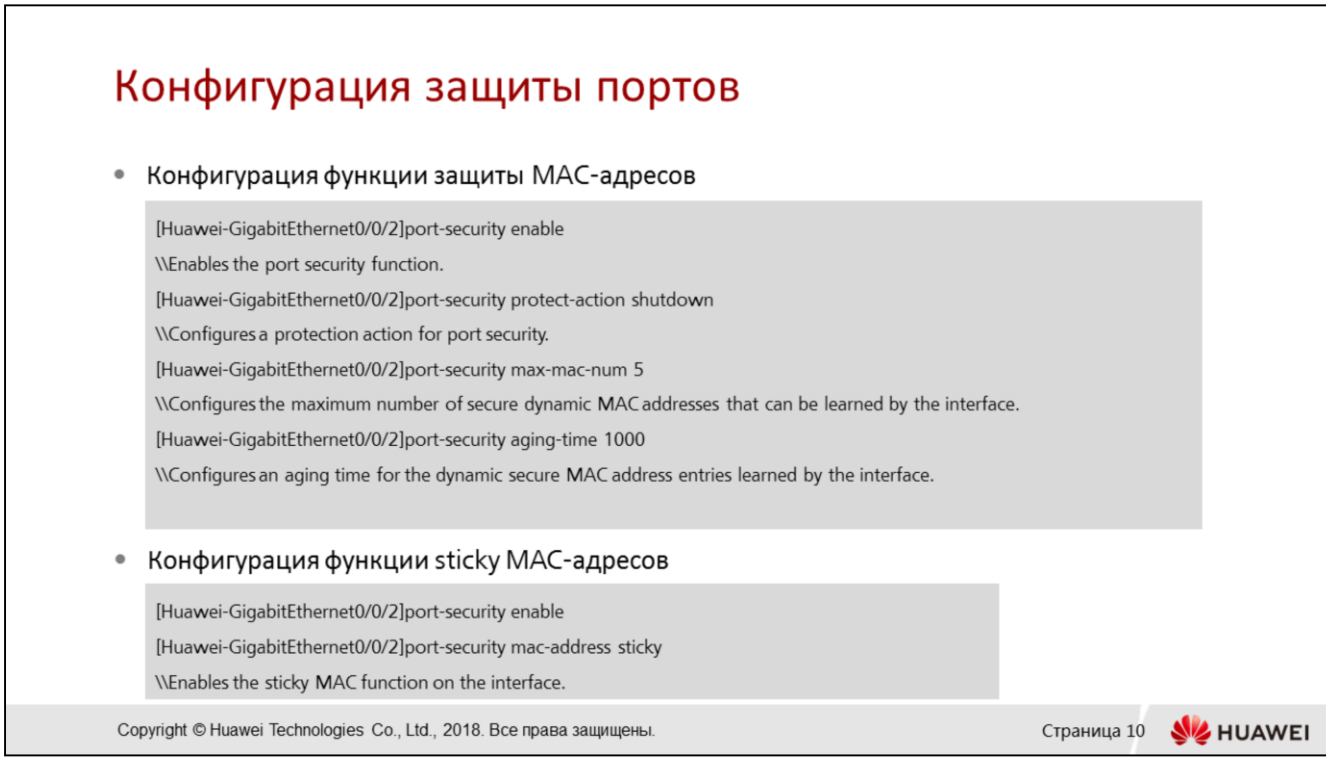
Защита портов

- Защита портов преобразует полученные интерфейсом динамические MAC-адреса в защищенные MAC-адреса (включая динамические, статические и sticky MAC-адреса). Данная функция предотвращает использование данного интерфейса неавторизованными пользователями для соединения с коммутатором и таким образом повышает безопасность устройства.
- Классификация безопасных MAC-адресов
  - Безопасный динамический MAC-адрес
    - MAC-адрес, конвертированный в интерфейсе с включенной функцией защиты портов, но выключенном режиме запоминания sticky MAC-адресов
  - Безопасный статический MAC-адрес
    - MAC-адрес, вручную сконфигурированный в интерфейсе с включенной функцией защиты портов
  - Sticky MAC-адреса
    - MAC-адрес, конвертированный в интерфейсе с включенными функцией защиты портов и режимом запоминания sticky MAC-адресов

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

HUAWEI

- После включения функции защиты портов в интерфейсе динамические записи MAC-адресов, ранее запомненные интерфейсом, удаляются. Последующие динамические записи MAC-адресов конвертируются в защищенные динамические записи MAC-адресов.
- После включения режима запоминания sticky MAC-адресов в интерфейсе существующие защищенные динамические записи MAC-адресов конвертируются в записи sticky MAC-адресов.
- После выключения функции защиты портов в интерфейсе защищенные динамические записи MAC-адресов удаляются из интерфейса, динамические записи MAC-адресов перераспределяются.
- После выключения режима запоминания sticky MAC-адресов в интерфейсе записи sticky MAC-адресов в интерфейсе конвертируются в динамические записи MAC-адресов.



- Описание
  - После включения режима запоминания sticky MAC-адресов в интерфейсе существующие защищенные динамические записи MAC-адресов конвертируются в записи sticky MAC-адресов.
  - После включения режима запоминания sticky MAC-адресов в интерфейсе записи sticky MAC-адресов не имеют времени старения даже при запуске команды **port-security aging-time**.
  - Сохраненные записи sticky MAC-адресов не теряются даже после перезагрузки устройства.
- Действия защиты портов:
  - Запретить (Restrict). Отбраковывает пакеты, MAC-адрес источника которых не существует, и посылает сигнал о тревоге. Рекомендуемое действие.
  - Защитить (Protect). Отбраковывает пакеты, MAC-адрес источника которых не существует, но не посылает сигнала о тревоге.
  - Выключить (Shutdown). Включает статус интерфейса «выключен из-за сбоя» (error-down) и посылает сигнал о тревоге.

Содержание

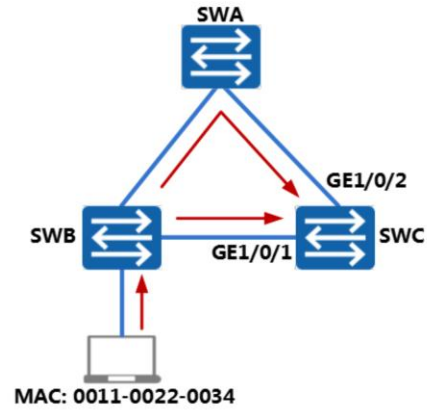
1. **Таблица MAC-адресов**
   - Классификация записей MAC-адресов
   - Защита портов
   - Нестабильность (флаппинг) MAC-адресов
2. Самообращенный запрос ARP
3. MSTP
4. Умное стекирование iStack
5. CSS
6. Eth-Trunk

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

HUAWEI

Нестабильность (флаппинг) MAC-адресов

- Нестабильность (флаппинг) MAC-адресов возникает, когда MAC-адрес получен двумя интерфейсами одной VLAN, и более поздняя запись MAC-адреса замещает более раннюю.
- Механизм предотвращения нестабильности MAC-адресов:
  - Увеличивает приоритет получения MAC-адреса интерфейса.
  - Запрещает замещение записей MAC-адресов между интерфейсами с одинаковым приоритетом.



Получение записи MAC-адреса, интерфейс назначения - GE 1/0/1.

MAC-адрес	Порт
0011-0022-0034	GE1/0/1

Интерфейс назначения записи MAC-адреса обновлен до GE 1/0/2, показывая, что проявилась нестабильность MA адреса

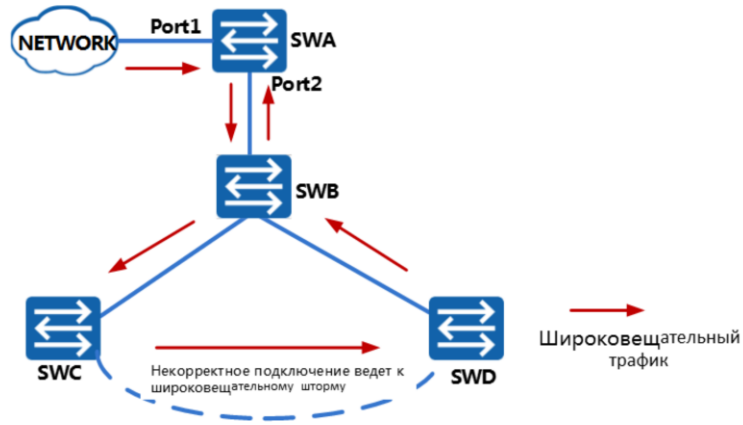
MAC-адрес	Порт
0011-0022-0034	GE1/0/2

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- На рисунке выше для устройства с MAC-адресом 0011-0022-0034 интерфейс назначения изменен с GE1/0/1 на GE1/0/2. Это нестабильность (флаппинг) MAC-адресов. Нестабильность MAC-адресов может вызвать увеличение потребления ресурсов ЦП коммутатора. В целом, нестабильность MAC-адресов не появляется в сетях без петель. Если в сети часто появляется нестабильность MAC-адресов, сообщения об ошибках и журналы записи нестабильностей MAC-адресов помогают обнаружить сбои и устранить петли.
- Нестабильность MAC-адресов появляется в случае возникновения петель в сети или атак. На этапе планирования структуры сети во избежание нестабильности MAC-адресов можно использовать нижеприведенные методы:
  - Увеличение приоритета получения MAC-адреса интерфейса. Если один и тот же MAC-адрес назначен интерфейсами с разным приоритетом, то запись MAC-адреса от интерфейса с наибольшим приоритетом будет иметь превосходство.
  - Запрещение замещения записей MAC-адресов между интерфейсами с одинаковым приоритетом. Если у подключенного к неавторизованному устройству интерфейсу такой же приоритет, как и у подключенного к авторизованному устройству, присвоенный позже MAC-адрес неавторизованного устройства не имеет преимущества перед исходной корректной записью MAC-адреса. Если авторизованное устройство выключено, запоминается запись MAC-адреса неавторизованного устройства. При включении авторизованного устройства его MAC-адрес не запоминается.

Обнаружение нестабильности (флаппинга) MAC-адресов

- Обнаружение нестабильности (флаппинга) MAC-адресов выявляет наличие нестабильности, определяя высокую частоту смены интерфейсов назначения записей MAC-адресов.



Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- При включенной функции обнаружения нестабильности MAC-адресов коммутатор посылает сообщение о неисправности при возникновении нестабильности MAC-адресов (например, в результате петли между интерфейсами назначения). Сообщение включает нестабильный MAC-адрес, идентификатор VLAN и интерфейсы назначения, между которыми возникла нестабильность. На основании сообщения администратор сети может определить расположение петли. Также коммутатор может выполнять действия по автоматическому устранению петли, определенные в настройках функции обнаружения нестабильности MAC-адресов. Действия включают quit-vlan (удаление интерфейса из VLAN) и error-down (отключение интерфейса).
- На рисунке выше сетевой кабель некорректно подключен к коммутаторам SwitchC и SwitchD, в результате чего возникает петля между коммутаторами SwitchB, SwitchC и SwitchD. Когда порт1 коммутатора SwitchA получает широковещательный пакет, SwitchA передает пакет на SwitchB. Пакет отправляется на порт2 коммутатора SwitchA. Так как на SwitchA включена функция обнаружения нестабильности MAC-адресов, он может определить, что MAC-адрес источника нестабилен при передаче с порта1 на порт2. Если между портом1 и портом2 часто проявляется нестабильность MAC-адресов, коммутатор A отправляет сообщение о неисправности.

Настройка предотвращения нестабильности MAC-адресов (Anti-flapping)

- Настройка приоритетов присвоения MAC-адресов для интерфейсов.

```
[Huawei-GigabitEthernet0/0/2]mac-learning priority 3
\\Configures a MAC address learning priority for an interface. By default, the priority of MAC address learning on an interface is 0. A larger value indicates a higher priority.
```

- Настройка устройства на запрет нестабильности MAC-адресов между интерфейсами с

```
[Huawei]undo mac-learning priority 3 allow-flapping
\\Configures a device to prohibit MAC address flapping between interfaces with the same priority.
```

- Настройка глобального обнаружения нестабильности MAC-адресов.

```
[Huawei]mac-address flapping detection
\\Configures global MAC address flapping detection.
```

- Настройка обнаружения нестабильности MAC-адресов на базе VLAN.

```
[Huawei]vlan 2
[Huawei-vlan2]loop-detect eth-loop block-time 100 retry-times 3
\\Configures VLAN-based MAC address flapping detection.
```

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- После настройки разных приоритетов назначения MAC-адресов для интерфейсов, когда одна запись MAC-адреса определяется двумя интерфейсами, запись, назначенная интерфейсом с более высоким приоритетом имеет превосходство.
- Настройка устройства на запрет нестабильности MAC-адресов между интерфейсами с одинаковым приоритетом также предотвращает нестабильность MAC-адресов и улучшает безопасность сети.

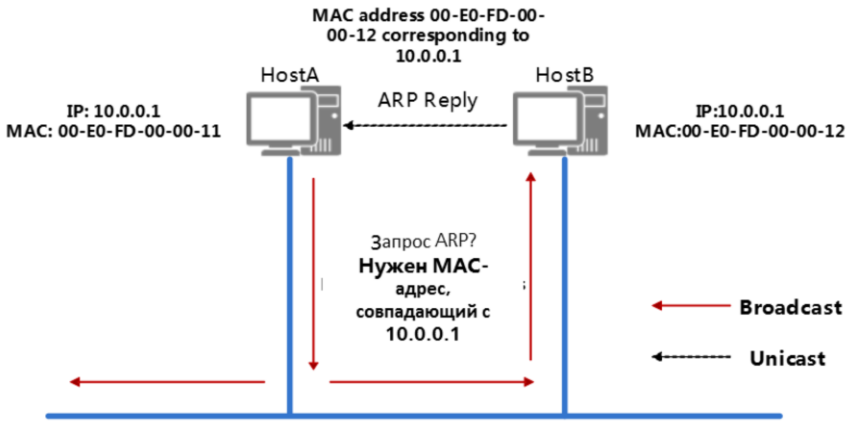
Содержание

1. Таблица MAC-адресов
2. **Самообращенный запрос ARP**
3. MSTP
4. Умное стекирование iStack
5. CSS
6. Eth-Trunk

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

Самообращенный запрос ARP

- Самообращенный запрос ARP позволяет устройству отправить запрос ARP, в котором его собственный IP указан в качестве IP-адреса назначения.



Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- У самообращенного запроса ARP есть следующие функции:
  - Проверка IP-адреса на наличие конфликтов.

    При смене статуса протокола интерфейса устройства на «Up» устройство отправляет пакеты самообращенного запроса ARP. Если устройство получает ответ ARP, то другое устройство использует тот же IP-адрес. При обнаружении конфликта IP-адресов устройство периодически отправляет пакеты ответа ARP до тех пор, пока конфликт не устранен.
  - Информирование о новом MAC-адресе.

    При замене MAC-адреса устройства в результате смены сетевого адаптера устройство отправляет пакет самообращенного запроса ARP для оповещения всех устройств о смене до истечения срока давности записи ARP.
  - Информирование других устройств о переключении ведущего/резервного устройств в группе VRRP.

    После переключения ведущего/резервного устройств ведущее устройство рассылает пакеты самообращенного запроса ARP устройствам в группе VRRP для оповещения о переключении.

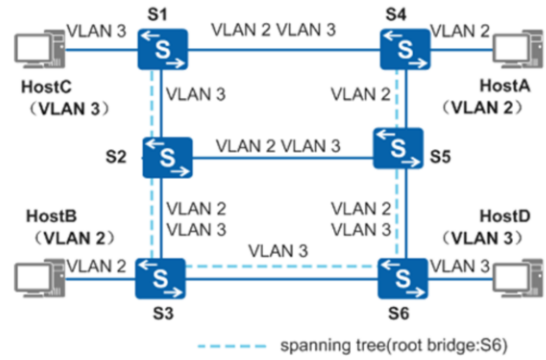
Содержание

1. Таблица MAC-адресов
2. Самообращенный запрос ARP
3. **MSTP**
   - Обзор протоколов STP/RSTP
   - Основы MSTP
4. Умное стекирование iStack
5. CSS
6. Eth-Trunk

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

Недостаток протоколов STP/RSTP

- У протоколов STP и RSTP есть недостаток: У всех VLAN в LAN одно и то же связующее дерево. В результате невозможно провести балансировку загрузки между сетями VLAN, а блокированные каналы не могут передавать трафик, что может привести к сбою передачи пакетов VLAN.



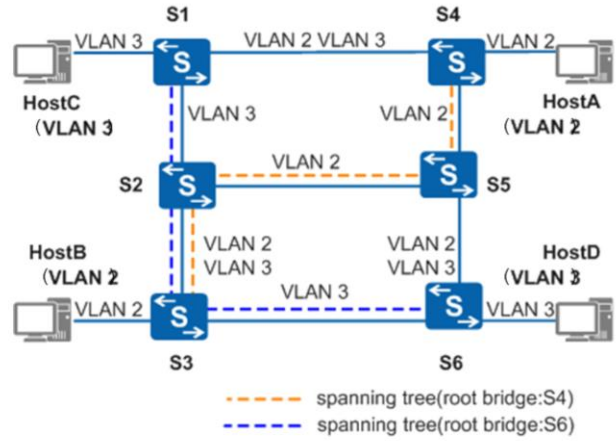
- На предыдущем рисунке связующее дерево отмечено пунктирными линиями, S6 - корневой мост. Каналы между S2 и S5, между S1 и S4 заблокированы. HostA и HostB принадлежат к сети VLAN 2. Так как канал между S2 и S5 заблокирован, и канал между S3 и S6 запрещает пакеты из сети VLAN 2, HostA и HostB не могут связаться друг с другом.

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- У всех сетей VLAN одно связующее дерево для протоколов STP и RSTP. Поэтому некоторые VLAN не могут связываться друг с другом, используются неоптимальные пути и балансировка трафика невозможна.
- Для устранения данного недостатка в 2002 году IEEE выпустила определяющий протокол MSTP стандарт 802.1s. Совместимый с STP и RSTP протокол MSTP может быстро объединять трафик и предоставлять множество путей для балансировки трафика VLAN.

Преимущества MSTP перед STP и RSTP

- Протокол MSTP разделяет коммутационную сеть на множество регионов, у каждого из которых есть несколько связующих деревьев.
- Каждое связующее дерево называется копией множества связующих деревьев (MSTI), каждый регион называется регионом множества связующих деревьев (регион MST).



Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- MSTI - это несколько VLAN. Привязка множества VLAN к одному дереву MSTI снижает стоимость пересылки и использования ресурсов. Топология каждого MSTI рассчитывается независимо, а трафик может распределяться между MSTI. Множество VLAN с одинаковой топологией можно привязать к одному дереву MSTI. Состояние пересылки VLAN для интерфейса определяется состоянием интерфейса в MSTI.
- На рисунке выше MSTP связывает VLAN и MSTI связывая их в схеме распределения. Каждая VLAN может быть приписана только одному MSTI. Это означает, что трафик сети VLAN может быть передан только одному MSTI. MSTI же может соответствовать множество сетей VLAN.
- После рассчета генерируются два дерева MSTI:
  - MSTI 1 использует S4 как корневой мост для пересылки пакетов VLAN 2.
  - MSTI 2 использует S6 как корневой мост для пересылки пакетов VLAN 3.
- Устройства в одной сети VLAN затем могут связываться друг с другом, пакеты разных VLAN затем распределяются по разным путям.

Содержание

1. Таблица MAC-адресов
2. Самообращенный запрос ARP
3. **MSTP**
   - Обзор протоколов STP/RSTP
   - Основы MSTP
4. Умное стекирование iStack
5. CSS
6. Eth-Trunk

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

Основные понятия MSTP

- Регион MST
- MSTI
- Таблица сопоставления VLAN
- CST, IST, SST, CIST
- Корень региона
- Корень CIST
- Ведущий мост
- Роль порта
- Статус порта

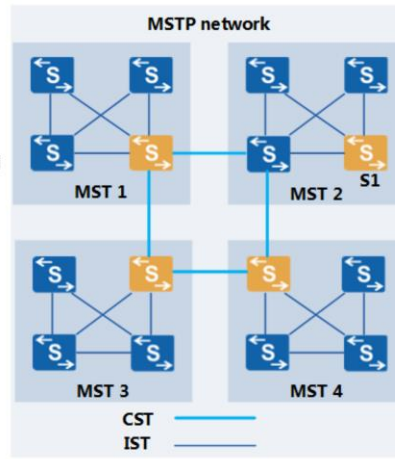


Рисунок 1. Сеть MSTP.

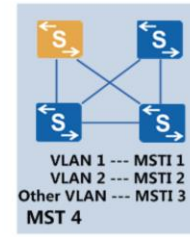


Рисунок 2. Соответствие между VLAN и MSTI.

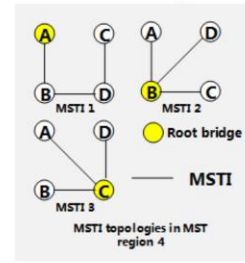


Рисунок 3. Расчет независимых связующих деревьев внутри каждого MSTI.

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- Регион MST состоит из множества коммутаторов и их сегментов сети. MSTI - это пример региона MST. В регионе MST может быть множество MSTI.
- Таблица сопоставления VLAN описывает сопоставления между VLAN и MSTI. Как показано на Рисунке 2, в регионе MST 4 VLAN 1 сопоставлен с MSTI 1, VLAN 2 сопоставлен с MSTI 2, а другие VLAN сопоставлены с MSTI 3.
- Общее связующее дерево (CST) соединяет все регионы MST в коммутаторной сети. Если каждый регион MST считается единым узлом, то CST - это связующее дерево, вычисленное при помощи протоколов STP или RSTP.
- Внутреннее связующее дерево (IST) располагается внутри региона MST. IST - это особое дерево MSTI с идентификатором 0.
- Единственное связующее дерево (SST) образуется, когда коммутатор с работающим STP или RSTP относится только к одному связующему дереву или когда в регионе MST только один коммутатор.
- Деревья IST всех регионов MST вместе с CST образуют полное связующее дерево, то есть CIST.
- Корни региона классифицируются на внутренние связующие деревья и корни региона MSTI.
  - На рисунке 1 наиболее близкими к корню CIST коммутаторами являются корни региона IST.
  - Регион MST может содержать множество связующих деревьев, каждое из которых называется MSTI. Корень региона MSTI - это корень MSTI. На рисунке 3 у каждого MSTI есть собственный корень региона.
- Корень CIST - это корневой мост CIST. S1 на рисунке 1 - корень CIST.
- Ведущие мосты, также известные как главные IST - это ближайшие к корню CIST коммутаторы. Оранжевые коммутаторы на рисунке 1 - это ведущие мосты. Если корень CIST находится в регионе MST, данный корень является ведущим мостом региона.
- Роль порта: MSTP, также как RSTP, определяет порт корня, назначенный, альтернативный,

резервный и граничный порты.

- Статус порта: MSTP, также как RSTP, определяет статус порта: переадресация (forwarding), самообучение (learning) и запрет получения данных (discarding).

Вычисление топологии MSTP

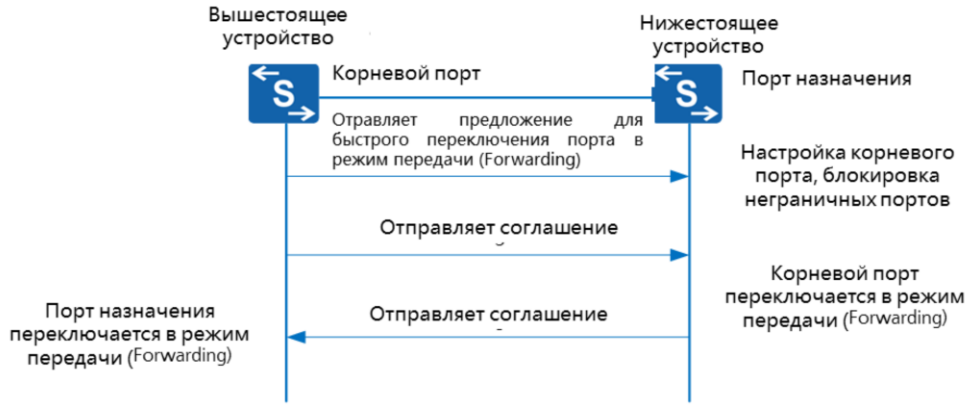
- Вычисление CIST
  - После сравнения BPDU коммутатор с наивысшим приоритетом во всей сети избирается корнем CIST. MSTP вычисляет IST для каждого региона MST, рассматривая каждый регион MST как единое устройство, и вычисляет CST для подключения регионов MST. CST и деревья IST образуют CIST для всей сети.
- Вычисление MSTI
  - В регионе MST протокол MSTP независимо вычисляет MSTI для каждой сети VLAN на основе соответсвий между VLAN и MSTI. Процесс вычисления похож на процесс, используемый STP для вычисления связующего дерева.
- Отклик MSTP на изменения топологии
  - MSTP откликается на изменения топологии похожим на отклик RSTP образом.

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- Свойства MSTI
  - Связующее дерево независимо вычисляется для каждого MSTI
  - Схожим с STP образом.
  - Связующие деревья MSTI могут иметь разные корни и топологии.
  - Каждое дерево MSTI отправляет пакеты BPDU по своему связующему дереву.
  - Топология каждого MSTI определяется при помощи команд.
  - Параметры связующего дерева для порта могут различаться в зависимости от разных MSTI.
  - Одному порту могут быть назначены разные роли или статусы для разных MSTI.
- В сети MSTP пакеты VLAN пересылаются следующим образом:
  - По MSTI в регионе MST
  - По CST между регионами MST

Быстрый переход в MSTP

- Протокол MSTP поддерживает стандартный и продвинуты механизмы предложения и соглашения (Proposal/Agreement, P/A).



Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- Как указано на рисунке выше, механизм P/A в MSTP работает следующим образом:
  1. Вышестоящее устройство отправляет пакет предложения BPDU нижестоящему устройству с указанием порту подключения нижестоящего устройства включиться в режим передачи (Forwarding). После получения данного BPDU нижестоящее устройство назначает порт подключения с вышестоящим устройством корневым и блокирует все не граничные порты.
  2. Вышестоящее устройство отправляет пакет BPDU соглашения. По получении данного BPDU корневой порт нижестоящего устройства переключается в режим передачи (Forwarding).
  3. Нижестоящее устройство отправляет пакет BPDU соглашения. После получения данного BPDU вышестоящее устройство назначает порт подключения с нижестоящим устройством портом назначения, порт переключается в режим передачи (Forwarding).
- По умолчанию коммутаторы Huawei используют быстрое переключение в продвинутом механизме P/A. Для соединения коммутатора Huawei с устройством стороннего производителя, которое использует быстрое переключение в стандартном механизме P/A, настройте стандартный механизм P/A на коммутаторе Huawei.

Настройка MSTP

- Настройка основных функций MSTP

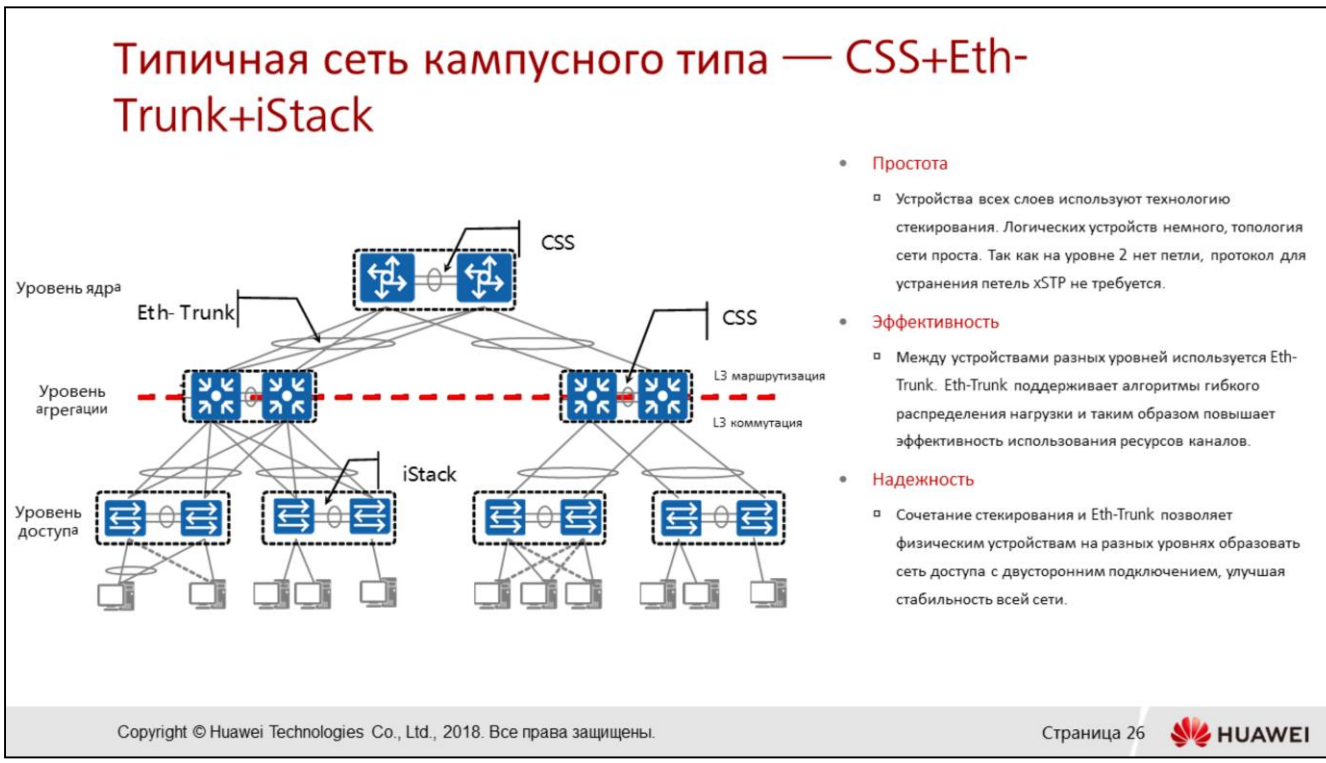
```
[SwitchA] stp region-configuration
\\Enters the MST region view.
[SwitchA-mst-region] region-name RG1
\\Configures a name for the MST region.
[SwitchA-mst-region] instance 1 vlan 2 to 10
\\Configures mappings between MSTIs and VLANs.
[SwitchA-mst-region] instance 2 vlan 11 to 20
[SwitchA-mst-region] active region-configuration
\\Activates the MST region configurations to make the domain name, VLAN mapping table, and MSTP revision level
take effect.
[SwitchA] stp instance 1 root primary
\\Configures the device as the root bridge for MSTI 1.
[SwitchA] stp instance 2 root secondary
\\Configures the device as the secondary root bridge for MSTI 2.
[SwitchA] stp pathcost-standard legacy
# Configures SwitchA to use Huawei's proprietary algorithm to calculate the path cost.
[SwitchA] stp enable
\\Enables MSTP on SwitchA.
```

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

Содержание

1. **Таблица MAC-адресов**
2. Самообращенный запрос ARP
3. MSTP
4. **Умное стекирование iStack**
   - Типичная сеть кампусного типа
   - Основы iStack
5. CSS
6. Eth-Trunk

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.



- На рисунке выше показана простая, эффективная и высоконадежная сеть кампусного типа CSS+iStack
- Простота
  - Устройства всех слоев используют технологию стекирования. Логических устройств немного, топология сети проста. Так как на уровне 2 нет петли, протокол для устранения петель xSTP не требуется.
- Эффективность
  - Между устройствами разных уровней используется Eth-Trunk. Eth-Trunk поддерживает алгоритмы гибкого распределения нагрузки и таким образом повышает эффективность использования ресурсов каналов.
- Надежность
  - Для увеличения надежности серверы и хосты можно настраивать с использованием функции распределения нагрузки на базе множественной агрегации каналов или активных и резервных каналов.
  - Сочетание стекирования и Eth-Trunk позволяет физическим устройствам на разных уровнях образовать сеть доступа с двусторонним подключением, улучшая стабильность всей сети.
- Недостатки
  - Высокие требования к производительности устройства. При наличии большого количества коммутаторов с фиксированной конфигурацией в стеке производительность главной платы

ведущего коммутатора может значительно уменьшиться.

- Занятость ресурсов сервисных портов при их использовании для стекирования или CSS.



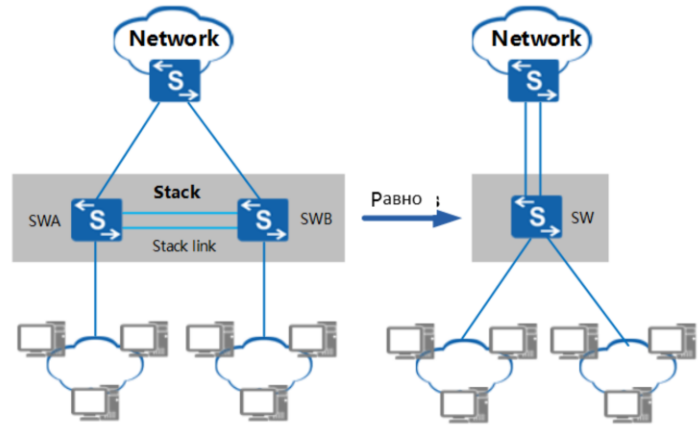
Содержание

1. Таблица MAC-адресов
2. Самообращенный запрос ARP
3. MSTP
4. **Умное стекирование iStack**
   - Типичная сеть кампусного типа
   - Основы iStack
5. CSS
6. Eth-Trunk

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

Стекирование устройств - iStack

- Умное стекирование (iStack) позволяет нескольким стековым коммутаторам работать как один логический коммутатор. На рисунке справа коммутатор A (SWA) и коммутатор B (SWB) после подключения стековыми кабелями и образования стека считаются единым устройством вышестоящими и нижестоящими устройствами.



Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

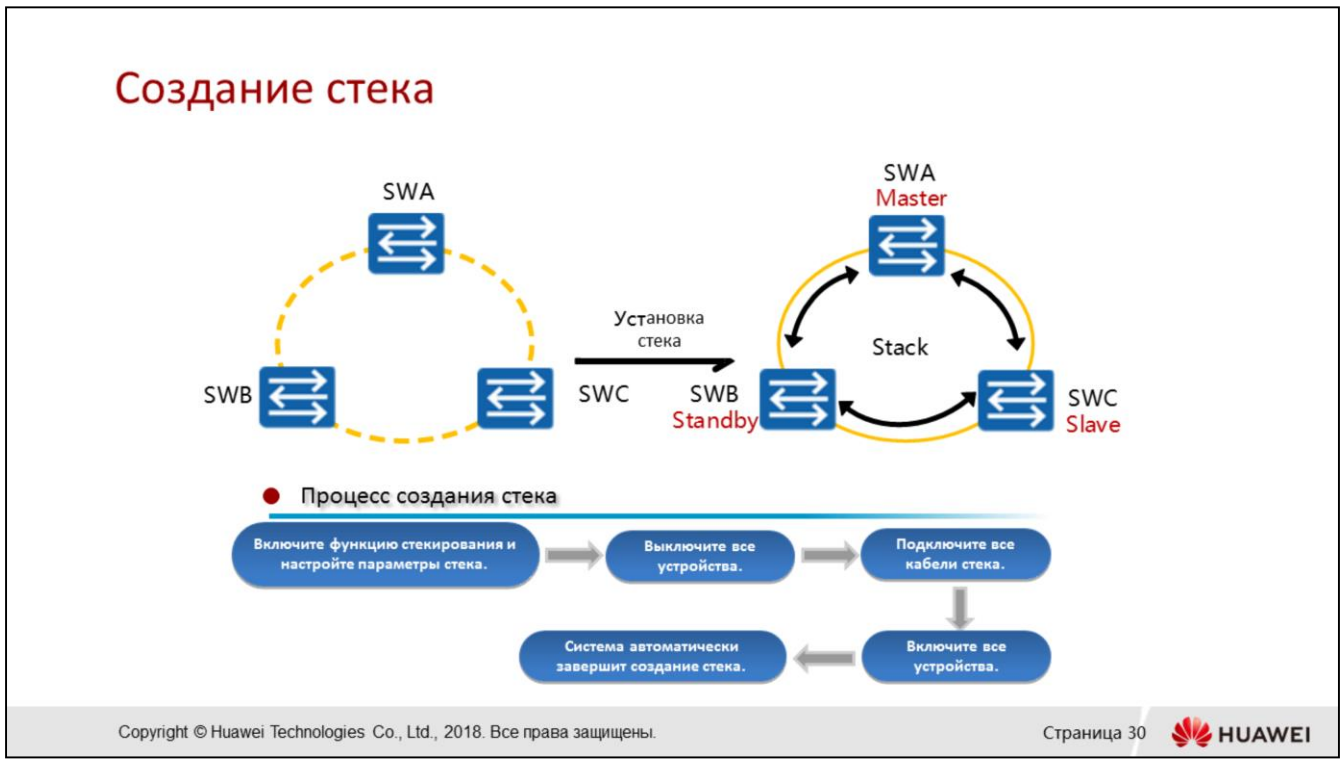
HUAWEI

- Стекирование увеличивает надежность и возможность масштабирования сети, упрощая при этом управление ею.
  - Высокая надежность Коммутаторы-элементы стека работают в режиме резервирования. При помощи агрегации каналов между устройствами возможно применить резервирование каналов.
  - Высокая масштабируемость. Количество интерфейсов, полосу частот и вычислительную мощность стека можно повысить, добавляя коммутаторы. Коммутатор можно подключить или отключить к стеку без влияния на другие коммутаторы стека. Новые коммутаторы автоматически синхронизируют файлы конфигурации и версии системного ПО с ведущим коммутатором.
  - Упрощенные управление и настройка. Для централизованного управления и настройки всех коммутаторов в стеке к нему можно подключиться с любого из коммутаторов-элементов. Кроме того, в целях упрощения конфигурации сети, после установки коммутатора в стек сложные протоколы по предотвращению петель на уровне 2 или протоколы защитной коммутации уровня 3 не требуются.

Основные понятия iStack

- Роли
  - Подключенные к стеку коммутаторы называются устройствами-элементами. Устройства-элементы стека могут выполнять одну из следующих ролей:
    - Ведущий коммутатор. Ведущий коммутатор управляет всем стеком. У стека может быть только один ведущий коммутатор.
    - Резервный коммутатор. Резервный коммутатор действует как запасной вариант ведущего коммутатора. Если ведущий коммутатор выходит из строя, резервный коммутатор принимает управление всеми службами и роль ведущего коммутатора. У стека может быть только один резервный коммутатор.
    - Ведомый коммутатор. Ведомый коммутатор пересылает служебный трафик. Большое количество ведомых коммутаторов увеличивает производительность пересылки трафика стека. Все коммутаторы в стеке, кроме ведущего и резервного, являются ведомыми.
- Идентификатор в стеке
  - Идентификатор в стеке определяет устройство-элемент стека и является идентификатором слота. Каждому устройству-элементу должен быть назначен уникальный идентификатор в стеке.
- Приоритет в стеке
  - Приоритет в стеке определяет роль устройства-элемента стека при назначении ролей. Более высокий приоритет в стеке увеличивает вероятность назначения устройства-элемента стека ведущим.

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.



- Последний шаг «Система автоматически завершит создание стека» включает три следующих этапа:
  1. Выбор ведущего коммутатора
     ① Сравнивается рабочий статус коммутаторов. Уже работающий коммутатор имеет преимущество перед только запускающимся коммутатором при выборе ведущего коммутатора.
     ② Если несколько коммутаторов запускаются в одно и то же время, коммутатор с наивысшим приоритетом в стеке становится ведущим.
     ③ Если несколько коммутаторов запускаются в одно и то же время и у них одинаковый приоритет в стеке, коммутатор с наименьшим MAC-адресом становится ведущим.
  2. Сбор данных о топологии и выбор резервного коммутатора
     - После выбора ведущего коммутатора он собирает данные о топологии со всех остальных коммутаторов-элементов, вычисляет передаваемые данные и интерфейсы для блокировки, высылает полученные данные коммутаторам-участникам и назначает им идентификаторы в стеке. Как запасной вариант ведущего коммутатора выбирается резервный коммутатор. Резервный коммутатор выбирается по следующим правилам: Если все коммутаторы, за исключением ведущего, включаются в одно и то же время:
       - Коммутатор с наивысшим приоритетом в стеке становится резервным коммутатором.
       - Если у нескольких коммутаторов одинаковый приоритет в стеке, коммутатор с наименьшим MAC-адресом становится резервным.
  3. Стабильная работа
- После назначения ролей и сбора данных о топологии остальные коммутаторы добавляются в стек в качестве ведомых. Они автоматически синхронизируют версии системного ПО и файлы конфигурации с ведущим коммутатором.
  - Стек поддерживает автоматическую загрузку новых версий ПО. Коммутаторы на очереди в стек могут управляться разными версиями ПО и могут создавать отдельный стек при условии совместимости друг с другом. При несоответствии версий ПО ведущего, резервного и ведомых коммутаторов резервный и ведомые коммутаторы автоматически загружают системное ПО с ведущего, перезагружаются с установкой новой версии и автоматически переподключаются к стеку.
  - Стек поддерживает синхронизацию файлов конфигурации. Для обеспечения работы всех коммутаторов как единого устройства и стабильной работы остальных коммутаторов в случае выхода из строя ведущего коммутатора на резервный и ведомые коммутаторы загружается и запускается файл конфигурации ведущего коммутатора.

Режимы стекирования

- Коммутаторы могут подключаться к стеку при помощи плат стека или сервисных портов.
  - Платы стека могут быть использованы одним из указанных способов:
    - Для соединения коммутаторов при помощи плат стека используются стековые кабели.
    - Карты стека встроены в задние панели коммутаторов, коммутаторы подключаются при помощи встроенных кабелей или портов стека.
  - При использовании сервисных портов для подключения к стеку платы стека не требуются. Сервисные порты - это физические порты, которые настраиваются как порты-участники стека и группируются в логический порт стека, как показано на рисунке ниже. Коммутаторы подключаются при помощи физических портов.



Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- Физический порт-элемент
  - Физический порт-элемент - это сервисный порт, используемый для подключения коммутаторов-элементов стека. Физические порты-элементы пересылают пакеты или протоколы пакетов стека между коммутаторами-элементами.
- Логический порт стека
  - Логический порт стека используется исключительно для стекирования и состоит из сгруппированных портов-участников. Каждый коммутатор-элемент стека поддерживает два порта стека: порт стека *n*/1 и порт стека *n*/2, где *n* обозначает идентификатор коммутатора-элемента в стеке.
- Соединения сервисных портов делятся на стандартные и выделенные в зависимости от типов кабеля.
  - Стандартное кабельное соединение
    - Стандартные стековые кабели включают оптические, сетевые и высокоскоростные кабели. Когда для подключения стека используются стандартные кабели, необходимо вручную настроить логические порты стека. В ином случае создание стека невозможно.
  - Выделенное кабельное соединение
    - У кабеля для выделенного соединения два наконечника: ведущий с прикрепленным ярлыком и ведомый без ярлыка. Коммутаторы могут автоматически создать стек после подключения при помощи кабеля для выделенного соединения согласно

правилам.

Подключение коммутатора к стеку

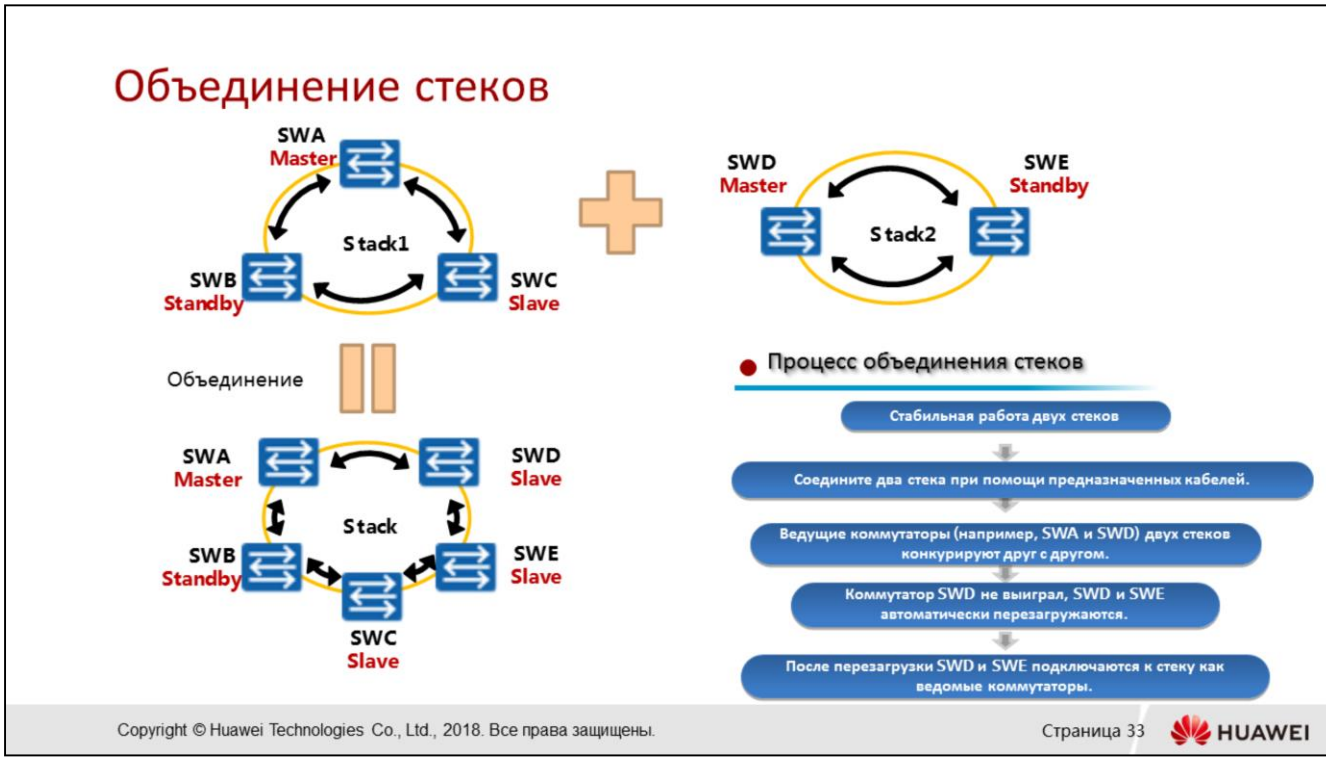




Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

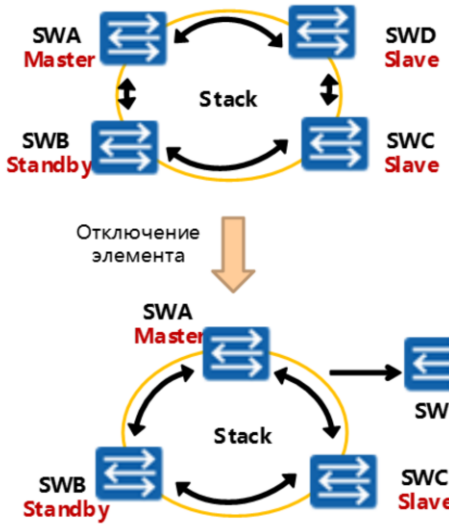
- Подключение коммутатора к стеку подразумевает подключение коммутатора к стабильному стеку. В процессе выполняются следующие шаги:
- Включите функцию стекирования и настройте параметры SWD.
  - Если для стекирования используются сервисные порты, физические порты добавляемого коммутатора должны быть добавлены к логическому порту стека в качестве портов-элементов. Если у стека линейная топология, выполните настройку на обоих (или одном) конце цепи.
  - Если для стекирования используются платы стека, на добавляемом коммутаторе необходимо включить функцию стекирования.
  - Для удобства управления устройствами назначьте новому коммутатору-элементу идентификатор в стеке. Если новому коммутатору-элементу не присвоен идентификатор в стеке, ведущий коммутатор автоматически его присвоит.
- Подключите SWD к стеку.
  - Если у стека линейная топология, добавьте новый коммутатор на любом конце топологии для того, чтобы минимизировать влияние на выполняемые услуги.
  - Если у стека кольцевая топология, необходимо разорвать физическое соединение, чтобы изменить топологию на линейную, а после добавить новый коммутатор на любом конце цепи. После этого по необходимости подключите коммутаторы на двух концах, чтобы они сформировали кольцо.
- Система автоматически завершит создание стека.
  1. После подключения коммутатора к стеку и его включения он избирается ведомым. Роли остальных коммутаторов в стеке остаются неизменными.
  2. Ведущий коммутатор обновляет информацию о топологии стека, синхронизирует информацию о топологии с остальными коммутаторами-элементами, назначает идентификатор в стеке новому коммутатору-элементу (в случае, если идентификатор в стеке новому коммутатору не назначен или назначенный идентификатор конфликтует с уже существующим).
  3. Новый коммутатор-элемент обновляет данные о своем идентификаторе в стеке и

синхронизирует файл конфигурации и системное ПО с ведущим коммутатором. Коммутатор работает стабильно.



- Объединение стеков подразумевает объединение двух стабильно работающих стеков в один. На предыдущем рисунке ведущие коммутаторы двух стеков SWA и SWE конкурируют друг с другом за роль ведущего коммутатора в новообразованном стеке. После избрания SWA новым ведущим коммутатором роли, конфигурации и службы коммутаторов-элементов его стека остаются неизменными. SWD, SWE и другой стек, напротив, перезапускаются и подключаются к новому стеку как ведомые коммутаторы. Ведущий коммутатор SWA присваивает новые идентификаторы в стеке устройствам SWD и SWE. SWD и SWE автоматически синхронизируют файлы конфигурации и версии системного ПО с ведущим коммутатором. Во время данного процесса службы, выполняемые SWD и SWE, прерываются.
- Объединение стеков происходит в одной из нижеприведенных ситуаций:
  - Разделение стека из-за сбоя связи или коммутатора-элемента. После восстановления связи или работы коммутатора-элемента разделенные стеки заново объединяются в один.
  - После включения функции стекирования на добавляемом к стеку коммутаторе включенный коммутатор подключается к работающему стеку при помощи стекового кабеля. Использование данного метода для подключения коммутатора к стеку не рекомендуется, так как работающий стек может перезагрузиться во время процесса объединения, что может повлиять на работу сервисов.

Удаление коммутатора-элемента из стека



Обстоятельства удаления коммутатора-элемента из стека

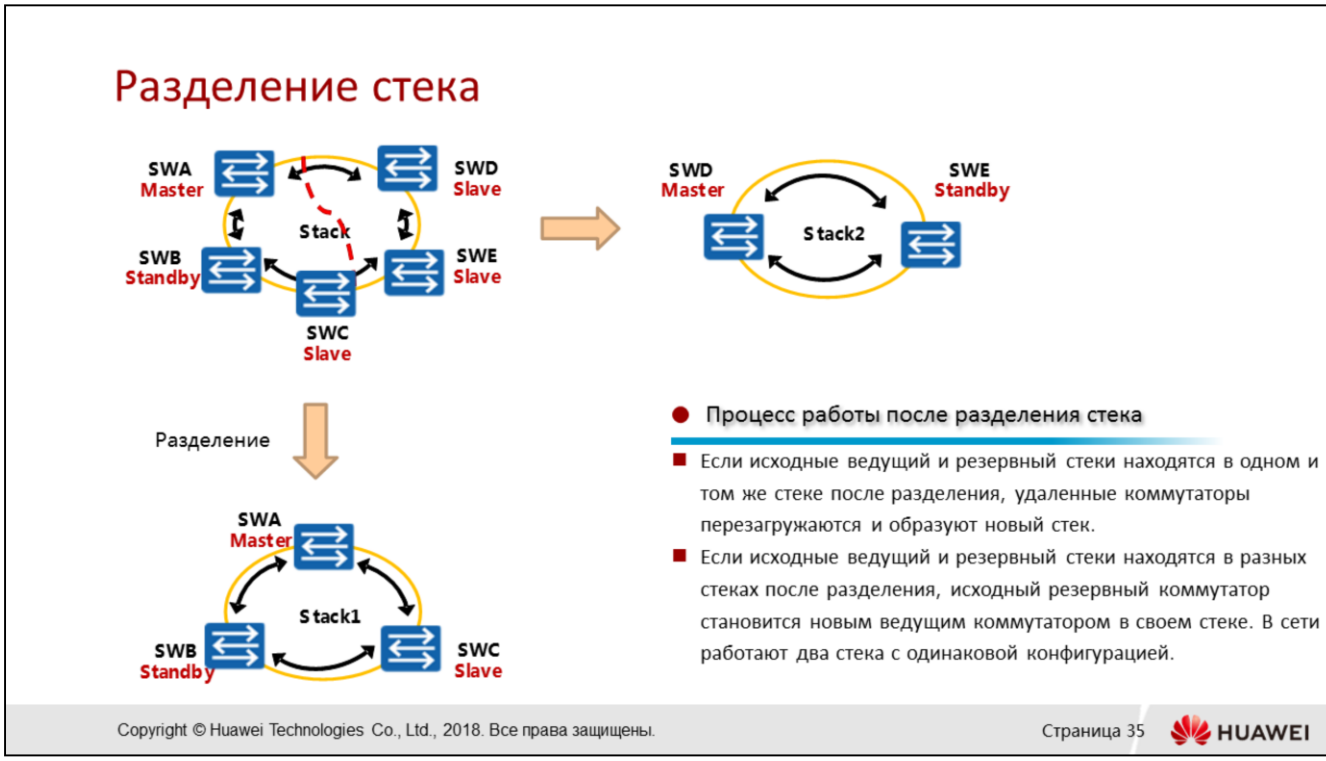
- Отключение стекового кабеля.
- Отключение соответствующего порта стека или физического порта-элемента.
- Перезагрузка коммутатора-элемента.
- Сбой работы коммутатора-элемента.

Процесс удаления коммутатора-элемента

- При удалении ведущего коммутатора новым ведущим коммутатором становится резервный. После этого стек обновляет топологию и продолжает работу.
- При удалении резервного коммутатора стек выбирает другой резервный коммутатор. После этого стек обновляет топологию и продолжает работу в штатном режиме.
- При удалении ведомого коммутатора стек обновляет топологию и продолжает работу.

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

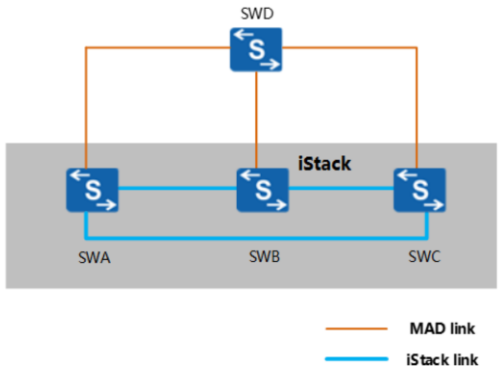
- Удаление коммутатора-элемента обозначает отключение коммутатора от стека. В зависимости от роли удаляемого коммутатора-элемента в стеке происходит следующее:
  - При удалении ведущего коммутатора новым ведущим коммутатором становится резервный. Новый ведущий коммутатор производит пересчет информации о топологии стека, синхронизирует обновленную информацию о топологии с другими коммутаторами-элементами и избирает новый резервный коммутатор. Затем стек продолжает стабильную работу.
  - При удалении резервного коммутатора ведущий коммутатор выбирает новый резервный коммутатор, производит пересчет информации о топологии стека и синхронизирует обновленную информацию о топологии с другими коммутаторами-элементами. Затем стек продолжает стабильную работу.
  - При удалении ведомого коммутатора ведущий коммутатор производит пересчет информации о топологии стека и синхронизирует обновленную информацию о топологии с другими коммутаторами-элементами. Затем стек продолжает стабильную работу.
- Коммутатор-элемент удаляется из стека после отключения соответствующих стековых кабелей и извлечения из стека. При удалении коммутатора-элемента обратите внимание на следующее:
  - После удаления коммутатора-элемента из стека с кольцевой топологией для надежной работы сети при помощи стекового кабеля подключите два порта, к которым был подключен удаленный коммутатор.
  - В линейной топологии удаление промежуточного коммутатора вызывает разделение стека. Перед удалением проанализируйте влияние на работу сервисов.



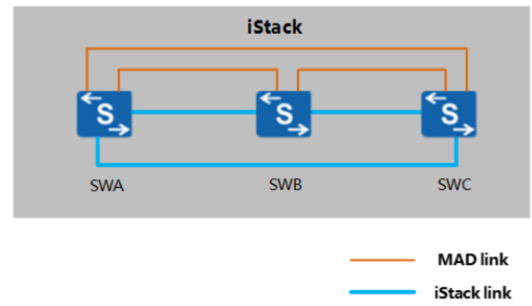
- Разделение стека подразумевает разделение одного стека на несколько в результате удаления включенных коммутаторов-элементов из стека или в результате многочисленных сбоев работы кабелей стека. В зависимости от того, находятся ли ведущий и резервный коммутаторы в одном и том же стеке после разделения, роли коммутаторов распределяются одним из следующих способов:
    - Сценарий, при котором исходные ведущий и резервный коммутаторы находятся в одном и том же стеке после разделения. Исходный ведущий коммутатор производит пересчет информации о топологии стека после удаления данных о топологии удаленных коммутаторов-элементов, синхронизирует обновленную информацию о топологии с другими коммутаторами-элементами. Когда удаленные коммутаторы-элементы обнаруживают истечение срока задержки тайм-аута пакетов протоколов, они перезапускаются и выбирают новый ведущий коммутатор.
    - Сценарий, при котором исходные ведущий и резервный коммутаторы находятся в разных стеках после разделения. Исходный ведущий коммутатор выбирает новый резервный коммутатор в своем стеке, производит пересчет информации о топологии стека и синхронизирует обновленную информацию о топологии с другими коммутаторами-элементами. Исходный резервный коммутатор становится новым ведущим коммутатором в своем стеке, производит пересчет информации о топологии стека, синхронизирует обновленную информацию о топологии с другими коммутаторами-элементами и избирает новый резервный коммутатор.

Обнаружение нескольких активных узлов (MAD). Прямой режим

- В прямом режиме устройства-элементы могут напрямую подключаться либо к промежуточному устройству, либо друг к другу по принципу «каждый с каждым»:



Подключение напрямую к промежуточному устройству



Подключение к другим устройствам по принципу «каждый с каждым»

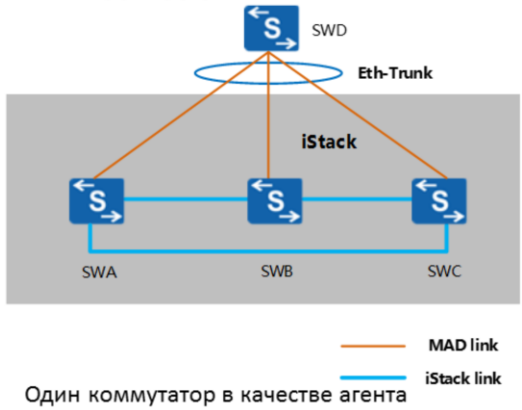
Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- Все коммутаторы-элементы стека используют один и тот же IP-адрес и MAC-адрес (MAC-адрес стека). После разделения стека два и более стека могут использовать одинаковые IP- и MAC-адреса. Во избежание сбоя сети в результате данного сценария требуется механизм проверки на конфликт IP- и MAC-адресов после разделения. Обнаружение нескольких активных узлов (MAD) - это протокол обнаружения разделений стека и работы с ними. При разделении стека в результате сбоя канала MAD осуществляет обнаружение разделения, работу с несколькими активными узлами и запускает механизмы восстановления после сбоя для сокращения воздействия разделения стека на сервисы до минимума.
- MAD может осуществляться в прямом режиме или режиме ретрансляции. Прямой режим и режим ретрансляции не могут быть одновременно сконфигурированы в одном и том же стеке.
- В прямом режиме устройства-элементы отдают предпочтение выделенным каналам MAD, а не стандартным сетевым кабелям. При работе в штатном режиме коммутаторы-элементы не отправляют пакеты MAD. После разделения стека каждый коммутатор-элемент посылает пакет MAD каждую секунду по каналу MAD для проверки наличия более одного ведущего коммутатора.
- Подключение напрямую к промежуточному устройству. У каждого коммутатора-элемента есть по меньшей мере одно подключение по каналу MAD с промежуточным устройством.
- Подключение к другим устройствам по принципу «каждый с каждым». В топологии с подключением по принципу «каждый с каждым» между любыми двумя коммутаторами-участниками есть по меньшей мере одно подключение по каналу MAD.
- Использование промежуточных устройств позволяет сократить каналы MAD между коммутаторами-участниками. Топология применима к стекам с большим расстоянием между коммутаторами-элементами. Подключение по принципу «каждый с каждым» предотвращает сбои, вызванные сбоями промежуточных устройств, но такое подключение требует занять множество интерфейсов

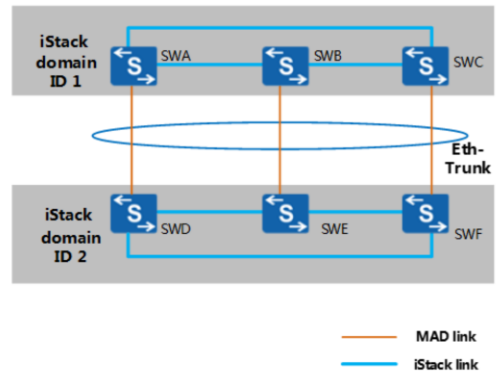
коммутаторов-участников. Таким образом, данная топология применима к стекам с небольшим количеством коммутаторов-элементамов.

Обнаружение нескольких активных узлов (MAD). Режим ретрансляции

- Режим ретрансляции может осуществляться двумя способами: агентом ретрансляции MAD может выступать один коммутатор или два стека могут выступать агентами ретрансляции MAD друг другу.



Один коммутатор в качестве агента ретрансляции MAD



Два стека в качестве агентов ретрансляции MAD друг другу

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- В режиме ретрансляции обнаружение ретрансляции MAD сконфигурировано в интерфейсе Eth-Trunk стека, функция обнаружения MAD агента включена. Каждый коммутатор-элемент должен быть подключен к агенту, в ином случае эти каналы должны быть добавлены в Eth-Trunk. В отличие от прямого режима, режим ретрансляции не требует подключения по дополнительным интерфейсам, так как интерфейс Eth-Trunk может выполнять другие функции при включенном режиме обнаружения ретрансляции MAD.
- В режиме ретрансляции при работе в штатном режиме коммутаторы-элементы отсылают пакеты MAD с интервалом в 30 сек. по каналам MAD и не обрабатывают полученные пакеты MAD. После разделения стека каждый коммутатор-элемент посылает пакет MAD каждую секунду по каналу MAD для проверки наличия более одного ведущего коммутатора.
- Работа с несколькими активными узлами
  - После разделения стека механизм MAD переводит новые стеки в состояние обнаружения (Detect) или восстановления (Recovery). Стек в состоянии обнаружения (Detect) продолжает работать, в то время как стек в состоянии восстановления (Recovery) отключается.
  - В случае обнаружения нескольких активных узлов MAD действует следующим образом: При обнаружении нескольких стеков в состоянии обнаружения (Detect) механизмом обнаружения разделений стеки конкурируют между собой для сохранения состояния обнаружения. Стеки, не выдержавшие конкуренции, входят в состояние восстановления (Recovery), все физические порты коммутаторов-элементов данных стеков, кроме зарезервированных, отключаются. Стеки в состоянии восстановления (Recovery) не отправляют сервисных пакетов.
- Восстановление после сбоя MAD
- После восстановления неисправного канала стеки объединяются одним из следующих способов:
  - Стек в состоянии восстановления (Recovery) перезагружается и объединяется со стеком в состоянии обнаружения (Detect), отключенные сервисные порты восстанавливаются до включенного состояния (Up). Весь стек восстанавливается.
  - Если стек в состоянии обнаружения (Detect) выходит из строя до восстановления канала, возможно удалить этот стек из сети и командой запустить стек в состоянии восстановления

(Recovery) для направления сервисного трафика последнему. Затем проходит устранение неисправностей стека и канала. После восстановления стека в режиме обнаружения (Detect) его возможно объединить с другим стеком.

Конфигурация стека

- Создание стека при помощи платы стека

```
[SwitchA] stack slot 0 priority 200
\\Configures a stack priority for SwitchA. By default, the stack priority of a member switch is 100.
[SwitchB] stack slot 0 renumber 1
\\Configures a stack ID for SwtichB.
[SwitchC] stack slot 0 renumber 2
```

- Создание стека при помощи платы стека.

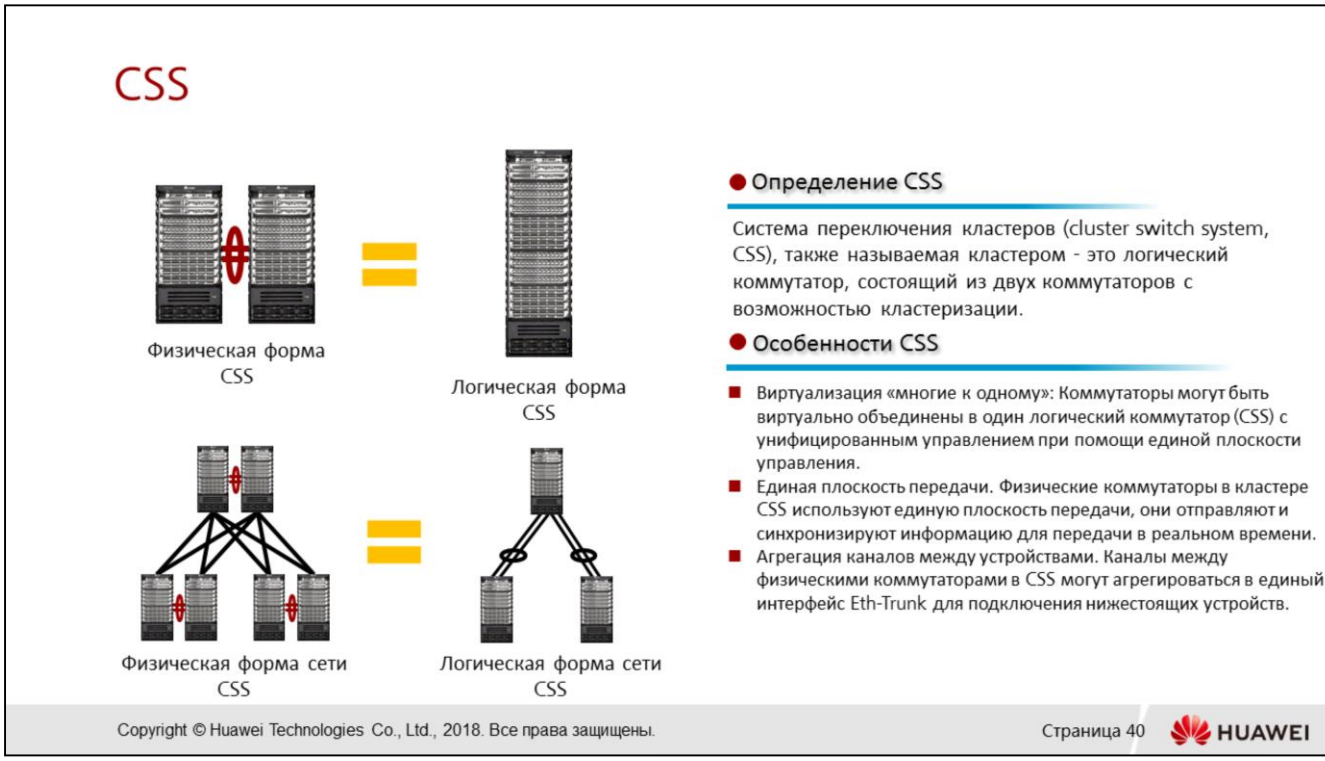
```
[SwitchA] interface stack-port 0/1
[SwitchA-stack-port0/1] port interface gigabitethernet 0/0/27 enable
\\Configures a physical port as a service port and adds it to a logical stack port. Perform similar operations on SwitchB and SwitchC.
[SwitchA] interface stack-port 0/2
[SwitchA-stack-port0/2] port interface gigabitethernet 0/0/28 enable
[SwitchA] stack slot 0 priority 200
\\Sets the stacking priority of SwitchA to 200.
[SwitchB] stack slot 0 renumber 1
\\Sets the stacking ID of SwitchB to 1.
[SwitchC] stack slot 0 renumber 2
```

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

Содержание

1. Таблица MAC-адресов
2. Самообращенный запрос ARP
3. MSTP
4. Умное стекирование iStack
5. **CSS**
6. Eth-Trunk

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.



- Разница между CSS и iStack состоит в том, что CSS является стеком модульных коммутаторов, в то время как в iStack включены неконфигурируемые коммутаторы. У данных систем разные названия и уникальные методы реализации, но они выполняют схожие функции.
- Кроме высокой скорости передачи, технология CSS обеспечивает надежность и масштабируемость сети при упрощенном управлении.
    - Высокая надежность. Коммутаторы-элементы CSS работают в режиме резервирования. При помощи агрегации каналов между шасси возможно применить резервирование каналов.
    - Высокая масштабируемость. Для увеличения количества портов, ширины полосы пропускания и способности обработки пакетов коммутаторы могут образовать CSS.
    - Упрощенные настройки и управление. После образования CSS двумя коммутаторами они виртуализируются в единый коммутатор. В систему CSS можно войти и управлять ею с любого из коммутаторов-элементов.

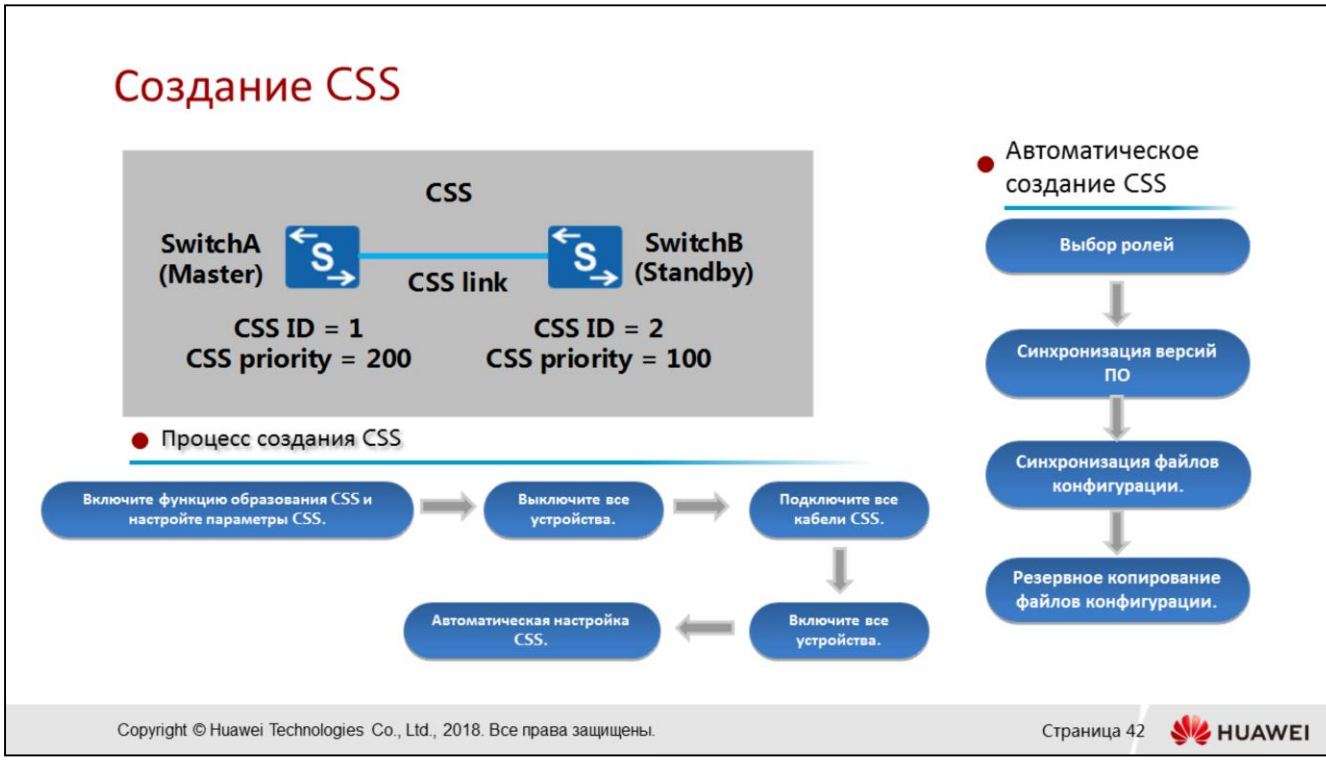
Основные понятия CSS

- Ведущий коммутатор
  - Управляет всей CSS. У CSS может быть только один ведущий коммутатор.
- Резервный коммутатор
  - Резервный коммутатор действует как запасной вариант ведущего коммутатора. Если ведущий коммутатор выходит из строя, резервный коммутатор принимает управление всеми службами и роль ведущего коммутатора CSS. У CSS может быть только один ведущий коммутатор.
- Идентификатор в CSS
  - Идентификатор в CSS используется для идентификации и управления коммутатором-элементом CSS. У каждого коммутатора-элемента CSS есть свой идентификатор.
- Приоритет в CSS
  - Приоритет в CSS определяет роль элемента CSS при распределении ролей. Более высокий приоритет в CSS увеличивает вероятность назначения устройства-элемента стека ведущим.

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

HUAWEI

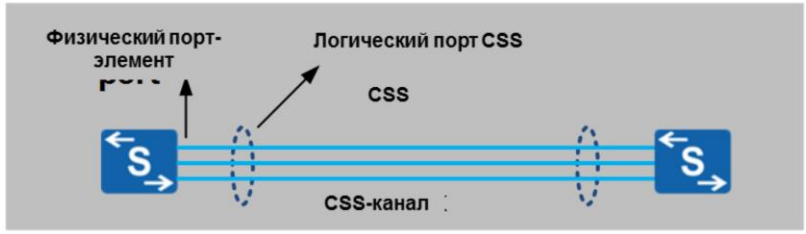
- В отличие от системы iStack, которая позволяет стекирование множества коммутаторов, в CSS есть только один ведущий и один резервный коммутаторы.



- После подключения двух коммутаторов при помощи кабелей кластера, включения функции CSS и перезагрузки CSS создается автоматически. Коммутаторы-элементы затем обмениваются пакетами данных для соревнования выбора ролей. Во время соревнования один коммутатор становится ведущим для управления CSS, а второй - резервным.
- Выбор ролей
    1. Запущенный первым коммутатор с включенным режимом CSS с одним шасси становится ведущим коммутатором.
    2. Если оба коммутатора запускаются в одно и то же время, коммутатор с наивысшим приоритетом в CSS становится ведущим.
    3. Если оба коммутатора запускаются в одно и то же время и у них одинаковый приоритет в CSS, коммутатор с наименьшим MAC-адресом становится ведущим.
    4. Если оба коммутатора запускаются в одно и то же время и имеют одинаковые MAC-адреса, коммутатор с наименьшим идентификатором в CSS становится ведущим.
- Синхронизация версий ПО
    - Технология CSS предусматривает автоматизированный механизм загрузки ПО. Коммутаторы могут управляться разными версиями ПО и могут создавать CSS при условии совместимости версий ПО. При несоответствии версий ПО резервного и ведущего коммутаторов резервный коммутатор автоматически загружает системное ПО с ведущего, перезагружаются с установкой новой версии и автоматически переподключается к CSS.
- Синхронизация файлов конфигурации.
    - Технология CSS использует строгий механизм синхронизации файлов конфигурации. Данный механизм обеспечивает функционирование коммутаторов-элементов CSS как единого коммутатора.
- Резервное копирование файлов конфигурации.
    - После включения функции CSS на коммутаторе он автоматически добавляет расширение .bak к исходному названию файла конфигурации и проводит его резервное копирование. Таким образом, коммутатор может вернуться к исходным настройкам при выключении функции CSS. Например, если расширение исходного файла конфигурации - .cfg, то расширением резервной копии файла конфигурации станет .cfg.bak. Для возврата к исходной конфигурации коммутатора после отключении функции CSS необходимо удалить .bak из названия файла конфигурации, изменить файл конфигурации без расширения .bak для следующего запуска и перезапустить коммутатор.

Режимы соединения CSS

- Коммутаторы могут образовать CSS при помощи CSS-плат или сервисных портов.
  - В режиме подключения при помощи CSS-плат коммутаторы подключаются при помощи выделенных CSS-плат и кабелей CSS в MPU.
  - В режиме подключения при помощи сервисных портов коммутаторы подключаются при помощи стандартных сервисных портов на сервисных платах, без применения CSS-плат. Подобно iStack, режим подключения при помощи портов требует двух типов портов: физических портов-элементов и логических портов CSS.



Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- Физический порт-элемент.
  - Физический порт-элемент - это сервисный порт, необходимый для образовании канала CSS между коммутаторами-элементами CSS. Физические порты-элементы пересылают пакеты или протоколы пакетов CSS между коммутаторами-элементами.
- Логический порт CSS.
  - Логический порт CSS используется исключительно для образования CSS и состоит из сгруппированных портов-участников. Каждый порт-элемент CSS поддерживает не более двух логических портов CSS.



- Один коммутатор с включенной функцией CSS считается CSS с одним шасси.
- В работающую систему CSS с одним шасси можно подключить коммутатор. Как показано на рисунке справа, коммутатор SwitchA образет CSS с одним шасси. После подключения SwitchB к CSS два коммутатора образуют новую CSS. Коммутатор SwitchA становится ведущим, а коммутатор SwitchB становится резервным.
- Коммутатор подключается к CSS с одним шасси в одном из описанных ниже сценариев:
  - После включения функции CSS и перезапуска одного коммутатора данный коммутатор переходит в режим CSS с одним шасси. После включения функции CSS и перезапуска другого коммутатора он подключается к CSS в качестве резервного.
  - Во включенной CSS с двумя шасси после перезапуска одного из коммутаторов он заново подключается к CSS в качестве резервного.
- Две CSS с одним шасси могут быть объединены в одну CSS. На рисунке справа показано, как две CSS с одним шасси объединяются в одну и выбирают ведущий коммутатор. Ведущий коммутатор оставляет исходную конфигурацию, но его MPU возвращает исходные настройки без влияния на работу служб. Резервный коммутатор перезапускается, подключается к новой CSS в качестве резервного и синхронизирует файл конфигурации с файлом ведущего коммутатора. Работа запущенных на этом коммутаторе служб прерывается.
- Объединение CSS происходит в одной из нижеприведенных ситуаций:
  - После настройки двух коммутаторов с включенной функцией CSS они запускаются как две CSS с одним шасси. После подключения их друг к другу при помощи кабелей кластера такие коммутаторы объединяются в одну CSS.

- CSS разделяется при неисправности канала или коммутатора-элемента CSS. После восстановления работы канала или элемента две CSS с одним шасси объединяются в одну.

Разделение CSS

- После образования CSS ведущий и резервный MPU системы CSS периодически обмениваются heartbeat-пакетами для поддержания статуса CSS. При неисправности кабеля кластера, платы CSS MPU, при выключении или перезагрузке одного из коммутаторов, соединение между коммутаторами прерывается. При истечении срока таймаута heartbeat-пакета (8 сек.), CSS разделяется на две CSS с одним шасси, как показано на рисунке ниже.

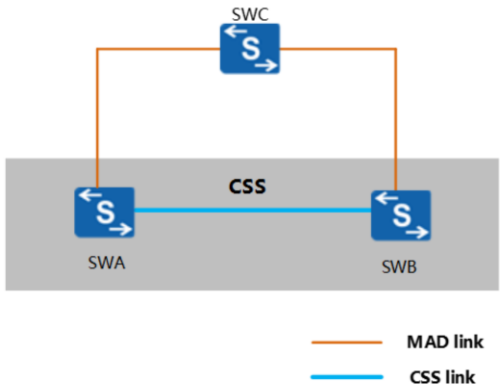


- После разделения CSS образуются две системы CSS с одинаковыми IP- MAC-адресами, так как два коммутатора управляются одинаковыми файлами конфигурации. Во избежание сбоя сети в результате данного сценария требуется механизм проверки на конфликт IP- и MAC-адресов после разделения CSS.

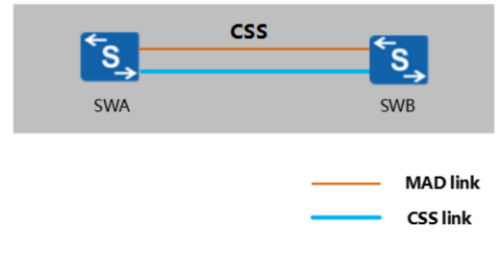
Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

Обнаружение нескольких активных узлов (MAD). Прямой режим

- В прямом режиме устройства-элементы могут напрямую подключаться либо к промежуточному устройству, либо друг к другу по принципу «каждый с каждым»:



Подключение напрямую к промежуточному устройству



Подключение коммутаторов-элементов напрямую друг к другу

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

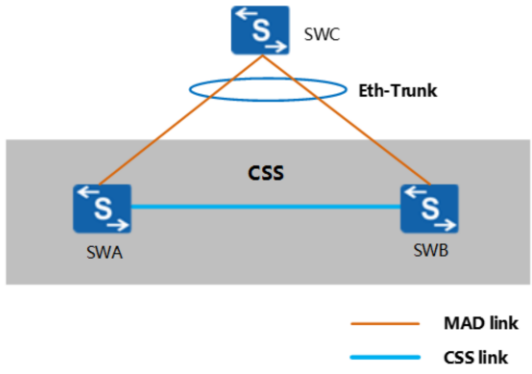
- Все коммутаторы-элементы CSS используют один и тот же IP-адрес и MAC-адрес (MAC-адрес системы CSS). После разделения CSS образуются две системы CSS с одним шасси, которые используют одинаковые IP- и MAC-адреса, так как оба коммутатора управляются файлами конфигурации исходной CSS. Во избежание данного сценария требуется механизм проверки на конфликт IP- и MAC-адресов после разделения CSS.
- Обнаружение нескольких активных узлов (MAD) - это протокол обнаружения разделений CSS и их устранения. При разделении CSS в результате сбоя канала MAD осуществляет обнаружение разделения, устранение нескольких активных узлов и запускает механизмы восстановления после сбоя для сокращения воздействия разделения CSS на сервисы до минимума.
- MAD может осуществляться в прямом режиме или режиме ретрансляции. Прямой режим и режим ретрансляции не могут быть одновременно сконфигурированы в одной и той же системе CSS.
- В прямом режиме устройства-элементы отдают предпочтение выделенным каналам MAD, а не стандартным сетевым кабелям. При работе в штатном режиме коммутаторы-элементы не отправляют пакеты MAD. После разделения CSS каждый коммутатор-элемент посылает пакет MAD каждую секунду по каналу MAD для проверки наличия более одного ведущего коммутатора.
- В прямом режиме устройства-элементы могут напрямую подключаться либо к промежуточному устройству, либо друг к другу по принципу «каждый с каждым»:
    - Подключение напрямую к промежуточному устройству. У каждого коммутатора-элемента есть по меньшей мере одно подключение по каналу MAD с промежуточным устройством.

Данный режим может быть запущен при удалении коммутаторов-элементов друг от друг.

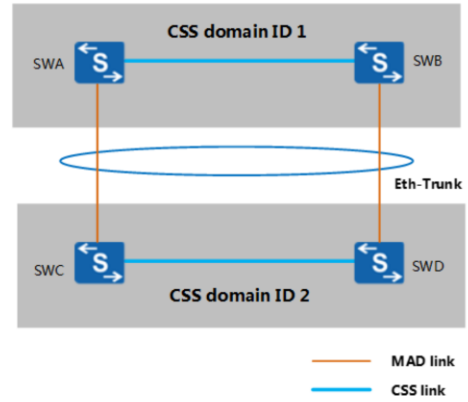
- Прямое подключение друг к другу. Для предотвращения влияния неисправностей промежуточных устройств на MAD промежуточное устройство не запускается.

Обнаружение нескольких активных узлов (MAD). Режим ретрансляции

- В режиме ретрансляции в качестве ретранслятора может работать независимый коммутатор или две системы CSS.



Один коммутатор в качестве агента ретрансляции MAD



Два CSS в качестве агентов ретрансляции MAD друг другу

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- В режиме ретрансляции обнаружение ретрансляции MAD сконфигурировано в интерфейсе Eth-Trunk CSS, функция обнаружения MAD агента включена. Каждый коммутатор-элемент должен быть подключен к агенту, в ином случае эти каналы должны быть добавлены в Eth-Trunk. В отличие от прямого режима, режим ретрансляции не требует подключения по дополнительным интерфейсам, так как интерфейс Eth-Trunk может выполнять другие функции при включенном режиме обнаружения ретрансляции MAD.
- В режиме ретрансляции при работе в штатном режиме коммутаторы-элементы отсылают пакеты MAD с интервалом в 30 сек. по каналам MAD и не обрабатывают полученные пакеты MAD. После разделения CSS каждый коммутатор-элемент посылает пакет MAD каждую секунду по каналу MAD для проверки наличия более одного ведущего коммутатора.
- Работа с несколькими активными узлами
  - После разделения CSS механизм MAD переводит новые CSS с одним шасси в состояние обнаружения (Detect) или восстановления (Recovery). CSS в состоянии обнаружения (Detect) продолжает работать, в то время как CSS в состоянии восстановления (Recovery) отключается.
  - В случае обнаружения нескольких активных узлов MAD действует следующим образом: При обнаружении двух CSS (коммутаторов) в состоянии обнаружения (Detect) MAD позволяет работу только одного коммутатора с наивысшим приоритетом в CSS. (Если у обоих коммутаторов одинаковый приоритет в CSS, поочередно сравниваются их MAC-адреса и идентификаторы в CSS.) Второй коммутатор затем переключается в состояние восстановления (Recovery) и все его физические порты, кроме зарезервированных, отключаются для предотвращения передачи сервисных пакетов коммутатором.
- Восстановление после сбоя MAD
- После восстановления неисправного канала CSS объединяются одним из следующих способов:
  - CSS в состоянии восстановления (Recovery) перезагружается и объединяется с CSS в состоянии обнаружения (Detect), отключенные сервисные порты восстанавливаются до включенного состояния (Up). Вся CSS восстанавливается.
  - Если CSS в состоянии обнаружения (Detect) выходит из строя до восстановления канала,

возможно удалить эту CSS из сети и командой запустить CSS в состоянии восстановления (Recovery) для направления сервисного трафика последней. Затем устраните неисправность CSS. После восстановления CSS в режиме обнаружения (Detect) ее возможно объединить с другим стеком.

Настройка CSS

- Образование CSS при помощи CSS-карт.

```
[SwitchA] set css mode css-card \\Configures the CSS card connection mode.
[SwitchA] set css id 1 \\Sets a CSS ID for SwitchA.
[SwitchA] set css priority 100 \\Sets a CSS priority for SwitchA.
[SwitchA] css enable \\Enables the CSS function on SwitchA.
```

- Образование CSS при помощи сервисных портов.

```
[SwitchA] set css mode lpu \\Configures the service port connection mode.
[SwitchA] set css id 1 \\Sets a CSS ID for SwitchA.
[SwitchA] set css priority 100 \\Sets a CSS priority for SwitchA.
[SwitchA] interface css-port 1 \\Enters the logical CSS port view.
[SwitchA-css-port1] port interface xgigabitethernet 1/0/1 to xgigabitethernet 1/0/2 enable
 \\Configures the service ports as physical member ports and add them to the logical CSS port.
[SwitchA] interface css-port 2
[SwitchA-css-port2] port interface xgigabitethernet 2/0/1 to xgigabitethernet 2/0/2 enable
[SwitchA] css enable \\Enables the CSS function on SwitchA.
```

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

Содержание

1. Таблица MAC-адресов
2. Самообращенный запрос ARP
3. MSTP
4. Умное стекирование iStack
5. CSS
6. **Eth-Trunk**
   - Основы Eth-Trunk
   - Реализация Eth-Trunk
   - E-Trunk

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

Основы Eth-Trunk

- Агрегация каналов Ethernet, также известная как Eth-Trunk, группирует множество физических каналов в один логический для увеличения доступной ширины пропускания канала. Сгруппированные каналы обеспечивают друг другу резервирование, увеличивая надежность канала.
- Подключенный к интерфейсам Eth-Trunk канал Eth-Trunk считается двухточечным соединением. Трафик может быть распределен по каналам-элементам Eth-Trunk. Различные протоколы и службы маршрутизации настраиваются в интерфейсе Eth-Trunk.



Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- Агрегация каналов увеличивает общую ширину полосы пропускания, надежность канала и поддерживает распределение нарузки трафика между каналами-элементами.
- Группа агрегирования каналов (LAG) и интерфейс элементов
  - Группа агрегирования каналов (LAG) - это логический канал, состоящий из множества каналов Ethernet. Интерфейсы, сгруппированные в один интерфейс Eth-Trunk (или LAG) являются интерфейсами-элементами.
- Активные и неактивные интерфейсы и каналы.
  - Интерфейсы-элементы Eth-Trunk могут быть активными и неактивными. Интерфейс, который осуществляет передачу данных, является активным; интерфейс, который не осуществляет передачу данных, является неактивным
  - Подключенный к активному интерфейсу канал считается активным; подключенный к неактивному интерфейсу канал считается неактивным.
- Верхний порог количества активных интерфейсов-элементов
  - Когда количество активных интерфейсов-элементов в интерфейсе Eth-Trunk достигает верхнего порога, добавленные заново интерфейсы не могут стать активными, но действуют как резервные. Интерфейсы заново добавленных интерфейсов работают в режиме Down.
- Нижний порог количества активных интерфейсов-элементов
  - Когда количество активных интерфейсов-элементов в интерфейсе Eth-Trunk падает ниже заданного порога, интерфейс Eth-Trunk переходит в режим Down. Таким образом у интерфейса Eth-Trunk минимальная требуемая ширина полосы пропускания.
- Режимы агрегации каналов, поддерживаемые устройством.
  - Одна плата: Интерфейсы-элементы интерфейса Eth-Trunk находятся на одной плате.
  - Разные платы: Интерфейсы-элементы интерфейса Eth-Trunk находятся на разных платах.
  - Одно шасси: Интерфейсы-элементы интерфейса Eth-Trunk находятся на устройствах-элементах кластера.
  - Разные устройства: Агрегация каналов между устройствами называется Enhanced Trunk (E-

Trunk). E-Trunk расширяет действие протокола LACP и обеспечивает агрегацию каналов между различными устройствами.

Принципы передачи

- Eth-Trunk располагается между подуровнями MAC и LLC и принадлежит к уровню канала передачи данных.



HASH-KEY	0	1	2	3	4	5	6	7
PORT	1	2	3	4	1	2	3	4

Пример таблицы переадресации Eth-Trunk

- Модуль Eth-Trunk поддерживает таблицу переадресации, которая состоит из описанных ниже частей:
  - ХЭШ-КЛЮЧ (HASH-KEY) - вычисляется при помощи хэш-алгоритма на базе MAC- или IP-адреса пакета.
  - ПОРТ - исходящий интерфейс для передачи пакетов. Номера интерфейсов изменяются в зависимости максимального количества поддерживаемых Eth-Trunk интерфейсов и могут быть привязаны к разным хэш-ключам.

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- Модуль Eth-Trunk передает кадры данных следующим образом:
  1. После того, как модуль Eth-Trunk получает кадр данных подуровня MAC, он извлекает MAC-адрес и IP-адрес источника кадра, MAC-адрес или IP-адрес назначения в зависимости от режима распределения нагрузки.
  2. Модуль Eth-Trunk получает хэш-ключи при помощи хэш-алгоритма.
  3. На основании хэш-ключей модуль Eth-Trunk находит номер интерфейса в таблице переадресации Eth-Trunk и затем отправляет кадр данных с соответствующего интерфейса.
- Например, интерфейс Eth-Trunk устройства поддерживает до восьми интерфейсов-элементов. Если физические интерфейсы 1, 2, 3 и 4 сгруппированы в один интерфейс Eth-Trunk, полученная таблица переадресации Eth-Trunk содержит восемь записей, как показано на рисунке выше. В данной таблице переадресации Eth-Trunk указаны хэш-ключи 0, 1, 2, 3, 4, 5, 6 и 7, которым соответствуют номера интерфейсов 1, 2, 3, 4, 1, 2, 3 и 4.
- Для предотвращения сбоев передачи кадров данных интерфейс Eth-Trunk использует распределение нагрузки по потокам данных. Передача данных изменяется в зависимости от режима распределения нагрузки.
- Доступны и могут быть выбраны режимы распределения нагрузки на базе следующих свойств кадров данных:
  - MAC-адреса источников
  - MAC-адреса назначения
  - IP-адреса источников
  - IP-адреса назначения
  - MAC-адреса источников и назначения
  - IP-адреса источников и назначения

- Идентификаторы VLAN и номера физических интерфейсов (продвинутый режим распределения нагрузки для пакетов уровня 2, IPv4, IPv6 и MPLS)

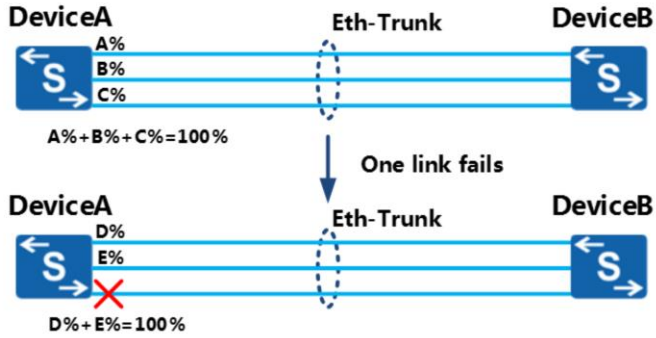
Содержание

1. Таблица MAC-адресов
2. Самообращенный запрос ARP
3. MSTP
4. Умное стекирование iStack
5. CSS
6. **Eth-Trunk**
   - Основы Eth-Trunk
   - Реализация Eth-Trunk
   - E-Trunk

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

Агрегация каналов в ручном режиме

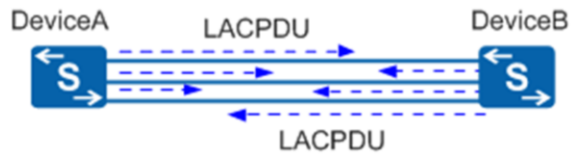
- В ручном (manual) режиме интерфейс Eth-Trunk создается и добавляется к другому интерфейсу Eth-Trunk вручную, протокол LACP не требуется. На рисунке ниже после создания вручную интерфейса Eth-Trunk на устройствах DeviceA и DeviceB все три активных канала передают трафик как каналы-элементы Eth-Trunk. При сбое работы одного канала остальные два канала-элемента Eth-Trunk продолжают распределять нагрузку.



Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

Агрегация каналов в режиме LACP (1)

- Для повышения надежности при помощи увеличения отказоустойчивости Eth-Trunk и резервирования каналов был представлен протокол агрегирования каналов (LACP). После образования канала Eth-Trunk протокол LACP динамически поддерживает или изменяет канал.
- Интерфейс Eth-Trunk в режиме LACP работает следующим образом:
  1. Устройства на обоих концах обмениваются пакетами LACPDU. На рисунке ниже показано добавление интерфейсов к интерфейсу Eth-Trunk после его создания на устройствах DeviceA и DeviceB и настройки работы в режиме LACP. Протокол LACP затем включается на обоих интерфейсах-элементах и устройства на обоих концах начинают обмен пакетами LACPDU.

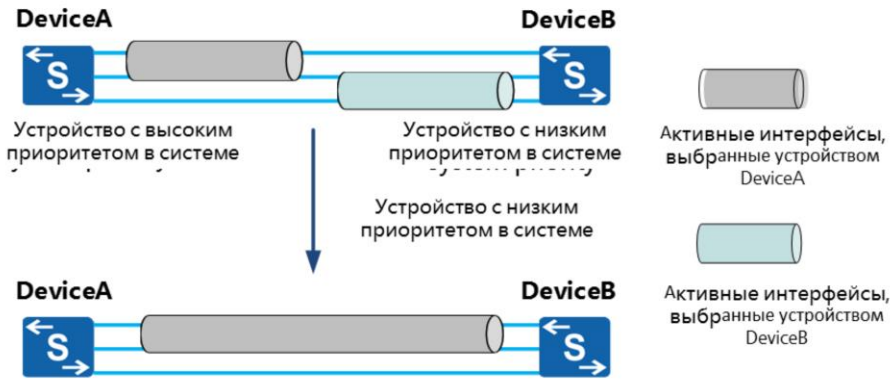


Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- Агрегация каналов в ручном режиме может увеличить доступную ширину полосы пропускания и позволяет обнаружить некоторые сбои, например, отключение канала-элемента внутри группы агрегации. Тем не менее, такие сбои, как сбои уровней каналов и некорректные подключения каналов, агрегация каналов обнаружить не может.

Агрегация каналов в режиме LACP (2)

2. Определите устройство-актор (Actor) и активные каналы.



Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- На рисунке выше устройства на обоих концах получают пакеты LACPDU друг от друга. В качестве примера используется DeviceB. Когда DeviceB получает пакеты LACPDU от DeviceA, устройство B проверяет и записывает информацию об устройстве DeviceA и сравнивает приоритеты системы LACP. Если приоритет системы LACP устройства DeviceA выше приоритета DeviceB, DeviceA становится устройством-актором (Actor). Если у обоих устройств одинаковый приоритет, актором становится устройство с наименьшим MAC-адресом.
- После выбора актора оба устройства выбирают активные интерфейсы в зависимости от приоритетов интерфейсов актора (Actor). Если приоритеты интерфейсов актора (Actor) одинаковы, активными назначаются интерфейсы с наименьшим номером. После выбора согласующихся активных интерфейсов интерфейс Eth-Trunk начинает распределение нагрузки между интерфейсами-элементами.

Настройка агрегации каналов

- Настройка агрегации каналов в ручном режиме

```
[SwitchA] interface eth-trunk 1
//Creates an Eth-Trunk interface and enters the Eth-Trunk interface view.
[SwitchA-Eth-Trunk1] mode manual load-balance
//Sets the manual link aggregation mode.
[SwitchA-Eth-Trunk1] trunkport gigabitethernet 0/0/1 to 0/0/3
//Adds interfaces to the Eth-Trunk interface.
```

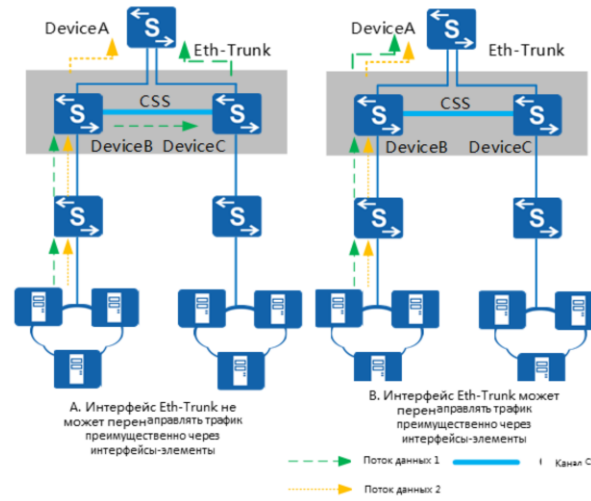
- Настройка агрегации каналов в режиме LACP

```
[SwitchA] interface eth-trunk 1
[SwitchA-Eth-Trunk1] mode lacp
//Sets the LACP link aggregation mode.
[SwitchA-Eth-Trunk1] max active-linknumber 2 \\Sets the upper threshold for the number of active member
interfaces to 2.
[SwitchA] interface gigabitethernet 0/0/1 \\Adds an interface to the Eth-Trunk interface.
[SwitchA-GigabitEthernet0/0/1] eth-trunk 1
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] eth-trunk 1
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] eth-trunk 1
```

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

Агрегация каналов в кластерах

- Физические интерфейсы на разных устройствах в кластере могут быть агрегированы в интерфейс Eth-Trunk. При сбое работы одного устройства в кластере или физического интерфейса-элемента Eth-Trunk данные могут быть переданы по кабелю кластера внутри шасси, таким образом обеспечивая надежность передачи данных и резервирование устройства.
- При работе сети в штатном режиме трафик с DeviceB или DeviceC передается при помощи локальных интерфейсов-элементов вместо кабелей кластера внутри шасси (как показано на рисунке слева).



Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- Когда устройства образуют кластер, интерфейс Eth-Trunk можно настраивать как исходящий интерфейс трафика для надежной передачи данных. В Eth-Trunk на разных устройствах должны работать интерфейсы-элементы. При передаче трафика кластером интерфейс Eth-Trunk может выбрать интерфейсы-элементы нескольких шасси для передачи трафика после использования хэш-алгоритма для вычисления исходящих интерфейсов. Ширина пропускания кабеля между устройствами в кластере ограничена. Передача трафика между несколькими шасси еще более увеличивает нагрузку на пропускную способность стекового кабеля и снижает эффективность передачи трафика. Для устранения данной проблемы локальные устройства могут отдавать предпочтение трафику интерфейса Eth-Trunk при передаче данных.
- Как показано на рисунке выше, устройства DeviceB и DeviceC образуют кластер, к которому при помощи интерфейса Eth-Trunk подключено устройство DeviceA. После настройки кластера для предпочтительной передачи трафика через локальные устройства могут возникнуть следующие ситуации:
  - Входящий на локальное устройство трафик передается локальным устройством напрямую.
    - Если на устройстве DeviceB в качестве исходящего интерфейса работает интерфейс-элемент Eth-Trunk, таблица переадресации Eth-Trunk устройства DeviceB содержит только локальные интерфейсы-элементы. Таким образом в качестве исходящих интерфейсов для трафика с DeviceB на DeviceA при помощи хэш-алгоритма выбраны только интерфейсы устройства DeviceB, что означает, что трафик передается напрямую устройством DeviceB.
  - Входящий на локальное устройство трафик передается другим устройством.
    - Если на устройстве DeviceB нет исходящих интерфейсов или все исходящие интерфейсы не работают, таблица переадресации Eth-Trunk устройства DeviceB содержит все доступные интерфейсы-элементы. Таким образом в качестве исходящих интерфейсов для трафика с DeviceB на DeviceA при помощи хэш-алгоритма выбраны интерфейсы устройства DeviceC, что означает, что трафик передается через устройство DeviceC.

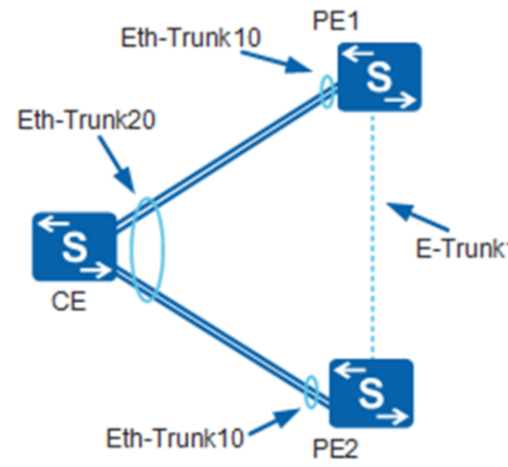
Содержание

1. Таблица MAC-адресов
2. Самообращенный запрос ARP
3. MSTP
4. Умное стекирование iStack
5. CSS
6. **Eth-Trunk**
   - Основы Eth-Trunk
   - Реализация Eth-Trunk
   - E-Trunk

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

Сравнение E-Trunk и Eth-Trunk

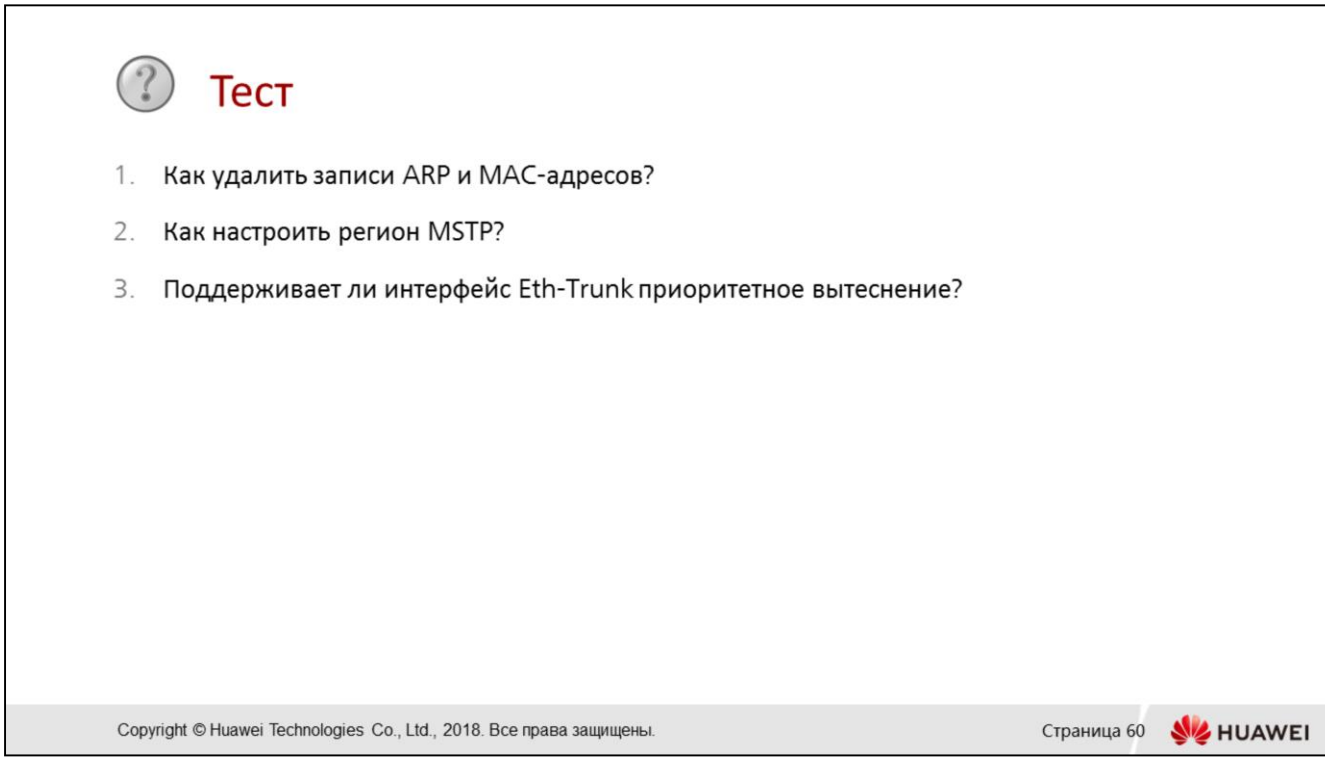
- Enhanced Trunk (E-Trunk) - это расширение протокола LACP. Оно осуществляет и контролирует агрегацию каналов между многочисленными устройствами для обеспечения надежности на уровне устройств, а не на уровне плат.
- На рисунке справа CE использует двойное подключение к PE1 и PE2 и на PE1 и PE2 запущен E-Trunk. При сбое работы канала между CE и PE1 или устройства PE1 трафик может быть переключен на канал между CE и PE2, таким образом осуществляя защиту на уровне устройств.



Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

- Когда CE использует двойное подключение к сетям VPLS, VLL или PWE3, для защиты устройств PE и каналов между устройствами CE и PE используется E-Trunk. Без системы E-Trunk устройство CE может подключиться только к одному из других устройств PE с использованием канала E-Trunk. При сбое работы канала Eth-Trunk или одного из устройств PE устройство CE не может с ним связываться. При помощи E-Trunk устройство CE может использовать двойное подключение к устройствам PE для их защиты и защиты каналов между CE и PE, осуществляя защиту на уровне устройств.
- На рисунке выше показано прямое подключение устройства CE к устройствам PE1 и PE2. Между устройствами PE1 и PE2 должен работать E-Trunk. Пример настройки приведен ниже: Создайте системы E-Trunk с одинаковыми идентификаторами и интерфейсы Eth-Trunk с одинаковыми идентификаторами устройств PE1 и PE2, добавьте интерфейсы Eth-Trunk в E-Trunk. Настройте интерфейс Eth-Trunk (Eth-Trunk 20) в режиме LACP на устройстве CE и подключите данный интерфейс Eth-Trunk к PE1 и PE2. Устройство CE не распознает E-Trunk.
- PE1 и PE2 обмениваются пакетами E-Trunk для определения своего статуса в качестве ведущего и резервного устройства E-Trunk. После определения ролей одно устройство PE работает как ведущее, второе - как резервное. Статус ведущего и резервного устройства PE зависит от приоритета в E-Trunk и идентификатора в системе E-Trunk, передаваемыми в пакетах E-Trunk устройств PE. PE с наивысшим приоритетом в E-Trunk (наименьшее значение) действует в качестве ведущего устройства. Если у устройств PE одинаковый приоритет в E-Trunk, PE с наименьшим идентификатором в системе E-Trunk действует в качестве ведущего устройства. В данном примере предполагается, что ведущим устройством является PE1. Eth-Trunk 10 устройства PE1 продолжает работу в режиме ведущего со статусом канала Up. PE2 работает в качестве резервного и Eth-Trunk 10 устройства PE2 продолжает работу в режиме резервного со статусом канала Down.
- При сбое работы канала между CE и PE1 устройство PE1 отправляет устройству PE2 пакет E-Trunk, в котором содержится информация о сбое Eth-Trunk 10. По получении пакета PE2 обнаруживает неисправность Eth-Trunk 10 на PE1 и меняет свой статус в Eth-Trunk на статус ведущего устройства. При помощи согласования LACP Eth-Trunk 10 на PE2 переходит в состояние Up. Трафик от устройства CE затем передается на PE2, тем самым предотвращая перерыв в передаче трафика устройства CE.
- Если оба устройства PE настроены с BFD и происходит сбой PE1, после обнаружения статуса сессии BFD Down устройством PE2 оно меняет свой статус на статус ведущего. Eth-Trunk 10 на PE2 переходит в режим ведущего. Если BFD на устройствах PE не настроен и PE2 не получает пакеты E-Trunk от PE1 до истечения

срока таймера, то PE2 меняет статус с резервного устройства на ведущее. Eth-Trunk 10 на PE2 переходит в режим ведущего. При помощи согласования LACP Eth-Trunk 10 на PE2 переходит в состояние Up. Трафик от устройства CE затем передается на PE2, тем самым предотвращая перерыв в передаче трафика устройства CE.



- Ответы
- Как удалить записи ARP и MAC-адресов?
  - Для удаления всех записей динамических MAC-адресов в режиме просмотра системы запустите команду **undo mac-address dynamic**.
  - Для удаления всех записей статических MAC-адресов в режиме просмотра системы запустите команду **undo mac-address static**.
  - Для удаления всех записей ARP в режиме просмотра системы запустите команду **undo arp static**.
  - Для удаления всех записей ARP в режиме просмотра пользователя запустите команду **reset arp**.
- Как настроить регион MSTP?
  - Для входа в режим просмотра данных о регионе MST в целях изменения данных о регионе введите команду **stp region-configuration**. У устройств в одном регионе MST должна быть одинаковая конфигурация региона MST. Любые изменения послужат причиной приписки устройства к другому региону MST. Для региона MST возможно настроить следующие параметры:
    - Выбор формата (Format selector): Значение по умолчанию равняется 0 и его нельзя настроить при помощи команд.
    - Название региона (Region name): название региона MST. Значением по умолчанию является MAC-адрес моста.
    - Уровень ревизий (Revision level): Значение по умолчанию равняется 0.
    - Соотнесение VLAN и устройств (Instance/Vlans Mapped): Соотнесение MSTI и VLAN. По умолчанию все VLAN приписаны к значению 0.
- Поддерживает ли интерфейс Eth-Trunk приоритетное вытеснение?
  - Только интерфейсы Eth-Trunk в режиме LACP поддерживают приоритетное вытеснение LACP. Для включения приоритетного вытеснения LACP введите команду **lacp preempt enable**. В режиме LACP при сбое работы активного канала запасной канал с наивысшим приоритетом из списка замещает неисправный. При включенном режиме приоритетного вытеснения LACP при

восстановлении работы неисправного канала с приоритетом выше приоритета заместительного канала восстановленный канал вытеснит заместительный канал и перейдет в активный режим. Настройки приоритетного вытеснения LACP на устройствах обоих концов канала Eth-Trunk должны совпадать, режим LACP должен быть включен или выключен.

Краткое содержание

- Таблица MAC-адресов
- Самообращенный запрос ARP
- MSTP
- Умное стекирование iStack
- CSS
- Eth-Trunk

Copyright © Huawei Technologies Co., Ltd., 2018. Все права защищены.

Спасибо!

www.huawei.com

HCIE-R&S

Технология WAN

www.huawei.com



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

- В документе приведено описание принципов работы и конфигурации интерфейсов, протоколов PPP, MP, PPPoE, интерфейса POS и канала IP-Trunk в глобальной сети (WAN).

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Цели

- По завершении курса вы будете знать:
  - Общую информацию об интерфейсах Ethernet и POS в глобальной сети (WAN).
  - Принципы работы и конфигурции PPP и MP.
  - Принципы работы и конфигурции IP-Trunk.
  - Принципы работы и конфигурции PPPoE.

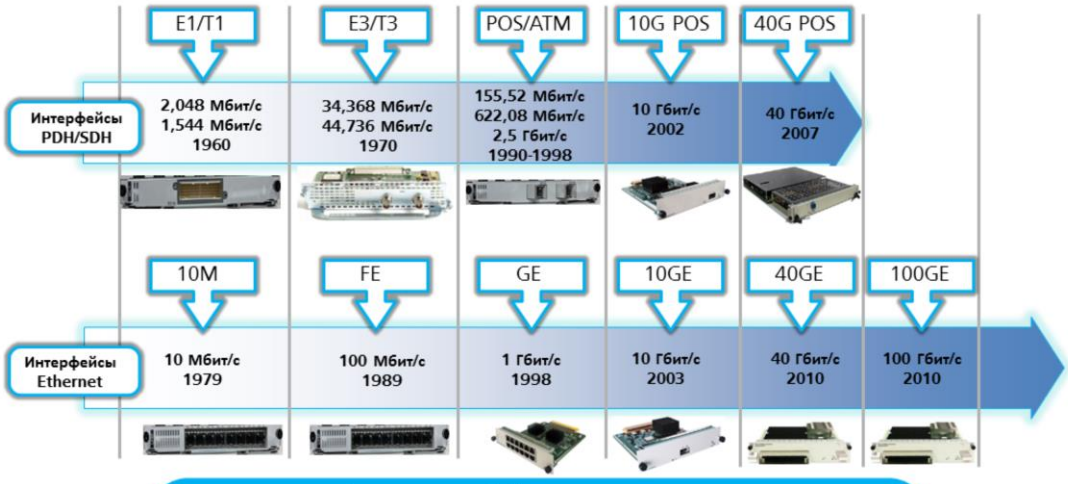
Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Содержание

1. **Интерфейсы WAN**
   - Эволюция интерфейсов WAN на маршрутизаторах
   - Интерфейс Ethernet
   - Интерфейс POS
   - Сравнение интерфейсов Ethernet и POS
2. Принцип работы и конфигурация протокола PPP
3. IP-Trunk
4. Принцип работы и конфигурация протокола PPPoE

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Эволюция пропускной способности физических интерфейсов на маршрутизаторах



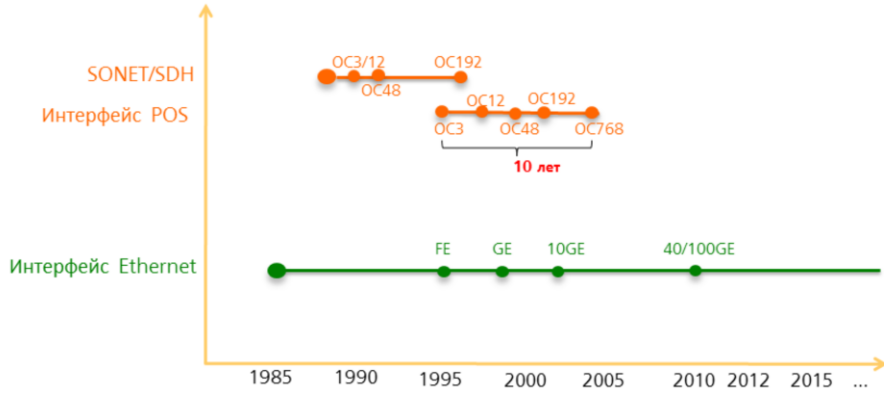
Эволюция интерфейсов маршрутизаторов

Основные параметры интерфейсов: пропускная способность, дальность передачи, стоимость, энергопотребление, плотность и совместимость

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Тенденции развития интерфейсов POS и Ethernet



- Широкое использование интерфейсов POS в действующей сети.
- Постоянное развитие интерфейсов Ethernet.

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Содержание

1. **Интерфейсы WAN**
   - Эволюция интерфейсов WAN на маршрутизаторах
   - Интерфейс Ethernet
   - Интерфейс POS
   - Сравнение интерфейсов Ethernet и POS
2. Принцип работы и конфигурация протокола PPP
3. IP-Trunk
4. Принцип работы и конфигурация протокола PPPoE

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Интерфейс Ethernet

- Технология Ethernet была разработана корпорацией Xerox PARC. Общепринято считать, что Ethernet был изобретён 22 мая 1973 года.
- Разновидности Ethernet:
  - 10M Ethernet (стандартный Ethernet)
  - 100M Ethernet (быстрый Ethernet)
  - 1000M Ethernet (гигабитный Ethernet)
  - 10GE Ethernet
  - 100GE Ethernet
  - ...

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

10M/100M Ethernet

- На физическом уровне спецификация Ethernet 10M/100M определяется значением скорости и средой передачи:
  - 10BASE-T: 2 неэкранированные витые пары категории 3, 4 и 5.
  - 100BASE-TX: 2 экранированные витые пары или высококачественные неэкранированные витые пары категории 5.
  - 100BASE-FX: два волоконно-оптических кабеля, один – для передачи сигналов, другой – для приема сигналов.

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

1000M Ethernet

- Типы интерфейсов:
  - 1000BASE-T: соответствует IEEE 802.3ab и использует неэкранированные витые пары категории 5.
  - 1000BASE-X: соответствует IEEE 802.3z и использует многомодовый волоконно-оптический кабель, одномодовый волоконно-оптический кабель и симметричную экранированную витую пару 150 Ом.
  - 1000BASE-CX: использует среду передачи, которая поддерживает передачу сигнала на расстоянии не более 25 м, поэтому используется редко.
  - 1000BASE-SX: многомодовые волоконно-оптические кабели на длине волны 850 нм.
  - 1000BASE-LX: одномодовые и многомодовые волоконно-оптические кабели на длине волны 1310 нм.

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

10GE Ethernet

- Стандарт: IEEE 802.3ae
- Типы интерфейса:
  - Последовательный интерфейс 10GBASE-S/L/E-R/W:
    - 10GBASE-S: многомодовые волоконно-оптические кабели на длине волны 850 нм.
    - 10GBASE-L: одномодовые волоконно-оптические кабели на длине волны 1310 нм.
    - 10GBASE-E: одномодовые волоконно-оптические кабели на длине волны 1550 нм.
    - W = WAN PHY (физический уровень WAN): скорость интерфейса – 9,95328 Гбит/с, инкапсуляция по стандарту SONET STS-192c и SDH VC-4-64C. Сеть DWDM или SDH/SONET может использоваться для подключения Ethernet 10G к сети оптической передачи.
    - R = LAN PHY (физический уровень LAN): скорость интерфейса – 10,3125 Гбит/с.
  - Параллельный интерфейс 10GBASE-LX4 с WDM (4 длины волн):
    - 10GBASE-LX4: многомодовые волоконно-оптические кабели на длине волны 1310 нм.

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

100GE Ethernet

- В июне 2010 года после четырех лет работы над стандартами технологии Ethernet 100 Гбит/с Ассоциация IEEE ратифицировала стандарт IEEE 802.3ba.
- Официально опубликованный стандарт 802.3ba предусматривает следующие спецификации физического уровня для уровня MAC 100 Гбит/с:
  - Одномодовый волоконно-оптический кабель (SMF) 40 км: физический уровень (PHY) – 100GBASE-ER4, волоконно-оптический кабель состоит из четырех каналов WDM 1310 нм с разнесением каналов 800 ГГц.
  - Одномодовый волоконно-оптический кабель 10 км: физический уровень (PHY) - 100GBASE-LR4, кабель состоит из четырех каналов WDM 1310 нм с разнесением 800 ГГц.
  - Многомодовый волоконно-оптический кабель OM3 10 м: физический уровень (PHY) - 100GBASE-SR10, волоконно-оптический кабель состоит из 10 независимых многомодовых волокон 850 нм
  - Медный кабель 7 м: физический уровень (PHY) - 100GBASE-CR10, медный кабель состоит из 10 независимых медных жил .

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Содержание

1. **Интерфейсы WAN**
   - Эволюция интерфейсов WAN на маршрутизаторах
   - Интерфейс Ethernet
   - Интерфейс POS
   - Сравнение интерфейсов Ethernet и POS
2. Принцип работы и конфигурация протокола PPP
3. IP-Trunk
4. Принцип работы и конфигурация протокола PPPoE

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Интерфейс POS

- Технология пакетной передачи данных поверх SONET/SDH (Packet over SONET/SDH – POS) позволяет маршрутизаторам опорной сети передавать пакеты IP непосредственно поверх фреймов SONET/SDH.
- Технология POS преобразует пакеты данных переменной длины непосредственно в полезную нагрузку SONET. POS использует физический уровень передачи данных SONET, обеспечивая высокоскоростное надежное P2P-соединение. Для передачи данных используются волоконно-оптические кабели.
- Скорости интерфейсов POS:
  - OC-3/STM-1: 155,52 Мбит/с
  - OC-12/STM-4: 622,08 Мбит/с
  - OC48/STM-16: 2488,32 Мбит/с
  - OC192/STM-64: 9953,28 Мбит/с
  - OC768/STM-256: 39813,12 Мбит/с
- Синхронная оптическая сеть (SONET) – протокол передачи данных для Северной Америки и Японии с поддержкой формата OC-n.
- Синхронная цифровая иерархия (SDH) – протокол передачи данных для Европы и Китая с поддержкой формата STM-n.

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Оптическая несущая уровня n (OC-n) обозначает стандартизированный ряд скоростей передачи информации по оптическому волокну. OC-1 представляет собой линию передачи с минимальной скоростью 51,84 Мбит/с.
- STM – модуль синхронной передачи

Содержание

1. **Интерфейсы WAN**
   - Эволюция интерфейсов WAN на маршрутизаторах
   - Интерфейс Ethernet
   - Интерфейс POS
     - Сравнение интерфейсов Ethernet и POS
2. Принцип работы и конфигурация протокола PPP
3. IP-Trunk
4. Принцип работы и конфигурация протокола PPPoE

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Сравнение интерфейсов Ethernet и POS

- Скорость интерфейсов Ethernet и POS может достигать 10 Гбит/с и 40 Гбит/с. После публикации стандарта 100-гигабитного Ethernet, скорость Ethernet-интерфейса превысила скорость POS-интерфейса.
- POS-интерфейс использует протокол PPP или HDLC в качестве протокола инкапсуляции уровня 2 для передачи IP-пакетов. Максимальная длина заголовка 2-го уровня составляет 9 или 7 байтов. 10-гигабитные интерфейсы LAN и WAN используют протокол инкапсуляции Ethernet, а длина заголовка 2-го уровня составляет 18 байт. Следовательно, эффективность передачи IP-пакетов по интерфейсу POS выше.
- Стоимость интерфейсов и плат Ethernet ниже. Например, цена 10-гигабитного Ethernet-интерфейса примерно в два раза ниже цены 10-гигабитного POS-интерфейса.

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Режимы LAN и WAN

- Оптический трансивер XFP 10G с моногомодовым портом может работать в режиме LAN или WAN. При необходимости можно настроить соответствующий режим.
- Разница между интерфейсами 10G LAN и WAN заключается в режиме инкапсуляции. Интерфейс 10G LAN использует только протокол инкапсуляции Ethernet, а интерфейс 10G WAN использует протокол инкапсуляции Ethernet на канальном уровне. Однако на физическом уровне инкапсулированные данные сразу преобразуются в последовательность SDH.
- Для передачи данных на большие расстояния в сети WAN интерфейс WAN может работать как в режиме LAN, так и в режиме WAN. Режимы интерфейсов двух маршрутизаторов на обоих концах WAN должны быть одинаковыми.
- Если между маршрутизаторами имеются промежуточные устройства, обратите внимание на режим интерфейса маршрутизаторов. Как правило, если на промежуточном устройстве используется интерфейс 10G POS, маршрутизатор может использовать интерфейсы 10G POS и 10GE WAN для связи. Если на промежуточном устройстве используется интерфейс 10G Ethernet, то маршрутизатор сможет использовать только интерфейс 10GE LAN. Обратите внимание, что новые промежуточные устройства поддерживают и интерфейс 10GE LAN/WAN, и интерфейс 10G POS, и вам нужно только изменить конфигурацию программного обеспечения.

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Содержание

1. Интерфейсы WAN
2. **Принцип работы и конфигурация PPP**
   - Основные понятия PPP
   - LCP
   - Аутентификация PAP
   - Аутентификация CHAP
   - NCP
   - Основные принципы MP
   - Конфигурация PPP и MP

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Основные понятия PPP – Три компонента

- Протокол PPP – это двухточечный протокол, который используется на канальном уровне в стеке протоколов TCP/IP.
- Три компонента PPP:
  - Метод инкапсуляции мультипротокольных дейтаграмм.
  - Протокол управления соединением (Link Control Protocol, LCP) служит для установки, настройки и тестирования соединений на канальном уровне.
  - Протокол управления сетевым уровнем (Network Control Protocol, NCP) включает протоколы, предназначенные для установки и настройки параметров различных протоколов сетевого уровня.

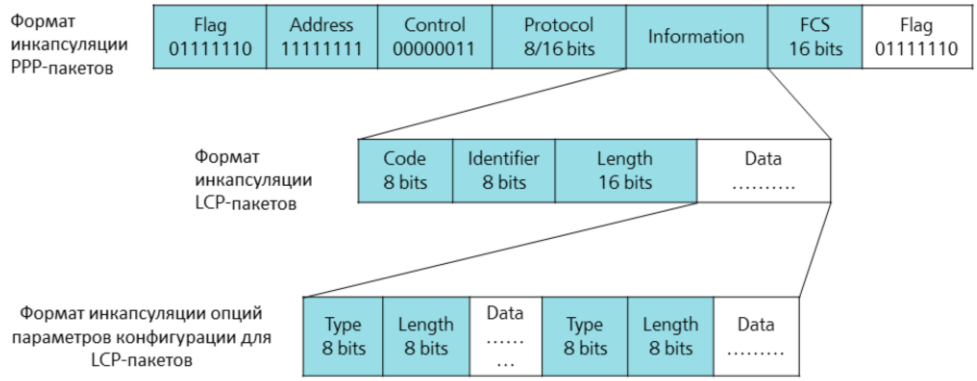
Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Протокол PPP включает три компонента: способ инкапсуляции данных, протокол управления каналом (LCP) и протокол управления сетевым уровнем (NCP).
- Режим инкапсуляции данных определяет способ инкапсуляции нескольких типов пакетов протоколов верхнего уровня.
- Протокол PPP настраивает LCP для применения к разным типом каналов. LCP может автоматически обнаруживать состояние канала (например, определять наличие петель) и настраивать параметры канала, например, максимальную длину пакета и протокол аутентификации. По сравнению с другими протоколами канального уровня PPP предоставляет функцию аутентификации. На обоих концах канала выполняется согласование протокола аутентификации, после чего выполняется аутентификация. Соединение устанавливается только после успешной аутентификации. Данная функция PPP позволяет операторам разрешить доступ рассредоточенным пользователям.
- Протокол PPP определяет группу протоколов NCP. Каждый протокол NCP соответствует протоколу сетевого уровня и используется для согласования таких параметров, как адреса сетевого уровня. IPCP используется для согласования и управления IP-адресами, а IPXCP используется для согласования и управления IPX.

Основные понятия PPP – Структура пакета

- Структура пакета PPP



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

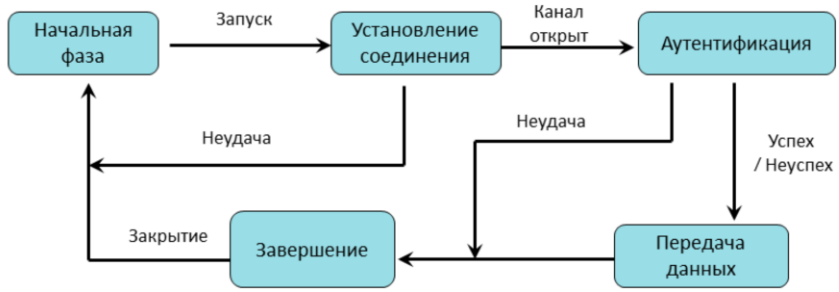
- Формат инкапсуляциии пакета PPP
  - Поле Flag (Флаг)
    - Поле **Flag** указывает на начало и конец физического кадра и всегда имеет значение 0x7E.
  - Поле Address (Адрес)
    - Поле **Address** указывает на соседа. Двум устройствам, связанным протоколом PPP, не требуется знать адреса канального уровня друг друга, поскольку протокол PPP используется в P2P-соединениях. Поле адреса заполняется широковещательным адресом, состоящим из единиц, и не имеет значения для PPP.
  - Поле Control (Управление)
    - Значение по умолчанию для поля **Control** всегда равно 0x03, что указывает на ненумерованный тип кадра. По умолчанию PPP не использует порядковые номера или механизмы подтверждения для обеспечения надежной передачи.
    - Поля **Address** и **Control** идентифицируют пакет PPP, поэтому значение заголовка пакета PPP - FF03.
  - Поле Protocol (Протокол)
    - Поле **Protocol** идентифицирует дейтаграмму, инкапсулированную в поле **Information** (Информация) пакета PPP.

- Формат инкапсуляциии LCP-пакета
  - Поле Code (Код)
    - Поле **Code** имеет длину 1 байт и определяет тип пакета LCP.
  - Поле Identifier (Идентификатор)
    - Поле **Identifier** имеет длину 1 байт и служит для нахождения соответствия между запросами и откликами. Если получен пакет с неправильным идентификатором, он отбрасывается.
    - Порядковый номер пакета Configure-Request обычно начинается с 0x01 и при каждой отправке пакета Configure-Request увеличивается на 1. После того, как получатель получит пакет Configure-Request, он должен отправить ответный пакет с тем же порядковым номером, что и полученный пакет Configure-Request.
  - Поле Length (Длина)
    - Поле **Length** указывает общее количество байтов в пакете согласования. Это сумма длин полей **Code**, **Identifier**, **Length** и **Data**.
    - Значение поля **Length** не может превышать значение MRU канала. Байты принятого пакета за пределами, заданными полем **Length**, игнорируются.
  - Поле Data (Данные)
    - Поле **Type** (Тип) определяет тип опции для согласования.

- Поле **Length** (Длина) определяет общую длину поля **Data**.
- Поле **Data** включает содержание опции согласования.

Основные понятия PPP – Процесс установления соединения

- Процесс установления соединения PPP



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Процесс установления соединения
  - Начальная фаза (Dead): процесс связи начинается с этой фазы и заканчивается ей. После перехода физического уровня в статус Up, PPP переходит в фазу установления соединения.
  - Установление соединения (Establish): в фазе Establish устройства выполняют LCP-согласование параметров канального уровня. Если согласование не выполняется, соединение PPP не устанавливается, и PPP переходит в фазу Dead. Если согласование выполняется успешно, PPP переходит в фазу Authenticate.
  - Аутентификация (Authenticate): на этапе Authenticate одноранговые устройства проходят процедуру аутентификации. Если аутентификация не пройдена, PPP переходит в фазу Terminate. Если аутентификация прошла успешно или аутентификация не настроена, PPP переходит в фазу Network.
  - Передача данных (Network): если согласование выполнено, соединение PPP устанавливается, и осуществляется передача пакетов на сетевом уровне. Если приложение верхнего уровня (например, цепь передачи данных по требованию) считает, что соединение необходимо разорвать или администратор вручную разрывает соединение PPP (Closing - закрытие), PPP переходит в фазу Terminate.
  - Завершение (Terminate): на этапе Terminate LCP отключает канал PPP. После отключения канала, PPP переходит в фазу Dead.
- Примечание. в этой части описаны рабочие фазы протокола PPP, а не статус

протокола PPP. PPP состоит из группы протоколов. Следовательно, PPP не имеет статуса протокола. Только определенные протоколы, такие как LCP и NCP, имеют статус протокола, их статус может меняться (protocol status machine).

Содержание

1. Интерфейсы WAN
2. **Принцип работы и конфигурация PPP**
   - Основные понятия PPP
   - LCP
   - Аутентификация PAP
   - Аутентификация CHAP
   - NCP
   - Основные принципы MP
   - Конфигурация PPP и MP

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

LCP – Тип пакета

Тип пакета	Описание функции
Configure-Request	Содержит список параметров LCP с измененными значениями по умолчанию
Configure-Ack	Указывает, что значения всех параметров LCP в пакете Configure-Request приняты
Configure-Nak	Указывает, что значения параметров LCP в пакете Configure-Request являются недействительными локально
Configure-Reject	Указывает, что параметры LCP в пакете Configure-Request не могут быть определены локально

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Существует три класса LCP-пакетов.

1. Пакеты конфигурации канала, которые используются для формировании виртуального канала (Configure-Request, Configure-Ack, Configure-Nak и Configure-Reject).

2. Пакеты закрытия канала (Terminate-Request и Terminate-Ack).

3. Пакеты поддержания, которые служат для управления и отладки каналов (Code-Reject, Protocol-Reject, Echo-Request, Echo-Reply и Discard-Request).

LCP – Параметры, используемые для согласования

Параметр	Функция	Правило согласования	Значение по умолчанию
Maximum receive unit (MRU)	Указывает общую длину поля **Information** в кадре PPP	Используется наименьшее значение на обоих концах.	1500
Authentication protocol	Аутентифицирует протокол аутентификации, используемый узлом	Устройство, прошедшее аутентификацию, должно поддерживать протокол аутентификации, используемый устройством-аутентификатором, и этот протокол должен быть правильно настроен. Иначе согласование не будет выполнено.	Non-authentication
Magic number Magic-Number	Определяет случайное число, используемое для обнаружения петель в канале. Если магическое число (Magic number) в полученном пакете LCP совпадает с локальным магическим числом, образуется петля	Если магическое число в полученном LCP-пакете и локальное магическое число различаются, то петли не образуются и согласование проходит успешно. Если на обоих концах используются одинаковые магические числа, то для обнаружения петель используется специальный механизм.	Enable

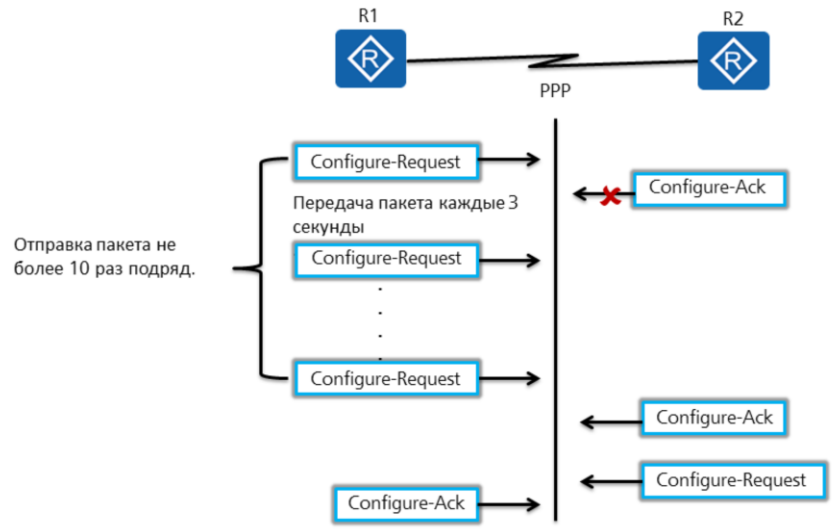
Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Параметры для согласования
  - В VRP MRU представлена максимальной единицей передачи (MTU), настроенной на интерфейсе.
  - Стандартными протоколами аутентификации PPP являются протоколы PAP и CHAP. Устройства на обоих концах канала PPP могут использовать разные протоколы аутентификации для аутентификации однорангового устойства. При этом проверяемое устройство должно поддерживать протокол аутентификации, который использует аутентификатор. Аутентификационная информация, например, имя пользователя и пароль, должна быть правильно настроена.
  - Для обнаружения петель и других отклонений LCP использует магическое число. Магическое число – это случайное число. Механизм случайного выбора должен гарантировать, что на обоих концах канала не будет сгенерирован одно и тот же магическое число.
  - После получения пакета Configure-Request система сравнивает магическое число, содержащееся в пакете, с локально сгенерированным магическим числом. Если числа различаются, то в канале не будут возникать петли. В этом случае отправляется пакет Configure-Ack, указывающий, что магическое число и другие параметры успешно согласованы. Если последующие пакеты содержат поле **Magic-Number**, то в этом поле будет установлено согласованное магическое число. В этом случае LCP не будет генерировать новые магические числа.
  - Если магическое число, содержащееся в пакете Configure-Request, совпадает с

локально сгенерированным магическим числом, система отправляет пакет Configure-Nak, содержащий новое магическое число. Далее LCP отправляет пакет Configure-Request с новым магическим числом независимо от того, содержит ли пакет Configure-Nak то же магическое число. Если в канале возникает петля, процесс продолжается. Если петля не возникает, обмен пакетами быстро восстанавливается.

LCP – Успешное согласование параметров канала

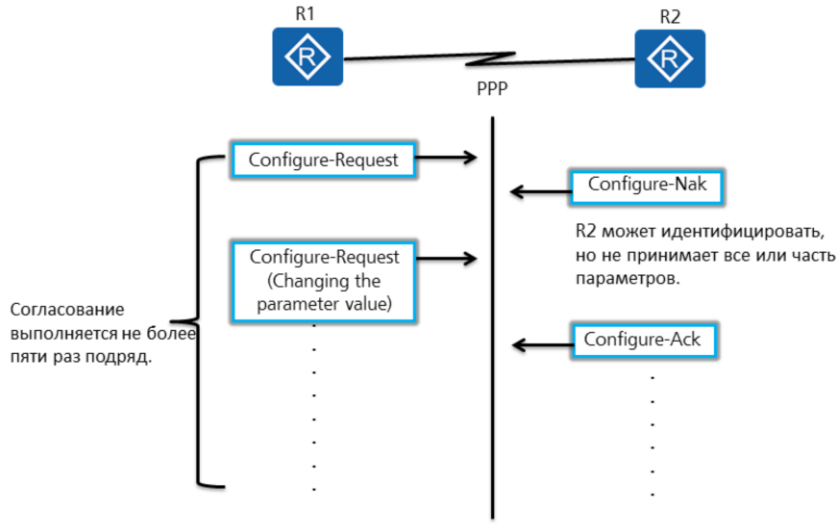


Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Согласование параметров канала выполнено.
  - Как показано на рисунке, маршрутизаторы R1 и R2 подключены через последовательные каналы и работают на протоколе PPP. Как только физический канал становится доступным, R1 и R2 выполняют согласование параметров канала с помощью LCP. В данном примере R1 отправляет пакет LCP.
  - R1 отправляет R2 (получателю) пакет Configure-Request, который содержит параметры канального уровня, сконфигурированные на R1 (отправителе). Для каждого параметра канального уровня используется структура "type, length, value" («тип, длина, значение»).
  - Если R2 (получатель) сможет идентифицировать все параметры канального уровня в пакете, и решит, что значение каждого параметра является соответствующим, то после получения пакета Configure-Request получатель возвращает пакет Configure-Ack отправителю.
  - Если R1 не получает пакет Configure-Ack, R2 будет передавать пакет Configure-Request каждые 3 секунды. Если R1 не получает пакет Configure-Ack после того, как R2 отправит пакет Configure-Request 10 раз подряд, R2 решает, что противоположный узел недоступен и прекращает отправку пакета Configure-Request.
- Примечание: на схеме выше показан процесс, в котором R2 решает, что настройки параметров канала на R1 являются правильными. R2 также должен отправить пакет Configure-Request на R1, чтобы проверить настройки параметров канала на R2.

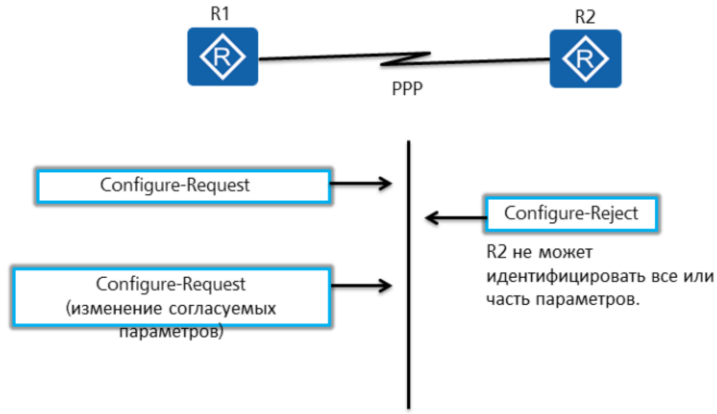
LCP – Сбой согласования параметров канала



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Сбой согласования параметров канала.
  - После получения пакета Configure-Request от R1, устройство R2 отправляет пакет Configure-Nak отправителю R1, если он идентифицирует все параметры канального уровня, передаваемые в пакете, но решает, что значения некоторых параметров неприемлемы, то есть согласование параметров не выполняется.
  - Пакет Configure-Nak содержит только непринятые параметры канального уровня. Значение каждого параметра канального уровня в пакете изменяется на значение (или диапазон значений), которые могут быть приняты отправителем (R2).
  - После получения пакета Configure-Nak, R1 повторно выбирает локальные параметры в соответствии с параметрами канального уровня в пакете и отправляет новый пакет Configure-Request.
  - Параметры, которые не проходят согласование пять раз подряд, отключаются и согласование больше не выполняется.

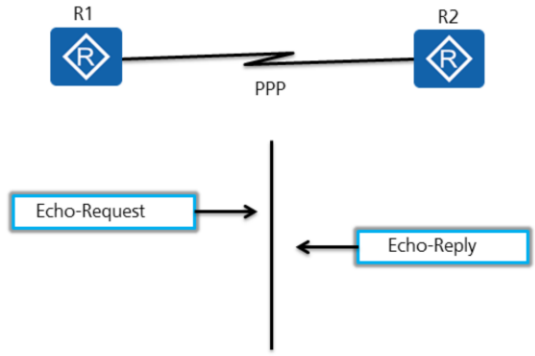
LCP – Сбой идентификации параметров



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- **Сбой идентификации согласуемых параметров канала**.
  - Если R2 не может идентифицировать некоторые или все параметры канального уровня, передаваемые в пакете, то после получения пакета Configure-Request, отправленного с R1, R2 должен отправить пакет Configure-Reject обратно на R1.
  - Пакет Configure-Reject содержит список только тех параметров канального уровня, которые не были идентифицированы.
  - После получения пакета Configure-Reject R1 отправляет новый пакет Configure-Request на R2. Пакет Configure-Request не содержит параметров, которые не были идентифицированы узлом (R2).

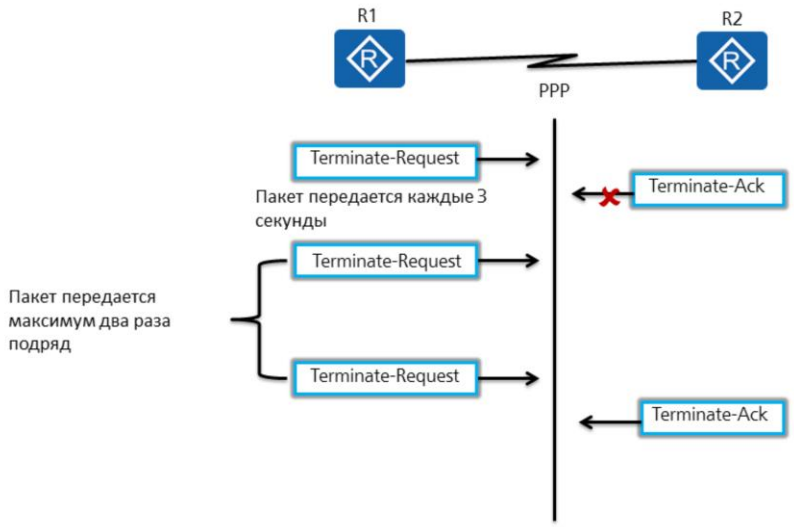
LCP – Проверка состояния канала



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Проверка состояния канала
  - После установления соединения LCP пакеты Echo-Request и Echo-Reply используются для определения состояния канала. После получения пакета Echo-Request устройство отвечает пакетом Echo-Reply, что указывает на то, что соединение работает корректно.
  - По умолчанию платформа VRP отправляет пакет Echo-Request каждые 10 секунд.

LCP – Соединение отключено



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Соединение отключено.
  - В случае сбоя аутентификации или отключения соединения администратором вручную, установленное соединение LCP может быть отключено.
  - Пакеты Terminate-Request и Terminate-Ack используются при отключении соединения LCP. Пакет Terminate-Request используется для передачи запроса на отключение соединения одноранговому узлу. Сразу после получения пакета Terminate-Request, LCP должен ответить пакетом Terminate-Ack, чтобы подтвердить, что соединение отключено.
  - Если пакет Terminate-Ack не получен, пакет Terminate-Request будет передаваться каждые три секунды. Если пакет Terminate-Ack не получен два раза подряд, одноранговый узел будет считаться недоступным, а соединение будет отключено.

Содержание

1. Интерфейсы WAN
2. **Принцип работы и конфигурация PPP**
   - Основные понятия PPP
   - LCP
   - Аутентификация PAP
   - Аутентификация CHAP
   - NCP
   - Основные принципы MP
   - Конфигурация PPP и MP

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

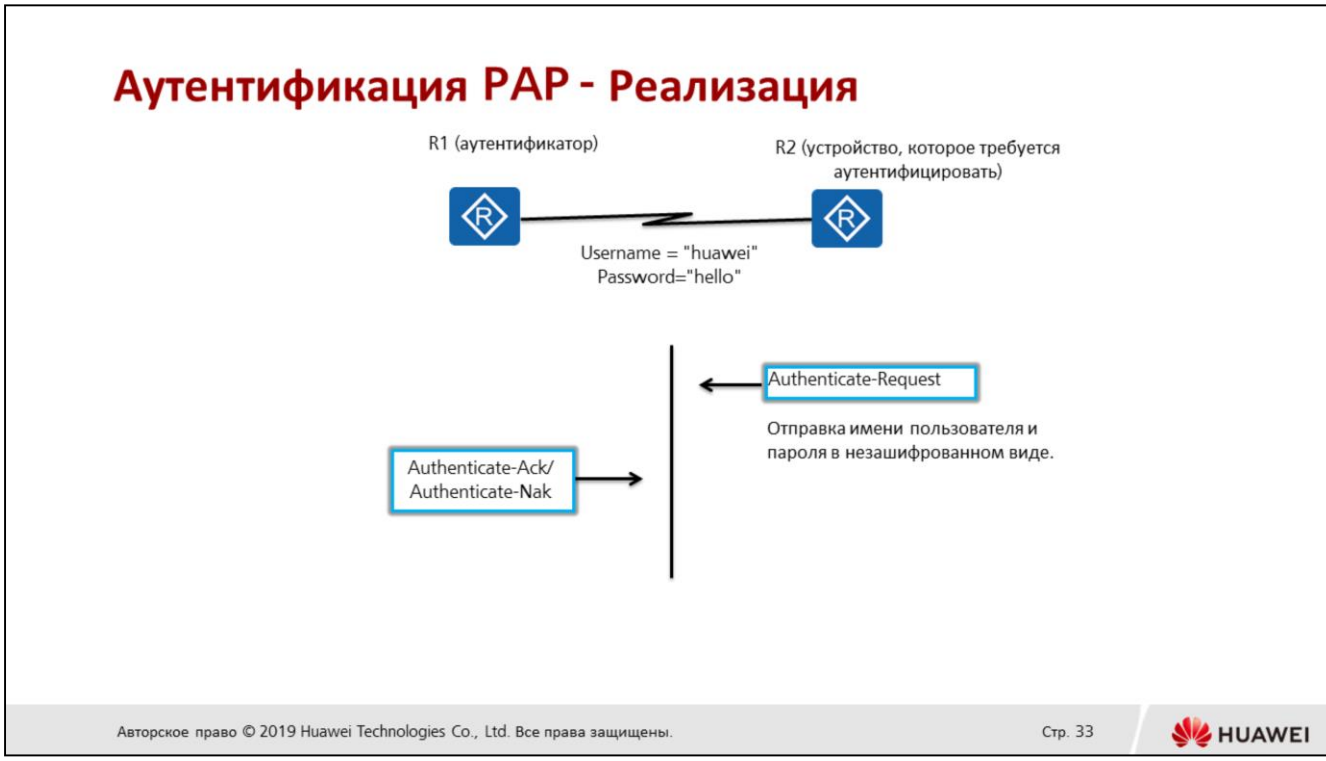
Аутентификация PAP – Тип пакета

Тип пакета	Функция
Authenticate-Request	Устройство, которое требуется аутентифицировать, отправляет сообщение Authenticate-Request с именем пользователя и паролем. Поле Data содержит имя пользователя и пароль в незашифрованном виде.
Authenticate-Ack	Аутентификатор отправляет сообщение об успешной аутентификации. Поле Data содержит текстовую информацию
Authenticate-Nak	Аутентификатор отправляет сообщение об ошибке аутентификации. Поле Data содержит текстовую информацию

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Пакет PAP икапсулируется в пакет PPP.



- Режим PAP
  - Устройство, которое требуется аутентифицировать, отправляет сконфигурированное незашифрованное имя пользователя и пароль аутентификатору в пакетах Authenticate-Request. В этом примере именем пользователя является **huawei**, а паролем – **hello**.
  - После получения имени пользователя и пароля, отправленных одноранговым узлом, аутентификатор проверяет правильность имени пользователя и пароля в соответствии с локально настроенной базой данных. Если они соответствуют базе данных, аутентификатор возвращает пакет Authenticate-Ack, указывая, что аутентификация пройдена. В случае несоответствия аутентификатор возвращает пакет Authenticate-Nak, указывая, что аутентификация не пройдена.

Содержание

1. Интерфейсы WAN
2. **Принцип работы и конфигурация PPP**
   - Основные понятия PPP
   - LCP
   - Аутентификация PAP
   - Аутентификация CHAP
   - NCP
   - Основные принципы MP
   - Конфигурация PPP и MP

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

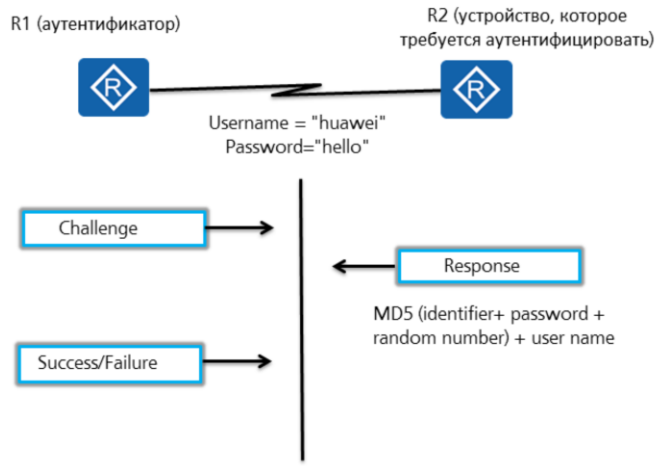
Аутентификация CHAP – Тип пакета

Тип пакета	Функция
Challenge	Аутентификатор отправляет сообщение Challenge на одноранговый узел.
Response	Одноранговый узел передает информацию пользователя в сообщении Response. Поле Data содержит имя пользователя и зашифрованный пароль.
Success	Если аутентификация прошла успешно, аутентификатор отправляет сообщение Success на одноранговый узел . Поле данных может содержать текстовую информацию.
Failure	Если аутентификация не пройдена, аутентификатор отправляет сообщение Failure на одноранговый узел. Поле Data может содержать текстовую информацию.

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Аутентификация CHAP - Реализация



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Для аутентификации CHAP требуется три обмена пакетами. Поле **Identifier** в пакете необходимо для сопоставления пакетов запроса и ответа, а пакеты, используемые в процессе аутентификации, используют одно и то же значение поля **Identifier**. Однонаправленная аутентификация CHAP применяется в двух сценариях: на аутентификаторе настроено имя пользователя, и на аутентификаторе не настроено с именем пользователя. Рекомендуется настроить на аутентификаторе имя пользователя.

- Если на аутентификаторе настроено имя пользователя (на интерфейсе настроена команда **ppp chap user username**), процесс аутентификации выглядит следующим образом:

  - Аутентификатор инициирует запрос аутентификации, отправляя на устройство, которое требуется аутентифицировать, пакеты Challenge, которые содержат имя локального пользователя.
  - После получения запроса аутентификации от аутентификатора устройство, которое требуется аутентифицировать, проверяет, настроена ли команда **ppp chap password** на локальном интерфейсе. Если команда настроена, устройство отправляет сгенерированный зашифрованный текст (который генерируется на основе идентификатора, пароля и случайного числа с использованием алгоритма MD5) и имя пользователя аутентификатору (Response). Если команда **ppp chap password** не настроена на интерфейсе, то устройство, которое требуется аутентифицировать, выполняет поиск пароля в таблице локальных пользователей по имени пользователя аутентификатора, и отправляет

аутентификатору зашифрованный текст (который генерируется на основе идентификатора, пароля и случайного числа с использованием алгоритма MD5) и имя пользователя однорангового узла (Response).

    - Аутентификатор шифрует сохраненный пароль, идентификатор и случайное число с помощью алгоритма MD5, и чтобы проверить правильность аутентификации сравнивает зашифрованное значение с зашифрованным текстом в полученном ответном пакете.

- Если на аутентификаторе не настроено имя пользоват (команда **ppp chap user username** не настроена на интерфейсе), процесс аутентификации выглядит следующим образом:

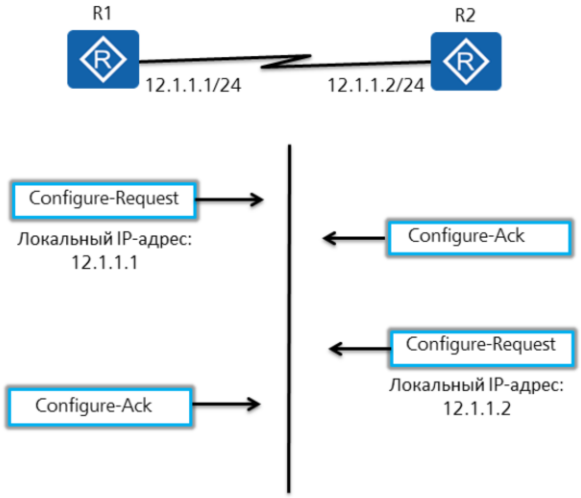
    - Аутентификатор инициирует запрос аутентификации, отправляя пакеты Challenge.
    - После получения пакета Challenge устройство, которое требуется аутентифицировать, шифрует пакет Challenge с помощью идентификатора, пароля и случайного числа, настроенных командой **ppp chap password**, используя алгоритм MD5 для создания зашифрованного текста. Затем он отправляет аутентификатору пакет Response, содержащий зашифрованный текст и имя локального пользователя.
    - Аутентификатор шифрует сохраненный пароль, идентификатор и случайное число с помощью алгоритма MD5, и чтобы проверить правильность аутентификации сравнивает зашифрованное значение с зашифрованным текстом в полученном ответном пакете.

Содержание

1. Интерфейсы WAN
2. **Принцип работы и конфигурация PPP**
   - Основные понятия PPP
   - LCP
   - Аутентификация PAP
   - Аутентификация CHAP
   - NCP
   - Основные принципы MP
   - Конфигурация PPP и MP

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

NCP – Согласование статического адреса с помощью IPCP

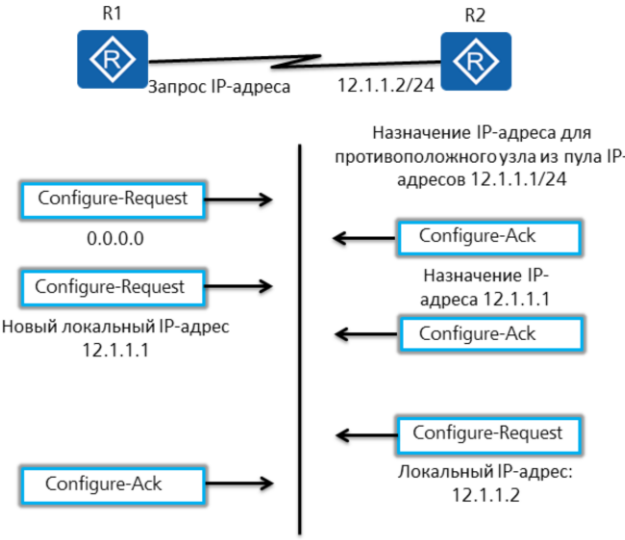


Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- IPCP используется для согласования параметров IP с тем, чтобы протокол PPP мог использоваться для передачи IP-пакетов.
- IPCP и LCP используют один и тот же механизм согласования и тип пакета. Ожнако IPCP не запускает LCP, а использует тот же процесс и тип пакета, что и LCP.

  - IP-адреса двух противоположных устройств: 12.1.1.1/24 и 12.1.1.2/24. Если IP-адреса обоих узлов находятся в разных сегментах сети, выполняется согласование IPCP.
  - Если на обоих концах настроены статические IP-адреса, процесс согласования выглядит следующим образом:
    - R1 и R2 отправляют пакеты Configure-Request, которые содержат локально настроенный IP-адрес.
    - После получения пакета Configure-Request от однорангового узла R1 и R2 проверяют IP-адрес в пакете. Если IP-адрес является действительным одиночным IP-адресом и отличается от локально настроенного IP-адреса (конфликт IP-адресов отсутствует), одноранговый узел может использовать этот адрес и отправляет пакет Configure-Ack.
    - Оба узла на концах канала PPP получают 32-битный IP-адрес, используемый одноранговым узелом, из сообщения, отправленного через IPCP.

NCP – согласование динамического адреса с помощью IPCP



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Как показано на рисунке, на R1 настроена функция запроса IP-адреса у противоположного узла. На R2 настроен пул IP-адресов 12.1.1.2/24, и он может назначать IP-адрес противоположному одноранговому узлу.
- Динамическое согласование IP-адресов между двумя противоположными устройствами выполняется следующим образом:
  - R1 отправляет пакет Configure-Request с IP-адресом 0.0.0.0 на устройство R2. Пакет Configure-Request с IP=адресом 0.0.0.0 указывает на то, что локальный узел запрашивает IP-адрес у противоположного узла.
  - R2 получает пакет Configure-Request, решает, что IP-адрес 0.0.0.0, содержащийся в данном пакете, является недействительным и отправляет пакет Configure-Nak с новым IP-адресом 12.1.1.1.
  - R1 получает пакет Configure-Nak, затем обновляет локальный IP-адрес и отправляет новый пакет Configure-Request, содержащий новый IP-адрес 12.1.1.1.
  - R2 получает пакет Configure-Request, решает, что IP-адрес, содержащийся в пакете, является действительным IP-адресом и отправляет пакет Configure-Ack обратно.
  - R2 отправляет пакет Configure-Request на устройство R1, чтобы запросить IP-адрес 12.1.1.2. R1 решает, что IP-адрес является действительным и отправляет пакет Configure-Ack обратно.

Содержание

1. Интерфейсы WAN
2. **Принцип работы и конфигурация PPP**
   - Основные понятия PPP
   - LCP
   - Аутентификация PAP
   - Аутентификация CHAP
   - NCP
   - Основные принципы работы MP
   - Конфигурация PPP и MP

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Основные принципы работы MP

- Цель MP
- Увеличение пропускной способности путем объединения нескольких каналов PPP в группу MP
- Согласование параметров канала в режиме MP
- На этапе LCP также проверяется, работает ли одноранговый интерфейс в режиме MP
- На этапе NCP устройства на обоих концах выполняют согласование NCP, используя параметры NCP (например, IP-адреса) интерфейса группы MP или виртуального шаблона интерфейса
- Режим реализации
- Виртуальный шаблон интерфейса
- Интерфейс группы MP

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Протокол Multilink PPP (MP) поддерживает фрагментацию пакетов, а фрагментированные пакеты передаются в один и тот же пункт назначения по нескольким каналам двухточечного соединения.

Содержание

1. Интерфейсы WAN
2. **Принцип работы и конфигурация PPP**
   - Основные понятия PPP
   - LCP
   - Аутентификация PAP
   - Аутентификация CHAP
   - NCP
   - Основные принципы работы MP
   - Конфигурация протоколов PPP и MP

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Конфигурация протокола PPP

- На интерфейсах, соединяющих R1 и R2, установите значение **PPP** для типа инкапсуляции, настройте аутентификацию **CHAP** и установите значение **Huawei** в качестве имени пользователя и значение **Hello** – в качестве пароля.




```
aaa
 local-user Huawei password cipher Hello
 local-user Huawei service-type ppp
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode chap
 ppp chap user Huawei
 ip address ppp-negotiate
```

```
interface Serial1/0/0
 link-protocol ppp
 remote address 12.1.1.1
 ppp chap user Huawei
 ppp chap password cipher Hello
 ip address 12.1.1.2 255.255.255.0
```

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Команды
  - Команда **ppp authentication-mode** настраивает режим аутентификации PPP, при котором локальное устройство аутентифицирует удаленное устройство.
  - Команда **ppp chap user** настраивает имя пользователя для аутентификации CHAP.
  - Команда **ppp chap password** настраивает пароль для аутентификации CHAP.
  - Команда **ip address ppp-negotiate** настраивает согласование IP-адреса на интерфейсе, чтобы этот интерфейс мог получить IP-адрес от удаленного узла.
  - Команда **remote address** настраивает на локальном устройстве функции назначения IP-адреса или определения пула IP-адресов для удаленного устройства.
- ppp authentication-mode { chap | pap }
  - chap: определяет значение Challenge Handshake Authentication Protocol (CHAP) для режима PPP-аутентификации.
  - ppp: определяет значение to Password Authentication Protocol (PAP) для режима PPP-аутентификации.
- ppp chap user username
  - username：username: определяет имя пользователя в аутентификации CHAP.
- ppp chap password { cipher | simple } password
  - cipher: отображает пароль в зашифрованном виде.

- simple: отображает пароль в незашифрованном виде.
- password: настраивает пароль для аутентификации CHAP.

Конфигурация протокола MP

- Для увеличения пропускной способности интерфейса необходимо объединить все взаимосвязанные интерфейсы PPP между R1 и R2 в группу MP. Настройте PAP-аутентификацию между R1 и R2, настройте R1 в качестве аутентификатора и R2 в качестве устройства, которое нужно аутентифицировать, и установите **Huawei** в качестве имени пользователя, а **Hello** – как пароль.




```
aaa
 local-user Huawei password cipher Hello
 local-user Huawei service-type ppp
#
interface Mp-group0/0/0
 ip address 12.1.1.1 255.255.255.0
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode pap
 ppp mp Mp-group 0/0/0
#
interface Serial1/0/1
 link-protocol ppp
 ppp authentication-mode pap
 ppp mp Mp-group 0/0/0
```

```
interface Mp-group0/0/0
 ip address 12.1.1.2 255.255.255.0
#
interface Serial1/0/0
 link-protocol ppp
 ppp pap local-user Huawei password simple Hello
 ppp mp Mp-group 0/0/0
#
interface Serial1/0/1
 link-protocol ppp
 ppp pap local-user Huawei password simple Hello
 ppp mp Mp-group 0/0/0
```

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Команды
  - Команда **interface mp-group** создает интерфейс MP-группы и отображает представление интерфейса MP-группы.
  - Команда **ppp mp mp-group** привязывает интерфейс к интерфейсу MP-группы, чтобы интерфейс работал в режиме MP.
  - Команда перезапускает интерфейс.



Содержание

1. Интерфейсы WAN Interfaces
2. Принцип работы и конфигурация PPP
3. **IP-Trunk**
4. Принцип работы и конфигурация PPPoE

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

IP-Trunk

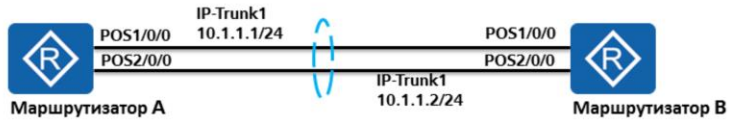
- Trunk-интерфейсы делятся на Eth-Trunk и IP-Trunk.
  - Eth-Trunk состоит только из каналов Ethernet.
  - IP-Trunk состоит из интерфейсов POS.
- IP-Trunk выполняет балансировку нагрузки в любом из следующих режимов:
  - Балансировка нагрузки между потоками: пакеты с одинаковыми IP-адресами источника и назначения передаются по одному каналу-участнику.
  - Балансировка нагрузки пакетов: пакеты передаются по разным каналам-участникам.
- Интерфейсы-участники IP-Trunk инкапсулируются с помощью HDLC. Принцип работы IP-Trunk аналогичен принципу работы Eth-Trunk.

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Trunk-интерфейсы делятся на Eth-Trunk и IP-Trunk.
  - Eth-Trunk состоит только из каналов Ethernet.
  - IP-Trunk состоит из интерфейсов POS.

Конфигурация IP-Trunk




```
#
sysname RouterA
#
interface Ip-Trunk1
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
interface Pos1/0/0
 link-protocol hdlc
 undo shutdown
 ip-trunk 1
#
interface Pos2/0/0
 link-protocol hdlc
 undo shutdown
 ip-trunk 1
#
```

```
#
sysname RouterB
#
interface Ip-Trunk1
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
interface Pos1/0/0
 link-protocol hdlc
 undo shutdown
 ip-trunk 1
#
interface Pos2/0/0
 link-protocol hdlc
 undo shutdown
 ip-trunk 1
#
```

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Содержание

1. Интерфейсы WAN
2. Принцип работы и конфигурация протокола PPP
3. IP-Trunk
4. **Принцип работы и конфигурация протокола PPPoE**
   - Принцип работы протокола PPPoE
   - Конфигурация протокола PPPoE

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Обзор PPPoE (1)

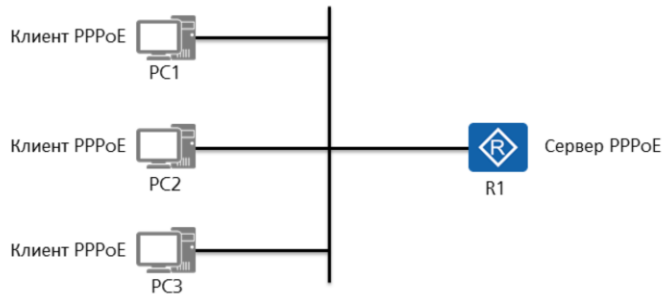
- PPP over Ethernet (PPPoE) – это протокол канального уровня, который инкапсулирует кадры PPP в кадры Ethernet. PPPoE позволяет нескольким хостам в Ethernet подключаться к удаленному серверу широкополосного доступа.
- Как правило, операторам требуется подключить несколько компьютеров на сайте к одному устройству удаленного доступа. Устройство доступа обеспечивает контроль и учет этих компьютеров способом, аналогичным удаленному доступу. Технология Ethernet при этом является наиболее экономически выгодной технологией среди всех технологий доступа, обеспечивающих подключение нескольких компьютеров к устройству доступа. Кроме того, протокол PPP предоставляет функции контроля доступа и учета. В результате появился протокол PPPoE, позволяющий операторам достигать своих целей.
- PPPoE позволяет большому количеству хостов в Ethernet подключаться к Интернету с помощью устройства удаленного доступа и контролирует каждый хост с помощью PPP. Протокол PPPoE имеет много областей применения, отличается высоким уровнем безопасности и предлагает удобные функции учета.

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Обзор PPPoE (2)

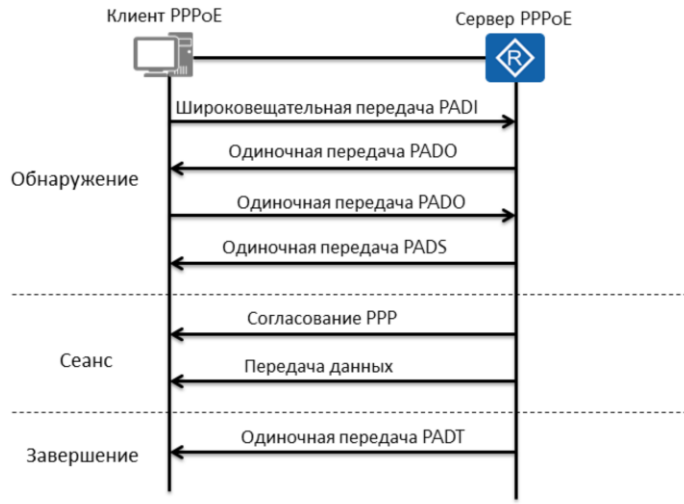
- Протокол PPP применяется в Ethernet для подключения нескольких хостов в широковещательной сети к серверу удаленного доступа.
- PPPoE использует модель клиент / сервер.



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Обзор PPPoE
  - PPPoE позволяет большому количеству хостов в Ethernet подключиться к Интернету с помощью устойства удаленного доступа, а также управлять каждым хостом с помощью PPP. PPPoE имеет много областей применения, отличается высоким уровнем безопасности и предлагает удобные функции учета.

Установление сеанса PPPoE



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Три этапа PPPoE: обнаружение (Discovery), сеанс (Session) и завершение (Terminate).
- Обнаружение
  - Клиент PPPoE передает пакет PPPoE Active Discovery Initial (PADI), который содержит информацию об услугах, необходимую клиенту PPPoE.
  - После получения пакета PADI все серверы PPPoE сравнивают запрошенную услугу с услугами, которые они могут предоставить. Серверы PPPoE, которые могут предоставить запрошенную услугу, отправляют пакеты PPPoE Active Discovery Offer (PADO) клиенту PPPoE в режиме одиночной передачи.
  - Клиент PPPoE может получать пакеты PADO от нескольких серверов PPPoE. Клиент PPPoE выбирает один из этих серверов PPPoE и отправляет пакет PPPoE Active Discovery Request (PADR) на выбранный сервер PPPoE в режиме одиночной передачи.
  - Сервер PPPoE генерирует уникальный идентификатор для идентификации сеанса PPPoE с клиентом PPPoE, а затем отправляет пакет PPPoE Active Discovery Session-confirmation (PADS) с этим идентификатором сеанса клиенту PPPoE. После установления сеанса PPPoE сервер PPPoE и клиент PPPoE входят в стадию сеанса PPPoE.
  - После установления сеанса PPPoE сервер PPPoE и клиент PPPoE совместно используют уникальный идентификатор сеанса PPPoE и изучают MAC-адреса одноранговых узлов.
- Сеанс
  - Процесс согласования PPP на этапе сеанса PPPoE аналогичен общему процессу согласования PPP. После успешного согласования PPP пакеты

данных PPP можно пересылать по установленному каналу PPP. На данном этапе сервер PPPoE и клиент PPPoE отправляют все пакеты данных Ethernet в режиме одиночной передачи.

- Завершение
  - На этапе сеанса клиент и сервер PPPoE обмениваются пакетами PADT, чтобы отключить соединение PPPoE. Отправить пакеты PADT можно в любое время после установления сеанса в режиме одиночной передачи. После получения пакета PADT трафик PPP больше не передается в этом сеансе.

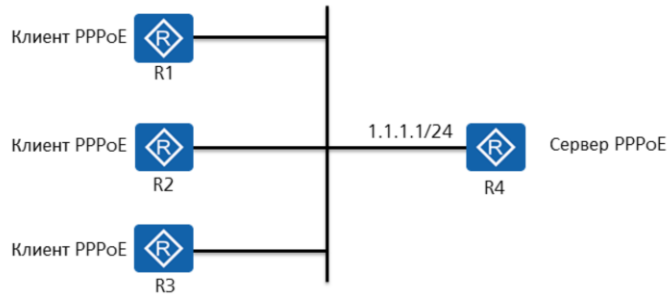
Содержание

1. Интерфейсы WAN
2. Принцип работы и конфигурация PPP
3. IP-Trunk
4. **Принцип работы и конфигурация протокола PPPoE**
   - Принцип работы протокола PPPoE
   - Конфигурации протокола PPPoE

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Конфигурация протокола PPPoE (1)

- Компания A планирует развернуть протокол PPPoE и имеет следующие требования:
  - R4 выполняет функции сервера PPPoE для назначения клиентам IP-адресов из пула IP-адресов 1.1.1.0/24 и использует PAP-аутентификацию.
  - R1 выполняет функции клиента PPPoE, и использует **HuaweiR1** в качестве имени пользователя, а **R1** – в качестве пароля для аутентификации.
  - R2 выполняет функции клиента PPPoE и использует **HuaweiR2** в качестве имени пользователя, а **R2** – в качестве пароля для аутентификации.
  - R3 выполняет функции клиента PPPoE и использует **HuaweiR3** в качестве имени пользователя, а **R3** – в качестве пароля для аутентификации.



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Конфигурация PPPoE (2)

- Конфигурация R1:

```
interface Dialer1
 link-protocol ppp
 ppp pap local-user HuaweiR1 password cipher R1
 ip address ppp-negotiate
 dialer user HuaweiR1
 dialer bundle 1
 dialer-group 1
#
interface GigabitEthernet0/0/0
 pppoe-client dial-bundle-number 1
#
dialer-rule
 dialer-rule 1 ip permit
```

- Конфигурация R4:

```
ip pool POOL_1
 gateway-list 1.1.1.1
 network 1.1.1.0 mask 255.255.255.0
#
aaa
 local-user HuaweiR1 password cipher R1
 local-user HuaweiR2 password cipher R2
 local-user HuaweiR3 password cipher R3
#
interface Virtual-Template0
 ppp authentication-mode pap
 remote address pool POOL_1
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/0
 pppoe-server bind Virtual-Template 0
```

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- В данном примере R1 имитирует клиента PPPoE при выполнении подключения PPPoE для доступа в Интернет. R4 выполняет функции сервера PPPoE для аутентификации и назначения адресов.

Краткое содержание

- Интерфейсы WAN
- Интерфейс Ethernet
- Интерфейсы POS /IP-Trunk
- PPP/MP
- PPPoE

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Спасибо!

www.huawei.com

Обучение R&S Huawei

Основы протокола IPv6

www.huawei.com

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Введение

- Как известно, нехватка адресов в протоколе IPv4 ограничивает дальнейшее развитие IP-технологий. Возникла срочная потребность в технологии, способной заменить IPv4. Технология IPv6 не только обладает функциями IPv4, но и отвечает требованиям к IP-адресам будущих отраслей. Все отрасли от правительств до рынков остро нуждаются в интернет-технологиях нового поколения и способствуют появлению и развитию технологии IPv6, которая может полностью решить эту проблему.
- Этот курс посвящен основам IPv6, в том числе истории создания технологии, формату пакетов, классификации адресов, базовому протокол и технологии миграции.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Цели

- После прохождения этого курса вы сможете:
  - Рассказать историю технологии IPv6.
  - Отличать адреса IPv6.
  - Понимать базовый протокол IPv6.
  - Описывать технологии перехода на IPv6.
  - Настраивать конфигурации IPv6.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Содержание

1. **История технологии IPv6**
2. Реализация протокола IPv6
3. Команды конфигурации IPv6
4. Советы по подготовке к экзаменам по протоколу IPv6

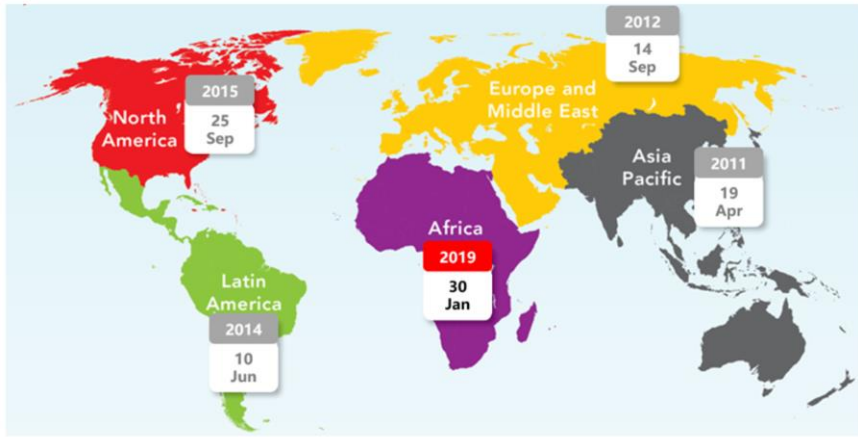
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.



- ICANN является главной организацией по управлению сетью Интернет.
- Не все адреса назначаются. Некоторые адреса зарезервированы для широковещательных, тестовых и частных сетей. Эти адреса называются адресами специальных категорий. Вы можете посмотреть такие адреса в протоколе RFC5735.

Порядок назначения IPv4-адресов в мире

- 3 февраля 2011 года IANA объявила о равномерном распределении последних 4,68 млн. IP-адресов интернет-регистраторам в пяти регионах мира. С этого момента IPv4-адреса больше не назначаются.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Протокол IPv4 успешно выдержал испытание на масштабируемость: в результате бурного роста сеть Интернет теперь связывает сотни миллионов компьютеров. Однако важно учитывать, что протокол был разработан десятки лет назад для небольшой сети того времени. Теперь очевидно, что создатели протокола не оценили масштаб будущей сети. С развитием Интернета и появлением новых областей его применения ограничения IPv4 стали очевидны.
- Быстрое расширение сети Интернет вышло далеко за рамки ожидания людей. Особенно в последнее десятилетие Интернет развивался огромными темпами. Интернет стал неотъемлемой частью повседневной жизни людей. Однако быстрое развитие сети стало причиной исчерпания IP-адресов.

Проблемы назначения IPv4-адресов

- Исчерпание общедоступных IPv4-адресов. Это самая важная причина замены протокола IPv4 на IPv6 .
- Увеличение числа пользователей Интернета. По мере развития технологических отраслей все больше пользователей и различных типов устройств подключаются к общественным сетям.
- Отсутствие модели сквозной связи. Механизм NAT может решить проблему взаимного доступа между закрытыми адресными пространствами и общественными сетями, но разрушает целостность сквозной связи.
- Неспособность адаптироваться к новым технологиям, таким как Интернет вещей (IoT). Все отрасли являются потенциальными пользователями протокола IPv6.
- Широковещательный механизм и зависимость от ARP приводит к частому возникновению неисправностей, связанных с локальной сетью на базе IPv4.
- Недостаточная мобильности.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Временные контрмеры

- В 1991 г. Инженерный совет Интернета (IETF) запустил секретное сетевое решение, чтобы отсрочить момент исчерпания адресов IPv4.
- В 1993 г. были внедрены механизмы преобразования сетевых адресов (NAT) и бесклассовой адресации (CIDR).
- Однако эти переходные схемы не могли предотвратить исчерпание адресов, только замедлить его. Проблема не была решена.
- Инженерный совет IETF представил Интернет-протокол следующего поколения IPv6 в 90-е годы. В настоящее время признана необходимость перехода на версию IPv6 с версии IPv4 в будущем.

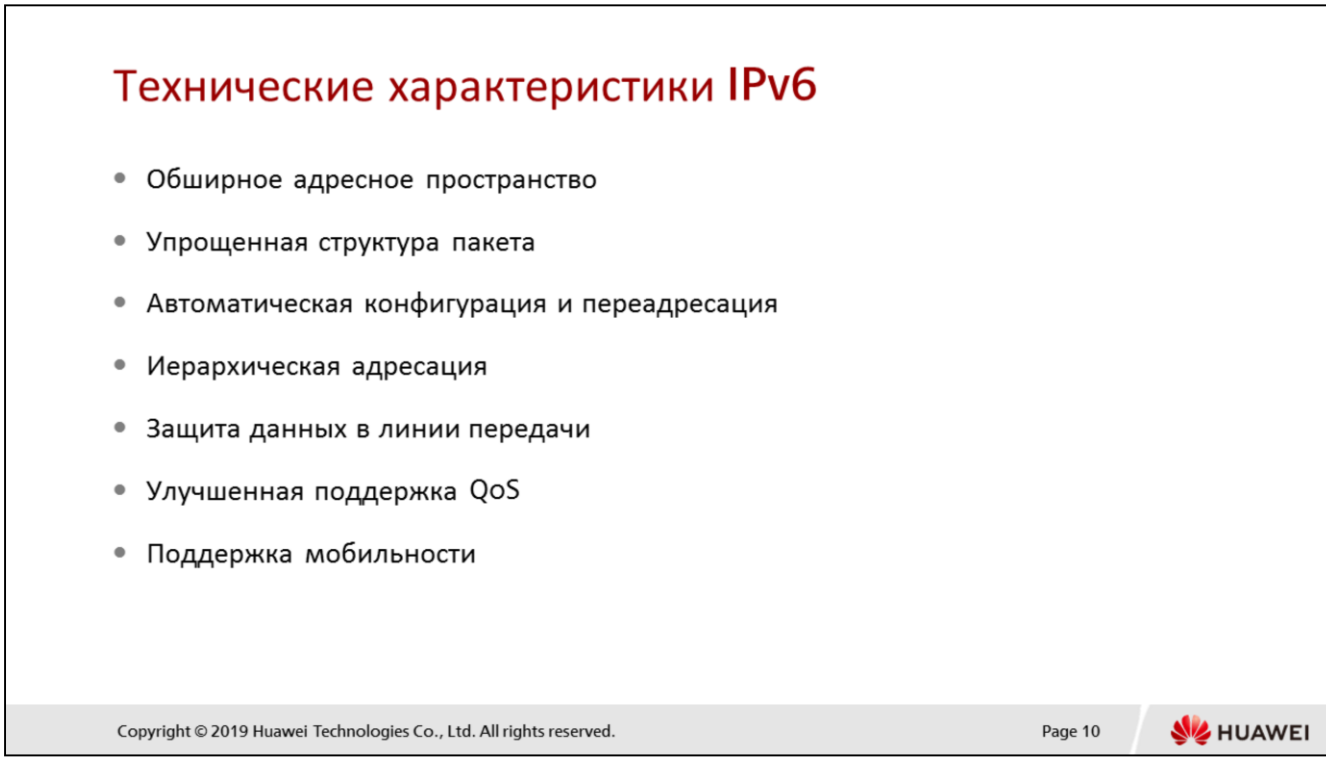
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Содержание

1. История технологии IPv6
2. **Реализация протокола IPv6**
   - **Форматы пакетов**
   - Классификация адресов
   - Базовый протокол
   - Технологии перехода
3. Команды конфигурации IPv6
4. Советы по подготовке к экзаменам по протоколу IPv6

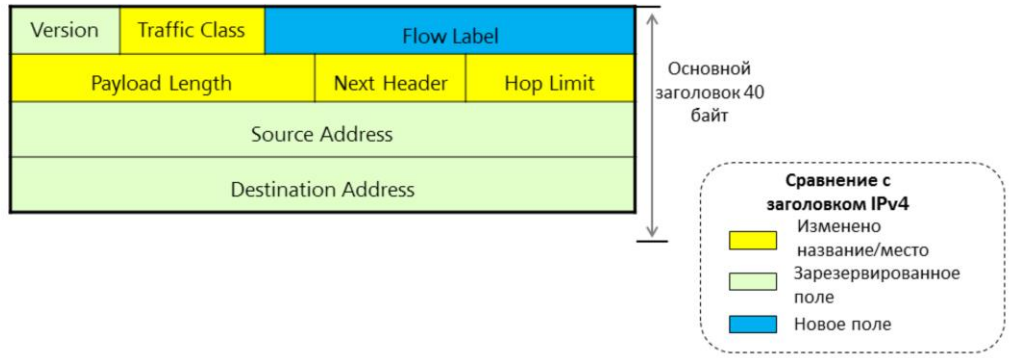
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.



- Функции IPv6:
  - Обширное адресное пространство. Адреса IPv6 имеют длину 128 бит. Такая длина обеспечивает адресное пространство 2^{128} возможных адресов (4,3 млрд. x 4,3 млрд. x 4,3 млрд. x 4,3 млрд.). Поэтому маловероятно, что когда-либо произойдет истощение адресов IPv6.
  - Упрощенная структура пакетов. В IPv6 используется новый формат заголовка. То есть, пакет IPv6 обладает новым заголовком вместо простого расширения адреса в заголовке пакета IPv4 до 128 бит. Заголовок пакета IPv6 включает фиксированный заголовок и расширенные заголовки. Некоторые менее важные и необязательные поля были перенесены в расширенные заголовки, которые находятся после фиксированного заголовка. Это повышает эффективность обработки заголовков IPv6 промежуточными маршрутизаторами в сети.
  - Автоматическая конфигурация и переадресация. IPv6 поддерживает автоматическую конфигурацию адресов, за счет чего хосты могут автоматически обнаруживать сети и получать адреса IPv6, что значительно улучшает управляемость внутренних сетей.
  - Иерархическая архитектура. Обширное адресное пространство позволяет создавать иерархическую архитектуру сети IPv6 для упрощения суммирования маршрутов и повышения эффективность переадресации.
  - Защита данных в линии передачи. IPv6 поддерживает аутентификацию IP Security (IPsec) и шифрование на сетевом уровне, обеспечивая сквозную безопасность.
  - Улучшенная поддержка QoS. IPv6 отводит специальное поле под названием flow label в заголовке пакета. Поле flow label позволяет маршрутизаторам в сети определять пакеты одного потока данных и выполнять специальную обработку. С помощью этой метки маршрутизатор может определять поток данных без анализа внутренних пакетов данных. Это обеспечивает поддержку QoS даже при шифровании полезной нагрузки пакетов данных.
  - Поддержка мобильности. Благодаря использованию расширенных заголовков, например Routing header и Destination option, протокол поддерживает мобильность.

Формат пакетов IPv6: основной заголовок

- Формат пакетов
  - Пакет IPv6 содержит основной заголовок IPv6, несколько расширенных заголовков IPv6 и блок данных протокола верхнего уровня.
  - Основной заголовок IPv6 имеет восемь полей с фиксированным размером 40 байт. Каждый пакет данных IPv6 должен содержать основной заголовок.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

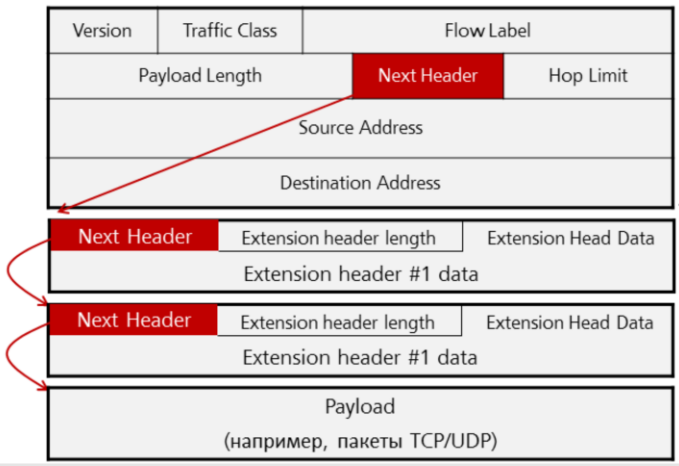
- Пакет IPv6 состоит из заголовка IPv6, нескольких расширенных заголовков и блока данных протокола верхнего уровня (PDU).
- Заголовок IPv6
  - Каждый пакет IPv6 должен содержать заголовок с фиксированной длиной 40 байт.
  - Заголовок IPv6 включает основную информацию о переадресации пакетов и обрабатывается всеми маршрутизаторами в пути переадресации.
- PDU протокола верхнего уровня
  - PDU протокола верхнего уровня состоит из заголовка протокола верхнего уровня и его полезной нагрузки, и может быть пакетом ICMPv6, TCP или UDP.
- Заголовок IPv6 содержит следующие поля:
  - Version (4 бита). В IPv6 значение поля Version имеет значение 6.
  - Traffic Class (8 бит). Это поле указывает на класс или приоритет пакета IPv6. Оно аналогично полю TOS в пакете IPv4 и используется в основном для управления QoS.
  - Flow Label (20 бит). Это поле было добавлено в IPv6 для разграничения трафика в реальном времени. Поток данных идентифицируется по Flow Label и IP-адресу источника. Промежуточные сетевые устройства могут эффективно разграничивать потоки данных на основании этого поля.
  - Payload Length (16 бит). Это поле указывает длину полезной нагрузки IPv6 в байтах. Полезной нагрузкой является часть пакета IPv6 после базового заголовка IPv6, включая расширенный заголовок расширения и PDU протокола верхнего уровня.
  - Next Header (8 бит).
  - Hop Limit (8 бит). Это поле аналогично полю Time to Live в пакете IPv4 и определяет максимальное количество узлов, через которые может пройти IP-пакет. Значение уменьшается на 1 при прохождении через каждый маршрутизатор, передающий пакет. Пакет отбрасывается,

если Hop Limit уменьшается до 0.

- Source Address (128 бит). Адрес отправителя пакета.
- Destination Address (128 бит). Адрес получателя пакета.

Формат пакетов IPv6: расширенный заголовок

- Использовать расширенный заголовок необязательно. Отправитель данных добавляет расширенный заголовок только тогда, когда это требуется.



- **Next Header: указывает на следующий заголовок длиной 8 бит.** Функция этого параметра совпадает с функцией Next Header в основном заголовке. Он указывает следующий расширенный заголовок (при наличии) или тип протокола верхнего уровня.
- **Extension Header Length: указывает длину расширенного заголовка 8 бит** (за исключением поля Next Header).
- **Extension Header Data: указывает данные расширенного заголовка с переменной длиной**. Включает ряд опций и поля для заполнения блока данных незначащей информацией.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- В заголовке пакета IPv4 есть поле опций (Options), которое включает опции безопасности, временной метки и записи маршрута. Переменная длина поля Options влияет на диапазон длины заголовка пакета IPv4 от 20 до 60 байт. Когда маршрутизаторы пересылают пакеты IPv4 с полем Options необходимо использовать множество ресурсов. Поэтому данные пакеты IPv4 используются редко.
- Для повышения эффективности обработки пакетов в протоколе IPv6 используются расширенные заголовки, которые являются заменой поля Options в заголовке пакета IPv4. Расширенные заголовки находятся между основным заголовком IPv6 и PDU верхнего уровня. Пакет IPv6 может включать от 0 расширенных заголовков. Отправитель пакета добавляет один и более расширенных заголовков в пакет только тогда, когда отправитель запрашивает у маршрутизаторов и конечного устройства выполнение специальной обработки. В отличие от IPv4, у протокола IPv6 есть расширенные заголовки переменной длина, не ограниченные 40 байтами. Это упрощает дальнейшее расширение. Для повышения эффективности обработки расширенного заголовка и работы транспортного протокола, требуется, чтобы длина расширенного заголовка была целым числом, кратным 8 байтам.
- При использовании нескольких расширенных заголовков, поле Next Header расширенного заголовка указывает на тип следующего заголовка за данным расширенным заголовком.

Формат пакетов IPv6: типы расширенных заголовков

- Когда пакет IPv6 использует более одного заголовка расширения, заголовки должны быть перечислены в следующем порядке:

Тип заголовка	Значение поля Next Header	Описание
Hop-by-Hop Options	0	Указывает параметры отправки для каждого узла в линии передачи. Каждый промежуточный узел в линии передачи должен считывать и обрабатывать поле. Сценарии применения: полезная нагрузка Jumbo, подсказка маршрутизатора, резервирование ресурсов.
Destination Options	60	Этот заголовок содержит информацию, которую обрабатывает только узел назначения пакета. В настоящее время этот заголовок используется в мобильном протокол IPv6.
Routing	43	Узел источника IPv6 использует этот заголовок для указания промежуточных маршрутизаторов, через которые пакет должен к месту назначения. Эта опция аналогична опции Loose Source и Record Route в IPv4.
Fragment	44	Как и пакеты IPv4, длина пакетов IPv6 не может превышать максимальную единицу передачи данных (MTU). Если длина пакета превышает MTU, пакет должен быть фрагментирован. В IPv6 заголовок Fragment используется узлом источника IPv6 для отправки пакета, превышающего MTU.
Authentication	51	IPSec использует этот заголовок для обеспечения аутентификации источника данных, проверки целостности данных и функций анти-повтора. Он также защищает некоторые поля в базовом заголовке IPv6.
Encapsulating Security Payload	50	Этот заголовок предоставляет те же функции, что и заголовок Authentication, а также шифрование пакетов IPv6.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Примечание:
  - Промежуточные маршрутизаторы определяют, следует ли обрабатывать расширенные заголовки на основе значения поля Next Header в основном заголовке IPv6. Промежуточные маршрутизаторы не должны изучать или обрабатывать все расширенные заголовки.
  - Каждый расширенный заголовок может появиться в пакете IPv6 только один раз, за исключением заголовка Destination Options, который может появиться дважды (один раз перед заголовком Routing и один раз перед заголовком верхнего уровня).

Содержание

1. История технологии IPv6
2. **Реализация протокола IPv6**
   - Форматы пакетов
   - **Классификация адресов**
   - Базовый протокол
   - Технологии перехода
3. Команды конфигурации IPv6
4. Советы по подготовке к экзаменам по протоколу IPv6

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Типы адресов IPv6

- Одиночный адрес (unicast address) – это идентификатор одного интерфейса. Пакет, отправленный на одиночный адрес, передается на интерфейс с этим адресом. Как правило, в IPv6 интерфейс имеет несколько адресов IPv6.
- Групповой адрес (multicast address) – это идентификатор набора интерфейсов. Пакет, отправленный на групповой адрес, передается на все интерфейсы с этим адресом. Только интерфейсы, добавленные в соответствующую группу многоадресной рассылки, слушают пакеты, отправленные на групповой адрес.
- Произвольный адрес (anycast address) – это идентификатор группы сетевых интерфейсов, которые обычно принадлежат разным узлам. Пакет, отправленный на произвольный адрес, доставляется в ближайший интерфейс с таким адресом, в зависимости от протоколов маршрутизации.
- В IPv6 не определены широковещательные адреса.

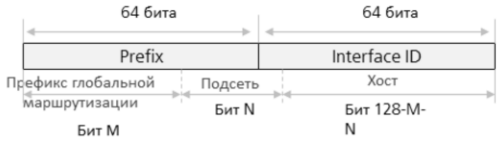


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Адреса IPv4 подразделяются на одиночные, групповые и широковещательные. Адреса IPv6 подразделяются на одиночные, групповые и произвольные.
  - Одиночный адрес идентифицирует один интерфейс. Пакет, отправленный на одиночный адрес, получает интерфейс с этим адресом.
  - Групповой адрес идентифицирует несколько интерфейсов. Пакет, отправленный на групповой адрес, получают все интерфейсы с этим адресом.
  - Произвольный адрес идентифицирует множество интерфейсов. Пакет для произвольного адреса отправляется на интерфейс, ближайший к отправителю в группе интерфейсов с таким адресом. Фактически, произвольные и одиночные адреса используют одно адресное пространство. То есть, маршрутизатор определяет, посылать ли пакет в одноадресном или произвольном режиме.

Одиночный адрес IPv6: комбинируемый глобальный одиночный адрес

- Глобальный одиночный адрес используется для сети Интернет на базе IPv6. Этот адрес является глобально уникальным и маршрутизируемым.
  - Похож на общедоступный адрес IPv4.
  - Состоит из префикса, ID подсети и ID интерфейса.



  - Префикс глобальной маршрутизации: присваивается организации провайдером. Как правило, значение состоит из минимум 48 бит. В настоящее время первые три бита каждого назначенного глобального префикса маршрутизации – 001. Таким образом, префикс равен 2000:: / 3.
  - ID подсети: используется организацией для построения локальной сети (объекта), аналогично функции ID подсети в IPv4. ID подсети отводится не более 64 бит.
  - ID хоста: идентифицирует устройство (хост), аналогично ID хоста в IPv4.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Глобальный одиночный адрес IPv6 – это адрес IPv6 с глобальным одноадресным префиксом, аналогичный общедоступному адресу IPv4. Глобальные одиночные адреса IPv6 поддерживают суммирование префиксов маршрутов, помогая ограничить число записей глобальной маршрутизации.

Одиночный адрес IPv6: адрес link-local

- Когда на узле работает протокол IPv6, каждому интерфейсу узла автоматически назначается адрес link-local. Этот адрес используется для связи с другими хостами в одном канале.
  - Адрес link-local в IPv6 может использоваться для связи между узлами в одном канале и широко используется для обнаружения соседей и конфигурации адресов без сохранения состояния (stateless address).
  - Адрес link-local использует префикс FE80:: / 10 и ID интерфейса в качестве последних 64 бит.
  - Каждый интерфейс IPv6 должен иметь адрес link-local.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Адреса link-local используются только в связи между узлами в одном локальном канале. Адрес link-local использует префикс FE80::/10 в качестве первых 10 бит (1111111010 в двоичном формате) и ID интерфейса в качестве последних 64 бит.
- Когда на узле работает протокол IPv6, каждому интерфейсу узла автоматически назначается адрес link-local, состоящий из фиксированного префикса и ID интерфейса в формате EUI-64. Этот механизм позволяет двум узлам IPv6 в одном канале взаимодействовать без дополнительных конфигураций, поэтому адреса link-local широко используются для обнаружения соседей и конфигурации адресов без сохранения состояния.
- Маршрутизаторы не отправляют устройствам в разных каналах пакеты IPv6 с адресом link-local в качестве адреса отправителя или получателя.

Одиночный адрес IPv6: уникальный локальный адрес

- Для замены адреса site-local и обеспечения уникальности локального адреса, протокол RFC4193 вводит понятие уникального локального адреса для предотвращения проблем, вызванных раскрытием частных адресов IPv4 в общедоступной сети.
  - Уникальный локальный адрес, похожий на адрес частной сети в IPv4, может использоваться только в локальной сети и не может быть маршрутизирован в Интернет-сети на базе протокола IPv6.
  - Фиксированным префиксом уникального локального адреса является FC00:: / 7. Префикс разделен на две части. Часть FC00:: / 8 не определена, а другая часть –FD00:: / 8 имеет следующий формат:

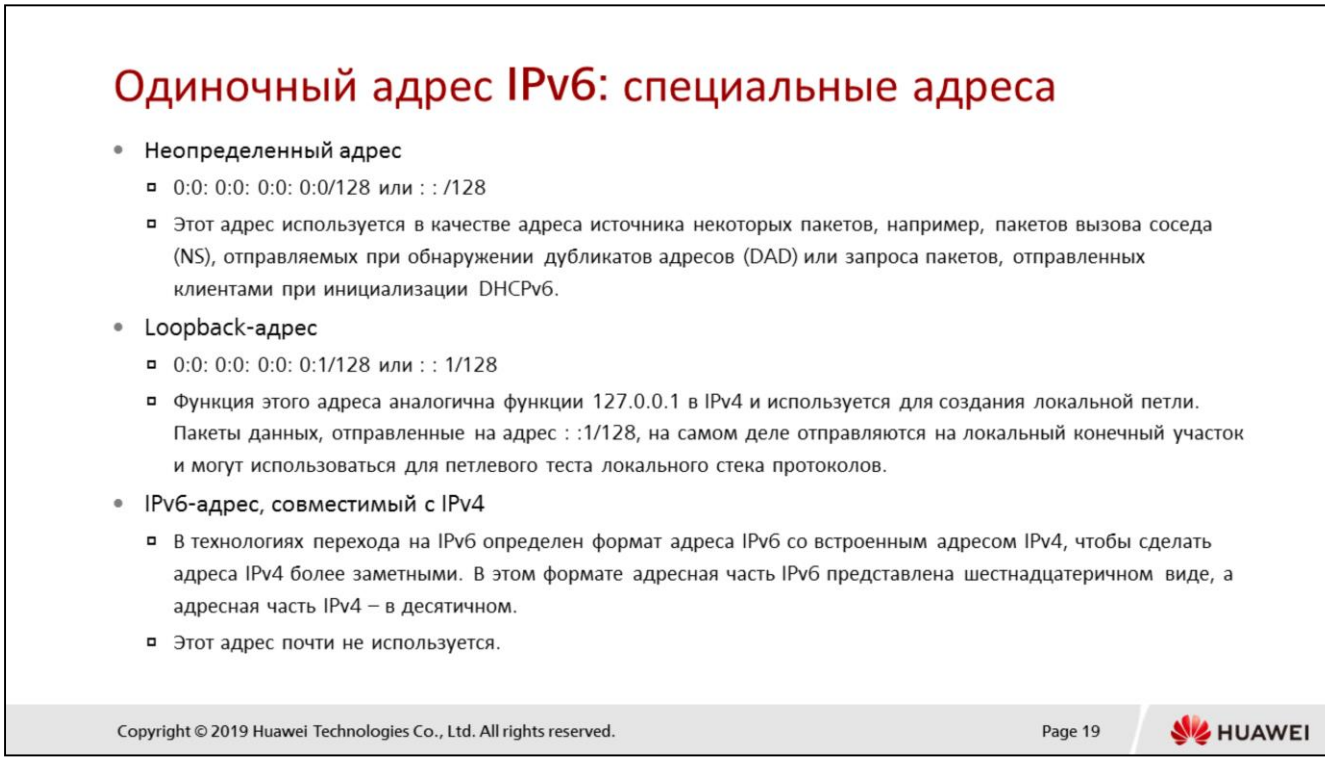


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Уникальные локальные адреса используются внутри объекта. Адреса site-local, согласно RFC 3879, были заменены уникальными локальными адресами (RFC4193).
- Уникальные локальные адреса аналогичны частным адресам IPv4. Любая организация, которая не получает глобальный одиночный адрес от провайдера, может использовать уникальный локальный адрес. Однако уникальные локальные адреса маршрутизируются только в локальной сети, а не в Интернете в целом.
- Описание:
  - Prefix: фиксированное значение FC00::/7.
  - L: установлено значение 1, если адрес действителен в локальной сети. Значение 0 зарезервировано для дальнейшего расширения.
  - Global ID: глобально уникальный префикс, который присваивается псевдослучайно (см. подробнее в RFC 4193).
  - Subnet ID: идентифицирует подсеть внутри объекта.
  - Interface ID: идентификатор интерфейса.
- Уникальный локальный адрес имеет следующие характеристики:
  - Имеет глобально уникальный префикс, который назначается псевдослучайно с высокой вероятностью уникальности.
  - Обеспечивает частные соединения между подсетями без создания адресных конфликтов.
  - Имеет общеизвестный префикс (FC00:: / 7), который позволяет легко фильтровать маршруты на границах объекта.
  - Не вступает в конфликт с какими-либо другими адресами, если он случайно маршрутизирован за пределы подсети.
  - Выполняет роль глобального одиночного адреса для приложений.

- Не зависит от Интернет-провайдеров.



- Неопределенный адрес
  - Неопределенный адрес IPv6 – это адрес 0:0: 0:0: 0:0: 0:0/128 или ::/ 128, который указывает на то, что у интерфейса или узла нет IP-адреса. Он может использоваться в качестве IP-адреса отправителя некоторых пакетов, таких как сообщения вызова соседа (NS), при обнаружении дублирующих адресов (DAD). Маршрутизаторы не отправляют пакеты с неопределенным адресом в качестве IP-адреса отправителя.
- Loopback-адрес
  - Loopback-адрес IPv6 – это адрес 0:0:0:0:0:0:0:1/128 или ::1/128. Аналогично loopback-адресу IPv4 127.0.0.1, loopback-адрес IPv6 используется, когда узел должен отправлять пакеты IPv6 самому себе. Loopback-адрес IPv6 обычно используется в качестве IP-адреса виртуального интерфейса, например, loopback-интерфейса. Loopback-адрес не может использоваться в качестве IP-адреса отправителя или получателя пакетов для переадресации.

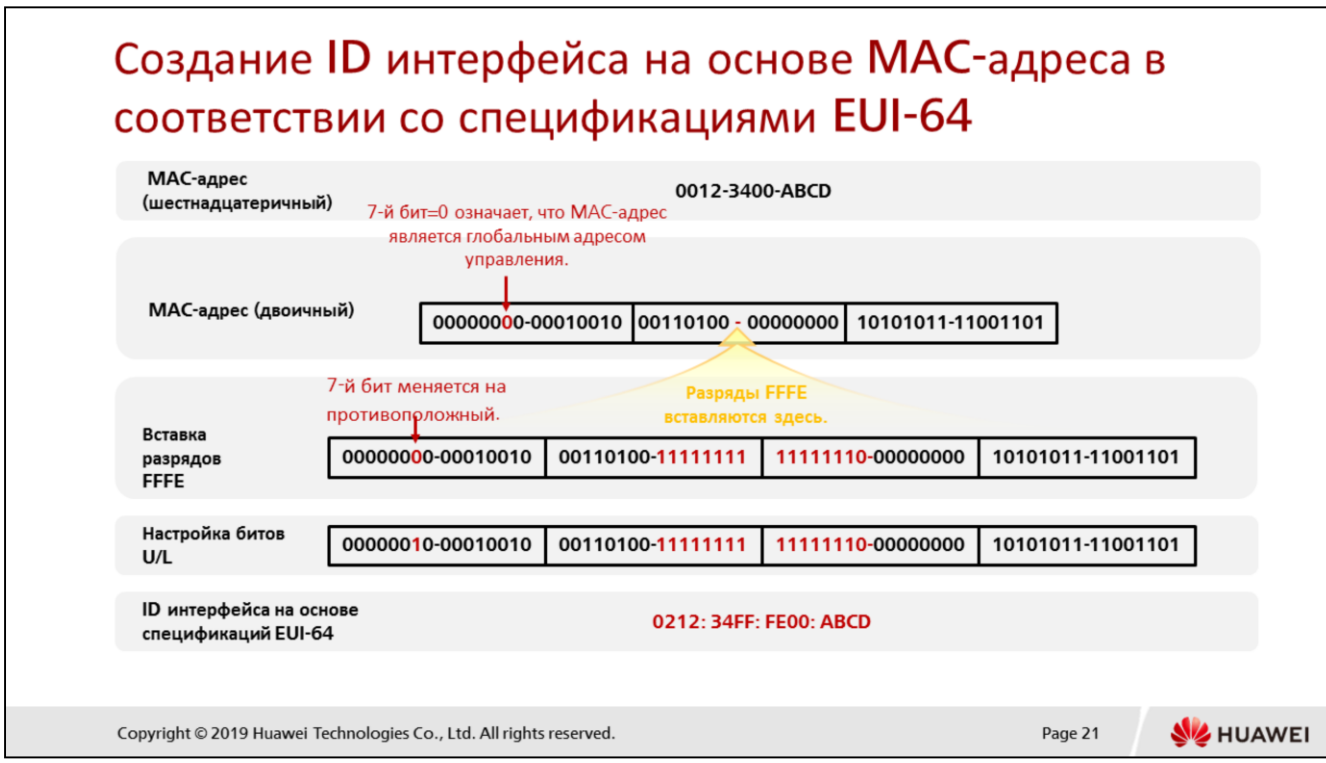
Методы создания ID интерфейса

- ID интерфейса (64 бита) используется для определения интерфейса в канале. ID интерфейса должен быть уникальным в каждом канале.
- Вы можете настроить ID интерфейса вручную, создать его через системное программное обеспечение или создать его в формате 64-битного расширенного уникального идентификатора IEEE (EUI-64).
  - Ручная конфигурация: рекомендуется сконфигурировать ID интерфейса на серверах и ключевых сетевых устройствах.
  - Автоматическое создание через системное программное обеспечение: этот метод предназначен для защиты конфиденциальности хоста.
  - Автоматическое создание в формате IEEE EUI-64: этот метод используется чаще всего.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Если первые 3 бита одиночного адреса IPv6 не равны 000, ID интерфейса должен содержать 64 бита. Если первые 3 бита равны 000, таких ограничений не существует.
- ID интерфейса составляет 64 бита и определяет интерфейс в канале. ID интерфейса должен быть уникальным в каждом канале. ID интерфейса используется для многих целей, наиболее распространенная из которых – привязка к префиксу адреса link-local, которая образует адрес link-local интерфейса. Также при автоматической настройке без отслеживания состояния ID интерфейса может быть привязан к префиксу глобального одиночного адреса IPv6 для формирования глобального одиночного адреса интерфейса.
- Критерии IEEE EUI-64
  - Преобразование MAC-адресов в ID интерфейса IPv6 снижает нагрузку по конфигурированию. При использовании автоматической настройки без отслеживания состояния (подробно описанной в более поздних разделах) требуется только префикс сети IPv6 для получения адреса IPv6.
  - Однако один из недостатков этого метода заключается в том, что адрес IPv6 легко вычисляется на основе MAC-адреса и поэтому может использоваться для злонамеренных действий.



- MAC-адрес интерфейса показан на предыдущем рисунке. Согласно спецификациям EUI-64 ID интерфейса может быть рассчитан на основе MAC-адреса. Как и MAC-адрес, ID интерфейса уникален на глобальном уровне. Процесс расчета выглядит следующим образом:
- EUI-64 вставляет разряд FFFE между идентификатором поставщика и идентификатором расширения MAC-адреса (разделенный пополам), а затем значение седьмого бита (бит U/L) 0 изменяется на 1, чтобы показать, что ID интерфейса уникален на глобальном уровне.
- В одиночном MAC-адресе седьмым битом первого байта является бит U/L (Universal/Local, также называемый G/L, где G означает «глобальный»), который используется для обозначения уникальности MAC-адреса. Если бит U/L равен 0, то MAC-адрес является глобальным адресом управления, который присваивается поставщиком с Уникальным идентификатором организации (OUI). Если бит U/L равен 1, то MAC-адрес является локальным адресом управления, который настраивается сетевым администратором на основании цели услуги.
- В ID интерфейса, созданного согласно стандарту EUI-64, значение седьмого бита противоположно значению 7 бита в MAC-адресе. 0 означает локальное управление, а 1 -глобальное управление. Следовательно, если в ID интерфейса бит U/L равен 1, то адрес глобально уникален; если значение равно 0, адрес локально уникален. Поэтому значение этого бита необходимо поменять на противоположное.

Групповой адрес IPv6

- Групповой адрес определяет группу интерфейсов. Данные, отправленные на групповой адрес, передаются нескольким устройствам, которые слушают адрес.
- Диапазон адресов: FF00: : / 8



- **Flags**
  - Означает постоянную или временную группу многоадресной рассылки.
  - 0000 означает постоянный или хорошо известный адрес.
  - 0001 означает временный адрес.
- **Scope**
  - Указывает диапазон группы многоадресной рассылки.
- **Group ID**
  - Указывает ID группы многоадресной рассылки.

0: Зарезервировано
1: Node-local
2: Link-local, например, FF02:: 1
5: Site-local
8: Organization-local
E: Global scope
F: Зарезервировано

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Как и групповой адрес IPv4, групповой адрес IPv6 идентифицируют группу интерфейсов, которые обычно принадлежат разным узлам. Узел может принадлежать любому количеству групп многоадресной рассылки. Пакеты, отправленные на групповой адрес IPv6, доставляются всем интерфейсам, идентифицированным по адресу многоадресной рассылки.
- Flag:
  - 0000: постоянный групповой адрес.
  - 0001: временный групповой адрес.
  - Примечание: первые три бита зарезервированы как 0.
- Область применения
  - 0001: указывает область local-interface. Он действует на одном интерфейсе и применим только к loopback-интерфейсам.
  - 0010: указывает на область действия link-local.
  - 0100: указывает на область действия local-administration, настраиваемую администратором.
  - 0101: указывает на область действия site-local.
  - 1000: указывает на область local-organization, то есть диапазон объектов одной организации.
  - 1110: указывает на глобальный охват.

- Group ID:
  - Идентификатор группы многоадресной рассылки.

Категория адресов IPv6: предопределенный групповой адрес

- Node-local
  - FF01: 0: 0: 0: 0: 0: 0: 1: групповой адрес всех узлов
  - FF01: 0: 0: 0: 0: 0: 0: 2: групповой адрес всех маршрутизаторов
- Link-local
  - FF02: 0: 0: 0: 0: 0: 0: 1: групповой адрес всех узлов
  - FF02: 0: 0: 0: 0: 0: 0: 2: групповой адрес всех маршрутизаторов
  - FF02: 0: 0: 0: 0: 1: FFXX: XXXX: групповой адрес запрошенных узлов
  - FF02: 0: 0: 0: 0: 0: 0: 5: групповой адрес всех маршрутизаторов с протоколом OSPF
  - FF02: 0: 0: 0: 0: 0: 0: 6: групповой адрес всех DR-маршрутизаторов с протоколом OSPF
  - FF02: 0: 0: 0: 0: 0: 0: D: групповой адрес всех PIM-маршрутизаторов

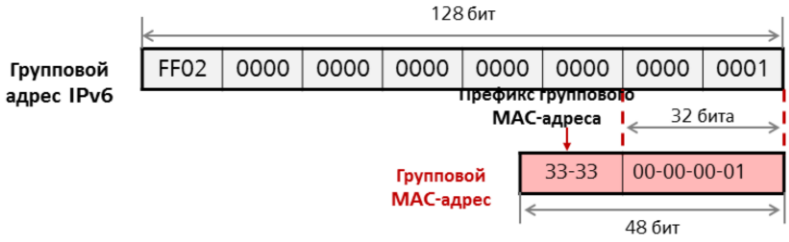
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Аналогично IPv4, IPv6 имеет специальные групповые адреса. Например:
  - **FF01::1 (адрес всех узлов в node-local)**
  - FF02: : 1 (адрес всех узлов в link-local)
  - FF01: : 2 (адрес всех маршрутизаторов в node-local)
  - FF02: : 2 (адрес всех маршрутизаторов в link-local)
  - FF05: : 2 (адрес всех маршрутизаторов в site-local)

Сопоставление между групповым адресом IPv6 и групповым MAC-адресом IPv6

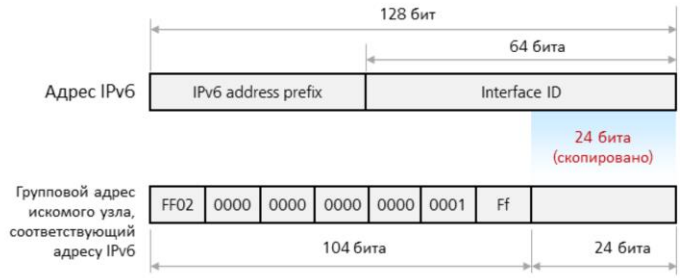
- В Ethernet многоадресный пакет IPv6 должен быть инкапсулирован в режиме Ethernet.
- IP-адрес назначения многоадресного пакета IPv6 является групповым адресом IPv6, а MAC-адрес назначения должен быть групповым MAC-адресом, который должен соответствовать групповым адресам IPv6.
- 33-33 является префиксом MAC-адреса, зарезервированным для групповых IPv6-адресов. Последние 32 бита MAC-адреса копируются из последних 32 бит соответствующего группового адреса IPv6.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Групповой адрес искомого узла

- Групповой адрес искомого узла (solicited-node multicast address) генерируется на основе одиночного или произвольного адреса узла. Когда узел имеет одиночный или произвольный адрес IPv6, для узла генерируется групповой адрес искомого узла, и узел присоединяется к группе многоадресной рассылки, соответствующей его одиночному или произвольному адресу IPv6.
- Одиночный или произвольный адрес соответствует групповому адресу искомого узла. Этот адрес используется для обнаружения соседей (ND) и дублированных адресов (DAD).
- Групповой адрес искомого узла состоит из фиксированного префикса FF02::1:FF00: 0/104 и последних 24 битов соответствующего адреса IPv6. Допустимой областью применения группового адреса искомого узла является область link-local.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

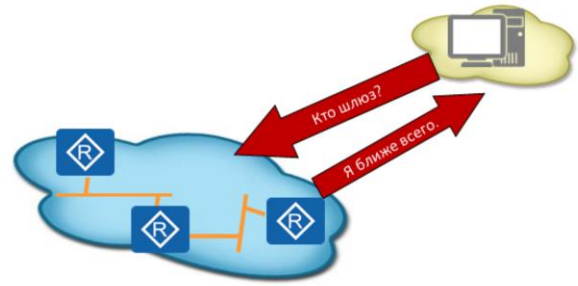
HUAWEI

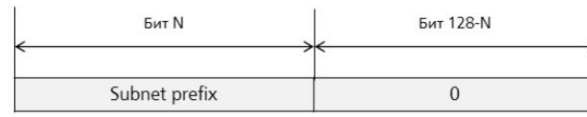
- Когда узел имеет одиночный или произвольный адрес IPv6, для узла генерируется групповой адрес искомого узла, и узел присоединяется к группе многоадресной рассылки, соответствующей его одиночному или произвольному адресу IPv6. Каждый одиночный или произвольный адрес соответствует групповому адресу искомого узла, который часто используется при преобразовании адресов, обнаружении соседей и обнаружении дублированных адресов.
- Групповой адрес искомого узла состоит из префикса FF02:: 1: FF00:0/104 и последних 24 бит соответствующего адреса IPv6. Допустимой областью применения группового адреса искомого узла является область link-local.
- Какова функция группового адреса искомого узла? Для примера возьмем протокол ARP в IPv4. ARP в основном используется для преобразования адресов. Когда устройству требуется разрешение IP-адреса для MAC-адреса, он посылает широковещательный кадр ARP-запроса, чтобы все узлы в широковещательном домене могли получить широковещательный кадр. Однако узлам, за исключением узла назначения, нет необходимости анализировать кадр (до полезной нагрузки ARP), так как это действие приведет к потере ресурсов устройства.
- Когда в сети IPv6 устройство нуждается в MAC-адресе, отображающем адрес IPv6, устройство отправляет пакет Request. Этот пакет представляет собой многоадресный пакет, чей адрес получателя IPv6 является групповым адресом искомого узла, соответствующим одиночному адресу получателя IPv6. MAC-адрес получателя пакета Request –это групповой MAC-адрес, соответствующий групповому адресу. Только узел назначения слушает групповой адрес искомого

узла. Поэтому когда другие устройства получают кадр, они идентифицируют его на основе MAC-адреса получателя на уровне сетевого адаптера и отбрасывают его.

Произвольный адрес IPv6

- Произвольные адреса IPv6 представляют собой специфические адреса IPv6. Произвольный адрес определяет группу интерфейсов, которые, как правило, относятся к разным узлам.
- Пакет, отправленный на произвольный адрес, отправляется на ближайший интерфейс, который идентифицируется по адресу.
- Произвольные адреса выделяются из пространства одиночных адресов с использованием любого из определенных форматов одиночных адресов.
- Таким образом, при конфигурировании произвольного адреса необходимо указать, что это произвольный адрес.





Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Произвольные адреса IPv6 представляют собой специфические адреса IPv6. Произвольный адрес определяет группу интерфейсов, которые, как правило, относятся к разным узлам. Пакет, отправленные на произвольный адрес, доставляются на ближайший интерфейс, идентифицированный по адресу, в зависимости от протоколов маршрутизации. Произвольный адрес используется для связи один-ко-многим. Получатель должен принадлежать группе интерфейсов. Например, мобильный абонент получает доступ к ближайшей приемной станции на основе физического местоположения. Таким образом, мобильные абоненты не ограничены своим местоположением.
- Произвольные адреса выделяются из пространства одиночных адресов с использованием любого из определенных форматов одиночных адресов. Таким образом, произвольные адреса синтаксически неотличимы от одиночных адресов. Узел, которому присвоен произвольный адрес, должен быть настроен так, чтобы он знал, что у него произвольный адрес. В настоящее время произвольные адреса используются только в качестве адресов назначения и назначаются только маршрутизаторам.
- Произвольный адрес маршрутизатора подсети определен в протоколе RFC 3513 и ID интерфейса такого адреса состоит из 0.
- Пакеты, предназначенные для произвольного адреса маршрутизатора подсети, доставляются на определенный маршрутизатор (ближайший маршрутизатор, идентифицированный по адресу) в подсети, указанной в префиксе адреса. Ближайший маршрутизатор определяется как ближайший с точки зрения

расстояния маршрутизации.

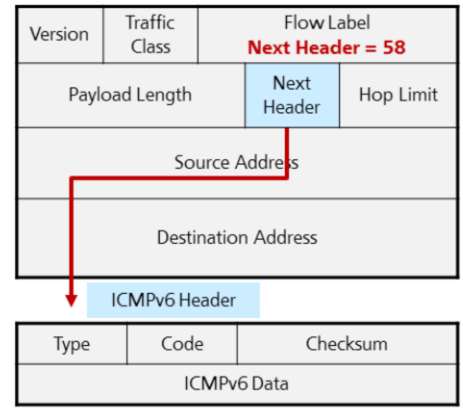
Содержание

1. История технологии IPv6
2. **Реализация протокола IPv6**
   - Форматы пакетов
   - Классификация адресов
   - **Базовый протокол**
   - Технологии перехода
3. Команды конфигурации IPv6
4. Советы по подготовке к экзаменам по протоколу IPv6

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Обзор ICMPv6

- ICMPv6 является одним из базовых протоколов IPv6 и используется узлами IPv6 для представления информации о переадресации пакетов или ошибках узлу-источнику.
- Номера типа протокола ICMPv6, то есть поле IPv6 Next Header, - 58.
- ICMPv6 предоставляет дополнительные механизмы наряду с текущими функциями ICMPv4, такими как обнаружение соседей (ND), конфигурация адресов без сохранения состояний, обнаружение дублирующих адресов (DAD) и обнаружение пути MTU (PMTU).



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Номер протокола ICMPv6 (т.е. значение поля Next Header в пакете IPv6) равен 58.
- В IPv4, ICMP передает информацию о переадресации IP-пакетов и ошибки в узел-источник. ICMP определяет некоторые сообщения, такие как Destination Unreachable, Packet Too Big, Time Exceeded, Echo Request и Echo Reply для облегчения диагностики неисправностей и управления информацией. В дополнение к текущим функциям ICMPv4, ICMPv6 предоставляет такие механизмы, как обнаружение соседей (ND), конфигурация адресов без сохранения состояний (включая обнаружение дублирующих адресов) и обнаружение пути MTU.
- Поэтому ICMPv6 является базовым протоколом для других механизмов IPv6.
- Описание пакета:
  - Type: задает тип сообщения. Значения от 0 до 127 указывают тип сообщения об ошибке, а значения от 128 до 255 обозначают тип информационного сообщения.
  - Code: указывает конкретный тип сообщения.
  - Checksum: указывает контрольную сумму сообщения ICMPv6.

ICMPv6

Сообщение	Тип	Описание	Код
Сообщение об ошибке	1	Destination Unreachable (адресат не досягаем)	0: нет маршрута
			1: связь с узлом назначения запрещена администратором
			2: Не указано
			3: Недоступный адрес
			4: Недоступный порт
	2	Packet Too Big (слишком большой пакет)	0
	3	Time Exceeded (истекло время)	0: Превышение количества узлов в транзите
			1: Превышено время сборки фрагментов
	4	Parameter Problem (проблема с параметром)	0: Ошибка в поле заголовка
			1: Неизвестный тип следующего заголовка
			2: Неизвестный параметр IPv6
Информационное сообщение	128	Echo Request (Эхо-запрос)	0
	129	Echo Reply (Эхо-ответ)	0

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Сообщение Destination Unreachable
  - Когда пакет данных не отправляется на узел назначения или в протокол верхнего уровня, маршрутизатор или узел назначения отправляет сообщение ICMPv6 Destination Unreachable. В сообщении ICMPv6 Destination Unreachable значение поля Type установлено на 1, а значение поля Code – от 0 до 4. Каждый код имеет определенное значение (см. RFC 2463):
    - 0: нет маршрута к узлу назначения
    - 1: связь с узлом назначения запрещена администратором
    - 2: не указано
    - 3: недоступный адрес
    - 4: недоступный порт
- Сообщение Packet Too Big
  - Сообщение Packet Too Big отправляется маршрутизатором в ответ на пакет, который маршрутизатор не может переадресовать, так как пакет больше MTU исходящего канала. Информация в этом сообщении используется для обнаружения пути MTU. В сообщении Packet Too Big значение поля Type установлено на 2, а значение поля Code – на 0.
- Сообщение Time Exceeded
  - Если маршрутизатор получает пакет с лимитом узлов, равным нулю, маршрутизатор отбрасывает пакет, создает сообщение ICMPv6 Time Exceeded и отправляет его узлу-источнику. В сообщении ICMPv6 Time Exceeded значение поля Type установлено на 3, а

значение поля Code – на 0 или 1.

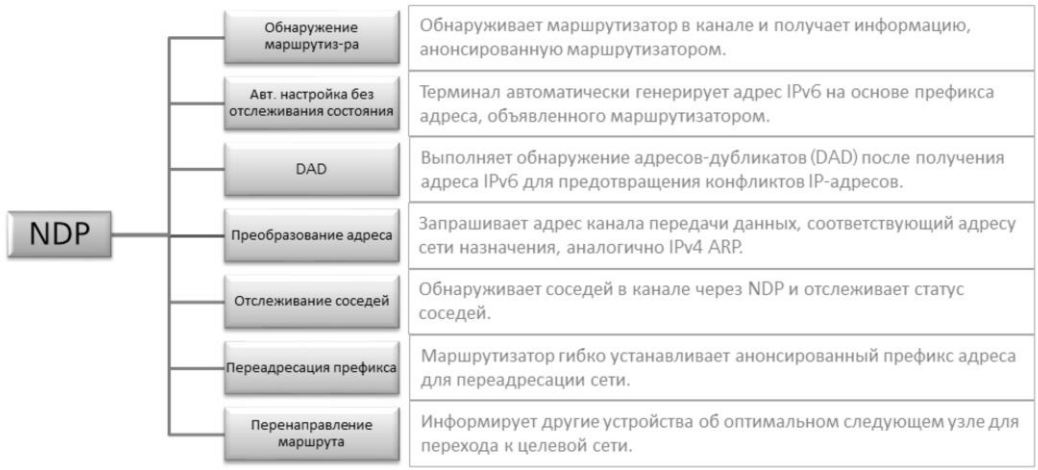
- 0: превышение количества узлов в транзите
- 1: превышено время сборки фрагментов

- Сообщение Parameter Problem
  - Если узел IPv6, обрабатывающий пакет, обнаруживает проблему с полем в заголовке IPv6 или расширенных заголовках, которая мешает завершению обработки пакета, он отбрасывает пакет и отправляет сообщение ICMPv6 Parameter Problem источнику пакета, указывая тип и местоположение проблемы. В сообщении Parameter Problem значение поля Type установлено на 4, значение поля Code варьируется от 0 до 2, а 32-битное поле Point указывает на местоположение проблемы. Значение поля Code выглядит следующим образом:
    - 0: ошибка в поле заголовка
    - 1: неизвестный тип следующего заголовка
    - 2: неизвестный параметр IPv6
- RFC2463 определяет только два типа информационных пакетов: сообщения Echo Request и Echo Reply
  - Сообщение Echo Request
    - Сообщения Echo Request отправляются в узлы назначения. Получив сообщение Echo Request, узел назначения отвечает сообщением Echo Reply. В сообщении Echo Request значение поля Type равно 128, значение поля Code равно 0. Поля Identifier и Sequence Number задаются на исходном узле. Они используются для сопоставления пакета Echo Reply с отправленным пакетом Echo Request.

- Сообщение Echo Reply
  - Получив сообщение Echo Request, узел назначения отвечает сообщением Echo Reply. В сообщении Echo Reply значение поля Type равно 129, а значение поля Code – 0. Значения полей Identifier и Sequence Number в сообщении Echo Reply должны быть такими же, как и в сообщении Echo Request.

Обзор протокола обнаружения соседей (NDP), используемого с IPv6

- Описание протокола NDP приведено в RFC2462 и RFC4861. NDP реализует многие важные механизмы IPv6, как показано на схеме ниже.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

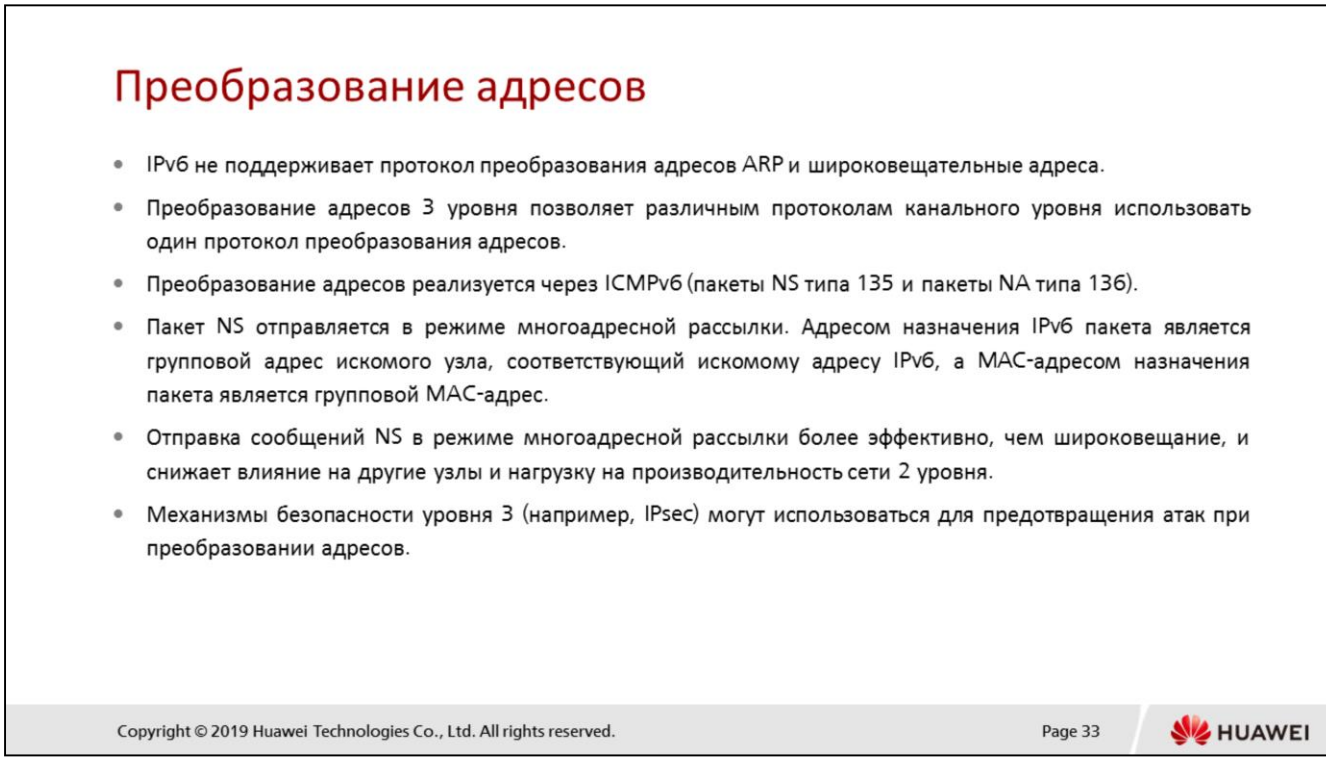
- Обнаружение маршрутизатора: данная функция помогает устройству обнаруживать маршрутизаторы в канале и получать информацию, анонсированную маршрутизаторами.
- Автоматическая настройка без отслеживания состояния: это функция выделения IPv6. Она позволяет хостам IPv6 легко подключаться к сетям IPv6 по стандарту plug and play. Благодаря этой функции вам не требуется вручную конфигурировать сложные IPv6-адреса или развертывать серверы приложений (например, серверы DHCP), чтобы назначать адреса хостам. Механизм автоматической настройки без отслеживания состояния использует сообщения Router Solicitation (RS) и Router Advertisement (RA) в ICMPv6.
- Обнаружение адресов-дубликатов (DAD): это важный механизм. Адрес IPv6 может использоваться только обработки DAD. Он определяет, существует ли конфликт адресов IPv6 в канале.
- Преобразование адресов: IPv6 не использует протокол ARP, как IPv4, но использует сообщения Neighbor Solicitation (NS) и Neighbor Advertisement (NA), определенные в NDP для преобразования адресов.
- Отслеживание соседей: IPv6 определяет соседнюю машину состояния между узлами и поддерживает преобразование адресов IPv6 и адресов 2 уровня (например, MAC-адресов) соседей. Соответствующие записи хранятся в таблице соседа IPv6 устройства.
- Переадресация префикса: маршрутизатор IPv6 анонсирует информацию префикса IPv6 локальному каналу через сообщения ICMPv6 RA. Таким образом, хосты могут автоматически генерировать свои собственные одиночные адреса IPv6 на основе информации префикса в сообщениях RA. Эти автоматически получаемые адреса имеют определенное время жизни (TTL). Анонсирование префикса адреса IPv6 в сообщениях PA и гибкая настройка TTL адресов позволяют старому префиксу плавно мигрировать в новый. Это устраняет необходимость переконфигурирования адресов на хостах, значительно сокращая необходимость в ручной настройке.
- Перенаправление маршрута: маршрутизатор посылает сообщение ICMPv6 Redirection на узел IPv6, чтобы уведомить его о существовании лучшего следующего узла к точке назначения в локальном канале. Функция перенаправления в IPv6 такая же, как аналогичная функция IPv4.

Пакеты ICMPv6, используемые NDP

Пакет ICMPv6 / Механизм	RS 133	RA 134	NS 135	NA 136	Redirection 137
Преобразование адресов			•	•	
Анонсирование префикса	•	•			
Переадресация префикса	•	•			
DAD			•	•	
Перенаправление маршрута					•

- RS: вызов маршрутизатора
- RA: объявление маршрутизатора
- NS: вызов соседа
- NA: объявление соседа

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.



- Адрес IPv4 можно преобразовать в адрес link-layer с помощью протокола ARP. Протокол ARP работает на уровне 2. В протоколе обнаружения соседей (RFC2461) описывается преобразование адресов IPv6 с использованием пакетов ICMPv6 для преобразования адресов на уровне 3. Этот механизм имеет следующие преимущества:
  - Расширенная независимость сред. Нам не нужно определять новый протокол преобразования адресов для каждого канального уровня, а можно использовать один протокол преобразования адресов на всех уровнях.
  - Механизм безопасности 3 уровня (например, подделка пакетов ARP Reply для кражи потоков данных) представляет собой серьезную угрозу безопасности в IPv4. Стандартный механизм аутентификации 3 уровня (например, IPsec) может использоваться для решения этой проблемы при преобразовании адресов.
  - Если пакет ARP Request отправляется в широковещательном режиме, он будет лавинно передаваться всем хостам в сети 2 уровня, что приведет к ухудшению производительности IPv4. На уровне 3 пакет запроса на преобразование адреса будет отправляться только группе искомого узла, к которой принадлежит адрес для преобразования. Передача в режиме многоадресной рассылки значительно снижает нагрузку на сеть.

Пакет преобразования адреса

- При преобразовании адресов используются два типа пакетов ICMPv6: пакет Neighbor Solicitation (NS) и пакет Neighbor Advertisement (NA)
- **Пакет NS**
  - Type = 135, Code = 0
  - Целевым адресом (Target Address) является адрес IPv6, который подлежит преобразованию, и он не может быть групповым адресом.
- **Пакет NA**
  - Type = 136, код = 0
  - Флаг R (Router flag) указывает, является ли отправитель маршрутизатором. Если значение равно 1, отправитель является маршрутизатором.
  - Флаг S (Solicited flag) указывает, посылается ли пакет Neighbor Advertisement (NA) в ответ на пакет Neighbor Solicitation (NS). Если значение равно 1, то пакет NA отправляется в ответ на пакет NS.
  - Флаг O (Override flag) указывает, аннулирует ли информация в пакете NA существующую информацию в адресе. Если значение равно 1, то новая информация записывается поверх существующей.
  - Target Address – это адрес IPv6, соответствующий адресу канального уровня.

Type	Code	checksum
Reserved		
Target Address		
Options…		

Type			Code	Checksum
R	S	O	Reserved	
Target Address				
Options…				

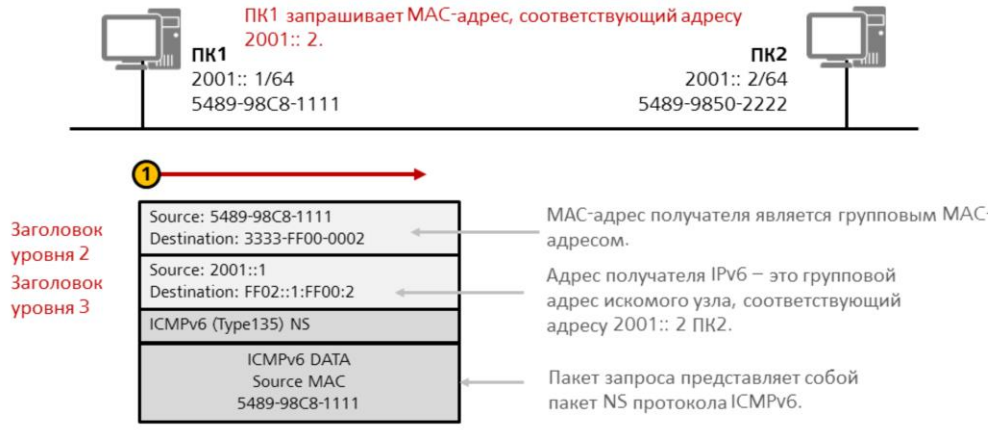
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- При преобразовании адресов используются два типа пакетов ICMPv6: сообщения Neighbor Solicit (NS) и Neighbor Advertisement (NA)
- Сообщение NS
  - Значение поля ICMP Type равно 135, а значение поля Code – 0.
  - Целевым адресом (Target Address) является адрес IPv6, который подлежит преобразованию, и он не может быть групповым адресом.
  - Адрес канального уровня отправителя сообщения NS инкапсулируется в поле Опции (Options).
- Сообщение NA
  - Значение поля ICMP Type равно 136, значение поля Code равно 0.
  - Флаг R (Router flag) указывает, является ли отправитель маршрутизатором. Если значение равно 1, отправитель является маршрутизатором.
  - Флаг S (Solicited flag) указывает, посылается ли сообщение NA в ответ на сообщение NS. Если значение равно 1, то пакет сообщение NA отправляется в ответ на сообщение NS.
  - Флаг O (Override flag) указывает, аннулирует ли информация в пакете NA существующую информацию в адресе. Если значение равно 1, то новая информация записывается поверх существующей.
  - Target Address – это адрес IPv6, соответствующий адресу канального уровня.
  - Запрашиваемый адрес канального уровня инкапсулируется в поле Options в

формате TLV. См. подробнее в RFC2463.

Преобразование адреса (1/2)

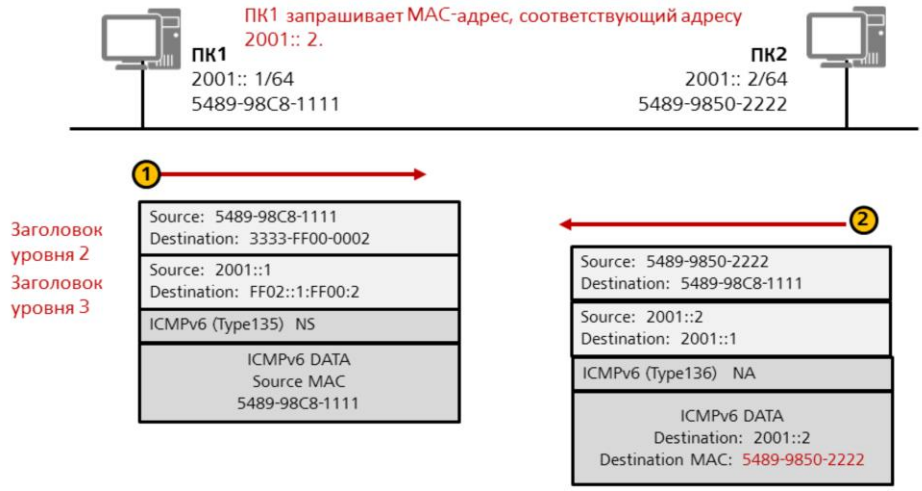


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Существует два типа сообщений: NS и NA. Как два хоста могут получить адреса канального уровня друг друга?
- В сценарии, показанном на рисунке выше, если ПК1 запрашивает MAC-адрес, соответствующий адресу 2001:: 2 ПК2, ПК1 посылает сообщение NS. Исходным адресом сообщения NS является 2001:: 1, а адресом назначения является групповой адрес искомого узла, соответствующий адресу 2001:: 2.
- Затем заголовок кадра инкапсулируется в пакет IPv6. MAC-адрес источника является MAC-адресом ПК1, а MAC-адресом назначения является отображение MAC-адреса группового адреса искомого узла, соответствующий адресу 2001:: 2. MAC-адрес назначения является групповым MAC-адресом.
- Таким образом, выполняется двунаправленный обмен адресами канального уровня.

Преобразование адреса (2/2)



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Другие узлы, за исключением R2, также получают кадр данных. Когда узел извлекает заголовок кадра, он находит, что MAC-адрес назначения является групповым MAC-адресом, который не прослушивается на локальном устройстве. Поэтому кадр данных отбрасывается сетевым адаптером.
- Локальный сетевой адаптер получает кадр данных с MAC-адресом назначения 3333-FF00-0002. После того, как ПК2 получает и проверяет кадр данных, локальный сетевой адаптер обнаруживает, что пакет представляет собой пакет IPv6 на основании поля Type в заголовке кадра. Затем он удаляет заголовок кадра и отправляет пакет IPv6 в стек протоколов IPv6 для обработки. Стек протоколов IPv6 обнаруживает, что пакет предназначен для группового адреса искомого узла FF02:: 1: FF00:2 на основании адреса получателя IPv6 в заголовке IPv6. Локальный сетевой адаптер присоединился к группе многоадресной рассылки. Поле Next Header в заголовке пакета IPv6 означает, что пакет ICMPv6 инкапсулируется после заголовка пакета IPv6. Поэтому ПК2 удаляет заголовок пакета IPv6 и отправляет пакет ICMPv6 в протокол ICMPv6 на обработку. Наконец, ICMPv6 обнаруживает, что пакет представляет собой сообщение NS, запрашивающее MAC-адрес, соответствующий адресу 2001:: 2. В ответ ПК2 отправляет ПК1 сообщение NA, содержащее MAC-адрес ПК2.

Проверка таблицы маршрутизации соседей IPv6

- В отличие от IPv4, IPv6 не использует таблицу ARP для кэширования соответствий между IP-адресами и MAC-адресами. Вместо этого у него есть таблица маршрутизации соседей IPv6. В устройстве передачи данных Huawei можно выполнить команду **display ipv6 neighbors**, чтобы посмотреть эту таблицу.

```
[R1] display ipv6 neighbors
------------------------------------------------------------------------------
IPv6 Address    : 2012::2
Link-layer      : 00e0-fcc2-13b6              State : STALE
Interface       : GE0/0/0                     Age   : 0
VLAN            : -                           CEVLAN: -
VPN name        :                             Is Router: TRUE
Secure FLAG     : UN-SECURE

IPv6 Address    : FE80::2E0:FCFF:FEC2:13B6
Link-layer      : 00e0-fcc2-13b6              State : STALE
Interface       : GE0/0/0                     Age   : 0
VLAN            : -                           CEVLAN: -
VPN name        :                             Is Router: TRUE
Secure FLAG     : UN-SECURE
------------------------------------------------------------------------------
Total: 2     Dynamic: 2     Static: 0
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- На устройстве с операционной системой Windows 7 можно выполнить команду **netsh interface ipv6 show neighbors** для проверки кэшированной информации соседа.

Типы состояния соседа

- Для мониторинга состояния каждого соседнего устройства узлу необходимо поддерживать актуальность таблицы информации о соседе, а переход между состояниями должен быть разрешен.
- Существует пять типов состояний соседей:
  - INCOMPLETE: это состояние указывает на то, что пакет NS был отправлен на групповой адрес искомого узла назначения, но пакет NA не был получен.
  - REACHABLE: это состояние указывает на то, что сосед доступен, и для подтверждения не нужно отправлять какие-либо пакеты.
  - STALE: это состояние указывает на то, что прошло более 30 секунд после получения последнего подтверждения доступности соседа.
  - DELAY: это состояние указывает на то, что пакет был отправлен, когда сосед находился в состоянии stale, и в течение пяти секунд не было получено подтверждение доступности соседа.
  - PROBE: это состояние указывает на то, что пакет NS повторно передается каждую секунду для обнаружения доступности соседа до получения подтверждения.

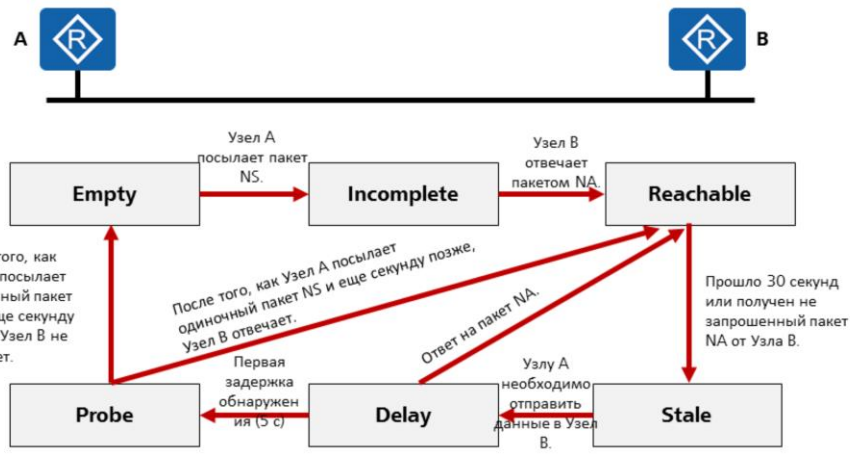
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- В предыдущих разделах описывается процесс преобразования адресов. Однако в процессе коммуникации необходимо поддерживать таблицу информации о соседях. В таблице у каждый сосед находится в своем состоянии и может переключаться между состояниями.
- RFC2461 определяет пять состояний соседей: Incomplete, Reachable, Stale, Delay и Probe.

Изменение состояния соседа

- Пример: Узел A хочет получить доступ к Узлу B, но кэш Узла A не содержит записи об Узле B. На следующем рисунке показано изменение состояний соседа.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Изменения состояния соседей является сложным процессом и не описывается здесь подробно. В следующем примере описывается изменение состояний Узла A во время его первого взаимодействия с Узлом B.
  - Узел A посылает сообщение NS и генерирует запись кэша. Состоянием соседа Узла A является Incomplete.
  - Если Узел B отвечает сообщением NA, то состояние соседа Узла A изменяется с Incomplete на Reachable. В противном случае состояние соседа меняется с Incomplete на Empty через 10 секунд, а Узел A удаляет эту запись.
  - После истечения времени проверки доступности соседа (30 секунд по умолчанию), состояние соседа изменяется с Reachable на Stale.
  - Если Узел A, находясь в состоянии Reachable, получает не запрошенное сообщение NA от Узла B и адрес канального уровня Узла B, передаваемый в сообщении, отличается полученного Узлом A адреса, то состояние соседа Узла A меняется на Stale.
  - Узел A посылает данные в Узел B. Состояние Узла A изменяется с Stale на Delay. Узел A затем посылает сообщение NS Request.
  - По истечении периода Delay_First_Probe_Time (по умолчанию 5 секунд), состояние соседа изменяется с Delay на Probe. Если в течение этого периода Узел A получает сообщение NA, то состояние соседа Узла A меняется на Reachable.
  - Узел A в состоянии Probe посылает несколько одиночных сообщений NS (MAX _ UNICAST _ SOLICIT) через настроенный интервал времени RetransTimer (1 секунда по умолчанию). Если Узел A получает ответ, его состояние меняется с Probe на Reachable. В противном случае, состояние изменяется на Empty и Узел A удаляет запись.
- Предыдущий механизм показывает, что отношения соседства IPv6 работают лучше, чем протокол IPv4 ARP. Механизм проверки состояния соседа IPv6 обеспечивает доступность соседа до начала сеанса связи, в то время как протокол ARP проверяет состояние соседа только с помощью механизма старения.

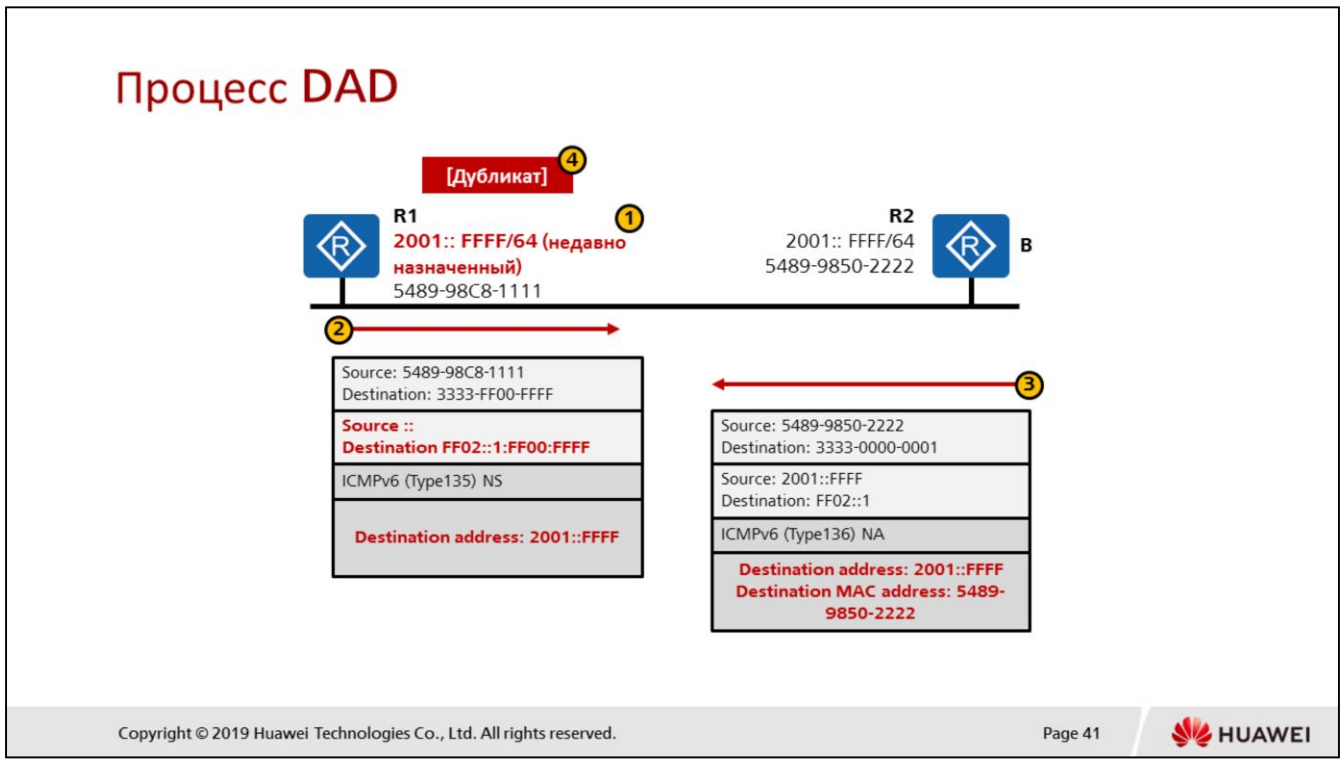
- См. в RFC2461 информацию о поддержании и изменении состояния соседа.

Обнаружение адресов-дубликатов (DAD)

- Обзор
  - Механизм DAD гарантирует, что в сети нет двух идентичных одиночных адресов.
  - Механизм DAD необходим для всех адресов.
  - Пакеты NS и NA участвуют в процессе DAD.
- Реализация
  - Адрес IPv6, назначенный интерфейсу, но не подтвержденный DAD, называется пробным адресом (tentative address). Интерфейс не может использовать пробный адрес для одиночной передачи IPv6, но он присоединится к группе многоадресной рассылки искомого узла.
  - DAD: узел посылает пакет NS в группу многоадресной рассылки искомого узла, к которой принадлежит пробный адрес. Если узел получает пакет NA с другого объекта, пробный адрес уже был использован, и этот узел не будет использовать этот пробный адрес для связи.
  - Перед назначением любого одиночного адреса IPv6 интерфейсу, включая локальный адрес (link-local), необходимо выполнить процесс DAD на интерфейсе.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI



- R2 – это сетевое устройство, использующее адрес, показанный на рисунке. Для R1 сконфигурирован новый IPv6-адрес 2001:: FFFF/64. После конфигурирования 2001:: FFFF/64 на интерфейсе R1, этот адрес становится пробным адресом и недоступен до тех пор, он не будет обработан процессом DAD.
  - R1 посылает сообщение NS на локальный канал в режиме многоадресной рассылки, при этом адресом IPv6 источника является "::", а адрес IPv6 назначения – групповым адрес искомого узла, соответствующим 2001:: FFFF, то есть FF02:: 1: FF00: FFFF для DAD. Сообщение NS содержит адрес назначения 2001:: FFFF для DAD.
  - Все узлы на канале получают это сообщение NS. Поскольку интерфейсы, на которых сконфигурирован адрес 2001:: FFFF, не добавляются в соответствующую группу многоадресной рассылки искомого узла, они отбрасывают сообщение NS. Поскольку на интерфейсе R2 сконфигурирован адрес 2001:: FFFF, он добавляется в группу многоадресной рассылки FF02:: 1: FF00: FFFF. После того, как R2 получает сообщение NS, предназначенное для адреса FF02:: 1: FF00: FFFF, он анализирует сообщение и обнаруживает, что адрес назначения для DAD совпадает с адресом локального интерфейса. Затем R2 отвечает сообщением NA с адресом назначения FF02:: 1, то есть групповым адресом всех узлов. Кроме того, в сообщении содержится адрес назначения 2001:: FFFF и MAC-адрес интерфейса на R2.
  - После того, как R1 получает сообщение NA, он знает, что адрес 2001:: FFFF уже используется в канале. Поэтому R1 обозначает адрес как дубликат, и его нельзя использовать для связи.

Процесс DAD на R1

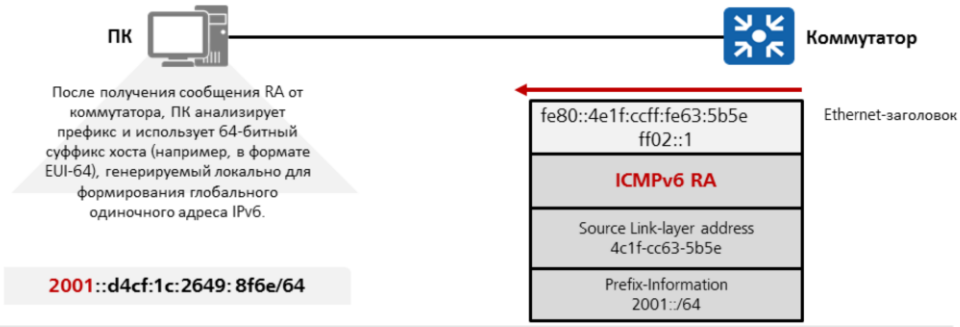


[R1] display ipv6 interface
GigabitEthernet0/0/0 current state: UP
IPv6 protocol current state: UP
IPv6 is enabled, link-local address is FE80::5489:98FF:FEC8:1111
Global unicast address(es):
2001: : FFFF, подсеть 2001::/64 [ДУБЛИКАТ]
Joined group address(es):
FF02::1:FF00:FFFF
FF02::1:FFC8:1111
FF02::2
FF02::1
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1
…

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Обзор SLAAC IPv6

- Автоконфигурация (SLAAC) – это стандартная функция IPv6, описанная в протоколе RFC2462.
- В IPv6 устройство может получать IP-адрес динамически или с помощью ручной настройки. В режиме динамического получения адреса доступны механизмы DHCPv6 и SLAAC.
- По сравнению с DHCPv6, SLAAC не требует прикладного сервера и является более легким.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- После включения автоконфигурирования IPv6 -адрес устройства не нужно настраивать вручную – устройство находится в состоянии plug and play, за счет чего снижается нагрузка на управление сетью.
- Процесс:
  - Хост автоматически генерирует локальный адрес сетевого адаптера на основе ID локального интерфейса.
  - Хост выполняет DAD на локальном адресе. Если конфликта адресов нет, локальный адрес можно использовать.
  - Хост отправляет сообщение RS для обнаружения любого маршрутизатора IPv6 на канале. Адресом отправителя сообщения является локальный адрес хоста.
  - Маршрутизатор отвечает сообщением RA с префиксом IPv6. Маршрутизатор может быть сконфигурирован для отправки сообщения RA, даже если он не получает сообщение RS.
  - Хост получает префикс адреса IPv6 на основе сообщения RA, отправленного маршрутизатором, и генерирует одиночный IPv6-адрес с помощью префикса и локально созданного ID интерфейса.
  - Хост выполняет анализ DAD созданного IPv6-адреса. Если конфликт не обнаружен, адрес можно использовать.

Обзор механизма обнаружения маршрутизатора

- Обнаружение маршрутизатора является основой механизма автоматической конфигурации адресов IPv6 и реализуется с помощью двух типов пакетов:
  - Пакет Router Advertisement (RA): каждый маршрутизатор периодически посылает многоадресные сообщения RA с сетевыми префиксами и идентификаторами в сети, чтобы объявить о своем существовании хостам и устройствам 2 уровня. Поле ICMP Type в сообщении RA имеет значение 134.
  - Пакет Router Solicitation (RS): после подключения к сети хост сразу отправляет сообщение RS для получения сетевых префиксов. Устройства в сетевом отвечают сообщениями RA. . Поле ICMP Type в сообщении RS имеет значение 133.

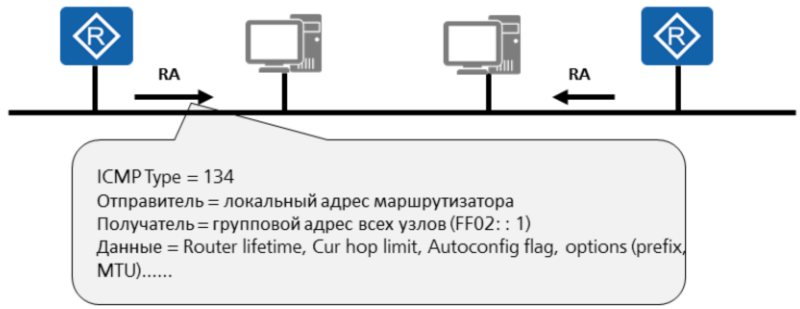
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Механизм обнаружения маршрутизаторов находит соседние устройства и узнает префиксы их адресов и параметры конфигурации для автоконфигурирования адресов.
- Как уже отмечалось выше, мы узнали, что адреса IPv6 можно получить с помощью автоконфигурации. То есть хосты получают сетевые префиксы через сообщения RA, отправляемые маршрутизаторами, генерируют ID интерфейсов и автоматически конфигурируют адреса IPv6.

Обнаружение маршрутизаторов: маршрутизатор периодически отправляет сообщения RA

- Маршрутизаторы на канале периодически отправляют сообщения RA.



- Хост, получающий сообщение RA, добавляется в список маршрутизаторов по умолчанию.
- Маршрутизатор, получающий сообщение RA, проверяет соответствие RA.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Как хост получает информацию, в том числе префикс сети? Существует два метода: хост может напрямую получать информацию в сообщении Router Advertisement (RA), полученном от маршрутизатора, или посылать сообщение Router Solicitation (RS) маршрутизатору и ждать, когда маршрутизатор ответит сообщением RA, из которого можно получить необходимую информацию.

Обнаружение маршрутизаторов: маршрутизатор отвечает сообщениями RA

- Когда хост отправляет сообщение RS при инициализации интерфейса, маршрутизатор отвечает сообщением RA.



Примечание: Сообщение RA может быть отправлено запрашивающему хосту в режиме одиночной передачи или многоадресной передачи всем узлам.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Процесс получения префикса и других параметров хостом

- При выполнении следующих условий префикс в сообщении RA может быть проигнорирован:
  - Поле **auto** в сообщении RA отображается как 0.
  - Префикс совпадает с префиксом существующего адреса (включая адрес link-local).
  - В сообщении RA значение поля **preferred lifetime** больше значения **valid lifetime**.
  - Сумма длины префикса и длины ID интерфейса не равна 128 бит.
- За исключением предыдущих условий, хост получает следующие временные параметры при получении префикса:
  - **preferred lifetime = срок действия нового соединения**
  - **valid lifetime = срок действия оригинального соединения**
- Хост периодически получает сообщения RA и обновляет свои временные параметры на основе полученных сообщений RA.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

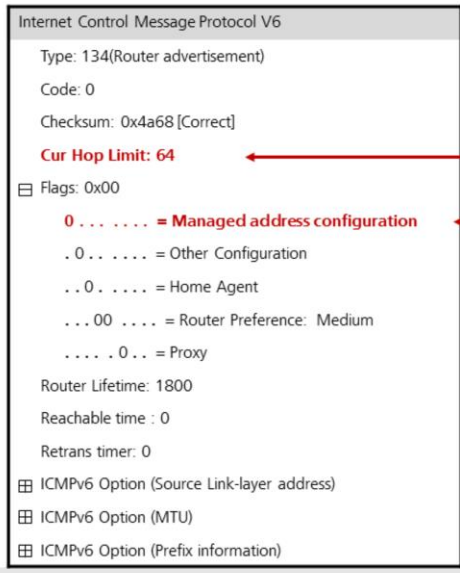
Параметры времени жизни

- Когда адрес находится в состоянии Deprecated, он не может инициировать соединение, но к нему можно подключаться. Этот дизайн используется для приложений верхнего уровня. Однако адрес становится недействительным после истечения времени жизни, и все соединения разрываются.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Поле Flags в сообщении RA ICMPv6 (1/2)



Это поле ограничивает количество узлов на хосте. После того, как ПК использует префикс, объявленный в сообщении RA для создания адреса IPv6, лимит узлов для пакетов IPv6, отправленных ПК, становится равен 64.

Значение бита M по умолчанию равно 0. При значении 0 хост, получающий сообщение RA, использует префикс IPv6, содержащийся в сообщении RA для автоконфигурации.

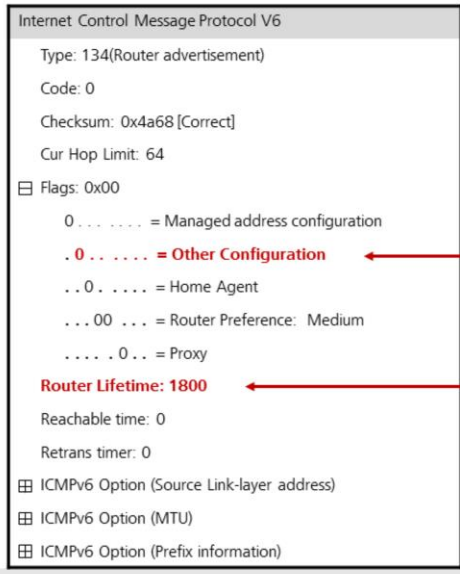
Выполните следующую команду, чтобы задать значение 1 в этом поле:

ipv6 nd autoconfig managed-address-flag

Если значение этого поля равно 1, то хост, получающий сообщение RA, использует функцию автоконфигурации, то есть для получения адреса IPv6 используется DHCPv6.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Поле Flags в сообщении RA ICMPv6 (2/2)



Значение по умолчанию поля Other Configuration равно 0, что указывает на то, что хост не должен использовать механизм автоконфигурации для настройки параметров помимо адреса IPv6.

Выполните следующую команду, чтобы установить значение 1 для этого поля:

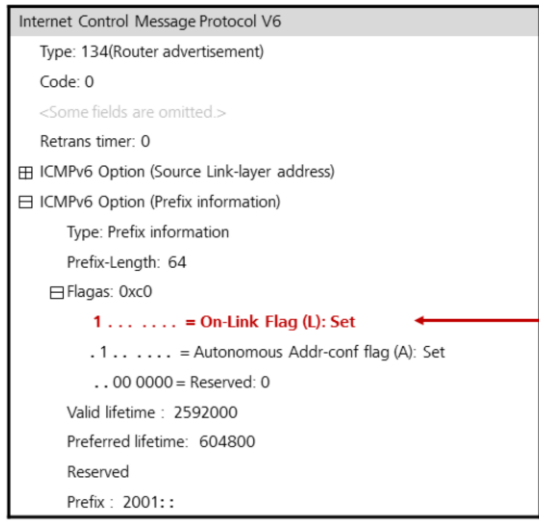
ipv6 nd autoconfig other-flag

Хост должен использовать DHCPv6 для настройки другой информации (кроме адреса IPv6), например DNS и доменного имени.

Единица измерения – секунды. Хост рассматривает это значение как срок жизни маршрутизатора по умолчанию. Если параметр Router Lifetime имеет значение 0, маршрутизатор будет исключен из списка шлюзов по умолчанию хоста.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Поле Flags префикса в сообщении RA ICMPv6 (1/2)

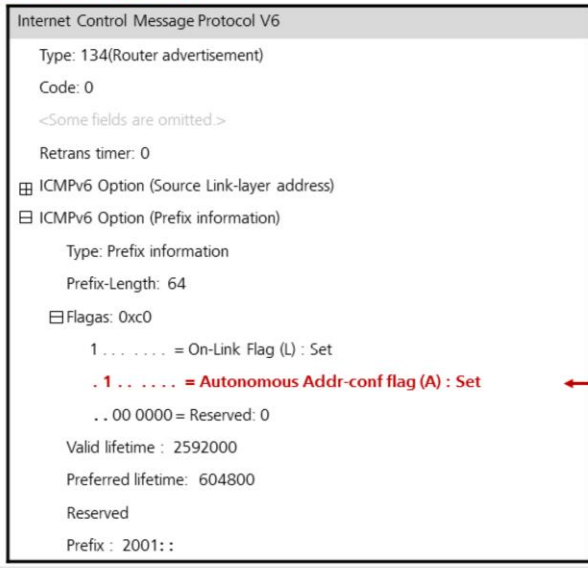


Значение по умолчанию бита L (RFC 2461) равно 1, что указывает на то, что префикс в сообщении RA назначается локальному каналу. Поэтому узлы, отправляющие данные на адреса, содержащие указанный префикс, рассматривают локальный канал как получателя.

Выполните следующую команду, чтобы установить значение 0 для этого параметра:
ipv6 nd ra prefix 2001: : 64 2592000 604800 off-link

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Поле Flags префикса в сообщении RA ICMPv6 (2/2)



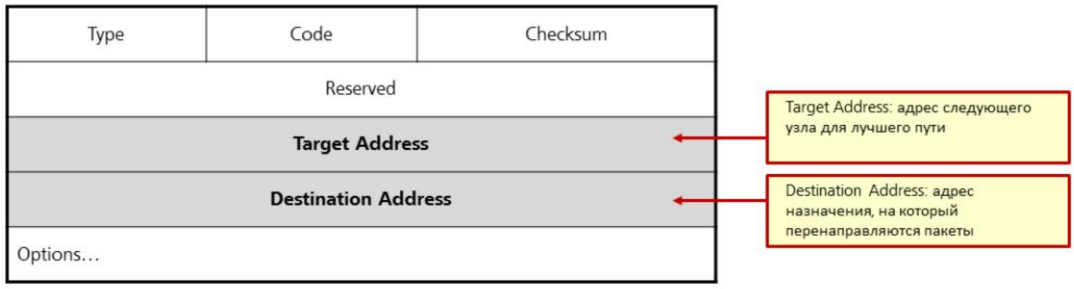
Значение по умолчанию бита A (RFC 2461) равно 1, что указывает на то, что хост на локальном канале может использовать этот префикс для автоконфигурации. Если значение равно 0, префикс не может быть использован для автоконфигурации.

Выполните следующую команду, чтобы установить значение 0 для этого бита:
ipv6 nd ra prefix 2001: : 64 2592000 604800 no-autoconfig

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Пакет перенаправления (Redirection)

- При наличии лучшего пути переадресации маршрутизатор-шлюз посылает сообщение Redirection для уведомления об этом хоста.
- Структура пакета Redirection следующая:

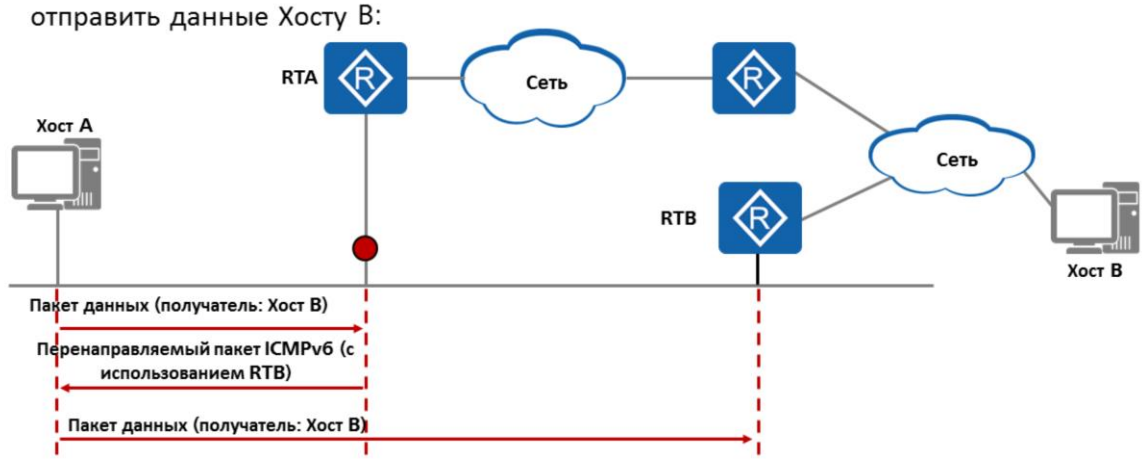


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- При наличии лучшего пути переадресации текущий маршрутизатор-шлюз отправляет сообщение Redirection, чтобы уведомить отправителя о том, что другой маршрутизатор-шлюз может отправлять пакеты.
  - В формате пакета значение поля Type равно 137 и значение поля Code равно 0.
  - Target Address указывает на оптимальный адрес следующего узла.
  - Destination Address – это адрес назначения пакета, который необходимо перенаправить.

Процесс перенаправления

- Маршрутизатором Хоста A по умолчанию является RTA. Когда Хосту A необходимо отправить данные Хосту B:



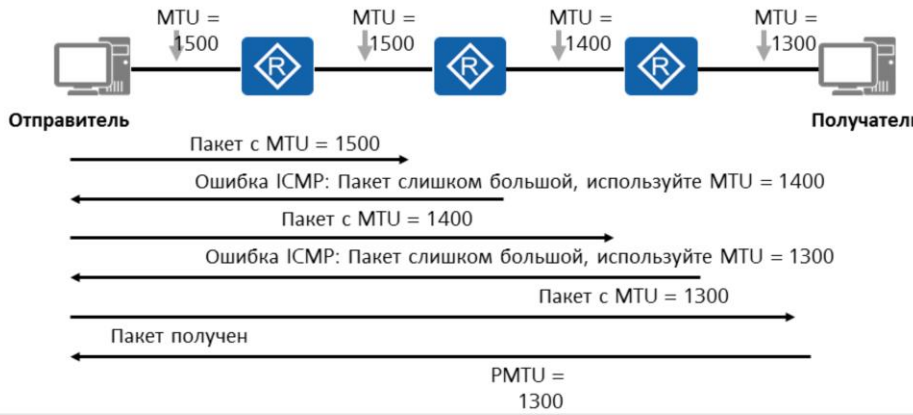
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Пример. Предположим, что Хост A хочет взаимодействовать с Хостом B, а маршрутизатором-шлюзом хоста A по умолчанию является RTA. Когда Хост A отправляет пакет Хосту B, пакет переадресуется RTA.
- RTA посылает сообщение Redirection с адресом назначения Хоста B Хосту A, чтобы уведомить Хост A о том, что RTB является лучшим следующим узлом.
- После получения сообщения Redirection Хост A добавляет маршрут хоста в таблицу маршрутизации по умолчанию. Пакеты, отправленные Хосту B, будут направлены непосредственно маршрутизатору RTB.
- Это простой процесс перенаправления. У вас может возникнуть вопрос: как RTA знает, что RTB является лучшим следующим узлом? Это связано с тем, что RTA обнаруживает, что пакеты поступают и выходят из одного интерфейса. То есть, пакеты, предназначенные для Хоста B, фактически переадресовываются маршрутизатору RTB после прохождения через маршрутизатор RTA. Таким образом, маршрутизатор RTA определяет, что прямой маршрут к RTB – это лучший путь.

Обнаружение PMTU (1/2)

- MTU пути (PMTU) является максимальная единица передачи данных (MTU) в пути.
- Протокол обнаружения PMTU определен в RFC 1981.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- После изучения переадресации пакетов IPv6 в предыдущих разделах мы знаем, что при переадресации не выполняется фрагментация и повторная сборка пакетов IPv6. Пакеты IPv6 фрагментируются только на исходном узле и собираются на узле назначения. Для обеспечения четкой передачи всех пакетов в пути, размер фрагментированных пакетов не может превышать минимальный MTU в пути, т.е. PMTU.
- В протоколе RFC1981 описывается механизм обнаружения PMTU, который реализуется посредством сообщений ICMPv6 Packet Too Big. Исходный узел сначала использует MTU своего исходящего интерфейса в качестве PMTU и посылает пробный пакет. Если на пути передачи существует меньшее PMTU, то транзитное устройство посылает исходному узлу сообщение Packet Too Big. Сообщение Packet Too Big содержит значение MTU исходящего интерфейса на транзитном устройстве. После получения этого сообщения, исходный узел изменяет значение PMTU на полученное значение MTU и отправляет пакеты на основе нового MTU. Этот процесс повторяется до тех пор, пока пакеты не будут доставлены до адреса назначения. Исходный узел получает PMTU адреса назначения.
- Например, пакеты передаются по четырем каналам со значениями MTU 1500, 1500, 1400 и 1300 байт. Перед отправкой пакета исходный узел фрагментирует пакет на основе PMTU 1500. Когда пакет отправляется на исходящий интерфейс с MTU 1400, устройство возвращает сообщение Packet Too Big с MTU 1400. Исходный узел затем фрагментирует пакет на основе MTU 1400 и снова посылает фрагментированный пакет. Процесс повторяется, когда пакет, основанный на MTU 1400, отправляется на исходящий интерфейс с MTU 1300, устройство возвращает другое сообщение

Packet Too Big с MTU 1300. Исходный узел получает сообщение и фрагментирует пакет на основе MTU 1300. Таким образом, исходный узел отправляет пакет на адрес назначения и выявляет PMTU пути передачи.

Обнаружение PMTU (2/2)

- Минимальный размер PMTU – 1280 байт (минимальный MTU, поддерживаемый канальным уровнем в IPv6, равен 1280 байт)
- Максимальный размер PMTU определяет канальный уровень. Например, туннель поддерживает MTU большого размера.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

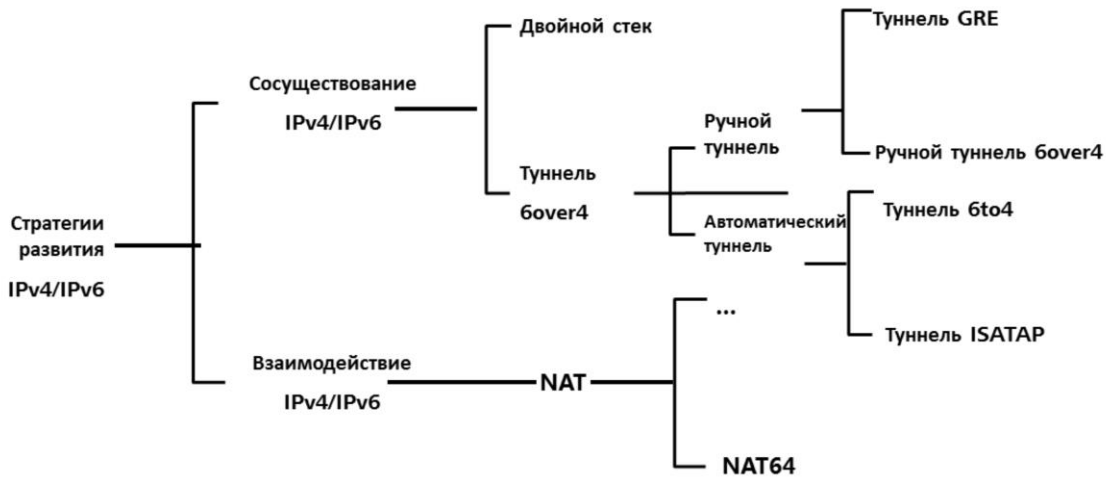
- Обратите внимание, что механизм обнаружения PMTU включается только в случае, если передаваемый пакет данных превышает минимальный размер PMTU. Если размер пакета меньше минимального PMTU, сообщение Packet Too Big не будет создано.
- Минимальный MTU, допустимый в IPv6, – 1280 байт. Поэтому PMTU не может быть меньше 1280 байт. Максимальный размер PMTU определяется канальным уровнем. Если канальный уровень представляет собой туннель, то значение PMTU может быть большим.

Содержание

1. История технологии IPv6
2. **Реализация протокола IPv6**
   - Форматы пакетов
   - Классификация адресов
   - Базовый протокол
   - **Технологии перехода**
3. Команды конфигурации IPv6
4. Советы по подготовке к экзаменам по протоколу IPv6

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Обзор технологий перехода на IPv6

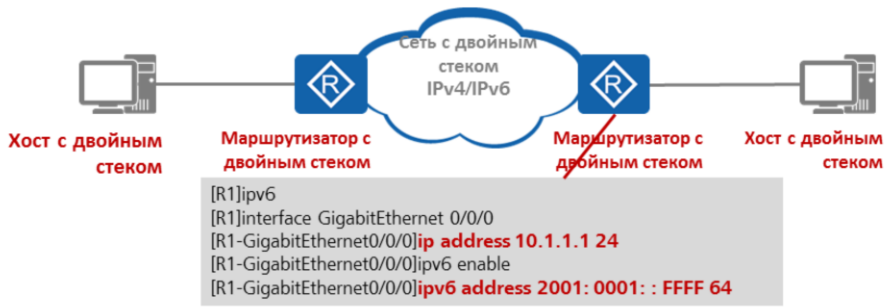


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Технологии, обеспечивающие сосуществование IPv4/IPv6:
  - Двойной стек протоколов IPv4/IPv6:
    - Узлы IPv6 поддерживают стеки протоколов IPv4 и IPv6.
  - Туннель:
    - Пакеты IPv6 выступают в качестве полезной нагрузки IPv4 для соединения нескольких островов IPv6 в интернет-сети IPv4.
- Технология взаимодействия IPv4/IPv6:
  - Предоставляет технологию взаимного доступа между IPv6 и IPv4.
  - Позволяет интернет-сетям на базе IPv6 и IPv4 сосуществовать и взаимодействовать друг с другом.

Двойной стек

- Двойной стек протоколов
  - Устройства должны поддерживать двойной стек IPv4/IPv6.
  - На интерфейсах, подключенных к сети с двойным стеком, должны быть сконфигурированы как с адреса IPv4, так и адреса IPv6.




```
[R1]ipv6
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]ip address 10.1.1.1 24
[R1-GigabitEthernet0/0/0]ipv6 enable
[R1-GigabitEthernet0/0/0]ipv6 address 2001: 0001: : FFFF 64
```

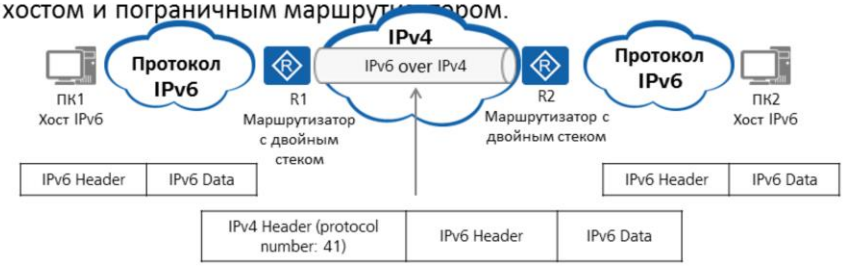
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Двойной стек – это технология, используемая для перехода от протокола IPv4 к протоколу IPv6. Узлы в сети с двойным стеком поддерживают стеки протоколов IPv4 и IPv6. Исходные узлы выбирают различные стеки протоколов в зависимости от узлов назначения. Сетевые устройства используют стеки протоколов для обработки и переадресации пакетов на основе типа протокола пакетов. Вы можете реализовать двойной стек на уникальном устройстве или магистральной сети с двойным стеком. В магистральной сети с двойным стеком все устройства должны поддерживать стеки протоколов IPv4 и IPv6. На интерфейсах, соединяющих сеть с двумя стеками, должны быть сконфигурированы адреса IPv4 и IPv6.
- В сети с двойным стеком IPv4/IPv6 хосты или сетевые устройства поддерживают стеки протоколов IPv4 и IPv6. Если узел поддерживает двойной стек, он может использовать стеки протоколов IPv4 и IPv6 и обрабатывать данные IPv4 и IPv6. На устройстве с двойным стеком приложения верхнего уровня предпочитают стек протоколов IPv6, а не IPv4. Например, приложение, поддерживающее двойной стек IPv4/IPv6, сначала отправляет запрос Authentication, Authorization, Audit, Account (AAAA) на DNS-сервер и отправляет запрос Authentication, Authorization, Audit или Account на DNS-сервер только в том случае, если не получает ответа на запрос AAAA. На основе технологии двойного стека сосуществуют протоколы IPv4 и IPv6, а также осуществляется переход от IPv4 к IPv6.
- Как показано на рисунке выше, маршрутизаторы являются устройствами с двойным стеком. По умолчанию маршрутизаторы поддерживают IPv4. На их интерфейсах сконфигурированы адреса IPv4. Поэтому эти маршрутизаторы могут передавать пакеты IPv4. Если активировать возможности переадресации данных IPv6

маршрутизаторов и присвоить их интерфейсам одиночные адреса IPv6, интерфейсы смогут передавать данные IPv6. В этом случае стеки протоколов IPv4 и IPv6 не будут мешать друг в другу и будут работать независимо.

Туннель 6over4, настроенный вручную

- Туннель 6over4, настроенный вручную
  - Тип туннеля 6over4, настроенного вручную
  - Адрес отправителя и адрес получателя должны задаваться вручную.
  - Туннель разворачивается между двумя пограничными маршрутизаторами или между хостом и пограничным маршрутизатором.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- При создании нескольких настроенных вручную туннелей IPv4 over IPv6 между одним пограничным устройством и несколькими устройствами, объем конфигураций, которые необходимо выполнить, огромен. Поэтому, как правило, такой туннель обычно создается между двумя пограничными маршрутизаторами для подключения сетей IPv6.
- Преимущества и недостатки настроенных вручную туннелей
  - Преимущества: туннель, сконфигурированный вручную, применим к любой среде, в которой IPv6 пересекает IPv4.
  - Недостатки: туннель необходимо сконфигурировать вручную.
- Механизм переадресации
  - Механизм переадресации туннеля IPv6 over IPv4, сконфигурированного вручную, выглядит следующим образом: после того, как пограничное устройство получает пакет из сети IPv6, оно ищет адрес назначения пакета IPv6 в таблице маршрутизации. Если пакет переадресуется из интерфейса виртуального туннеля, устройство инкапсулирует пакет на основе адресов источника и назначения IPv4, сконфигурированных на интерфейсе. Пакет IPv6 инкапсулируется как пакет IPv4 и обрабатывается стеком протоколов IPv4. Инкапсулированный пакет переадресуется через сеть IPv4 на удаленный конец туннеля. После того, как пограничный маршрутизатор на удаленном конце туннеля получает инкапсулированный пакет, он декапсулирует пакет и обрабатывает его с помощью стека протоколов IPv6.

Туннель GRE 6over4

- Туннель GRE 6over4
  - Тип туннеля 6over4, настроенного вручную
  - Адреса конечных точек туннеля 6over4 GRE задаются вручную.
  - GRE передает протокол IPv6.

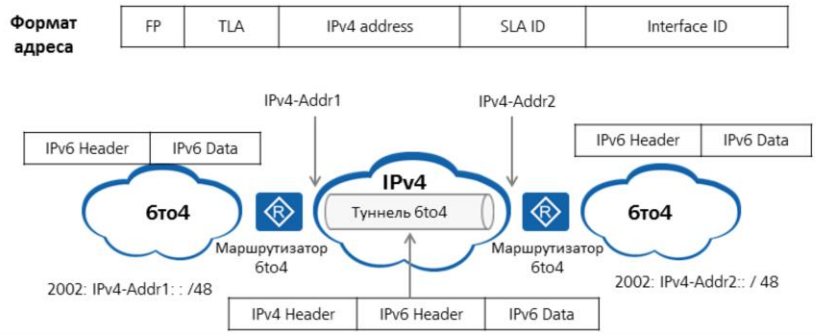


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Туннель GRE IPv6 over IPv4 использует стандартную технологию туннелирования GRE для обеспечения двухточечных соединений. Вам необходимо вручную указать адреса для обоих концов туннеля. Любые типы пакетов протоколов, поддерживаемых GRE, могут быть инкапсулированы и переданы через туннель GRE. Протоколы могут включать IPv4, IPv6, сетевую модель OSI и MPLS.
- Механизм переадресации туннеля GRE IPv6 over IPv4 аналогичен механизму переадресации туннеля IPv6 over IPv4, настроенного вручную.

Туннель 6to4 (1/3)

- Туннель 6to4
  - Тип автоматического туннеля 6over4
  - Туннель 6to4 может настраиваться между двумя маршрутизаторами, двумя хостами или хостом и маршрутизатором.
  - Используется специальный адрес 2002:IPv4::/48.



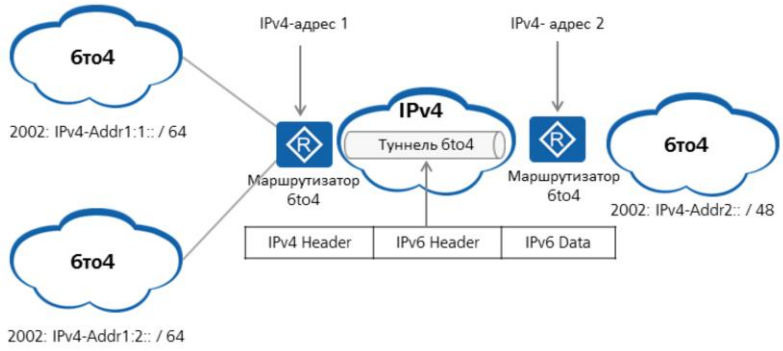
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Туннель IPv6-to-IPv4 (6to4) является автоматическим туннелем и использует адрес IPv4, встроенный в адрес IPv6. В отличие от IPv6-туннелей, совместимых с IPv4, туннели 6to4 можно создать между двумя маршрутизаторами, маршрутизатором и хостом и двумя хостами.
- Формат адреса:
  - FP: префикс формата глобального одиночного адреса. Значение 001.
  - TLA ID: идентификатор агрегации на верхнем уровне. Значение имеет 13 бит и преобразовано в 0 0000 0000 0010 в двоичном формате.
  - SLA ID: идентификатор агрегации на уровне объекта.
- Адрес 6to4 выражается в формате 2002::/16. Сеть 6to4 отображается как 2002: IPv4 address:: / 48. Адрес 6to4 имеет 64-битный префикс, состоящий из 48-битного адреса 2002: IPv4 и 16-битного SLA. Адрес 2002: IPv4 в формате 2002: a.b.c.d определяется адресом IPv4, назначенным маршрутизатору, и SLA определяется пользователем.

Туннель 6to4 (2/3)

- Туннель 6to4
  - Туннель 6to4 можно подключать к нескольким сетям 6to4.
  - Туннель 6to4 может быть идентифицирован по SLA ID.

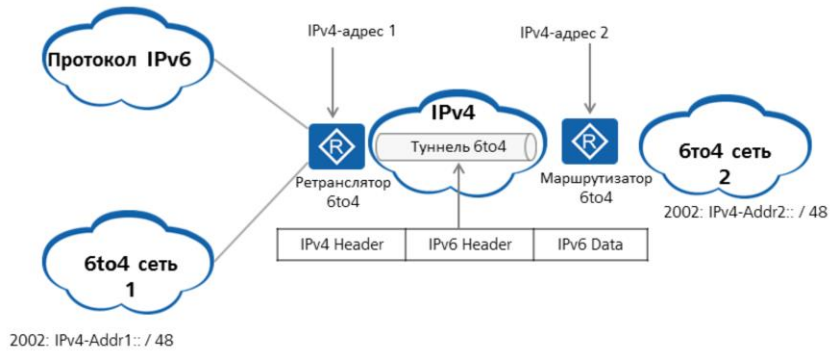


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Один адрес IPv4 может использоваться как исходный адрес только одного туннеля 6to4. Когда пограничный маршрутизатор подключается к нескольким сетям 6to4 с использованием адреса IPv4, который является исходным адресом туннеля, у сетей 6to4 будет один туннель и их можно определить по SLA ID в адресе 6to4.

Туннель 6to4 (3/3)

- Ретрансляция 6to4
  - Туннель 6to4 обеспечивает взаимодействие между сетью 6to4 и сетью IPv6.



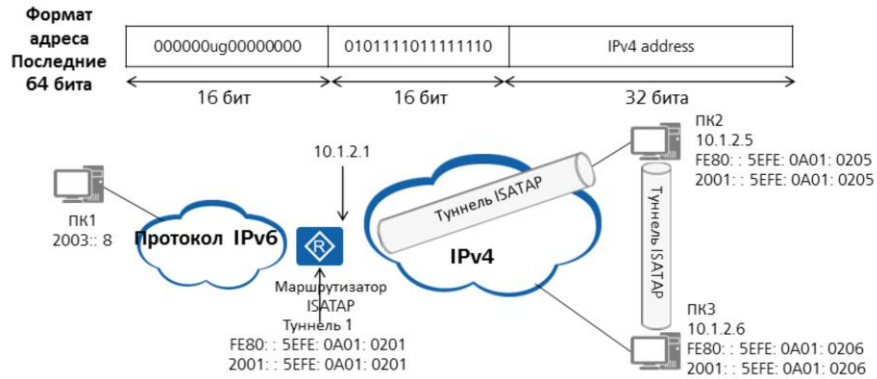
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Ретранслятор 6to4 используется, когда общая сеть IPv6 взаимодействует с сетью 6to4 через сеть IPv4. Ретранслятор 6to4 – это устройство следующего узла, которое передает пакеты IPv6, адресом назначения которых является не адрес 6to4, но адрес следующего узла является адресом 6to4. Адрес назначения IPv4 туннеля получен из адреса следующего узла 6to4.

- Если хосту в 6to4-сети 2 необходимо взаимодействовать с сетью IPv6, следующий узел маршрута должен быть сконфигурирован как адрес 6to4 ретранслятора на пограничном маршрутизаторе. Адрес ретранслятора соответствует исходному адресу туннеля 6to4 ретранслятора. Пакет, отправленный из сети 6to4-сети 2 в сеть IPv6, переадресуется на ретранслятор в соответствии с следующим узлом, указанным в таблице маршрутизации. Затем ретранслятор передает пакет в сеть IPv6. Когда пакет необходимо отправить из сети IPv6 в сеть 6to4, ретранслятор инкапсулирует пакет качестве пакета IPv4 в соответствии с адресом назначения (адресом 6to4) пакета, чтобы пакет можно было отправить в 6to4-сеть 2.

Туннель ISATAP

- Туннель ISATAP
  - Тип автоматического туннеля 6over4
  - Туннель 6to4 может быть развернут между хостами, от хоста к маршрутизатору или от маршрутизатора к хосту.
  - Используется специальный адрес туннеля ISATAP.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- ISATAP – это еще одна технология автоматического туннелирования. Туннель ISATAP использует адрес IPv6 специального формата со встроенным адресом IPv4. В отличие от адреса 6to4, который использует адрес IPv4 в качестве префикса сети, адрес ISATAP использует адрес IPv4 в качестве ID интерфейса.
- Описание адреса
- Бит "u" в адресе IPv4, который является глобально уникальным, имеет значение 1. В иных случаях бит "u" имеет значение 0. "G" -это индивидуальный/групповой бит IEEE. Адрес ISATAP содержит ID интерфейса и может быть глобальным одиночным адресом, локальным адресом (link-local), адресом ULA или групповым адресом. Устройство получает первые 64 бита адреса ISATAP, отправляя пакеты Request на маршрутизатор ISATAP. Устройства на обоих концах туннеля ISATAP запускают протокол обнаружения соседей (ND). Туннель ISATAP рассматривает сеть IPv4 как не широковещательную сеть с множественным доступом (NBMA).
- Описание процесса переадресации:
- ПК 2 и ПК 3 находятся в сети IPv4. Они поддерживают двойной стек протоколов и имеют частные IPv4 адреса. Для активации функции ISATAP на ПК 2 и ПК 3 выполните следующие действия:
  - Сконфигурируйте интерфейс туннеля ISATAP для создания ID интерфейса, основанного на адресе IPv4.
  - Генерируйте локальный (link-local) адрес IPv6 на основе ID интерфейса. Когда хост получает адрес локального адреса IPv6, он может получить доступ к сети IPv6 на локальном канале.
  - Хост автоматически получает глобальный одиночный адрес IPv6 и адрес ULA.
  - Хост получает адрес IPv4 от адреса следующего узла IPv6 в качестве адреса назначения и передает пакеты через интерфейс туннеля для связи с другим хостом IPv6. Если хост назначения расположен на том же сетевом узле, что и исходный хост, адрес следующего узла – это адрес

хоста назначения. Если хост назначения не расположен на локальном сетевом узле, адрес следующего узла – это адрес маршрутизатора ISATAP.

NAT64

- NAT64 – это технология преобразования сетевых адресов, которая может гибко преобразовывать пакеты IPv4 и IPv6.
- NAT64 сопоставляет поля в пакетах IPv6 с полями в пакетах IPv4, чтобы пакеты данных были преобразованы на границе между двумя типами сетей.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- По умолчанию узлы сети IPv4 не могут напрямую взаимодействовать с узлами сети IPv6, поскольку эти два стека протоколов несовместимы. Однако эту проблему можно решить, если на устройстве реализовано преобразование пакетов между протоколами IPv6 и IPv4.



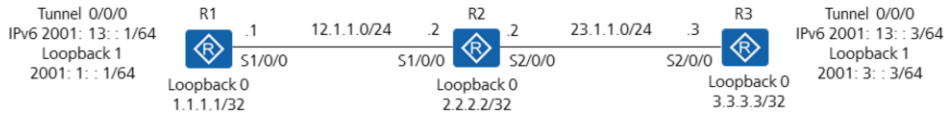
Содержание

1. История технологии IPv6
2. Реализация протокола IPv6
3. **Команды конфигурации IPv6**
4. Советы по подготовке к экзаменам по протоколу IPv6

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Конфигурирование туннеля GRE (1/2)

- На рисунке ниже показана топология сети компании A. Выполните следующие конфигурации:
  - Адреса IPv4 маршрутизаторов R1, R2 и R3 показаны на рисунке ниже. Три устройства развернуты в Зоне 0 OSPFv2. Конфигурации выполнены.
  - Требуемые адреса IPv6 отмечены.
  - Туннель GRE IPv6 over IPv4 развернут для реализации взаимодействия между интерфейсами loopback1 маршрутизаторов R1 и R3.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Описание примера:
- Заданы адреса IPv6 и IPv4.

Туннель GRE: основные команды конфигурации

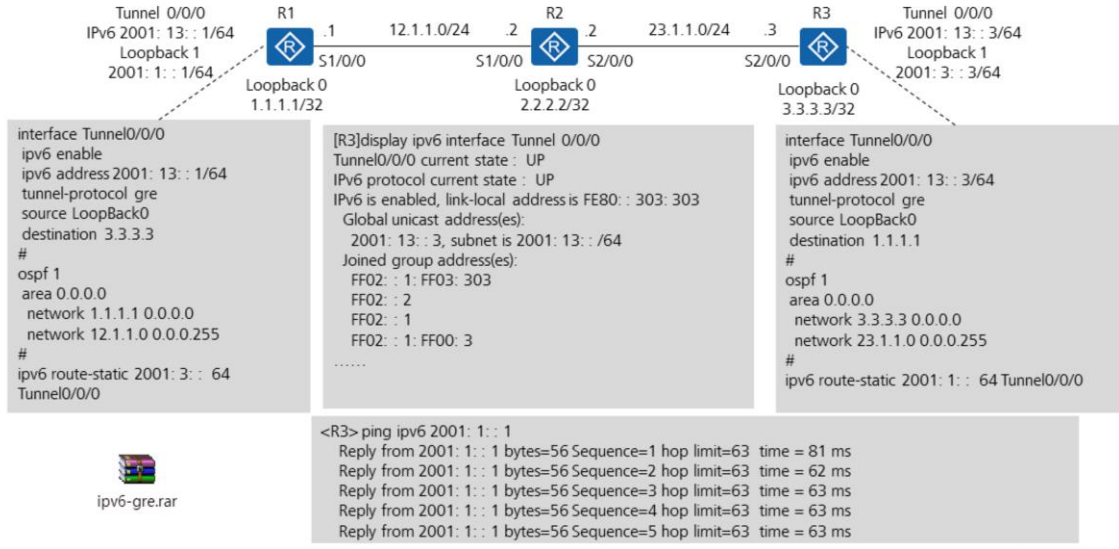
Этап	Действие	Команда
1	Перейдите в режим системы.	**system-view**
2	Создайте интерфейс туннеля.	**interface tunnel** *interface-number*
3	**Установите режим туннеля как GRE.**	**tunnel-protocol gre**
4	Укажите исходный интерфейс туннеля.	**source** { *ipv4-address* | *interface-type interface-number* }
5	Укажите интерфейс назначения туннеля.	**destination ipv4-address**
6	**Сконфигурируйте проверку заголовка пакета GRE.**	**gre checksum**
7	**Задайте ключевое слово заголовка пакета GRE.**	**gre key key-number**
8	Сконфигурируйте адрес IPv6 для интерфейса туннеля.	**ipv6 address** *ipv6-address prefix-length*

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Проверка заголовка пакета GRE является необязательной. Если она сконфигурирована, отправитель вычисляет контрольную сумму на основании информации в заголовке GRE и полезной нагрузки и отправляет пакет, содержащий контрольную сумму, получателю. Получатель вычисляет контрольную сумму на основе информации в полученном пакете и сравнивает расчетное значение с контрольной суммой в пакете. Если они одинаковы, получатель переадресует пакет. Если они отличаются, получатель отбрасывает пакет. Если функция контрольной суммы включена на локальной конечной точке и отключена на удаленной конечной точке, локальная точка не вычисляет контрольную сумму полученных пакетов.
- Установка ключевых слов для заголовка пакета GRE является необязательной. Если поле KEY в заголовке пакета GRE настроено, получатель проверяет ключевое слово заголовка принятого пакета GRE. Если оно соответствует ключевому слову, сконфигурированному локально, аутентификация выполнена успешно. В противном случае пакет отбрасывается.

Конфигурирование туннеля GRE (2/2)



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Значение команд:
  - Команда **interface tunnel** создает интерфейс туннеля и переключает на вид интерфейса туннеля.
  - Команда **tunnel-protocol gre** устанавливает режим туннеля на ручной.
  - Команда **source {ipv4-address | interface-type interface-number}** задает исходный интерфейс туннеля.
  - Команда **destination {ipv4-address}** задает интерфейс назначения туннеля.
  - Команда **ipv6 address {ipv6-address prefix-length}** задает адрес IPv6 интерфейса туннеля.



Содержание

1. История технологии IPv6
2. Реализация протокола IPv6
3. Команды конфигурации IPv6
4. **Советы по подготовке к экзаменам по протоколу IPv6**

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Советы по подготовке к экзамену по IPv6

Вам необходимо:

- Хорошо знать команды протокола IPv6.
- Знать процессы внедрения и применение IPv6.
- Знать, как использовать инструменты политики, как IPv6.
- Прочитать документы HedEx.
  - Включая применимые случаи.
- Знать примеры, разобранные в курсе.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Рекомендации

- Веб-сайт Huawei E-Learning:
  - http://support.huawei.com/learning/Index!toTrainIndex
- Библиотека примеров Huawei:
  - http://support.huawei.com/enterprise/servicecenter?lang=en

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Спасибо!

www.huawei.com

HCIE-R&S

— OSPF

www.huawei.com

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Введение

- OSPF (Open Shortest Path First) — это открытый протокол выбора первого кратчайшего пути, разработанный Инженерным советом Интернета (IETF). OSPF является протоколом внутреннего шлюза (IGP) и обеспечивает маршрутизацию по состоянию канала.
- Протокол OSPF обеспечивает быструю сходимость, маршрутизацию без петель и обладает отличной масштабируемостью, поэтому широко применяется в сетях.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Цели

- После завершения этого курса вы будете:
- Понимать принципы работы протокола OSPF.
- Повысите навыки устранения неполадок OSPF.
- Расширите возможности использования OSPF.
- Понимать основные принципы работы протокола OSPFv3.
- Понимать различия между OSPFv3 и OSPFv2.
- Понимать методов конфигурации OSPFv3 и основных команд.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Содержание

- **Принципы работы OSPFv2**
  - Основные понятия и особенности OSPFv2
  - Сравнение протоколов OSPF и IS-IS
- Диагностика ошибок в протоколе OSPFv2
- Общая информация о OSPFv3
- Различия между OSPFv3 и OSPFv2
- Методы конфигурации OSPFv3 и основные команды
- Рекомендации по подготовке к экзамену по протоколу OSPF

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Основные понятия OSPFv2: типы LSA-пакетов

Тип LSA	Функция
Router-LSA (тип 1)	Описывает состояние канала и стоимость устройства. Пакет Router-LSA генерируется каждым устройством и анонсируется в пределах зоны, к которой принадлежит устройство.
Network-LSA (тип 2)	Описывает состояние всех каналов в сегменте сети. Пакет Network-LSA генерируется выделенным маршрутизатором (DR) и анонсируется в пределах зоны, к которой принадлежит DR.
Network-summary-LSA (тип 3)	Описывает маршруты в сетевом сегменте. Пакет Network-summary-LSA генерируется пограничным маршрутизатором зоны (ABR) и анонсируется в не полностью тупиковых зонах (non-totally stub) или не совсем тупиковых зонах (NSSA).
ASBR-summary-LSA (тип 4)	Описывает маршрут к пограничному маршрутизатору автономной системы (ASBR). Пакет ASBR-summary-LSA генерируется ABR-маршрутизатором и анонсируется во все связанные зоны, за исключением зоны, к которой принадлежит ASBR-маршрутизатор.
AS-external-LSA (тип 5)	Описывает маршрут к точке назначения вне автономной системы (AS). Пакет AS-external-LSA генерируется ASBR-маршрутизатором и анонсируется во все связанные зоны, кроме тупиковых зон и зон NSSA.
NSSA LSA (тип 7)	Описывает маршрут к точке назначения вне AS. Пакет NSSA LSA генерируется ASBR-маршрутизатором и анонсируется только внутри зон NSSA.
Opaque LSA (типы 9, 10, 11)	Обеспечивает универсальный механизм для расширений OSPF: LSA типа 9, например, grace LSA, используемый при мягкой перезагрузке, анонсируется только в сегменте сети, в которой находится интерфейс, анонсирующий LSA-пакет. LSA типа 10, например LSA, используемый для поддержки TE, анонсируется в пределах зоны. LSA типа 11 анонсируется внутри AS. В настоящее время для LSA типа 11 нет областей применения.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Информация заголовка LSA-пакета (все пакеты OSPF, за исключением пакетов Hello, включают информацию LSA):
  - LS age: время в секундах после создания LSA.
  - Options: дополнительные возможности, поддерживаемые устройством.
  - LS type: формат и функция LSA. Чаще всего используется пять типов LSA.
  - Link State ID: значение этого поля изменяется в зависимости от LSA.
  - Advertising Router: идентификатор маршрутизатора, создающего LSA.
  - Sequence Number: обнаружение старых и дублирующих LSA. Порядковый номер LSA увеличивается каждый раз, когда маршрутизатор инициирует создание нового экземпляра LSA. Это обновление помогает другим маршрутизаторам определить последний экземпляр LSA.
  - Checksum: контрольная сумма полного содержимого LSA. В зависимости от поля age контрольная сумма пересчитывается каждый раз, когда увеличивается время старения.
  - Length: длина LSA с учетом длины заголовка LSA.
- Пакет router-LSA должен описывать состояния всех интерфейсов или каналов исходящего маршрутизатора LSA.
  - Link State ID: идентификатор исходящего маршрутизатора LSA.
  - Flag:
    - V: если установлено значение 1, то исходящий маршрутизатор LSA является конечной точкой одного или нескольких виртуальных каналов с полной смежностью.
    - E: установлено значение 1, если исходный маршрутизатор является ASBR-маршрутизатором.
    - B: установлено значение 1, если исходный маршрутизатор является ABR-маршрутизатором.
  - Number of links: количество каналов маршрутизаторов.
  - Link Type:
    - если установлено значение 1, то сеть является сетью «точка-точка». Для общих

каналов PPP необходимо использовать сети «точка-точка».

- если установлено значение 2, канал связан с транзитной сетью. Сегмент транзитной сети содержит широковещательные или сетевые сегменты NBMA по меньшей мере двух маршрутизаторов.

        - Если установлено значение 3, канал подключен к тупиковой сети. Как правило, у сети нет установленных отношений соседства, например, как у сети Ethernet, у которой есть только один исходящий интерфейс или только loopback-интерфейсы.
        - Если установлено значение 4, канал является виртуальным.
    - Link ID:
        - Если параметр Link Type равен 1, в этом поле указан ID соседнего маршрутизатора.
        - Если параметр Link Type равен 2, в этом поле указан IP-адрес интерфейса DR-маршрутизатора.
        - Если параметр Link Type равен 3, в этом поле указан адрес IP-сети или подсети.
        - Если параметр Link Type равен 4, в этом поле указан ID соседнего маршрутизатора.
    - Link Data:
        - Если параметр Link Type равен 1, в этом поле указан IP-адрес интерфейса подключенного исходящего маршрутизатора.
        - Если параметр Link Type равен 2, в этом поле указан IP-адрес интерфейса подключенного исходящего маршрутизатора.
        - Если параметр Link Type равен 3, в этом поле указана маска подсети сети.
        - Если параметр Link Type равен 4, в этом поле указан IP-адрес интерфейса виртуального канала на исходящем маршрутизаторе.
    - ToS: В настоящее время не поддерживается.
    - Metric: стоимость канала или интерфейса.
- Network-LSA
    - Link State ID: адрес интерфейса DR-маршрутизатора.
    - Network Mask: адрес или маска подсети, используемые в сети.
    - Attached router: перечень идентификаторов всех маршрутизаторов с полной смежностью с DR-маршрутизатором, включая идентификатор DR-маршрутизатора.
- Network-summary-LSA and ASBR-summary-LSA
    - Link State ID: в LSA 3 типа в этом поле указан IP-адрес анонсированной сети или подсети. В LSA 4 типа в этом поле указан ID анонсируемого ASBR-маршрутизатора.
    - Network Mask: в LSA 3 типа в этом поле указана маска подсети анонсируемой сети. В LSA 4 типа это поле не имеет смысла и, как правило, имеет значение 0.0.0.0.
    - Metric: стоимость маршрута от исходящего маршрутизатора до пункта назначения.
- AS-external-LSA
    - Link State ID: IP-адрес анонсируемой сети или подсети.
    - Network Mask: маска подсети анонсируемой сети.
    - E: тип внешней метрики, используемой маршрутом. Если бит E равен 1, то тип метрики – E2. Если бит E равен 0, тип метрики – E1.
    - Metric: стоимость маршрута. Значение определяется ASBR-маршрутизатором.
    - Forwarding Address: адрес, на который переадресуются пакеты данных. Если адрес переадресации равен 0.0.0.0, пакеты данных будут переадресованы на исходящий ASBR-маршрутизатор.
    - External Route Tag: внешний маршрут.
- NSSA LSA
    - Forwarding Address: если следующий узел импортированного внешнего маршрута находится в домене маршрутизации OSPF, в качестве адреса переадресации указывается следующий транзитный участок импортируемого внешнего маршрута. Если следующий узел импортированного внешнего маршрута находится вне домена маршрутизации OSPF, в качестве адреса переадресации указывается IP-адрес сегмента тупиковой сети (например, интерфейс loopback 0) в домене маршрутизации OSPF на ASBR-маршрутизаторе. При наличии нескольких сегментов тупиковой сети выбирается IP-адрес с самым большим значением.

Основные понятия OSPFv2: типы маршрутов

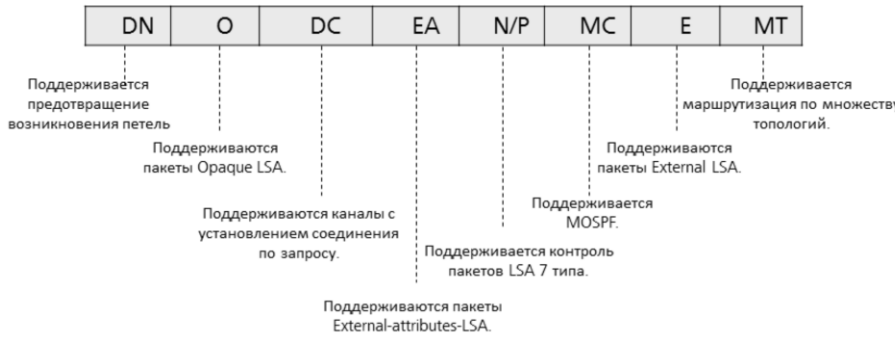
- Маршруты AS внутри зон (intra-area) и между зонами (inter-area) находятся в пределах AS. Внешние маршруты AS – это маршруты к точкам назначения за пределами AS.
- Протокол OSPF классифицирует импортированные внешние маршруты AS как внешние маршруты 1 и 2 типа.
- В следующей таблице описаны маршруты OSPF в порядке убывания приоритета.

Тип маршрута	Описание
Маршруты внутри зон	Маршруты в пределах зоны.
Маршруты между зонами	Маршруты между зонами.
Внешние маршруты 1 типа	Внешние маршруты 1 типа обладают высокой надежностью. Расчетная стоимость внешнего маршрута близка к стоимости маршрута в AS и сопоставима с стоимостью маршрута OSPF. Стоимость внешнего маршрута 1 типа = Стоимость маршрута от устройства до ASBR-маршрутизатора + Стоимость маршрута от ASBR-маршрутизатора до точки назначения
Внешние маршруты 2 типа	Внешние маршруты 2 типа обладают низкой надежностью. OSPF считает, что стоимость маршрута от ASBR-маршрутизатора к точке назначения за пределами AS намного превышает стоимость любого внутреннего маршрута к ASBR-маршрутизатору. Стоимость внешнего маршрута 2 типа = Стоимость маршрута от ASBR-маршрутизатора до точки назначения вне AS.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Основные понятия OSPFv2: поле Options

- Поле Options:
  - Поле Options передается во всех Hello-пакетах, DD-пакетах и LSA-пакетах.
  - В поле Options отображаются дополнительные возможности, поддерживаемые маршрутизатором.
- Поле Options содержит следующую информацию:

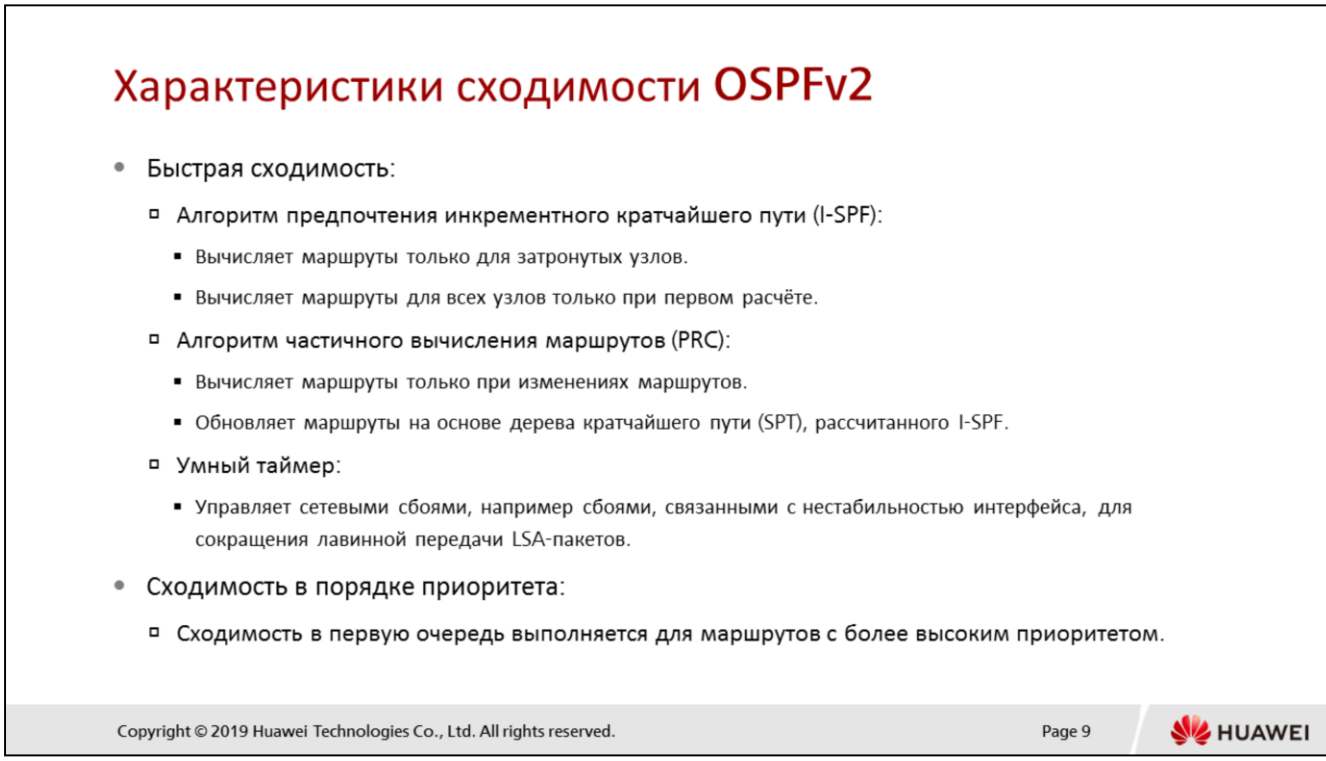


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Описание битов в поле Options:
  - DN: данный бит предотвращает петли в сетях MPLS VPN. В бите DN установлено значение 1, если PE посылает LSA-пакет 3, 5 или 7 типа в CE. LSA-пакет не участвует в вычислении маршрута OSPF на другом PE, который получает этот LSA-пакет от CE.
  - O: данный бит указывает на тип пакета Opaque LSA (тип 9, 10 или 11), который поддерживает исходящий маршрутизатор.
  - DC: данный бит имеет значение 1, если исходящий маршрутизатор поддерживает каналы с установлением соединения по запросу.
  - EA: данный бит имеет значение 1, если исходящий маршрутизатор может получать и пересылать пакеты типа external-attributes-LSA (LSA 8 типа).
  - N: данный бит передается только в пакетах Hello. Если бит имеет значение 1, маршрутизатор поддерживает пакеты LSA 7 типа. Если бит равен 0, маршрутизатор не может отправлять или принимать LSA NSSA.
  - P: данный бит передается только в пакетах LSA NSSA. Он используется, чтобы сообщать ABR-маршрутизаторам зоны NSSA о необходимости перевода пакетов LSA 7 типа в LSA 5 типа.
  - MC: данный бит имеет значение 1, если исходящий маршрутизатор может переадресовать многоадресные пакеты данных.
  - E: данный бит имеет значение 1, если исходящий маршрутизатор может получать пакеты AS-external-LSAs (LSA 5 типа). Данный бит имеет значение 1 во всех LSA 5 типа и LSA, которые создаются в магистральных или нетупиковых зонах. Бит имеет значение 0 в LSA из тупиковых зон. Если бит имеет значение 1 в пакете Hello, то интерфейс может отправлять и принимать LSA

5 типа.

- MT: данный бит указывает на то, что исходящий маршрутизатор поддерживает протокол OSPF multi-topology.



- Быстрая сходимость:
  - I-SPF вычисляет маршрут только для затронутых ошибкой узлов, кроме случаев, когда вычисление выполняется впервые. Генерируемое дерево кратчайшего пути (SPT) такое же, как и SPT, генерируемое при использовании другого обычного алгоритма. Поэтому, по сравнению с SPF, I-SPF потребляет меньше ресурсов ЦП и ускоряет сходимость сети.
  - Подобно I-SPF, алгоритм PRC вычисляет только маршруты, в которых произошли изменения. Однако PRC не вычисляет SPT. Вместо этого алгоритм использует SPT, рассчитанное I-SPF для обновления маршрутов. При вычислении маршрута лист является маршрутом, а узел – маршрутизатором. К изменению маршрута приводит изменение дерева SPT или листа (leaf). Изменение SPT не имеет отношения к изменению листа. Алгоритм PRC обрабатывает маршрутную информацию следующим образом:
    - Если дерево SPT изменилось, алгоритм PRC обрабатывает маршрутную информацию всех листьев на измененном узле.
    - Если дерево SPT не изменилось, алгоритм PRC не обрабатывает маршрутную информацию любого узла.
    - Если изменился лист, алгоритм PRC обрабатывает маршрутную информацию только на листе.
    - Если лист не изменился, PRC не обрабатывает его маршрутную информацию.
- Умный таймер. В протоколе OSPF используется умный таймер для контроля вычисления маршрутов, создания и приема LSA-пакетов. Это ускоряет сходимость маршрутов. Умный таймер OSPF работает следующим образом:
  - В сети, где маршруты вычисляются повторно, умный таймер OSPF динамически корректирует расчет маршрута на основе конфигурации пользователя и технологии экспоненциальной задержки для сокращения вычислений маршрутов и снижения потребления ресурсов ЦП. Маршруты рассчитываются после стабилизации топологии сети.
  - Если в нестабильной сети маршрутизатор генерирует или получает LSA-пакеты из-за частых изменений топологии, умный таймер OSPF может динамически настраивать интервал

вычисления маршрутов. В рамках этого интервала не будут генерироваться или обрабатываться LSA-пакеты, благодаря чему недействительные LSA-пакеты не будут генерироваться или анонсироваться по всей сети.

- Функции умного таймера для вычисления пути:
  - Согласно локальной базе данных LSDB OSPF-маршрутизатор использует алгоритм SPF для расчета дерева кратчайшего пути, выполняя роль корня, и определяет следующий узел к сети назначения в соответствии с деревом кратчайшего пути. Вы можете задать правильный интервал расчета SPF, чтобы предотвратить исчерпание полосы пропускания и ресурсов маршрутизатора из-за частых изменений в сети.
  - В сети, где время сходимости маршрутов должно быть короче, установите миллисекунду как единицу интервала, чтобы увеличить частоту вычисления маршрутов. Это увеличивает сходимость.
  - При изменении базы данных LSDB в OSPF необходимо пересчитывать кратчайшие пути. Если в сети часто происходят изменения и часто вычисляется кратчайший путь, будет использоваться большой объем системных ресурсов и эффективность маршрутизаторов будет снижена. Вы можете настроить умный таймер и установить нужный интервал вычисления SPF, чтобы предотвратить большой расход ресурсов полосы пропускания и маршрутизатора.
  - Ниже приводится подробная информация о интервале расчета SPF:

Первый интервал расчета SPF определяется параметром *start-interval*.

Последующие интервалы расчета SPF определяются параметром *hold-interval* x 2 x (n-1).

Когда интервал, указанный в параметре *hold-interval* x 2 x (n-1), достигает максимального интервала *max-interval*, OSPF выполняет вычисление SPF при максимальном интервале три раза подряд, и затем возвращается к первому этапу. То есть, OSPF выполняет расчет SPF согласно первому

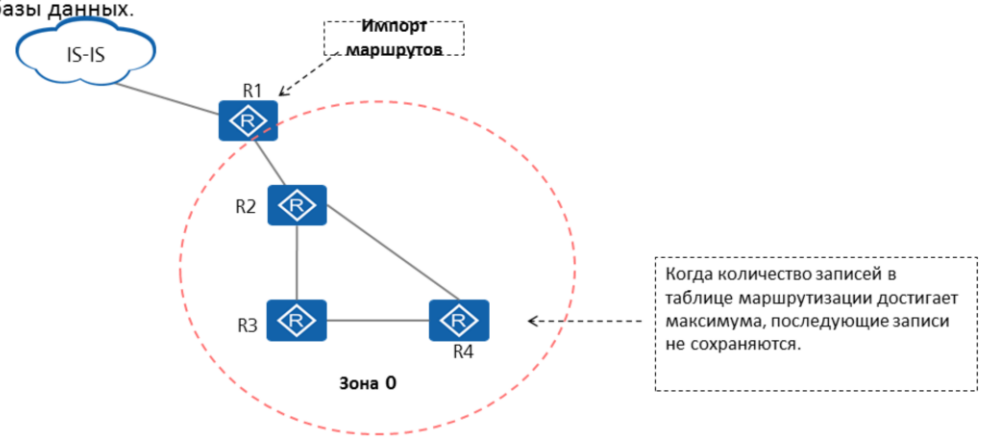
интервалу, указанному в параметре *start-interval.*

- Сходимость в порядке приоритета:

Вы можете настроить на устройстве фильтрацию определенных маршрутов на основе списка IP-префиксов. Вы можете настроить приоритет сходимости для маршрутов, чтобы сходимость сначала выполнялась для важных маршрутов, за счет чего будет повышена надежность сети.

Переполнение базы данных в OSPFv2

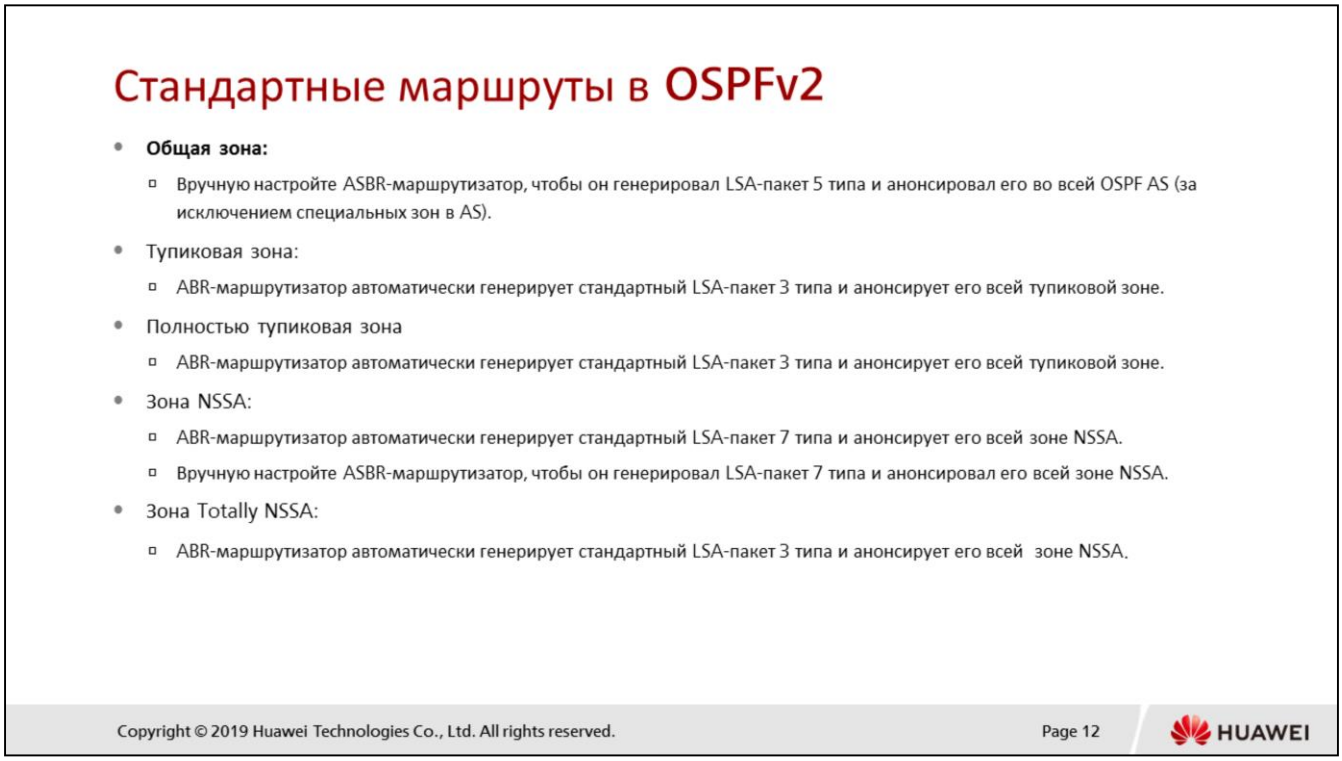
- Переполнение базы данных:
  - Ограничьте количество нестандартных внешних маршрутов, чтобы предотвратить переполнение базы данных.



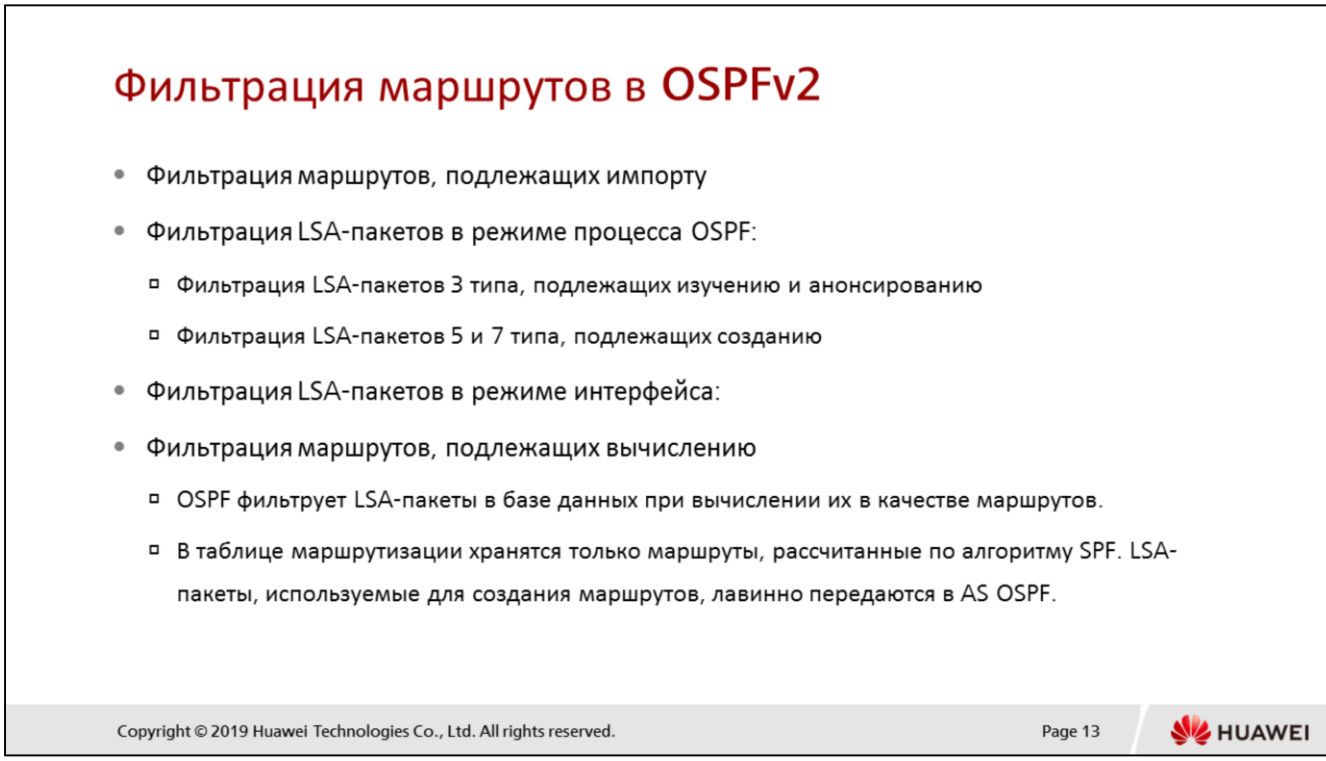
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Ограничение максимального количества нестандартных внешних маршрутов на маршрутизаторе может предотвратить переполнение базы данных. Все маршрутизаторы в сети OSPF должны иметь одинаковое максимальное значение. Если количество внешних маршрутов на маршрутизаторе достигнет максимального значения, маршрутизатор войдет в состояние переполнения и запустит таймер переполнения. Маршрутизатор автоматически выйдет из состояния переполнения после истечения времени таймера (5 секунд по умолчанию).
- Процесс переполнения базы данных OSPF:
  - Когда маршрутизатор входит в состояние переполнения, он удаляет все нестандартные внешние маршруты, созданные локально.
  - В состоянии переполнения маршрутизатор не генерирует нестандартные внешние маршруты и не отвечает пакетами подтверждения при получении таких маршрутов. Вместо этого он отбрасывает недавно полученные нестандартные внешние маршруты. После истечения времени таймера переполнения маршрутизатор проверяет, превышает ли количество внешних маршрутов максимальное значение. Если да, маршрутизатор перезапускает таймер. В противном случае маршрутизатор выйдет из состояния переполнения.
  - Когда маршрутизатор выходит из состояния переполнения, он удаляет таймер переполнения и может генерировать нестандартные внешние маршруты, принимать новые нестандартные внешние маршруты, отвечать пакетами подтверждения на полученные нестандартные внешние маршруты и подготовиться к переходу в состояние переполнения в следующий раз.



- Стандартные маршруты OSPF используются, когда:
  - ABR-маршрутизатор анонсирует стандартные пакеты summary LSA (тип 3), чтобы направлять переадресацию пакетов между областями.
  - ASBR-маршрутизатор анонсирует стандартные пакеты external ASE LSA (тип 5) или стандартные пакеты external LSA NSSA (тип 7)), чтобы направлять переадресацию пакетов во внешние AS.
- Принципы анонсирования стандартных маршрутов OSPF:
  - Маршрутизатор OSPF может анонсировать LSA-пакеты стандартных маршрутов только при подключении маршрутизатора к внешней AS.
  - Если маршрутизатор OSPF анонсировал LSA-пакет стандартного маршрута, он больше не узнает такой же тип стандартного маршрута, анонсированный другими маршрутизаторами. То есть маршрутизатор использует только LSA-пакеты, анонсированные им самим, для расчета маршрутов. LSA-пакеты, анонсированные другими маршрутизаторами, будут по-прежнему храниться в базе данных LSDB.
  - Если маршрутизатор должен использовать маршрут для анонсирования LSA-пакета, несущего стандартный внешний маршрут, это маршрут не должен быть полученным локальным процессом OSPF. Маршрутизатор в зоне использует стандартный внешний маршрут для переадресации пакетов за пределы зоны. Если следующими узлами маршрутов в зоне являются маршрутизаторы внутри зоны, пакеты невозможно переадресовать за ее пределы.



- OSPF поддерживает фильтрацию маршрутов с помощью политик маршрутизации. В протоколе OSPF не настроена фильтрация маршрутов по умолчанию.
- Такие политики включают: route-policy, filter, filter-policy, filter-LSA-out, access-list и prefix-list.
- Фильтрация маршрутов OSPF может использоваться для:
  - Фильтрации маршрутов, подлежащих импорту.
    - OSPF может импортировать маршруты, узнанные другими протоколами маршрутизации. Вы можете настроить политики маршрутизации для фильтрации маршрутов, подлежащих импорту, чтобы OSPF импортировал только маршруты, соответствующие определенным условиям.
    - Импортированные маршруты в таблице маршрутизации можно анонсировать.
  - Фильтрации LSA-пакетов 3 типа, подлежащие изучению и анонсированию.
    - Вы можете запустить команды **filter import** и **filter export** на ABR-маршрутизаторе, чтобы фильтровать входящие и исходящие LSA-пакеты 3 типа. Эти команды можно выполнять только на ABR-маршрутизаторе (только ABR-маршрутизаторы могут анонсировать LSA-пакеты 3 типа).
  - Фильтрации LSA-пакетов 5 и 7 типа.
    - После импорта внешних маршрутов OSPF он генерирует LSA-пакеты 5 и 7 типа. Команду **filter-policy export** можно запустить для фильтрации LSA-пакетов 5 и 7 типа. Эту команду можно выполнять только на ASBR-маршрутизаторах.
  - Фильтрации LSA-пакетов на определенных интерфейсах. Команду **ospf filter-lsa-out** можно запустить для фильтрации всех LSA-пакетов 3, 5 и 7 типа, за исключением пакетов grace LSA, созданных на основе префиксов маршрутов, указанных в таблице ACL, чтобы фильтровать LSA, подлежащие анонсированию.
  - Фильтрации LSA-пакетов для вычисления маршрутов.
    - Вы можете запустить команду **filter-policy import**, чтобы фильтровать внутризоновые, межзоновые и внешние LSA-пакеты в базе данных, которые можно использовать при

вычислении маршрута. Функция фильтрации определяет, можно ли добавить маршрут в локальную таблицу маршрутизации. Маршрут будет добавлен в локальную таблицу маршрутизации только в том случае, если он соответствует правилу фильтрации. LSA-пакет, генерирующий маршрут, анонсируется в AS OSPF.

Содержание

- **Принципы работы OSPFv2**
  - Основные понятия и особенности OSPFv2
  - Сравнение протоколов OSPF и IS-IS
- Диагностика ошибок в протоколе OSPFv2
- Общая информация о OSPFv3
- Различия между OSPFv3 и OSPFv2
- Методы конфигурации OSPFv3 и основные команды
- Рекомендации по подготовке к экзамену по протоколу OSPF

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

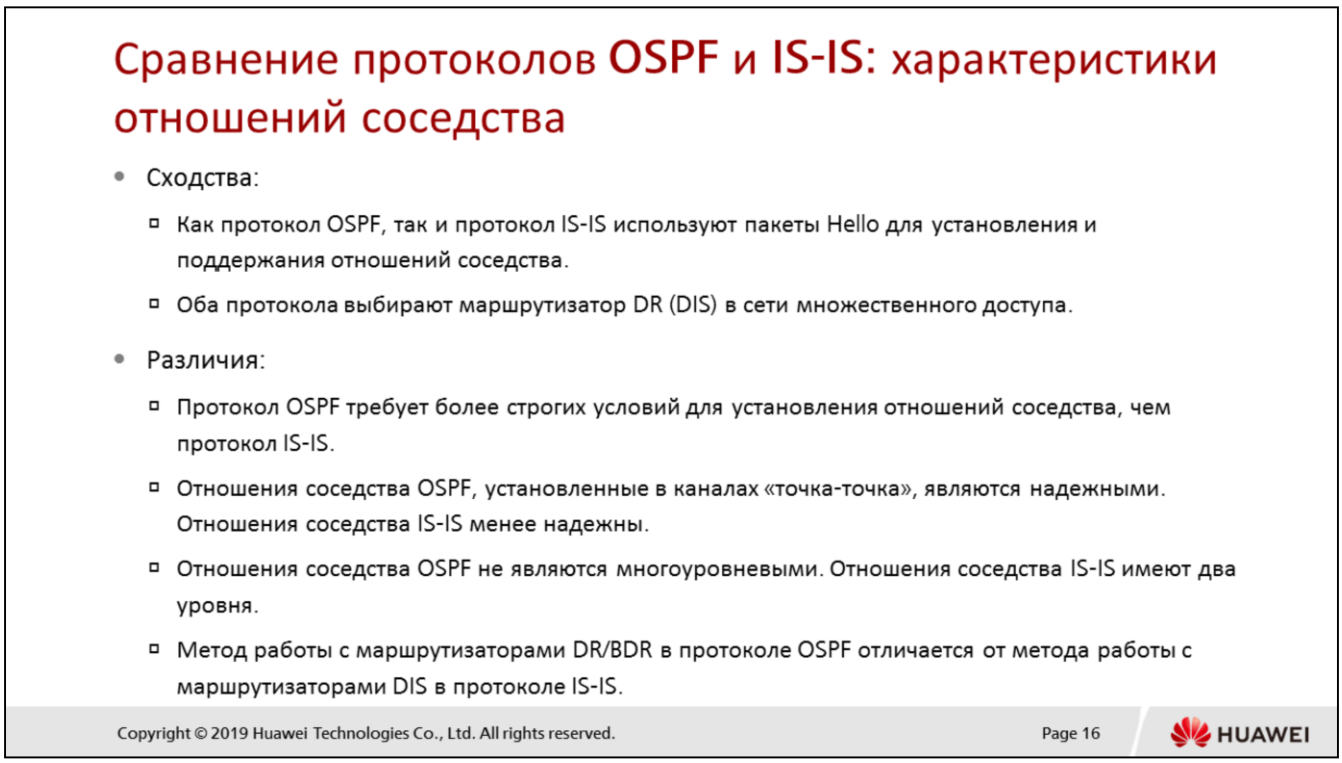
Сравнение протоколов OSPF и IS-IS: основные характеристики

- Сходства:
  - Как OSPF, так и IS-IS являются протоколами внутреннего шлюза (IGP) и широко применяются в сетях.
  - Оба протокола применяются в IP-сетях.
  - Оба протокола применяются в сетях с иерархической и многозональной структурой.
- Различия:
  - Протокол OSPF применяется только в IP-сетях. Протокол IS-IS применяется как в IP-сетях, так и в CLNP-сетях.
  - Протокол OSPF поддерживает различные типы сетей. Протокол IS-IS поддерживает только два типа сетей.
  - Протокол OSPF поддерживает виртуальные каналы. Протокол IS-IS обладает аналогичными функциями, но продукты большинства поставщиков IS-IS не поддерживают виртуальные каналы.
  - Протокол OSPF работает на IP-уровне. Протокол IS-IS работает на уровне канала передачи данных.
  - Протокол OSPF делит сеть на зоны на основании интерфейсов. Протокол IS-IS делит сеть на зоны на основании устройств.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Дополнительная информация:
  - Протокол OSPF поддерживает сети P2P, P2MP, NBMA и широковещательные сети. Протокол IS-IS поддерживает только P2P-сети и широковещательные сети.
  - Протокол OSPF работает в IP-сети и использует протокол 89.



- Дополнительная информация:
  - При установлении отношений соседства протокол OSPF проверяет в пакете Hello такую информацию, как маска, параметр аутентификации, интервал Hello/dead и зона. Условия установлении отношений соседства в протоколе IS-IS относительно свободные.
  - Протокол OSPF требует трехстороннего квитирования при установлении отношений соседства на канале P2P. IS-IS не требует квитирования. Тем не менее, устройства Huawei требуют выполнять трехстороннее квитирование в сети IS-IS P2P по умолчанию, благодаря чему повышается надежность при установлении отношений соседства.
  - Отношения соседства IS-IS классифицируются как отношения 1 и 2 уровня.
  - Протокол OSPF выбирает маршрутизатор DR/BDR на основании приоритетов и идентификаторов маршрутизаторов. После выбора DR/BDR данные роли не могут быть унаследованы другими маршрутизаторами. В OSPF все устройства DRother формируют двусторонние отношения соседства с маршрутизатором DR/BDR; все устройства DRother формируют двусторонние отношения соседства, которые являются неполноценными отношениями. Если в протоколе OSPF приоритет выбора маршрутизатора равен 0, маршрутизатор включен в процесс выбора маршрутизатора DR/BDR.
  - Протокол IS-IS выбирает DIS-маршрутизатор на основе приоритета выбора и MAC-адресов маршрутизаторов. После выбора DIS-маршрутизатор нельзя принудительно отключить. В протоколе IS-IS все маршрутизаторы образуют смежности. Если приоритет выбора маршрутизатора равен 0, то маршрутизатор включен в процесс выбора DIS-маршрутизатора с низким приоритетом.

Сравнение протоколов OSPF и IS-IS: характеристики синхронизации базы данных

- Сходства:
  - Как протокол OSPF, так и протокол IS-IS создают единую базу данных состояния каналов (LSDB).
- Различия:
  - В протоколе OSPF существуют различные типы LSA-пакетов, в протоколе IS-IS – всего несколько типов LSP-пакетов.
  - Процессы синхронизации баз данных OSPF и IS-IS отличаются.
  - В протоколе OSPF время существования LSA-пакета увеличивается во время передачи. Срок службы LSP-пакетов в протоколе IS-IS уменьшается во время передачи.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Дополнительная информация:
  - В протоколе IS-IS есть всего несколько типов LSP-пакетов, но существует возможность расширения функций с использованием полей TLV в LSP-пакетах.

Сравнение протоколов OSPF и IS-IS: прочие характеристики

- Сходства:
  - Как в протоколе OSPF, так и в протоколе IS-IS используется алгоритм первого кратчайшего пути (SPF) для расчета маршрутов.
  - В обоих протоколах существует возможность предотвращения петель, поддержка быстрой сходимости и крупномасштабных сетей.
- Различия:
  - Тип стоимости в протоколе OSPF простой, а в протоколе IS-IS – сложный.
  - Протокол OSPF поддерживает коммутируемые сети с соединением по требованию, протокол IS-IS не поддерживает сети такого типа.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Дополнительная информация:
  - Стоимость маршрутов OSPF рассчитывается исходя из полосы пропускания. В протоколе IS-IS существует четыре типа стоимости: narrow, narrow-compatible, wide и wide-compatible. Однако используется только тип стоимости wide.



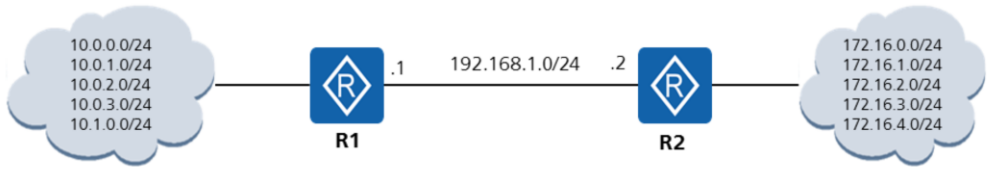
Содержание

- Принципы работы OSPFv2
- **Диагностика ошибок в протоколе OSPFv2**
- Общая информация о OSPFv3
- Различия между OSPFv3 и OSPFv2
- Методы конфигурации OSPFv3 и основные команды
- Рекомендации по подготовке к экзамену по протоколу OSPF

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Диагностика ошибок в протоколе OSPF

- После включения протокола OSPF в сети маршрутизаторы R1 и R2 не могут выполнить эхо-запросы друг другу.
- Как проанализировать и устранить ошибку?



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Процедура поиска и устранения ошибок

- Плоскость управления:
  - Если отношения соседства находятся в состоянии Down (отказ):
    - Проверьте, нормально ли работают физические интерфейсы.
    - Проверьте корректность конфигураций маски, аутентификации и идентификатора зоны.
    - Проверьте, анонсирует ли протокол OSPF информацию об интерфейсе.
  - Если отношения соседства находятся в состоянии Init:
    - Проверьте, исправен ли локальный интерфейс и соседнее устройство.
  - Если отношения соседства находятся в состоянии 2-way:
    - Проверьте, имеет ли приоритет интерфейса значение 0.
  - Если отношения соседства находятся в состоянии Exstart:
    - Проверьте, работает ли команда **ospf mtu-enable** на интерфейсах. Если да, проверьте корректность максимальных единиц передачи данных (MTU).
  - Если отношения соседства находятся в состоянии Exchange/Loading:
    - Проверьте, исправны ли локальные и соседние устройства и интерфейсы.

- Плоскость передачи данных:
  - Проверьте, настроена ли фильтрация трафика на взаимосвязанных интерфейсах.
  - Проверьте, настроена ли маршрутизация на основе политик на взаимосвязанных интерфейсах.
  - Проверьте, отбрасываются ли пакеты эхо-запросов промежуточным брандмауэром.
  - Если отношения соседства находятся в состоянии full:
    - Проверьте, соответствуют ли друг другу типы сетей интерфейсов.
    - Проверьте корректность настроек параметров команды **network**.
    - Убедитесь, что внешние маршруты, подлежащие импорту, отфильтрованы на основе сконфигурированной политики маршрутизации.
    - Проверьте, фильтруются ли LSA-пакеты 5 и 7 типа на основе конфигурации **filter-policy export**.
    - Проверьте, фильтруются ли локальные маршруты, используемые при расчете маршрута, на основе конфигурации **filter-policy import**.
    - Проверьте, настроена ли фильтрация LSA-пакетов между зонами в режиме процессов OSPF.
    - Проверьте, отключена ли на устройствах возможность совместного анонсирования LSA-пакетов 3, 5 и 7 типа в режиме процессов OSPF.
    - Проверьте, настроена ли интерфейсах фильтрация анонсируемых LSA-пакетов.
    - Проверьте, генерируется ли другим протоколом маршрут с более длинным битом маски или более высоким приоритетом в протоколе и исходящим интерфейсом, отличным от исходящего интерфейса маршрута OSPF.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- По умолчанию протокол OSPF не проверяет MTU DD-пакетов.



Содержание

- Принципы работы OSPFv2
- Диагностика ошибок в протоколе OSPFv2
- **Общая информация о OSPFv3**
- Различия между OSPFv3 и OSPFv2
- Методы конфигурации OSPFv3 и основные команды
- Рекомендации по подготовке к экзамену по протоколу OSPF

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Общая информация о версии протокола OSPFv3

- Механизмы версий протокола OSPFv3 и OSPFv2 схожи. Для поддержки формата адреса IPv6 в протоколе OSPFv3 были внесены некоторые изменения по сравнению с OSPFv2.
- OSPFv3 – это усовершенствованная версия протокола OSPFv2, независимая от него.
- В версии OSPFv3 также используется значение 89 в качестве номера протокола и 32-битное неподписанное целое число в качестве идентификатора маршрутизатора.

OSPFv2	OSPFv3
IPv4	IPv6
Data link layer	

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Влияние IPv6 на версию OSPFv3

Изменения в адресах IPv6	Протокол OSPFv3
Адрес IPv6 имеет 128 бит.	Длина LSA-пакетов увеличена.
Добавлены адреса link-local. Адреса link-local используются для отправки пакетов по каналом, за исключением виртуальных каналов.	
На интерфейсе можно настроить несколько глобальных одиночных IPv6-адресов.	Связь осуществляется через каналы, а не подсети.
Заголовок расширения для аутентификации IPv6	Заголовки расширения используются для аутентификации и шифрования пакетов.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Сходства между версиями OSPFv3 и OSPFv2

- Типы сетей и интерфейсов
- Машины состояний интерфейсов и соседства
- База данных состояния канала (LSDB)
- Лавинная передача
- Пять типов пакетов протокола OSPF: Hello, DD, LSR, LSU и LSAck
- Расчет маршрута

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.



Содержание

- Принципы работы OSPFv2
- Диагностика ошибок в протоколе OSPFv2
- Общая информация о OSPFv3
- **Различия между OSPFv3 и OSPFv2**
- Методы конфигурации OSPFv3 и основные команды
- Рекомендации по подготовке к экзамену по протоколу OSPF

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

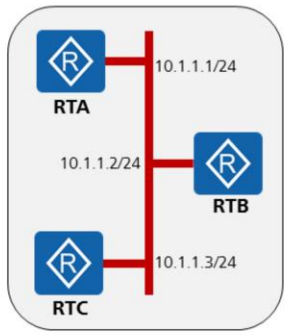
Различия между OSPFv3 и OSPFv2

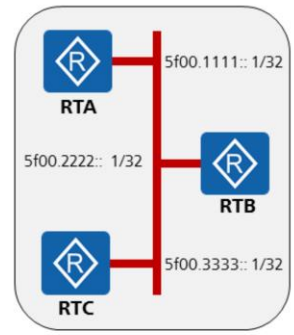
- Работа на основе каналов
- Адреса link-local
- Мультиплексирование с множеством экземпляров
- Аутентификация
- Тупиковая зона
- Пакет
- Содержимое в поле Options
- Тип и содержимое LSA-пакетов

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Работа на основе каналов

- OSPFv2 работает на основе сетей. Два маршрутизатора должны находиться в одном сегменте сети, чтобы установить отношения соседства.
- OSPFv3 реализуется на основе каналов. Канал может быть разделен на несколько подсетей. Два узла могут взаимодействовать друг с другом, если они находятся в одном канале, независимо от того, находятся ли они в одной подсети.





Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- В IPv6 используется концепция каналов. В одном канале может размещаться несколько IP-подсетей, т.е. префиксов IPv6. В отличие от IPv4, IPv6 позволяет двум узлам в одном канале взаимодействовать друг с другом, даже если они не имеют одинакового префикса IPv6. Это значительно меняет работу протокола OSPF.
- OSPFv3 работает на основе каналов, а не IP-подсетей. В OSPFv3 часто используются понятия «канал» и «префикс». Однако эти понятия отличаются. Два узла в одном канале могут иметь разные префиксы. Поэтому понятия «сеть» и «подсеть» необходимо заменить на «канал» при использовании версии протокола OSPFv3. Кроме того, интерфейс OSPFv3 подключается к каналу вместо IP-подсети. В протоколе OSPFv3 были внесены изменения в процесс получения пакетов OSPF и форматы пакетов Hello и LSA-пакетов.

Адрес link-local

- Маршрутизатор OSPFv3 использует адрес link-local в качестве исходного адреса для отправки пакетов.
- В виртуальном канале сетевой адрес или локальный адрес объекта должен использоваться в качестве исходного адреса пакета OSPFv3.
- Адрес link-local действителен только в локальном канале, и он распространяется только в локальном канале. Таким образом, адрес link-local может быть передаваться только внутри LSA-пакета канала.

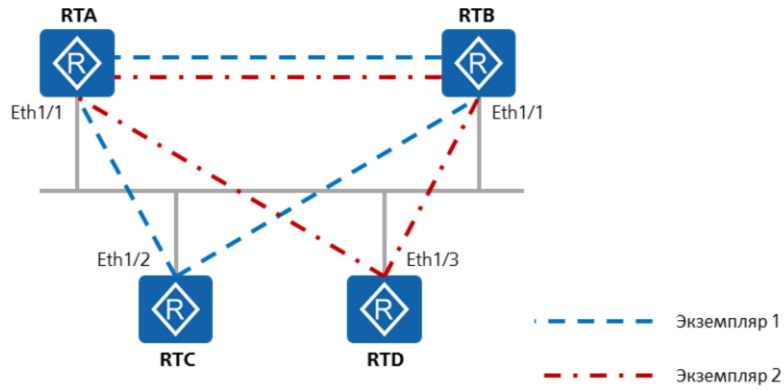
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Согласно протоколу RFC 2373 в отношении IPv6, адрес link-local предназначен для использования в одном канале для реализации таких функций, как обнаружение соседей и автонастройка. Маршрутизаторы IPv6 не пересылают пакеты с адресами link-local источника. Диапазон одиночного адреса link-local находится в диапазоне адресов IPv6 – FE80/10.

Мультиплексирование нескольких экземпляров

- Протокол OSPFv3 позволяет нескольким экземплярам работать в одном канале, мультиплексировать каналы и сокращать затраты.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Маршрутизаторы A, B, C и D подключены к одной широковещательной сети. У них общий канал связи, и они могут устанавливать отношения соседства. Экземпляр 1 создается в каналах Eth1/1 маршрутизатора A, Eth1/1 маршрутизатора B и Eth1/2 маршрутизатора C. Экземпляр 2 создается в каналах Eth1/1 маршрутизатора A, Eth1/1 маршрутизатора B и Eth1/3 маршрутизатора D. Таким образом, маршрутизаторы A, B и C могут устанавливать отношения соседства, а также маршрутизаторы A, B и D могут устанавливать отношения соседства.

- Эта схема реализуется путем добавления поля Instance ID в заголовки пакетов OSPFv3. Если ID экземпляра, сконфигурированный на интерфейсе, отличается от ID экземпляра в полученном пакете OSPF v3, интерфейс отбрасывает пакет и не устанавливает отношения соседства.

Аутентификация

- Изменение в порядке проверки:
  - Заголовок пакета OSPFv3 не содержит поля AuType и Authentication. Проверка в OSPFv3 обычно выполняется с помощью заголовка расширения аутентификации IPv6.
- Изменение контрольной суммы:
  - В OSPFv3 используется стандартная контрольная сумма IPv6.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- В протоколе OSPFv3 не обеспечена функция аутентификации. Вместо этого используется механизм обеспечения безопасности, предоставленный протоколом IPv6 для проверки действительности пакетов. Поэтому поле аутентификации в пакетах OSPFv2 содержится в заголовках пакетов OSPFv3.

Тупиковая зона

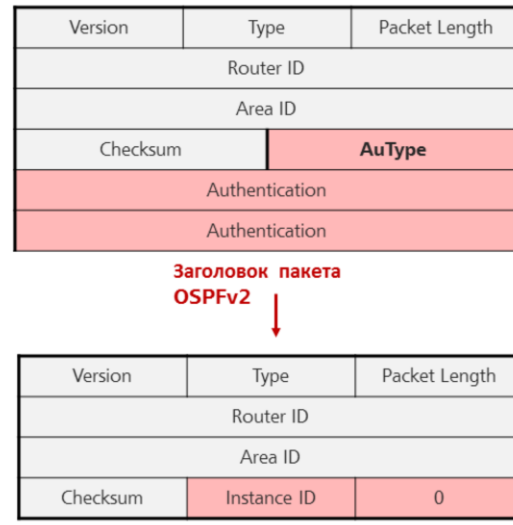
- Протокол OSPFv3 может осуществлять лавинную передачу неизвестных LSA-пакетов. Чтобы предотвратить появления большого количества неизвестных LSA-пакетов в тупиковой зоне, протокол OSPFv3 ограничивает лавинную передачу: неизвестные LSA-пакеты могут оказаться в тупиковой зоне только в том случае, когда LSA-пакеты можно распространять в пределах зоны или по каналу, а бит U не имеет значение 1.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Изменения в пакетах: описание поля заголовка

- Version: значение 2 соответствует версии протокола OSPFv2, значение 3 – версии OSPFv3.
- Type: значение 1 соответствует пакетам Hello, 2 – пакетам DD, 3 – пакетам LSR, 4 – пакетам LSU и 5 – пакетам LSAck.
- Packet Length: пакет OSPFv3 имеет два байта.
- Router ID (идентификатор маршрутизатора)
- Area ID (идентификатор зоны)
- Checksum (контрольная сумма)
- Instance ID (идентификатор экземпляра): это поле определяет экземпляры OSPF, запущенные в одном канале. Идентификаторы экземпляров действительны только для локальных каналов.
- Reserved: это поле всегда имеет значение 0.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Аналогично версии OSPFv2, в версии OSPFv3 тот же заголовок пакета, но разные поля для пяти типов пакетов OSPFv3.
- Пакеты LSU и LSAck в протоколе OSPFv3 почти совпадают с пакетами OSPFv2. Однако поля в заголовках пакетов OSPFv3, пакетах Hello, DD-пакетах и пакетах LSR немного отличаются от пакетов OSPFv2. Были внесены следующие изменения:
  - Номер версии изменен с 2 на 3.
  - Изменения заголовка пакета. По сравнению с заголовком пакета OSPFv2, заголовок пакета OSPFv3 содержит только 16 байт. Поле аутентификации удалено, но добавлено поле Идентификатор экземпляра. Поле Идентификатор экземпляра обеспечивает работу нескольких экземпляров в одном канале и действует только в диапазоне link-local. Если идентификатор экземпляра полученного пакета Hello отличается от идентификатора экземпляра, сконфигурированного для интерфейса приема пакетов, интерфейс не устанавливает отношения соседства.

Изменения в пакетах: пакеты Hello

Заголовок пакета Hello в OSPFv2

Version	Type	Packet Length
Router ID		
Area ID		
Checksum	AuType	
Authentication		
Authentication		
Network Mask		
HelloInterval	Options	Rtr Priority
RouterDeadInterval		
Designated Router ID		
Backup Designated Router ID		
Neighbor		

Заголовок пакета Hello в OSPFv3

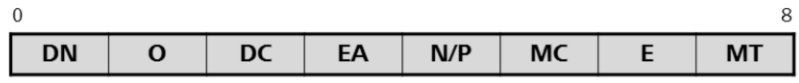
Version	Type	Packet Length
Router ID		
Area ID		
Checksum	Instance ID	0
Interface ID		
Rtr Priority	Options	
HelloInterval	RouterDeadInterval	
Designated Router ID		
Backup Designated Router ID		
Neighbor		

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

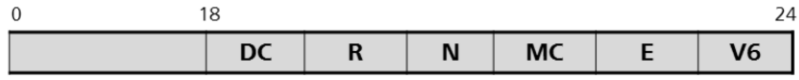
HUAWEI

- По сравнению с пакетом Hello в протоколе OSPFv2, в пакете Hello в протоколе OSPFv3 нет поля Network Mask, но есть поле Interface ID для идентификации интерфейса, отправляющего пакет Hello.
- Instance ID (ID экземпляра): 4 байта. Указывает ID интерфейса, отправляющего пакет. Это поле используется для идентификации интерфейсов, отправляющих пакеты, одного маршрутизатора, но не содержит информации об адресе.
- Rtr Pri: 1 байт. Указывает на приоритет маршрутизатора. Маршрутизатор с наивысшим приоритетом становится DR-маршрутизатором.
- Options: 3 байта. В протоколе OSPFv3 это поле расширено до 24 бит.

Изменения в пакетах: поле Options



Формат поля Options в пакете OSPFv2

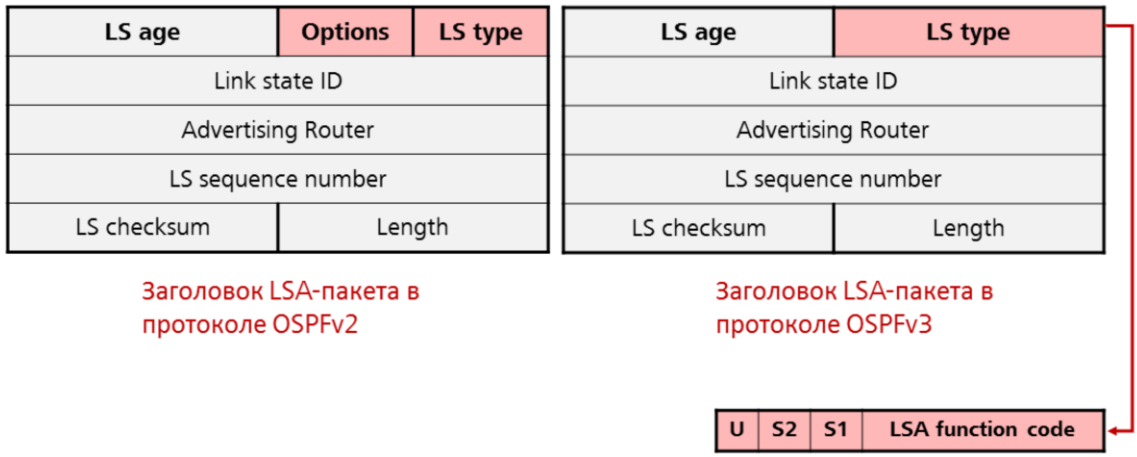


Формат поля Options в пакете OSPFv3

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- В версии OSPFv2 поле Options содержится во всех пакетах Hello, DD-пакетах и LSA-пакетах.
- В OSPFv3 поле Options содержится только в пакетах Hello, DD-пакетах, пакетах router LSA, network LSA, inter-area-router LSA и link LSA.
- Как показано на предыдущем рисунке, протокол OSPFv3 добавляет биты R и V6 в поле Options.
  - Бит R: указывает, является ли устройство маршрутизатором с возможностью переадресации. Если бит R имеет значение 0, то маршрутная информация устройства не используется при вычислении маршрута. Если текущее устройство не должно передавать пакеты с нелокальными адресами, значение бита R может быть равно 0.
  - Бит V6: если бит V6 равен 0, маршрутизатор или канал не участвуют в вычислении маршрута IPv6.
  - E: Если значение равно 0, пакеты AS-external-LSA не поддерживаются.
  - MC: связан с многоадресной передачей.
  - N: указывает, является ли зона зоной NSSA.
  - DC: указывает, поддерживается ли установка соединения по требованию.
- Сопоставление бит в поле Options имеет следующие результаты:
  - Если поле Options пакета Hello не совпадает, отношения соседства не будут установлены.
  - Если значение бита E равно 0, лавинная передача пакетов AS-external-LSA не осуществляется.
  - Если значение бита V6 равно 0, маршрутизатор не участвует в вычислении маршрута IPv6.
  - Поле Options позволяет маршрутизатору OSPF поддерживать дополнительные возможности и анонсировать свои возможности другим маршрутизаторам. С помощью этого механизма маршрутизаторы с различными возможностями могут взаимодействовать в домене маршрутизации OSPF.

Отличия в формате LSA-пакетов: заголовок



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Поле LS Type указывает на тип LSA-пакета. В LSA-пакете версии OSPFv2 это поле имеет 8 бит, в LSA-пакете версии OSPFv3 – 16 бит.
  - Бит U указывает, как маршрутизатор обрабатывает неизвестные LSA-пакеты. Значение 0 указывает на то, что неизвестные LSA-пакеты обрабатываются как LSA-пакеты с адресами link-local. Значение 1 указывает на то, что неизвестные LSA-пакеты обрабатываются на основе области распространения, указанной в битах S2 и S1.
  - Биты S2 и S1 указывают на область распространения LSA-пакетов. Значение 00 указывает на то, что LSA-пакеты будут распространяться в локальном канале, генерирующем LSA-пакеты. Значение 01 указывает на то, что LSA-пакеты будут распространяться в зоне нахождения маршрутизатора, генерирующего LSA-пакеты. Значение 10 означает, что LSA-пакеты будут распространяться во всей AS. Значение 11 зарезервировано.
  - LSA Function Code: описывает тип LSA.

Поле LSA Type: поддержка обработки неизвестных LSA-пакетов

- Бит U определяет, как маршрутизатор обрабатывает неизвестные LSA-пакеты.

Бит U	Метод обработки
0	Обрабатывает неизвестные LSA-пакеты аналогично пакетам с адресами link-local.
1	Хранит и осуществляет лавинную передачу неизвестных LSA-пакетов.

- Биты S2 и S1 определяют область лавинной передачи LSA-пакетов.

C2	C1	Область лавинной передачи
0	0	Область Link-local
0	1	Зона
1	0	AS
1	1	Зарезервировано

- Типы LSA-пакетов соответствуют битам U, S2 и S1.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- В OSPFv2 неизвестные LSA-пакеты отбрасываются.
- В OSPFv3 обработка неизвестного LSA-пакета осуществляется на основе информации в бите U в поле LS Type неизвестного LSA-пакета.
  - Если бит U имеет значение 1, неизвестный LSA-пакет распространяется в области, определенной в поле LS Type пакета.
  - Если бит U имеет значение 0, то неизвестный LSA-пакет распространяется в пределах канала.
- Область распространения LSA-пакетов определяет поле LS Type в LSA-пакете. В настоящее время существует 3 типа областей распространения LSA-пакетов.
  - Область Link-local
    - LSA-пакеты распространяются только в локальных каналах. В версии OSPFv3 были добавлены пакеты Link-LSA.
  - Зона
    - Пакеты Router-LSA, network-LSA, inter-area-prefix-LSA, inter-area-router-LSA и intra-area-prefix-LSA (впервые добавленных в версии OSPFv3) распространяются в пределах зоны.
  - AS
    - LSA-пакеты (AS-external-LSA) распространяются в пределах всей AS.

LSA Type: код функции

Код функции LSA	LS Type	Описание
1	0x2001	Router-LSA
2	0x2002	Network-LSA
3	0x2003	Inter-Area-Prefix-LSA
4	0x2004	Inter-Area-Router-LSA
5	0x4005	AS-External-LSA
6	0x2006	Group-membership-LSA
7	0x2007	Type-7-LSA
8	0x0008	Link-LSA
9	0x2009	Intra-Area-Prefix-LSA

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Link State ID

- Это поле состоит из 4 байтов. Оно не содержит информацию об адресе. В следующей таблице приведены значение этого поля в различных типах LSA-пакетов в версиях OSPFv2 и OSPFv3.

LSA	OSPFv2 LS ID	OSPFv3 LS ID
Router-LSA	ID маршрутизатора	Локальное уникальное 32-битное целое число
Network-LSA	Сегмент сети IPv4, в котором находится DR-маршрутизатор	ID интерфейса DR-маршрутизатора
Type 4 LSA	ID маршрутизатора	Локальное уникальное 32-битное целое число
Type 3, 5, or 7 LSA	Сегмент сети IPv4	Локальное уникальное 32-битное целое число
Link-LSA	---	ID интерфейса
Intra-Area-Prefix-LSA	----	Локальное уникальное 32-битное целое число

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Отличия между типами LSA-пакетов: типа LSA-пакетов в версии OSPFv3

LSA-пакеты в OSPFv2	LSA-пакеты в OSPFv3	Сходства и различия между LSA-пакетами в OSPFv3 и OSPFv2
Router-LSA	Router-LSA	Названия одинаковые, функции схожи. Однако в OSPFv3 в этом типе LSA-пакета не приводится информация об адресе, и данный пакет используется только для описания топологии домена маршрутизации.
Network-LSA	Network-LSA	
Network-summary-LSA	Inter-area-prefix LSA	Функции схожи, но названия отличаются.
ASBR-summary-LSA	Inter-area-router LSA	
AS-external-LSA	AS-External-LSA	Функции и названия одинаковые.
Нет	Link-LSA	Новый LSA-пакет
	Intra-area-prefix-LSA	Новый LSA-пакет

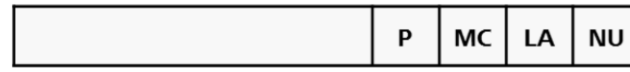
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- В версии OSPFv3 были добавлены пакеты link LSA и intra-area-prefix LSA.
  - Пакет router LSA не содержит информацию об адресе. Маршрутизатор с включенным протоколом OSPFv3 создает отдельный пакет link LSA для каждого канала, подключенного к маршрутизатору. Маршрутизатор анонсирует адрес link-local текущего интерфейса и серию адресов IPv6 маршрутизатора остальным маршрутизаторам в канале.
  - В протоколе OSPFv3 пакеты router LSA и network LSA не содержат информации о маршрутизации. Информация о маршрутизации приводится в пакетах intra-area-prefix LSA, которые используются для анонсирования одного или нескольких префиксов адресов IPv6.

Изменение метода представления префикса: поле Prefix Option

- Это поле используется для описания характеристик префикса, чтобы система могла принимать соответствующие решения и обработку при расчете различных маршрутов.
  - NU: не одноадресный бит
  - LA: бит локального адреса
  - MC: многоадресный бит
  - P: бит распространения



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

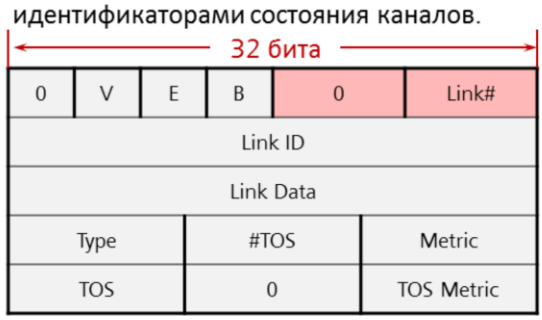
HUAWEI

- В протоколе OSPFv2 информация о префиксе в LSA-пакете указывается с помощью комбинации сегмента IP-сети и маски. Сегмент IP-сети и маска находятся в разных местах LSA-пакета, поэтому структура LSA-пакета не ясна. В OSPFv3 в LSA-пакете существует три параметра (Prefix-Length, PrefixOptions и Prefix) для обозначения информации префикса. Каждый префикс, анонсированный в LSA-пакете, имеет свое поле PrefixOptions.
- Prefix-Length
  - Это поле состоит 1 байта и указывает на длину префикса. Значение этого поля равно 0 для стандартного маршрута.
- PrefixOptions. Это поле состоит 1 байта и указывает на опцию префикса, которая используется для описания некоторых специальных полей атрибутов префикса. Оно содержит следующие биты:
  - NU: не одноадресный бит. Если значение бита равно 1, префикс не учитывается при вычислении одноадресного маршрута IPv6.
  - La: бит локального адреса. Если значение бита равно 1, префикс обозначает адрес интерфейса маршрутизатора.
  - MC: многоадресный бит. Если значение бита равно 1, префикс учитывается при вычислении многоадресного маршрута. В противном случае префикс не учитывается.
  - P: бит распространения. Этот бит должен иметь значение 1, если префикс зоны NSSA должен быть объявлен ABR-маршрутизатору.
- Префикс
  - Длина является целым числом, кратным 4 байтам. Обозначает IPv6-адрес префикса.

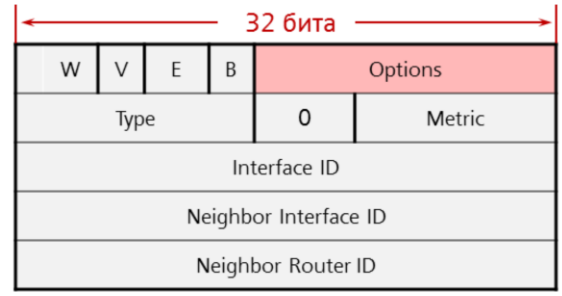
- Длина префикса переменная, но должна быть целым числом, кратным 32 битам (4 байтам). Она может быть заполнена нулями. Таким образом, длина может составлять 0, 4, 8, 12 или 16 байт.

Router LSA

- LS Type: 0x2001; область распространения: в пределах зоны.
- Каждый пакет router-LSA содержит описания нескольких каналов. Описание каждого канала содержит информацию об интерфейсе.
- Можно использовать несколько пакетов router-LSA, которые будут отличаться идентификаторами состояния каналов.



Пакет Router-LSA в OSPFv2



Пакет Router-LSA в OSPFv3

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- W: многоадресный маршрут.
- V: маршрутизатор является конечной точкой виртуального соединения.
- E: маршрутизатор является ASBR-маршрутизатором.
- B: маршрутизатор является ABR-маршрутизатором.
- Type: 1 байт. Обозначает тип канала.
- Metric: 2 байта. Это стоимость при отправке пакета данных из интерфейса.
- Interface ID: 4 байта. Определяет интерфейс, но не содержит информацию об адресах.
- Neighbor Interface ID: 4 байта. Определяет идентификатор соседнего интерфейса.
- Neighbor Router ID: 4 байта. Определяет идентификатор маршрутизатора соседа.

Тип канала в пакете Router-LSA

Тип	Описание	Neighbor Router ID	Neighbor Interface ID
1	Канал, подключенный к другому маршрутизатору в режиме P2P	ID соседнего маршрутизатора	ID интерфейса соседа
2	Канал, подключенный к транзитной сети	ID DR-маршрутизатора	ID интерфейса DR-маршрутизатора
3	Зарезервированный канал	---	---
4	Виртуальный канал	ID соседнего маршрутизатора	Идентификатор интерфейса виртуального канала соседа

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Пакет router-LSA, созданный маршрутизатором, распространяется только в пределах зоны, в которой находится маршрутизатор. Данный LSA-пакет описывает все отношения соседства в состоянии маршрутизатора full. Это означает, что в пакете router-LSA не описываются тупиковые зоны (в OSPFv2 каналы к тупиковым зонам описываются в LSA 3 типа.) Пакет router-LSA должен содержать описание для каждого соседа в канале P2MP. Длина каждого описания канала зафиксирована. Поэтому количество каналов в пакете router-LSA можно определить по длине LSA-пакета в заголовке.
- Пакет router-LSA может содержать несколько описаний каналов. Маршрутизатор может создать несколько пакетов router-LSA, отличающиеся идентификаторами состояния каналов. При расчете SPF все пакеты router-LSA, созданные одним маршрутизатором, должны быть объединены.
- Пакет router-LSA в OSPFv3 не содержит информацию префикса, а описывает только топологические соединения.

Пример пакета Router-LSA

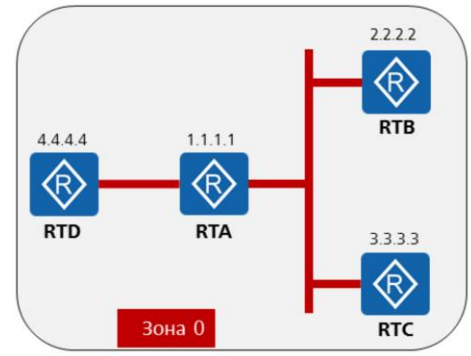
```
<RTA> display ospfv3 lsdb router

  Router-LSA (Area 0.0.0.0)

 LS Age: 872
 LS Type: Router-LSA
 Link State ID: 0.0.0.0
 Originating Router: 1.1.1.1
 LS Seq Number: 0x80000008
 Checksum: 0x0FC2
 Length: 56
 Flags: 0x00 (-|-|-|-)
 Options: 0x000013 (-|R|-|-|E|V6)

  Link connected to: a Transit Network
    Metric: 1
    Interface ID: 0x18000202
    Neighbor Interface ID:  0X18000202 ← ID интерфейса DR-маршрутизатора
    Neighbor Router ID:  2.2.2.2 ← ID DR-маршрутизатора

  Link connected to: another Router (point-to-point)
    Metric: 1562
    Interface ID: 0x18000286
    Neighbor Interface ID:  0X18000206 ← ID интерфейса соседа
    Neighbor Router ID:  4.4.4.4 ← ID маршрутизатора соседа
```

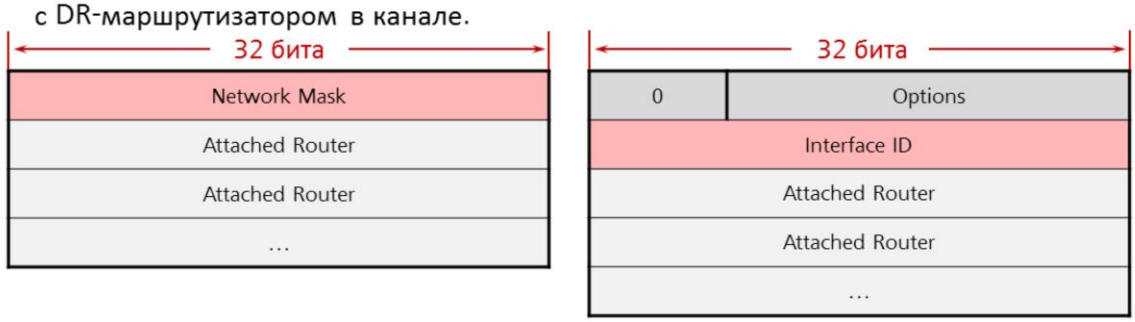


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Изменения в пакете Network-LSA

- Пакет network-LSA создается DR-маршрутизатором и распространяется в пределах зоны.
- Пакет network-LSA описывает все маршрутизаторы, имеющие полноценную связь с DR-маршрутизатором в канале.



Пакет Network LSA в OSPFv2

Пакет Network LSA в OSPFv3

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Options: 3 байта. Это поле представляет собой набор полей Options пакетов link-LSA всех маршрутизаторов в канале, то есть набор возможностей, поддерживаемых маршрутизаторами.
- Attached Router:
  - Четыре байта для каждого маршрутизатора. В этом поле описаны ID всех маршрутизаторов, имеющих полноценную связь с DR-маршрутизаторов в канале.
  - Пакет network-LSA в OSPFv3 создает DR-маршрутизатор, и его лавинная передача осуществляется в пределах зоны. Идентификатор состояния канала является идентификатором интерфейса DR-маршрутизатора. Поле маски, существующее в OSPFv2, было удалено. Поэтому пакет network-LSA в OSPFv3 не содержит информацию префикса, а описывает только топологические соединения.
  - Кроме того, поле Options описывает набор возможностей всех

маршрутизаторов в канале. Таким образом, DR-маршрутизатор не влияет на передачу LSA-пакетов других маршрутизаторов.

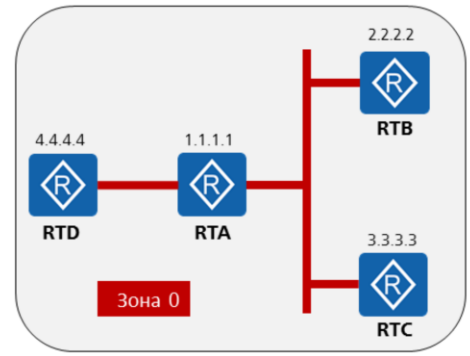
Пример пакета Network-LSA

```
<RTA>display ospfv3 lsdb network


 OSPFv3 Router with ID (1.1.1.1) (Process 1)


 Network-LSA (Area 0.0.0.0)

 LS Age: 95
 LS Type: Network-LSA
 Link State ID:  24.0.2.2 ← ID интерфейса  DR-маршрутизатора
 Originating Router:  2.2.2.2 ← ID DR-маршрутизатора
LS Seq Number: 0x80000006
 Checksum: 0xCB18
 Length: 36
 Options: 0x000013 (-|R|-|-|E|V6)
   Attached Router: 2.2.2.2
   Attached Router: 1.1.1.1
   Attached Router: 3.3.3.3
```



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Пакет Link-LSA (новый тип пакета в OSPFv3)

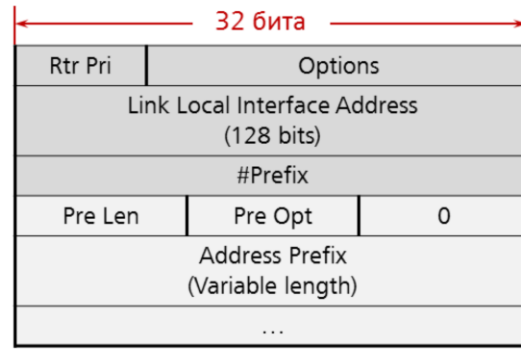
- Пакет link-LSA – это новый тип LSA-пакета, который появился в версии протокола OSPFv3. Пакет link-LSA генерируется маршрутизатором для каждого интерфейса OSPFv3 и распространяется в канале. Данный пакет выполняет следующие функции:
  - Анонсирование адреса local-link в качестве адреса следующего узла для других маршрутизаторов на канале.
  - Анонсирование всех префиксов IPv6 на локальном канале другим маршрутизаторам в канале.
  - Предоставление значение поля Options DR-маршрутизатору в широковещательной сети или сети NBMA.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Структура пакета Link-LSA

- Rtr Pri: приоритет маршрутизатора в канале.
- Options: возможности маршрутизатора.
- Link Local Interface Address: локальный адрес интерфейса, который используется для вычисления следующего узла маршрута.
- #Prefix: количество префиксов.
- Others: три параметра (Prefix-Length, PrefixOptions и Prefix).



Link LSA

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Пример пакета Link-LSA

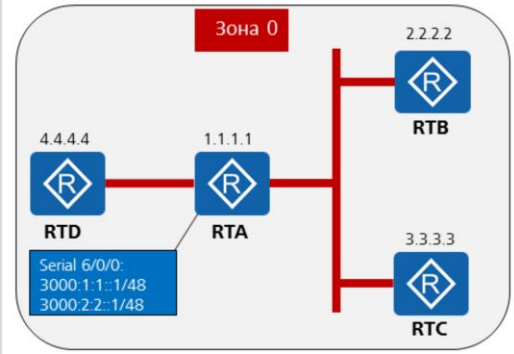
```
[RTA]display ospfv3 lsdb link 24.0.2.134 ← Отображает пакет link-LSA указанного идентификатора состояния канала.

Link-LSA (Interface Serial6/0/0)

  LS Age: 17
  LS Type: Link-LSA
  Link State ID: 24.0.2.134 ← Interface index
  Originating Router: 1.1.1.1
  LS Seq Number: 0x80000024
  Checksum: 0x7F10
  Length: 68
  Priority: 1
  Options: 0x000013 (-|R|-|-|E|V6)
  Link-Local Address: FE80::5ECC:5200:1
  Number of Prefixes: 2 ← Передаются два префикса.

    Prefix: 3000:1:1::/48
    Prefix Options: 0 (-|-|-|-)

    Prefix: 3000:2:2::/48
    Prefix Options: 0 (-|-|-|-)
```



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Пакет Intra-Area-Prefix-LSA

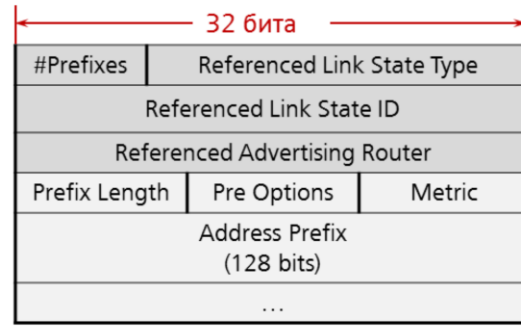
- Для чего созданы пакеты intra-area-prefix-LSA?
  - В OSPFv2 адресная информация содержится в пакетах router-LSA в тупиковых сетях и пакетах network-LSA в транзитных сетях. Однако в OSPFv3 пакеты router-LSA и network-LSA не содержат адресную информацию. Поэтому были созданы пакеты Intra-area-prefix-LSA.
- Intra-area-prefix-LSA содержат следующую информацию о префиксе IPv6:
  - Префиксы маршрутизатора
  - Префиксы тупиковых сетей
  - Префиксы транзитных сетей
- Маршрутизатор или транзитная сеть могут создать множество пакетов intra-area-prefix-LSA.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Пакеты Intra-Area-Prefix-LSA

- В OSPFv2 пакеты router-LSA и network-LSA используются для анонсирования маршрутов внутри зон. В OSPFv3 эти два типа LSA не содержат адресную информацию. Поэтому для анонсирования маршрутов внутри зон были созданы пакеты Intra-area-prefix-LSA.
- # Prefixes: количество префиксов, содержащихся в LSA.
- Referenced Link State Type:
  - = 1: префикс подключенного маршрутизатора (включая тупиковую сеть)
  - = 2: Префикс прикрепленной транзитной сети
- Referenced Link State ID:
  - Тип 1: 0;
  - Тип 2: ID интерфейса DR-маршрутизатора.
- Referenced Advertising Router:
  - Тип 1: ID подключенного маршрутизатора
  - Тип 2: ID DR-маршрутизатора
- Others: Prefix-Length, PrefixOptions и Prefix



Intra-area-prefix-LSA

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

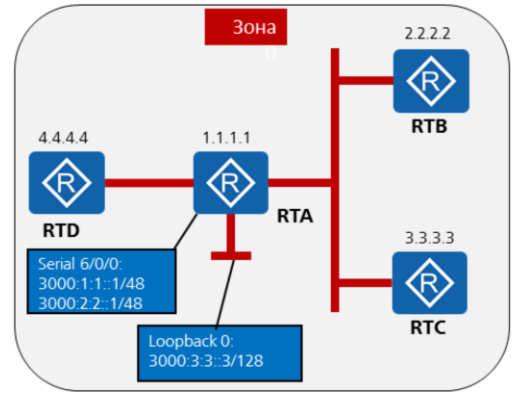
- Пакет intra-area-prefix-LSA в протоколе OSPFv3 распространяется в пределах зоны для анонсирования информации префикса внутри зоны. В соответствии с разными LSA-пакетами существуют две ситуации:
  - При ссылке на пакет router-LSA, пакет intra-area-prefix-LSA генерируется каждым маршрутизатором для анонсирования префиксов двухточечных соединений и префиксов тупиковых сетей.
  - При ссылке на пакет network-LSA, пакет intra-area-prefix-LSA генерируется DR-маршрутизатором для анонсирования всех префиксов в сети, соответствующих каналу. Эти префиксы извлекаются из пакетов link-LSA, генерируемых всеми маршрутизаторами в канале. Тем не менее, информация об адресе link-local в пакетах link-LSA и префиксах, в которых бит NU или LA равен 1, исключена.

Пример пакета Intra-Area-Prefix-LSA (подключение к маршрутизатору)

```
<RTA>display ospfv3 lsdb intra-prefix
            Intra-Area-Prefix-LSA (Area 0.0.0.0)
 LS Age: 20
 LS Type: Intra-Area-Prefix-LSA
 Link State ID: 0.0.0.1
 Originating Router: 1.1.1.1
 LS Seq Number: 0x8000003E
 Checksum: 0xA932
 Length: 76
 Number of Prefixes: 3
 Referenced LS Type:  0x2001 ← Ссылка на пакет router-LSA.
 Referenced Link State ID:  0.0.0.0 ← Первый LS ID в пакете router LSA
 Referenced Originating Router:  1.1.1.1 ← Идентификатор
маршрутизатора.
   Prefix: 3000:2:2::/48
   Prefix Options: 0 (-|-|-)
   Metric: 1562

   Prefix: 3000:1:1::/48
   Prefix Options: 0 (-|-|-)
   Metric: 1562

   Prefix: 3000:3:3::3/128
   Prefix Options:  2 (-|-|LA|-) ← Адрес локального хоста
   Metric: 0
```



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

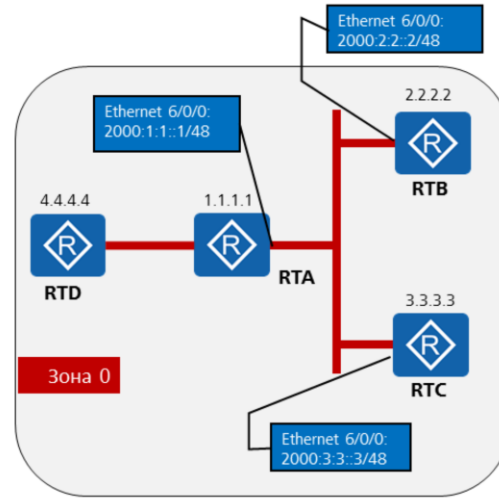
Intra-Area-Prefix-LSA (подключение к транзитной сети)

```
<RTA>display ospfv3 lsdb intra-prefix
                Intra-Area-Prefix-LSA (Area 0.0.0.0)
  LS Age: 1407
  LS Type: Intra-Area-Prefix-LSA
  Link State ID: 0.0.0.2
  Originating Router: 2.2.2.2
  LS Seq Number: 0x80000028
  Checksum: 0xB1E7
  Length: 68
  Number of Prefixes: 3
  Referenced LS Type: 0x2002 ← Ссылка на пакет network-LSA.
  Referenced Link State ID: 24.0.2.2 ← Идентификатор интерфейса DR-маршрутизатора
  Referenced Originating Router: 2.2.2.2 ← Идентификатор интерфейса DR-маршрутизатора

    Prefix: 2000:1:1::/48
    Prefix Options: 0 (-|-|-)
    Metric: 0

    Prefix: 2000:2:2::/48
    Prefix Options: 0 (-|-|-)
    Metric: 0

    Prefix: 2000:3:3::/48
    Prefix Options: 0 (-|-|-)
    Metric: 0
```



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

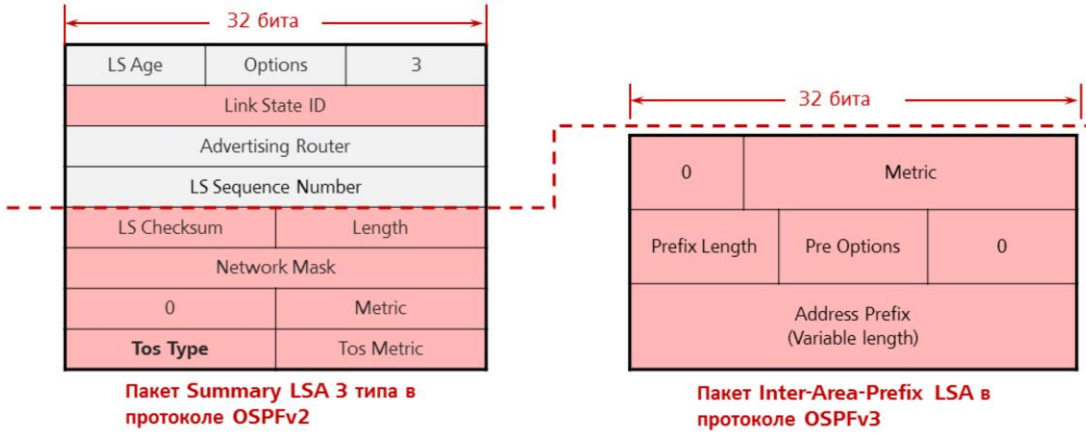
Изменения в LSA-пакетах 3 типа: Inter-Area-Prefix-LSA

- В протоколе OSPFv2 этот тип LSA-пакета называется пакетом summary-LSA 3 типа. В протоколе OSPFv3 этот тип LSA-пакета называется Inter-area-prefix-LSA. В нем приводится информация о префиксах других зон.
  - LSA-пакет 3 типа генерируется ABR-маршрутизатором и лавинно передается в пределах зоны.
  - LSA-пакет данного типа описывает информацию маршрутизации других областей в локальной AS.
  - Каждый пакет inter-area-prefix-LSA содержит префикс адреса.
  - LSA-пакет не содержит адреса link-local.
  - LSA-пакет имеет 32-битное целое число в качестве идентификатора состояния канала, чтобы отличить себя от других LSA-пакетов, генерируемых тем же маршрутизатором.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Структура пакета Inter-Area-Prefix-LSA Structure



Пакет Summary LSA 3 типа в протоколе OSPFv2

Пакет Inter-Area-Prefix LSA в протоколе OSPFv3

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Metric: 20 бит. Стоимость маршрута от ABR-маршрутизатора до маршрута префикса.
- Prefix information: Prefix-Length, PrefixOptions и Prefix.
- В протоколе OSPFv2 поле Link State ID в заголовке LSA указывает на сетевой адрес. Маска передается в LSA-пакете.
- В протоколе OSPFv3 поле Link State ID в заголовке пакета inter-area-prefix-LSA не содержит информации префикса. Поле Link State ID представляет собой 32-разрядный номер, используемый для дифференциации LSA-пакетов, создаваемых одним маршрутизатором. Все префиксы описаны с помощью трех элементов префикса.
- Пакеты inter-area-prefix-LSA генерируются ABR-маршрутизатором и лавинно передаются в пределах зоны. Каждый пакет inter-area-prefix-LSA содержит префикс адреса, но не содержит адресов link-local.

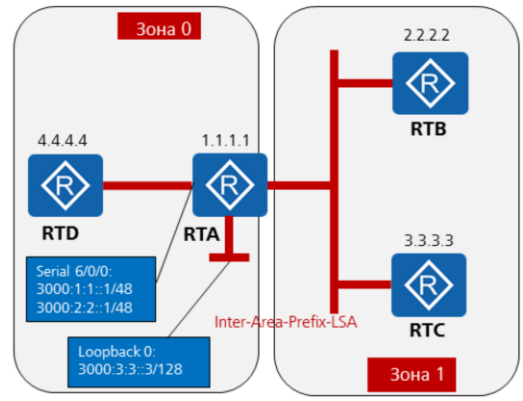
Пример пакета Inter-Area-Prefix-LSA

```
<RTC>display ospfv3 lsdb inter-prefix

     Inter-Area-Prefix-LSA (Area 0.0.0.1)

 LS Age: 89
 LS Type: Inter-Area-Prefix-LSA
 Link State ID: 0.0.0.3
 Originating Router: 1.1.1.1
 LS Seq Number: 0x80000002
 Checksum: 0xB5F6
 Length: 36

  Metric: 1562
  Prefix: 3000:1:1::/48
  Prefix Options: 0
```



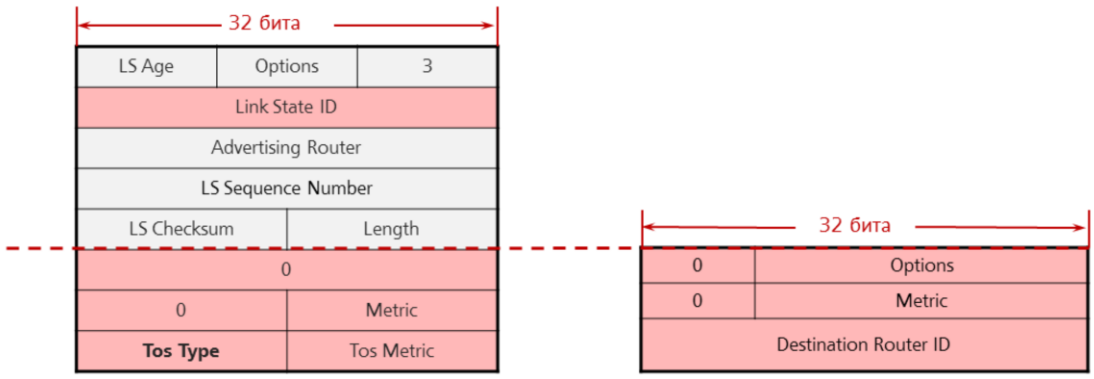
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Изменения в LSA 4 типа: пакет Inter-Area-Router-LSA

- В протоколе OSPFv2 этот тип LSA-пакета называется пакетом summary-LSA 4 типа. В протоколе OSPFv3 этот тип LSA-пакета называется Inter-area-router-LSA. В нем приводится информация об ASBR-маршрутизаторе, подключенном к другим областям.
  - LSA-пакет 4 типа генерируется ABR-маршрутизатором и распространяется в пределах зоны.
  - Данный тип LSA-пакета включает информацию об ASBR-маршрутизаторе других областей в локальной AS.
  - Каждый пакет inter-area-router-LSA содержит информацию об одном ASBR-маршрутизаторе.
  - Поле Options в LSA-пакете 4 типа описывает те же возможности, которые описывает пакет router LSA, генерируемый соответствующим ASBR-маршрутизатором.
  - LSA 4 типа использует 32-битное целое число в качестве идентификатора состояния канала, чтобы отличить себя от других LSA-пакетов, генерируемых тем же маршрутизатором.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Структура пакета Inter-Area-Router-LSA в протоколе OSPFv3



Пакет Summary LSA 4 типа в протоколе OSPFv2

Пакет Inter-Area-Router LSA в протоколе OSPFv3

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Options: 3 байта. В данном поле описываются возможности ASBR-маршрутизатора назначения, а не возможности маршрутизатора, генерирующего LSA-пакеты.
- Metric: 3 байта. Стоимость маршрута от ABR-маршрутизатора до ASBR-маршрутизатора назначения.
- Destination Router ID: 4 байта. ID ASBR-маршрутизатора назначения.
- В протоколе OSPFv2 в поле Link State ID в заголовке LSA-пакета указывается ID ASBR-маршрутизатора назначения. В протоколе OSPFv3 поле Link State ID в заголовке пакета inter-area-router-LSA не имеет какого-либо конкретного значения. Это 32-битное число, используемое для дифференциации LSA-пакетов, генерируемых одним маршрутизатором.
- Пакет inter-area-router-LSA генерируется ABR-маршрутизатором и лавинно передается в пределах зоны. Каждый пакет inter-area-router-LSA содержит информацию о ASBR-маршрутизаторе назначения.

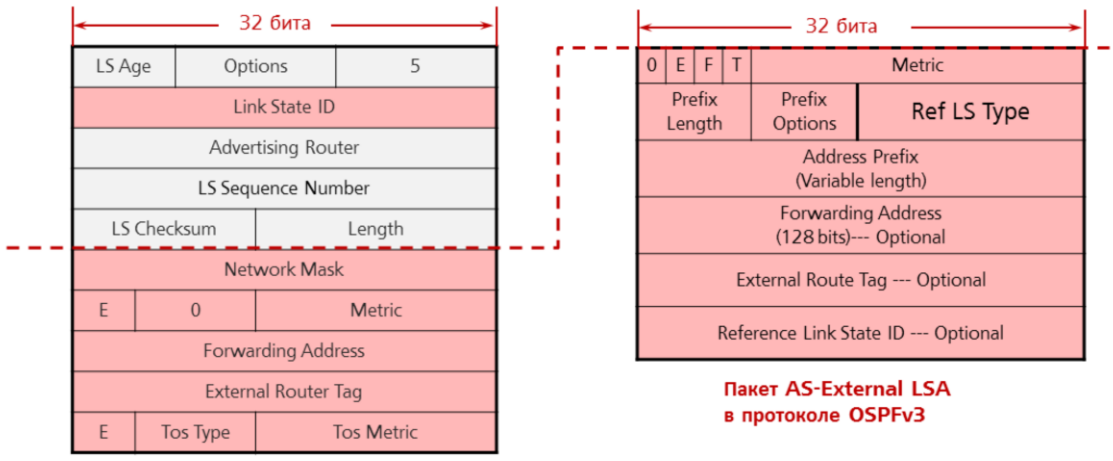
Пакет AS-External-LSA

- Пакет AS-external-LSA генерируется ASBR-маршрутизатором и описывает информацию маршрутизации внешних зон.
- Такие пакеты распространяются внутри AS.
- Идентификатор состояния канала в данном типе LSA-пакета не содержит адресную информацию, но используется для того, чтобы отличить себя от других пакетов AS-External-LSA.
- Пакет AS-External-LSA не содержит адреса link-local.
- Дополнительные поля:
  - Forwarding Address
  - External Router Tag
  - Referenced Link State ID: зарезервированное поле.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Структура пакета AS-External-LSA Structure



Пакет AS-External LSA в протоколе OSPFv2

Пакет AS-External LSA в протоколе OSPFv3

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- E: тип метрики внешнего маршрута. Значение 1 указывает на метрику внешнего маршрута 2 типа. Эта метрика не увеличивается при передаче маршрута. Значение 0 указывает на метрику внешнего маршрута 1 типа. Эта метрика увеличивается при передаче маршрута.
- F: Значение 1 указывает на передачу поля Forwarding Address.
- T: Значение 1 указывает на передачу поля External Route Tag.
- Prefix information: Prefix-Length, PrefixOptions и Prefix.
- Ref LS Type: 2 байта. Если значение не равно 0, передается поле Referenced Link State ID.
- Forwarding Address: 16 байт. Это поле является необязательным, включает 128-битный адрес IPv6. Это поле передается, если бит F равен 1. Оно указывает адрес, на который должен быть переадресован пакет, прежде чем пакет достигнет пункта назначения. Этот адрес может использоваться, если анонсирующий маршрутизатор не является оптимальным следующим узлом.
- External Route Tag: 4 байта. Это поле является необязательным. Оно может использоваться для установления связи между ASBR-маршрутизаторами. Как правило, маршруты, импортированные пограничными маршрутизаторами OSPF в AS, могут быть отфильтрованы путем настройки значения этого бита.
- Referenced Link State ID: 4 байта. Это поле передается, если поле Ref LS Type не имеет значение 0. Если это поле существует, в другом LSA-пакете можно найти дополнительную информацию об анонсированном внешнем маршруте. Информация, на которую ссылается пакет, выглядит следующим образом:
  - LS type является значением поля Referenced LS Type в пакете AS-external-LSA.
  - ID состояния канала – это значение поля Referenced Link State ID в пакете AS-external-LSA.
  - Анонсирующий маршрутизатор – это значение поля Advertising Router в пакете AS-external-LSA.
  - Эта возможность обеспечивает расширения и не используется в настоящее время.
- В протоколе OSPFv2 поле Link State ID в заголовке LSA-пакета указывает на сетевой адрес. Маска передается в LSA-пакете.
- В протоколе OSPFv3 поле Link State ID в заголовке пакета AS-External-LSA не содержит информации префикса. Это 32-битное число, используемое для дифференциации LSA-пакетов, генерируемых одним

маршрутизатором. Все префиксы описываются с помощью трех элементов префиксов.

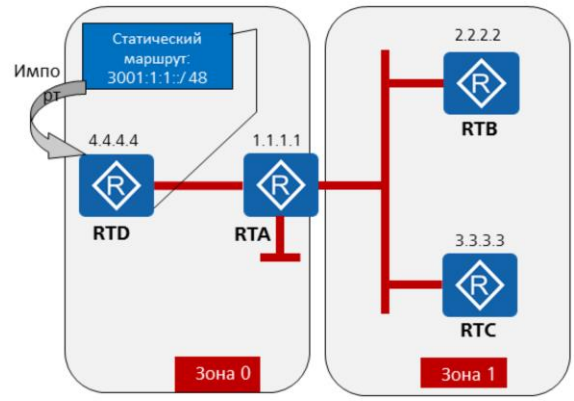
- Пакет AS-external-LSA генерируется ASBR-маршрутизатором и лавинно передается внутри AS. Каждый пакет AS-external-LSA содержит префикс адреса, но не содержит информацию об адресе link-local.

Пример пакета AS-External-LSA

```
<RTB>display ospfv3 lsdb external
OSPFv3 Router with ID (2.2.2.2) (Process 1)

        AS-External-LSA

  LS Age: 1027
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.1
  Originating Router: 4.4.4.4
  LS Seq Number: 0x80000004
  Checksum: 0xD0C7
  Length: 36
   Metric Type: 2 (Larger than any link state path)
    Metric: 1
    Prefix: 3001:1:1::/48 ← Импортированный
статический маршрут
    Prefix Options: 0 (-|-|-|-)
```



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.



Содержание

- Принципы работы OSPFv2
- Диагностика ошибок в протоколе OSPFv2
- Общая информация о OSPFv3
- Различия между OSPFv3 и OSPFv2
- **Методы конфигурации OSPFv3 и основные команды**
- Рекомендации по подготовке к экзамену по протоколу OSPF

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Техобслуживание и отладка

Операция	Команда
Включение отладки событий OSPFv3.	debugging ospfv3 event { abr | asbr | vlink | all }
Включение отладки состояния интерфейса OSPFv3.	debugging ospfv3 ifsm [status | event | timer]
Включение отладки LSA-пакетов OSPFv3.	debugging ospfv3 lsa { all | flooding | generate | install | maxage | refresh | verbose }
Включение отладки статуса соседа OSPFv3.	debugging ospfv3 nfsm [status | event | timer]
Включение отладки пакетов OSPFv3.	debugging ospfv3 packet all [verbose] debugging ospfv3 packet { hello | dd | request | update | ack } * [verbose] debugging ospfv3 packet verbose
Включение отладки расчета маршрута OSPFv3.	debugging ospfv3 route [ase | install | spf | ia]

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Отображение данных LSDB (1)

```
<RTA>display ospfv3 lsdb

        OSPFv3 Router with ID (1.1.1.1) (Process 1)
          Link-LSA (Interface Ethernet6/0/0)

Link State ID   Origin Router   Age  Seq#      CkSum  Prefix
24.0.2.2        1.1.1.1         0720 0x80000032 0x7314    1
24.0.2.2        2.2.2.2         0693 0x80000032 0xb1ce    1
24.0.2.2        3.3.3.3         0661 0x80000032 0xef89    1

          Link-LSA (Interface Serial6/0/0)

Link State ID   Origin Router   Age  Seq#      CkSum  Prefix
24.0.2.134      1.1.1.1          0004 0x80000061 0xa61d    1
24.0.2.6        4.4.4.4         0408 0x8000005f 0x5b11    1

          Router-LSA (Area 0.0.0.0)

Link State ID   Origin Router   Age  Seq#      CkSum    Link
0.0.0.0         1.1.1.1         0714 0x80000067 0x685c    1
0.0.0.0         4.4.4.4         0818 0x80000061 0x28a1    1
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Отображение данных LSDB (2)

```
            Inter-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID   Origin Router    Age  Seq#       CkSum
0.0.0.2         1.1.1.1          0645 0x80000032 0xf9b2
0.0.0.3         1.1.1.1          0645 0x80000032 0x0e9b
0.0.0.4         1.1.1.1          0645 0x80000032 0x2284

            Intra-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID   Origin Router    Age  Seq#       CkSum  Prefix  Reference
0.0.0.1         1.1.1.1          0004 0x8000008b 0x0917     2  Router-LSA
0.0.0.1         4.4.4.4          0813 0x80000085 0x2cb2     1  Router-LSA

            Router-LSA (Area 0.0.0.1)
Link State ID   Origin Router    Age  Seq#       CkSum    Link
0.0.0.0         1.1.1.1          0645 0x80000036 0xc6d9    1
0.0.0.0         2.2.2.2          0633 0x80000036 0xa5f7    1
0.0.0.0         3.3.3.3          0620 0x80000034 0x8b10    1

            Network-LSA (Area 0.0.0.1)
Link State ID   Origin Router    Age  Seq#       CkSum
24.0.2.2        3.3.3.3          0620 0x80000033 0x337f
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Отображение данных LSDB (3)

```
 Inter-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   Origin Router    Age   Seq#       CkSum
0.0.0.3         1.1.1.1          0709  0x80000033 0x5328
0.0.0.5         1.1.1.1          0709  0x80000033 0x51e8

          Inter-Area-Router-LSA (Area 0.0.0.1)

Link State ID   Origin Router    Age   Seq#       CkSum
0.0.0.1         1.1.1.1          0815  0x80000031 0x8f32

          Intra-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   Origin Router    Age   Seq#       CkSum  Prefix  Reference
0.0.0.1         3.3.3.3          0620  0x80000032 0xbbcc     3  Network-LSA

          AS-External-LSA

Link State ID   Origin Router    Age   Seq#       CkSum
0.0.0.1         4.4.4.4          0818  0x80000031 0x76f4 E2
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Отображение информации об интерфейсе

```
<RTA>display ospfv3 interface ethernet6/0/0

Ethernet6/0/0 is up, line protocol is up
  Interface ID 0x18000202 ← Индекс интерфейса
  Interface MTU 1500
  IPv6 Prefixes
    FE80::200:5EFF:FECC:5200 (Link-Local Address) ← Адрес link-local интерфейса
    2000:1:1::1/48
  OSPFv3 Process (1), Area 0.0.0.1, Instance ID 0
    Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State DROther, Priority 1
    Designated Router (ID) 3.3.3.3
      Interface Address FE80::200:5EFF:FECC:5202
    Backup Designated Router (ID) 2.2.2.2
      Interface Address FE80::200:5EFF:FECC:5201
    Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:01
    Neighbor Count is 2, Adjacent neighbor count is 2
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Отображение информации о соседе

```
<RTA>display ospfv3 peer

OSPFv3 Process (1)

OSPFv3 Area (0.0.0.0)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
4.4.4.4           1   Full/ -         00:00:39    S6/0/0           0

OSPFv3 Area (0.0.0.1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
2.2.2.2           1   Full/Backup     00:00:31    Eth6/0/0         0
3.3.3.3           1   Full/DR         00:00:37    Eth6/0/0         0
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Отображение информации о топологии

```
<RTA>display ospfv3 topology

OSPFv3 Process (1)
OSPFv3 Area (0.0.0.0) topology
Type  ID(If-Index)      Bits     Metric   Next-Hop       Interface
Rtr   1.1.1.1           B        --
Rtr   4.4.4.4           E        1562     4.4.4.4        Serial6/0/0

OSPFv3 Area (0.0.0.1) topology
Type  ID(If-Index)      Bits     Metric   Next-Hop       Interface
Rtr   1.1.1.1           B        --
Rtr   2.2.2.2                    1        2.2.2.2        Ethernet6/0/0
Rtr   3.3.3.3                    1        3.3.3.3        Ethernet6/0/0
Net   3.3.3.3(402653698)         1        0.0.0.0        Ethernet6/0/0
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Отображение информации таблицы маршрутизации OSPFv3

```
<RTC>display ospfv3 routing

 OSPFv3 Process (1)
  Destination                          Metric
    Next-hop
    2000:1:1::/48                        1
         via FE80::200:5EFF:FECC:5200,  Ethernet6/0/0
    2000:2:2::/48                        1
         via FE80::200:5EFF:FECC:5201,  Ethernet6/0/0
    2000:3:3::/48                        1
         directly-connected,  Ethernet6/0/0
  IA 3000:1:1::/48                     1563
         via FE80::200:5EFF:FECC:5200,  Ethernet6/0/0
  IA 3000:3:3::3/128                     1
         via FE80::200:5EFF:FECC:5200,  Ethernet6/0/0
  E2 3001:1:1::/48                       1
         via FE80::200:5EFF:FECC:5200,  Ethernet6/0/0
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.



Содержание

- Принципы работы OSPFv2
- Диагностика ошибок в протоколе OSPFv2
- Общая информация о OSPFv3
- Различия между OSPFv3 и OSPFv2
- Методы конфигурации OSPFv3 и основные команды
- **Советы по подготовке к экзамену по протоколу OSPF**

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Рекомендации по подготовке к экзамену по протоколу OSPF

- Изучите команды OSPF.
- Изучите конфигурации политики OSPF.
- Прочитайте документы HedEx.
  - Ознакомьтесь с примерами в документах HedEx.
- Изучите основные команды отображения и отладки.
- Ознакомьтесь с примерами, приведенными в курсе.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Рекомендации

- Веб-сайт Huawei learning
  - Http://support.huawei.com/learning/en/newindex.html
- Библиотека примеров службы поддержки Huawei
  - http://support.huawei.com/enterprise/servicecenter?lang=en

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Спасибо!

www.huawei.com

HCIE-R&S
— Протокол IS-IS

www.huawei.com

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Введение

- Протокол обмена данными между промежуточными системами (Intermediate System-to-Intermediate System, IS-IS) — это протокол внутренних шлюзов (IGP) в IP-сетях. Благодаря использованию кодировки TLV, IS-IS обладает отличной масштабируемостью и высокой надежностью. Благодаря масштабируемости, применение IS-IS не ограничивается стандартными IP-сетями. Протокол IS-IS также можно использовать в центрах обработки данных, в сетях IPv6 и в IP-сети в иных сценариях. В данной главе основное внимание уделяется расширенным функциональным возможностям и конфигурациям IS-IS и IPv6 IS-IS. Кроме того, здесь описывается развертывание и внедрение протокола dual IS-IS в действующей сети.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Цели

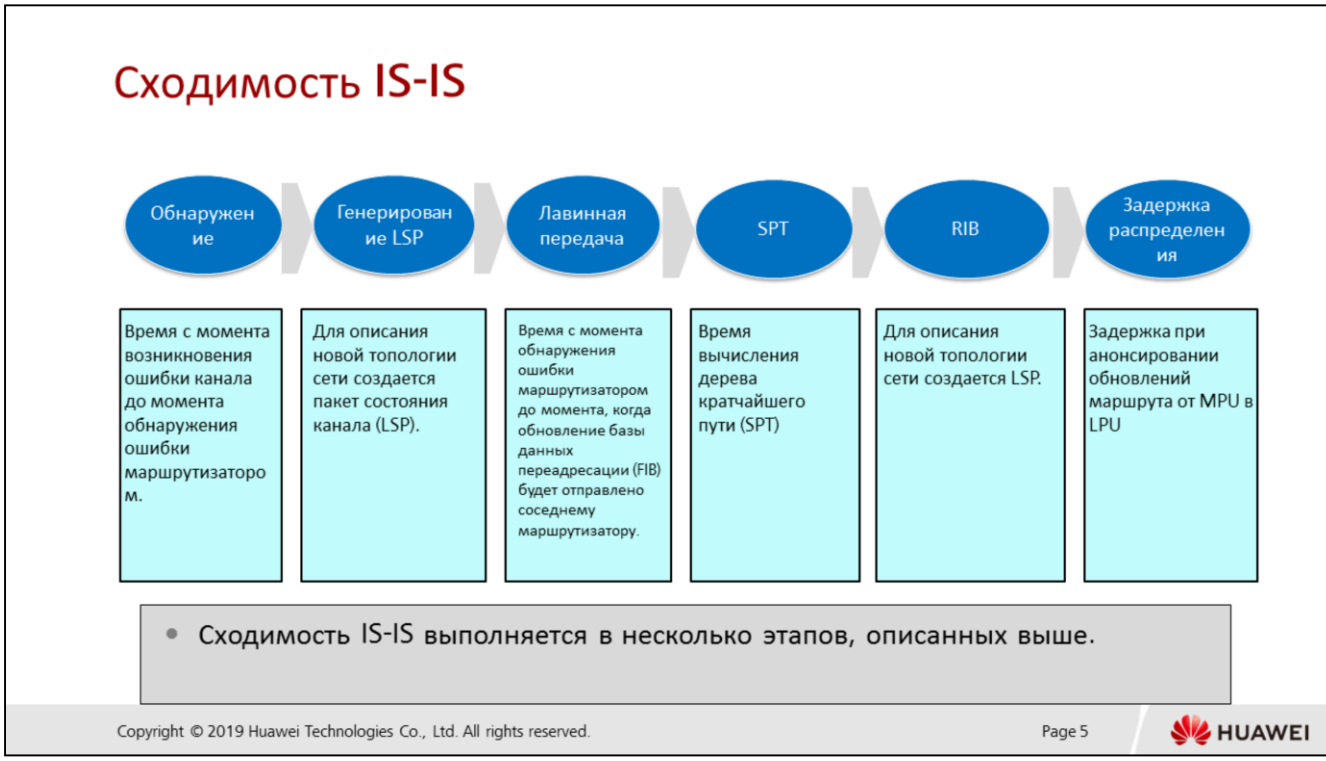
- После прохождения этого курса вы будете знать:
  - Расширенные функции IS-IS.
  - Принципы работы с функциями и конфигурациями IPv6 IS-IS.
  - Применение IS-IS.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Содержание

1. **Расширенные функции IS-IS**
   - Быстрая сходимость IS-IS
   - Административный тег IS-IS
   - Фрагментация пакетов LSP в IS-IS
   - Фильтрация маршрутов IS-IS
2. Основные принципы и конфигурации IPv6 IS-IS
3. Примеры применения IS-IS к двойному стеку

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.



- Сходимость IS-IS выполняется в несколько этапов:
  - Обнаружение: время с момента возникновения ошибки на канале до момента момента обнаружения ошибки маршрутизатором.

    : время, необходимое для создания LSP для описания новой топологии сети

    : время с момента обнаружения ошибки маршрутизатором до момента анонсирования маршрутизатором обновления FIB соседям
  - SPT: время для расчета дерева кратчайшего пути
  - RIB: время на обновление записей RIB и FIB основным процессором

    : задержка при анонсировании обновлений маршрута от системной платы в сервисную плату
- Этапы RIB и задержки распределения связаны с аппаратными средствами маршрутизатора, такими как процессор MPU, процессор LPU, память и сетевой процессор. Эти два этапа оказывают незначительное влияние на время сходимости. Поэтому в следующем разделе описываются только первые четыре фазы.

Обнаружение ошибки канала



Обнаружение ошибки канала IS-IS в обычных случаях

- В обычных случаях обнаружение состояния канала IS-IS зависит только от протокола IS-IS, то есть от пакетов IS-IS Hello (IIH). Пакеты IIH поддерживают обнаружение ошибок второго уровня, что неприменимо к сетям, требующим быстрой сходимости.
- Чтобы сократить время обнаружения ошибок, настройте небольшой интервал передачи пакетов IIH.

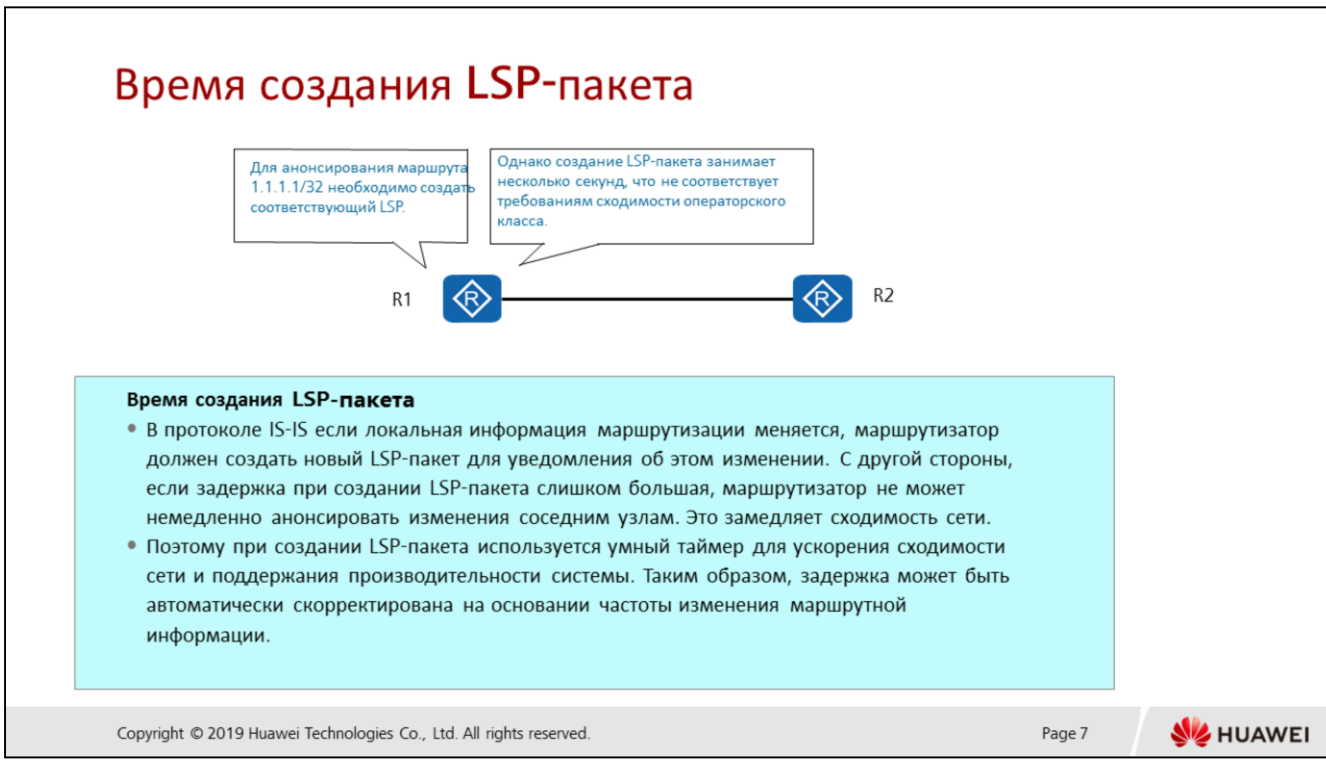
Обнаружение ошибки канала IS-IS с помощью других протоколов

- Сеть SDH/SONET (POS) и оптический интерфейс Ethernet поддерживают обнаружение состояния канала в пределах нескольких миллисекунд, обеспечивая более высокую скорость сходимость сети. Однако это решение зависит от типа интерфейса.
- Протокол BFD обычно применяется к IP-сетям для обнаружения состояния канала. BFD поддерживает обнаружение состояния канала в пределах нескольких миллисекунд и не зависит от типа интерфейса.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Существующие механизмы обнаружения неисправностей включают:
  - Обнаружение на уровне аппаратных средств. Например, аварийные сигналы SDH используются для обнаружения ошибок в каналах. Аппаратные средства могут быстро обнаруживать неисправность; однако не все носители могут обеспечить такой механизм обнаружения.
  - Механизм Hello-пакетов. Как правило, это механизм приветствия, который предлагает протокол маршрутизации. Механизм Hello-пакетов может обнаруживать неисправность за несколько секунд. При высокоскоростной передаче данных (например, при гигабитных скоростях) время обнаружения более одной секунды приводит к потере большого объема данных. Для услуг, чувствительных к времени задержки, например голосовых услуг, задержка более одной секунды неприемлема. Кроме того, этот механизм основывается на протоколах маршрутизации. Как правило, IS-IS использует пакеты IIH для обнаружения соседей и неисправностей. Это занимает несколько секунд.
  - Другие механизмы обнаружения. Другие механизмы обнаружения могут предоставляться различными протоколами или поставщиками устройств. Если в сети есть устройства от нескольких поставщиков, эти механизмы обнаружения, такие как BFD, трудно реализовать.



- Когда истекает время на умном таймере для создания LSP-пакета, система создает новый LSP-пакет в соответствии с текущей топологией. В исходном механизме реализации на таймере задан интервал, который, однако это не отвечает требованиям быстрой сходимости и низкого уровня использования ЦП.
- Поэтому при создании LSP-пакета используется умный таймер для ускорения сходимости сети и поддержания производительности системы. Так задержка может быть автоматически скорректирована на основании частоты изменения маршрутной информации. Таймер может быстро реагировать на чрезвычайные ситуации (например, при изменении статуса интерфейса на Up или Down), в результате ускоряя сходимость сети. Кроме того, при частом изменении топологии сети интервал, заданный на умном таймере, автоматически

увеличивается, за счет чего снижается потребление ресурсов ЦП.

Ускорение распространения LSP-пакетов



Быстрое распространение LSP-пакетов

- Согласно протоколам RFC, когда маршрутизатор получает LSP-пакет, созданный позднее LSP-пакета, хранящегося в локальной базе данных состояния каналов (LSDB), он обновляет локальную базу LSDB и периодически распространяет выполняется медленно.
- Механизм быстрого распространения LSP-пакетов является усовершенствованной версией вышеуказанного механизма. Когда маршрутизатор, сконфигурированный с этой функцией, получает один или несколько новых LSP-пакетов, он распространяет LSP-пакеты в меньшем количестве, чем указанное, перед расчетом маршрута для ускорения синхронизации LSDB. Этот механизм значительно ускоряет сходимость сети.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Вы можете задать количество LSP-пакетов для каждого этапа распространения. Это количество будет действительно для всех интерфейсов. Если количество отправляемых LSP-пакетов больше указанного, будут отправляться *lsp-count* LSP. Если таймер настроен и он не истекает до расчета маршрута, LSP-пакеты будут распространяться сразу при получении. В противном случае LSP-пакеты будут распространяться при истечении таймера.
- Если в команде не указан уровень, функция будет включена для уровней 1 и 2.

Ускорение расчета кратчайшего пути (SPF)



Умный таймер SPF

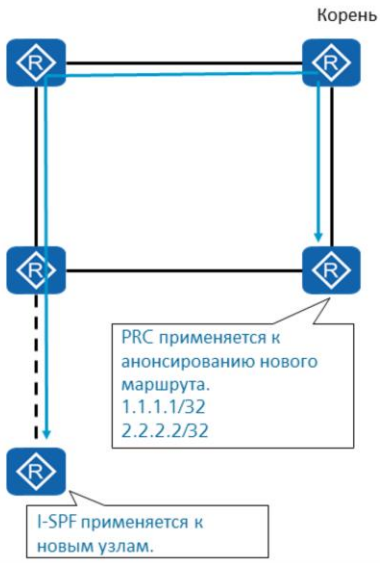
- Хотя алгоритм расчета маршрута улучшен, на скорость сходимости влияет долгое время инициирования расчета маршрута. Таймер с интервалом в пределах миллисекунд поможет сократить этот интервал. Однако при частых изменениях в сети будут чрезмерно расходоваться ресурсы ЦП.
- Умный таймер SPF решает обе эти проблемы.
- Если топология сети часто меняется, умный таймер увеличивает интервал расчета маршрута, чтобы предотвратить слишком большое потребление ресурсов ЦП.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Как правило, сеть IS-IS работает стабильно. Вероятность возникновения большого количества изменений в сети очень мала, и маршрутизатор IS-IS не часто вычисляет маршруты. Период инициирования расчета маршрута очень короткий (в пределах миллисекунд). Если топология сети очень часто меняется, умный таймер увеличивает интервал времени расчета, чтобы предотвратить слишком большое потребление ресурсов ЦП.

Настройка метода расчета SPF



- Incremental SPF (I-SPF) вычисляет только измененные маршруты, а не все маршруты.
- При первом расчете I-SPF вычисляет маршруты на всех узлах. После этого он рассчитывает только маршруты на затронутых ошибкой узлах.

- Аналогично I-SPF, в PRC рассматриваются только измененные части сети. Однако PRC не вычисляет кратчайший путь, а обновляет конечные (leaf) маршруты на основе SPT, рассчитанного I-SPF.

- Изменение широковещательной сети на сеть «точка-точка» уменьшает количество псевдоузлов в сети и сокращает время расчета SPF.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Согласно ISO-10589 для расчета маршрутов используется алгоритм Дейкстры. Когда в сети изменяется узел, перерасчет всех маршрутов выполняется с помощью этого алгоритма. Расчет занимает длительное время и потребляет слишком много ресурсов ЦП, что влияет на скорость сходимости.
- I-SPF улучшает этот алгоритм. За исключением первого раза, в расчетах учитываются только измененные узлы. SPT, генерируемый в конце, совпадает с SPT, сгенерированным алгоритмом Дейкстры. За счет этого снижается использование ЦП и ускоряется сходимость сети.
- При расчете маршрута маршрут представляет собой лист (leaf), а маршрутизатор – узел. Если SPT изменится после расчета I-SPF, PRC обрабатывает все листья только на измененном узле. Если SPT остается неизменным, PRC обрабатывает только измененные листья.
- Например, если протокол IS-IS включен на интерфейсе узла, SPT, рассчитанный I-SPF, остается без изменений. PRC обновляет только маршруты этого интерфейса, потребляя меньше ресурсов ЦП.
- PRC совместно с I-SPF повышает сходимость сети. Это алгоритм заменил исходный алгоритм SPF.
- По умолчанию маршрутизаторы Huawei используют I-SPF и PRC для расчета маршрутов, и для этого не требуется выполнять конфигурации с помощью

команд.

Конфигурация быстрой сходимости IS-IS

- R1 и R2 взаимосвязаны, и они взаимодействуют друг с другом через IS-IS. Необходимо повысить скорость сходимости двух маршрутизаторов через BFD.




```
isis 1
is-level level-2
timer lsp-generation 1 1 120 level-2
flash-flood level-2
network-entity 10.0000.0000.0001.00
timer spf 1 20 100
#
bfd
bfd atob bind peer-ip 10.1.1.2 interface GigabitEthernet1/0/1
 discriminator local 1
discriminator remote 2
Commit
#
interface GigabitEthernet1/0/1
isis bfd static
```

```
isis 1
is-level level-2
timer lsp-generation 1 1 120 level-2
flash-flood level-2
network-entity 10.0000.0000.0002.00
timer spf 1 20 100
#
bfd
bfd atob bind peer-ip 10.1.1.1 interface GigabitEthernet1/0/1
 discriminator local 2
discriminator remote 1
Commit
#
interface GigabitEthernet1/0/1
isis bfd static
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Содержание

1. **Расширенные функции IS-IS**
   - Быстрая сходимость IS-IS
   - Административный тег IS-IS
   - Фрагментация LSP в протоколе IS-IS
   - Фильтрация маршрутов IS-IS
2. Основные принципы и конфигурации IPv6 IS-IS
3. Примеры применения IS-IS к двойному стеку

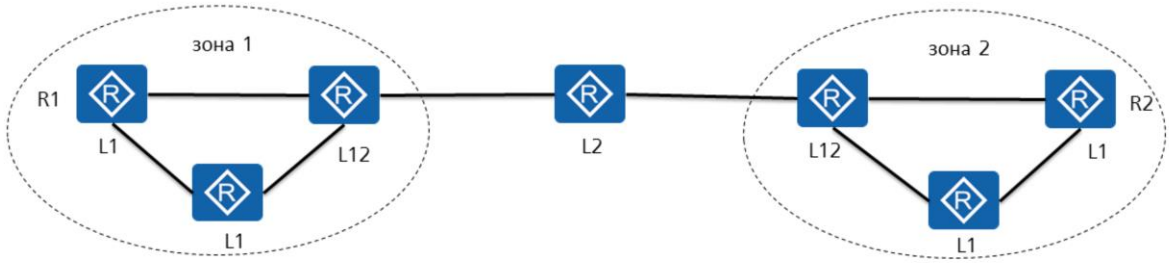
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Основные функции

- С помощью административных тегов вы можете контролировать анонсирование IP-префиксов в домене маршрутизации IS-IS для упрощения управления маршрутами. Вы можете использовать административные теги для управления импортом маршрутов различных уровней и зон и управления множественными экземплярами IS-IS на одном маршрутизаторе.
- Значение административного тега связано с определенными атрибутами. Когда значение параметра cost-style указано как wide, wide-compatible или compatible и IS-IS анонсирует префикс IP-адреса с этими атрибутами, IS-IS добавляет административный тег к TLV в префиксе. Тег распространяется вместе с префиксом во всем домене маршрутизации.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

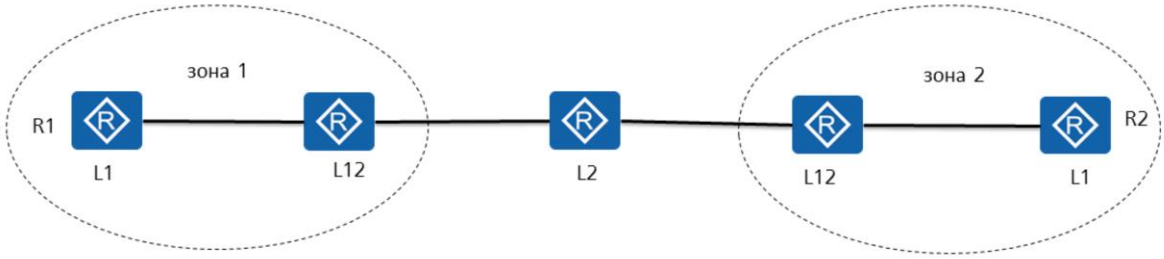
Принцип работы (1)



- R1 должен взаимодействовать с R2 в зоне 2. Однако для обеспечения информационной безопасности маршрутизаторы в зоне 2 не могут получать пакеты, отправленные R1. Сначала вы можете настроить один административный тег для интерфейсов IS-IS на R1 и R2. Затем маршрутизатор уровня 1-2 зоны 1 выдает только маршруты, соответствующие сконфигурированному административному тегу от зон от Уровня-2 до Уровня-1. Таким образом, среди всех маршрутизаторов в области 2 R1 взаимодействует только с R2.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Принцип работы (2)



- После применения административного тега R1 в зоне 1 сможет взаимодействовать только с R2 в зоне 2.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Содержание

1. **Расширенные функции IS-IS**
   - Быстрая сходимость IS-IS
   - Административный тег IS-IS
   - Фрагментация LSP в протоколе IS-IS
   - Фильтрация маршрутов IS-IS
2. Основные принципы и конфигурации IPv6 IS-IS
3. Примеры применения IS-IS к двойному стеку

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Основные термины

- Исходная система: маршрутизатор с протоколом IS-IS. Один процесс IS-IS может функционировать как несколько виртуальных маршрутизаторов для анонсирования LSP, а исходная система относится к процессу IS-IS.
- Идентификатор нормальной системы: идентификатор исходной системы.
- Виртуальная система: система, которую определяет дополнительный системный идентификатор для создания расширенных фрагментов LSP. Эти фрагменты несут дополнительные идентификаторы системы в своих идентификаторах LSP.
- Дополнительный системный идентификатор (ID): назначается администраторами сети для идентификации виртуальной системы. Для каждого дополнительного идентификатора системы можно создать не более 256 расширенных фрагментов LSP.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Принципы работы

- В IS-IS каждый системный ID идентифицирует систему, которая может создавать не более 256 фрагментов LSP. При наличии дополнительных системных ID (можно создать до 50 виртуальных систем) процесс IS-IS может создавать не более 13 056 фрагментов LSP.
- После настройки расширения фрагмента LSP система запрашивает перезапуск процесса IS-IS, если информация потеряна из-за превышения максимального количества LSP. После перезапуска исходная система загружает как можно больше информации маршрутизации в LSP, добавляет перегруженную информацию в LSP виртуальной системы для передачи и использует TLV 24 для уведомления других маршрутизаторов о своей связи с виртуальной системой.

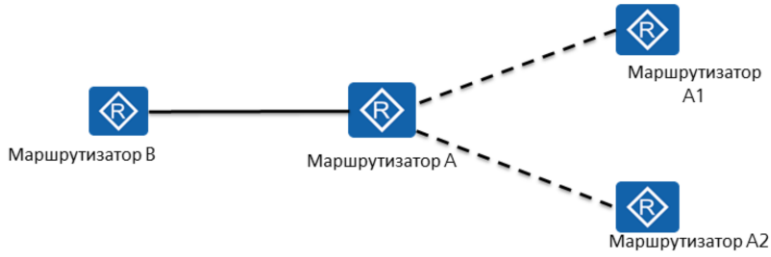
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Когда маршрутизатору IS-IS необходимо анонсировать LSP, содержащие много информации, он создает несколько фрагментов LSP для передачи большего объема информации IS-IS.
- Фрагменты IS-IS LSP идентифицируются по полю LSP Number в их идентификаторах LSP. Это поле состоит из 1 байта. Процесс IS-IS может создавать максимум 256 фрагментов LSP, поэтому передаче подлежит ограниченное количество маршрутов. Согласно RFC 3786 можно сконфигурировать ID виртуальных систем, и для IS-IS можно создать виртуальные LSP, несущие маршрутную информацию.

Режимы работы

- Маршрутизатор IS-IS может выполнять расширение фрагмента LSP в двух режимах.



Режим	Сценарий применения
Режим 1	Некоторые маршрутизаторы в сети не поддерживают расширение фрагмента LSP.
Режим 2	Все маршрутизаторы в сети поддерживают расширение фрагмента LSP.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Режим 1 используется, когда некоторые маршрутизаторы в сети не поддерживают расширение фрагмента LSP.
- В Режиме 1 виртуальные системы участвуют в расчете SPF. Исходная система анонсирует LSP, содержащие информацию о каналах к каждой виртуальной системе. Аналогичным образом, каждая виртуальная система анонсирует LSP, содержащие информацию о каналах к исходной системе. Виртуальные системы выглядят как физические маршрутизаторы, подключающиеся к исходной системе. Режим 1 – это переходный режим для более ранних версий, не поддерживающих расширение фрагмента LSP. В предыдущих версиях IS-IS не может идентифицировать IS Alias ID TLV и обрабатывает полученный LSP, анонсированный виртуальной системой как LSP, анонсированный процессом IS-IS.
- Режим 2 используется, когда все маршрутизаторы в сети поддерживают расширение фрагмента LSP.
- В Режиме 2 виртуальные системы не участвуют в расчете SPF. Все маршрутизаторы в сети знают, что LSP, создаваемые виртуальными системами, фактически принадлежат исходной системе. Маршрутизатор IS-IS, работающий в Режиме 2, может идентифицировать IS Alias ID TLV, который используется в качестве для справки при расчете SPT и маршрутов.
- Примечание: Когда исходная система и виртуальная система отправляют LSP с номером фрагмента 0, LSP должны содержать IS Alias ID TLV для указания исходной системы независимо от режима работы (1 или 2).

Содержание

1. **Расширенные функции IS-IS**
   - Быстрая сходимость IS-IS
   - Административный тег IS-IS
   - Фрагментация LSP в протоколе IS-IS
   - Фильтрация маршрутов IS-IS
2. Основные принципы и конфигурации IPv6 IS-IS
3. Примеры применения IS-IS к двойному стеку

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Фильтрация протоколом IS-IS маршрутов, рассчитанных на основе базы данных LSDB (1)

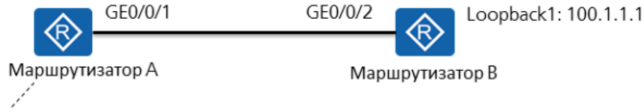
- Настроив в протоколе IS-IS фильтрацию маршрутов, рассчитанных на основе базы данных LSDB, вы сможете контролировать количество маршрутов IS-IS, которые будут добавлены в таблицу IP-маршрутизации, и уменьшить размер такой таблицы.
- Настройка правила ACL:
- **acl** { **name** *basic-acl-name* { **basic** | [**basic**] **number** *basic-acl-number* } | [**number**] *basic-acl-number* } [**match-order** { **config** | **auto** }]

  rule [*rule-id*] [**name** *rule-name*] { **deny** | **permit** } [**fragment-type** { **fragment** | **non-fragment** | **non-subseq** | **fragment-subseq** | **fragment-spe-first** } | **source** { *source-ip-address* { *source-wildcard* | **0** | *src-netmask* } | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*]
- Настройка фильтра:
- **filter-policy** { *acl-number* | **acl-name** *acl-name* } **import**

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Фильтрация протоколом IS-IS маршрутов, рассчитанных на основе базы данных LSDB (2)

- Маршрутизатор A и Маршрутизатор B устанавливают отношения соседства IS-IS. Маршрутизатор A может узнать маршрут к loopback1 Маршрутизатора B через IS-IS.



- До фильтрации:

```
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

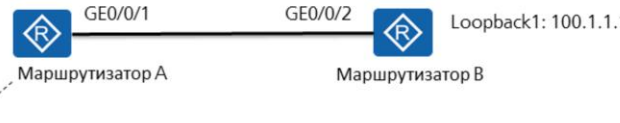
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
       10.1.1.0/30  Direct  0    0           D   10.1.1.1        GigabitEthernet0/0/1
       10.1.1.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
       10.1.1.3/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
     100.1.1.1/32   ISIS-L2 15   10          D   10.1.1.2        GigabitEthernet0/0/1
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Фильтрация протоколом IS-IS маршрутов, рассчитанных на основе базы данных LSDB (3)

- Маршрутизатор A и Маршрутизатор B устанавливают отношения соседства IS-IS. Для протокола IS-IS применяется политика управления трафиком, чтобы таблица маршрутизации маршрутизатора A не содержала маршрута к loopback1 маршрутизатора B, но маршрут к loopback1 маршрутизатора B существовал в базе данных IS-IS LSDB маршрутизатора A.



- Настройка политики фильтрации.

```
#
 acl name huawei 2000
  rule 5 deny source 100.1.1.1 0
 #
 isis 1
 is-level level-2
 network-entity 01.0000.0000.0001.00
 Filter-policy acl-name huawei import
 #
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Фильтрация протоколом IS-IS маршрутов, рассчитанных на основе базы данных LSDB (4)

- После конфигурирования политики фильтрации таблица маршрутизации Маршрутизатора A не содержит маршрута к loopback1 Маршрутизатора B, но маршрут к loopback1 Маршрутизатора B существует в базе данных IS-IS LSDB маршрутизатора A.



- Посмотрите таблицу маршрутизации.

```
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
       10.1.1.0/30  Direct  0    0           D   10.1.1.1        GigabitEthernet0/0/1
       10.1.1.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
       10.1.1.3/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Примечание:
- Префикс отфильтрованного маршрута по-прежнему существует в IS-IS LSDB LSP.

Фильтрация импортированных маршрутов протоколом IS-IS (1)

- Можно настроить в IS-IS фильтрацию импортируемых внешних маршрутов, чтобы контролировать количество маршрутов IS-IS в сети.
- Сконфигурируйте список IP-префиксов.
- **ip ip-prefix** *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *ip-address mask-length* [**greater-equal** *greater-equal-value*] [**less-equal** *less-equal-value*]
- Настройте политику маршрутизации:
- **route-policy** *route-policy-name* { **permit** | **deny** } **node**

  if-match acl { *acl-number* | *acl-name* }

  if-match ip-prefix *ip-prefix-name*

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Фильтрация импортированных маршрутов протоколом IS-IS (2)

- Маршрутизатор A и Маршрутизатор B устанавливают отношения соседства IS-IS. Маршрутизатор B может импортировать прямой маршрут к loopback1 в свою базу данных IS-IS LSDB и анонсировать маршрут на Маршрутизатору A.



- До фильтрации:

Route Flags: R - relay, D - download to fib

Routing Tables: Public
Destinations : 9 Routes : 9

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
1.1.1.1/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.1.1.0/30	Direct	0	0	D	10.1.1.1	GigabitEthernet0/0/1
10.1.1.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.1.1.3/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
100.1.1.1/32	ISIS-L2	15	10	D	10.1.1.2	GigabitEthernet0/0/1

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Фильтрация импортированных маршрутов протоколом IS-IS (3)

- Маршрутизатор A и Маршрутизатор B устанавливают отношения соседства IS-IS. Когда маршрутизатор B импортирует прямой маршрут к loopback1 в свою базу данных IS-IS LSDB, вступает в силу политика фильтрации импортируемых маршрутов.



- Настройте политику фильтрации.

```
#
 ip ip-prefix huawei index 10 deny 100.1.1.1 32
 #
 route-policy huawei deny node 10
 if-match ip-prefix huawei
 #
 isis 1
 is-level level-2
 network-entity 01.0000.0000.0002.00
 import-route direct route-policy huawei
 #
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Фильтрация импортированных маршрутов протоколом IS-IS (4)

- После настройки политики фильтрации прямой маршрут к loopback1 Маршрутизатора B не импортируется в базу данных IS-IS LSDB Маршрутизатора B. Поэтому Маршрутизатор A не узнает маршрут к loopback1 Маршрутизатора B.



- Посмотрите таблицу маршрутизации.

```
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
       10.1.1.0/30  Direct  0    0           D   10.1.1.1        GigabitEthernet0/0/1
       10.1.1.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
       10.1.1.3/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Фильтрация внешних маршрутов протоколом IS-IS при анонсировании (1)

- IS-IS фильтрует импортированные внешние маршруты при их анонсировании.
- Сконфигурируйте политику фильтрации для внешних маршрутов, подлежащих анонсированию.
- **filter-policy** { *acl-number* | **acl-name** | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*]]

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Фильтрация внешних маршрутов протоколом IS-IS при анонсировании (2)

- Маршрутизатор A и Маршрутизатор B устанавливают отношения соседства IS-IS. Маршрутизатор B может импортировать прямой маршрут к loopback1 в свою базу данных IS-IS LSDB и анонсировать маршрут к Маршрутизатору A. Маршрутизатор A узнает маршрут к loopback1 маршрутизатора B.



- До фильтрации:

Route Flags: R - relay, D - download to fib

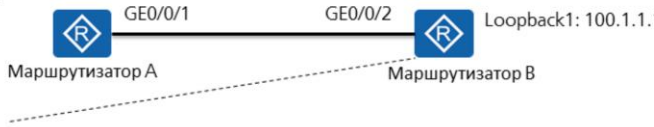
Routing Tables: Public
Destinations : 9 Routes : 9

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
1.1.1.1/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.1.1.0/30	Direct	0	0	D	10.1.1.1	GigabitEthernet0/0/1
10.1.1.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.1.1.3/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
100.1.1.1/32	ISIS-L2	15	10	D	10.1.1.2	GigabitEthernet0/0/1

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Фильтрация внешних маршрутов протоколом IS-IS при анонсировании (3)

- Маршрутизатор A и Маршрутизатор B устанавливают отношения соседства IS-IS. Прямой маршрут к loopback1 Маршрутизатора B импортируется в базу данных IS-IS LSDB Маршрутизатора B. Когда маршрутизатор B анонсирует LSP Маршрутизатору A, вступает в силу политика, фильтрующая маршрут к loopback1 маршрутизатора B.



- Настройте политику фильтрации.

```
#
 ip ip-prefix huawei index 10 deny 100.1.1.1 32
 #
 isis 1
 is-level level-2
 network-entity 01.0000.0000.0002.00
 import-route direct
 filter-policy acl-name huawei export
 #
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Фильтрация внешних маршрутов протоколом IS-IS при анонсировании (4)

- После настройки политики фильтрации база данных IS-IS LSDB Маршрутизатора A не содержит маршрута к loopback1 маршрутизатора B. В результате Маршрутизатор A не узнает маршрут к loopback1 маршрутизатора B.



- Посмотрите таблицу маршрутизации.

```
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
       10.1.1.0/30  Direct  0    0           D   10.1.1.1        GigabitEthernet0/0/1
       10.1.1.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
       10.1.1.3/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
```

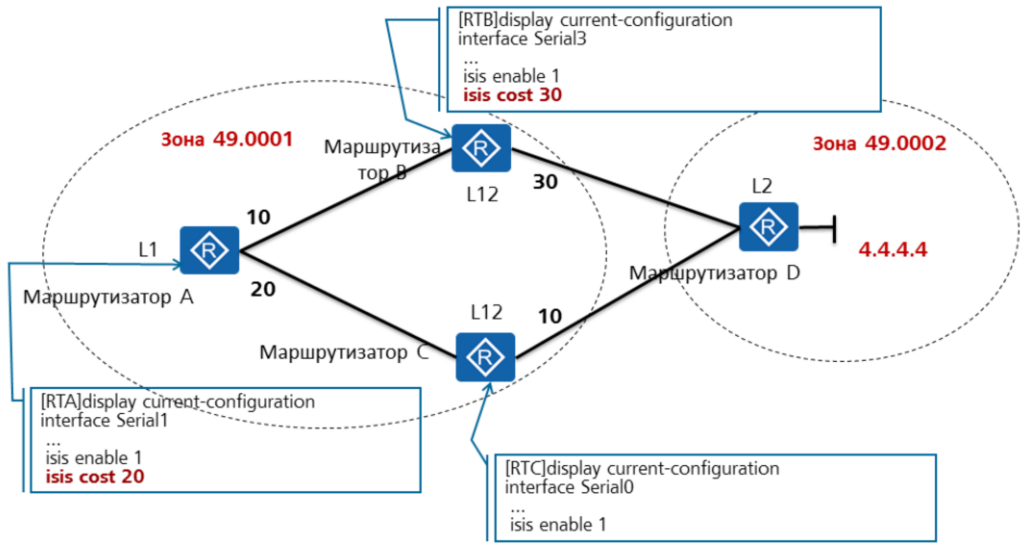
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Содержание

1. **Расширенные функции IS-IS**
   - Быстрая сходимость IS-IS
   - Административный тег IS-IS
   - Фрагментация LSP в протоколе IS-IS
   - Фильтрация маршрутов IS-IS
   - Утечка маршрутов IS-IS
2. Основные принципы и конфигурации IPv6 IS-IS
3. Примеры применения IS-IS к двойному стеку

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

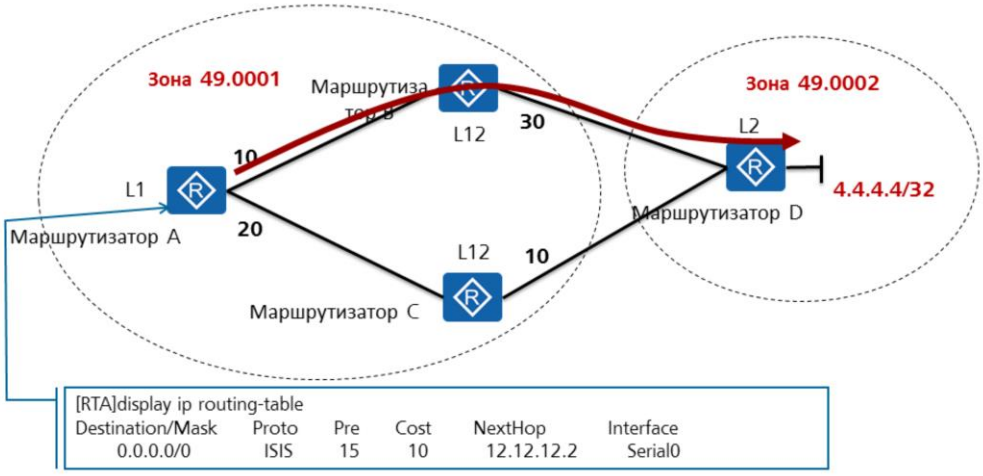
Утечка маршрутов IS-IS (1)



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Введение:
  - Информация маршрутизации зоны Уровня-1 анонсируется зоне Уровня-2 через маршрутизатор Уровня-1-2. Таким образом, маршрутизаторы Уровня-1-2 и Уровня-2 знают маршрутную информацию всего домена IS-IS. Маршрутизатор Уровня-2 по умолчанию не информирует зону Уровня-1 об извлеченной информации маршрутизации других областей Уровня-1 и магистральной области. Поэтому маршрутизаторы Уровня-1 не знают маршрутную информацию за пределами своей зоны. В результате маршрутизаторы Уровня-1 не могут выбрать оптимальные маршруты к месту назначения вне своей зоны.
- Утечка маршрутов IS-IS может решить эту проблему.

Утечка маршрутов IS-IS (2)

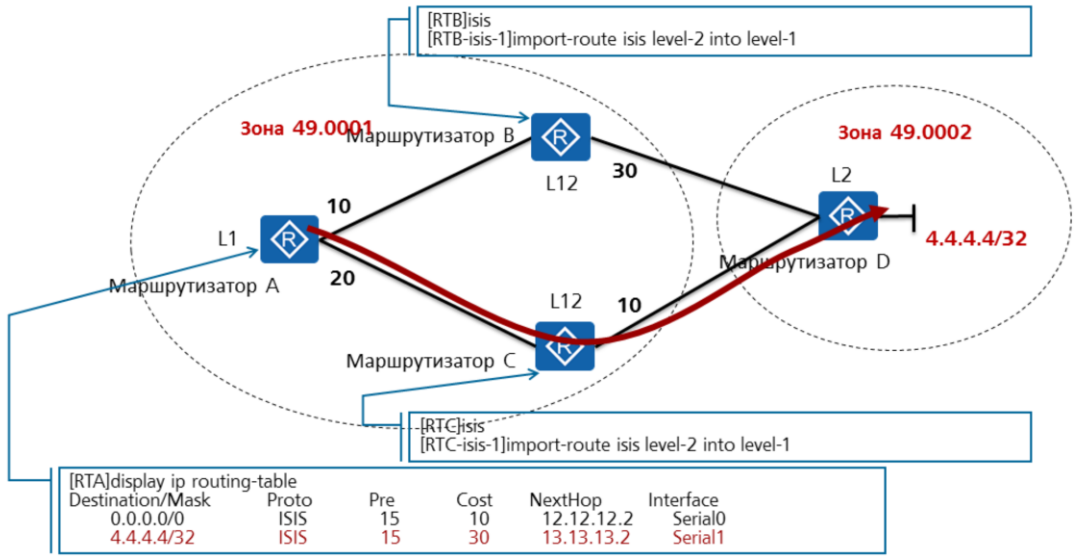


[RTA]display ip routing-table

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/0	ISIS	15	10	12.12.12.2	Serial0

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Утечка маршрутов IS-IS (3)



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- При получении двух идентичных маршрутов маршрутизатор Уровня-1 предпочитает маршрут из локальной зоны, а не из зоны Уровня-2, даже если стоимость маршрута Уровня-2 меньше.

Содержание

1. Расширенные функции IS-IS
2. **Основные принципы и конфигурации IPv6 IS-IS**
   - Расширение протокола IS-IS
   - Маршрутизация по одной или множеству топологий в протоколе IS-IS
   - Конфигурация IPv6 IS-IS
3. Примеры применения IS-IS к двойному стеку

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Содержание

1. Расширенные функции IS-IS
2. **Основные принципы и конфигурации IPv6 IS-IS**
   - Расширение протокола IS-IS
   - Маршрутизация по одной или множеству топологий в протоколе IS-IS
   - Конфигурация IPv6 IS-IS
3. Примеры применения IS-IS к двойному стеку

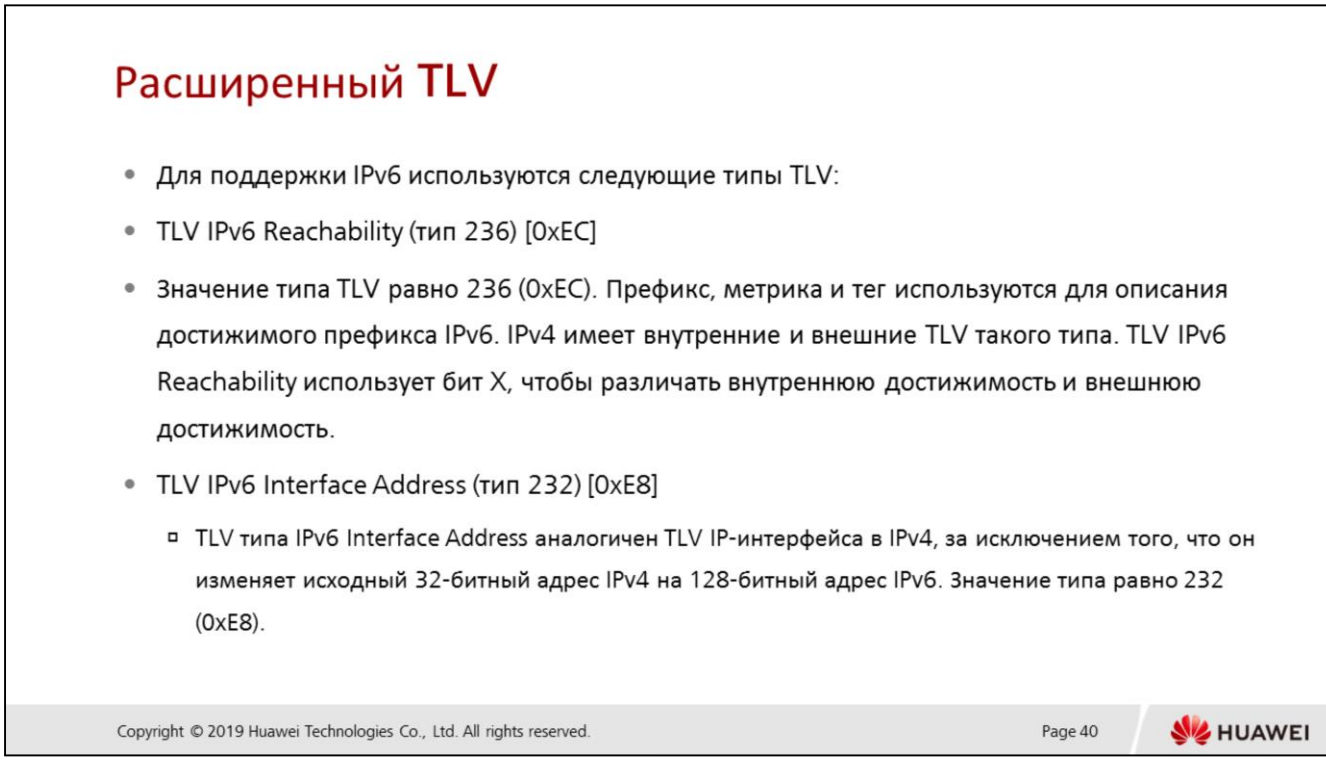
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Общая информация о протоколе IS-IS

- IS-IS – это протокол IGP.
- Протокол IS-IS использует алгоритм SPF для расчета маршрутов.
- Архитектура IS-IS строится на базе кодировки TLV, благодаря чему обеспечивается высокая масштабируемость.
  - Для поддержки новых протоколов и функций вам нужно только расширить формат TLV с помощью новых TLV или под-TLV.
  - Структура может быть легко расширена для поддержки IPv6, TE, MT и других протоколов и функций.
  - В IS-IS не нужно много менять для поддержки IPv6. Поэтому такие сети обладают высокой наследуемостью. Для поддержки IPv6 требуется разработка OSPFv3, если используется протокол OSPF.

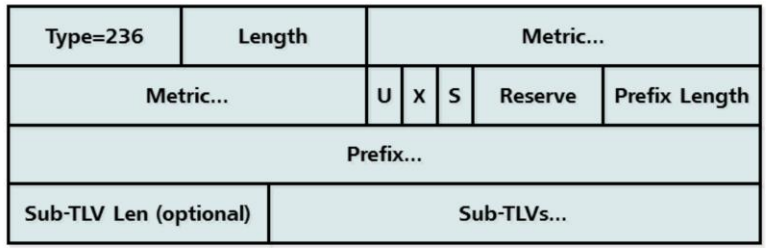
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI



- Описание расширенного протокола IS-IS для IPv6 приведено в проекте *draft-ietf-isis-ipv6-05* Инженерного совета интернета (IETF). Проект представляет два TLV и идентификатора протокола сетевого уровня (NLPID) расширенного протокола IS-IS для поддержки IPv6.
- Эти два TLV включают:
  - TLV IPv6 reachability. Значение типа TLV равно 236 (0xEC). Префикс, метрика и тег используются для описания достижимого префикса IPv6. IPv4 имеет внутренние и внешние TLV такого типа. TLV IPv6 Reachability использует бит X, чтобы различать внутреннюю и внешнюю достижимость.
  - TLV IPv6 Interface Address. TLV типа IPv6 Interface Address аналогичен TLV IP-интерфейса в IPv4, за исключением того, что он изменяет исходный 32-битный адрес IPv4 на 128-битный адрес IPv6. Значение типа равно 232 (0xE8).

TLV IPv6 Reachability



- U: этот бит указывает, анонсируется ли префикс с высокого уровня (используется для предотвращения петель).
- X: этот бит указывает, импортируется ли префикс из других протоколов маршрутизации.
- S: флаг суб-TLV (опционально)

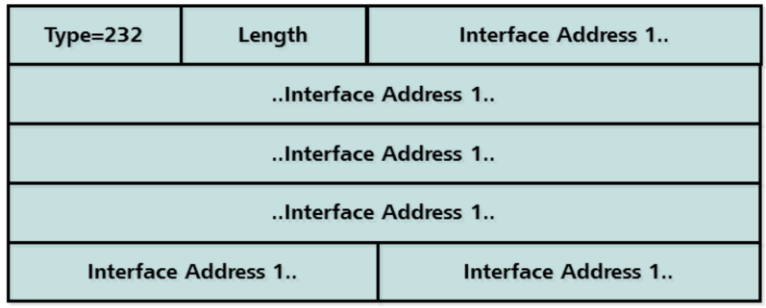
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Эта структура данных может повторяться множество раз (при наличии множества префиксов маршрутов).
- Поле Metric было изменено, и поле MAX_PATH_METRIC (1023) изменено на MAX_V6_PATH_METRIC (0xFE000000). Если значение поля Metric префикса больше значения MAX_V6_PATH_METRIC, оно не используется для построения таблицы маршрутизации, а используется в особых целях.
- TLV128: информация о внутренней доступности IP-сети. TLV130: информация о внешней доступности IP-сети. В TLV236 бит X используется для разграничения между внешней и внутренней достижимостью.

TLV IPv6 Interface Address (1)

- **TLV** IPv6 Interface Address (тип 232) [0xE8]
  - TLV 232 аналогичен TLV 132.
  - Длина адреса каждого интерфейса изменена на 128 бит.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Примечание. В пакетах Hello TLV адреса интерфейса содержит только локальный адрес интерфейса, отправляющего пакеты Hello. Для LSP TLV адреса интерфейса содержит только нелокальный адрес интерфейса IPv6 в IS.

TLV IPv6 Interface Address (2)

- Структура этого TLV взята у TLV132. Поскольку TLV132 поддерживает не более 64 IP-адресов (32 бита), TLV232 поддерживает до 16 адресов IPv6 (128 бит).
- Содержимое поля отличается в разных блоках данных протокола (PDU). В Hello PDU, TLV адреса интерфейса может содержать только локальный адрес интерфейса, отправляющего пакет Hello. Для LSP TLV адреса интерфейса может содержать только нелокальный адрес интерфейса IPv6 в IS.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

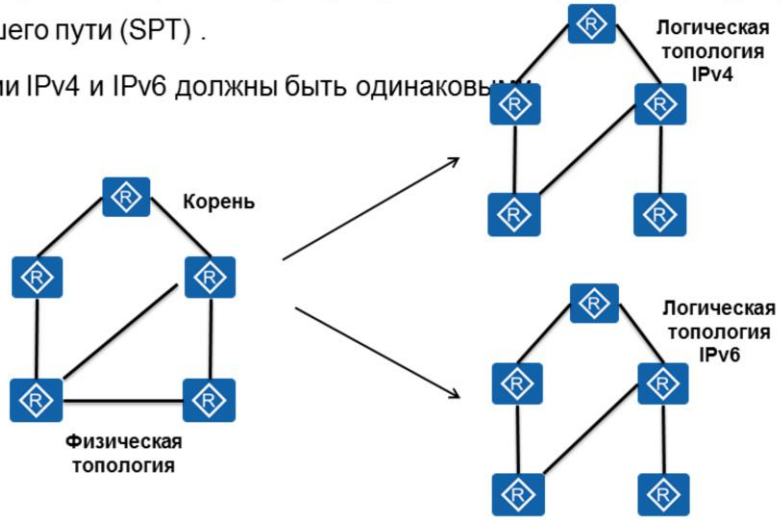
Содержание

1. Расширенные функции IS-IS
2. **Основные принципы и конфигурации IPv6 IS-IS**
   - Расширение протокола IS-IS
   - Маршрутизация по одной или множеству топологий в протоколе IS-IS
   - Конфигурация IPv6 IS-IS
3. Примеры применения IS-IS к двойному стеку

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

IS-IS с одной топологией (ST)

- Для всех протоколов, использующих протокол IS-IS, создается одно дерево кратчайшего пути (SPT) .
- Топологии IPv4 и IPv6 должны быть одинаковыми.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Недостатки применения одной топологии

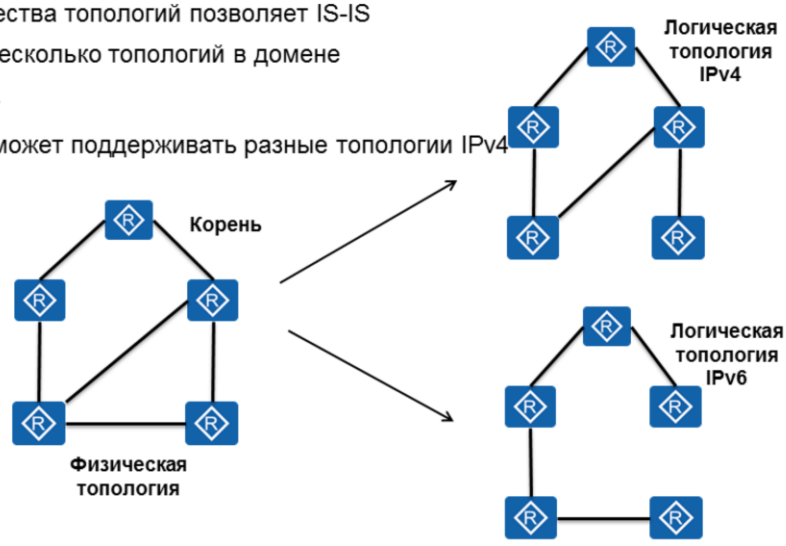
- AS-IS
  - Поскольку требования к надежности сетей растут, операторы хотят иметь обслуживающую сеть с независимой топологией, т.е. сеть внутриполостного техобслуживания.
  - IS-IS имеет одно дерево SPT для всех протоколов, поэтому топологии IPv4 и IPv6 должны быть одинаковыми.
- Недостатки
  - Использование одной топологии невозможно в отношении сети с множеством топологий.
  - Для поддержания одной топологии на всех интерфейсах должны одновременно работать протоколы IS-IS IPv4 и IS-IS IPv6, что лишает сеть гибкости.
  - Зоны IPv6 нельзя подключить через зону IPv4, поскольку трафик IPv6 будет отброшен в зоне IPv4.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

IS-IS с множеством топологий (MT)

- Создание множества топологий позволяет IS-IS поддерживать несколько топологий в домене маршрутизации.
- Протокол IS-IS может поддерживать разные топологии IPv4 и IPv6.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

MT: разделения топологий

- Протокол IS-IS включает следующие процессы:
  - Установление отношений соседства
  - Анонсирование доступных маршрутов (Prefix Reachable) и доступных маршрутизаторов (IS Reachable)
  - Расчет SPF и маршрута
- Для изоляции нескольких топологий параметр в вышеуказанных процессах должен передаваться параметр MT (расчет SPF и маршрута должны выполняться на маршрутизаторе).
- В проекте *draft-ietf-isis-wg-multi-topology-11* приводится четыре новых TLV для реализации взаимодействия IS-IS MT в общей среде.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Добавлено четыре TLV:
  - TLV 229 – Multi-Topology Identifier
  - TLV 222 – Multi-Topologies Intermediate System
  - TLV 235 – Multi-Topologies Reachable IPv4 Prefixes
  - TLV 237 – Multi-Topologies Reachable IPv6 Prefixes
- Зарезервированные значения MT ID

Содержание

1. Расширенные функции IS-IS
2. **Основные принципы и конфигурации IPv6 IS-IS**
   - Расширение протокола IS-IS
   - Маршрутизация по одной или множеству топологий в протоколе IS-IS
   - Конфигурация IPv6 IS-IS
3. Примеры применения IS-IS к двойному стеку

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Конфигурация IPv6 IS-IS

- Включите протокол IS-IS MT.

```
[Huawei-isis-1]ipv6  enable topology ipv6
```

- Включите протокол IS-IS на интерфейсе.

```
[Huawei-GigabitEthernetX/Y/Z]isis ipv6 enable
```

- Проверьте отношения соседства IS-IS.

```
[Huawei]dis isis peer
```

- Проверьте информацию маршрутизации IS-IS.

```
[Huawei]dis isis route
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Содержание

1. Расширенные функции IS-IS
2. Основные принципы и конфигурации IPv6 IS-IS
3. **Примеры применения IS-IS к двойному стеку**

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Планирование сети IS-IS (1)

- **Планирование заголовка сетевого объекта (NET)**
- NET имеет формат AA.BBBB.CCCC.DDDD.SSSS.SSSS.SSSS.00.
  - ID зоны = AA.BBBB.CCCC.DDDD
    - AA: идентификатор полномочий и формата (AFI). Значение равно 49.
    - BBBB: код страны. Например, код Китая – 0086.
    - CCCC: код провинции. Например, код провинции Ляонин – 0003.
    - DDDD: код объекта, на котором находятся устройства. Например, код для объекта Dalian в провинции Ляонин – 3821.
  - ID системы = SSSS.SSSS.SSSS
    - ID системы извлекается из адреса loopback 0.
  - Адрес NSEL закрепляется как 00.
- **Планирование на основе уровней и регионов**
  - Режим Уровня-2 (предпочтительно): все маршрутизаторы IS-IS расположены в магистральной сети.
  - Режим Уровня-1: все маршрутизаторы IS-IS расположены в одной области.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Планирование сети IS-IS (2)

- **Планирование стоимости**
- Гибкое планирование стоимости для IS-IS
  - Стоимость может формироваться на основе полосы пропускания канала.
  - Структура стоимости определяет направление сетевого трафика.
  - Перед планированием стоимости необходимо четко определить направления сетевого трафика в различных сценариях сквозной маршрутизации.
- Протокол IS-IS поддерживает три метода настройки стоимости канала:
  - Установка значения стоимости канала в режиме интерфейса
  - Установка значения стоимости для всех интерфейсов в экземпляре IS-IS в системном режиме
  - Автоматический расчет стоимости канала на основе полосы пропускания канала в системном режиме

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Планирование сети IS-IS (3)

- **Планирование обеспечения надежности**
- Быстрая сходимость IS-IS
  - BFD для IS-IS обеспечивает быстрое обнаружение ошибок каналов.
  - I-SPF ускоряет сходимость (поддерживается по умолчанию).
  - Частичный расчет маршрута (PRC) ускоряет сходимость (поддерживается по умолчанию).
  - Быстрая лавинная передача LSP ускоряет синхронизацию базы данных LSDB.
  - Умный таймер: Ускоряет конвергенцию маршрутов и повышает стабильность сети.

Параметр таймера	**Заданное значение**
Интервал приветствия	Значение по умолчанию
Мертвый интервал	Значение по умолчанию
BFD для IS-IS	Значение по умолчанию
Быстрая лавинная передача	Значение по умолчанию
Timer spf { max | init | increment }	1 50 100
Timer lsp-generation { max | init | increment }	2 50 100

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Рекомендуется использовать все возможности для обеспечения быстрой сходимости IS-IS.

Планирование сети IS-IS (4)

- **Обеспечение безопасности**
  - Протокол IS-IS поддерживает три режима аутентификации: аутентификация интерфейса, аутентификация зон и аутентификация домена
  - Три режима аутентификации поддерживают как простую аутентификацию с помощью пароля, так и аутентификацию MD5. Рекомендуется использовать аутентификацию MD5, поскольку она обеспечивает более высокий уровень безопасности.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Рекомендуется использовать все возможности для обеспечения быстрой сходимости IS-IS.

Планирование сети IS-IS (5)

- **Конфигурирование рабочей сети**

```
isis 1
 is-level level-2
 cost-style wide
 circuit-cost 100000 level-2
 network-entity 86.4680.0551.0611.3313.7003.00
 is-name city-equipment room-device name-network
type.device type
 preference 155
 log-peer-change
 maximum load-balancing 16
 timer lsp-max-age 65500
 timer lsp-refresh 32768
 #
 ipv6 enable topology ipv6
 ipv6 preference 155
 ipv6 maximum load-balancing 16
 ipv6 circuit-cost 100000
 #
```

```
interface GigabitEthernet1/0/0
 description uT:city name-equipment room name-
network element name-serial
number.network.device model:port number
 undo shutdown
 ipv6 enable
 ip address X.X.X.X
 ipv6 address XXXX:X:XXXX:XXXX::X/127
 ipv6 address auto link-local
 isis enable 551
 isis ipv6 enable 551
 isis circuit-type p2p
 isis circuit-level level-2
 isis ipv6 cost 3000 level-2
 isis cost 3000 level-2
 isis small-hello
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Рекомендуется использовать все возможности для обеспечения быстрой сходимости IS-IS.

Краткое содержание

- Расширенные функции IS-IS
- Основные принципы и конфигурации IPv6 IS-IS
- Примеры применения IS-IS к двойному стеку

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Спасибо!

www.huawei.com

HCIE-R&S

— Основы протоколов BGP и BGP4+

www.huawei.com

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Введение

- В данном документе приводится основная информация о протоколах BGP и BGP4+. BGP (Border Gateway Protocol, протокол граничного шлюза) — это динамический протокол маршрутизации. Протокол BGP предназначен для передачи маршрутов IPv4 и IPv6 между автономными системами (AS), уведомления о доступности маршрутов и выбора оптимального маршрута между AS на основании политики маршрутизации. Для использования VPN на основе MPLS (MPLS VPN) необходимо настроить многопротокольный BGP внутри AS и между AS.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Цели

- После завершения этого курса вы будете:
  - Понимать принципы работы BGP.
  - Понимать принципы работы BGP4+.
  - Уметь использовать основные команды конфигурирования BGP.
  - Понимать планы поиска и устранения неисправностей для BGP.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Содержание

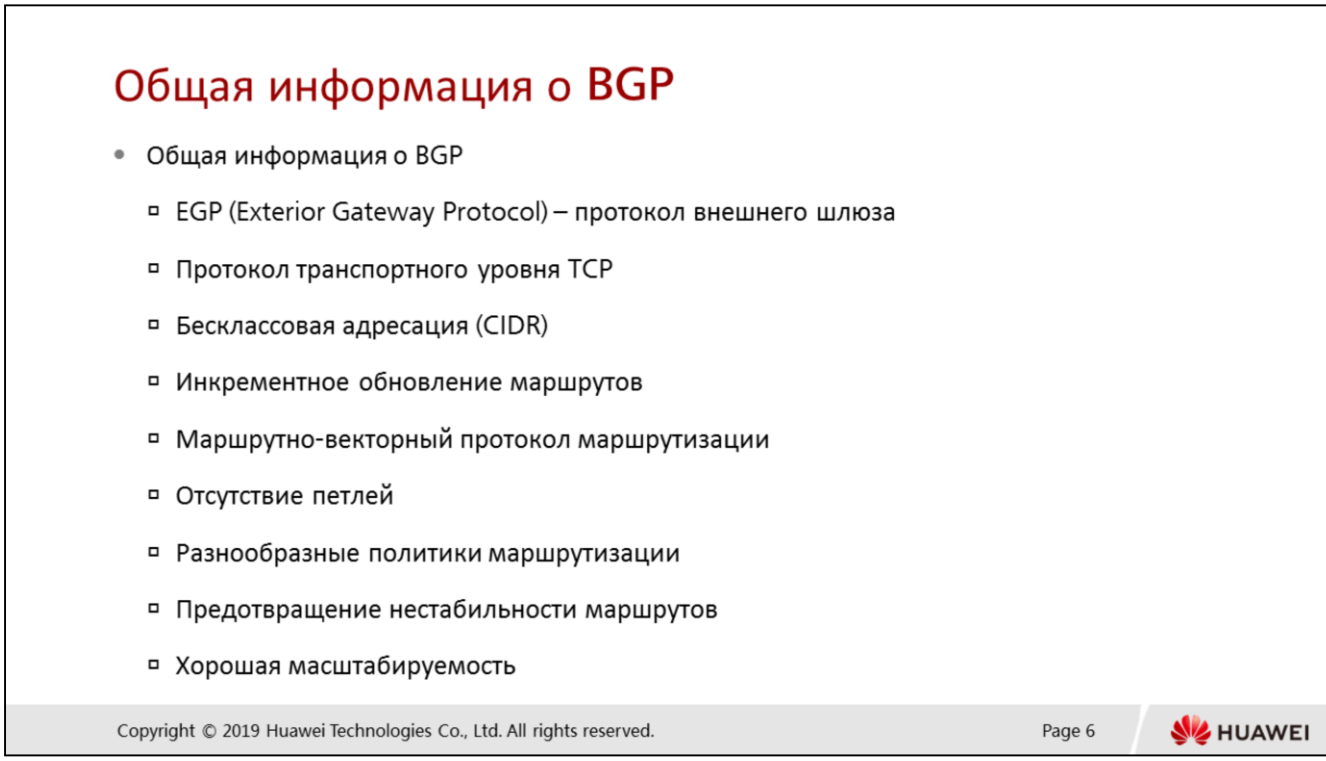
1. Принципы работы BGP
2. Принципы работы BGP4+
3. Основные конфигурации BGP и BGP4+
4. Диагностика неисправностей BGP

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Содержание

1. Принципы работы BGP
   - Общая информация о BGP
   - Понятия BGP
   - Внедрение BGP
   - Атрибуты BGP
   - Вычисление маршрута BGP

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

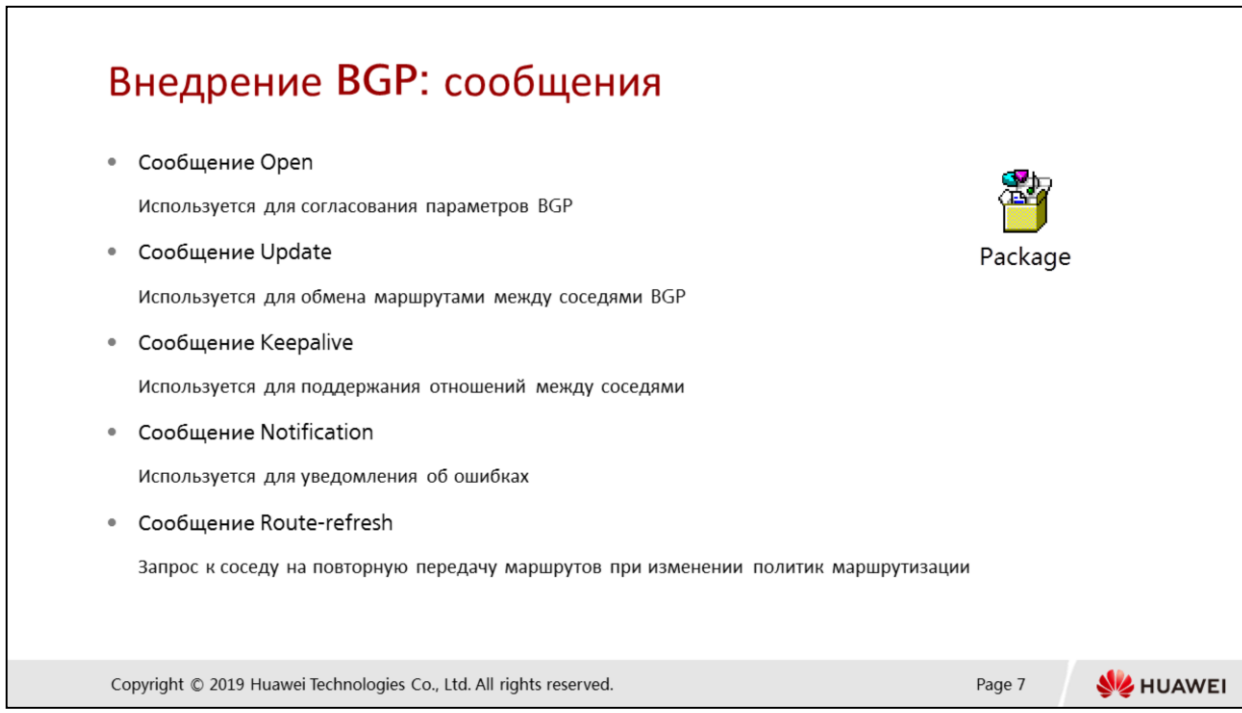


- BGP – динамический протокол маршрутизации, используемый между автономными системами (AS). Три предыдущие версии BGP: BGP-1 (стандарт RFC 1105), BGP-2 (стандарт RFC 1163) и BGP-3 (стандарт RFC 1267). BGP обменивается информацией о доступных маршрутах между AS, устанавливает пути между AS, предотвращает возникновение петель маршрутизации и применяет политики маршрутизации между AS. На данный момент используется версия протокола BGP-4, которая описывается в стандарте RFC 4271.
- BGP широко используется интернет-провайдерами как внешний протокол маршрутизации в Интернете.

- Общая информация о BGP
  - В отличие от протоколов внутренних шлюзов (IGP), например, протоколов OSPF и RIP, протокол BGP является протоколом внешнего шлюза (EGP), который контролирует анонсирование маршрутов и выбирает оптимальный маршрута между AS вместо обнаружения топологий сетей.
  - Протокол BGP использует протокол TCP (порт 179) в качестве протокола транспортного уровня. Это повышает надежность BGP и не требует дополнительного механизма для обеспечения управляемости соединения.
  - Протокол BGP выбирает маршруты между AS, для чего требуется высокий уровень стабильности. Протокол TCP обеспечивает высокую надежность и используется для повышения стабильности BGP.
    - Соседи BGP должны быть связаны логически. Между ними должно быть открыто TCP-соединение. Номер порта-адресата – 179, номером локального порта является случайное значение.
    - При обновлении маршрутов BGP передает только обновленные маршруты, значительно снижая загрузку полосы пропускания. Поэтому протокол BGP используется в Интернете, где требуется передача множества маршрутов.
  - В протоколе BGP предотвращается образование маршрутных петель.
    - Между AS: маршруты BGP содержат информацию об AS. Маршруты, которые содержат номер локальной AS отбрасываются, предотвращая возникновение петель между AS.
    - Внутри AS: BGP не анонсирует маршруты, полученные в AS, соседям BGP в AS, предотвращая возникновение петель внутри AS.
  - BGP использует различные политики маршрутизации для гибкой фильтрации и выбора маршрутов.
  - BGP использует механизм для предотвращения нестабильности маршрутов, за счет чего повышается стабильность интернет-

соединения.

- BGP легко масштабируется и адаптируется к развитию сети. Это расширяемый протокол благодаря формату атрибутов TLV.



- Протокол BGP работает с помощью пяти типов сообщений: Open, Update, Notification, Keepalive и Route-refresh.
  - Open – это первое сообщение, отправляемое после установления TCP-соединения, которое используется для установления отношений соседства. Когда сосед получает сообщение Open и переговоры между соседями проходят успешно, сосед отправляет сообщение Keepalive для подтверждения отношений соседства. Затем соседи могут обмениваться сообщениями Update, Notification, Keepalive и Route-refresh.
  - Update – это сообщение для обмена маршрутами между BGP-соседями. Сообщения Update могут использоваться для анонсирования доступных маршрутов с одинаковыми атрибутами или удаления нескольких недоступных маршрутов.
    - Сообщения Update могут анонсировать множество доступных маршрутов с одинаковыми атрибутами. У этих маршрутов может быть одинаковая группа атрибутов. Атрибуты маршрута, содержащиеся в сообщении Update, применимы ко всем адресам назначения (указанным в IP-префиксах), которые содержатся в поле NLRI сообщения Update.
    - Сообщение Update может использоваться для удаления нескольких недоступных маршрутов. Каждый маршрут определяется по адресу назначения (с помощью IP-префикса), который идентифицирует маршруты, ранее анонсированные между узлами BGP.
    - Сообщение Update может использоваться только для удаления маршрутов. В этом случае в сообщении не должны содержаться атрибуты маршрута или NLRI. Кроме того, сообщение Update может использоваться только для анонсирования доступных

маршрутов. В этом случае в сообщении не должна содержаться информация об удаленных маршрутах.

- Сообщение Keepalive периодически отправляется соседу для поддержания отношений соседства.
- Сообщение Notification отправляется соседу, когда BGP находит ошибку. Затем BGP-соединение незамедлительно обрывается.
- Сообщение Route-refresh используется для уведомления соседа о возможности обновить маршруты. Если все BGP-соседи поддерживают route-refresh и политика импорта маршрутов локального маршрутизатора была изменена, локальный маршрутизатор отправляет сообщение Route-refresh соседям или группам соседей. После получения сообщения соседи или группы соседей повторно отправляют маршрутную информацию на локальный BGP-маршрутизатор. Таким образом в динамическом режиме обновляются маршрутные таблицы BGP и применяются новые политики маршрутизации без разрыва BGP-соединений.

- Использование сообщений BGP.
  - BGP использует протокол TCP для установления соединений. Номер локального порта прослушивания – 179. Аналогично установлению TCP-соединения, при установлении BGP-соединения выполняется серия сессий и квитирования. Посредством квитирования TCP сообщает свои параметры, например, номер порта. Параметры квитирования, используемые в BGP, включают в себя версию BGP, время удержания BGP-соединения, идентификатор локального маршрутизатора и информацию об авторизации. Эта информация содержится в сообщениях Open.

- После установления соединения BGP отправляет сообщение Update соседу, когда требуется отправить маршрут. При анонсировании маршрута сообщение Update содержит атрибуты маршрута, чтобы помочь BGP-соседу выбрать оптимальный маршрут. При изменении локального BGP-маршрута, BGP-соседу отправляется сообщение Update с уведомлением об изменении.
- После обмена маршрутной информацией в течение некоторого времени у локального BGP-маршрутизатора и BGP-соседа не будет нового маршрута, и BGP-соединение станет стабильным. В этом случае сосед будет периодически отправлять сообщения Keepalive для проверки BGP-соединения. Если локальный BGP-маршрутизатор не получает сообщения Keepalive от соседа, он будет считать BGP-соединение прерванным, завершит соединение и удалит все BGP-маршруты, полученные от соседа.
- При выявлении ошибки, например, если версия BGP соседа не поддерживается на локальном уровне или локальный BGP-маршрутизатор получает недействительное сообщение Update, локальный BGP-маршрутизатор отправляет сообщение Notification BGP-соседу. Когда локальный BGP-маршрутизатор разрывает BGP-соединение, он также отправляет сообщение Notification.

- Заголовок сообщения BGP
  - Маркер (Marker): длина значения – 16 октетов. Все значения в поле установлены как 1.
  - Длина (Length): 2-октетное целое число без знака указывает на общую длину BGP-сообщения, включая заголовок.
  - Тип (Type): 1-октетное целое число без знака указывает на тип BGP-сообщения:
    - Open
    - Update
    - Keepalive
    - Notification
    - Route-refresh
- Формат сообщения Open:
  - Версия (Version): номер версии BGP. Для BGPv4 значение равно 4.
  - Моя автономная система (My Autonomous System): номер локальной AS. У EBGP-подключения и IBGP-подключения разные номера AS у BGP-соседей.
  - Время удержания (Hold Time): время удержания, которое должны подтвердить BGP-соседи. Оно должно совпадать у соседей при установлении отношений соседства. Если значение времени удержания у соседей отличается, BGP выбирает меньшее значение. Если маршрутизатор не получает сообщение Keepalive или Update от своих соседей в течение этого времени, BGP-соединение будет считаться прерванным. Если значение времени удержания равно 0, сообщения Keepalive не отправляются.
  - Идентификатор BGP (BGP Identifier): идентификатор BGP-маршрутизатора. Это поле представлено в формате IP-адреса и идентифицирует BGP-маршрутизатор.
  - Длина дополнительных параметров (Opt Parm Len): длина дополнительных параметров. Если значение равно 0, дополнительных параметров нет.
  - Дополнительные параметры (Optional Parameters): дополнительные параметры используются для аутентификации BGP или многопротокольного расширения. Каждый параметр включает тип параметра, длину параметра и значение параметра.
- Формат сообщения Update:

- Длина удаленных маршрутов (Withdrawn Routes Length): 2-октетное целое число без знака указывает общую длину поля Withdrawn Routes . Значение 0 указывает на то, что ни один маршрут не был удален, и что поля удаленных маршрутов нет в этом сообщении Update.
- Удаленные маршруты (Withdrawn Routes): это поле переменной длины, которое содержит список префиксов IP-адресов для удаленных маршрутов. Каждый префикс IP-адреса зашифрован в формате <длина, префикс>. Например, префикс <19, 198.18.160.0> обозначает сеть 198.18.160.0/255.255.224.0.
- Длина атрибута маршрута (Path Attribute Length): 2-октетное целое число без знака указывает общую длину поля атрибута маршрута. Значение 0 указывает на то, в поле атрибута маршрута нет данных, и что этого поля нет в сообщении Update.
- Информация о доступности сети (NLRI): это поле переменной длины, которое содержит список префиксов IP-адресов. Каждый префикс IP-адреса зашифрован в формате <длина, префикс>, аналогично полю удаленных маршрутов.

- Формат сообщения Keepalive
  - Сообщение Keepalive содержит только заголовок сообщения BGP.
  - Интервал отправки сообщений Keepalive по умолчанию – 60 секунд, время удержания для сессии BGP по умолчанию – 180 секунд. При получении сообщения Keepalive BGP-соседом, время удержания для сессии BGP сбрасывается до 180 секунд. Если время удержания истекает, соединение с соседом считается прерванным.
- Формат сообщения Notification
  - Errorcode: 1-октетное целое число без знака указывает на тип ошибки. Каждый тип ошибки имеет уникальный код, а у каждого кода ошибки есть один или несколько подкодов. Если подкод не определен, в поле Error Subcode указывается 0.
  - Errsubcode: Подкод ошибки.



- У автомата конечных состояний BGP есть 6 состояний: Idle, Connect, Active, OpenSent, OpenConfirm и Established.
    - Изначально BGP находится в состоянии Idle. В состоянии Idle BGP-устройство отказывается принимать все входящие BGP-соединения. BGP-устройство инициирует TCP-соединение с BGP-соседом и изменяет свое состояние на Connect только после получения события Start из системы.
        - Событие Start возникает, когда оператор настраивает процесс BGP или сбрасывает существующий процесс BGP либо ПО маршрутизатора сбрасывает процесс BGP.
        - Если в любом состоянии автомата возникает ошибка, например, BGP-устройство получает пакет Notification или уведомление о прекращении TCP-соединения, BGP-устройство меняет состояние на Idle.
    - В состоянии Connect BGP-устройство запускает таймер повторной попытки подключения (значение по умолчанию – 32 секунды) и ожидает установления TCP-соединения.
        - В этом состоянии BGP-устройство инициирует запросы на установление TCP-соединения.
        - Если TCP-соединение установлено, BGP-устройство отправляет соседу сообщение Open и изменяет состояние на OpenSent.
        - Если TCP-соединение не установлено, BGP-устройство изменяет состояние на Active.
        - Если BGP-устройство не получает ответ от соседа до истечения времени повторной попытки подключения, BGP-устройство пытается установить TCP-соединение с другим

соседом и остается в состоянии Connect.

- В ответ на любое другое событие (инициированное системой или оператором) BGP-устройство меняет свое состояние на Idle.

- В состоянии Active BGP-устройство продолжает попытки установить TCP-соединение с соседом.
    - В этом состоянии BGP-устройство ожидает от соседа инициацию TCP-соединения.
    - Если TCP-соединение установлено, BGP-устройство отправляет соседу сообщение Open, закрывает таймер повторной попытки подключения и изменяет состояние на OpenSent.
    - Если TCP-соединение не установлено, BGP-устройство остается в состоянии Active.
    - Если BGP-устройство не получает ответ от соседа до истечения времени повторной попытки подключения, BGP-устройство возвращается в состояние Connect.
- В состоянии OpenSent BGP-устройство ожидает сообщение Open от соседа и затем проверяет действительность полученного сообщения, включая номер AS, версию и пароль аутентификации.
    - Если полученное сообщение Open действительно, BGP-устройство отправляет сообщение Keepalive и меняет состояние на OpenConfirm.
    - Если полученное сообщение Open недействительно, BGP-устройство отправляет соседу сообщение Notification и возвращается в состояние Idle.
- В состоянии OpenConfirm BGP-устройство ожидает сообщение Keepalive или Notification от соседа. Если BGP-устройство получает сообщение Keepalive, оно меняет состояние на Established. Если BGP-устройство получает сообщение Notification, оно возвращается в состояние Idle.

- В состоянии Established BGP-устройство обменивается сообщениями Update, Keepalive, Route-refresh и Notification с соседом.
    - Если BGP-устройство получает действительное сообщение Update или Keepalive, он считает, что сосед работает корректно и поддерживает BGP-соединение с соседом.
    - Если BGP-устройство получает недействительное сообщение Update или Keepalive, оно отправляет соседу сообщение Notification и возвращается в состояние Idle.
    - Если BGP-устройство получает сообщение Route-refresh, оно не меняет свое состояние.
    - Если BGP-устройство получает сообщение Notification, оно возвращается в состояние Idle.
    - Если BGP-устройство получает уведомление о прекращении TCP-соединения, оно разрывает TCP-соединение с соседом и возвращается в состояние Idle.

Внедрение BGP: базы данных

- Таблица IP-маршрутизации (IP-RIB)

  Глобальная база маршрутной информации, в которой хранится вся информация IP-маршрутизации

- Таблица маршрутизации BGP (Loc-RIB)

  База локальной маршрутной информации, которую выбрал локальный узел BGP

- База данных BGP-соседей

  Список BGP-соседей

- Adj-RIB-In

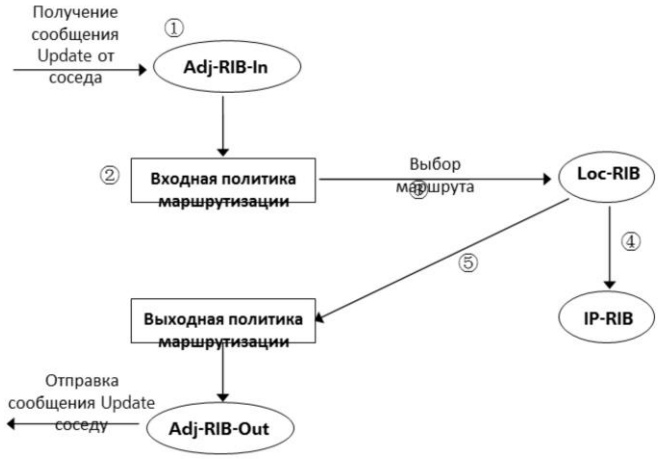
  База необработанной маршрутной информации, анонсированной соседом локальному узлу BGP

- Adj-RIB-Out

  База маршрутной информации, анонсированной узлом BGP определенном соседу

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

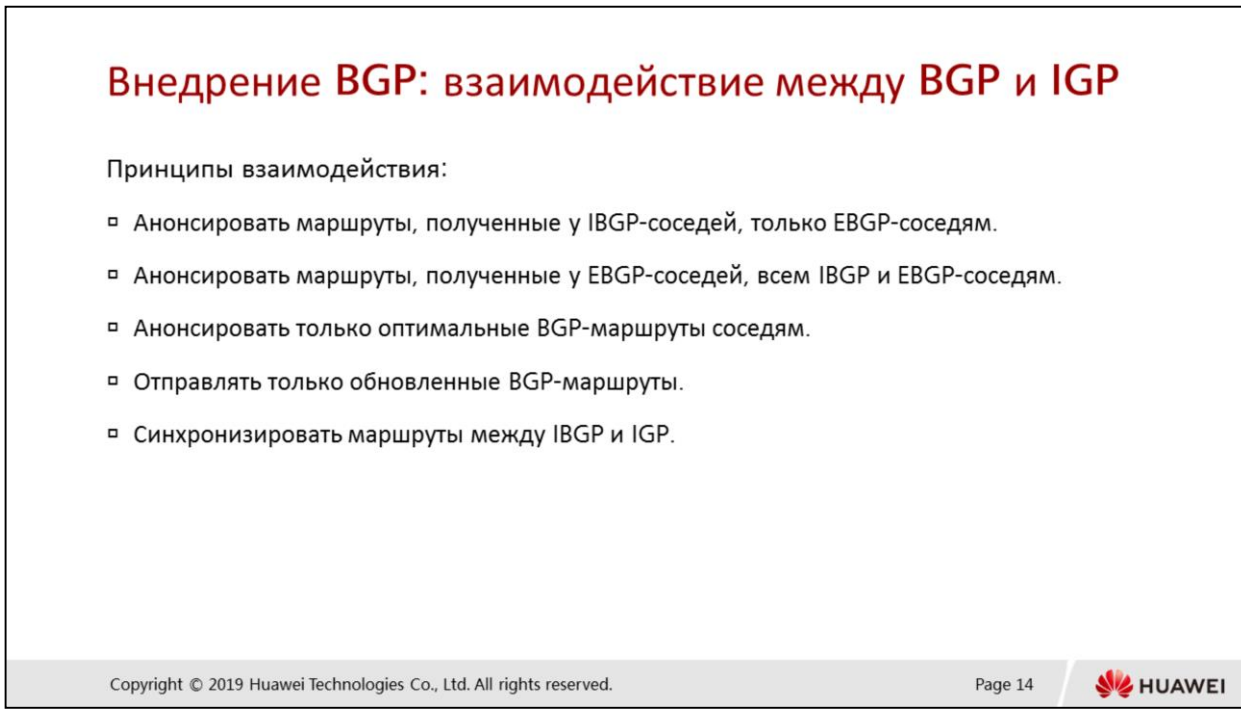
Внедрение BGP: обработка маршрутной информации BGP



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Обработка маршрутной информации BGP:
  - При получении сообщения Update от соседа BGP-маршрутизатор сохраняет его в базе Adj-RIB-In и указывает соседа, от которого он получил маршрут. После фильтрации сообщений Update с помощью входной политики маршрутизации BGP-маршрутизатор определяет оптимальный путь для каждого префикса IP-адреса на основе алгоритма выбора пути.
  - Оптимальные пути хранятся в базе Loc-RIB и устанавливаются в локальной базе IP-RIB.
  - Помимо оптимальных путей, полученных от соседа, в базе Loc-RIB также хранятся префиксы маршрутов BGP, полученные от локального маршрутизатора и выбранные в качестве оптимальных путей. Маршруты, сохраненные в базе Loc-RIB, должны фильтроваться на базе выходной политики маршрутизации до анонсирования другим соседям. Только маршруты, прошедшие фильтр выходной политики маршрутизации, хранятся в Adj-RIB-Out.

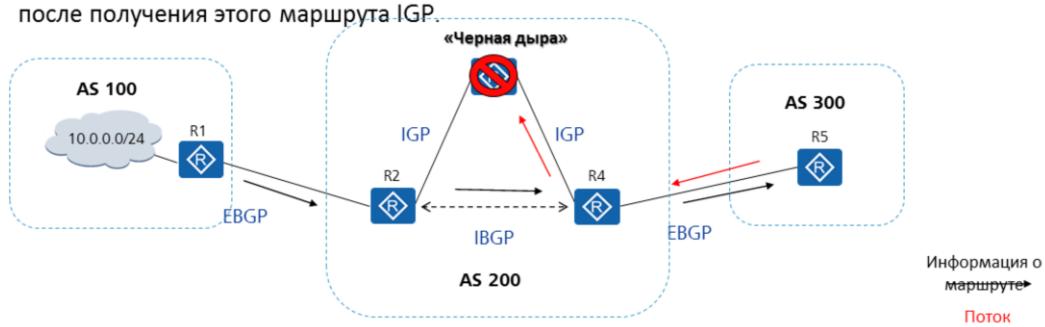


- BGP-устройство добавляет оптимальные маршруты в таблицу маршрутизации BGP для создания BGP-маршрутов.
  - BGP-устройство анонсирует BGP-маршруты, полученные от IBGP-соседей, только EBGP-соседям.
  - BGP-устройство анонсирует BGP-маршруты, полученные от EBGP-соседей, соседям EBGP и IBGP.
  - BGP-устройство анонсирует оптимальный маршрут соседям, когда к одному пункту назначения существует несколько действительных маршрутов.
  - BGP-устройство отправляет только обновленные BGP-маршруты при изменении маршрутов.
  - BGP-устройство анонсирует EBGP-соседям маршруты, полученные от IBGP-соседей, только когда идентичные маршруты существуют в IGP.

Внедрение BGP: синхронизация между IBGP и IGP

- Синхронизация

  До добавления IBGP-маршрута в таблицу маршрутизации и анонсирования его EBGP-соседу BGP-маршрутизатор проверяет таблицу маршрутизации IGP. IBGP-маршрут можно добавить в таблицу маршрутизации и анонсировать только после получения этого маршрута IGP.



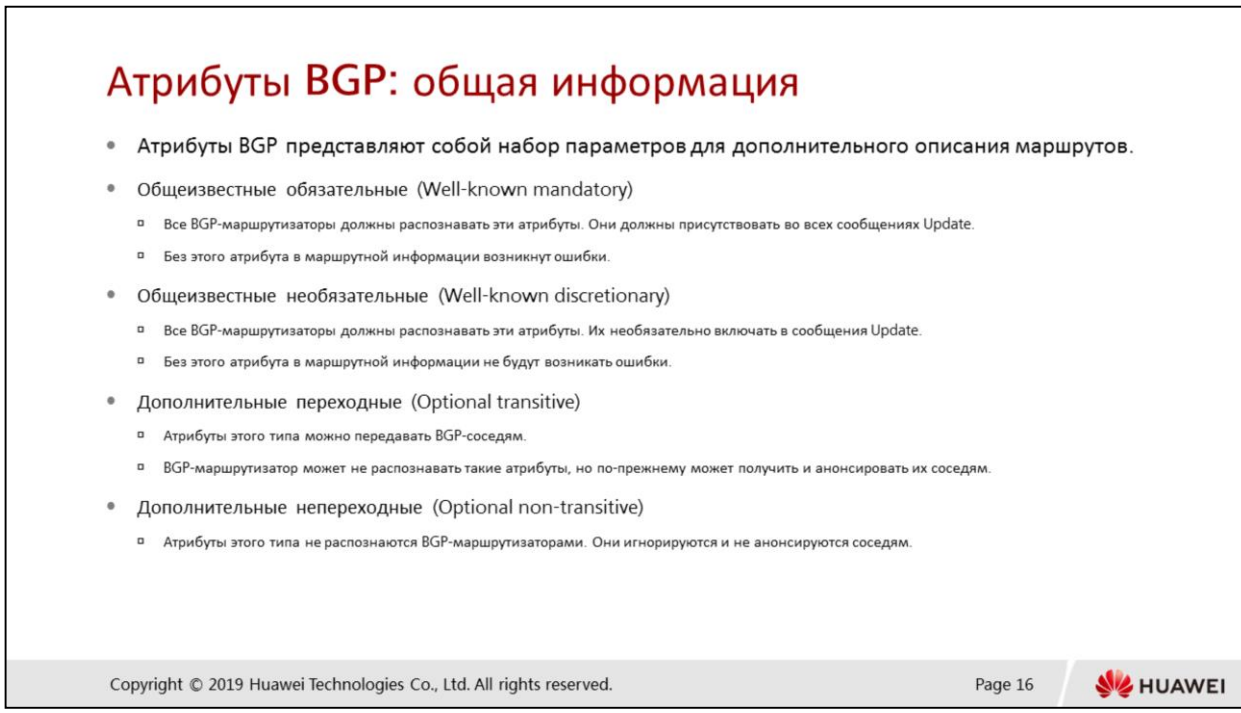
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Между IBGP и IGP выполняется синхронизация, чтобы предотвратить импорт недоступных маршрутов в устройства внешней AS.

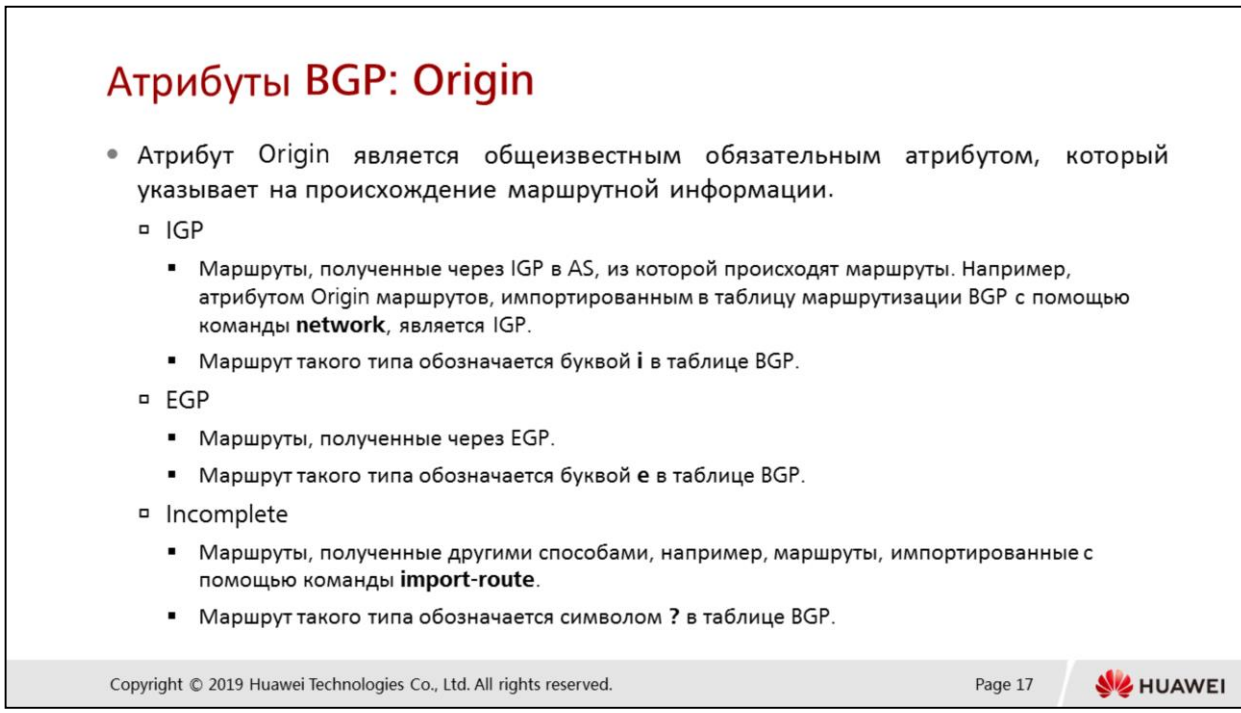
- Описание топологии (при включенной синхронизации)
  - Маршрутизатор R4 узнает о сегменте сети 10.0.0.0/24, анонсированном R1 через BGP. До анонсирования сегмента сети маршрутизатору R5, маршрутизатор R4 проверяет, есть ли этот сегмент в таблице маршрутизации IGP. Если да, R4 анонсирует сегмент сети маршрутизатору R5. Если нет, R4 не может анонсировать его маршрутизатору R5.

- **Меры предосторожности**
  - Механизм синхронизации между BGP и IGP отключен в VRP по умолчанию и не может быть изменен. Однако синхронизацию можно отменить в одном их следующих сценариев:
  - Локальная AS не является транзитной AS.
  - Все маршрутизаторы в AS установили полные IBGP-соединения.



- Атрибуты BGP-маршрутов представляют собой набор параметров для дополнительного описания маршрутов. Благодаря атрибутам BGP может фильтровать и выбирать маршруты.

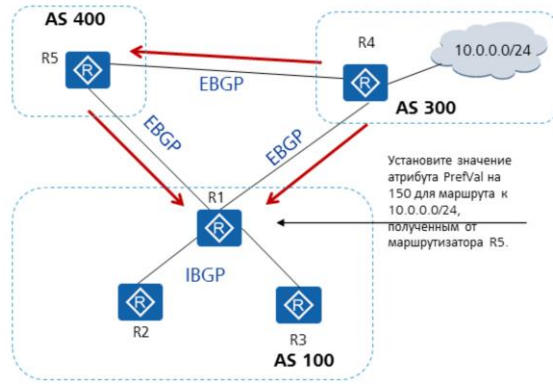
- Часто используемые атрибуты:
  - Origin: общеизвестный обязательный
  - AS_Path: общеизвестный обязательный
  - Next_Hop: общеизвестный обязательный
  - Local_Pref: общеизвестный необязательный
  - community: дополнительный переходный
  - Multi-exit-discriminator (MED): дополнительный непереходный
  - Originator_ID: дополнительный непереходный
  - Cluster_List: дополнительный непереходный



- Атрибут Origin указывает на происхождение маршрута и маркирует маршрут BGP. У атрибута Origin может быть три значения:
  - IGP: маршрут, у которого атрибут Origin имеет значение EGP, имеет высший приоритет. Атрибут Origin имеет значение IGP для маршрутов, полученных через IGP в AS, из которой происходят эти маршруты. Например, атрибут Origin маршрутов, импортированный в таблицу маршрутизации BGP с помощью команды **network**, имеет значение IGP.
  - EGP: маршрут, у которого атрибут Origin имеет значение EGP, является следующим по приоритету. Атрибут Origin имеет значение EGP у маршрутов, полученных через EGP.
  - Incomplete: маршрут, у которого атрибут Origin имеет значение Incomplete, имеет самый низкий приоритет. Атрибут Origin имеет значение Incomplete для маршрутов, полученных через иными способами. Например, атрибут Origin маршрутов, импортированных в таблицу маршрутизации BGP с помощью команды **import-route**, имеет значение Incomplete.

Атрибуты BGP: PrefVal

- Атрибут PrefVal создан Huawei и действителен только на устройстве, где он настраивается. Атрибут PrefVal настраивает пользователь. Поэтому при выборе маршрута BGP сначала сравнивает значения PreVal.



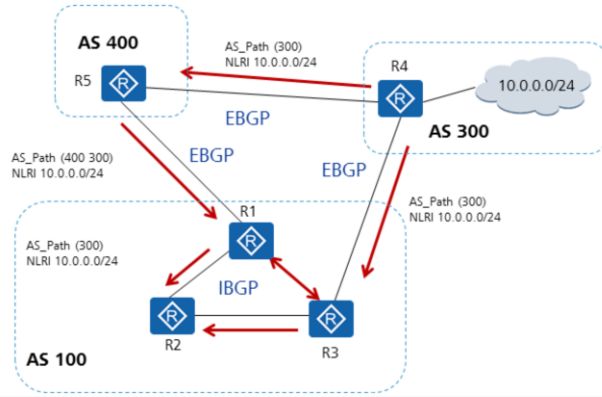
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- При выборе маршрута BGP сначала сравнивает значения PrefVal. Значение по умолчанию равно 0. Большее значение указывает на более высокий приоритет.

Атрибуты BGP: AS_Path

- Атрибут AS_Path содержит номера всех AS, через которые проходит маршрут, от источника до назначения по вектору. Это общеизвестный обязательный атрибут.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

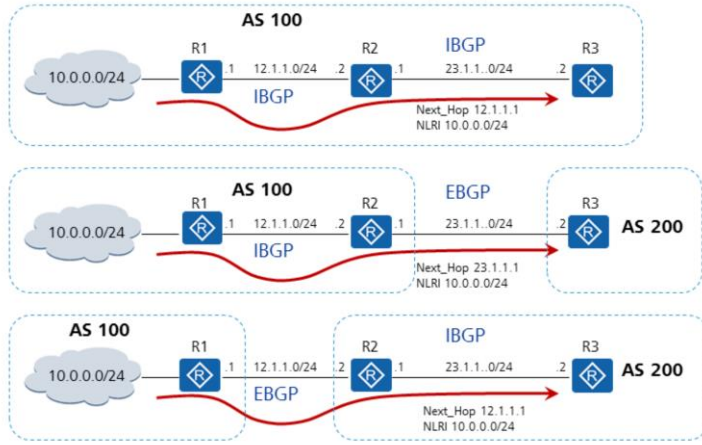
HUAWEI

- Атрибут AS_Path может использоваться для выбора маршрута BGP. Чем короче длина атрибута AS_Path, тем выше приоритет. Кроме того, чтобы предотвратить возникновение петлей между AS, BGP-маршрутизатор не принимает маршруты, в списке AS_Path которых содержатся номера локальных AS, анонсированные EBGP-соседями.
    - Когда узел BGP анонсирует локальный маршрут:
        - При анонсировании маршрута за пределами локальной AS узел BGP добавляет номер локальной AS в список AS_Path и передает его соседним маршрутизаторам посредством сообщений Update.
        - При передаче маршрута локальной AS узел BGP создает пустой список AS_Path в сообщении Update.
    - Когда узел BGP передает маршрут, полученный от другого узла BGP из сообщений Update:
        - При анонсировании маршрута другим AS узел BGP добавляет номер локальной AS в начало списка AS_Path. В соответствии с атрибутом AS_Path BGP-маршрутизатор, который получает маршрут, может определить, через какие AS проходит маршрут до конечной сети. Номер AS, которая находится ближе всего к локальной AS, находится вверху списка AS_Path. Номера других AS перечислены в порядке прохождения маршрута через AS.
        - Когда узел BGP анонсирует маршрут локальной AS, он не меняет AS_Path.
- Топология сети:
    - Когда маршрутизатор R4 анонсирует AS 400 и AS 100 сегмент сети 10.0.0.0/24, он добавляет номер локальной AS в атрибут AS-Path. Когда маршрутизатор R5 анонсирует AS 100 сегмент сети 10.0.0.0/24, он также добавляет номер своей локальной AS в атрибут AS-Path. Когда маршрутизаторы R1, R2 и R3 в AC 100 анонсируют сегмент сети 10.0.0.0/24 друг другу,

атрибуты AS_PATH маршрутов не меняются. Если прочие условия для выбора маршрута BGP совпадают, BGP выбирает маршрут с самым коротким значением атрибута AS_Path, т.е. маршрут от R3 до R4.

Атрибут BGP: Next_Hop

- Атрибут Next_Hop указывает на адрес следующего узла, через который проходит маршрут. Это общеизвестный обязательный атрибут.



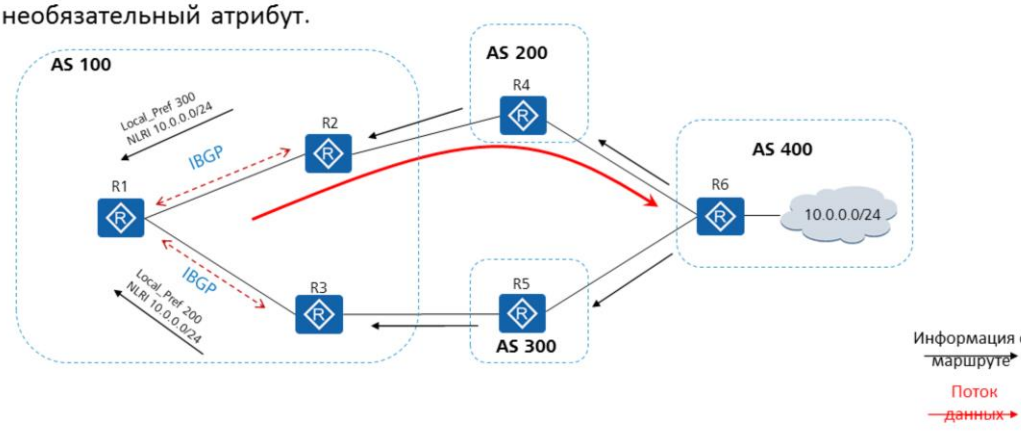
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Атрибут Next_Hop указывает на адрес следующего узла, через который проходит маршрут. Атрибут Next_Hop BGP отличается от такого же атрибута IGP, поскольку он не может являться IP-адресом BGP-соседа. Узел BGP обрабатывает атрибут Next_Hop на основании следующих правил:
  - При анонсировании локально образованного маршрута IBGP-соседу узел BGP устанавливает атрибут Next_Hop маршрута как адрес локального интерфейса, через который устанавливаются отношения соседства BGP.
  - При анонсировании маршрута EBGP-соседу узел BGP устанавливает атрибут Next_Hop маршрута как адрес локального интерфейса, через который устанавливаются отношения соседства BGP.
  - При анонсировании IBGP-соседу маршрута, полученного от EBGP-соседа, узел BGP не меняет атрибут Next_Hop маршрута.

Атрибуты BGP: Local_Pref

- Атрибут Local_Pref указывает на приоритет BGP-маршрутизатора. Большее значение указывает на более высокий приоритет. Это общеизвестный необязательный атрибут.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

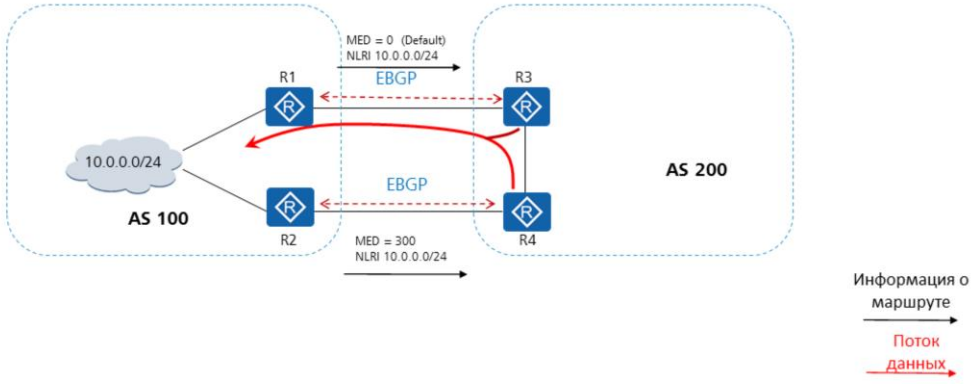
HUAWEI

- Local_Pref
  - Этим атрибутом обмениваются только IBGP-соседи. Этот атрибут не передается в другие AS. Он указывает на приоритет BGP-маршрутизаторов.
  - После того, как BGP-маршрутизатор получает множество маршрутов с одинаковым конечным адресом, но разными адресами следующей AS для достижения сети назначения от разных IBGP-соседей, он выбирает маршрут с большим значением атрибута Local-Pref.

- Описание топологии
  - Отношения соседства IBGP устанавливаются между маршрутизаторами R1, R2 и R3 в AS 100. Маршрутизаторы R2 и R3 устанавливают отношения соседства EBGP с маршрутизаторами в AS 200 и AS 300 соответственно. В этом случае и маршрутизатор R2, и маршрутизатор R3 получают маршрут 10.0.0.0/24 от своих EBGP-соседей. Чтобы три маршрутизатора в AS 100 выбирали R2 в качестве выхода маршрута 10.0.0.0/24 в локальной AS, вам нужно изменить атрибут Local Pref маршрута только в маршрутизаторах R2 и R3.

Атрибуты BGP: MED

- Атрибут MED аналогичен значению стоимости в IGP и используется для выбора маршрута между AS. Это необязательный непереходный атрибут.

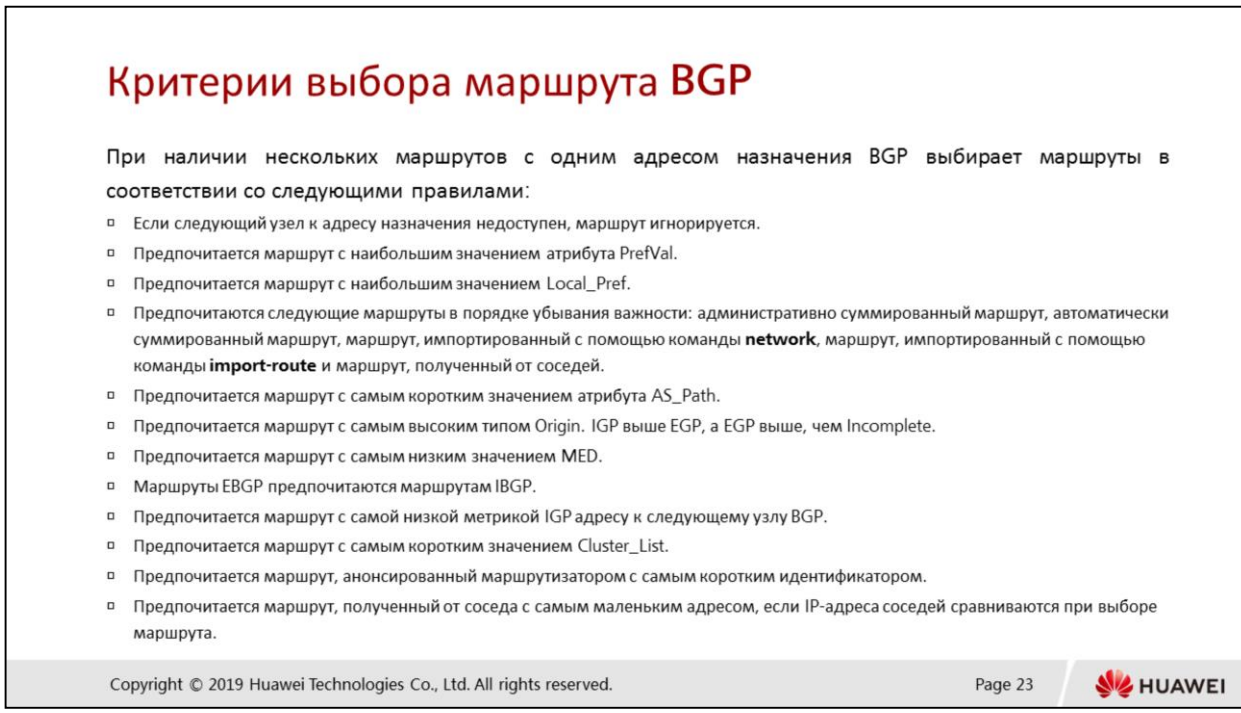


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Когда BGP-устройство получает несколько маршрутов к одному адресу назначения, но с разными следующими узлами от разных EBGP-соседей в одной AS, BGP-устройство выбирает маршрут с наименьшим значением атрибута MED в качестве оптимального.

- Атрибутом MED обмениваются только две соседские AS. AS, которая получает атрибут MED, не анонсирует его другим AS. Атрибут MED можно настраивать вручную. Если для маршрута не настроен атрибут MED, для него устанавливается значение по умолчанию 0.

- Описание топологии
  - Маршрутизаторы R1 и R2 анонсируют сегмент сети 10.0.0.0/24 своим EBGP-соседям – маршрутизаторам R3 и R4. Маршрутизаторы R3 и R4 предпочитают выбирать маршрут с меньшим значением MED при прочих равных условиях. Таким образом, маршрутизаторы R3 и R4 получают доступ к сегменту 10.0.0.0/24 через R1.



- Критерии выбора маршрута BGP:
- IP-адрес следующего узла, указанный для BGP-маршрута, должен быть доступным.
- Атрибут PrefVal создан Huawei и действителен только на устройстве, на котором он настраивается.
- Если для маршрута не настроен атрибут Local_Pref, для него устанавливается значение по умолчанию 100. Вы можете настроить значение Local-Pref по умолчанию для BGP-маршрута с помощью команды **default local-preference**.
- Маршруты, созданные локально, включают маршруты, импортированные с помощью команды **network** или **import-route**, маршруты, суммированные администратором, и маршруты, суммированные автоматически.
    - Предпочтительно использовать суммарный маршрут. Суммарный маршрут обладает приоритетом над не суммарным маршрутом.
    - Маршрут, суммированные администратором с помощью команды **aggregate**, предпочтительнее, чем маршрут, суммированный автоматически с помощью команды **summary automatic**.
    - Маршрут, импортированный с помощью команды **network** , предпочтительнее, чем маршрут, импортированный с помощью команды **import-route**.
- Предпочтение отдается маршруту с самым коротким значением атрибута AS_Path.
    - Атрибут AS_Path содержит атрибуты AS_Confed_Sequence и AS_Confed_Set.
    - BGP-маршрутизатор предполагает, что AS_SET содержит только один номер AS вне

зависимости от фактического количества AS, которое он содержит.

- После выполнения команды **bestroute as-path-ignore** атрибуты маршрутов AS_Path не сравниваются при выборе маршрута.

- Предпочтение отдается маршруту с самым низким значением MED.
    - BGP сравнивает атрибуты MED только маршрутов из одной AS, но не их конфедерации подсистем AS. То есть атрибуты MED двух маршрутов сравниваются только тогда, когда первый номер AS в AS_SEQUENCE (за исключением AS_CONFED_SEQUENCE) одинаков для этих маршрутов.
    - Маршруту без атрибута MED присваивается значение 0 для атрибута MED, если не выполнена команда **bestroute med-none-as-maximum**. Если вы запустите команду **bestroute med-none-as-maximum**, маршруту будет присвоено максимальное значение MED – 4294967295.
    - После выполнения команды **compare-different-as-med** сравниваются атрибуты MED в маршрутах, полученных от соседей в разных AS. Используйте эту команду только тогда, когда разные AS используют одинаковый IGP и режим выбора маршрутов. В противном случае может возникнуть петля.
    - Если вы запустите команду **bestroute med-confederation**, атрибуты MED будут сопоставляться для маршрутов, если атрибуты AS_Path маршрутов не будут содержать номера внешних AS (не конфедерации подсистем AS) и первый номер AS в AS_CONFED_SEQUENCE будет совпадать.
    - После выполнения команды **deterministic-med** маршруты не будут выбираться в порядке получения.

- Балансировка нагрузки

- При наличии нескольких маршрутов с одинаковой стоимостью к одному адресу назначения вы можете выполнить балансировку нагрузки между этими маршрутами.
- BGP-маршруты с одинаковой стоимостью можно использовать для балансировки нагрузки только тогда, когда совпадают атрибуты, описанные до правила «Предпочитается маршрут с самой низкой метрикой IGP адресу к следующему узлу BGP».

Содержание

1. Принципы работы BGP
2. Принципы работы BGP4+
3. Основные конфигурации BGP и BGP4+
4. Диагностика неисправностей BGP

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Содержание

1. Принципы работы BGP4+
   - Обзор BGP4+
   - Анонсирование возможностей BGP4+
   - Расширенные атрибуты BGP4+

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

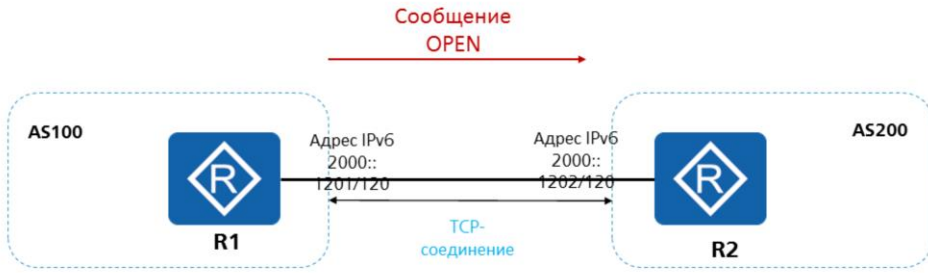
Обзор BGP4+

- Обзор BGP4+
  - Расширение BGP4
  - Поддержка согласования возможностей
  - Поддержка нескольких семейств адресов, включая IPv6, VPNv4 и VPNv6
  - Передача маршрутной информации о нескольких семействах адресов с помощью расширенных атрибутов

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Анонсирование возможностей BGP4+ (1/2)

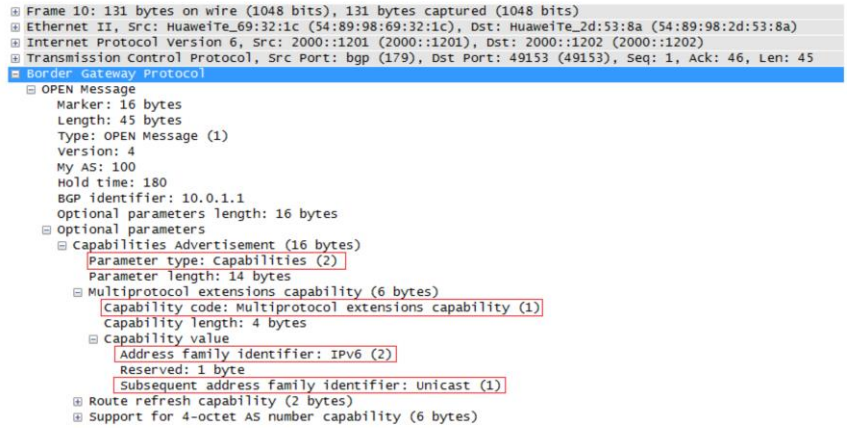
- При необходимости передачи адресов IPv6 между двумя соседями BGP, два маршрутизатора BGP должны передавать друг другу возможности IPv6 в сообщении Open.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Анонсирование возможностей BGP4+ (2/2)

- Поле Advertisement Capabilities в сообщении Open используется для согласования расширенных возможностей.



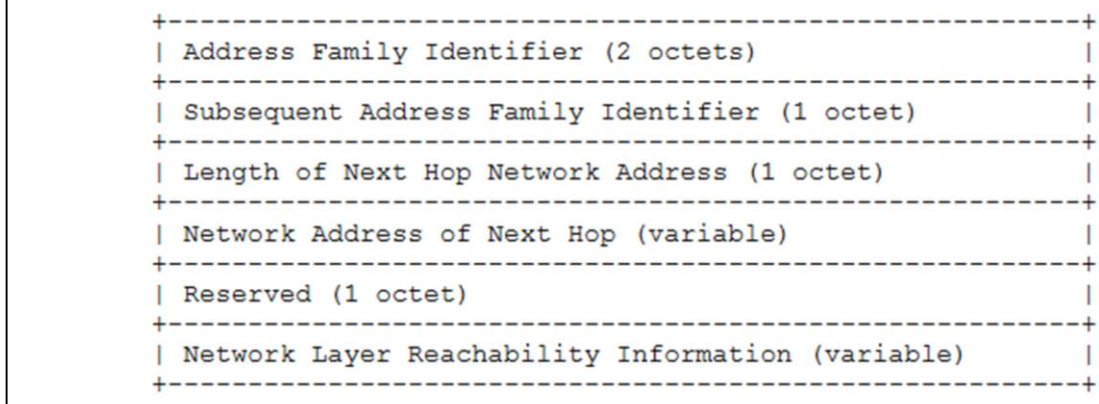
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Помимо согласования возможностей между семействами адресов, в поле Capabilities Advertisement могут быть согласованы следующие возможности:
  - 4-байтовый номер AS
  - Функция Route-refresh
  - Многоуровневые метки

Расширенный атрибут BGP4+: MP_ REACH_NLRI (1/3)

- MP_REACH_NLRI (Type Code = 14)
  - Этот атрибут используется для анонсирования маршрутов IPv6.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

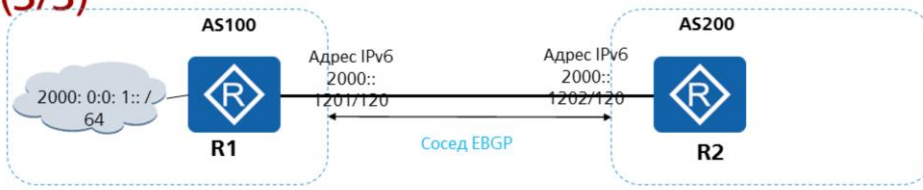
- Информация о семействе адресов: включает идентификатор Address Family Identifier (AFI) из 2 октетов и Subsequent Address Family Identifier (SAFI) из 1 октета.
- Length of Next Hop Network Address: состоит из 1 октета, указывающего на длину адреса следующего узла. Как правило, значение равно 16.
- Network Address of Next Hop: длина является переменной и зависит от длины сетевого адреса узла. Как правило, значение является глобальным одиночным адресом.
- Reserved: состоит из 1 октета. Значение должно быть равно 0.
- NLRI: перечисляет маршруты, содержащие такие же атрибуты. Если значение этого поля равно 0, этот маршрут является маршрутом по умолчанию.

Расширенный атрибут BGP4+: MP_ REACH_NLRI (2/3)

- При передаче маршрутов IPv6:
  - AFI = 2, SAFI = 1 (одиночный), SAFI = 2 (групповой)
  - Поле Next Hop Address Length определяет количество адресов следующих узлов.
    - Если значение равно 16, адрес следующего узла – это глобальный одиночный адрес маршрутизатора следующего узла.
    - Если значение равно 32, адрес следующего узла – это глобальный одиночный адрес и адрес link-local маршрутизатора следующего узла.
  - Зарезервированное поле. Значение равно 0.
  - Информация о доступности уровней (NLRI) является полем переменной длины и указывает префикс и маску маршрута

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Расширенный атрибут BGP4+: MP_ REACH_NLRI (3/3)



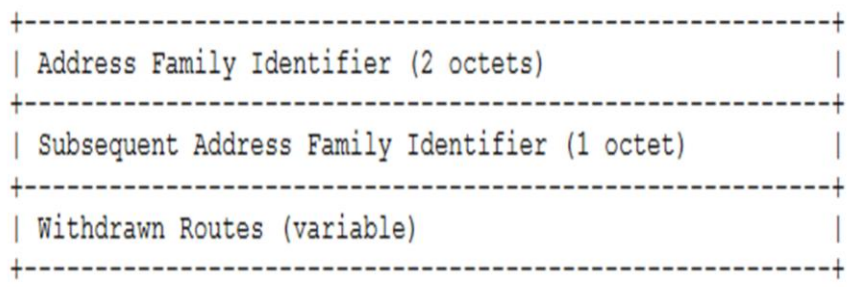

```
Border Gateway Protocol
  UPDATE Message
    Marker: 16 bytes
    Length: 77 bytes
    Type: UPDATE Message (2)
    Unfeasible routes length: 0 bytes
    Total path attribute length: 54 bytes
    Path attributes
      ORIGIN: IGP (4 bytes)
      AS_PATH: 100 (9 bytes)
      MULTI_EXIT_DISC: 0 (7 bytes)
      MP_REACH_NLRI (34 bytes)
        Flags: 0x90 (Optional, Non-transitive, Complete, Extended Length)
        Type code: MP_REACH_NLRI (14)
        Length: 30 bytes
        Address family: IPv6 (2)
        Subsequent address family identifier: Unicast (1)
        Next hop network address (16 bytes)
          Next hop: 2000::1201 (16)
        Subnetwork points of attachment: 0
        Network layer reachability information (9 bytes)
          2000:0:0:1::/64
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Расширенный атрибут BGP4+: MP_UNREACH_NLRI (1/2)

- MP_UNREACH_NLRI (Type Code = 15)
  - Этот атрибут используется для удаления маршрутов.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Address Family Information: включает AFI из 2 октетов и SAFI из 1 октета.
- Withdrawn Routes: указывает маршрут, который должен быть удален, в формате <длина маски, префикс маршрута>. Если длина маски равна 0, маршрут, который должен быть удален, является стандартным маршрутом.

Расширенный атрибут BGP4+: MP_UNREACH_NLRI (2/2)

- Когда маршрут IPv6 должен быть удален:
  - AFI = 2, SAFI = 1 (одиночный), SAFI = 2 (групповой)
  - Поле Withdrawn Routes указывает префикс и маску маршрута, подлежащего удалению.

```
⊟ Border Gateway Protocol
  ⊟ UPDATE Message
      Marker: 16 bytes
      Length: 39 bytes
      Type: UPDATE Message (2)
      Unfeasible routes length: 0 bytes
      Total path attribute length: 16 bytes
    ⊟ Path attributes
      ⊟ MP_UNREACH_NLRI (16 bytes)
        ⊞ Flags: 0x90 (Optional, Non-transitive, Complete, Extended Length)
          Type code: MP_UNREACH_NLRI (15)
          Length: 12 bytes
          Address family: IPv6 (2)
          Subsequent address family identifier: Unicast (1)
        ⊟ Withdrawn routes (9 bytes)
          ⊞ 2000:0:0:1::/64
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

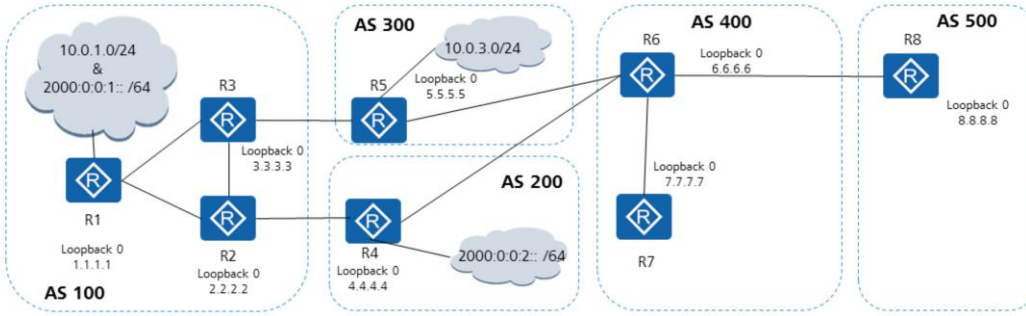
Содержание

1. Принципы работы BGP
2. Принципы работы BGP4+
3. Основные конфигурации BGP и BGP4+
4. Диагностика неисправностей BGP

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Базовая конфигурация BGP (1/2)

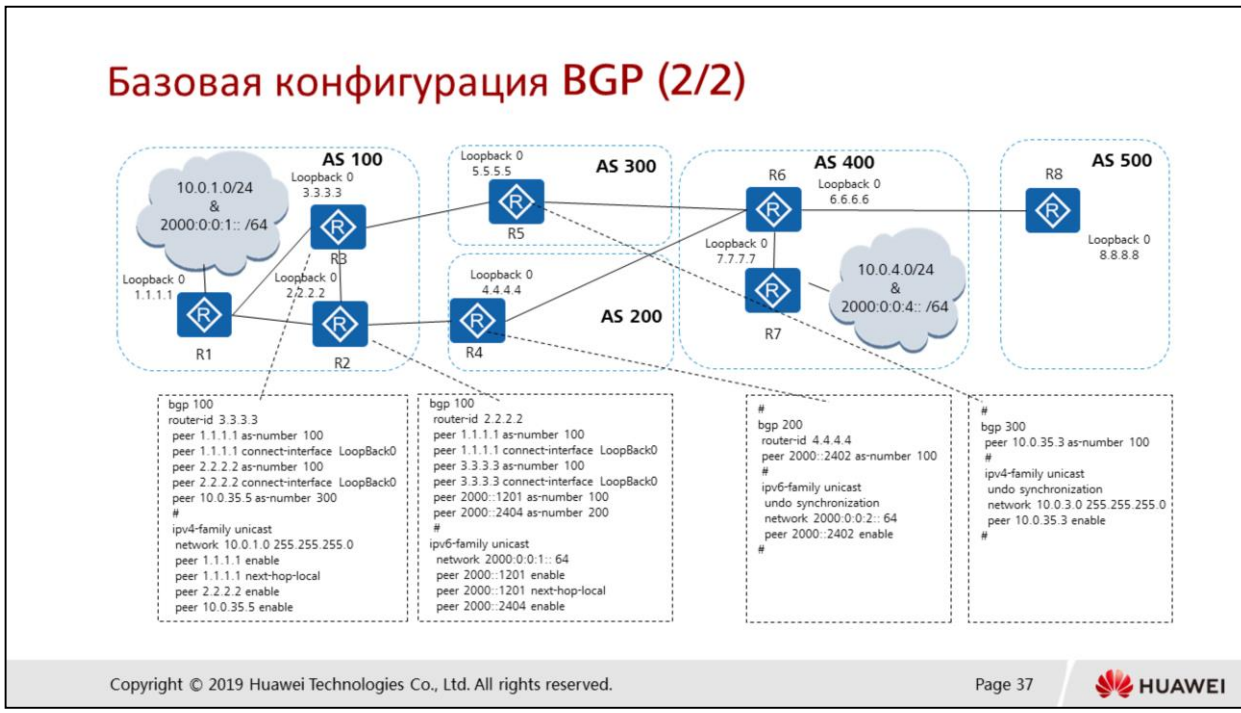
- Требования к конфигурации:
  1. Между ASBR-маршрутизаторами в каждой AS необходимо установить отношения соседства EBGP.
  2. В каждой AS необходимо установить стабильные отношения соседства IBGP.
  3. Сети IPv4 и IPv6 могут взаимодействовать друг с другом.
  4. Маршрутизаторы в каждой AS могут взаимодействовать друг с другом через IGP.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Правила конфигурирования IP-адресов:
  - Сетевым сегментом IPv4 для интерфейсов, непосредственно соединяющих Rx и Ry (X < Y), является 10.0.xy.0/24. Адрес IPv4 соответствующего интерфейса на Rx – 10.0.xy.x, а на Ry – 10.0.xy.y.
  - Сетевым сегментом IPv6 для интерфейсов, непосредственно соединяющих Rx и Ry (X < Y), является 2000:: xy00/120. Адрес IPv6 соответствующего интерфейса на Rx – 2000:: xy0x, а на Ry –2000:: xy0y.
  - Адрес IPv6 loopback 0-интерфейса на каждом маршрутизаторе – 2000::z (где z – это ID маршрутизатора).
- Примечания:
  - Протоколы OSPF и IS-IS могут работать в AS, чтобы маршрутизаторы в AS могли взаимодействовать друг с другом.
  - Стабильные отношения IBGP можно установить с помощью loopback-интерфейсов.
  - Отношения соседства EBGP можно установить напрямую через физические интерфейсы.



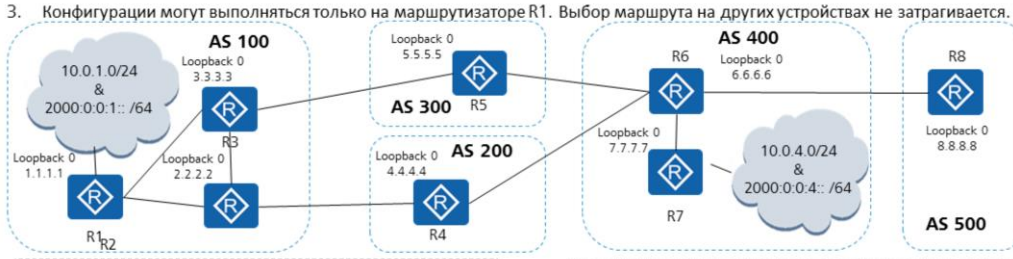
- Описание команд:
  - Команда **peer as-number** указывает номер AS для соседа или группы соседей.
  - Команда **peer connect-interface** определяет интерфейс источника, из которого отправляются пакеты BGP, и адрес источника, используемый для инициирования соединения.
  - Команда **peer next-hop-local** конфигурирует устройство BGP, чтобы оно установило свой IP-адрес в качестве следующего узла маршрутов, когда устройство BGP анонсирует маршруты к соседу или группе соседей IBGP.
- Использование команды:
  - Предыдущие команды выполняются в режиме процессов BGP.
- Описание параметров
  - peer ipv4-address as-number
    - Ip-address: указывает адрес IPv4 соседа.
    - as-number: указывает номер AS соседа.
  - peer ipv4-address connect-interface interface-type interface-number [ipv4-source-address]
    - Ip-address: указывает адрес IPv4 соседа.
    - Interface-type interface-number: определяет тип и номер интерфейса.
    - Ipv4-source-address: определяет адрес источника IPv4 для установления соединения BGP.
  - peer ipv4-address next-hop-local
    - Ip-address: указывает адрес IPv4 соседа.
- **Меры предосторожности**
  - При конфигурировании устройства для использования loopback-интерфейса в качестве интерфейса источника сообщений BGP, обратите внимание на следующие моменты:
    - IP-адрес loopback-интерфейса должен быть доступен.
    - Для установления соединения EBGP необходимо также выполнить команду **peer ebgp-max-hop**, чтобы разрешить двум устройствам установить непрямые отношения соседства.
- Команды **peer next-hop-local** и **peer next-hop-invariable** являются взаимоисключающими.
- **PrefRcv** в выводе команды **display bgp peer** указывает на количество префиксов маршрутов, получаемых

маршрутизатором BGP от его соседа.

- Конфигурация в сети IPv6 аналогична конфигурации IPv4. Разница заключается в том, что после указания адреса соседа и номера AS необходимо перейти в режим ipv6 unicast family view и выполнить команду **peer peer-ip-address enable** для активации BGP.

Конфигурирование BGP: Атрибут PrefVal (1/2)

- Требования к конфигурации:
  1. Маршрут от R1 к сетевому сегменту 10.0.4.0/24 в AS 400 проходит последовательно через маршрутизаторы R1, R2, R4, R6 и R7.
  2. Маршрут от R1 к сетевому сегменту 2000:0:0:4::/64 в AS 400 проходит последовательно через маршрутизаторы R1, R3, R5, R6 и R7.
  3. Конфигурации могут выполняться только на маршрутизаторе R1. Выбор маршрута на других устройствах не затрагивается.




```
<R1>display bgp ipv6 routing-table 2000:0:0:4::64
BGP routing table entry information of 2000:0:0:4::/64:
  From: 2000::1202 (2.2.2.2)
  Original nexthop: 2000::1202
  AS-path 200 400, origin igp, localpref 100, pref-val 0, valid, internal, best,
select, active, pre 255
From: 2000::1303 (3.3.3.3)
Original nexthop: 2000::1303
  AS-path 300 400, origin igp, localpref 100, pref-val 0, valid, internal, pre 25
5, not preferred for router ID
```

```
<R1>display bgp routing-table

Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

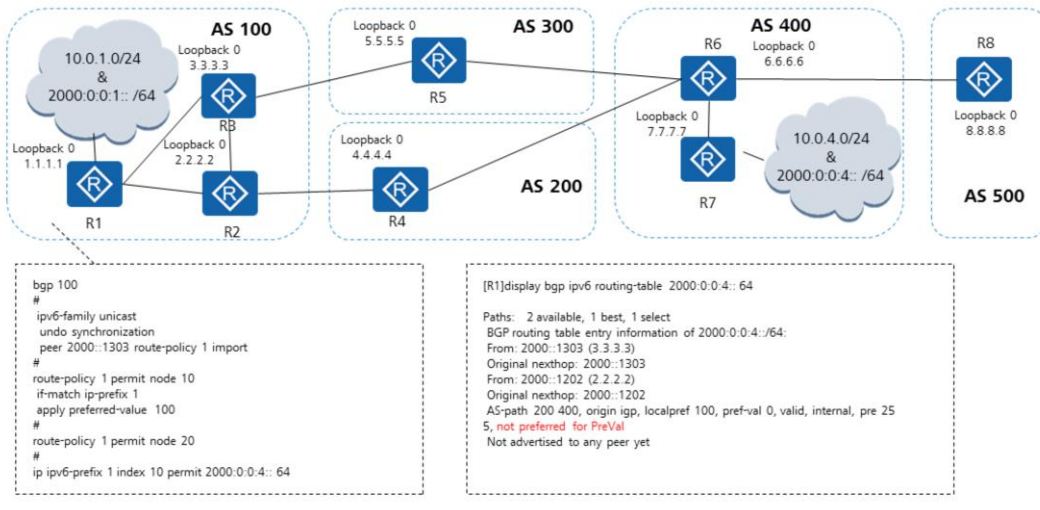
*>i  10.0.4.0/24   2.2.2.2                   100       0       200 400i
* i               3.3.3.3                   100       0       300 400i
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Топология такая же, как в базовой конфигурации BGP. Устанавливаются отношения соседства BGP.

Конфигурирование BGP: Атрибут PrefVal (2/2)



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

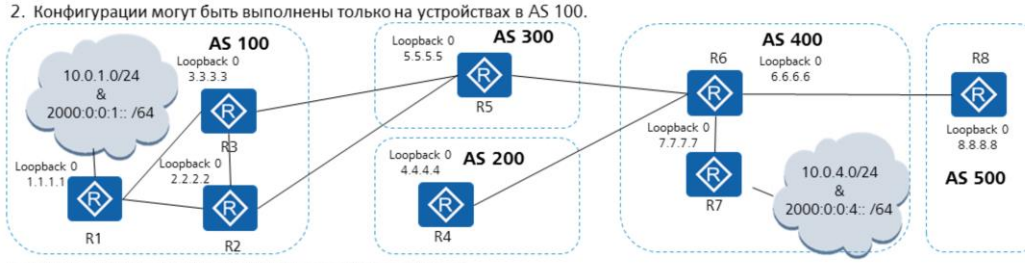
HUAWEI

- Описание команд:
  - Команда **peer route-policy** определяет политику маршрутизации для фильтрации маршрутов, полученных от соседа или группы соседей, или фильтрации маршрутов, которые должны быть анонсированы соседу или группе соседей.
  - Команда **apply preferred-value** устанавливает действие для изменения предпочтительного значения маршрутов BGP в политике маршрутизации.
- Использование команды:
  - Команда **peer route-policy** выполняется в режиме BGP.
- Описание параметров
  - peer ipv4-address route-policy route-policy-name {import | export}
    - ipv4-address: указывает адрес IPv4 соседа.
    - route-policy-name: определяет имя политики маршрутизации.
    - import: применяет политику маршрутизации к маршрутам, полученным от соседа или группы соседей.
    - export: применяет политику маршрутизации к маршруту, подлежащему анонсированию соседу или группе соседей.
    - preferred-value: определяет предпочтительное значение маршрутов BGP. При выборе маршрута предпочтение отдается маршруту BGP с самым большим предпочтительным значением. Значение является целым числом в диапазоне от 0 до 65535, а значение по умолчанию равно 0.
- Результат тестирования
  - С помощью команд **display bgp routing-table** и **display bgp ipv6 routing-table** вы можете посмотреть таблицу маршрутизации BGP.
  - **Меры предосторожности**
  - Предпочтительным значением является собственный атрибут BGP, и эта команда

действует только на маршрутах BGP. Предпочтительное значение указывает вес маршрута BGP при выборе маршрута BGP. Он не является стандартным атрибутом, описанным в стандарте RFC, и действует только на локальном устройстве. Предпочтительное значение неприменимо к экспортной политике BGP.

Конфигурирование BGP: атрибут Local_Pref (1/2)

- Требования к конфигурации:
  1. Оба маршрута от R1 к адресам 10.0.4.0/24 и 2000: 0:0: 4:: / 64 в AS 400 последовательно проходят через маршрутизаторы R1, R3, R5, R6 и R7.
  2. Конфигурации могут быть выполнены только на устройствах в AS 100.



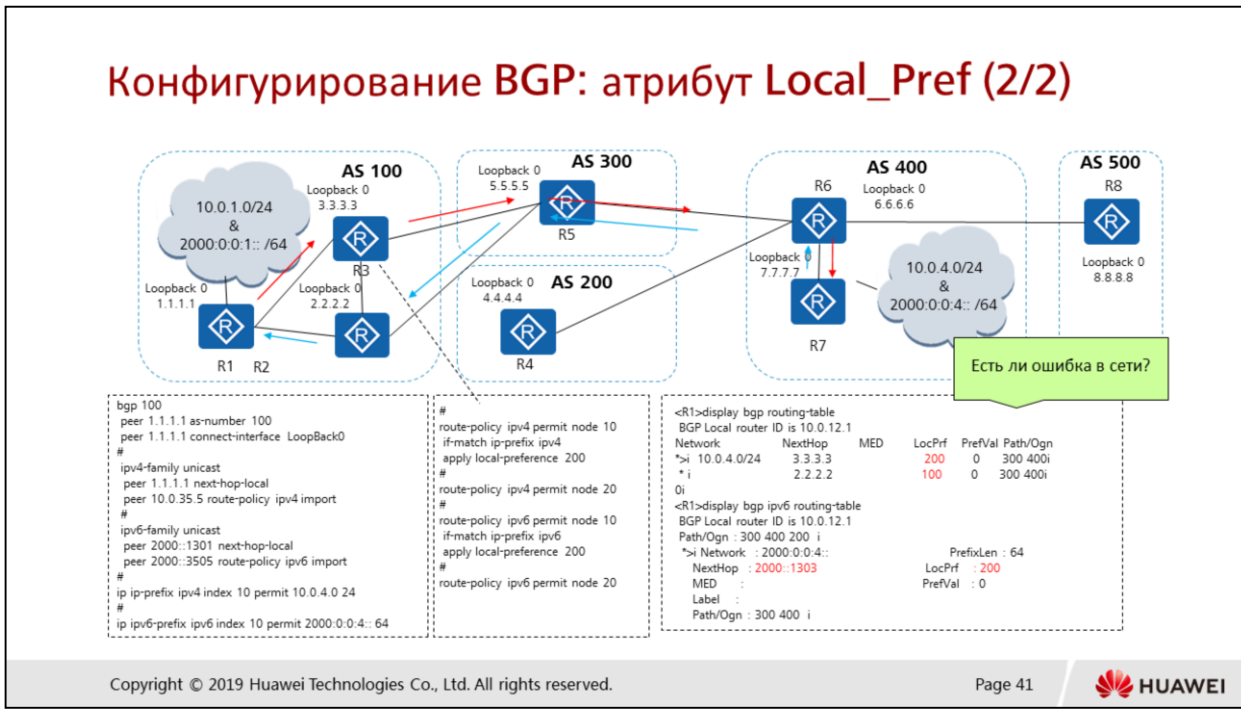

```
[R1]display bgp routing-table
Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

*>i  10.0.4.0/24     2.2.2.2                  100          0     300 400i
 * i                 3.3.3.3                  100          0     300 400i
[R1]display bgp ipv6 routing-table

 *>i Network  : 2000:0:0:4::                 PrefixLen : 64
     NextHop  : 2000::1202                   LocPrf    : 100
     MED      :                              PrefVal   : 0
     Label    :
     Path/Ogn : 300 400  i
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

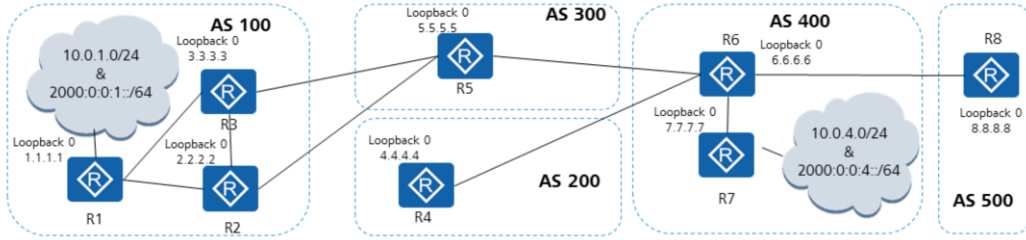
- Топология такая же, как в базовой конфигурации BGP. Устанавливаются отношения соседства BGP.



- Описание команды:
  - Команда **apply local-preference preference** устанавливает локальный приоритет маршрута BGP.
  - Описание параметров:
  - Предпочтения: определяет локальный приоритет маршрута BGP. Значение – целое число в диапазоне от 0 до 4294967295. Значение по умолчанию – 100.
- **Меры предосторожности**
  - Когда политика маршрутизации вступает в силу, она влияет на выбор маршрута BGP.
  - Атрибут Local_Pref применяется к выбору маршрута в AS и не анонсируется за пределы AS. В этом случае команда **apply local-preference** не действует, когда сконфигурирована политика экспортной маршрутизации для соседей EBGP.

Конфигурирование BGP: Атрибут MED (1/2)

- Требования к конфигурации:
  1. Проблема в сети, возникшая при конфигурировании атрибута Local-Pref, решена.
  2. Конфигурации могут выполняться только на устройствах в AS 100.




```
<R5>display bgp routing-table
Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

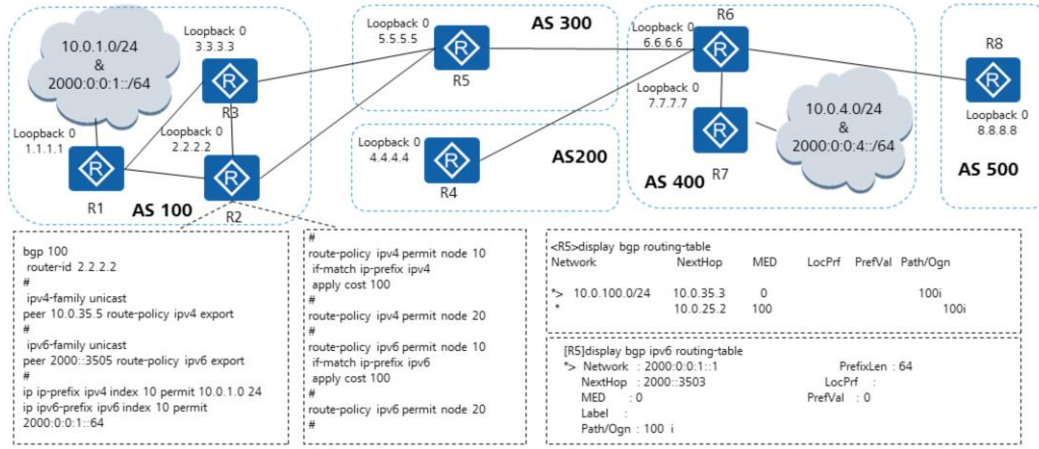
*> 10.0.100.0/24   10.0.25.2                 0         100i
*                  10.0.35.3                 0         100i
```

```
[R5]display bgp ipv6 routing-table
*> Network  : 2000:0:0:1::1                PrefixLen : 64
   NextHop  : 2000::2502                   LocPrf    :
   MED      : 0                            PrefVal   : 0
   Label    :
   Path/Ogn : 100  i
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Чтобы решить проблему несоответствия входящих и исходящих маршрутов трафика, вы можете сконфигурировать маршрутизатор R2 так, чтобы он анонсировал маршруты с более высоким значением атрибута MED, и в результате маршрутизатор R5 выбирал маршруты, анонсированные R3.

Конфигурирование BGP: Атрибут MED (2/2)



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

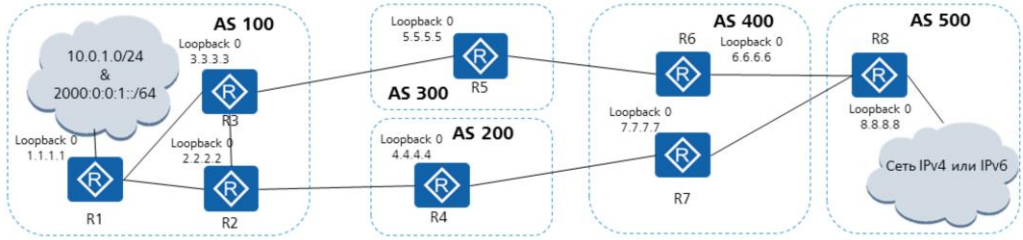
HUAWEI

- Описание команды:
  - Команда **apply cost [+ | -]** cost устанавливает действие изменения стоимости маршрутов в политике маршрутизации.
  - Описание параметров:
  - +: увеличивает стоимость маршрута.
  - -: снижает стоимость маршрута.
  - cost: определяет стоимость маршрута. Для контроля выбора маршрута вам необходимо изменить стоимость маршрута на определенное значение для предотвращения петель маршрутизации.
  - **Меры предосторожности**
- По умолчанию BGP сравнивает значения атрибутов MED маршрутов, которые поступают из одной AS, за исключением подсистем AS в конфедерации. Чтобы разрешить BGP сравнивать значения атрибутов MED маршрутов в конфедерации при выборе оптимального маршрута, выполните команду **bestroute med-confederation**.
- После выполнения команды **bestroute med-confederation** BGP сравнивает значения атрибутов MED только в том случае, если AS_Path не содержит номер внешней AS (не входящей в конфедерацию).
  - Например, автономные системы AS 65000, 65001, 65002 и 65004 принадлежат одной конфедерации. Маршруты к одному и тому же пункту назначения перечислены ниже:
    - path1: AS_Path = 65000 65004, MED = 2
    - path2: AS_Path = 65001 65004, MED = 3
    - path3: AS_Path = 65002 65004, MED = 4
    - path4: AS_Path = 65003 65004, MED = 1
- После запуска команды **bestroute med-confederation** атрибуты AS_Path путей 1, 2 и 3 не содержат номеров AS, принадлежащих другим конфедерациям, но атрибут AS_Path пути 4

содержит номер AS, принадлежащий другой конфедерации. Поэтому при выборе маршрутов на основе значений атрибута MED, BGP сравнивает значения MED только для путей 1, 2 и 3.

Конфигурирование BGP: атрибут AS_Path 1 (1/2)

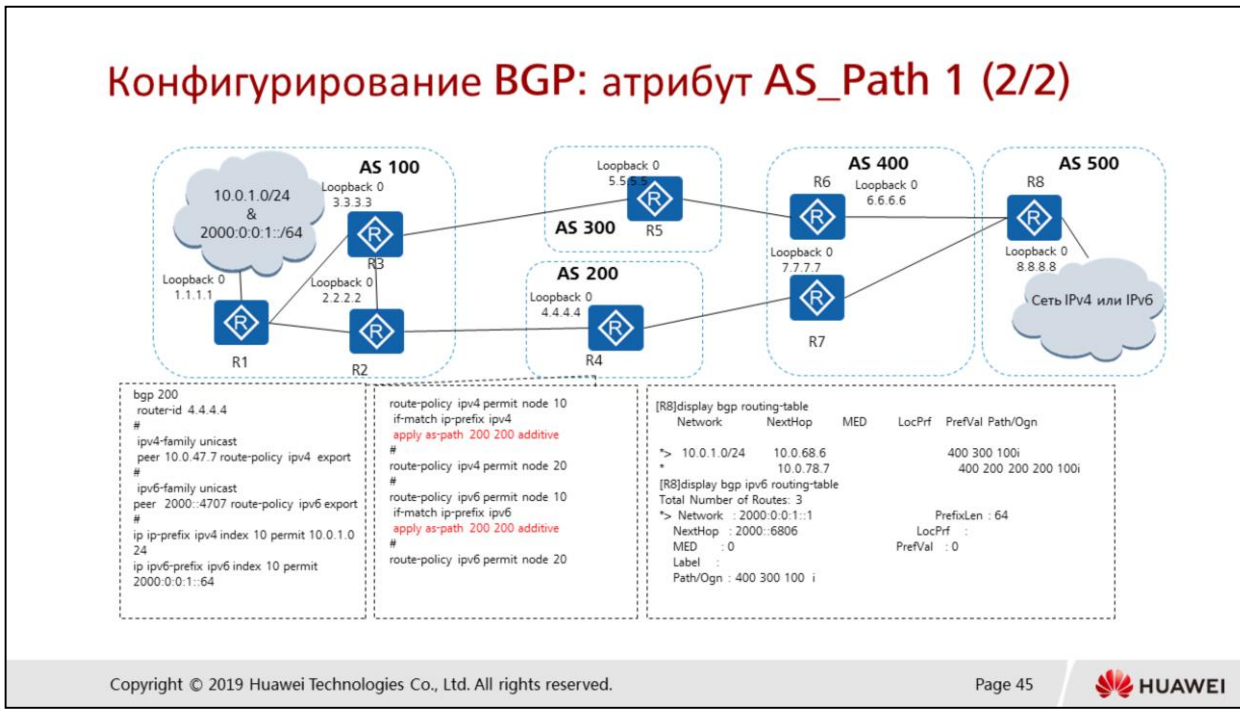
- Требования к конфигурации
  1. Пользователи в AS 500 должны предварительно выбрать маршрут, проходящий через AS 300 к AS 100.
  2. Конфигурации могут быть выполнены только на маршрутизаторе в AS 200.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Топология и конфигурации являются такими же, как в базовой конфигурации BGP. Установлены базовые отношения соседства BGP.

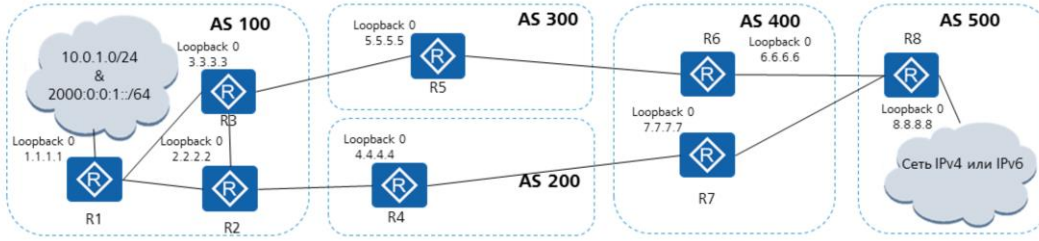


- Описание команды:
  - **apply as-path** { { as-number-plain | as-number-dot } &<1-10> { additive } | none overwrite }
- Описание параметров:
  - *as-number-plain:* определяет номер AS в виде целого числа для добавления в список AS_Path или замены номера AS в существующем списке AS_Path. В одной команде может быть указано не более 10 номеров AS.
  - *as-number-dot:* указывает номер AS в виде числа с точкой для добавления в список AS_Path или замены номера AS в существующем списке AS_Path. В одной команде может быть указано не более 10 номеров AS.
  - **additive:** добавляет указанный номер AS в существующий список AS_Path.
  - **overwrite:** заменяет номер AS в существующем списке AS_Path на указанный номер AS.
  - **None:** очищает существующий список AS _ Path.
- **Меры предосторожности**
  - Когда политика маршрутизации вступает в силу, она влияет на выбор маршрута BGP.
  - Команда **apply as-path** изменяет путь, через который проходит сетевой трафик, или создает петли маршрутизации и вызывает неверный выбор маршрута. Используйте эту команду только в том случае, если вы знакомы с

топологией сети и влиянием команды на услуги.

Конфигурирование BGP: атрибут AS_Path 2 (1/2)

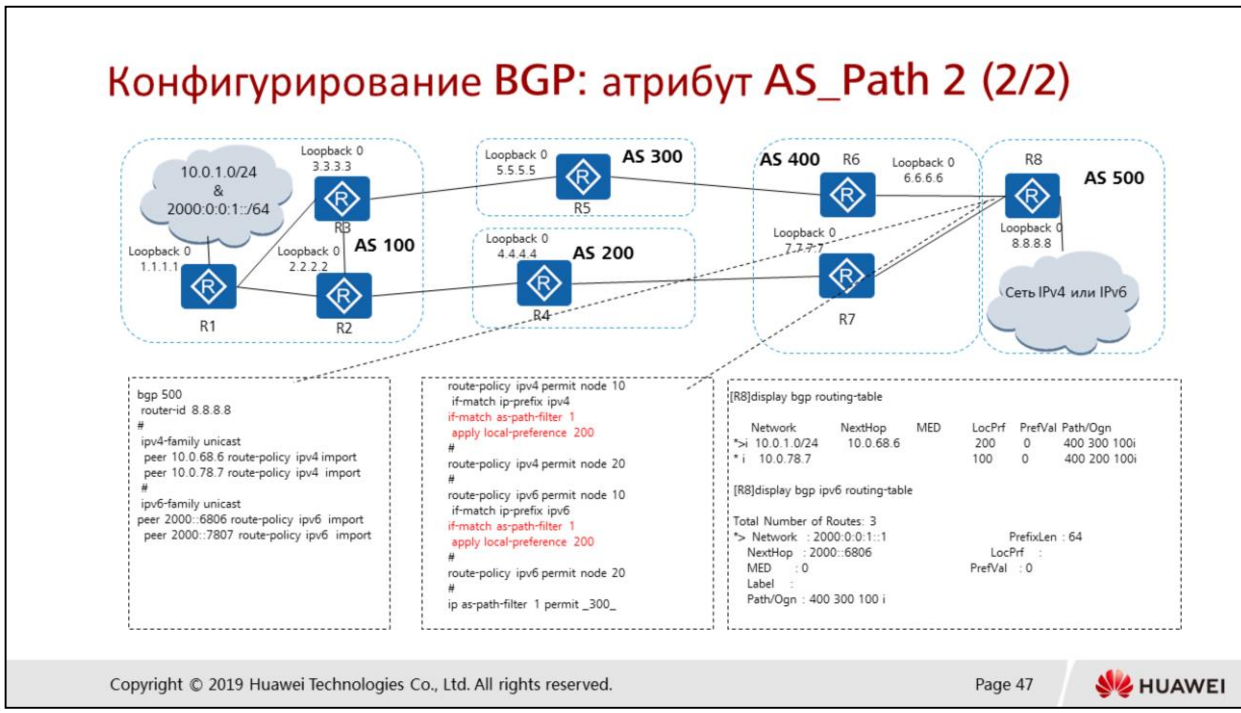
- Требования к конфигурации
  1. Пользователи в AS 500 должны предварительно выбрать маршрут, проходящий через AS 300 до AS 100.
  2. Конфигурации могут быть выполнены только на маршрутизаторе в AS 500.
  3. Маршрутизатор в AS 500 не знает топологии всей сети.



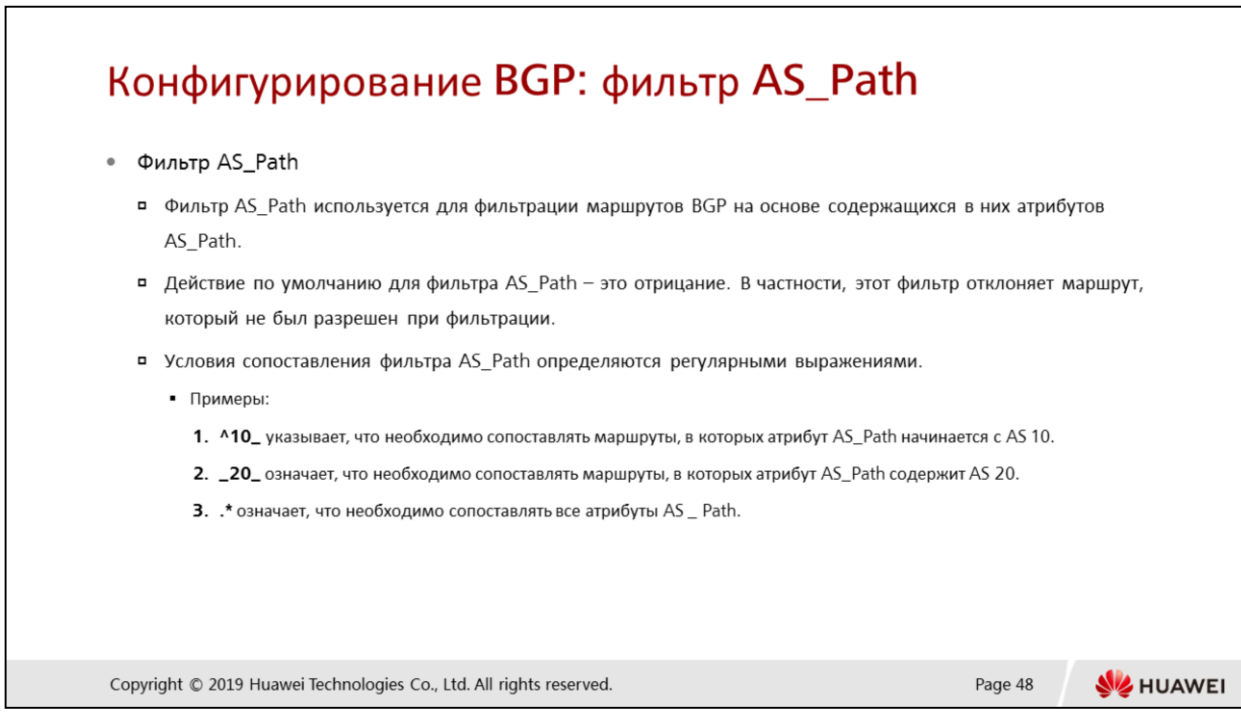
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Топология и конфигурации такие же, как в базовой конфигурации BGP. Установлены базовые отношения соседства BGP.



- Описание команды:
  - **if-match as-path-filter** { as-path-filter-number &<1-16> | as-path-filter-name }
- Описание параметров:
  - as-path-filter-number: указывает номер фильтра AS_Path. Значение – целое число в диапазоне от 1 до 256. В команде может быть указано не более 16 фильтров AS_Path.
  - *as-path-filter-name:* определяет имя фильтра AS_Path. Значение представляет собой строку из 1-51 чувствительных к регистру символов, пробелы не поддерживаются. Строка не может состоять из одних цифр.
- **Меры предосторожности**
  - В команде может быть указано не более 16 фильтров AS_Path. Взаимосвязь между этими фильтрами AS_Path устанавливается по типу OR. В частности, если у маршрута есть совпадение с одним из этих фильтров AS_Path, он соответствует правилам команды.



- **Описание команды:**
  - Команда **ip as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } { **deny** | **permit** } *regular-expression* создает фильтр AS_Path.
- Описание параметров:
  - as-path-filter-number: указывает номер фильтра AS_Path. Значение – целое число в диапазоне от 1 до 256.
  - *as-path-filter-name:* определяет имя фильтра AS_Path. Значение представляет собой строку из 1-51 чувствительных к регистру символов, пробелы не поддерживаются. Строка не может состоять из одних цифр. Пробелы допускаются только в том случае, если строка заключена в двойные кавычки ("").
  - deny: устанавливает действие отрицания для фильтра AS_Path.
  - permit: устанавливает действие разрешения для фильтра AS_Path.

Конфигурирование BGP: Регулярные выражения для фильтров AS_Path (1/2)

Специальный символ	Функция	Пример
\	Символ escape. Он преобразует специальный или стандартный символ, следующий за ним, в стандартный символ.	* соответствует звездочке (*).
^	Соответствует началу строки.	^10 соответствует "10,20,30", "100,200,300" и т.д.
$	Соответствует концу строки.	1$ соответствует 101, 11 и т.д.
*	Обозначает от нуля до сколько угодно символов, указанных перед звездочкой	10* соответствует 1, 10, 100, 1000 и т.д. (10)* соответствует нулю, 10, 1010, 101010 и т.д.
+	Указывает на то, что регулярное выражение перед звездочкой (*) встречается 1 или более раз	10+ соответствует 10, 100, 1000 и т.д. (10) + соответствует 10, 1010, 10101 и т.д.
?	Указывает на то, что регулярное выражение перед звездочкой (*) встречается 0 или 1 раз	10? соответствует 1 или 10. (10)? соответствует нулю или 10.
.	Соответствует любому единственному символу.	.0 соответствует 20, 30 и т.д.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

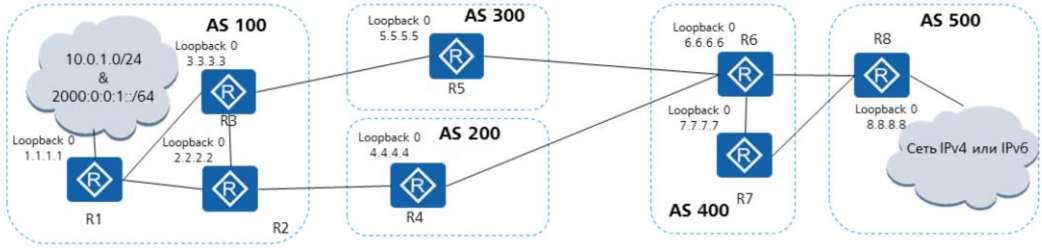
Конфигурирование BGP: Регулярные выражения для фильтров AS_Path (2/2)

Специальный символ	Функция	Пример
()	Определяет выражение, которое может быть пустым. Выражение в скобках должно совпадать с самим собой.	100 (2) + соответствует 1002 и 10022.
_	Соответствует регулярным выражениям со специальным символом, таким как запятая (,), левая фигурная скобка ({), правая фигурная скобка (}), левая круглая скобка ((), правая круглая скобка ()) или пробел. Специальные символы могут использоваться в начале регулярного выражения с той же функцией, что и символ вставки (^) или в конце регулярного выражения с той же функцией, что и знак доллара ($).	_ 65001 _ соответствует 65001, 20 65001, 65001 30, 65001 и т.д.
x|y	Соответствует x или y.	100 | 200 соответствует 100 или 200. 1 (2 | 3) 4 соответствует 124 или 134.
[xyz]	Соответствует любому символу, содержащемуся в регулярном выражении.	[123] соответствует символу 2 в 255.
[^xyz]	Соответствует любым символам, за исключением тех, которые перечислены в регулярном выражении.	[^123] соответствует любому символу, за исключением 1, 2 и 3.
[a-z]	Соответствует любому символу в пределах указанного диапазона.	[0-9] соответствует любому символу в диапазоне от 0 до 9.
[^a-z]	Соответствует любому символу за пределами указанного диапазона.	[^ 0-9] соответствует всем нечисловым символам.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Конфигурирование BGP: Балансировка нагрузки (1/2)

- Требования к конфигурации
  1. Маршрутизатор в AS 500 может получить доступ к AS 100 через два канала.
  2. Конфигурации могут быть выполнены только на маршрутизаторе в AS 500.

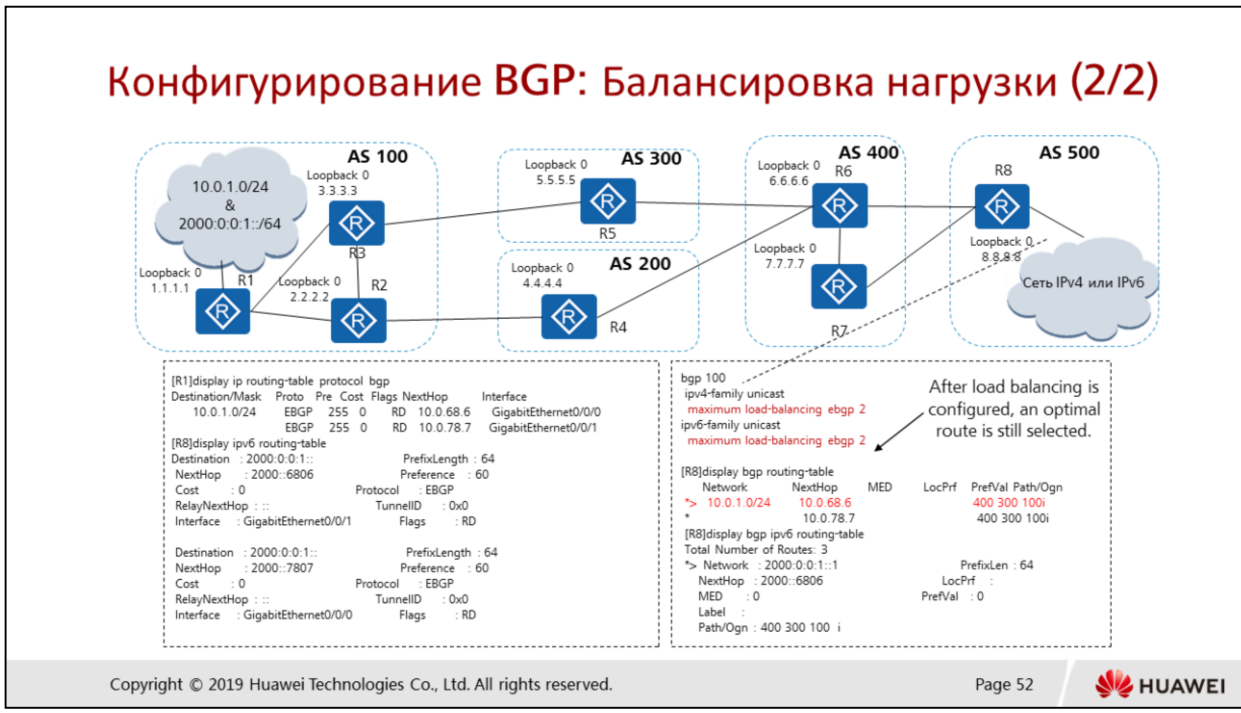



```
[R8]display ip routing-table protocol bgp
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
      10.0.1.0/24   EBGP    255  0           RD  10.0.68.6       GigabitEthernet0/0/0

[R8]display ipv6 routing-table protocol bgp
 Destination  : 2000:0:0:1::                PrefixLength : 64
 NextHop      : 2000::6806                  Preference   : 255
 Cost         : 0                           Protocol     : EBGP
 RelayNextHop : ::                          TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0        Flags        : D
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Топология и конфигурации такие же, как в базовой конфигурации BGP. Установлены базовые отношения соседства BGP.



- Описание команды:
  - Команда **maximum load-balancing** конфигурирует максимальное количество маршрутов с одинаковой стоимостью для балансировки нагрузки.
- Использование команды:
  - Команда **maximum load-balancing** выполняется в режиме BGP.
- Описание параметров:
  - ebgp: только маршруты EBGP участвуют в балансировке нагрузки.
  - ibgp: только маршруты IBGP участвуют в балансировке нагрузки.
  - number: указывает максимальное количество маршрутов с одинаковой стоимостью в таблице маршрутизации BGP.

- Меры предосторожности:
  - Команда **maximum load-balancing number** не может быть сконфигурирована вместе с командой **maximum load-balancing ebgp number** или командой **maximum load-balancing ibgp number**.
  - Для балансировки нагрузки могут использоваться маршруты, имеющие одинаковую длину AS_Path и последовательность AS_Path. Команда **load-balancing as-path-ignore** не позволяет маршрутизатору сопоставлять атрибуты AS_Path маршрутов при выборе маршрутов для балансировки нагрузки.

- Результат тестирования:
    - Выполнив команду **display ip routing-table protocol bgp,** вы можете посмотреть маршруты с одинаковой стоимостью, полученные через BGP.

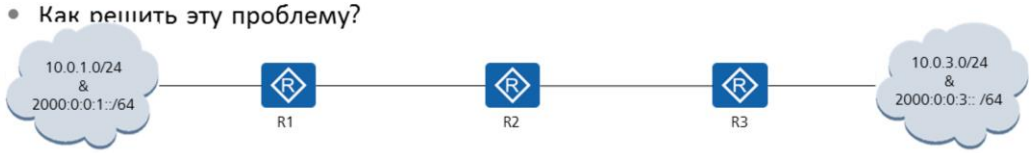
Содержание

1. Принципы работы BGP
2. Принципы работы BGP4+
3. Основные конфигурации BGP и BGP4+
4. Диагностика неисправностей BGP

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Ошибка BGP

- Между маршрутизаторами R1 и R2 и маршрутизаторами R2 и R3 установлены отношения соседства BGP.
- После выполнения конфигураций сети, подключенные к маршрутизаторам R1 и R3, не могут взаимодействовать друг с другом.
- Как решить эту проблему?



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Поиск и устранение неисправностей BGP (1/3)

- Предположим, что неисправность вызвана настройками BGP:
  - Если отношения соседства BGP не могут перейти в состояние Established, это означает, что:
    - Протокол IGP недоступен.
    - Список ACL сконфигурирован для фильтрации пакетов, портом назначения которых является TCP-порт 179.
    - ID соседнего маршрутизатора конфликтует с ID локального маршрутизатора.
    - Номер AS соседа некорректный.
    - Loopback-интерфейсы используются для установления отношений соседства BGP, но команда **peer connect-interface** не настроена.
    - Команда **peer ebgp-max-hop** не настроена, когда установлены отношения соседства EBGP.
    - Конфигурации команды **peer valid-ttl-hops** некорректны.
    - Количество маршрутов, отправленных удаленным маршрутизатором, превышает верхний предел, сконфигурированный с помощью команды **peer route-limit**.
    - Команда **peer ignore** сконфигурирована на соседе.
    - Семейства адресов устройств на обоих концах не совпадают.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Поиск и устранение неисправностей BGP (2/3)

- Если отношения соседства BGP установлены корректно, но таблица маршрутизации BGP не содержит эту запись маршрута, проверьте:
  - Доступен ли адрес следующего узла.
  - Сконфигурирована ли политика управления на входе.
  - Есть ли ограничения по получению префиксов маршрутов.
  - Сконфигурирована ли политика на выходе соседа.
  - Является ли префикс оптимальным в таблице маршрутизации BGP.
  - Сконфигурирована ли команда **active-route-advertise** на соседе.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Поиск и устранение неисправностей BGP (3/3)

- Если отношения соседства BGP установлены корректно, но некоторые записи в таблице маршрутизации BGP не являются оптимальными, проверьте:
  - Какие записи не являются оптимальными в соответствии с правилами выбора маршрута.
  - Подавлены ли маршруты с определенными префиксами.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.



Тест

1. BGP выполняет согласование возможностей семейства адресов в сообщениях Open.
   A. Верно
   B. Неверно

2. Если у маршрутов одинаковая длина AS_Path, но разные последовательности AS_Path, это не влияет на балансировку нагрузки.
   A. Верно
   B. Неверно

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Ответы:
  - Верно.
  - Неверно. Для балансировки нагрузки могут использоваться только маршруты с одинаковой длиной AS_Path и последовательностью AS_Path.

Краткое содержание

- Принципы работы протоколов BGP4 и BGP4+
  - Принципы работы протокола BGP
  - Атрибуты и функции протокола BGP
  - Принципы работы и атрибуты протокола BGP4+
- Конфигурация протоколов BGP4 и BGP4+
  - Команды конфигурирования на устройствах Huawei
  - Конфигурации в различных сценариях
- Поиск и устранение неисправностей в BGP
  - Процесс поиска и устранения неисправностей в BGP

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Спасибо!

www.huawei.com

HCIE-R&S

Расширенные функции протокола BGP и Интернет

www.huawei.com

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Введение

- Расширенные функции и технологии протокола граничного шлюза (BGP)
- Использование функций и технологий BGP для повышения производительности сети
- Устранение возможных проблем в сети BGP

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Цели

- По окончании этого курса вы будете знать:
  - Основные инструменты и технологии BGP в сетях с большим количеством маршрутов.
  - Расширенные функции BGP.
  - Концепцию построения сети Интернет.
  - Принципы конфигурирования атрибутов BGP и устранения неполадок.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Содержание

- **Технологии для работы с большим количеством маршрутов BGP**
- Расширенные функции BGP
- Улучшенные функции BGP
- Основы проектирования интернет-сети
- Устранение неполадок в BGP-сети

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

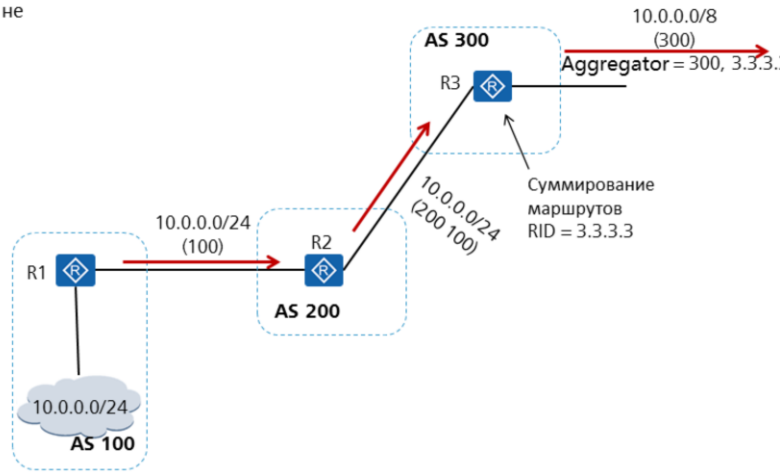
Технологии для работы с большим количеством маршрутов BGP

- Следующие инструменты и технологии используются для упрощения конфигураций, сокращения маршрутов и повышения производительности устройств в крупномасштабных сетях или сетях с большим количеством маршрутов:
  - Суммирование маршрутов
  - Создание групп соседей
  - Атрибуты Community
  - Отражение маршрутов (Route reflection)
  - Конфедерация BGP (BGP confederation)

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Суммирование маршрутов

- Суммирование маршрутов
  - Соседям будут анонсированы суммарные, а не отдельные маршруты, чтобы уменьшить их таблицы маршрутизации.
  - Если один маршрут нестабилен, вычисление маршрута BGP-соседа не запускается.
  - Существует два варианта суммирования маршрутов: автоматическое и административное.
    - Маршруты IPv4:
      - Административное суммирование
      - Автоматическое суммирование
    - Маршруты IPv6:
      - Административное суммирование



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- В крупномасштабной сети таблица маршрутизации BGP имеет огромный размер, в результате чего значительно увеличивается нагрузка на устройство, повышается вероятность нестабильности маршрутов и снижается стабильность сети.

- Суммирование маршрутов – это механизм, который объединяет несколько маршрутов в один. За счет этого механизма размер таблицы маршрутизации уменьшается, поскольку соседям анонсируются только суммированные, а не отдельные маршруты. Если суммарный маршрут становится нестабильным, это не оказывает негативного воздействия на сеть, поэтому стабильность сети повышается.

- Атрибут Aggregator (необязательный переходный) используется для суммирования маршрутов. Этот атрибут идентифицирует узел, на котором суммируются маршруты, и передает ID маршрутизатора и номер AS узла.

Автоматическое суммирование маршрутов

- Автоматическое суммирование маршрутов
  - Суммирование маршрутов, импортируемых BGP, на основе классов.
  - Подавление анонсирования отдельных маршрутов после суммирования.
  - Суммирование маршрутов, которые BGP импортирует по типам протоколов (**import-route**), а не префиксам или маскам (**network**).

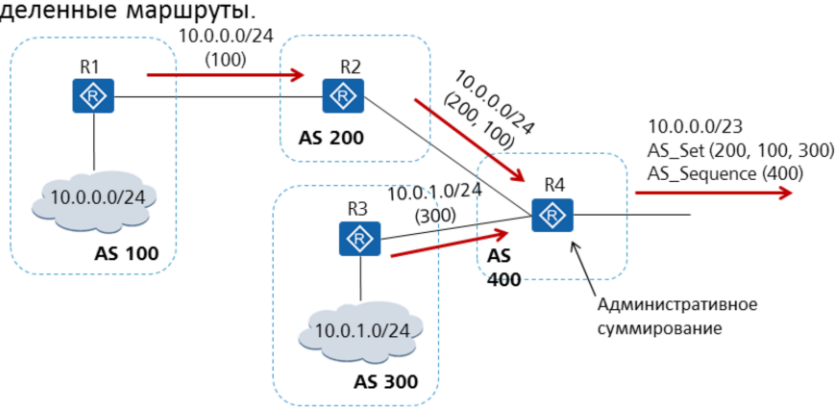


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Меры предосторожности при автоматическом суммировании
  - Эта команда суммирует маршруты, импортированные BGP. Импортированными маршрутами могут быть прямые маршруты, статические маршруты, маршруты OSPF и маршруты IS-IS. При включении суммирования маршрутов BGP суммирует маршруты каждого естественного сегмента сети в один маршрут. Информация об отдельных маршрутах больше не передается в сообщениях BGP Update. Данная команда применяется к маршрутам, импортированных с помощью команды network.
  - BGP анонсирует соседям только суммированные маршруты.
  - Автоматическое суммирование отключено в BGP по умолчанию.
  - Суммарный маршрут содержит атрибуты Atomic_Aggregate и Aggregator.

Административное суммирование маршрутов (1/2)

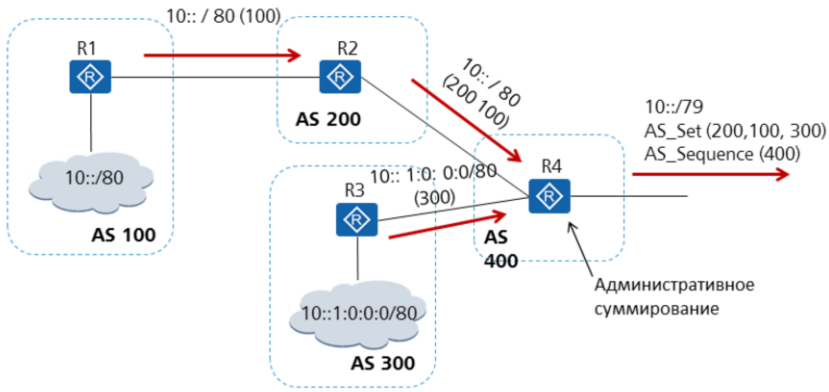
- Административное суммирование маршрутов
  - Суммирование маршрутов в локальной таблице маршрутизации BGP. BGP управляет атрибутами суммированных маршрутов и определяет, следует ли анонсировать определенные маршруты.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Административное суммирование
  - Вы можете выполнить команду, чтобы определить, следует ли подавлять конкретные маршруты. После подавления суммарные маршруты включают в себя атрибут Atomic_Aggregate.
  - Суммарный маршрут не включает атрибуты AS-Path конкретных маршрутов.
  - Атрибут AS_Set используется, чтобы передавать номер AS для предотвращения петель. Разница между атрибутами AS_Set и AS_Sequence заключается в следующем: атрибут AS_Set – это неупорядоченный список номеров AS, используемый для суммирования маршрутов. Атрибут AS_Sequence – это упорядоченный список номеров AS. Каждый раз, когда сообщение проходит через AS, к нему добавляется номер AS. Номера AS перечислены в порядке убывания.

Административное суммирование маршрутов (2/2)



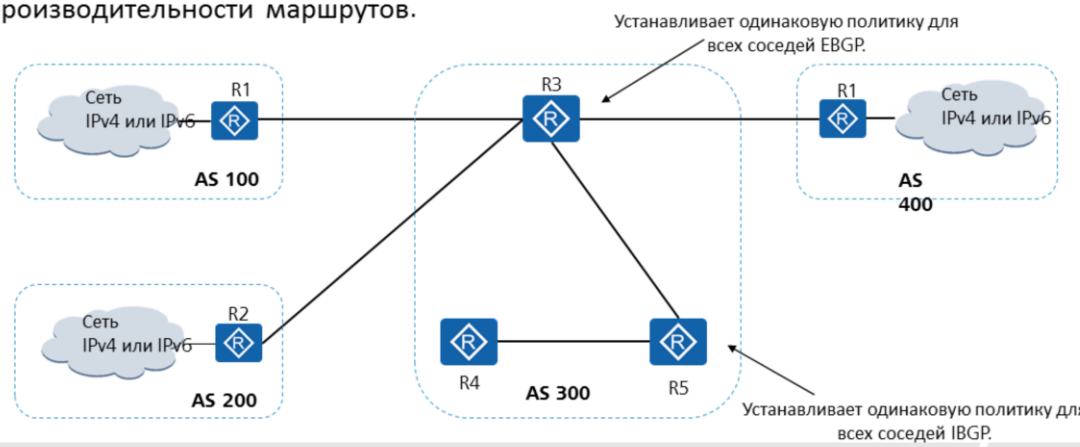
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Административное суммирование
  - Вы можете выполнить команду, чтобы определить, следует ли подавлять конкретные маршруты. После подавления суммарные маршруты включают в себя атрибут Atomic_Aggregate.
  - Суммарный маршрут не включает атрибуты AS-Path конкретных маршрутов.
  - Атрибут AS_Set используется, чтобы передавать номер AS для предотвращения петель. Разница между атрибутами AS_Set и AS_Sequence заключается в следующем: атрибут AS_Set – это неупорядоченный список номеров AS, используемый для суммирования маршрутов. Атрибут AS_Sequence – это упорядоченный список номеров AS. Каждый раз, когда сообщение проходит через AS, к нему добавляется номер AS. Номера AS перечислены в порядке убывания.

Группа соседей (Peer group)

- Выполняется настройка группы соседей с одинаковой политикой.
- За счет этого упрощается конфигурация BGP и снижается потеря производительности маршрутов.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

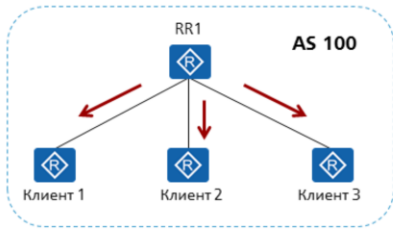
- Выполняется настройка группы соседей с одинаковой политикой. Когда в группу добавляется сосед, он получает такую же конфигурацию, как у группы. Если конфигурация группы соседей меняется, конфигурации членов группы также меняются.

- В крупномасштабной сети BGP существует большое количество соседей, у многих из которых одинаковая политика. При конфигурировании таких соседей некоторые команды используются много раз. В этой ситуации для упрощения работы можно настроить группу соседей.

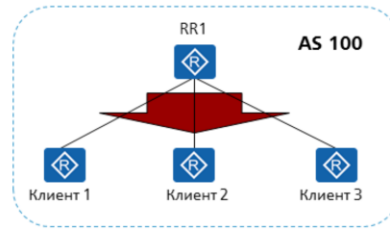
- Сосед в группе соседей может иметь собственную политику в отношении анонсирования и приема маршрутов.

Функция динамического обновления группы соседей

- Динамическое обновление группы соседей BGP
  - Функция динамического обновления определяет всех соседей BGP с одинаковой политикой экспорта в группу обновления соседей.
  - Каждый маршрут, который подлежит анонсированию, группируется один раз и затем анонсируется всем соседям в группе обновления.



Функция динамического обновления отключена



Функция динамического обновления включена

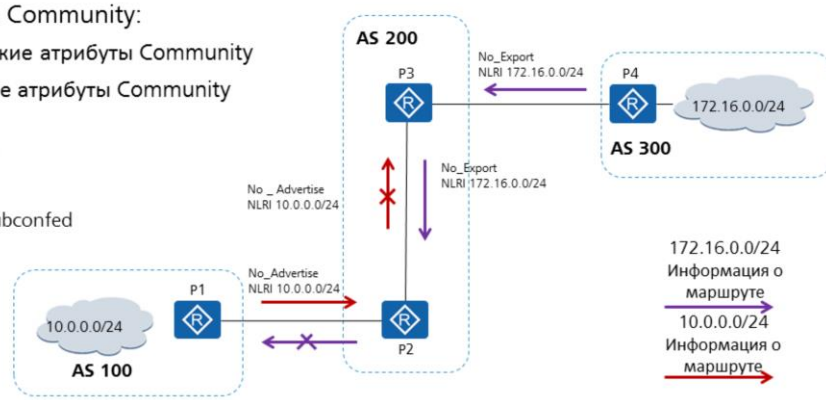
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Динамическое обновление групп соседей BGP
  - По умолчанию BGP группирует маршруты для каждого соседа (даже если у соседей одинаковая политика экспорта).
  - После соседям в группе обновления, за счет включения функции динамического обновления каждый маршрут, который должен быть анонсирован, группируется только один раз, а затем анонсируется всем чего увеличивается эффективность группировки.
- Описание топологии
  - У отражателя (RR) есть три клиента, и ему необходимо отразить 100 000 маршрутов. Если отражатель группирует маршруты для каждого соседа, то в общей сложности маршруты группируются 100 000 x 3 раз до того, как отражатель анонсирует маршруты трем клиентам. Функция динамического обновления уменьшает общее количество группировки маршрутов до 100 000 x 1, за счет чего производительность повышается в три раза.

Характеристики атрибутов BGP — атрибут Community

- Атрибут community используется для идентификации маршрутов BGP с одинаковыми характеристиками. Этот атрибут является дополнительным переходным.
  - Типы атрибутов Community:
    - Пользовательские атрибуты Community
    - Общеизвестные атрибуты Community
      - Internet
      - No_Advertise
      - No_Export
      - No_Export_Subconfed



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Атрибут Community – общеизвестные атрибуты

- Атрибут community представляет собой список, состоящий из 4 байт:
  - aa:nn: целые числа от 0 до 65535.
  - Номер атрибута Community: целое число от 0 до 4294967295.
  - Согласно RFC 1997, диапазоны от 0 (0x00000000) до 65535 (0x0000FFFF) и от 4294901760 (0xFFFF0000) до 4294967295 (0xFFFFFFFF) зарезервированы.

Название атрибута community	Идентификатор атрибута community	Описание
Internet	0 (0x00000000)	По умолчанию все маршруты имеют атрибут Internet community. Маршруты с этим атрибутом могут быть анонсированы всем соседям BGP.
No_Export	4294967041 (0xFFFFFF01)	Если полученный маршрут имеет этот атрибут, его можно анонсировать в локальной AS, не на за ее пределами.
No_Advertise	4294967042 (0xFFFFFF02)	Если полученный маршрут имеет этот атрибут, его нельзя анонсировать другим соседям BGP.
No_Export_Subconfed	4294967043 (0xFFFFFF03)	Если полученный маршрут имеет этот атрибут, его нельзя анонсировать за пределами локальной AS или другим подсистемам AS.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

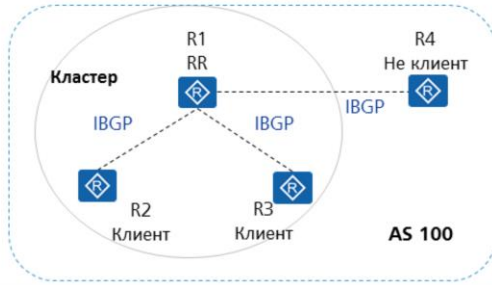
HUAWEI

- Атрибут community представляет собой набор адресов назначения с одинаковыми характеристиками. Атрибут community представляет собой список из 4 байт. На устройстве атрибут представлен в формате aa:nn или идентифицируется по номеру.
  - aa:nn: значения aa и nn являются целыми числами от 0 до 65535. Вы можете задать желаемое значение. Значение aa представляет собой номер AS, а значение nn представляет собой ID атрибута community, назначенный администратором. Например, если для маршрута из AS 100 администратор назначил ID атрибута community 1, атрибут community маршрута равен 100: 1.
  - Номер Community является целым числом от 0 до 4294967295. Согласно RFC 1997, диапазоны от 0 (0x00000000) до 65535 (0x0000FFFF) и 4294901760 (0xFFFF0000) до 4294967295 (0xFFFFFFFF) зарезервированы.
- Использование атрибута community упрощает применение политик маршрутизации, обслуживание сетей и управление сетями. Данный атрибут используется для того, чтобы группа устройств BGP в нескольких AS могла иметь одну политику. Данный атрибут является атрибутом маршрута. Он передается между соседями BGP и не ограничивается пределами AS. Перед анонсированием маршрута с атрибутом community соседям устройство BGP может изменить исходный атрибут community.
- Общеизвестные атрибуты community
  - Internet: по умолчанию все маршруты принадлежат интернет-сети. Маршруты с этим атрибутом могут быть анонсированы всем соседям BGP.
  - No_Advertise: если полученный маршрут имеет этот атрибут, его нельзя анонсировать другим соседям BGP.
  - No_Export: если полученный маршрут имеет этот атрибут, его нельзя анонсировать другим AS, за исключением локальной AS. Если используется конфедерация, то маршрут с этим атрибутом нельзя анонсировать вне конфедерации, но можно анонсировать другим подсистемам AS в конфедерации.

- No_Export_Subconfed: если полученный маршрут имеет этот атрибут, его нельзя анонсировать вне локальной AS или другим подсистемам AS в конфедерации.

Отражатель маршрутов

- Отражатель маршрутов (RR)
  - Маршруты, полученные от соседей IBGP, можно анонсировать определенным соседям IBGP. Это предотвращает путаницу в отношениях соседства IBGP и уменьшает количество IBGP-сессий.
  - Маршрутизаторы функционируют как отражатели и клиенты.



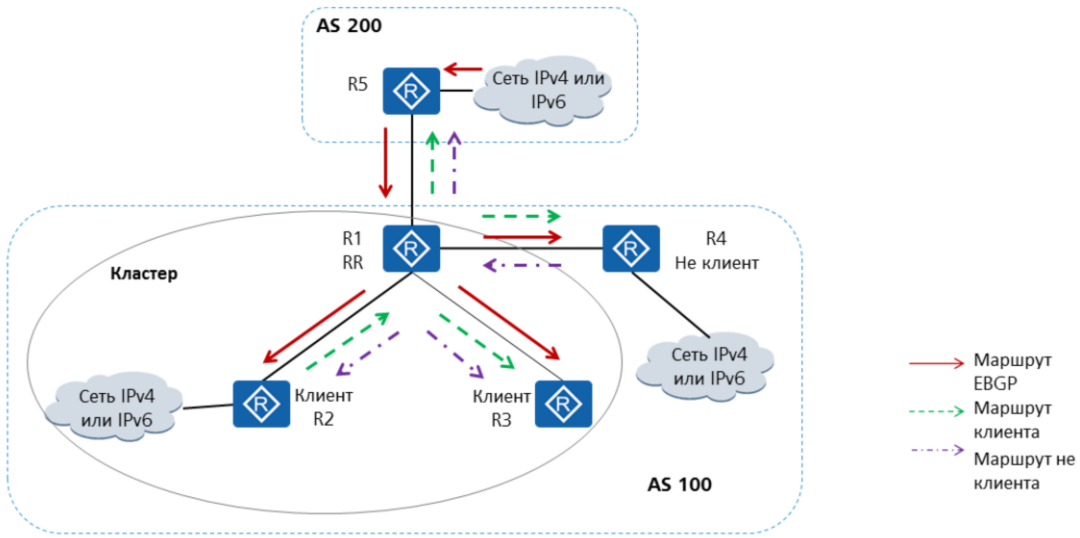
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Для создания соединения между соседями IBGP необходимо установить полносвязные соединения между соседями IBGP. Если в AS существует n маршрутизаторов, то количество подключений IBGP должно быть n x (n – 1)/2. При наличии большого числа соседей IBGP используются сетевые ресурсы и ресурсы ЦП. Этого можно избежать с помощью отражения маршрутов.
- В AS один или два маршрутизатора функционируют как отражатели, а другие маршрутизаторы – как клиенты. Между клиентом и каждым отражателем устанавливается соединение IBGP. Отражатель и его клиенты образуют кластер. Отражатель отражает маршрутную информацию между клиентами, и между клиентами не требуется устанавливать соединение BGP.
- Концепция отражателя маршрутов
  - Отражатель маршрутов (RR) отражает маршруты, полученные от соседа IBGP, другим соседям IBGP.
  - Клиент – это устройство IBGP, которое устанавливает отношения соседства с отражателем. Клиент в AS напрямую подключается к отражателю.
  - Не клиент – это устройство IBGP, которое не является ни отражателем, ни клиентом. Между не клиентами и отражателями в AS и между не клиентами необходимо установить полносвязные соединения.
  - Инициатор – это устройство, которое инициирует маршрут в AS. Атрибут Originator_ID используется для предотвращения возникновения петель маршрутизации в кластере.

- Кластер – это набор отражателей и их клиентов. Атрибут Cluster_List используется для предотвращения возникновения петель маршрутизации между кластерами.

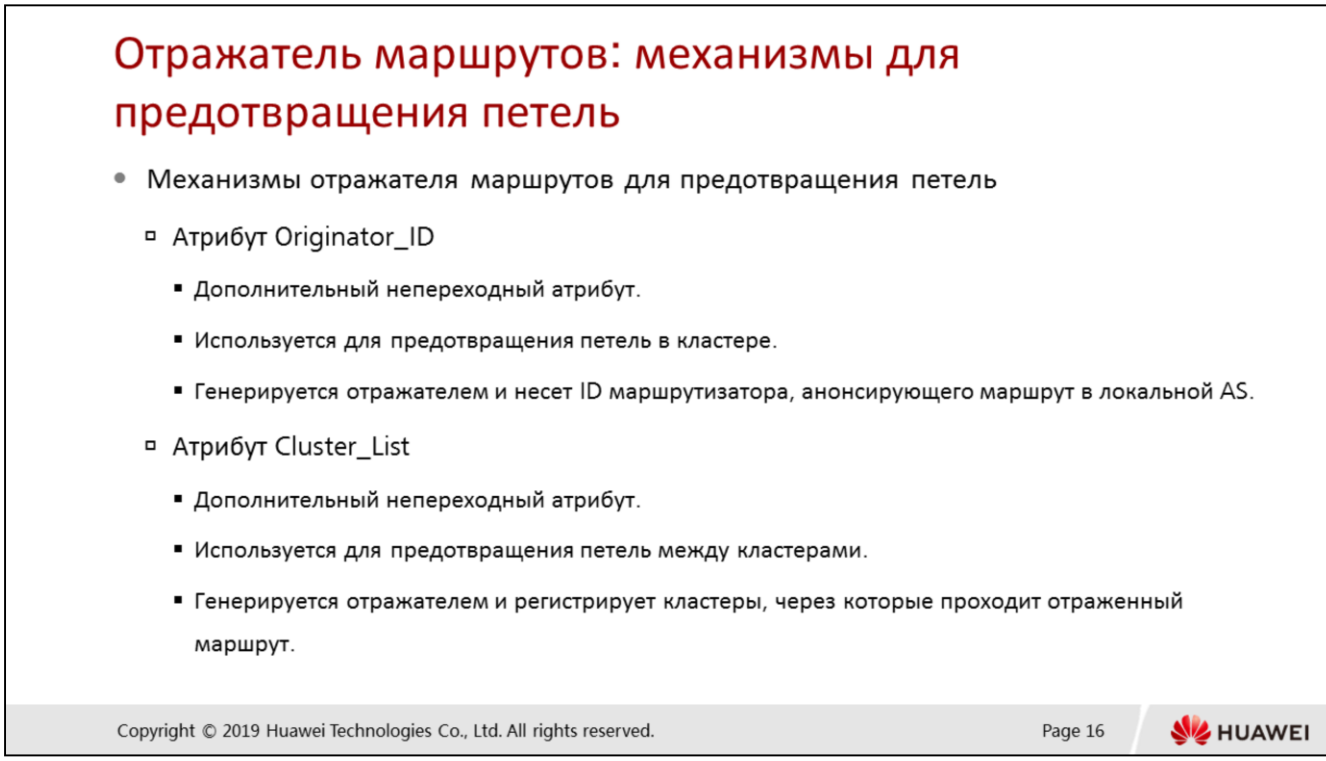
Отражатель маршрутов: правила отражения



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Отражатель использует следующие правила, чтобы анонсировать полученные маршруты соседям IBGP:
  - Маршруты, полученные от соседей EBGP, анонсируются всем не клиентам и клиентам.
  - Маршруты, полученные от соседей EBGP-не клиентов, анонсируются всем клиентам отражателя.
  - Маршрут, полученный от клиента, анонсируется всем не клиентам и другим клиентам отражателя (за исключением клиента, который анонсирует маршрут).
- Отражатель легко настроить. Необходимо настроить только маршрутизатор, который выполняет функции отражателя. Клиенту не нужно знать, что он является клиентом по конфигурации.
- В некоторых сетях между клиентами отражателя установлены полносвязные соединения, и они могут напрямую обмениваться информацией маршрутизации. В этом случае отражение маршрутов между клиентами не нужно и будет только тратить ресурсы полосы пропускания. VRP поддерживает команду undo reflect between-clients для отключения на отражателе функции отражения другим клиентам маршрутов, полученных от клиента.



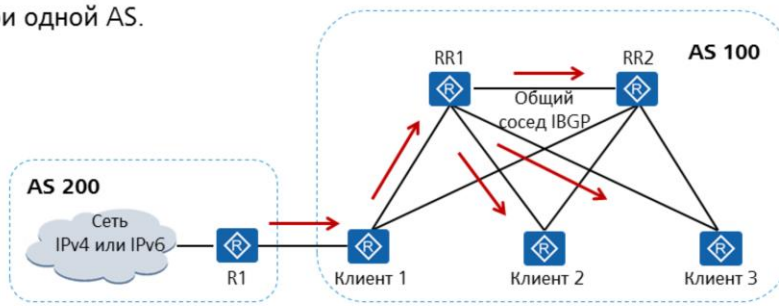
- Атрибут Originator_ID генерирует отражатель. Он содержит ID маршрутизатора, инициировавшего маршрут, чтобы предотвратить возникновение петель маршрутизации в кластере.
  - Если маршрут впервые отражен отражателем, отражатель добавляет атрибут Originator_ID к маршруту для идентификации устройства, инициировавшего маршрут. Если атрибут Originator_ID уже содержится в маршруте, отражатель не создает такой атрибут повторно.
  - При получении маршрута с атрибутом Originator_ID устройство сравнивает полученный ID маршрутизатора с локальным. Если они совпадают, устройство является инициатором и не принимает маршрут.

- Отражатель и его клиенты образуют кластер. В рамках AS каждый отражатель использует уникальный идентификатор кластера.
  - Для предотвращения петель маршрутизации между кластерами отражатель использует атрибут Cluster_List для записи идентификаторов всех кластеров, через которые проходит маршрут.
  - Если отражатель отражает маршруты между клиентами или между клиентами и не клиентами, он добавляет Cluster_ID в верх списка Cluster_List. Если Cluster_List пуст, отражатель создает его.
  - Когда отражатель получает обновленный маршрут, он сравнивает Cluster_ID со списком Cluster_List. При обнаружении совпадения маршрут отбрасывается.

Если совпадений не найдено, отражатель добавляет Cluster_ID кластера в список Cluster_List и затем отражает обновленный маршрут.

Отражатель маршрутов: резервный отражатель

- Резервный отражатель
  - Отражатели в одном кластере имеют один Cluster_ID.
  - Cluster_List предотвращает возникновение петель маршрутизации между отражателями внутри одной AS.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Резервный отражатель используется для решения проблемы единой точки отказа (SPOF).

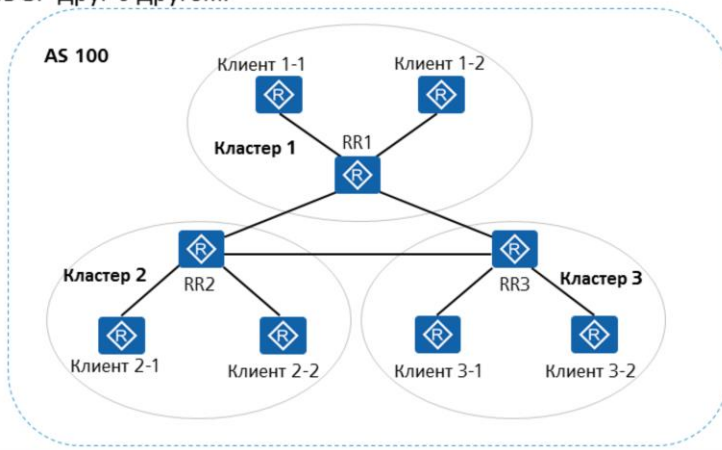
- Резервный отражатель
  - На VRP выполните команду **reflector** *cluster-id,* чтобы установить один Cluster_ID для всех отражателей в кластере.
  - В резервной среде клиент получает несколько маршрутов с одной точкой назначения после того, как маршруты отражены разными отражателями. В этой ситуации клиент выбирает оптимальный маршрут на основе политики выбора маршрутов BGP.
  - Cluster_List обеспечивает отсутствие петли маршрутизации между отражателями в одной AS.

- Описание топологии
  - После получения обновленного маршрута (10.0.0.0/24), анонсированного соседом EBGP, Клиент 1 анонсирует маршрут отражателям RR1 и RR2 с помощью IBGP.
  - Получив обновленный маршрут, RR1 отражает его другим клиентам (Клиенту 2 и Клиенту 3) и не клиенту (RR2) и добавляет Cluster_ID локального кластера в верх списка Cluster_List.
  - После получения отраженного маршрута RR2 проверяет Cluster_List и обнаруживает, что его Cluster_ID включен в Cluster_List. Поэтому RR2

отбрасывает обновленный маршрут и не отражает его клиентам.

Отражатель маршрутов: отражатели одного уровня

- Отражатели одного уровня
  - AS может состоять из нескольких кластеров, а отражатели устанавливают отношения соседства IBGP друг с другом.

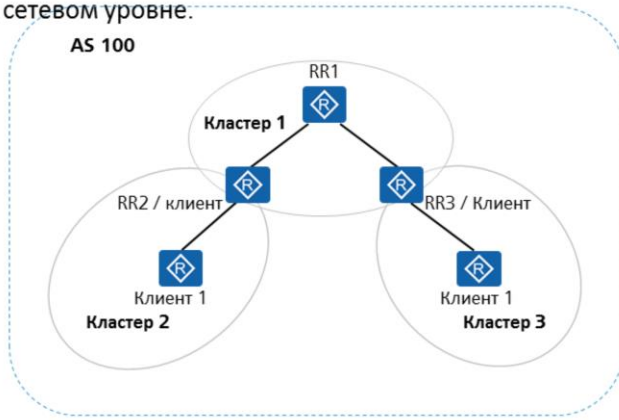


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Магистральная сеть разделена на несколько кластеров отражения. Каждый отражатель не является клиентом других отражателей в других кластерах, и все отражатели устанавливают полносвязные соединения. Каждый клиент устанавливает соединения IBGP с отражателями только в локальном кластере. Таким образом, все маршрутизаторы BGP в AS получают информацию об отраженном маршруте.

Отражатель маршрутов: иерархическая структура

- Иерархический отражатель
  - Отражатель на нижнем сетевом уровне конфигурируется как клиент другого отражателя на более высоком сетевом уровне.

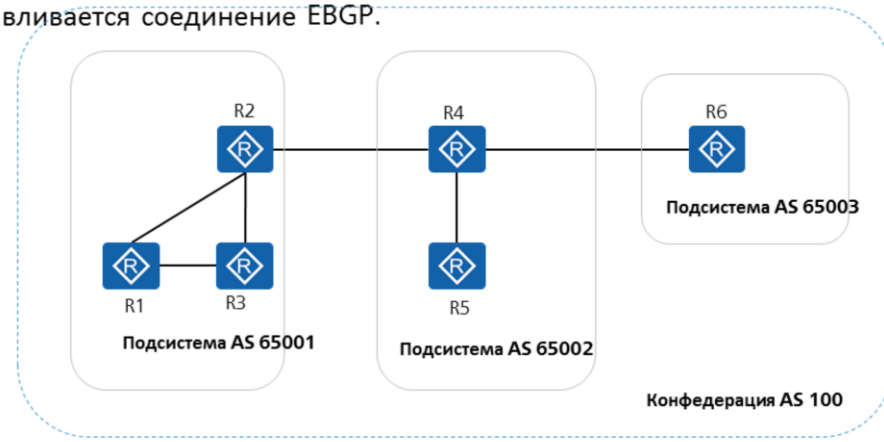


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Отражатель уровня 1 (RR-1) создается в Кластере 1. Отражатель в Кластере 2 и Кластере 3 (RR-2 и RR-3) функционируют как клиенты RR-1.

Конфедерация BGP

- AS делится на несколько подсистем AS. Все подсистемы AS устанавливают полносвязные отношения соседства IBGP. Между подсистемами AS устанавливается соединение EBGP.

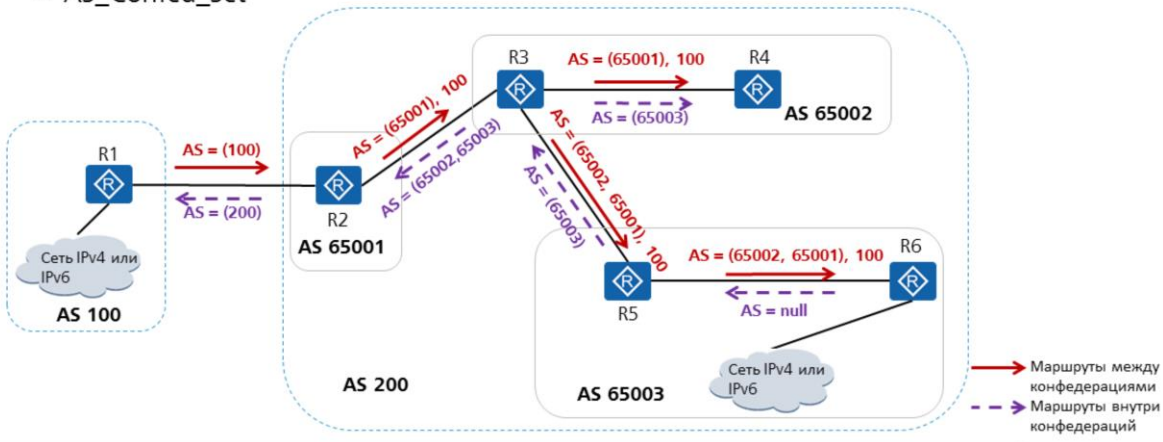


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Конфедерация
  - AS в конфедерации подразделяется на несколько подсистем AS. Внутри каждой подсистемы AS устанавливаются полносвязные соединения IBGP. Между каждой парой подсистем AS устанавливается соединение EBGP. Однако AS за пределами конфедерации рассматривают конфедерацию как одну AS.
  - После конфигурирования конфедерации исходный номер AS используется в качестве ID конфедерации каждого маршрутизатора.
  - Исходные атрибуты IBGP включают атрибуты Local_Pref, MED и Next_Hop. Атрибуты, связанные с конфедерацией, автоматически удаляются, когда маршруты отправляются за пределы конфедерации. То есть администратору не требуется указывать дополнительную информацию, например номер подсистемы AS, на выходе из конфедерации.

Конфедерация BGP: механизмы предотвращения петель

- Механизмы предотвращения петель в конфедерациях BGP
  - AS_Confed_Sequence
  - AS_Confed_Set



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Атрибут AS-Path – это общеизвестный обязательный атрибут, который состоит из номеров AS. Существует четыре типа атрибута AS-Path:
  - AS_Set: состоит из списка неупорядоченных номеров AS, содержащихся в сообщении Update. При суммировании маршрутов вы можете использовать политику с применением атрибута AS_Set для предотвращения потери информации о путях.
  - AS_Sequence: состоит из серии упорядоченных номеров AS, содержащихся в сообщении Update. Как правило, типом AS-Path является AS_Sequence.
  - AS_Confed_Sequence: состоит из списка неупорядоченных номеров подсистем AS в локальной конфедерации, которые содержатся в сообщении Update. Атрибут AS_Confed_Sequence используется таким же образом, как атрибут AS_Set, и передается только в локальной конфедерации.
  - AS_Confed_Set: состоит из списка неупорядоченных номеров подсистем AS в локальной конфедерации, которые содержатся в сообщении Update. Атрибут AS_Confed_Set используется таким же образом, как атрибут AS_Set, и передается только в локальной конфедерации.
- Номера подсистем AS в конфедерации невидимы для AS, не входящих в конфедерацию. Номера подсистем AS удаляются из маршрутов до того, как маршруты будут анонсированы из конфедерации в другие AS, не входящие в конфедерацию.

Сравнение методов отражения маршрутов и создания конфедерации в BGP

Отражение маршрутов	Конфедерация
Не нужно менять существующую топологию сети. Хорошая совместимость.	Топологию необходимо изменить.
Конфигурация проста. Клиент не знает, что является клиентом.	Все устройства необходимо перенастроить. Они должны поддерживать функцию конфедерации.
Между кластерами необходимо установить полносвязные соединения.	Подсистемы AS в конфедерации устанавливают специальные соединения EBGP. Устанавливать полносвязные соединения не требуется.
Широко используется в крупных сетях.	Используется редко.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

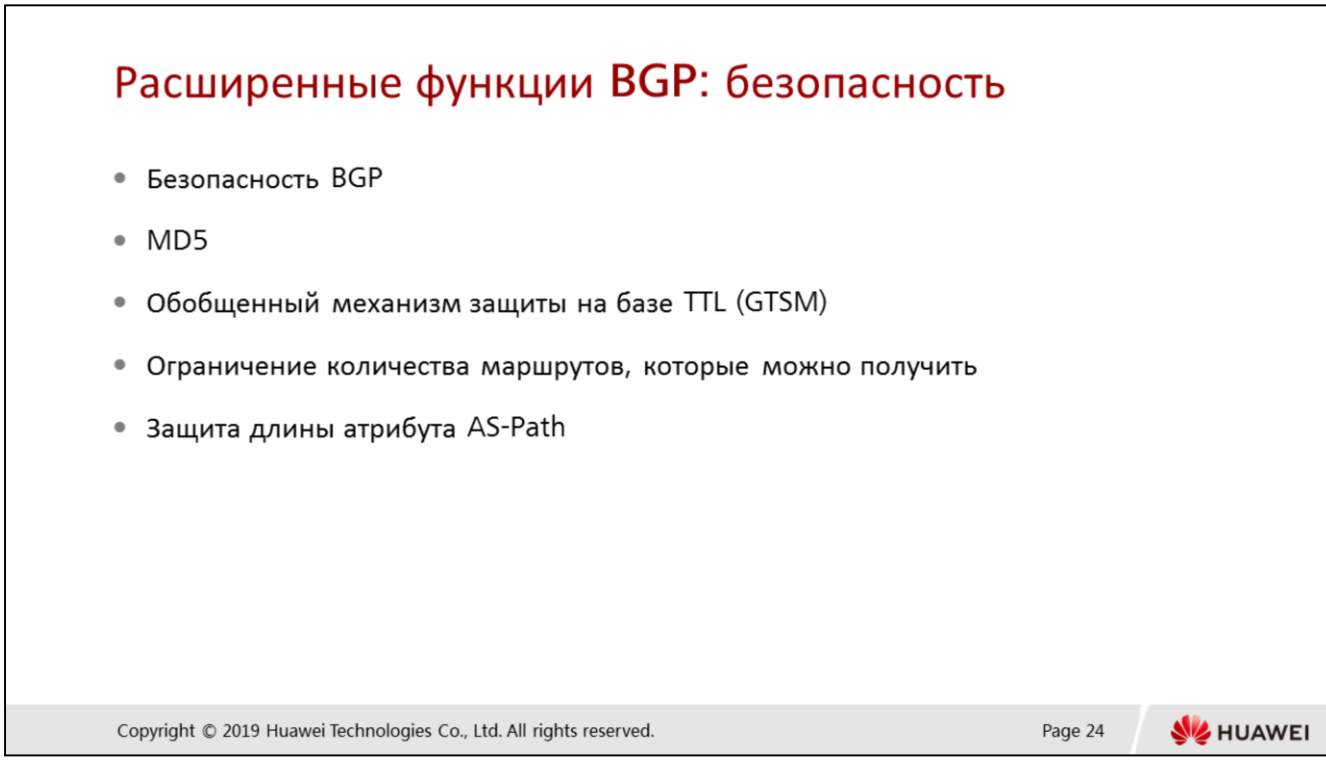
- Сравнение механизмов отражения маршрутов и конфедерации
  - Конфедерация требует повторного деления сети, что приводит к значительному числу изменений в действующей сети.
  - В случае с отражателями маршрутов вам необходимо сконфигурировать только отражатели, настраивать клиентов не требуется. Функцию конфедерации, напротив, необходимо сконфигурировать на всех маршрутизаторах в конфедерации.
  - Между отражателями необходимо установить полносвязные соединения IBGP.
  - Отражение маршрутов используется широко. Конфедерация применяется редко.



Содержание

- Технологии для работы с большим количеством маршрутов BGP
- **Расширенные функции BGP**
- Улучшенные функции BGP
- Основы проектирования интернет-сети
- Устранение неполадок в BGP-сети

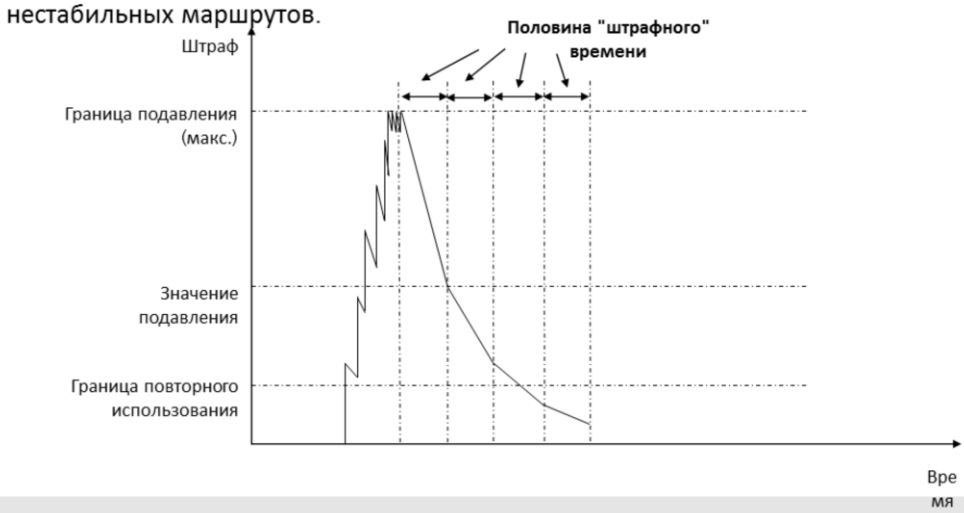
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.



- Функции обеспечения безопасности BGP:
  - MD5: BGP использует протокол транспортного уровня TCP. Для повышения безопасности BGP настройте аутентификацию MD5 при установлении TCP-соединения. Обратите внимание, что аутентификация MD5 BGP не применяется к сообщениям BGP. При использовании аутентификации MD5 необходимо установить пароль для TCP-соединения. Если аутентификация не будет выполнена, TCP-соединение не будет установлено.
  - Обобщенный механизм защиты на базе TTL (GTSM) проверяет, попадает ли в предел определенного диапазона значение TTL в заголовке IP-сообщения, что обеспечивает защиту услуг на IP-уровне и повышение безопасности системы. После включения GTSM для BGP интерфейсная плата проверяет значение TTL, содержащееся в каждом сообщении BGP. В соответствии с фактическими требованиями к сети политику GTSM можно сконфигурировать таким образом, чтобы сообщения, в которых значения TTL выходят за пределы установленного диапазона, принимались или отклонялись. Когда действие GTSM по умолчанию установлено на "discard"(отклонить), вы можете выбрать диапазон значений TTL на основе топологии сети. Сообщения, не соответствующие диапазону значений TTL, отбрасываются напрямую интерфейсной платой. Это предотвращает потребление ресурсов ЦП сообщениями BGP, имитируемыми злоумышленниками. Эта функция несовместима с функцией EBGP multi-hop.
  - Ограничение количества маршрутов, которые могут быть получены. Благодаря этому механизму предотвращаются атаки методом истощения ресурсов.
- Защита длины атрибута AS-Path. Длина атрибута AS-Path ограничена на входящих и исходящих интерфейсах. Сообщения, в которых длина атрибута AS-Path превышает заданный предел, отклоняются.

Расширенные функции BGP: сглаживание маршрутной информации (Route Dampening)

- Сглаживание маршрутной информации используется для решения проблемы нестабильных маршрутов.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Сглаживание маршрутной информации (Route dampening) используется для решения проблемы нестабильных маршрутов. В большинстве случаев BGP используется в сложных сетях, в которых часто меняются маршруты. Чтобы свести к минимуму неблагоприятное воздействие, вызываемое постоянной нестабильностью маршрутов, BGP использует механизм сглаживания для подавления нестабильных маршрутов.
- Штраф (penalty) указывает на стабильность маршрута. Чем больше штраф, тем менее стабилен маршрут. Каждый раз, когда маршрут становится нестабильным (статус меняется с активного на неактивный), BGP присваивает штраф (1000) маршруту. Если штрафное значение превышает заданное значение подавления, маршрут будет подавлен и не будет добавлен в таблицу маршрутизации или анонсирован другим соседям BGP.
- Если штраф маршрута достигает максимального значения подавления, штраф не будет увеличиваться. Поэтому в случае, если маршрут изменяется множество раз в течение короткого периода времени, штраф не будет накапливаться до высокого значения, при котором маршрут останется в подавленном состоянии.
- Штрафное значение подавленного маршрута уменьшается наполовину за интервал времени. Этот интервал является половиной штрафного времени (half-life). Когда штрафное значение уменьшается до определенного значения, маршрут становится доступным и снова добавляется в таблицу маршрутизации. Кроме того, маршрут анонсируется другим соседям BGP. Штрафное значение, значение подавления и значение половины штрафного времени можно установить вручную.
- Сглаживание применяется только к маршрутам EBGP. Сгладить маршруты IBGP нельзя, так как маршруты локальной AS сконфигурированы как маршруты IBGP. Информация о маршруте внутри AS в таблицах переадресации должна быть как можно более единообразной. Если сглаживание маршрутной информации применяется к маршрутам IBGP, а на устройствах отличаются параметры

сглаживания, информация в таблицах переадресации становится противоречивой.

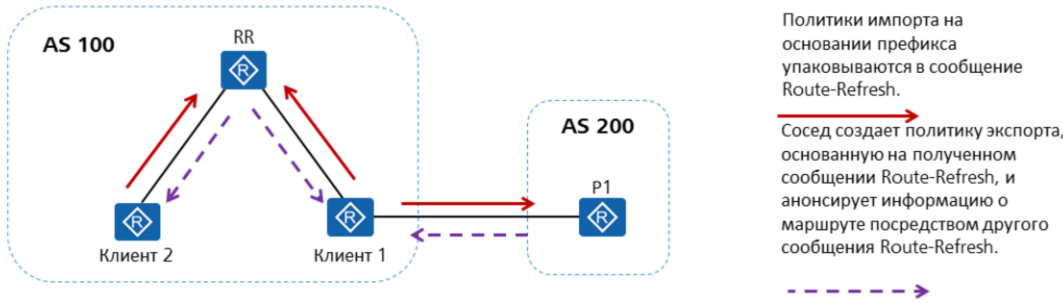
Содержание

- Технологии для работы с большим количеством маршрутов BGP
- Расширенные функции BGP
- **Улучшенные функции BGP**
- Основы проектирования интернет-сети
- Устранение неполадок в BGP-сети

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Улучшенные функции BGP: BGP ORF

- Фильтрация исходящих маршрутов BGP на основании префикса (ORF):
  - Политика экспорта соседа создается на основе локальной политики импорта для анонсирования маршрутов BGP по требованию.
  - Фильтрация BGP ORF бывает двух видов: ORF на основании префикса и VPN ORF.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Стандарты RFC 5291 и RFC 5292 описывают функцию фильтрации BGP ORF на основе префикса. Эту функцию можно использовать для отправки политики импорта на основе префикса, сконфигурированной на локальном устройстве, BGP-соседям с помощью сообщений Route-Refresh. Каждый сосед BGP создает политику экспорта на основе принятой политики и фильтрует маршруты до анонсирования. Это не позволяет локальному устройству получать большое количество нежелательных маршрутов, снижает использование ЦП локального устройства, объем конфигураций на соседе BGP и уменьшает использование полосы пропускания канала.
- Описание топологии
  - При условии прямых отношений соседства EBGP после подтверждения функции ORF на основе префикса между клиентом 1 и R1 клиент 1 инкапсулирует локально настроенную политику импорта на основе префикса в сообщение Route-Refresh и отправляет его R1. После получения сообщения R1 создает политику экспорта и отправляет сообщение Route-Refresh Клиенту 1. Клиент 1 принимает только те маршруты, которые ему необходимы. R1 не требуется политика маршрутизации, за счет чего вам потребуется выполнять меньше конфигураций.
- Клиенты 1 и 2 являются клиентами RR. Клиенты 1 и 2 «договариваются» с RR о фильтрации ORF на основе префикса. Клиенты 1 и 2 инкапсулируют локально настроенные политики импорта на основе префикса в сообщения Route-Refresh и отправляют их в RR. RR создает политику экспорта, опираясь на политики импорта

на основе префикса, полученные от Клиентов 1 и 2, и отражает маршруты Клиентам 1 и 2 посредством сообщений Route-Refresh. Клиенты 1 и 2 принимают только нужные маршруты. RR не требуется политика маршрутизации, за счет чего вам потребуется выполнять меньше конфигураций.

Расширенные функции BGP: Active-Route-Advertise

- Active-Route-Advertise
  - Маршрут BGP можно анонсировать только соседу после его внесения в таблицу маршрутизации сети IPv4 или IPv6.

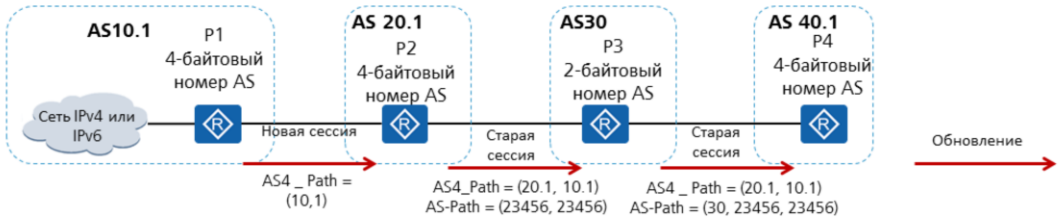


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Active-Route-Advertise
  - По умолчанию маршруты могут быть анонсированы соседям только в том случае, если они являются предпочтительными маршрутами BGP. После настройки функции Active-Route-Advertise устройство будет анонсировать только предпочтительные маршруты BGP, которые являются активными в плоскости управления маршрутами.
  - Эту функцию нельзя использовать одновременно с командой routing-table rib-only, которая используется для предотвращения внесения маршрутов BGP в таблицу IP-маршрутизации.

Расширенные функции BGP: 4-байтовый номер AS

- 4-байтовый номер AS
  - Номер AS удлиняется с 2 байт до 4 байт.
- Расширение протокола
  - Для согласования возможностей BGP-соединения определен новый тип открытого кода возможностей.
  - Два новых дополнительных транзитивных атрибута: AS4_Path и AS4_Aggregator
  - Атрибут AS_Trans (зарезервированное значение: 23456) используется для отображения 4-байтового номера AS в качестве 2-байтового номера AS.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

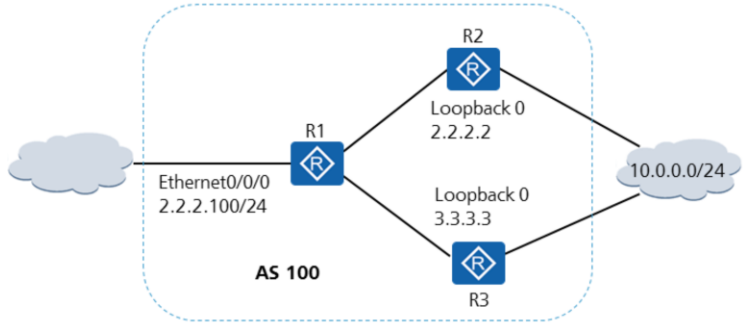
- Роли, определенные на основе поддержки функции 4-байтового номера AS
  - Новый узел: сосед, поддерживающий 4-байтовые номера AS
  - Старый узел: сосед, не поддерживающий 4-байтовые номера AS
  - Новая сессия: Соединение BGP, установленное между новыми узлами
  - Старая сессия: Соединение BGP, установленное между новым узлом и старым узлом или между старыми узлами
- Расширение протокола
  - Для передачи 4-байтовых номеров AS через старую сессию определены два новых дополнительных транзитивных атрибута: AS4_Path (код атрибута: 0x11) и AS4_Aggregator (код атрибута: 0x12).
  - Если новый узел устанавливает отношения соседства со старым узлом, определяется атрибут AS_Trans (зарезервированное значение: 23456) для передачи 4-байтового номера AS в качестве 2-байтового номера AS.
  - Новый номер AS может быть в любом из следующих форматов:
    - Splain: десятичное число.
    - asdot+: в формате 2-байтового значения. Таким образом, 2-байтовый ASN123 может быть написан как 0.123, а ASN65536 равен 1.0. Максимальное значение: 65535.65535.
    - asdot: старый 2-байтовый номер AS остается в своем формате, а новый

номер 4-байтовый номер AS переходит в формат asdot + (2-байтовый номер AS варьируется от 1 до 65535; 4-байтовый номер AS варьируется от 1,0 до 65535.65535)

- Устройства Huawei поддерживают формат asdot.
- Описание топологии:
  - R2 получает от R1 маршрут, содержащий 4-байтовый номер AS. Номер AS – 10.1.
  - Если R2 устанавливает отношения соседства с R3, R3 должен учитывать, что номер AS R2 представлен атрибутом AS_Trans.
  - Перед тем, как R2 анонсирует маршрут к R3, R2 записывает значение AS_Trans в атрибуте AS-Path и добавляет 10.1 и его номер AS 20.1 к атрибуту AS4_Path в желаемом порядке.
  - R3 не обрабатывает неизвестный атрибут AS4_Path и сохраняет его. R3 анонсирует маршрут к R4 на основании правил BGP.
  - R3 считает, что номер AS R4 также представлен атрибутом AS_Trans.
  - Таким образом, когда R4 получает маршрут от R3, R4 заменяет значение AS_Trans в AS-Path с номерами AS, записанными в атрибуте AS4_Path, и восстанавливает значения 30, 20.1 и 10.1 в атрибуте AS-Path.

Расширенные функции BGP: Рекурсивная маршрутизация с помощью следующего узла на основе политики

- Рекурсивная маршрутизация с помощью следующего узла на основе политики
  - Политика маршрутизации используется для ограничения рекурсивных маршрутов. Если рекурсивный маршрут не соответствует политике, рекурсия не выполняется.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Рекурсивная маршрутизация с помощью следующего узла на основании политики
  - BGP выполняет рекурсивную маршрутизацию для маршрутов, содержащих непрямые следующие узлы. Если рекурсивные маршруты не фильтруются, трафик может быть рекурсивно переадресован по неверному пути. Рекурсивная маршрутизация с помощью следующего узла на основании политики ограничивает рекурсивные маршруты с помощью маршрутизации. Если рекурсивный маршрут не соответствует политике, рекурсия маршрута не выполняется.
- Описание топологии
  - R1, R2 и R3 устанавливают отношения соседства IBGP с использованием loopback-адресов. R1 получает маршруты BGP с префиксом 10.0.0.0/24 от R2 и R3. Исходный следующий узел маршрута BGP, анонсированный R2, – это 2.2.2.2. Кроме того, IP-адрес и маска Ethernet 0/0/0 на R1 – 2.2.2.100/24.
  - Когда R2 работает правильно, R1 получает маршрут с префиксом 10.0.0.0/24 от R2 и выполняет рекурсию этого маршрута к маршруту IGP 2.2.2.2/32. Когда IGP становится неисправным на R2, маршрут IGP к 2.2.2.2/32 удаляется. В результате рекурсия на основе следующего узла запускается повторно. На R1 исходный следующий узел 2.2.2.2 используется для выполнения рекурсии самого длинного совпавшего значения в таблице IP-маршрутизации. Исходный маршрут становится рекурсией маршрута к 2.2.2.0/24. Однако пользователь ожидает, что когда маршрут к 2.2.2.2 недоступен, можно выбрать маршрут к 3.3.3.3. Рекурсия из-за удаления маршрута на самом деле связана с конвергенцией BGP. В результате создается переходная черная дыра.
  - Настройте политику рекурсивной маршрутизации на основе следующего узла для фильтрации рекурсивных маршрутов на основе длины маски маршрутов, проложенных к исходным следующим узлам. Вы можете настроить политику рекурсивной маршрутизации таким образом, чтобы исходный следующий

узел 2.2.2.2 мог зависеть только от маршрута IGP к 2.2.2.2/32.



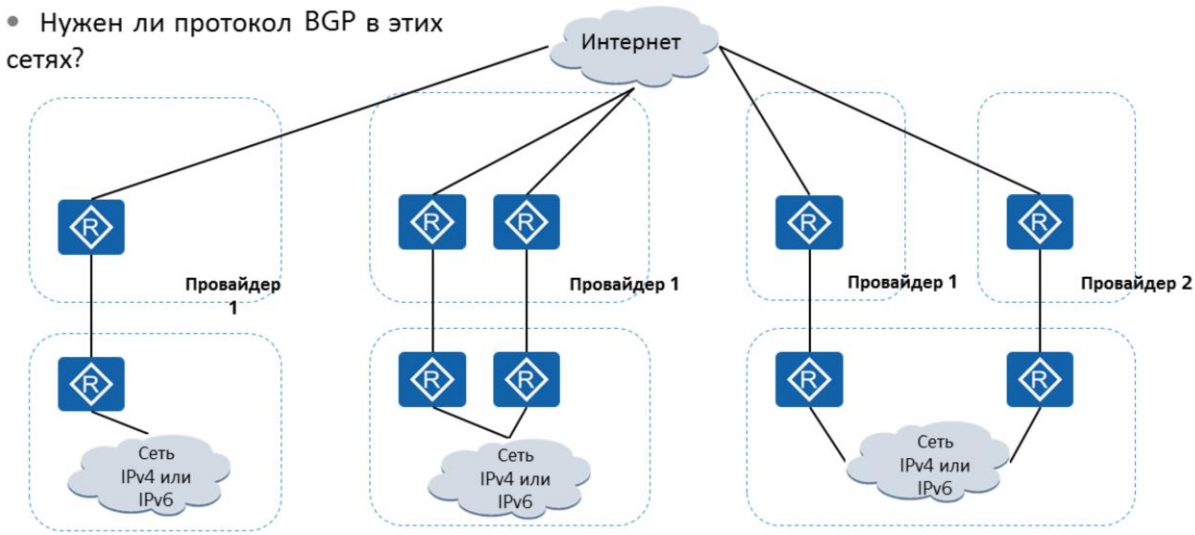
Содержание

- Технологии для работы с большим количеством маршрутов BGP
- Расширенные функции BGP
- Улучшенные функции BGP
- **Основы проектирования интернет-сети**
- Устранение неполадок в BGP-сети

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

В каких типах сетей нужен протокол BGP?

- Нужен ли протокол BGP в этих сетях?



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Стандартные типы топологии корпоративной сети:
  - AS с подключением к одному ISP (каждый выход подключается к одному интернет-провайдеру)
  - AS с резервируемым подключением к одному ISP (несколько выходов подключаются только к одному интернет-провайдеру)
  - AS с резервируемым подключением к двум ISP (несколько выходов подключаются к нескольким интернет-провайдерам)
- AS с подключением к одному ISP: один выход подключается только к одному интернет-провайдеру.
  - В этом случае не требуется настраивать BGP. Можно добавить маршрут по умолчанию к граничному устройству пользователя, которое анонсирует AS пользователя стандартный маршрут.
- AS с резервируемым подключением к одному ISP: резервирование осуществляется на каналах и сетевых устройствах. В этой ситуации частные номера AS используются в пользовательских сетях.
  - Если два канала работают в режиме активный/резервный, BGP не требуется. Два выхода анонсируют стандартные маршруты с разной стоимостью устройствам в локальной AS (если OSPF используется в качестве IGP, стоимость внешнего маршрута рассчитывается в режиме E2, а используется только внешняя стоимость).
  - Если два маршрутизатора работают в режиме балансировки нагрузки:
    - Метод 1: два маршрутизатора анонсируют локальной AS стандартные маршруты, тип стоимости которых -E1 (OSPF используется в качестве IGP), чтобы другие маршрутизаторы в AS могли выбрать ближайший выходной маршрутизатор для достижения внешней сети. В этом случае BGP не

требуется. Однако, когда физическое расстояние между двумя выходами большое и время задержки критически важно, можно использовать BGP для получения более конкретных записей маршрутизации.

- Метод 2: BGP-соединение устанавливается между устройством и устройством ISP. Устройство получает более конкретные записи маршрутизации от BGP и использует политику маршрутизации для обозначения конкретного IP-адреса назначения для определенного выходного маршрута.
- AS с резервируемым подключением к двум ISP: резервирование осуществляется на каналах и сетевых устройствах, а также выполняется резервирование интернет-канала.
    - Для такой AS определите, является ли адресное пространство независимым от интернет-провайдера и доступны ли публичные номера AS.
    - Предпочтительно использовать три метода развертывания, когда пользовательская сеть имеет адресное пространство и публичные номера AS, не зависящие от провайдеров.
        - Метод 1: в активном/ резервном режиме выходные маршрутизаторы анонсируют внутренним устройствам стандартные маршруты с разной стоимостью.
        - Метод 2: в режиме балансировки нагрузки выходные маршрутизаторы анонсируют внутренней сети стандартные маршруты. Используется только механизм расчета стоимости IGP. IGP определяет, какой выходной маршрутизатор будет выбран.
        - Метод 3: Развертывание BGP.
    - Подписание контракта с интернет-провайдером. Основываясь на

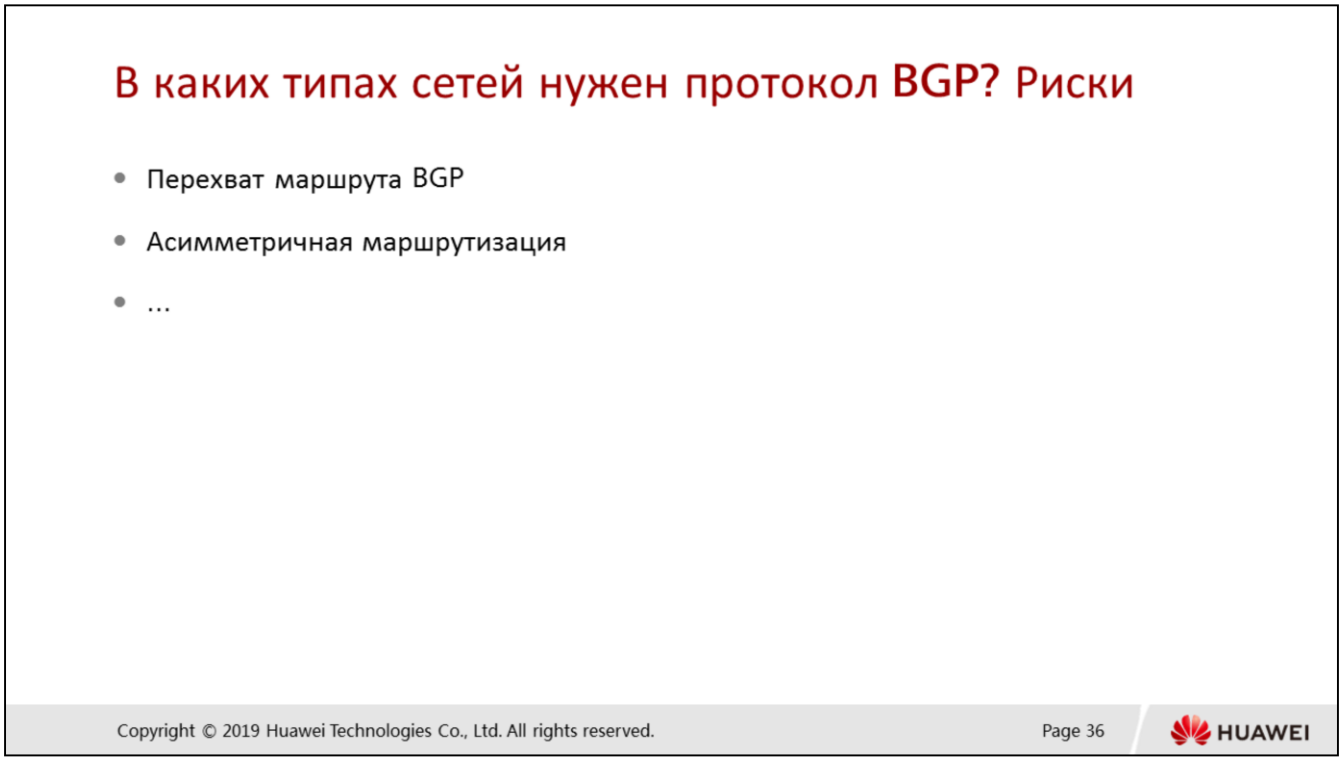
характеристиках сервисного трафика, используйте различные инструменты политики маршрутизации. При необходимости настройте анонсирование стандартных маршрутов.

- Управляйте входящим и исходящим трафиком предприятия эффективно.
- Как правило, BGP развертывается в сети, принадлежащей нескольким AS, поскольку методы 1 и 2 не подходят для управления маршрутами. Тем не менее, вам придется выбрать между преимуществами протокола и возрастающей сложностью маршрутизации.

В каких типах сетей нужен протокол BGP? Факторы

- Существует большое количество маршрутов, которые нельзя суммировать.
- Выполняется перекрестное взаимодействие подразделений (неудобная коммуникация, обмен конфиденциальной информацией)
- В домене маршрутизации используется несколько протоколов IGP.
- Протокол IGP не предоставляет инструменты для настройки необходимых политик.
- Сеть принадлежит нескольким провайдерам.
- ...
- Протокол BGP следует развертывать при условии соблюдения вышеуказанных условий после планирования проекта и сети.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

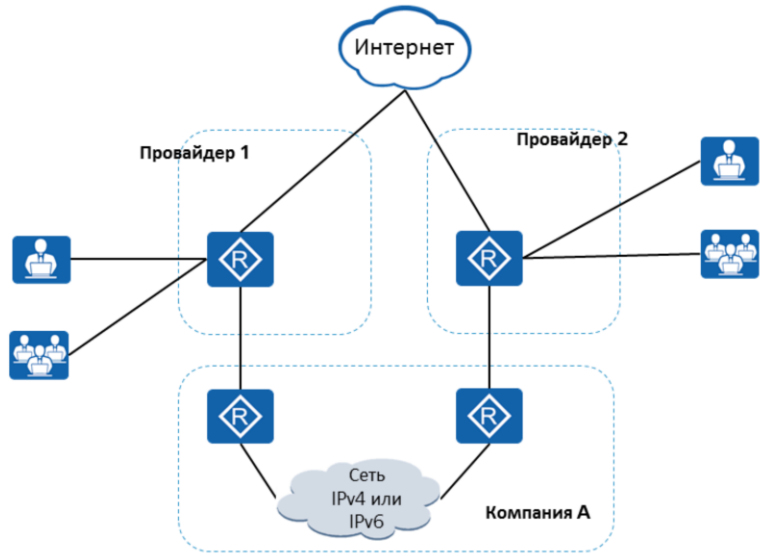


- Перехват маршрута BGP
  - Причина: в BGP предусмотрены простые функции аутентификации. Если две AS установили BGP-соединения, они безоговорочно доверяют информации, полученной друг от друга, включая диапазон IP-адресов, заявленных соседней AS.
  - Риск: устройство в AS может поверить сообщению Update, отправленному соседом BGP в другую AS. Если будет анонсирован маршрут к несуществующему сегменту IP-сети во вредоносной AS, атрибуты BGP, такие как AS-Path, будут заражены, и другая AS будет считать этот путь кратчайшим к сетевому сегменту назначения. В этом случае вредоносная AS может перехватить трафик данных.
- Асимметричная маршрутизация
  - Причина: неправильные атрибуты или суммирование маршрутов становятся причиной недостаточной точности маршрута. В результате пути исходящего и входящего трафика отличаются друг от друга.
  - Риск: во-первых, асимметричный трафик затрудняет прогнозирование модели интернет-трафика. Следовательно, затрудняется сопоставление сетей, планирование загрузки, обнаружение неисправностей и устранение неполадок. Во-вторых, асимметричный трафик вызывает дисбаланс в использовании канала. Полоса пропускания некоторых каналов будет загружена, а пропускная способность других каналов не будет использоваться эффективно. В-третьих, асимметричный трафик вызывает большие несоответствия задержек исходящего и входящего трафика. Это колебание задержки может поставить под угрозу некоторые сервисы, чувствительные к задержкам (например, передачу голоса или

видео в режиме реального времени).

Меры предосторожности при развертывании и обслуживании BGP-сети

- В качестве примера используется AS с резервируемым подключением к ISP:
  - Компания A подключается к двум AS. Маршрут, анонсированный ISP1, некорректно анонсируется ISP2 из-за ошибки конфигурации.
  - Отфильтруйте и выберите маршруты, анонсированные провайдерами на основании услуг.
  - Обратите внимание на операции, выполненные соседней AS, чтобы предотвратить негативное воздействие неправильных операций на локальную сеть.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Основы проектирования интернет-сети: оптимизация BGP

- Оптимизация возможностей BGP
  - Создание сессии с соседом (peer session)
  - Обновление происхождения маршрутов
  - Оптимизация политики маршрутизации
  - Фильтрация маршрутов и контроль атрибутов
  - Суммирование маршрутов

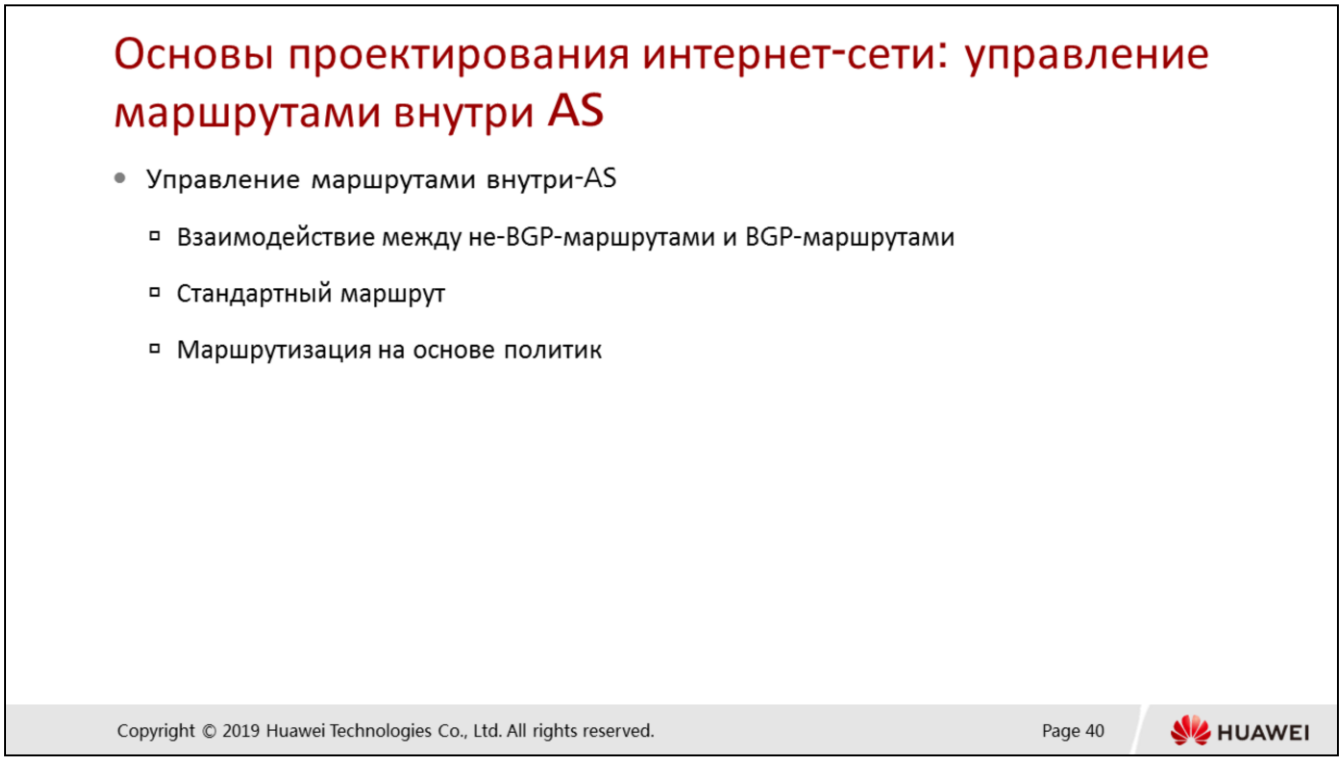
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Основы проектирования интернет-сети: повышение доступности BGP

- Повышение доступности BGP
  - Резервирование
  - Симметричный трафик
  - Балансировка нагрузки

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.



- Взаимодействие между не-BGP-маршрутами и BGP-маршрутами
  - Как правило, IGP и BGP импортируют маршруты. Необходимо использовать правильные политики фильтрации для импорта корректных маршрутов между IGP и BGP.
- Управление стандартными маршрутами
  - Можно настроить политику для доставки стандартных маршрутов на основе определенных условий.
- Маршрутизация на основе политик
  - Маршрутизация на основе политик используется для оптимизации путей передачи трафика.

Основы проектирования интернет-сети: ограничение крупных AS

- Ограничение крупных AS
  - Динамическое обновление групп соседей BGP
  - Отражатель маршрутов
  - Конфедерация

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Основы проектирования интернет-сети: проектирование стабильной интернет-сети

- Проектирование стабильной интернет-сети
  - Сокращение нестабильных маршрутов
  - Повышение стабильности BGP

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

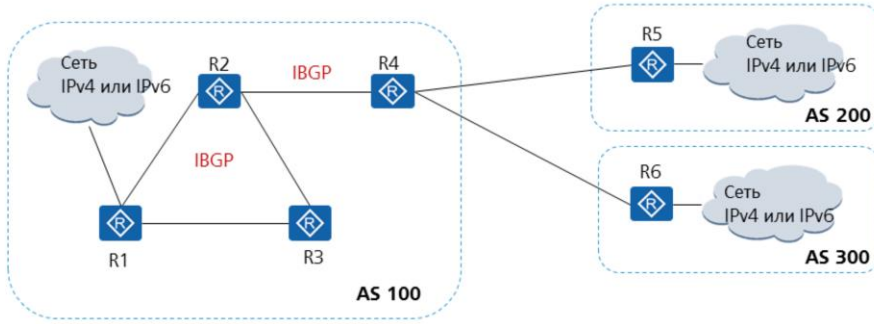
Содержание

- Технологии для работы с большим количеством маршрутов BGP
- Расширенные функции BGP
- Улучшенные функции BGP
- Основы проектирования интернет-сети
- **Расширенные конфигурации BGP**
- Устранение неполадок в BGP-сети

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Конфигурирование группы соседей (1)

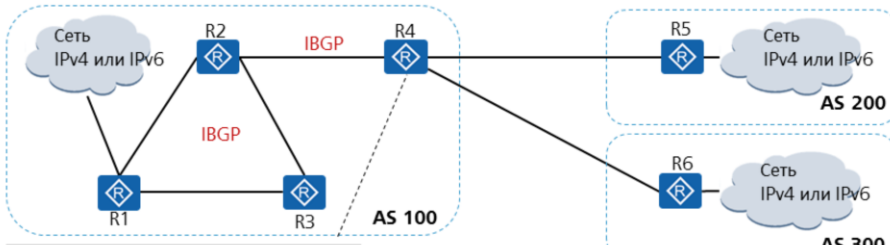
- Требования к конфигурации:
  - Развернут протокол IGP, и все устройства находятся в магистральной зоне OSPF.
  - Loopback-адреса используются для установления отношений соседства EBGP между R4, R5 и R6. Конфигурация R4 необходима для экономии ресурсов.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Описание примера
  - В этом примере правила подключения устройств следующие:
    - Если RX и RY связаны, их адреса соединения – XY.1.1.X и XY.1.1.Y соответственно, а длина маски – 24 бита.
  - OSPFv2 и OSPFv3 работают корректно, и маршруты к адресам соединения устройств и loopback-адресам анонсируются OSPFv2 или OSPFv3.
- Анализ примера
  - Соседи EBGP используют loopback-интерфейсы для установления отношений соседства.

Конфигурирование группы соседей (2)




```
bgp 100
group 100 external
 peer 100 ebgp-max-hop 2
 peer 100 connect-interface  LoopBack0
 peer 5.5.5.5 as-number 200
 peer 5.5.5.5 group 100
 peer 6.6.6.6 as-number 300
 peer 6.6.6.6 group 100
 #
 ipv4-family  unicast
  undo synchronization
  peer 100 enable
  peer 5.5.5.5 enable
  peer 5.5.5.5 group 100
  peer 6.6.6.6 enable
  peer 6.6.6.6 group 100
```

```
[R4]display bgp peer
BGP local router ID : 4.4.4.4
 Local AS number : 100
 Total number of peers : 2                 Peers in established state : 2
  Peer      V   AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv
  5.5.5.5   4   200      3        3      0   00:01:06 Established      0
  6.6.6.6   4   300      2        2      0   00:00:50 Established      0
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Описание команд
  - Команда **peer as-number** устанавливает номер соседней AS для определенного соседа или группы соседей.
  - Команда **peer connect-interface** определяет имя интерфейса источника, используемого для отправки сообщений BGP, и адрес источника, используемый для инициации соединения.
  - Команда **peer next-hop-local** позволяет устройству установить IP-адрес следующего узла для локального IP-адреса до того, как устройство анонсирует маршруты к соседу или группе соседей IBGP.
  - Команда **group** создает группу соседей.
- Принципы использования
  - Предыдущие команды выполняются в режиме BGP process view.
- Описание параметров
  - **peer ipv4-address** *as-number*
    - *Ip-address:* адрес IPv4 соседа.
    - *as-number:* номер AS соседа.
  - **peer ipv4-address connect-interface** *interface-type interface-number [ipv4-source-address*]
    - *Ip-address:* адрес IPv4 соседа.

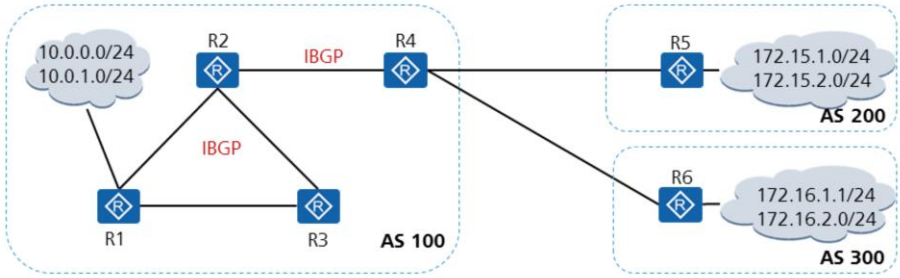
- *Interface-type interface-number:* тип и номер интерфейса.
- *ipv4-source-address:* адрес источника IPv4, используемый для установления соединения.

- **peer** *ipv4-address* **next-hop-local**
  - *ip -address:* адрес IPv4 соседа.
- **group** *group-name* **[external | internal**]
  - *group-name:* имя группы соседей.
  - **external**: создает группу соседей EBGP.
  - **internal**: создает группу соседей IBGP.

- **Меры предосторожности**
  - Когда loopback-интерфейс используется в качестве исходного интерфейса BGP- сообщений, обратите внимание на следующее:
  - Убедитесь, что loopback-интерфейс соседа BGP доступен.
  - Для соединений EBGP выполните команду **peer ebgp-max-hop**, чтобы позволить EBGP установить отношения соседства через непрямые соединения.
  - Команды **peer next-hop-local** и **peer next-hop-invariable** являются взаимно исключающими.
  - В выводе команды **display bgp peer** значение **Rec** указывает на количество префиксов маршрутов, полученных от соседа локальным участком.
  - Конфигурация IPv6 аналогична конфигурации IPv4.

Конфигурирование автоматического суммирования маршрутов BGP и стандартных маршрутов (1)

- Оптимизируйте пути в AS 300 с соблюдением следующих требований:
  - Импортируйте маршрут к сетевому сегменту 172.16.X.0/24 в BGP и выполните автоматическое суммирование.
  - Когда маршрут к 172.16.0.0/16 появляется на R4, R4 должен анонсировать стандартный маршрут к AS300.

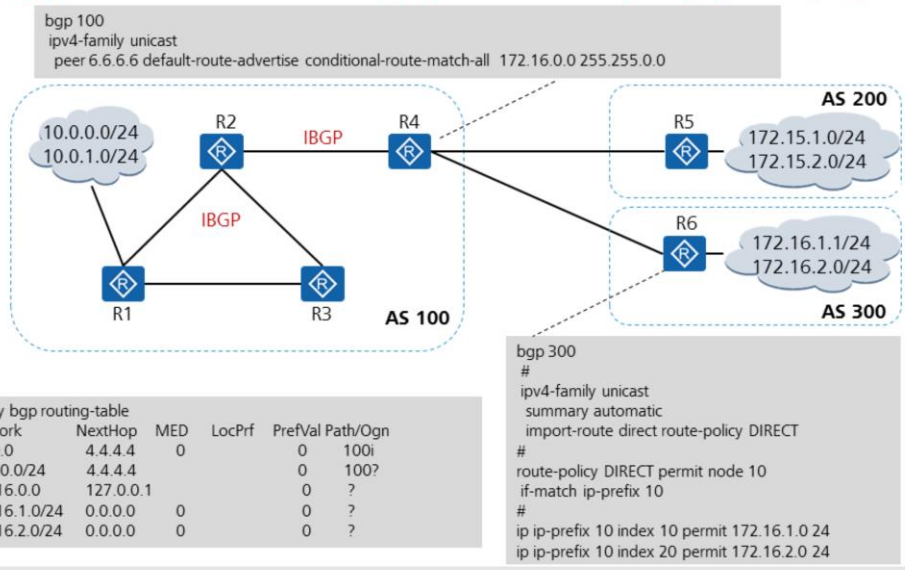


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Описание примера
  - В данном примере расширены требования из предыдущего примера. Конфигурация основана на конфигурации в предыдущем примере.
  - В соответствии с требованием 2 стандартный маршрут должен быть связан с маршрутом к 172.16.0.0/16. Если маршрут к 172.16.0.0/16 исчезнет, стандартный маршрут тоже исчезнет.

Конфигурирование автоматического суммирования маршрутов BGP и стандартных маршрутов (1)



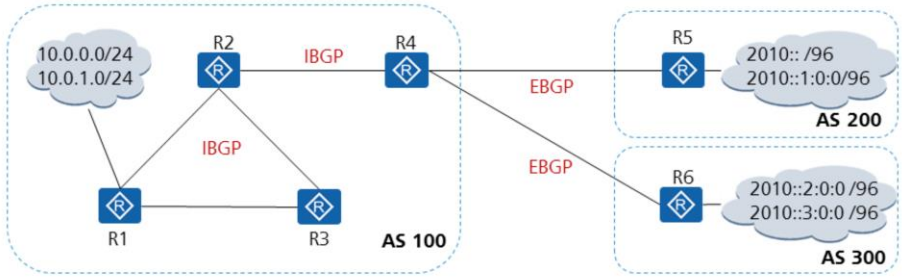
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Описание команд
  - Команда **peer route-policy** определяет политику маршрутизации, используемую для приема маршрутов от соседа или группы соседей или анонсирования им маршрутов.
  - Команда **peer default-route-advertise** выполняет конфигурацию устройства для анонсирования стандартных маршрутов соседу или группе соседей.
- Принципы использования
  - Команда **peer route-policy** выполняется в режиме BGP view.
  - Команда **peer default-route-advertise** выполняется в режиме BGP view.
- Описание параметров
  - **peer** *ipv4-address* **route-policy** *route-policy-name* { **import | export** }
    - *ipv4-address:* адрес IPv4 соседа.
    - *route-policy-name:* имя политики маршрутизации.
    - **import**: применяет политику маршрутизации к маршрутам, анонсированным соседом или группой соседей.
    - **export**: применяет политику маршрутизации к маршрутам, анонсированным соседу или группе соседей.

- **peer** { *group-name* | *ipv4-address* } **default-route-advertise** [**route-policy** *route-policy-name*] [**conditional-route-match-all**{ *ipv4-address1 { mask1* | *mask-length1* } } &<1-4> | **conditional-route-match-any** { *ipv4-address2 { mask2* | *mask-length2* } } &<1-4>]
  - *ipv4-address:* адрес IPv4 соседа BGP.
  - **route-policy** *route-policy-name*: имя политики маршрутизации.
  - **conditional-route-match-all** *ipv4-address1* { *mask1* | *mask-length1* }: адрес IPv4 и маска или длина маски маршрута.
  - При совпадении всех условий отправляется стандартный маршрут.
  - **conditional-route-match-any** *ipv4-address2 {mask2* | *mask-length2*}: адрес IPv4 и маска или длина маски маршрута. Если какое-либо условие выполнено, то анонсируется стандартный маршрут.
- Проверка
  - Выполните команду **display ip routing-table** для просмотра информации в таблице маршрутизации.

Конфигурирование административного суммирования маршрутов BGP (1)

- Требования к конфигурации:
  - R1 импортирует маршрут к сети 10.0.X.0/24 и отмечает его атрибут community как 200:200.
  - На R1 используйте community 200: 200 для административного суммирования маршрутов. После суммирования маска маршрута будет иметь значение /23 и определенные маршруты будут подавлены. Кроме того, необходимо предотвратить образование петель.
  - На R4 суммируйте маршруты, принадлежащие сетевому сегменту 2010::x:0:0/96 и установите маску подсети на значение 94 для суммарного маршрута.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Описание примера
  - В данном примере расширены требования из предыдущего примера. Конфигурация основана на конфигурации в предыдущем примере.

Конфигурирование административного суммирования маршрутов BGP (2)

```
[R1]
bgp 100
  ipv4-family unicast
  aggregate 10.0.0.0 255.255.254.0 as-set detail-suppressed origin-policy COMM
  import-route direct route-policy DIRECT
#
route-policy DIRECT permit node 10
 if-match ip-prefix 10
 apply community 200:200
#
route-policy COMM permit node 10
 if-match community-filter 200:200
#
ip ip-prefix 10 index 10 permit 10.0.1.0 24
ip ip-prefix 10 index 20 permit 10.0.0.0 24
```

```
[R4]
bgp 100
#
 ipv6-family unicast
 aggregate 2010:: 94 detail-suppressed
 peer 2011::24:2 next-hop-local
#
```

```
[R4]dis bgp routing-table

  Total Number of Routes: 5
     Network          NextHop        MED        LocPrf    PrefVal Path/Ogn

*>   10.0.0.0/23      1.1.1.1          0                    0                 ?
```

```
[R2]dis ipv6 routing-table protocol bgp
 Destination  : 2010::                    PrefixLength : 94
 NextHop      : 2011::24:4                 Preference   : 255
 Cost         : 0                          Protocol     : IBGP
 RelayNextHop : ::                         TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/0       Flags        : D
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Описание команды:
  - Команда **aggregate** создает суммарный маршрут в таблице маршрутизации BGP.
- Принципы использования
  - Команда **aggregate** выполняется в режиме BGP view.
- Описание параметров
  - **aggregate** *ipv4-address { mask | mask-length }* [**as-set | attribute-policy** *route-policy-name1* | **detail-suppressed | origin-policy** *route-policy-name2* | *suppress-policyroute-policy-name3*] *
    - *ipv4-address:* адрес IPv6 суммарного маршрута.
    - *mask*: использует маршруты IBGP только при балансировке нагрузки.
    - *mask-length:* длина маски сети суммарного маршрута.
    - **as-set**: генерирует маршруты с атрибутом AS_Set.
    - **attribute-policy** *route-policy-name1*: имя политики атрибутов для суммарного маршрута.
    - **detail-suppressed**: анонсирует суммарные маршруты.
    - **origin-policy** *route-policy-name2*: имя политики для создания суммарных маршрутов.
    - **suppress-policy** *route-policy-name3*: имя политики для подавления анонсирования определенных маршрутов.
- Меры предосторожности
  - И при административном, и при автоматическом суммировании маршрутов маршрут к NULL0 создается локально.
  - Конфигурация IPv6 аналогична конфигурации IPv4.

- Результат эксперимента
  - Выполните команду **display ip routing-table protocol bgp**, чтобы посмотреть маршруты, полученные BGP.



Содержание

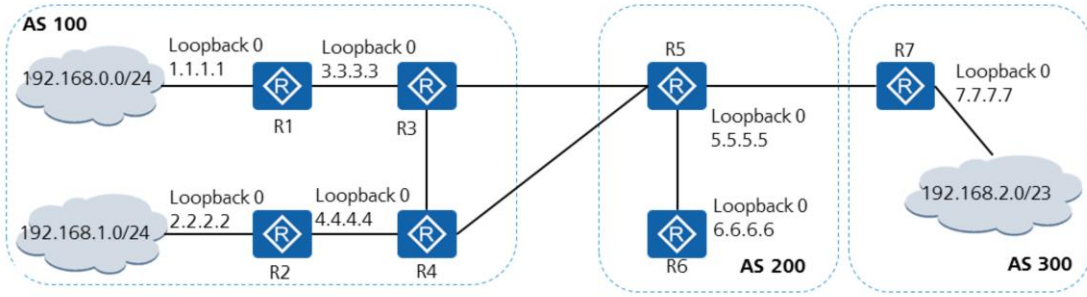
- Технологии для работы с большим количеством маршрутов BGP
- Расширенные функции BGP
- Улучшенные функции BGP
- Основы проектирования Интернет-сети
- Расширенные конфигурации BGP
- **Реализация требований и устранение неполадок в BGP-сети**

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Реализация требований и устранение неполадок в BGP-сети – Пример 1 (1)

Требование:

- OSPF работает в AS 100. Все маршрутизаторы относятся к зоне 0. Отношения соседства IBGP устанавливаются между напрямую подключенными маршрутизаторами с использованием loopback- интерфейсов. Количество установленных соединений BGP сведено к минимуму.
  - R5 и R6 используют loopback-интерфейсы для установления отношений соседства IBGP. R5 использует прямые интерфейсы для установления отношений соседства EBGP с R3 и R4 и loopback-интерфейс для установления отношений соседства EBGP с R7.
  - R1 напрямую подключается к 192.168.0.0/24, R2 – к 192.168.1.0/24, R7 – к 192.168.2.0/23. Эти три сегмента сети должны иметь возможность взаимодействовать друг с другом, а количество маршрутов на R6 должно быть сведено к минимуму.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Сегмент сети между Rx и Ry (X < Y) – 10.0.xy.0/24. IP-адрес интерфейса Rx – 10.0.xy.x, IP-адрес интерфейса Ry – 10.0.xy.y.
- Сконфигурированы все адреса интерфейсов.

Реализация требований и устранение неполадок в BGP-сети – Пример 1 (2)

- Конфигурации устройств в AS 100:

```
[R1]
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 10.0.12.1 0.0.0.0
#
bgp 100
 peer 2.2.2.2 as-number 100
 peer 2.2.2.2 connect-interface LoopBack0
 #
 ipv4-family unicast
 network 192.168.0.0
  peer 2.2.2.2 enable
```

```
[R2]
ospf 1
 area 0.0.0.0
  network 2.2.2.2  0.0.0.0
  network 10.0.12.2 0.0.0.0
  network 10.0.23.2 0.0.0.0
#
bgp 100
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 connect-interface  LoopBack0
 peer 3.3.3.3 as-number 100
 peer 3.3.3.3 connect-interface  LoopBack0
 peer 10.0.25.5 as-number 200
 #
 ipv4-family unicast
  undo synchronization
  peer 1.1.1.1 enable
  peer 1.1.1.1 reflect-client
  peer 1.1.1.1 next-hop-local
  peer 3.3.3.3 enable
  peer 10.0.25.5 enable
#
```

```
[R3]
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 10.0.34.3 0.0.0.0
  network 10.0.23.3 0.0.0.0
#
bgp 100
 peer 2.2.2.2  as-number 100
 peer 2.2.2.2  connect-interface  LoopBack0
 peer 4.4.4.4 as-number 100
 peer 4.4.4.4 connect-interface  LoopBack0
 peer 10.0.35.5 as-number 200
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.2  enable
  peer 4.4.4.4 enable
  peer 4.4.4.4 reflect-client
  peer 1.1.1.1 next-hop-local
  peer 10.0.35.5 enable
#
```

```
[R4]
ospf 1
 area 0.0.0.0
  network  0.0.0.0
  network 10.0.34.4 0.0.0.0
#
bgp 100
 peer 3.3.3.3 as-number 100
 peer 3.3.3.3 connect-interface LoopBack0
 #
 ipv4-family unicast
 network 192.168.1.0
  peer 3.3.3.3 enable
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Выполните команду **display bgp peer,** чтобы проверить, были ли установлены отношения соседства BGP.
- Выполните команду **display bgp routing-table**, чтобы проверить, была ли получена информация о маршрутизации.

Реализация требований и устранение неполадок в BGP-сети – Пример 1 (3)

- Конфигурации устройств в AS 200:

```
[R5]
#
bgp 200
 peer 10.0.25.2 as-number 100
 peer 10.0.35.3 as-number 100
 peer 10.0.56.6 as-number 200
peer 7.7.7.7 as-number 300
peer 7.7.7.7 ebgp-max-hop 2
 #
 ipv4-family unicast
  undo synchronization
  aggregate 192.168.0.0 255.255.252.0 as-set detail-suppressed
  peer 10.0.25.2 enable
  peer 10.0.35.3 enable
  peer 10.0.56.6 enable
  peer 7.7.7.7 enable
#
ip route-static 7.7.7.7 255.255.255.255 10.0.57.7
```

```
[R6]
#
bgp 200
peer 10.0.56.6 as-number 200
#
 ipv4-family unicast
  undo synchronization
  peer 10.0.56.5 enable
#
```

- Конфигурации устройств в AS 300:

```
[R7]
#
bgp 300
peer 5.5.5.5 as-number 200
#
 ipv4-family unicast
  undo synchronization
  peer 5.5.5.5enable
#
ip route-static 5.5.5.5 255.255.255.255 10.0.57.5
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Сегмент сети между Rx и Ry (X < Y) – 10.0.xy.0/24. IP-адрес интерфейса Rx – 10.0.xy.x, IP-адрес интерфейса Ry –10.0.xy.y.
- Сконфигурированы все адреса интерфейсов.

Реализация требований и устранение неполадок в BGP-сети – Пример 1 (4)

- После выполнения конфигураций все отношения соседства BGP установлены. Однако два сегмента сети в AS 100 не имеют доступа к сегменту сети в AS 300.
  - Проверьте таблицы маршрутизации R1 и R3.

```
<R1>dis bgp routing-table
Network          NextHop      MED      LocPrf   PrefVal Path/Ogn

 *>  192.168.0.0      0.0.0.0      0                      0    i
 *>i 192.168.1.0      4.4.4.4      0        100           0    i

[R3-bgp]dis bgp routing-table
Network          NextHop      MED      LocPrf   PrefVal Path/Ogn

 *>i 192.168.0.0      1.1.1.1      0        100           0    i
 *>i 192.168.1.0      4.4.4.4      0        100           0    i
```

```
[R5]dis bgp routing-table

Total Number of Routes: 6
     Network          NextHop      MED      LocPrf   PrefVal Path/Ogn

 *>  192.168.0.0/22   127.0.0.1                      0        {100 300}i
 s>  192.168.0.0      10.0.25.2                      0        100i
 *                    10.0.35.3                      0        100i
 s>  192.168.1.0      10.0.25.2                      0        100i
 *                    10.0.35.3                      0        100i
 s>  192.168.2.0/23   10.0.56.6    0                 0        300i
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Вывод команды показывает, что атрибут AS_Set содержит номер локальной AS. Поэтому суммарный маршрут не принимается. В данном случае вам нужно отключить подавление определенных маршрутов или удалить конфигурацию AS_Set.

Реализация требований и устранение неполадок в BGP-сети – Пример 1 (5)

- Измененная конфигурация R5:

```
#
bgp 200
#
 ipv4-family unicast
  undo synchronization
  aggregate 192.168.0.0 255.255.252.0 detail-suppressed
```

- Проверьте таблицы маршрутизации R1 и R3.

```
<R1>dis bgp routing-table
      Network         NextHop      MED    LocPrf    PrefVal          Path/Ogn
*>i   192.168.0.0/22  2.2.2.2                100         0            200i
 *>   192.168.0.0     0.0.0.0      0                     0            i
 *>i  192.168.1.0     4.4.4.4      0         100         0            I

[R3-bgp]dis bgp routing-table
      Network         NextHop      MED    LocPrf    PrefVal          Path/Ogn
*>i   192.168.0.0/22  10.0.35.5              100         0            200i
 *>i  192.168.0.0     1.1.1.1      0         100         0            i
 *>i  192.168.1.0     4.4.4.4      0         100         0            i
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

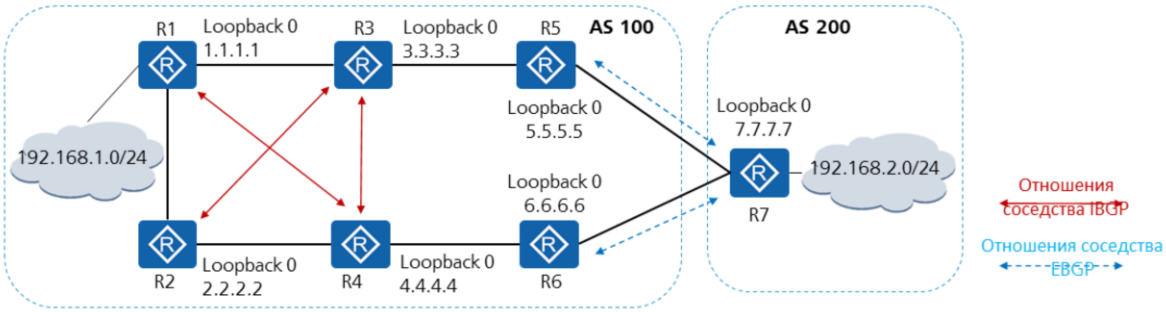
HUAWEI

- Краткое описание примера:
  - Выполняйте настройку суммирования маршрутов с осторожностью. Неправильная конфигурация может вызвать следующие проблемы:
    - Сеть не будет узнавать правильные маршруты.
    - Могут возникать петли.

Реализация требований и устранение неполадок в BGP-сети – Пример 2 (1)

Требования:

- Протокол OSPF работает в AS 100. Все маршрутизаторы относятся к зоне 0. Между маршрутизаторами установлены отношения соседства IBGP с использованием loopback-адресов. Отношения соседства показаны на рисунке.
- Отношения соседства EBGP устанавливается между R7 и R5 и между R7 и R6 посредством напрямую подключенных интерфейсов.
- Чтобы все маршрутизаторы могли узнавать маршруты AS 200, настройте RR-маршрутизатор. R5 является клиентом R3, а R6 – клиентом R4.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Сегмент сети между Rx и Ry (X < Y) – 10.0.xy.0/24. IP-адрес интерфейса Rx – 10.0.xy.x, IP-адрес интерфейса Ry – 10.0.xy.y.
- Сконфигурированы все адреса интерфейсов.
- R5 является клиентом R3, а R6 – клиентом R4.

Реализация требований и устранение неполадок в BGP-сети – Пример 2 (2)

- Конфигурации R1 и R4:

```
[R1]
ospf 1 router-id 1.1.1.1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 10.0.12.1 0.0.0.0
  network 10.0.13.1 0.0.0.0
#
bgp 100
 peer 4.4.4.4 as-number 100
 peer 4.4.4.4 connect-interface LoopBack0
 #
 ipv4-family unicast
  undo synchronization
  network 192.168.1.0
 255.255.255.0
  peer 4.4.4.4 enable
```

```
[R4]
#
ospf 1 router-id 4.4.4.4
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 10.0.24.4 0.0.0.0
  network 10.0.46.4 0.0.0.0
#
#
bgp 100
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 connect-interface LoopBack0
 peer 6.6.6.6 as-number 100
 peer 6.6.6.6 connect-interface LoopBack0
 #
 ipv4-family unicast
  undo synchronization
  peer 1.1.1.1 enable
  peer 6.6.6.6 enable
  peer 6.6.6.6 reflect-client
#
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- После выполнения конфигураций все отношения соседства BGP установлены, и информация о всех маршрутах получена в OSPF.
- Конфигурация R2 аналогична конфигурации R1. Конфигурация R3 аналогична конфигурации R4. Конфигурация R5 аналогична конфигурации R6.
- После завершения настройки R1 анонсирует BGP-сети прямой маршрут к 192.168.1.0/24. R7 анонсирует BGP-сети прямой маршрут к 192.168.2.0/24.

Реализация требований и устранение неполадок в BGP-сети – Пример 2 (3)

- Конфигурации R6 и R7:

```
[R6]
ospf 1 router-id 6.6.6.6
 area 0.0.0.0
  network 6.6.6.6 0.0.0.0
  network 10.0.46.6 0.0.0.0
  network 10.0.67.6 0.0.0.0
#
bgp 100
 peer 4.4.4.4 as-number 100
 peer 4.4.4.4 connect-interface LoopBack0
 peer 4.4.4.4 next-hop-local
 peer 10.0.67.7 as-number 200
 #
 ipv4-family unicast
  undo synchronization
  peer 4.4.4.4 enable
  peer 10.0.67.7 enable
```

```
[R7]
#
bgp 200
 router-id 7.7.7.7
 peer 10.0.57.5 as-number 100
 peer 10.0.67.6 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  peer 10.0.57.5 enable
  network 192.168.2.0 255.255.255.0
  peer 10.0.67.6 enable
#
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- После выполнения конфигураций все отношения соседства BGP установлены, и информация о всех маршрутах получена в OSPF.
- Конфигурация R2 аналогична конфигурации R1. Конфигурация R3 аналогична конфигурации R4. Конфигурация R5 аналогична конфигурации R6.
- После завершения настройки R1 анонсирует BGP-сети прямой маршрут к 192.168.1.0/24. R7 анонсирует BGP-сети прямой маршрут к 192.168.2.0/24.

Реализация требований и устранение неполадок в BGP-сети – Пример 2 (4)

- Проверьте записи маршрутизации R1 и R7.

```
[R1]dis bgp routing-table

 Total Number of Routes: 2
      Network          NextHop        MED        LocPrf    PrefVal Path/Ogn
*>i   192.168.2.0      6.6.6.6                0          100       0             200i

[R1]display ip routing-table
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
192.168.2.0/24      IBGP    255  0           6.6.6.6       Ethernet0/0/1
```

```
[R1]ping -a 192.168.1.1 192.168.2.1
  PING 192.168.2.1: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 192.168.2.1 ping statistics ---
    5 message(s) transmitted
    0 message(s) received
    100.00% message loss
```

```
<R7>dis bgp routing-table

 Total Number of Routes: 2
      Network          NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   192.168.1.0      10.0.67.6                       0          100i
 *>   192.168.2.0      0.0.0.0                0          0                 I

<R7>display ip routing-table
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
127.0.0.1/32        Direct  0    0           D   127.0.0.1       InLoopBack0
192.168.1.0/24      EBGP    255  0           D   10.0.67.6       Ethernet0/0/1
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- После выполнения конфигураций все отношения соседства BGP установлены, и все маршруты получены в OSPF.
- Конфигурация R2 аналогична конфигурации R1. Конфигурация R3 аналогична конфигурации R4. Конфигурация R5 аналогична конфигурации R6.
- После установления отношений соседства BGP каждый маршрутизатор анонсирует маршрут к собственному loopback-адресу.

Реализация требований и устранение неполадок в BGP-сети – Пример 2 (5)

- Проверьте записи маршрутизации R1 и R7.

```
R1]display ip routing-table
Destination/Mask  Proto  Pre  Cost      NextHop         Interface
192.168.2.0/24    IBGP   255  0         6.6.6.6         Ethernet0/0/1
6.6.6.6/32        OSPF   10   3         10.0.12.2       Ethernet0/0/1
```

```
[R2]display ip routing-table
Destination/Mask  Proto  Pre  Cost      NextHop         Interface
192.168.2.0/24    IBGP   255  0         5.5.5.5         Ethernet0/0/1
5.5.5.5/32        OSPF   10   3         10.0.12.1       Ethernet0/0/1
```

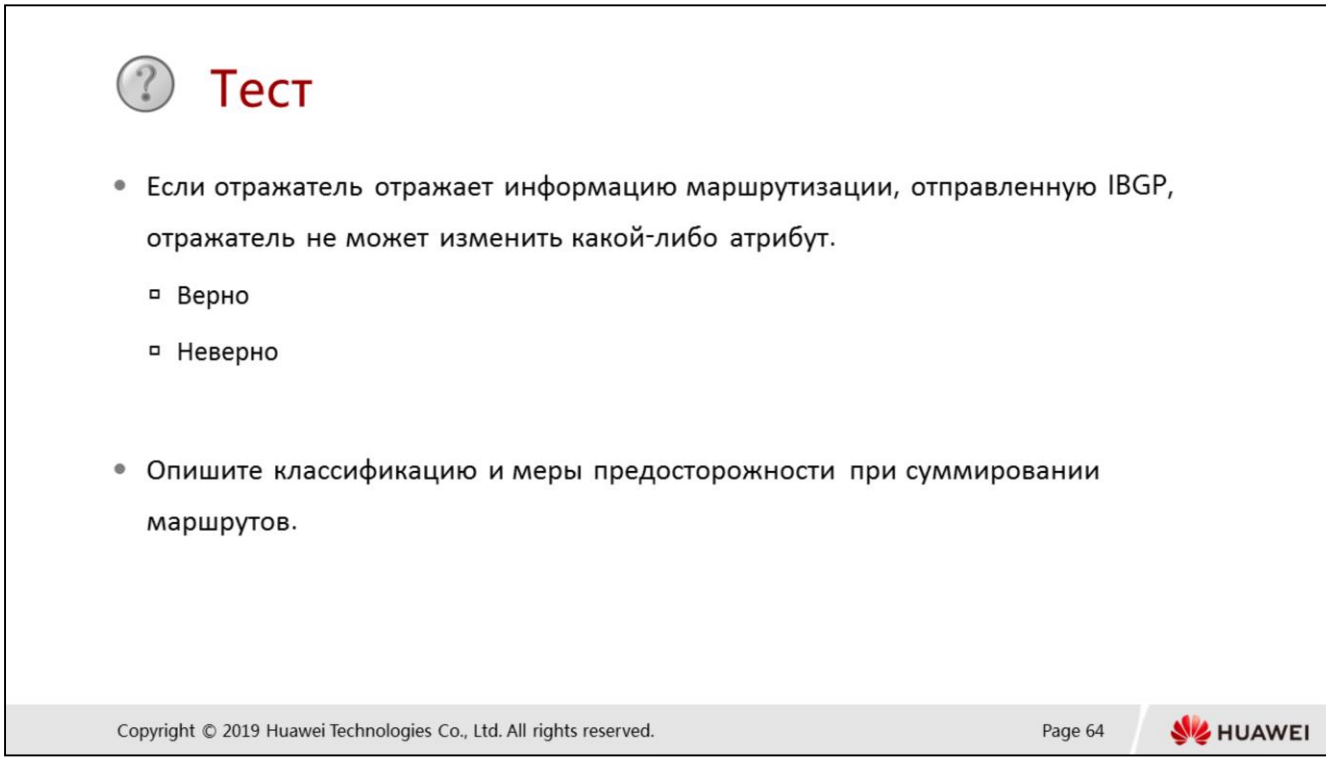
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Анализ неполадок:
  - R7 анонсирует префикс маршрута 192.168.2.0/24 маршрутизаторам R5 и R6.
  - R5 и R6 получают пакеты и анонсируют префикс своим IBGP-соседям R3 и R4 соответственно.
  - В данном разделе анализируется работа маршрутизатора R4. На R4 выполняется процесс выбора пути. R3 также отправляет префикс маршрута 192.168.2.0/24 в R4. В соответствии с предыдущими 13 правилами выбора маршрута BGP, R4 выбирает маршрут с наименьшей стоимостью IGP. Следовательно, R6 выбирается в качестве следующего узла. Затем R4 отправляет информацию об оптимальном пути к R3 и R1.
  - Аналогичным образом, R3 выбирает R5 в качестве следующего узла.
  - Ключ находится в R1 и R2. R1 может получать обновления маршрута только от R4. Таким образом, следующим узлом к 192.168.1.0/24 является R4. Аналогичным образом, следующим узлом R2 к 192.168.1.0/24 является R5.
  - После рекурсивного запроса маршрутов IGP пакеты от 192.168.1.1 до 192.168.2.1 переадресовываются между R1 и R2 до тех пор, пока TTL в IP-пакетах не будет сокращен до 0.

Реализация требований и устранение неполадок в BGP-сети – Пример 2 (6)

- Краткое описание примера:
  - Для конфигурирования отражателя используйте следующие правила:
    - Не настраивайте отношения соседства между отражателем и клиентом через не клиента.
    - Не настраивайте отношения соседства между отражателем и не клиентом через клиента.
    - Не устанавливайте отношения соседства IBGP между клиентом отражателя и не клиентом.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.



- Ответы:
  1. A
  2. Суммирование маршрутов бывает автоматическим и административным.
     - Автоматическое суммирование: суммированию подлежат только маршруты, импортированные с помощью команды **import-route**. Для суммирования можно использовать только естественные маски. IPv6 не поддерживает автоматическое суммирование.
     - Административное суммирование: суммированию подлежат маршруты IPv4 и IPv6. Можно настроить подавление определенных маршрутов и опцию AS_Set.

Краткое содержание

- Развертывание сети при большом количестве маршрутов BGP
  - Суммирование маршрутов
  - Группы соседей
  - Отражатели маршрутов
  - Конфедерация
  - Атрибуты community
- Основы проектирования интернет-сети
  - В каких типах сетей нужен протокол BGP?
  - Оптимизация BGP-сети
- Стандартная конфигурация BGP и устранение неполадок

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Дополнительная информация

- RFC 3065: RFC 3065 Autonomous System Confederations for BGP
- RFC 4271: RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- RFC 4360: RFC 4360 BGP Extended Communities Attribute
- RFC 4456: RFC 4456 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
- RFC 4760: RFC 4760 Multiprotocol Extensions for BGP-4
- RFC 4893: RFC 4893 BGP Support for Four-octet AS Number Space

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Рекомендации

- Раздел Huawei Learning
  - http://support.huawei.com/learning/en/newindex.html
- Библиотека примеров на сайте технической поддержки Huawei
  - http://support.huawei.com/enterprise/servicecenter?lang=en

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Спасибо!

www.huawei.com

HCIE-R&S
— Импорт и управление маршрутами

www.huawei.com

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Введение

- В сложных IP-сетях политики маршрутизации, как правило, реализуются на основе фактических сетевых требований к изменению маршрутов переадресации сетевого трафика путем изменения атрибутов маршрутов (включая достижимость маршрута). Политика маршрутизации может использоваться для фильтрации маршрутов, установки атрибутов маршрутов и контроля приема, анонсирования и импорта маршрутов.
- В данном документе описывается реализация и конфигурации часто используемых фильтров маршрутов, политик маршрутизации и маршрутизации на основе политик (PBR).

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Цели

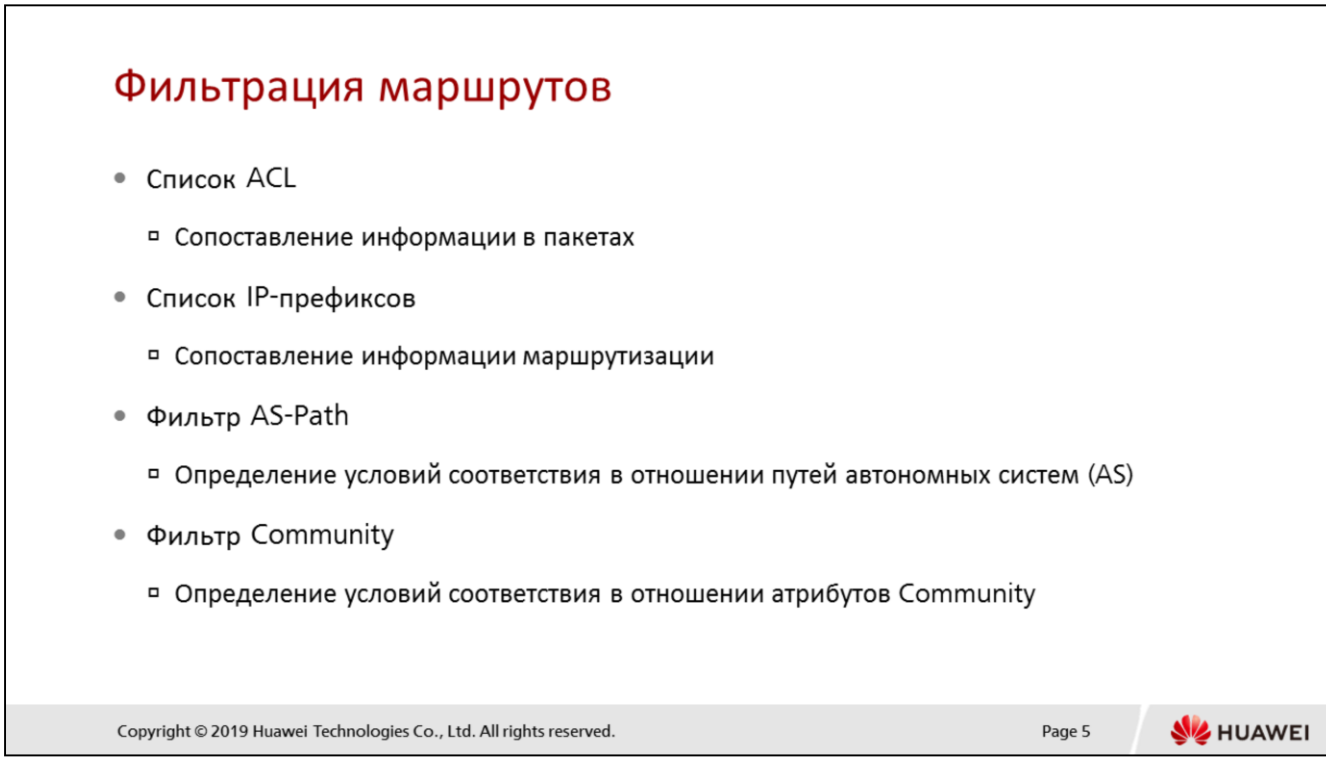
- После завершения этого курса вы будете:
  - Уметь работать с фильтрами маршрутов, таких как списки контроля доступа (ACL) и списки IP-префиксов.
  - Понимать принципы и методы конфигурирования политик маршрутизации.
  - Понимать принципы и методы конфигурирования PBR.
  - Использовать политики маршрутизации и PBR для управления маршрутами и переадресации пакетов.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Содержание

1. **Фильтрация маршрутов**
   - **Список ACL**
   - Список IP-префиксов
   - Фильтр AS-Path
   - Фильтр Community
2. Политика маршрутизации и PBR
3. Политика маршрутизации и команды конфигурирования PBR
4. Анализ примеров

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

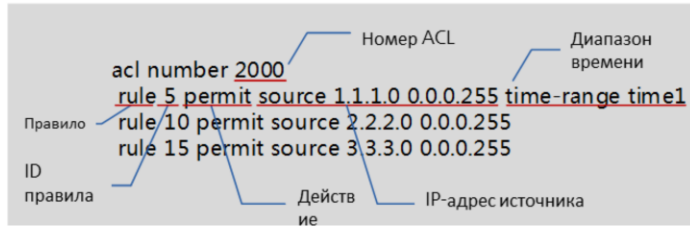


- Список ACL
  - ACL состоит из списка правил. Каждое правило содержит условие, определяющее разрешение или отказ. Эти правила классифицируют пакеты на основе содержащейся в них информации. После применения правил ACL маршрутизаторы определяют, какие пакеты следует принять и отклонить.
  - ACL определяет набор правил и идентифицирует пакеты данных, которые необходимо отфильтровать. Затем маршрутизаторы принимают или отклоняют пакеты данных в соответствии с сконфигурированными правилами. Кроме того, на ACL могут ссылаться на другие сервисные модули в качестве базовой конфигурации.
- Список IP-префиксов
  - Список IP-префиксов сопоставляет маршруты с каждой записью в списке для фильтрации маршрутов согласно определенному режиму сопоставления.
  - Список IP-префиксов может использоваться для фильтрации только информации маршрутизации, но не может фильтровать пакеты данных.
- Фильтр AS-Path
  - Информация о каждом маршруте протокола граничного шлюза (BGP) содержит домен путей AS. Фильтры AS-Path определяют правила сопоставления, применяемые к доменам путей AS. Фильтр AS-Path используется для фильтрации только в BGP.
- Фильтр Community
  - Информация о каждом маршруте BGP может включать один или несколько атрибутов

community. Фильтр community определяет условия сопоставления атрибутов community.

Фильтрация маршрутов: создание списка ACL

- Список ACL представляет собой набор одного или нескольких правил. Правила описывают параметры сопоставления пакетов, такие как IP-адрес источника, IP-адрес назначения и номер порта пакетов.
- Список ACL фильтрует пакеты на основе правил. Устройство с сконфигурированным списком ACL сравнивает пакеты по правилам ACL для фильтрации пакетов определенного типа, а затем принимает или отклоняет эти пакеты в соответствии с политиками, используемыми сервисным модулем, к которому применяется ACL.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Номер ACL: идентифицирует нумерованный ACL.
  - В зависимости от функций существуют таки типы ACL, как базовый ACL, расширенный ACL, ACL 2 уровня и пользовательский ACL. У таких ACL разные диапазоны нумерации.
  - Вы также можете настроить имя ACL, чтобы помнить его цель. В таком случае имя ACL будет выступать в качестве имени домена, представляющее IP-адрес. Такой ACL называется именованным ACL.
  - Номер ACL может быть частью имени ACL. То есть, вы также можете указать номер ACL в дополнении к имени. Если вы не укажете номер ACL, система назначит ему номер автоматически.
- Правило: описывает условия сопоставления пакетов.
  - ID правила: идентифицирует правило ACL. Идентификаторы правил могут быть установлены вручную или автоматически назначены системой. Идентификатор правила ACL может обозначаться числом от 0 до 4294967294. Идентификаторы правил в ACL назначаются в порядке возрастания. Поэтому на рисунке выше правило 5 находится в первой строке ACL, а правило 15 – в нижней строке. Система сверяет пакеты с правилами с первой строки до нижней строки и останавливает сверку, если пакеты соответствует какому-либо правилу.
  - Действие: разрешение и отказ.
  - Условия: списки ACL содержат условия для выполнения сопоставления. В дополнение к исходному IP-адресу и временному диапазону, показанному на рисунке выше, ACL поддерживает многие другие условия, например, информацию в заголовке кадра Ethernet 2 уровня (например, MAC-адрес источника, MAC-адрес назначения и тип протокола Ethernet), информацию пакета 3 уровня (например, IP-адрес назначения и тип протокола) и информацию пакета 4 уровня (например, номер порта TCP/UDP).
  - Если ACL содержит правила, система сопоставляет пакеты с правилами в порядке возрастания идентификаторов правил. Если пакеты соответствуют разрешающему правилу, система прекращает сопоставление и возвращает сообщение о соответствии "positive match (permit)". Если пакеты соответствуют правилу отклонения, система прекращает сопоставление и

возвращает сообщение о несоответствии "positive match (deny)". Если пакеты не соответствуют какому-либо правилу в ACL, система продолжает сопоставлять пакеты со следующим правилом. Если пакеты не соответствуют какому-либо правилу в ACL, система возвращает результат "negative match".

Фильтрация маршрутов: классификация ACL

- Списки ACL классифицируются по различным параметрам.
  - По типу именования ACL:
    - Нумерованный ACL
    - Именованный ACL
  - По методу определения правил ACL:
    - Основные ACL (диапазон номеров: 2000–2999)
    - Расширенные ACL (диапазон номеров: 3000–3999)
    - ACL 2 уровня (диапазон номеров: 4000–4999)
    - Пользовательские ACL (диапазон номеров: 6000–6031)

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Основной ACL
  - Основной ACL определяет правила на основе IP-адресов отправителей, информации о фрагментации и временного диапазона.
- Расширенный ACL
  - Расширенный ACL определяет правила на основе адреса IPv4 отправителя, адреса IPv4 получателя, типа протокола IPv4, типа протокола ICMP, номеров портов TCP отправителя/получателя, номеров портов UDP отправителя/получателя и временного диапазона.
- ACL 2 уровня
  - ACL 2 уровня определяет правила на основе информации в заголовках кадров Ethernet пакетов, таких как MAC-адрес отправителя, MAC-адрес получателя и тип протокола 2 уровня.
- Пользовательский ACL
  - Пользовательский ACL определяет правила на основе адреса IPv4 отправителя, адреса IPv4 получателя, типа протокола IPv4, типа протокола ICMP, номеров портов TCP отправителя/получателя, номеров портов UDP отправителя/получателя.
- Кроме того, существуют ACL IPv6 (ACL6), включая основные ACL6 и расширенные ACL6.
  - Основной ACL6: определяет правила на основе адреса IPv6 отправителя, информации о фрагментации и временного диапазона.
  - Расширенный ACL6: определяет правила на основе адреса IPv6 отправителя, адреса IPv6

получателя, типа протокола IPv6, типа протокола ICMPv6, номеров портов TCP отправителя/получателя, номеров портов UDP отправителя/получателя и временного диапазона.

Фильтрация маршрутов: порядок сопоставления пакетов с правилами ACL

- Порядок конфигурации (config)
  - Пакеты сопоставляются с правилами ACL в порядке возрастания идентификаторов правил.
- Автоматический порядок (auto)
  - Пакеты сопоставляются с правилами ACL в соответствии со степенью точности правил (принцип «в глубину»). В следующей таблице приведен порядка сопоставления пакетов с правилами ACL.

Тип ACL	Порядок сопоставления
Основной ACL	1. Сначала сопоставляется правило, определяющее параметры экземпляра VPN. 2. Затем сопоставляется правило, определяющее наименьший диапазон IP-адресов отправителя. 3. Сопоставляется правило с наименьшим идентификатором.
Расширенный ACL	1. Сначала сопоставляется правило, определяющее параметры экземпляра VPN. 2. Сначала сопоставляется правило, определяющее тип протокола по IP. 3. Затем сопоставляется правило, определяющее наименьший диапазон IP-адресов отправителя. 4. Сопоставляется правило, определяющее наименьший диапазон IP-адресов получателя. 5. Сопоставляется правило, определяющее наименьший диапазон номеров портов 4 уровня. 6. Сопоставляется правило с наименьшим идентификатором.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Порядок сопоставления пакетов с правилами ACL
  - ACL состоит из нескольких условий отказа и разрешения, каждое из которых описывает правило. Эти правила могут повторяться или противоречить друг другу. Одно правило может содержать другое правило, но два правила должны быть разными.
  - Поддерживаются порядка сопоставления пакетов с правилами ACL: порядок конфигурации (config) и автоматический порядок (auto). Когда система сопоставляет пакет данных с правилами ACL, порядок сопоставления правил определяет приоритет. ACL обрабатывает совпадение или противоречия между правилами на основании приоритета. По умолчанию установлен порядок сопоставления **config**.
- Порядок конфигурации (config)
  - Правило с меньшим идентификатором в одну из первых строк ACL. Это правило сопоставляется с пакетом в первую очередь.
  - Если у правила нет идентификатора, установленного вручную, система автоматически назначает ему идентификатор. Идентификатор будет больше, чем самый большой идентификатор правила в ACL, и будет минимальным целым числом, кратным инкременту. Поэтому это правило сопоставляется с пакетом в последнюю очередь.
- Автоматический порядок (auto)
  - Система сопоставляет пакеты с правилами ACL в соответствии со степенью точности правил (принцип «в глубину»).
  - Система сопоставляет пакеты с правилами в порядке убывания точности. Правило с наивысшей точностью определяет строжайшие условия (например, тип протокола и диапазоны IP-адресов отправителя и получателя). Например, правило ACL может быть сконфигурировано на основе шаблонной маски IP-адреса. Меньший шаблон идентифицирует меньший сегмент сети и более строгие условия.
  - Если правила ACL имеют один и тот же порядок, они сопоставляются в порядке

возрастания идентификаторов правил.

ACL в протоколе IPv6

- Списки ACL в протоколе IPv6 (также называемые ACL6s) фильтруют пакеты IPv6 на основе сконфигурированных правил. Применение ACL6 аналогично применению ACL.
- Классификация ACL6

Категория	Диапазон номеров	Сценарий использования
Основной ACL6	2000–2999	Основной ACL6 определяет правила на основе адресов IPv6 отправителя, экземпляров VPN, флагов фрагментации и временных диапазонов пакетов IPv6.
Расширенный ACL6	3000–3999	Расширенный ACL определяет правила на основе адресов IPv6 отправителя и получателя, типов протоколов IPv6 и свойствах протокола (например, номеров портов TCP отправителя и получателя, типе протокола ICMPv6 и коде ICMPv6).

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

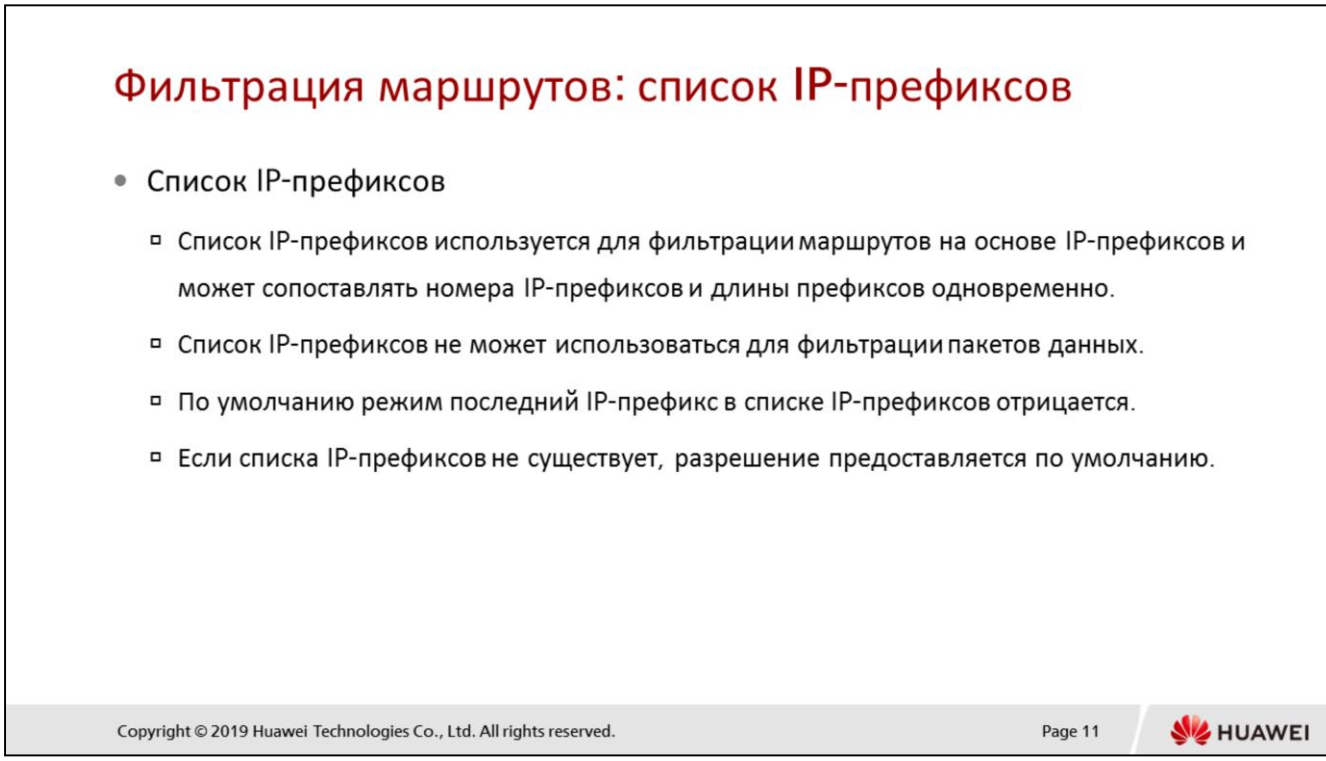
HUAWEI

- Конфигурация списков ACL6 и ACL выполняется с помощью различных команд. ACL6 и ACL могут иметь одинаковый номер и не влияют друг на друга.
- Пример:
  - [RouterA] acl ipv6 number 3001
  - [RouterA-acl6-adv-3001] rule deny ipv6 source 3001::2/64
  - [RouterA] acl 3001
  - [Router-acl-adv-3001] rule permit ip source 202.169.10.5 0.0.0.0

Содержание

1. **Фильтрация маршрутов**
   - Список ACL
   - **Список IP-префиксов**
   - Фильтр AS-Path
   - Фильтр Community
2. Политика маршрутизации и PBR
3. Политика маршрутизации и команды конфигурирования PBR
4. Анализ примеров

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.



- Список IP-префиксов
  - Каждый список IP-префиксов может содержать несколько IP-префиксов, и каждая запись IP-префикса соответствует индексу. Система сравнивает префикс маршрута с IP-префиксами в списке в порядке возрастания индексов. Если какой-либо IP-префикс совпадает, система прекращает сопоставление с прочими IP-префиксами. Если не обнаружено ни одного совпадения с IP-префиксами в списке, маршрут отфильтровывается.
  - Список IP-префиксов поддерживает точное сопоставление или сопоставление в пределах указанной длины маски.
  - Сравнение со списком IP-префиксов может применяться к определенному маршруту или маршрутам с определенной длиной маски. Длина маски префикса также может быть указана с помощью ключевых слов **greater-equal** (больше или равно) или **less-equal** (меньше или равно). Если ключевое слово **greater-equal** или **less-equal** не указано, используется точное соответствие. То есть, сопоставляется только маршрут с той же длиной маски, что и в списке IP префиксов. Если указано только ключевое слово **greater-equal**, сопоставляются только маршруты, длина маски которых колеблется от **greater-equal** до 32 бит. Если указано только ключевое слово **less-equal**, то сопоставляются маршруты, длина маски которых варьируется от указанного значения до значения less-equal.
  - Значения *greater-equal-value* и *less-equal-value* должны отвечать следующим требованиям: *mask-length (длина маски) ≤ greater-equal-value ≤ less-equal-value ≤ 32.*
- Характеристики списка IP-префиксов
  - Если ни один из IP-префиксов в списке не совпал, по умолчанию последний IP-префикс в

списке отрицается.

- Если списка IP-префиксов не существует, разрешение предоставляется по умолчанию.

Примеры списка IP префиксов

- ip ip-prefix FILTER index 10 permit 1.1.1.0 24
  - Это точное соответствие. Допускается только маршрут к 1.1.1.1/24.
- ip ip-prefix FILTER index 10 permit 1.1.1.0 24 less-equal 32
  - Разрешены только маршруты к 1.1.1.0 с длиной маски от 24 бит до 32 бит
- ip ip-prefix FILTER index 10 permit 1.1.1.0 24 greater-equal 26
  - Разрешены только маршруты к 1.1.1.0 с длиной маски от 26 бит до 32 бит.
- ip ip-prefix FILTER index 10 permit 1.1.1.0 24 greater-equal 26 less-equal 32
  - Разрешены только маршруты к 1.1.1.0 с длиной маски от 26 бит до 32 бит.
- ip ip-prefix FILTER index 10 permit 0.0.0.0 0 greater-equal 8 less-equal 32
  - Разрешены маршруты с длиной маски от 8 бит до 32 бит.
- ip ip-prefix FILTER index 20 permit 0.0.0.0 0 less-equal 32
  - Разрешены все маршруты.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Список IPv6-префиксов

- Списки IPv6-префиксов фильтруют пакеты IPv6 на основе сконфигурированных правил. Они работают аналогично спискам IP-префиксов.
- Список IPv6-префиксов используется для фильтрации маршрутов на основе адресов IPv6. Список IPv6-префиксов может содержать несколько записей с каждой записью, в каждой из которых будет указан диапазон IPv6-префиксов. Связь между записями устанавливается с помощью "OR". То есть, если информация маршрута соответствует одной записи, маршрут соответствует; если маршрут не соответствует какой-либо записи, маршрут не соответствует.
- Все маршруты, информация которых не была сопоставлена со списком, отклоняются по умолчанию. Если все записи устанавливают действие deny, все маршруты отфильтровываются. Поэтому после нескольких правил deny необходимо настроить параметр **permit :: 0 less-equal 128**, чтобы разрешить все прочие маршруты IPv6.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Примеры списка IPv6-префиксов

- Настройте разрешение маршрутов с длиной маски от 32 бит до 64 бит.
  - [Huawei] ip ipv6-prefix abc permit :: 0 greater-equal 32 less-equal 64
- Настройте отклонение маршрутов с IP-префиксом FC00:3:0:D00::/32 и префиксами длиннее 32 бит и разрешение других маршрутов IPv6.
  - [Huawei] ip ipv6-prefix abc deny 3FFE:D00:: 32 less-equal 128
  - [Huawei] ip ipv6-prefix abc permit :: 0 less-equal 128
- Сконфигурируйте список IPv6-префиксов с именем p3 для отклонения маршрутов к IPv6-адресам, начиная с ::1 to ::FFFF:FFFF.
  - [Huawei] ip ipv6-prefix p3 index 10 deny :: 96 match-network
  - [Huawei] ip ipv6-prefix p3 index 20 permit :: 0 less-equal 128

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Содержание

1. **Фильтрация маршрутов**
   - Список ACL
   - Список IP-префиксов
   - **Фильтр AS-Path**
   - Фильтр Community
2. Политика маршрутизации и PBR
3. Политика маршрутизации и команды конфигурирования PBR
4. Анализ примеров

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Фильтрация маршрутов: фильтр AS-Path

- Фильтр AS-Path Filter
  - Фильтры AS-Path используют атрибут AS-Path протокола BGP для фильтрации маршрутов.
  - Фильтры AS-Path используют регулярные выражения для определения правил сопоставления.
- Примеры
  - ip as-path-filter 10 permit .*
    - Сконфигурируйте фильтр AS-Path 10, чтобы разрешить все маршруты.
  - ip as-path-filter 10 permit _100$
    - Сконфигурируйте фильтр AS-Path 10, чтобы разрешить маршруты, исходящие из AS100.
  - ip as-path-filter 10 permit ^100_
    - Сконфигурируйте фильтр AS-Path 10, чтобы разрешить маршруты, полученных от AS100.
  - ip as-path-filter 10 permit _100|200$
    - Сконфигурируйте фильтр AS-Path 10, чтобы разрешить маршруты, исходящие из AS100 или AS200.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Фильтр AS-Path использует атрибут AS-Path протокола BGP для фильтрации маршрутов. Он используется только тогда, когда BGP анонсирует и принимает маршруты.

- Атрибут AS-Path записывает номер AS, через который проходит маршрут, в левую часть списка AS-Path. Обратите на это особое внимание при конфигурировании фильтра AS-Path.
  - Если маршрут исходит из AS100, проходит через AS300, AS200 и AS500 и затем достигает AS600, в AS600 атрибутом AS-Path маршрута является 500 200 300 100.

Фильтрация маршрутов: часто используемые регулярные выражения

Выражение	Значение
^$	Маршруты, исходящие из локальной AS
.*	Все маршруты
_10_	Маршруты, проходящие через AS10
^10_	Маршруты, полученные только от AS10
_10$	Все маршруты, исходящие из AS10

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI



Содержание

1. **Фильтрация маршрутов**
   - Список ACL
   - Список IP-префиксов
   - Фильтр AS-Path
   - **Фильтр Community**
2. Политика маршрутизации и PBR
3. Политика маршрутизации и команды конфигурирования PBR
4. Анализ примеров

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Фильтрация маршрутов: фильтр Community

- Фильтр Community
  - Фильтры Community используют атрибуты Community BGP для фильтрации маршрутов.
- Примеры
  - ip community-filter 1 permit 100:1
    - **Установите атрибут community для сопоставления маршрутов с 100: 1.**
  - ip community-filter 1 permit no-export
    - **Установите атрибут community для сопоставления маршрутов с no-export.**

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Фильтр community использует атрибуты community BGP для фильтрации маршрутов. Он используется только тогда, когда BGP анонсирует и принимает маршруты.

- Атрибуты community включают основные и расширенные атрибуты community.
  - Атрибуты community, настроенные пользователем, и общеизвестные атрибуты community являются основными атрибутами community.
  - Атрибуты route target (RT) и Site of Origin (SoO) в сценариях использования MPLS VPN являются расширенными атрибутами community.

Содержание

1. Фильтрация маршрутов
2. **Политика маршрутизации и PBR**
   - **Политика маршрутизации**
   - PBR
   - Сравнение политики маршрутизации и PBR
3. Политика маршрутизации и команды конфигурирования PBR
4. Анализ примеров

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Политика маршрутизации

- Политика маршрутизации
  - Политика маршрутизации используется для фильтрации маршрутов и установки атрибутов маршрута. Изменяя атрибуты маршрута, политика маршрутизации может изменять пути передачи сетевого трафика.
  - Политика маршрутизации настраивается с помощью команды **route-policy**.
- Механизм работы политики маршрутизации



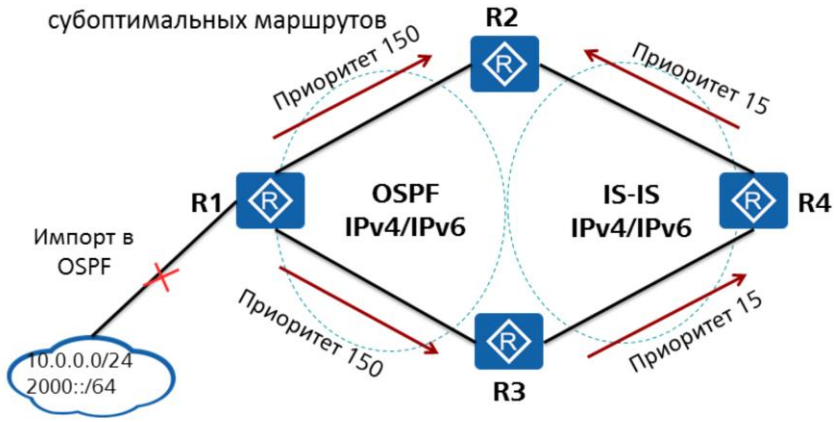
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Политика маршрутизации изменяет путь переадресации пакетов путем фильтрации маршрутов и настройки атрибутов маршрута. Например, атрибуты маршрутов (включая Reachability) могут быть установлены для изменения пути переадресации сетевого трафика.
- Политика маршрутизации используется главным образом в следующих сценариях:
  - Контроль импорта маршрутов.
    - Политика маршрутизации может использоваться для предотвращения использования субоптимальных путей или возникновения петель при импорте маршрутов.
  - Контроль приема и анонсирования маршрутов.
    - Принимаются или анонсируются только требуемые и действительные маршруты.
  - Изменение атрибутов указанных маршрутов.
    - Атрибуты маршрутов, отфильтрованных политикой маршрутизации, могут быть изменены для настройки и оптимизации сетей.
- Механизм работы политики маршрутизации
  - Политика маршрутизации состоит из нескольких узлов. Система проверяет маршруты в узлах политики маршрутизации в порядке возрастания идентификаторов узлов. Один узел может быть сконфигурирован с несколькими условиями **if-match** и **apply**. Условия **if-match** определяют правила сопоставления для этого узла, а условия **apply** определяют действия для маршрутов, соответствующих правилам. Связь между условиями **if-match** устанавливается с помощью "AND". То есть, маршрут должен соответствовать всем условиям **if-match**. Связь между узлами политики маршрутизации устанавливается с помощью "OR". То есть, если маршрут совпадает с одним узлом, маршрут соответствует политике маршрутизации. Если маршрут не совпадает с каким-либо узлом, маршрут не соответствует политике маршрутизации.
  - Взаимосвязь между условиями **if-match** в узле политики маршрутизации устанавливается с помощью "AND". Маршрут должен соответствовать всем правилам до выполнения действия, определенного условием **apply**. Связь между условиями **if-match** в командах **if-match route-type** и **if-match interface** устанавливается с помощью "OR", но связь между условиями **if-**

match в этих двух командах и других командах устанавливается с помощью "AND".

Политика маршрутизации: контроль импорта маршрутов

- Контроль импорта маршрутов.
  - Контроль импорта маршрутов для предотвращения петель или использования субоптимальных маршрутов

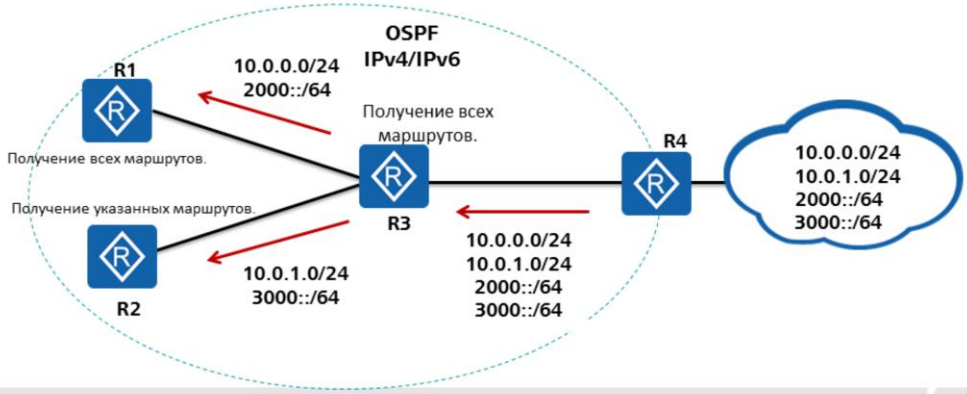


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- В вышеприведенной топологии показано повторное двунаправленное анонсирование маршрута. При отсутствии контроля могут выбираться субоптимальные маршруты и возникать петли. Анализ неисправностей выглядит следующим образом:
  - Маршрутизатор R1 импортирует маршруты к сетевым сегментам 10.0.0.0/24 и 2000::/64 в OSPF. Маршрутизаторы R2 и R3 импортируют маршруты в IS-IS соответственно. Предположим, что R2 импортирует маршруты в IS-IS раньше, чем R3. Затем R2 получит маршруты к 10.0.0.0/24 и 2000::/64 как из OSPF, так и из IS-IS. R2 предпочтет маршруты, полученные из IS-IS, в соответствии с приоритетами в протоколах маршрутизации (в процессе OSPF предпочтение внешних маршрутов составляет 150, а предпочтение маршрутов IS-IS -15.) Поэтому, когда R2 получает доступ к сегментам сети 10.0.0.0/24 и 2000:: / 64, используется субоптимальный маршрут R4-R3-R1. Чтобы предотвратить эту проблему, выполните команду **route-policy** на R2, чтобы сделать приоритет маршрута OSPF ASE выше, чем для маршрута, извлеченного из IS-IS, чтобы R2 выбрал правильный маршрут.
  - Если интерфейс на R1, подключенный к сетевым сегментам 10.0.0.0/24 и 2000:: / 64, закрыт, внешние LSA-пакеты устаревают в зоне OSPF. R2 импортирует маршрут в OSPF, поскольку он извлек сегменты сети 10.0.0.0/24 и 2000:: / 64 из IS-IS. Таким образом, R1 и R3 могут узнавать маршруты к сетевым сегментам 10.0.0.0/24 и 2000:: / 64 от R2. Когда R2 получает доступ к сетевым сегментам 10.0.0.0/24 и 2000:: / 64, трафик передается по пути R4-> R3-> R1-> R2, в результате чего возникает петля маршрутизации. Чтобы предотвратить петлю, можно добавить теги к записям маршрутизации и фильтровать маршруты с определенными тегами для предотвращения петель.

Политика маршрутизации: контроль приема и анонсирования маршрутов

- Контроль приема и анонсирования маршрутов.
  - Для оптимизации записей маршрутизации принимаются определенные маршруты.
  - Как правило, эта функция реализуется с помощью команды **filter-policy**.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Контроль приема и анонсирования маршрутов.
  - Принимаются только нужные и действительные маршруты. Это сокращает размер таблицы маршрутизации и повышает безопасность сети.

- Описание топологии
  - R4 импортирует маршруты к точкам 10.0.X.0/24, 2000::/64 и 3000::/64 в OSPF. В соответствии с сервисными требованиями, R1 может получать только маршруты к 10.0.0.0/24 и 2000::/64, а R2 может получать только маршруты к 10.0.1.0/24 и 3000::/64. Это требование можно осуществить с помощью команды filter-policy.

Политика маршрутизации: политика фильтрации (OSPF)

- Filter-policy Import
  - Команда **filter-policy import** используется для конфигурирования политики фильтрации для фильтрации полученных маршрутов. Только маршруты, прошедшие фильтрацию, могут быть добавлены в таблицу маршрутизации. Маршруты, не прошедшие фильтрацию, не могут быть добавлены в таблицу маршрутизации, но могут быть анонсированы.
  - Информация маршрутизации OSPF регистрируется в базе данных состояния канала (LSDB). Вместо фильтрации полученных или отправленных LSA-пакетов, устройство фильтрует маршруты, рассчитанные OSPF с помощью команды **filter-policy import**.
- Filter-policy Export
  - После импорта внешних маршрутов в OSPF с помощью команды **import-route** вы можете использовать команду **filter-policy export** для фильтрации импортируемых маршрутов, которые должны анонсироваться для предотвращения петель. Только внешние маршруты, прошедшие фильтрацию, могут быть преобразованы в LSA-пакеты 5 или 7 типа и анонсированы.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Команда **filter-policy import** настраивает политику фильтрации для фильтрации маршрутов, получаемых OSPF.
- Команда **filter-policy export** настраивает политику фильтрации для фильтрации импортируемых маршрутов, подлежащих анонсированию.
  - Параметр **protocol** или **process-id** может быть задан для определения указанного протокола или процесса. Если параметр **protocol** или **process-id** не указан, OSPF фильтрует все импортированные маршруты.
  - Эта команда может быть сконфигурирована только на пограничных маршрутизаторах автономной системы (ASBR), так как LSA-пакеты 5 и 7 типа создают ABSR-маршрутизаторы.

Политика маршрутизации: политика фильтрации (IS-IS)

- Filter-policy Import
  - Записи маршрутизации IS-IS необходимо добавить в таблицу IP-маршрутизации для управления переадресацией IP-пакетов. Если таблица маршрутизации IS-IS содержит маршруты к определенному сегменту сети, но они скорее всего не будут добавлены в таблицу IP-маршрутизации, выполните команду filter-policy import с указанием условий (например, основным списком ACL, IP-префиксом и политики маршрутизации), чтобы разрешить добавлять только необходимые маршруты IS-IS в таблицу IP-маршрутизации.
- Filter-policy Export
  - Когда IS-IS и другие протоколы маршрутизации работают в сети, а пограничный маршрутизатор в домене маршрутизации IS-IS импортировал маршруты других протоколов маршрутизации, пограничный маршрутизатор будет анонсировать все импортированные маршруты своим соседям IS-IS по умолчанию. Для настройки анонсирования только определенных импортируемых маршрутов соседям используется команда filter-policy export.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Команда **filter-policy import** настраивает политику фильтрации, позволяющую IS-IS фильтровать полученные маршруты для добавления в таблицу IP-маршрутизации.
  - Выполнение этой команды на маршрутизаторе не влияет на лавинную передачу LSP-пакетов и синхронизацию базы данных LSDB на маршрутизаторе, но влияет на локальную таблицу IP-маршрутизации.
- Команда **filter-policy export** настраивает политику фильтрации, позволяющую IS-IS фильтровать импортируемые маршруты, подлежащие анонсированию.
  - Выполнение этой команды не влияет на маршруты на локальном устройстве, но соседям IS-IS будут анонсированы только определенные импортированные маршруты.

Политика маршрутизации: политика фильтрации (BGP)

- Filter-policy Import
  - Команда filter-policy import используется для фильтрации маршрутов, полученных устройством с включенным протоколом BGP, для определения необходимости их добавления в таблицу маршрутизации BGP.
- Filter-policy Export
  - Команда filter-policy export используется для фильтрации маршрутов, которые должны быть анонсированы глобально.
  - После запуска команды filter-policy export BGP фильтрует маршруты, импортированные с помощью команды import-route (BGP). Только маршруты, прошедшие фильтрацию, могут быть добавлены в локальную таблицу маршрутизации BGP и анонсированы BGP.

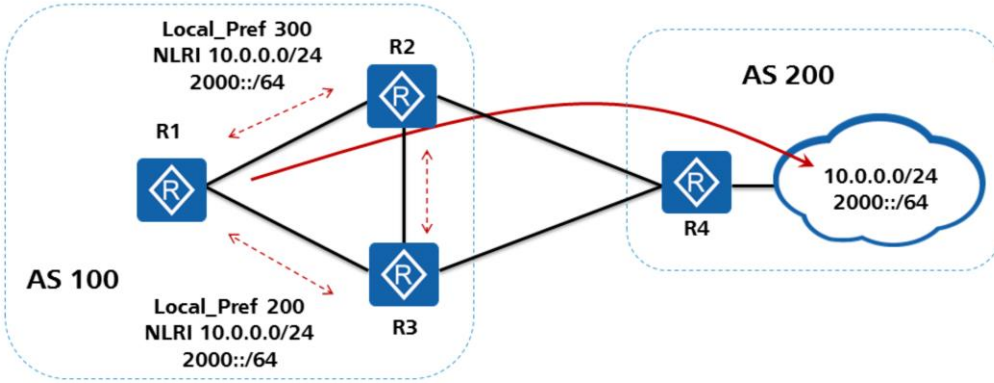
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Команда **filter-policy import** настраивает на устройстве фильтрацию полученных маршрутов.
- Команда **filter-policy export** настраивает на устройстве фильтрацию маршрутов, подлежащие анонсированию. BGP анонсирует только маршруты, прошедшие фильтрацию.
  - Если параметр **protocol** указан в команде, то только маршруты, импортированные из указанного протокола, будут проходить фильтрацию. Если параметр **protocol** не указан, фильтрацию будут проходить маршруты, импортированные из всех протоколов.

Политика маршрутизации: настройка атрибутов определенных маршрутов

- Установите атрибуты для определенных маршрутов.
  - Вы можете задать атрибуты для определенных маршрутов с помощью политик маршрутизации.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Описание топологии
  - Выполните команду **route-policy**, чтобы изменить атрибут **Local_Pref** маршрутов BGP, который влияет на направление переадресации трафика. На R2 атрибут **Local_Pref** маршрутов к 10.0.0.0/24 и 2000::/64 получен из EBGP в 300. На R3 настройте атрибут **Local_Pref** маршрутов, полученных из EBGP в 200. R1, R2 и R3 обмениваются маршрутами друг с другом через IBGP. Наконец, R2 выбирается как выход локальной AS к точкам 10.0.0.0/24 и 2000::/64.



Содержание

1. Фильтрация маршрутов
2. **Политика маршрутизации и PBR**
   - Политика маршрутизации
   - **PBR**
   - Сравнение политики маршрутизации и PBR
3. Политика маршрутизации и команды конфигурирования PBR
4. Анализ примеров

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

PBR

- Как правило, устройства ищут в своих таблицах IP-маршрутизации маршруты пакетов на основе адресов назначения пакетов, и затем пересылают пакеты. PBR позволяет сетевым администраторам определять политику изменения маршрутов пакетов на основе адресов источника пакетов, размера пакетов и качества канала в дополнение к адресам назначения пакетов.
- PBR имеет следующие преимущества:
  - Позволяет сетевым администраторам определять политику маршрутизации пакетов, за счет чего повышается гибкость выбора маршрута и управляемость.
  - Позволяет переадресовать различные потоки данных на разные каналы, благодаря чему повышается эффективность канала.
  - Использование экономически эффективных каналов для передачи сервисных данных без ущерба для качества услуг, за счет чего снижается стоимость корпоративных услуг передачи данных.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- PBR отличается от политик маршрутизации следующим образом:
  - PBR применяется к пакетам данных и предоставляет средства для изменения пути переадресации пакетов данных в соответствии с определенными политиками вместо следования маршрутам в существующей таблице маршрутизации.
  - Политика маршрутизации реализует маршрутизацию на основе информации маршрутизации. Политика маршрутизации изменяет путь переадресации пакетов путем фильтрации маршрутов и настройки атрибутов маршрутов. Например, вы можете установить атрибуты маршрутов (включая Reachability), чтобы изменить путь переадресации сетевого трафика.

Классификация PBR

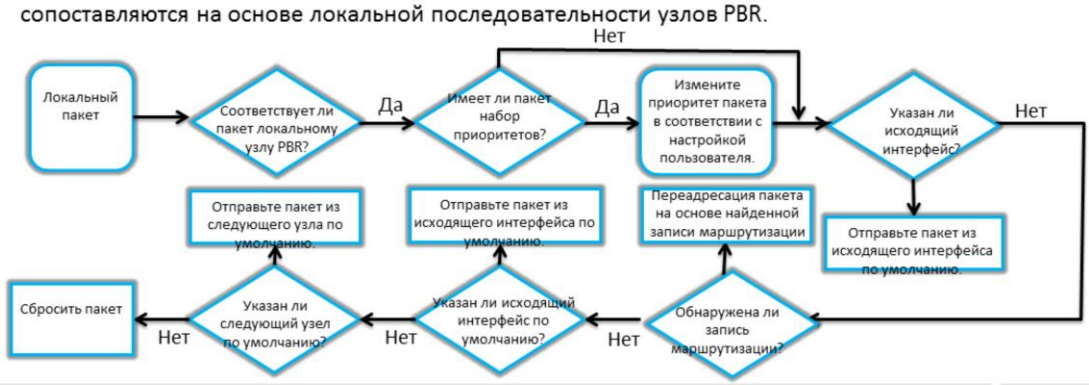
- PBR можно разделить на локальную PBR, интерфейсную PBR и умную маршрутизацию на основе политик (SPR).
- Локальная PBR
  - Локальная PBR применяется только к пакетам, созданным локально, но не к переадресованным пакетам.
- Интерфейсная PBR
  - Интерфейсная PBR применяется только к переадресованным пакетам, но не к пакетам, созданным локально (например, к локальным пакетам ping).
- SPR
  - SPR позволяет устройствам выбирать маршруты на основе качестве канала и требований к качеству канала.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Локальная PBR

- Локальная PBR
  - Локальная PBR применяется только к пакетам, созданным локально, но не к переадресованным пакетам.
  - Локальная PBR на устройстве может иметь несколько локальных узлов PBR. Пакеты сопоставляются на основе локальной последовательности узлов PBR.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Порядок сопоставления
  - Если устройство находит соответствующий локальный узел PBR, он выполняет следующие шаги:
    1. Проверяет, был ли установлен приоритет пакетов. Если да, устройство применяет настроенный приоритет к пакетам и выполняет следующий шаг. Если нет, устройство выполняет следующий шаг.
    2. Проверяет, сконфигурирован ли исходящий интерфейс для локальной PBR. Если да, устройство отправляет пакеты из исходящего интерфейса. Если нет, устройство выполняет следующий шаг.
    3. Проверяет, сконфигурированы ли следующие узлы для локальной PBR (могут быть сконфигурированы два следующих узла для балансировки нагрузки). Если да, устройство отправляет пакеты на следующий узел. Если нет, маршрутизатор ищет маршрутную таблицу для маршрута на основе адресов назначения пакетов. Если маршрут не доступен, устройство выполняет следующий шаг.
  1. Проверяет, сконфигурирован ли исходящий интерфейс по умолчанию для локальной PBR. Если да, устройство отправляет пакеты из исходящего интерфейса по умолчанию. Если нет, устройство выполняет следующий шаг.
  2. Проверяет, сконфигурированы ли по умолчанию следующие узлы для локальной PBR. Если да, устройство отправляет пакеты на следующие узлы по умолчанию. Если нет, устройство выполняет следующий шаг.
  3. Отбрасывает пакеты и генерирует сообщения **ICMP _ UNREACH**.

- Если устройство не обнаруживает соответствующий локальный узел PBR, он ищет таблицу маршрутизации для маршрута на основании адресов назначения пакетов, и затем отправляет пакеты.



Содержание

1. Фильтрация маршрутов
2. **Политика маршрутизации и PBR**
   - Политика маршрутизации
   - PBR
   - **Сравнение политики маршрутизации и PBR**
3. Политика маршрутизации и команды конфигурирования PBR
4. Анализ примеров

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Сравнение политики маршрутизации и PBR

Функция	Характеристики
Политика маршрутизации	1. Политика маршрутизации обеспечивают переадресацию пакетов в соответствии с адресом назначения в таблице маршрутизации. 2. Политика маршрутизации работает в плоскости управления и обслуживает протоколы маршрутизации и таблицы маршрутизации. 3. Политика маршрутизации используется с протоколом маршрутизации для формирования политики. 4. Команда route-policy используется для создания политики маршрутизации.
PBR	1. Пакеты пересылаются на основе политики. Если пакеты не переадресованы на основании политики, устройство ищет таблицу маршрутизации для переадресации пакетов. 2. PBR работает в плоскости переадресации и обслуживает политики переадресации. 3. PBR необходимо конфигурировать вручную, чтобы обеспечить переадресацию пакетов в соответствии с политиками. 4. Команда policy-based-route используется для конфигурирования PBR.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

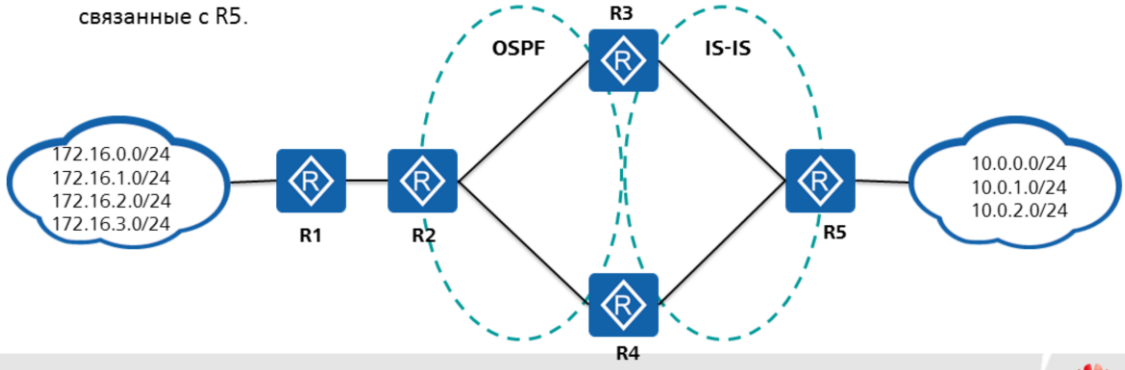
Содержание

1. Фильтрация маршрутов
2. Политика маршрутизации и PBR
3. **Политика маршрутизации и команды конфигурирования PBR**
   - **Конфигурирование импорта маршрутов**
   - Конфигурирование оптимизации маршрутов на основе политик
   - Конфигурирование PBR
4. Анализ примеров

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Конфигурирование импорта прямых маршрутов (1/2)

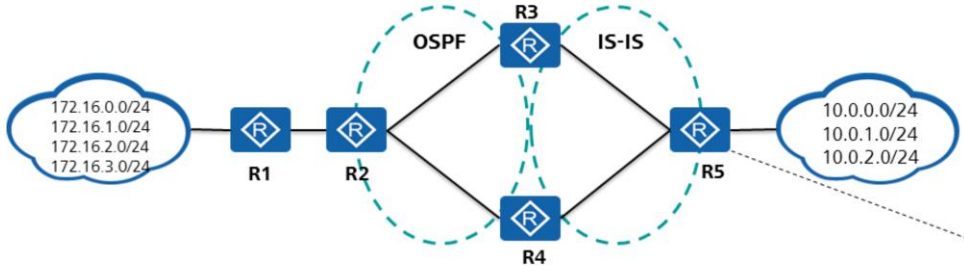
- На рисунке ниже показана топология сети компании A. Необходимо выполнить следующие конфигурации:
  - Включите протокол OSPF на R2, R3 и R4 и протокол IS-IS на R3, R4 и R5.
  - Импортируйте в протокол IS-IS маршруты к сетевому сегменту 10.0.X.0/24, непосредственно связанные с R5.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- В этом случае адреса для взаимосвязанных устройств следующие:
  - Например, если RTX взаимосвязан с RTY, адреса взаимосвязи будут адреса XY.1.1.X и XY.1.1.Y, а длина маски - 24 бита.

Конфигурирование импорта прямых маршрутов (2/2)




```
[R3]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------
Routing Tables: Public
         Destinations : 13        Routes : 13

Destination/Mask    Proto   Pre  Cost      Flags NextHop
10.0.0.0/24         ISIS-L2 15   10          D   35.1.1.5
10.0.1.0/24         ISIS-L2 15   10          D   35.1.1.5
10.0.2.0/24         ISIS-L2 15   10          D   35.1.1.5
.............
```

```
isis 1
 is-level level-2
 cost-style wide
 network-entity 49.0050.0500.5005.00
 import-route direct route-policy DIRECTIN
#
route-policy DIRECTIN permit node 10
 if-match ip-prefix 10
#
ip ip-prefix 10 index 10 permit 10.0.0.0 16 greater-equal 24 less-equal
24
#
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

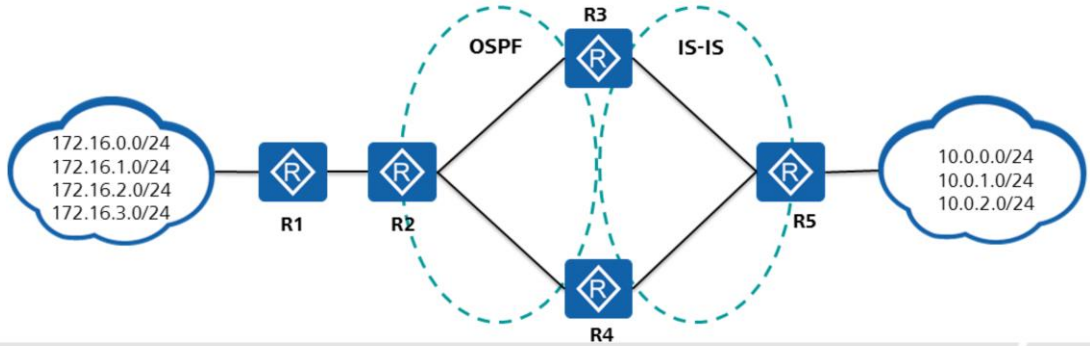
HUAWEI

- Использование команды
  - Команда route-policy создает политику маршрутизации и отображает политику маршрутизации.
- Описание параметров
  - route-policy route-policy-name { permit | deny } node
    - route-policy-name: определяет имя политики маршрутизации.
    - permit: определяет в качестве режима сопоставления политики маршрутизации действие разрешения. Если маршрут соответствует всем условиям if-match узла, маршрут соответствует узлу, и все действия, определенные в условии apply, применяются к маршруту. В противном случае маршрут будет сопоставляться со следующим узлом.
    - deny: определяет в качестве режима сопоставления политики маршрутизации действие отклонения. Если маршрут совпадает соответствует всем условиям if-match узла, маршрут отклоняется и не сопоставляется со следующим узлом.
    - node : указывает индекс узла в политике маршрутизации.
- Меры предосторожности
  - Политика маршрутизации используется для фильтрации маршрутов и настройки атрибутов для маршрутов, соответствующих политике маршрутизации. Политика маршрутизации состоит из нескольких узлов. Один узел может быть сконфигурирован с несколькими условиями **if-match** и **apply**. Условия **if-match** определяют правила сопоставления для этого узла, а условие **apply** определяет действия в отношении маршрутов, соответствующих правилам. Связь между условиями **if-match** устанавливается с помощью "AND". То есть, маршрут должен соответствовать всем условиям **if-match**. Связь между условиями **if-match** устанавливается с помощью "AND". То есть, маршрут должен соответствовать всем условиям **if-match**. Если маршрут не совпадает с каким-либо узлом, он не соответствует

политике маршрутизации.

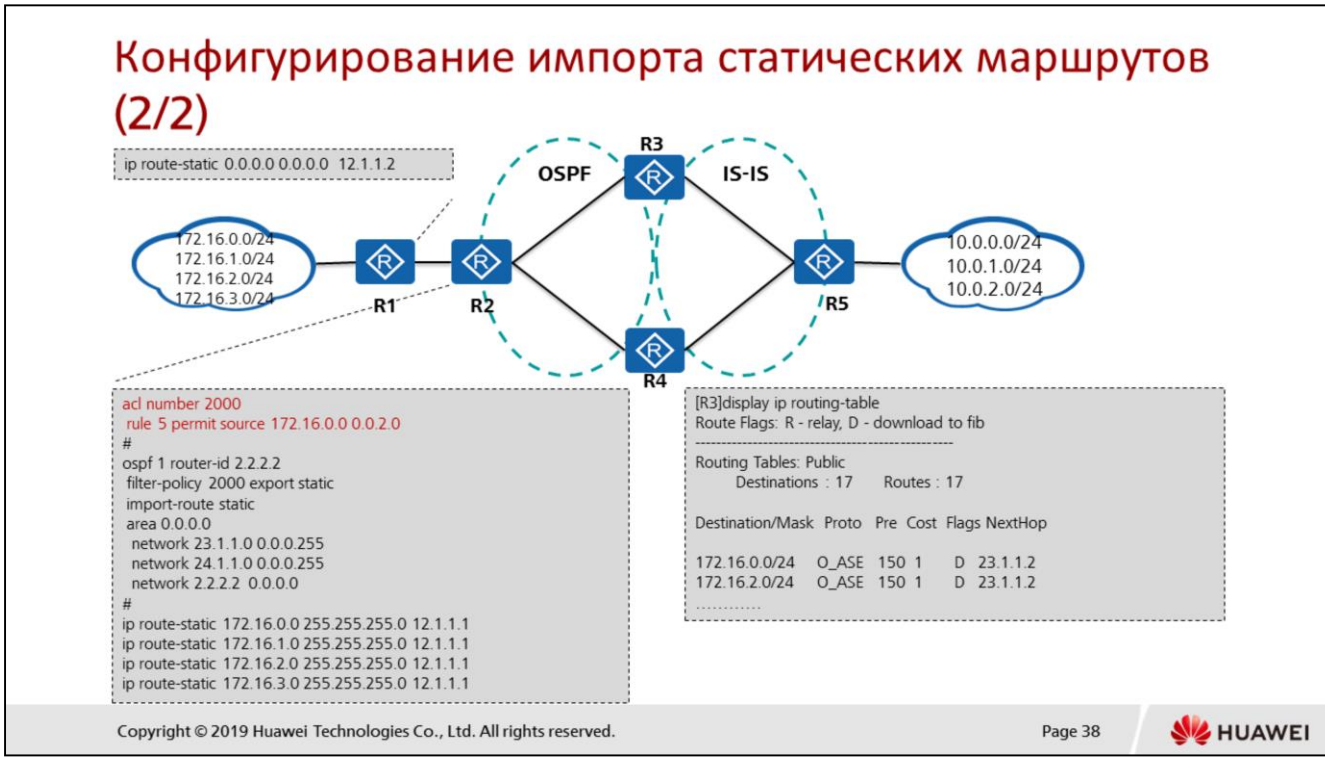
Конфигурирование импорта статических маршрутов (1/2)

- Компании A необходимо развернуть сеть между R1 и R2 с соблюдением следующих требований:
  - Статические маршруты конфигурируются между R1 и R2, чтобы R1 и R2 могли взаимодействовать друг с другом.
  - Маршруты к 172.16.X.0/24 импортируются в OSPF. Домен OSPF может узнавать только маршруты к 172.16.0.0/24 и 172.16.2.0/24. Выполните команды filter-policy и ACL для получения оптимальной конфигурации.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Эти требования расширяются на основе требований, приведенных в предыдущем примере. Выполните конфигурацию на основе конфигураций в предыдущем примере.
- Это требование предоставляется для того, чтобы помочь вам понять политику фильтрации и списки ACL. Оптимальная конфигурация означает, что вы можете использовать наименьшее количество команд для получения желаемого результата.

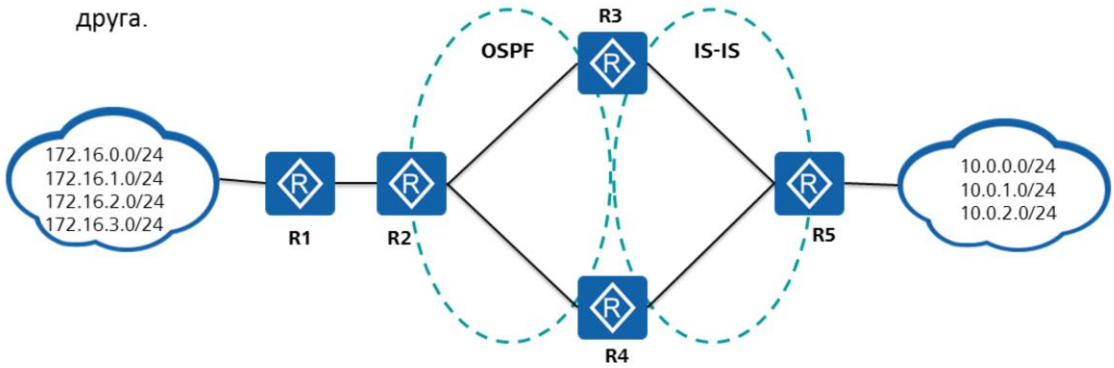


- Использование команды
  - Команда **filter-policy export** конфигурирует политику фильтрации для фильтрации импортируемых маршрутов, подлежащих анонсированию.
- Описание параметров
  - filter-policy { acl-number | acl-name | ip-prefix ip-prefix-name } export [protocol [process-id]]
    - acl-number: определяет номер основного ACL.
    - Acl-nameacl-name: определяет имя ACL.
    - ip-prefixip-prefix-name: определяет имя списка IP-префиксов.
    - Protocol: определяет имя политики маршрутизации.
    - process-id: определяет ID процесса, когда протоколом, выполняющим анонсирование, является протокол RIP, IS-IS или OSPF.
- Меры предосторожности
  - После того, как OSPF импортирует внешние маршруты с помощью команды **import-route**, вы можете использовать команду **filter-policy export** для фильтрации импортируемых маршрутов, подлежащих анонсированию. Только внешние маршруты, прошедшие фильтрацию, могут быть преобразованы в LSA-пакеты 5 типа (AS-external LSA) и анонсированы.
  - Параметр *protocol* или *process-id* может быть задан для фильтрации маршрутов определенного протокола или процесса. Если параметр *protocol* или *process-id* не указан,

OSPF фильтрует все импортированные маршруты.

Конфигурирование двустороннего импорта маршрутов (1/2)

- Компании A необходимо реализовать взаимодействие между сетями с соблюдением следующих требований:
  - Протоколы OSPF и IS-IS на R3 и R4 должны импортировать маршруты друг друга.

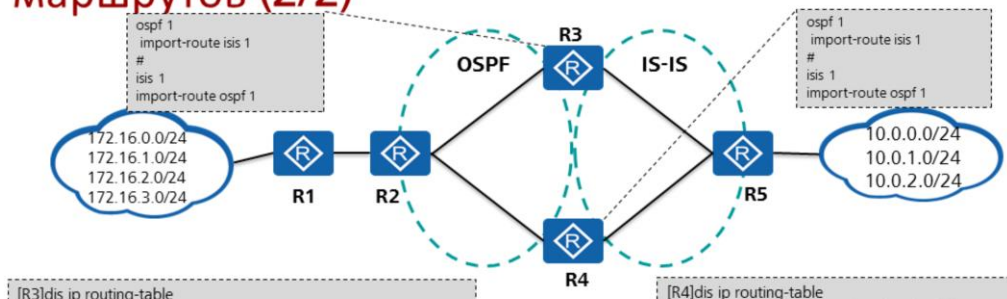


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Топология сети в данном примере совпадает с топологией в предыдущем примере. После выполнения необходимых конфигураций необходимо проверить, существуют ли субоптимальные маршруты или петли.

Конфигурирование двустороннего импорта маршрутов (2/2)




```
[R3]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 17        Routes : 17

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.0.0/24  ISIS-L2  15   10      D   35.1.1.5        GigabitEthernet0/0/0
        10.0.1.0/24  ISIS-L2  15   10      D   35.1.1.5        GigabitEthernet0/0/0
        10.0.2.0/24  ISIS-L2  15   10      D   35.1.1.5        GigabitEthernet0/0/0
        24.1.1.0/24  OSPF     10   2       D   23.1.1.2        GigabitEthernet0/0/1
        45.1.1.0/24  ISIS-L2  15   20      D   35.1.1.5        GigabitEthernet0/0/0
      172.16.0.0/24  O_ASE    150  1       D   23.1.1.2        GigabitEthernet0/0/1
      172.16.2.0/24  O_ASE    150  1       D   23.1.1.2        GigabitEthernet0/0/1
```

```
[R4]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 17        Routes : 17

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.0.0/24  ISIS-L2  15   10      D   45.1.1.5        GigabitEthernet0/0/0
        10.0.1.0/24  ISIS-L2  15   10      D   45.1.1.5        GigabitEthernet0/0/0
        10.0.2.0/24  ISIS-L2  15   10      D   45.1.1.5        GigabitEthernet0/0/0
        23.1.1.0/24  OSPF     10   2       D   24.1.1.2        GigabitEthernet0/0/1
        35.1.1.0/24  ISIS-L2  15   20      D   45.1.1.5        GigabitEthernet0/0/0
      172.16.0.0/24  ISIS-L2  15   20      D   45.1.1.5        GigabitEthernet0/0/0
      172.16.2.0/24  ISIS-L2  15   20      D   45.1.1.5        GigabitEthernet0/0/0
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- После того, как протоколы OSPF и IS-IS на R3 и R4 импортируют маршруты друг друга, между R4 и сетевым сегментом 172.16.X.0/24 возникают субоптимальные маршруты. Это связано с тем, что R3 сначала распределяет маршруты OSPF в домен маршрутизации IS-IS. Поэтому R4 получает маршруты к 172.16.X.0/24 как из OSPF, так и из IS-IS. Значение предпочтения для внешних маршрутов OSPF составляет 150, а маршрутов IS-IS -15. Поэтому R4 выбирает маршрут IS-IS к 172.16.X.0/24, который является субоптимальным маршрутом.

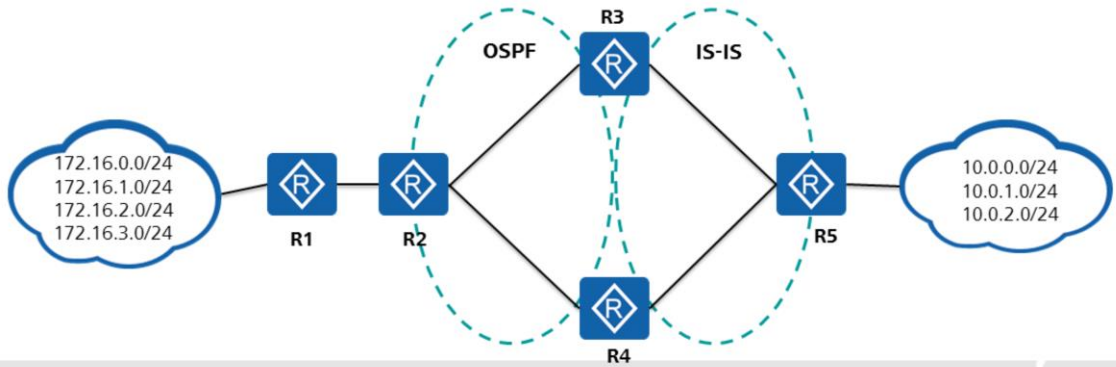
Содержание

1. Фильтрация маршрутов
2. Политика маршрутизации и PBR
3. **Политика маршрутизации и команды конфигурирования PBR**
   - Конфигурирование импорта маршрутов
   - **Конфигурирование оптимизации маршрутов на основе политик**
   - Конфигурирование PBR
4. Анализ примеров

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Конфигурирование политики маршрутизации для оптимизации маршрутов (1/3)

- Компания A хочет оптимизировать свою сеть и имеет следующие требования:
  - В случае изменения сети не должны образовываться петли маршрутизации.
  - R4 может получить доступ к сегменту сети 172.16.X.0/24 через оптимальный маршрут.

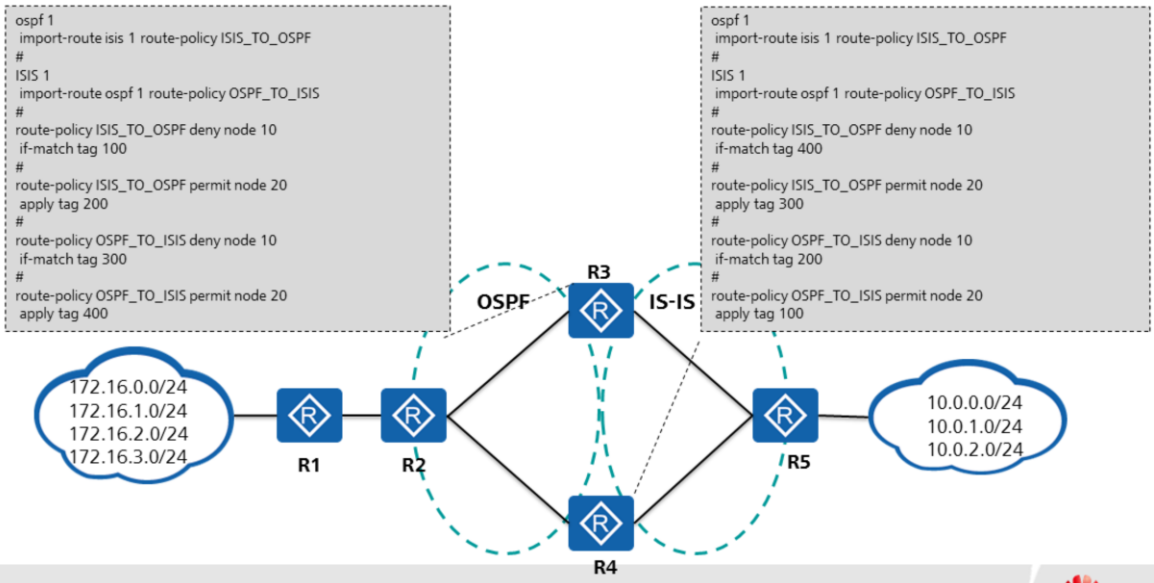


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Это расширенные требования, созданные на основе требований, приведенных в предыдущем примере. Выполните конфигурацию на основе предыдущего примера.
  - Маршрут для R4 для доступа к сетевому сегменту 172.16.X.0/24 необходимо изменить, чтобы предотвратить создание субоптимального маршрута, проходящего через домен IS-IS.
  - Вы можете использовать тег для управления импортом маршрутов между OSPF и IS-IS, чтобы предотвратить петли маршрутизации.

Конфигурирование политики маршрутизации для оптимизации маршрутов (2/3)

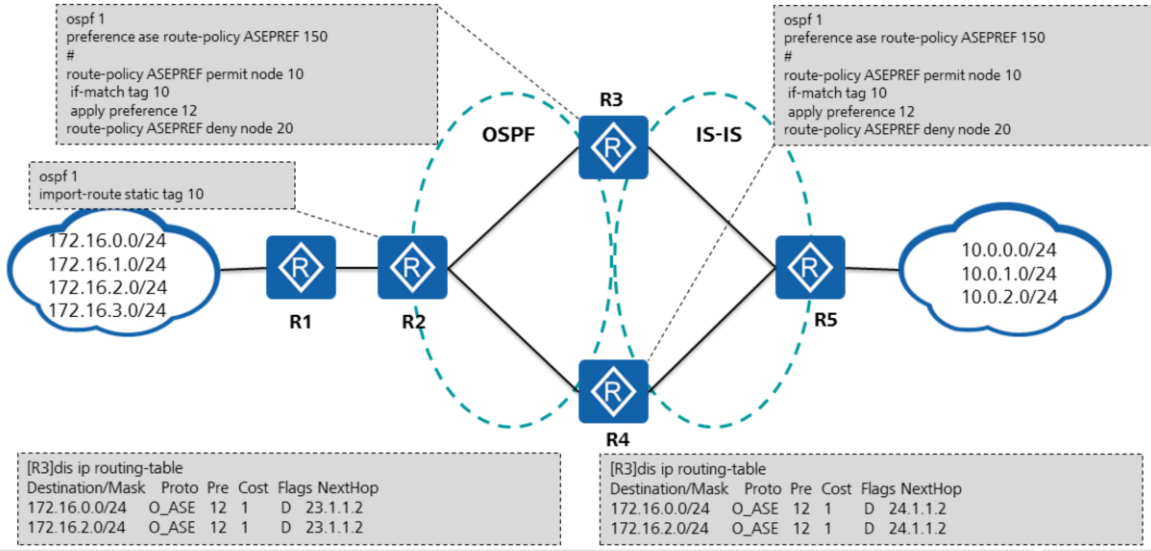


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Если импортируемые маршруты не отфильтрованы, при изменениях в сети могут возникнуть петли маршрутизации. Чтобы предотвратить возникновение петель маршрутизации, убедитесь, что при взаимном импорте протоколов маршрутизации импортируются только маршруты каждого домена маршрутизации. В предыдущем примере конфигурации для контроля импорта маршрутов используются теги. При использовании тегов не требуется запись маршрутизации. Когда количество записей маршрутизации в домене маршрутизации увеличивается или уменьшается, значение тега импортируемых маршрутов меняется без ручного настройки. За счет этого обеспечивается хорошая масштабируемость.
- Хотя настройка политики маршрутизации в предыдущем сценарии может предотвратить петли маршрутизации, она не может решить проблему субоптимальных маршрутов.

Конфигурирование политики маршрутизации для оптимизации маршрутов (3/3)

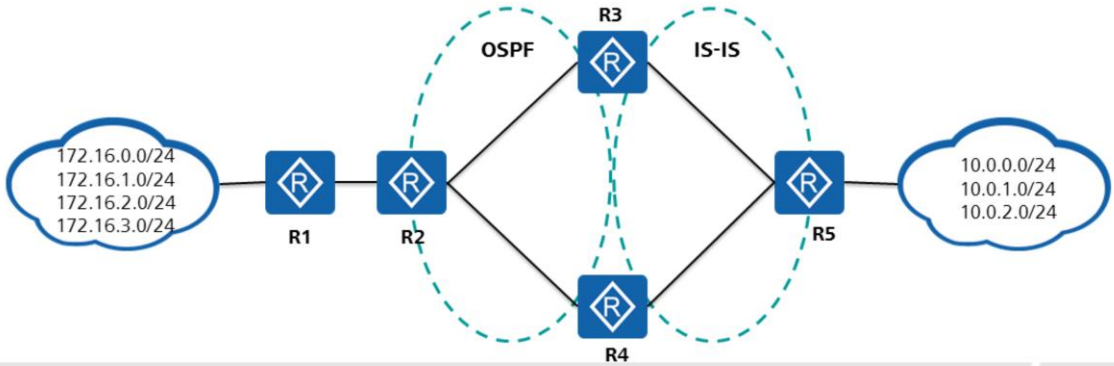


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Субоптимальные маршруты генерируются главным образом потому, что R3 или R4 получают маршруты к адресу 172.16.X.0/24 и из домена OSPF, и из домена IS-IS при взаимном импорте маршрутов. Значение предпочтения у внешних маршрутов OSPF больше, чем у маршрутов IS-IS (меньшее значение имеет более высокий приоритет). В результате R3 или R4 выбирают субоптимальный маршрут. Чтобы решить эту проблему, измените значение предпочтения внешних маршрутов OSPF. Такой проблемы не возникнет, пока значение предпочтения маршрутов OSPF_ASE будет меньше, чем значение маршрутов IS-IS.
- Не рекомендуется устанавливать значение предпочтения маршрутов OSPF_ASE меньше значения внутренних маршрутов OSPF (10).

Оптимизация маршрутов (1/3)

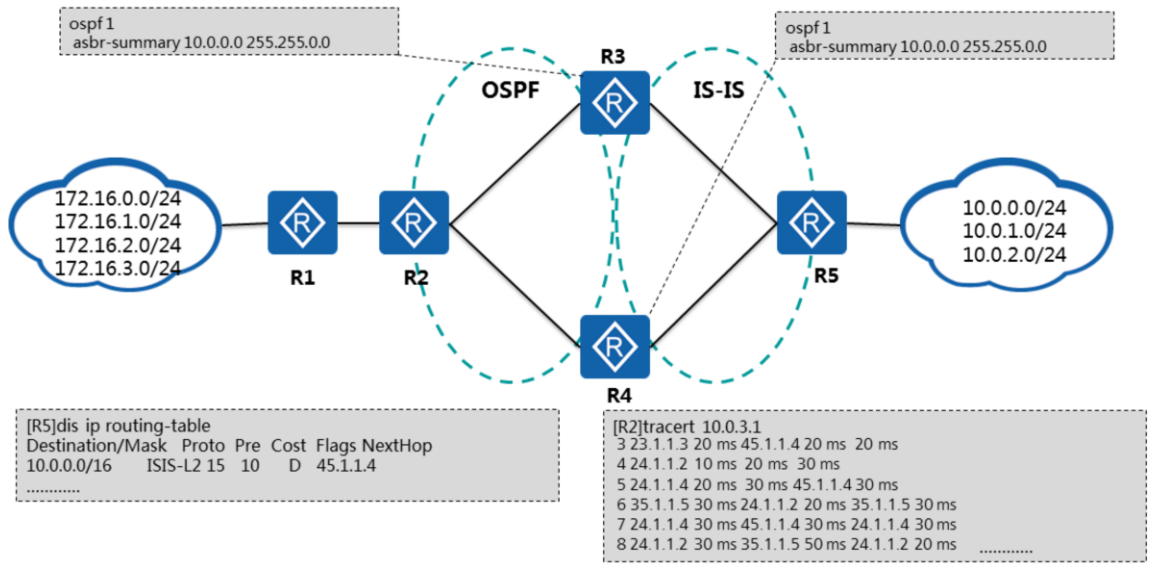
- Компания A хочет оптимизировать свою сеть и имеет следующие требования:
  - R3 и R4 находятся в домене OSPF. Маршруты к 10.0.X.0/24 суммируются как 10.0.0.0/16. Петля маршрутизации не возникает.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Это расширенные требования, созданные на основе требований, приведенных в предыдущем примере. Выполните конфигурацию на основе предыдущего примера.

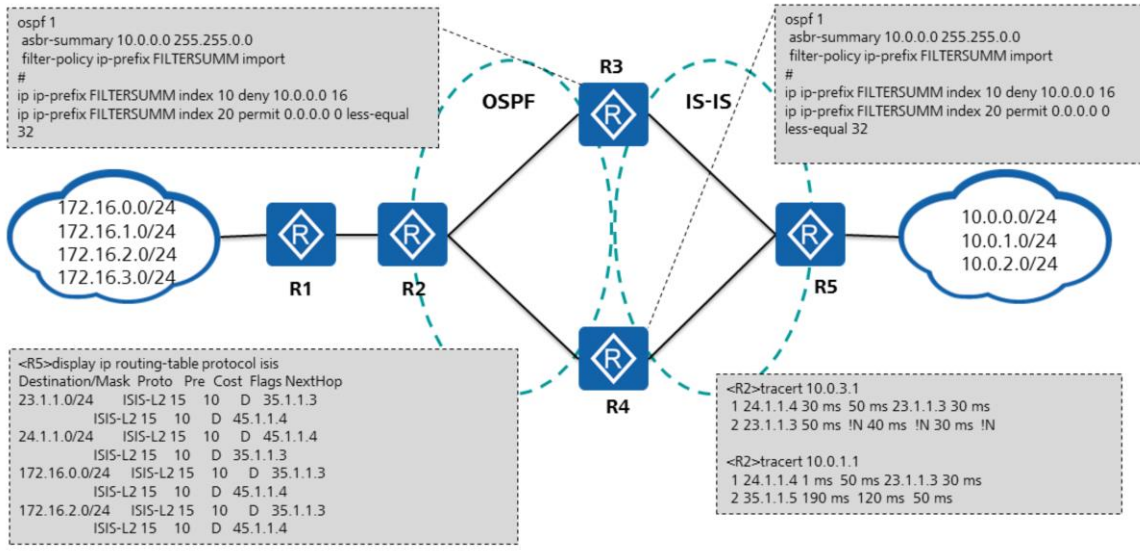
Оптимизация маршрутов (2/3)



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Когда выполняется только суммирование маршрутов, возникают две проблемы. Первая проблема заключается в том, что R5 узнает суммарные маршруты. Вторая проблема – это возникновение петли при получении несуществующего IP-адреса от маршрутизатора R2.
- Первая проблема связана с тем, что R3 и R4 узнают суммарные маршруты друг от друга и затем импортируют их в домен IS-IS. Суммирование OSPF сначала выполняется в R3. Затем созданный суммарный маршрут передается R4 через R2. R4 импортирует этот суммарный маршрут в IS-IS и анонсирует его R5.
- Затем возникает вторая проблема. В R2 существуют два маршрута с одинаковой стоимостью к 10.0.0.0/16, а их следующими узлами являются R3 и R4 соответственно. При изменении номера порта назначения tracert, пакет tracert отправляется на R3 или R4.
  - Когда пакет tracert отправляется маршрутизатору R4: R4 выполняет суммирование маршрутов OSPF позже, чем R3. В этом случае у R4 есть только один суммарный маршрут OSPF, анонсированный R3. Следующим узлом маршрута от R4 к 10.0.0.0/16 является R2. В результате возникает петля маршрутизации.
  - Когда пакет tracert отправляется маршрутизатору R3: после создания суммарного маршрута OSPF на R4, R4 анонсирует этот суммарный маршрут R3. После создания суммарного маршрута OSPF на R3, R3 анонсирует этот суммарный маршрут R4. Затем R4 импортирует этот суммарный маршрут в IS-IS и анонсирует его R3 через R5. Наконец, у R3 есть два маршрута с 16-битными масками подсети. R3 сравнивает протокол маршрутизации этих двух маршрутов и выбирает маршрут IS-IS с более высоким приоритетом и R4 в качестве следующего узла. Поскольку R4 выполняет суммирование маршрутов позже, чем R3, R4 получает суммарный маршрут OSPF, анонсированный R3. Следующим узлом маршрута от R4 к 10.0.0.0/16 является R2. В результате возникает петля маршрутизации.
- Чтобы решить упомянутые выше проблемы, сделайте так, чтобы R3 и R4 не могли узнать суммарные маршруты друг от друга и не могли импортировать суммарные маршруты в домен маршрутизации IS-IS. Поэтому вам необходимо только отфильтровать суммарные маршруты на R3 и R4, которые они получают друг от друга.

Оптимизация маршрутов (3/3)



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Создайте политики фильтрации на R3 и R4, чтобы предотвратить получение указанных суммарных маршрутов из протокола OSPF. Тогда суммарные маршруты не будут импортированы в домен маршрутизации IS-IS, и не будут возникать петли.

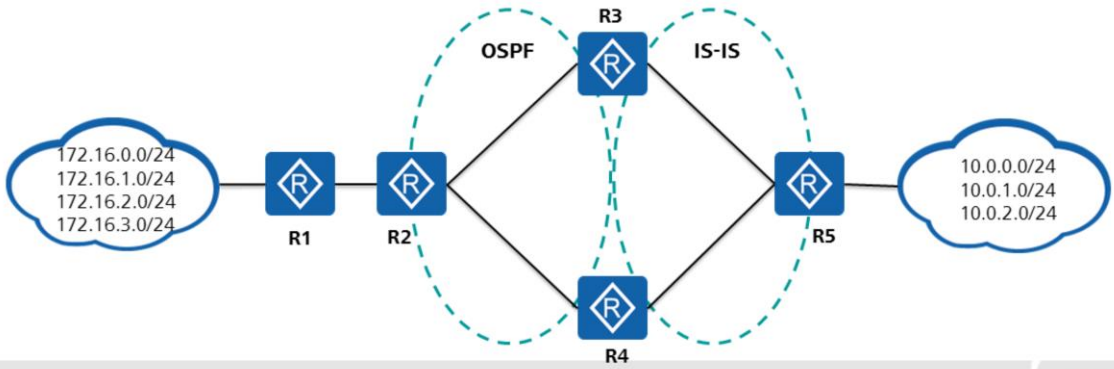
Содержание

1. Фильтрация маршрутов
2. Политика маршрутизации и PBR
3. **Политика маршрутизации и команды конфигурирования PBR**
   - Конфигурирование импорта маршрутов
   - Конфигурирование оптимизации маршрутов на основе политик
   - **Конфигурирование PBR**
4. Анализ примеров

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Конфигурирование PBR (1/2)

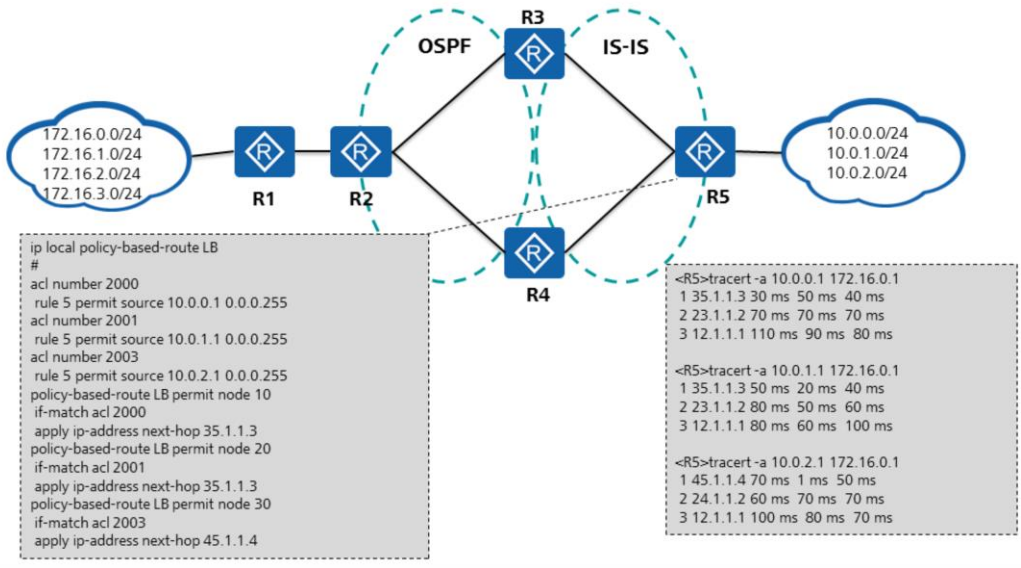
- Компания A хочет оптимизировать свою сеть и имеет следующие требования:
  - Трафик доступа от 10.0.0.0/24 и 10.0.1.0/24 к 172.16.X.0/24 должен проходить через R3.
  - Трафик доступа от 10.0.2.0/24 для доступа к 172.16.X.0/24 проходит через R4.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Это расширенные требования, созданные на основе требований, приведенных в предыдущем примере. Выполните конфигурацию на основе предыдущего примера.

Конфигурирование PBR (2/2)



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Использование команды
  - Команда **policy-based-route** создает или изменяет политику и узел PBR.
  - Команда **ip local policy-based-route** включает локальная PBR.
- Описание параметров
  - policy-based-route *policy-name* {permit | deny} node *node-id*
    - policy-name: определяет имя политики.
    - Permit: указывает режим PBR, в котором PBR включена для пакетов, соответствующих правилам.
    - Deny: означает режим PBR, в котором PBR отключена для пакетов, не соответствующих правилам.
    - node-id: определяет порядковый номер узла PBR.
  - ip local policy-based-route *policy-name*
    - policy-name: определяет имя локальной политики.
- Меры предосторожности
  - Если для пакетов необходимо указать исходящий интерфейс при конфигурировании PBR, исходящий интерфейс не может быть широковещательным интерфейсом, например интерфейсом Ethernet.
- Результат тестирования
  - Когда на R5 задаются различные исходные адреса для трассировки пакетов с одним пунктом назначения, оказывается, что пакеты пересылаются разными путями.
  - Примечание. Политика маршрутизации, применяемая в команде **ip local policy-based-route** вступает в силу только для пакетов данных, исходящих от локального

маршрутизатора.

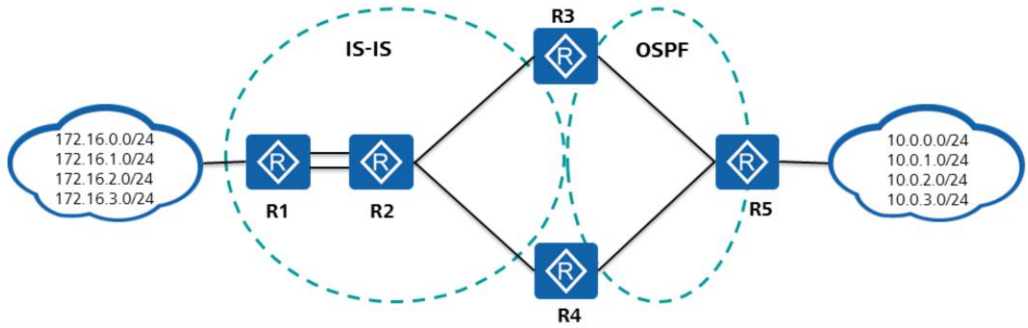
Содержание

1. Фильтрация маршрутов
2. Политика маршрутизации и PBR
3. Политика маршрутизации и команды конфигурирования PBR
4. Анализ примеров
   - **Пример 1**
   - Пример 2

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Пример 1

- На рисунке ниже показана топология сети компании B. У компании следующие требования:
  - R3, R4 и R5 принадлежат зоне 0 протокола OSPF. Только маршруты к 10.0.X.0/24 импортируются в зону OSPF.
  - На R5 маршруты к 10.0.X.0/24 суммируются в один маршрут к 10.0.0.0/16. R3 и R4 могут передавать стандартные маршруты в зону OSPF.
  - В сети нет петель.

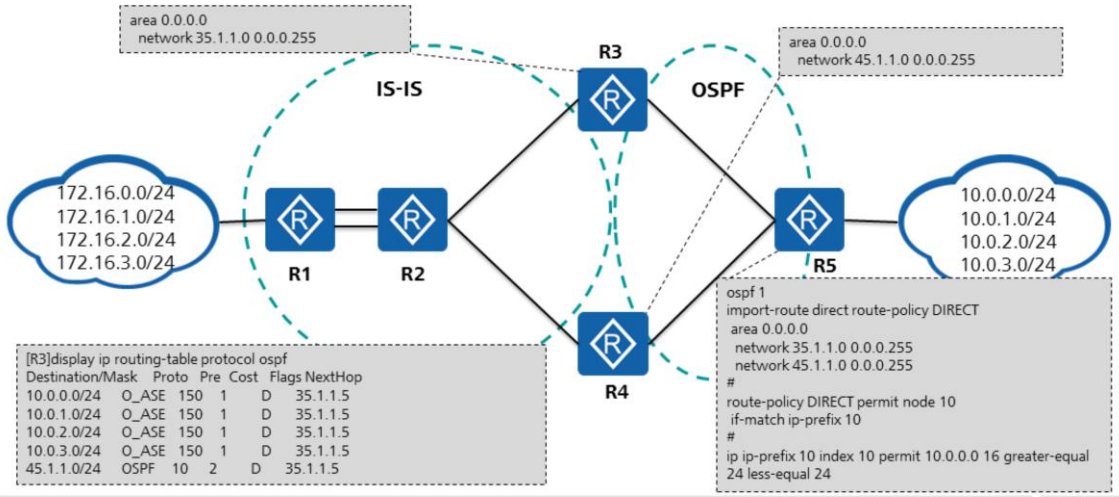


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- В этом случае адреса для подключаемых устройств следующие:
  - Например, если RTX связан с RTY, адреса взаимосвязи – XY.1.1.X и XY.1.1.Y, а длина маски – 24 бита.

Пример 1: требование 1

- R3, R4 и R5 принадлежат зоне 0 протокола OSPF. Только маршруты к 10.0.X.0/24 импортируются в зону OSPF.



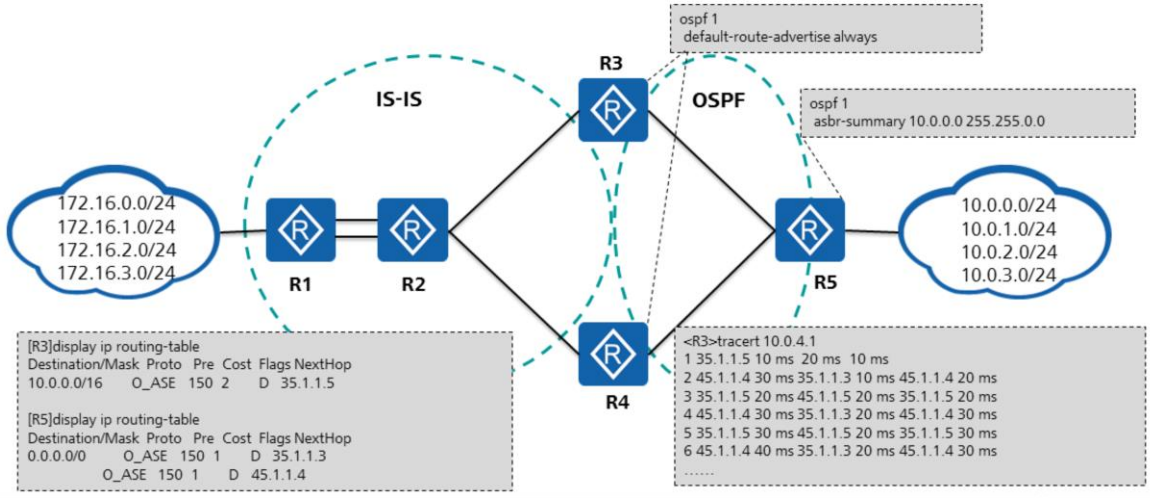
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Обратите внимание, что при импорте маршрутов в R5 требуется точное соответствие.

Пример 1: требование 2

- На R5 маршруты к 10.0.X.0/24 обобщаются в суммарный маршрут к 10.0.0.0/16. R3 и R4 могут передавать стандартные маршруты в зону OSPF.



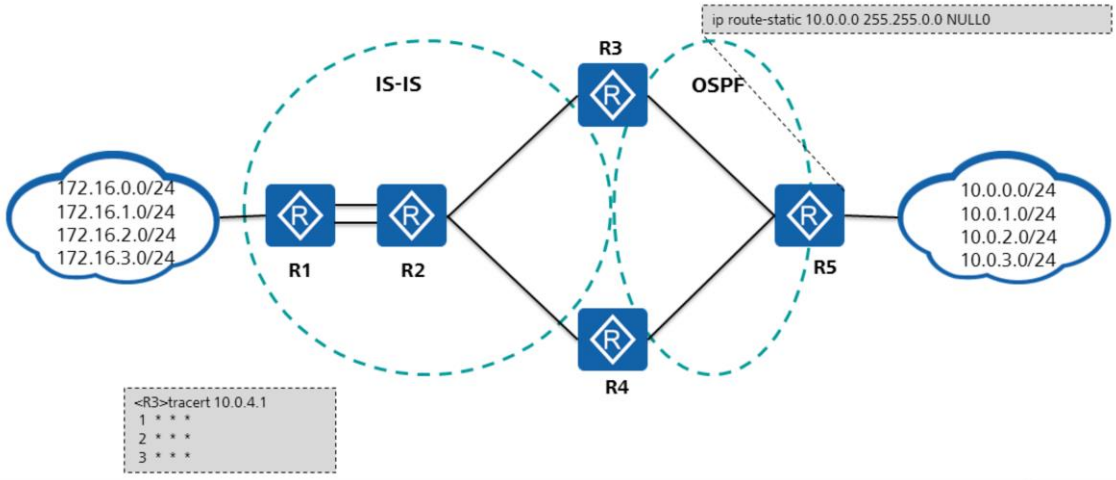
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Петля возникает при выполнении команды **tracert** для трассировки несуществующего IP-адреса в сетевом сегменте 10.0.0.0/16. Петля возникает потому, что при создании суммарного маршрута OSPF автоматически не создается маршрут, указывающий на Null 0.

Пример 1: требование 3

- В сети не возникает петель.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Чтобы устранить петли, используйте на R5 команду для конфигурирования статического маршрута, указывающего на Null 0.

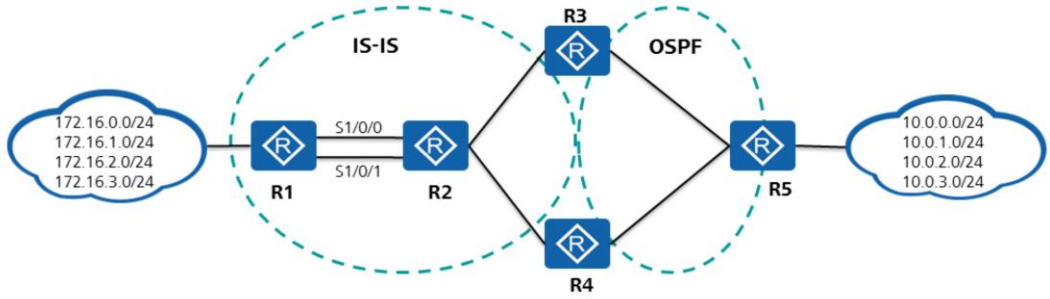
Содержание

1. Фильтрация маршрутов
2. Политика маршрутизации и PBR
3. Политика маршрутизации и команды конфигурирования PBR
4. Анализ примеров
   - Пример 1
   - **Пример 2**

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Пример 2

- Компания B хочет расширить свою сеть на основе оригинальных конфигураций. Требования заключаются в следующем:
  - Основные конфигурации IS-IS выполнены.
  - На основе политики фильтрации маршруты к 172.16.0.0/24 и 172.16.2.0/24 импортируются в IS-IS.
  - R3 и R4 импортируют маршруты друг друга. Не возникают петли и не используются субоптимальные маршруты.
  - Трафик доступа от 172.16.0.0/24 и 172.16.2.0/24 к сети OSPF проходит через S1/0/0.



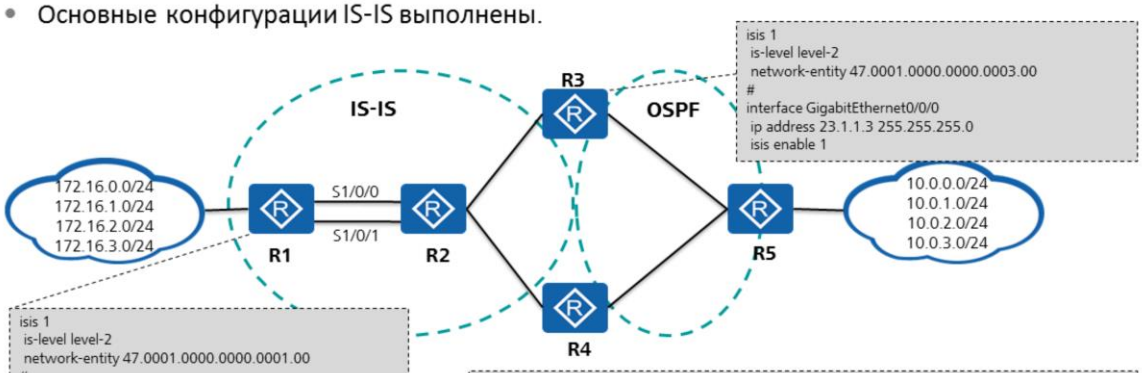
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Эти расширенные требования на основе требований, приведенных в предыдущем примере. Выполните конфигурацию на основе предыдущего примера.
- В этом примере адреса для подключаемых устройств следующие:
  - Например, если RTX взаимосвязан с RTY, адреса соединений – XY.1.1.X и XY.1.1.Y, а длина маски – 24 бита.
    - IP-адрес S1/0/0 – 12.1.1.1/24 на R1 и 12.1.1.2/24 на R2. IP-адрес S1/0/1 – 21.1.1.1/24 на R1 и 21.1.1.2/24 на R2.

Пример 2: предварительная настройка

- Основные конфигурации IS-IS выполнены.




```
isis 1
 is-level level-2
 network-entity 47.0001.0000.0000.0003.00
#
interface GigabitEthernet0/0/0
 ip address 23.1.1.3 255.255.255.0
 isis enable 1
```

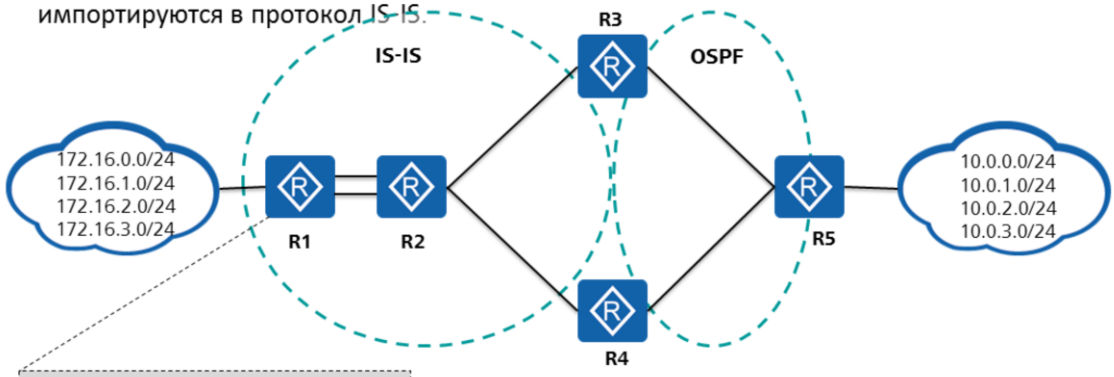
```
isis 1
 is-level level-2
 network-entity 47.0001.0000.0000.0001.00
#
interface Serial1/0/0
 link-protocol ppp
 ip address 12.1.1.1 255.255.255.0
 isis enable 1
#
interface Serial1/0/1
 link-protocol ppp
 ip address 21.1.1.1 255.255.255.0
 isis enable 1
```

```
[R2]display isis peer
                Peer information for ISIS(1)
 System Id     Interface   Circuit Id      State HoldTime Type  PRI
------------------------------------------------------------------
0000.0000.0001 S1/0/0      0000000001      Up  22s      L2  --
0000.0000.0001 S1/0/1      0000000002      Up  24s      L2  --
0000.0000.0003 GE0/0/0     0000.0000.0002.01 Up  28s      L2  64
0000.0000.0004 GE0/0/1     0000.0000.0004.01 Up  7s       L2  64
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Пример 2: требование 1

- На основе политики фильтрации маршруты к 172.16.0.0/24 и 172.16.2.0/24 импортируются в протокол IS-IS.




```
acl number 2000
 rule 5 permit source 172.16.0.0 0.0.2.0
#
isis 1
 filter-policy 2000 export direct
 import-route direct
```

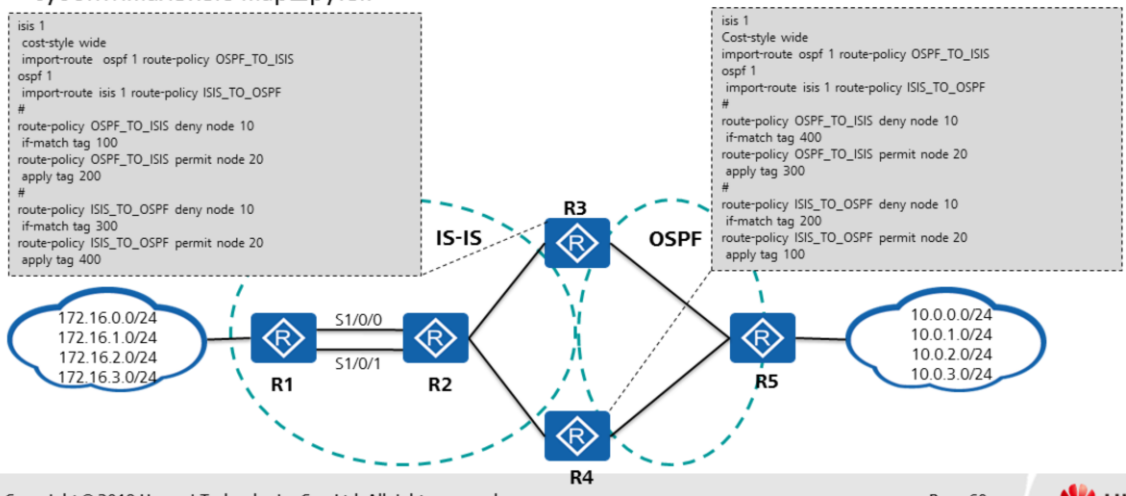
```
[R3]display ip routing-table protocol isis
Destination/Mask   Proto   Pre  Cost      Flags NextHop
172.16.0.0/24      ISIS-L2 15   84        D   23.1.1.2
172.16.2.0/24      ISIS-L2 15   84        D   23.1.1.2
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Используйте политику фильтрации со списком ACL для импорта маршрутов к двум сегментам сети, указанных в требованиях к протоколу IS-IS.
- Примечание. Для фильтрации импортируемых маршрутов протокола маршрутизации с использованием политики фильтрации используется команда **filter-policy export**.

Пример 2: требование 2 (1/2)

- R3 и R4 импортируют маршруты друг друга. Не возникают петли и не используются субоптимальные маршруты.

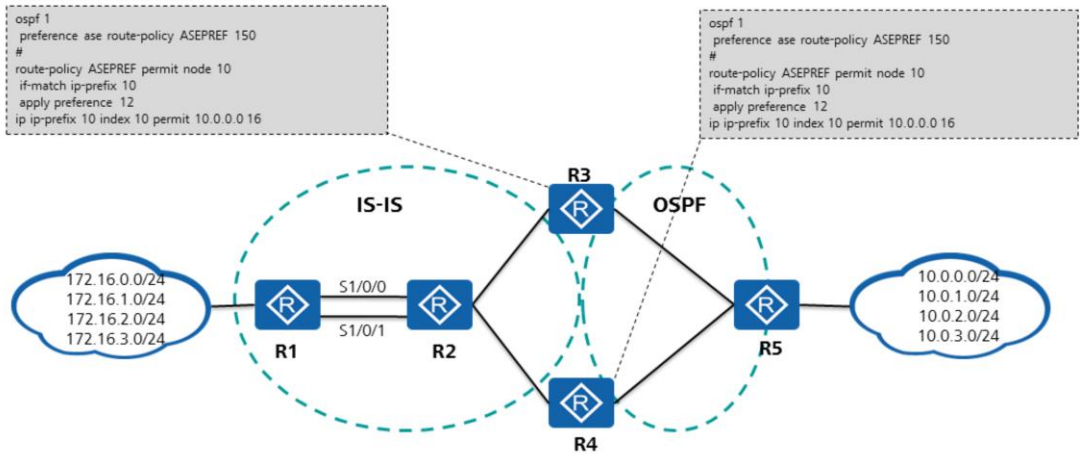


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- В этом случае можно добавить тег в маршруты при импорте маршрутов, чтобы предотвратить возникновение петель маршрутизации. Если протокол IS-IS должен поддерживать тег, то тип стоимости должен быть широким; в противном случае маршруты IS-IS не будут переносить тег.
- Тег используется для предотвращения петель маршрутизации, но не может предотвратить создание субоптимальных маршрутов. Чтобы предотвратить создание субоптимальных маршрутов, измените значение предпочтения соответствующих маршрутов.

Пример 2: требование 2 (2/2)

- R3 и R4 импортируют маршруты друг друга. Не возникают петли и не используются субоптимальные маршруты.

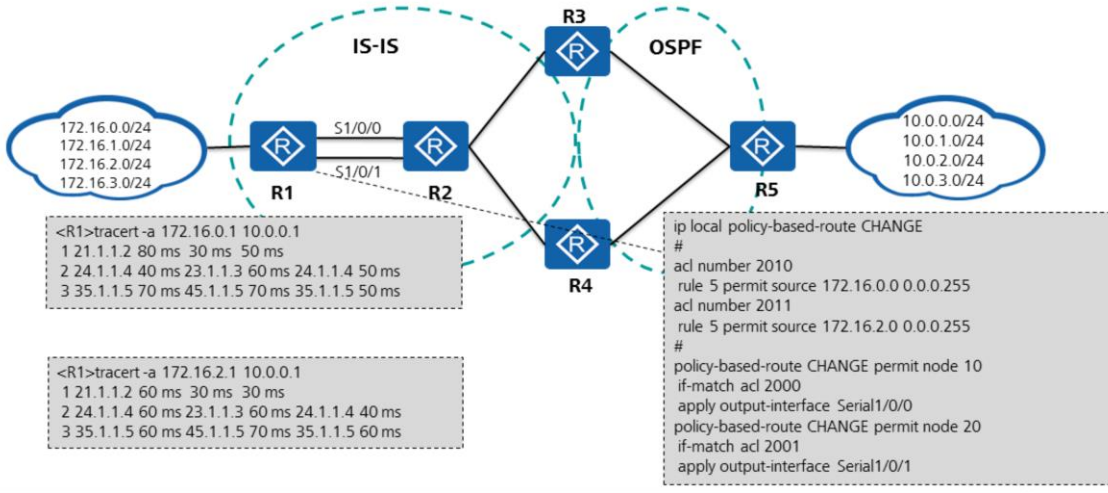


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Конфигурации в данном примере препятствуют образованию субоптимальных маршрутов в сетевом сегменте 10.0.0.0/16 на R3 и R4. Скорости импорта маршрутов отличаются в маршрутизаторах R3 и R4. В результате R3 или R4 одновременно узнают маршруты к 10.0.0.0/16 из IS-IS и OSPF. Если R3 первым импортирует маршруты, R4 одновременно узнает маршруты к 10.0.0.0/16 из протоколов IS-IS и OSPF. При выборе маршрутов R4 сравнивает значения предпочтений этих маршрутов. Значение предпочтения внешних маршрутов OSPF составляет 150, а маршрутов IS-IS – 15. Поэтому R4 выбирает маршрут к 10.0.0.0/16 через домен IS-IS. Этот маршрут является субоптимальным маршрутом. На R4 необходимо изменить значение предпочтения внешних маршрутов OSPF к 10.0.0.0/16, чтобы оно стало меньше значения предпочтения маршрутов IS-IS. Таким образом буду устранены субоптимальные маршруты. Рекомендуется, чтобы значение предпочтения внешних маршрутов OSPF было больше, чем значение предпочтения внутренних маршрутов OSPF (10).

Пример 2: требование 3

- Трафик доступа от 172.16.0.0/24 и 172.16.2.0/24 к сети OSPF проходит через S1/0/0.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Тест

1. Какие функции используются для управления маршрутизацией?
   A. Анонсирование маршрута
   B. Принятие маршрута
   C. Фильтрация и контроль импортируемых маршрутов
   D. Настройка атрибутов указанных маршрутов
2. Что означает список префиксов, сконфигурированный с помощью команды ip ip-prefix Prefix1 permit 160.0.0.0 8?
   A. Первые три бита префикса должны быть "101", а длина маски должна быть от 8 до 32 бит.
   B. Первые три бита префикса должны быть "101", а длина маски должна быть 8 бит.
   C. Номер префикса должен быть "160", а длина маски должна быть от 8 до 32 бит.
   D. Номер префикса должен быть 160, а длина маски должна быть 8 бит.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- ABCD
- D



Тест

3. Какие из утверждений о политике маршрутизации верны?

   A. Политика маршрутизации состоит из условий **if-match** или условий **if-match** и **apply**.

   B. Политика маршрутизации может иметь несколько узлов. Если маршрут соответствует всем условиям на одном узле политики маршрутизации, маршрут соответствует политике маршрутизации.

   C. Политика маршрутизации может иметь несколько узлов. Если маршрут соответствует любому условию на одном узле политики маршрутизации, маршрут соответствует политике маршрутизации.

   D. Если маршрут соответствует первому узлу в политике маршрутизации и отклоняется, а также соответствует второму узлу, то выполняется действие, определенное на втором узле.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- AB

Краткое содержание

- ACL
- Список IP-префиксов
- Фильтр AS-Path
- Фильтр Community
- Политика маршрутизации
- PBR

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Спасибо!

www.huawei.com

HCIE-R&S

— MLD

www.huawei.com

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Введение

- Протокол Multicast Listener Discovery (MLD) позволяет каждому маршрутизатору IPv6 обнаруживать групповых получателей (т.е. узлы, ожидающие получения многоадресной рассылки) в сети, к которой они подключены напрямую, и идентифицировать групповые адреса, в которых заинтересованы соседние узлы.
- В данном документе описываются основы протокола и конфигурационные команды различных версий MLD.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Цели

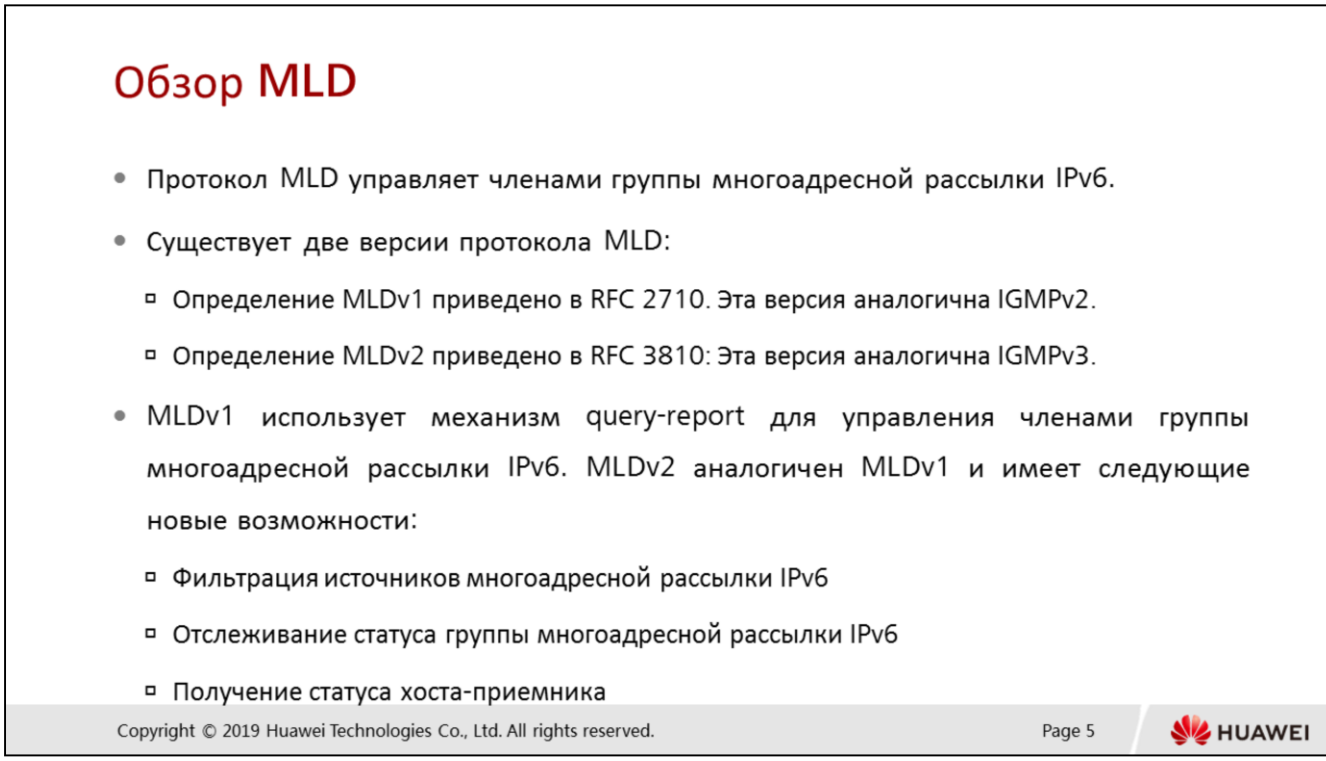
- После завершения этого курса вы будете:
  - Понимать функции и основы протокола MLD.
  - Понимать различия между MLDv1 и MLDv2.
  - Понимать функции SSM mapping.
  - Знать основные конфигурационные команды MLD.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Содержание

- Обзор MLD
- MLDv1
- MLDv2
- SSM Mapping

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.



- Протокол MLD управляет членами группы многоадресной рассылки IPv6, а ее принципы работы и функции аналогичны функциям IGMP. MLD позволяет каждому маршрутизатору IPv6 обнаруживать получателей многоадресной рассылки (т.е. узлы, ожидающие получения многоадресной рассылки) в сети, которой они подключены напрямую, и идентифицировать групповые адреса, которые интересуют соседние узлы. Сообщения затем предлагаются протоколу многоадресной маршрутизации, используемому маршрутизатором, чтобы данные многоадресной рассылки пересылались на все каналы, в которых существуют получатели.
- MLD – это асимметричный протокол, который определяет поведение получателей многоадресной рассылки и маршрутизаторов. Для группового адреса, который слушает маршрутизатор, маршрутизатор выступает в двух ролях протокола, включая ответ на свое собственное сообщение.
- Если у маршрутизатора более одного интерфейса в одной сети, ему нужно запустить протокол только на одном из интерфейсов. Кроме того, получатели должны запустить этот протокол на всех интерфейсах, чтобы протоколы верхнего уровня получали необходимые данные многоадресной рассылки от интерфейсов.
- Обе версии MLD поддерживают модель многоадресной рассылки ASM. Версию MLDv2 можно использовать в модели SSM, в то время как MLDv1 требуется использовать с функцией SSM mapping.

Функции MLD

- MLD позволяет маршрутизаторам IPv6 обнаруживать многоадресные слушатели на их непосредственно подключенных сетевых сегментах.
- Маршрутизаторы могут использовать MLD, чтобы проверить, существуют ли получатели многоадресной рассылки в сетевых сегментах, с которыми они соединены напрямую, и записывать соответствующую информацию в свои базы данных. Маршрутизаторы также хранят информацию о таймерах, связанных с этими групповыми адресами.
- Маршрутизаторы с настроенным протоколом MLD используют одиночный адрес link-local IPv6 как адрес источника для отправки сообщений MLD.
- MLD использует ICMP для передачи сообщений. Все сообщения MLD ограничены локальным каналов с 1 узлом.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Получатель многоадресной рассылки является хостом, который хочет получать данные многоадресной рассылки.

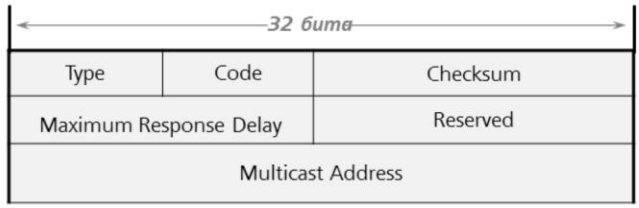
Содержание

- Обзор MLD
- MLDv1
- MLDv2
- SSM Mapping

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Формат сообщения MLDv1

- Тип: существует три типа сообщений MLD.
  - Сообщение Multicast Listener Query (значение типа = 130), которое можно разделить на следующие подтипы:
    - Сообщение General Query: используется для получения групповых адресов получателей в подключенной сети.
    - Сообщение Multicast-Address-Specific Query: используется для поиска получателя для конкретного группового адреса в подключенной сети.
  - Сообщение Multicast Listener Report (значение типа = 131)
  - Сообщение Multicast Listener Done (значение типа = 132)

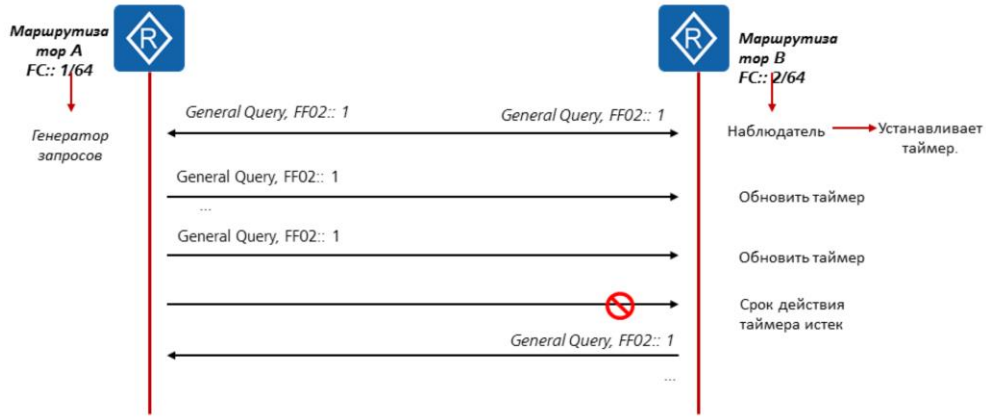


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Тип: существует три типа сообщений MLD.
  - Сообщение Multicast Listener Query (значение типа = 130), которое можно разделить на следующие подтипы:
    - Сообщение General Query: используется для получения групповых адресов получателей в подключенной сети.
    - Сообщение Multicast-Address-Specific Query: используется для поиска получателя для конкретного группового адреса в подключенной сети.
  - Сообщение Multicast Listener Report (значение типа = 131)
  - Сообщение Multicast Listener Done (значение типа = 132)
- Код
  - Поле имеет значение 1 во время передачи или игнорируется во время приема.
- Контрольная сумма
  - Стандартная контрольная сумма ICMPv6, охватывающая все сообщения MLD, а также псевдозаголовки в полях заголовка IPv6
- Максимальная задержка ответа
  - Максимальная задержка для отправки ответного сообщения в миллисекундах. Она действительна только в запросах. В других сообщениях это поле имеет значение 0 во время передачи и игнорируется во время приема.
- Зарезервировано
  - Поле имеет значение 1 для отправителей и игнорируется для получателей.
- Групповой адрес
  - Если отправлено сообщение General Query, групповой адрес имеет значение 0. Если отправлено сообщение Group-Specific Query, групповой адрес настраивается как конкретный групповой адрес IPv6. В сообщении Report or Leave групповой адрес устанавливается как конкретный групповой адрес IPv6, который должен получить или перестать получать отправитель.

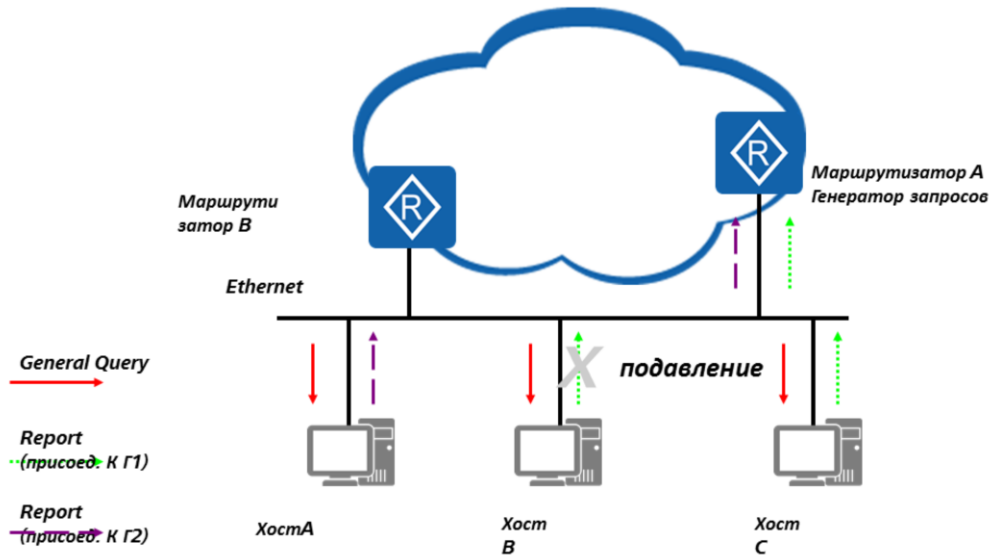
Механизм выбора генератора запросов (Querier)



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- 1. Каждый маршрутизатор MLDv1 считает себя генератором запросов при включении и посылает сообщение General Query с адресом назначения FF02:: 1 всем хостам и маршрутизаторам в локальном сегменте сети.
- 2. Когда другие маршрутизаторы получают сообщение General Query, они сопоставляют IPv6-адрес источника сообщения с IP-адресом своего интерфейса. Маршрутизатор с наименьшим IPv6-адресом становится генератором запросов (querier), а другие маршрутизаторы – наблюдателями (non-querier).
- 3. Все наблюдатели запускают таймер (Other Querier Present Timer). Если наблюдатели получают сообщение Query от генератора запросов до истечения таймера, они сбрасывают таймер. Если наблюдатели не получают сообщение Query от генератора запросов при истечении срока действия таймера, они запускают выбор нового генератора запросов.

Процесс присоединения к группе

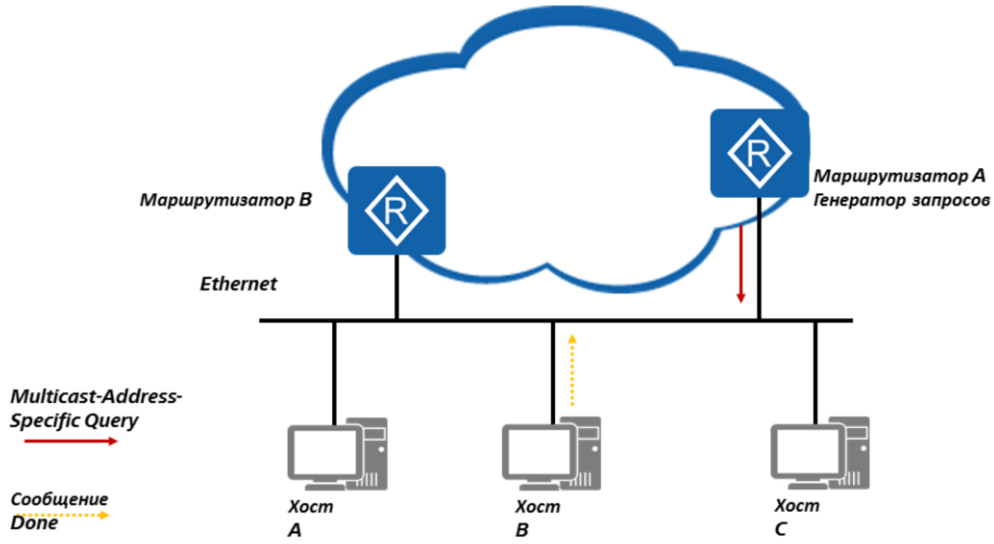


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- VRP реализует протокол MLDv1 в соответствии с RFC 2710. MLDv1 управляет членами группы многоадресной рассылки с помощью механизма запроса/ответа.
- У MLDv1 существует два типа запросов:
  - Сообщение General Query: используется для определения наличия получателя группы многоадресной рассылки в прямом канале.
  - Сообщение Multicast-Address-Specific Query: используется для определения наличия получателя определенного группового адреса в прямом канале.
- Если несколько многоадресных маршрутизаторов с MLD существуют в общем сегменте сети, запускается механизм выбора генератора запросов. Маршрутизатор с самым маленьким адресом IPv6 в сетевом сегменте выступает в качестве генератора запросов, а другие маршрутизаторы выступает в качестве наблюдателей.
- Базовый процесс, в рамках которого хост присоединяется к группе многоадресной рассылки (в качестве примера используются сообщения General Query):
  - 1. Генератор запросов периодически посылает сообщение General Query с адресом назначения FF02:: 1 на все локальные (link-local) хосты в общем сетевом сегменте в режиме многоадресной рассылки.
  - 2. Все хосты в сетевом сегменте получают сообщение General Query. Если Хост B и Хост C хотят присоединиться к группе многоадресной рассылки Г1, установите задержку ответа в помощью таймера.
  - 3. После истечения срока действия таймера хост, желающий присоединиться к группе многоадресной рассылки, посылает сообщение Report всем хостам и маршрутизаторам в сетевом сегменте в многоадресном режиме для ответа на запрос. В сообщении Report содержится адрес Г1.
  - 4. После получения сообщения Report все хосты и маршрутизаторы в сетевом сегменте получают информацию многоадресной рассылки о Г1. В этом случае другие хосты, желающие присоединиться к группе многоадресной рассылки Г1, не отправляют одно и то же сообщение Report. Если Хост A хочет присоединиться к другой группе многоадресной рассылки Г2, он отправляет сообщение Report, содержащее адрес Г2, в ответ на сообщение General Query.
  - 5. После завершения процесса запроса/ответа запрос генератор запросов может узнать, существуют ли получатели Г1 в сетевом сегменте, к которому он подключен напрямую, и создает записи многоадресной маршрутизации (*, Г1), где * означает любой источник многоадресной рассылки.
  - 6. Через механизм многоадресной маршрутизации генератор запросов запрашивает информацию из источников многоадресной рассылки. При наличии получателей в сетевом сегменте, к которому он подключен напрямую, данные переадресовываются в сетевой сегмент, а хосты, входящие в группу многоадресной

рассылки, получают данные.

Процесс выхода из группы



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Если хост хочет покинуть группу многоадресной рассылки, он посылает сообщение Done на канал через групповой адрес (адрес назначения FF02:: 2) и передает адрес, который он должен прекратить слушать, в поле multicast address.
- Если адрес группы многоадресной рассылки, из которой хочет выйти хост, находится в списке адресов генератора запросов в канале и генератор запросов получает сообщение Done от канала, то генератор запросов отправляет сообщения Multicast-Address-Specific Query из Last Listener Query Count. Интервал: Last Listener Query Interval. Как правило, Last Listener Query Interval имеет значение Maximum Response Delay в сообщении Multicast-Address-Specific Query. Если срок действия последнего запроса истекает, и сообщение Report, содержащее адрес многоадресной рассылки, не отправляется генератору запросов в канале, адрес удаляется из списка адресов прослушивания.

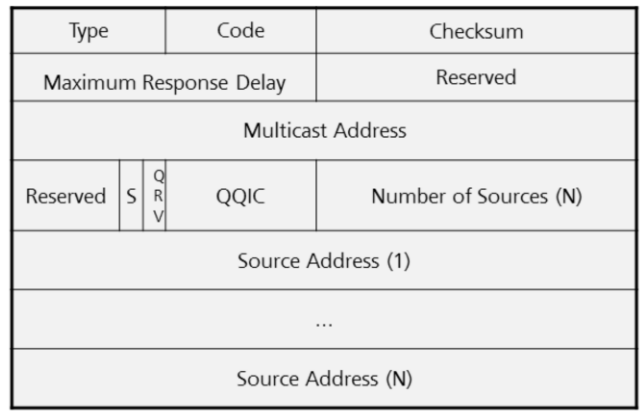


Содержание

1. Обзор MLD
2. MLDv1
3. **MLDv2**
4. SSM Mapping

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

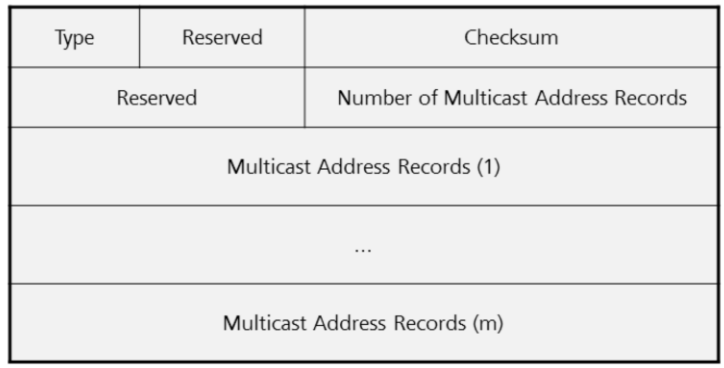
Формат сообщения Query в MLDv2



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Первые 192 бита в сообщении MLDv2 такие же, как в сообщении MLDv1.
- Флаг S (Прекратить серверную обработку, Suppress Router-side Processing):
  - установка этого флага указывает всем маршрутизаторам, получившим данное сообщение, прекратить обновления по таймеру.
- QRV (Переменная надежности запрашивающего, Querier's Robustness Variable) :
  - QRV является значением по умолчанию сообщения Last Listener Query Count и обозначает количество раз, которое маршрутизатор посылает сообщения Multicast-Address-Specific Query, пока не определит, что других слушателей не осталось.
- QQIC (Код интервала запроса, Querier's Query Interval Code):
- Number of Sources:
  - Это поле имеет значение 0 в сообщениях General Query или Multicast-Address-Specific Query.
  - Это поле указывает количество адресов источников, содержащихся в сообщении Group-Source-Specific Query.
- Source Address:
  - Адрес источника многоадресной рассылки

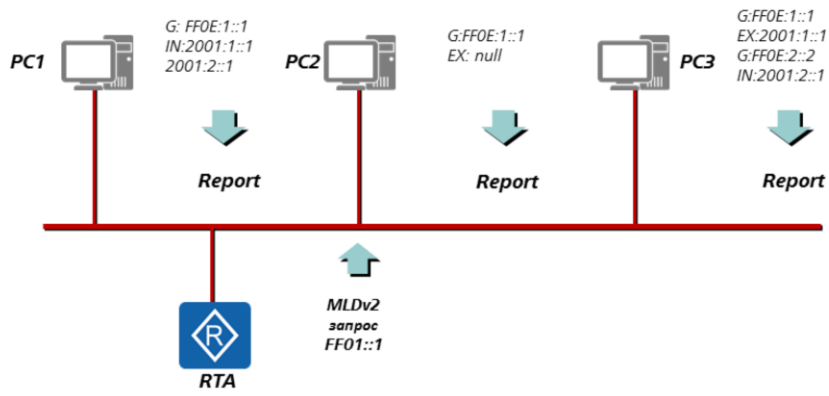
Формат сообщения Report в MLDv2



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Хост отправляет сообщение MLD Report с текущем состоянием прослушивания многоадресной рассылки.
- Type:
  - Тип = 143
- Reserved:
  - Значение 0 для передачи или игнорируется при приеме.
- Checksum:
  - Стандартная контрольная сумма ICMPv6, охватывающая все сообщение MLD и псевдозаголовок полей заголовков IPv6
- Number of Multicast Address Records
- Multicast Address Records:
  - В поле приведена информация о каждом групповом адресе, который слушает хост в интерфейсе. Информация включает тип записи, групповой адрес и адрес источника.

Запросы с указанием группы и источника (Group-Source-Specific Query)



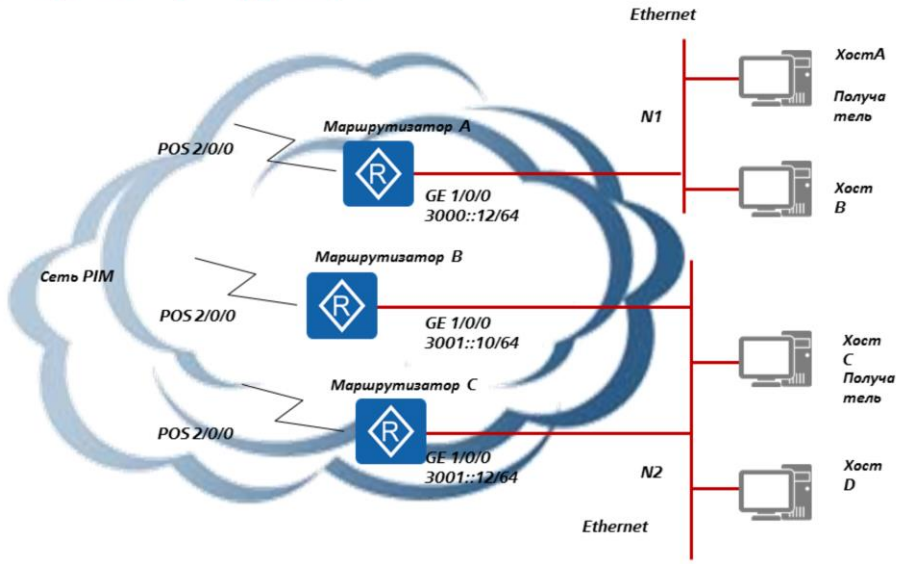
Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Версия MLDv2 совместима с версией MLDv1. Принципы работы MLDv2 аналогичны принципам MLDv1. MLDv2 поддерживает списки источников и режимы фильтрации. Вы можете указать адреса источников, чтобы присоединиться к группе многоадресной рассылки, реализующей SSM.
- Фильтрация источников многоадресной рассылки IPv6: помимо запроса для конкретной группы, в MLDv2 добавлены следующие режимы фильтрации для источников многоадресной рассылки: Include или Exclude.
  - Если после присоединения к группе многоадресной рассылки хосту нужно только получать пакеты из указанных источников, таких как S1 и S2, в сообщениях MLD Report можно настроить фильтр Include Sources (S1, S2,...).
  - Если после присоединения к группе многоадресной рассылки хосту не хочет получать пакеты от определенных источников, таких как S1 и S2, в сообщениях MLD Report можно настроить фильтр Exclude Sources (S1, S2,...).
- Отслеживание статуса группы многоадресной рассылки IPv6: маршрутизаторы с MLDv2 поддерживают статус группы многоадресной рассылки IPv6 на основании группового адреса подключенного канала. Состояния группы IPv6:
  - режим фильтрации: генератор запросов отслеживает состояние Include или Exclude.
  - список источников: генератор запросов отслеживает добавление или удаление источников.
  - таймеры: включить таймер фильтра, когда запрос MLD querier переключается в режим Include после истечения срока действия группового адреса IPv6 и источник таймера регистрирует.
- Прослушивание статуса хоста получателя: маршрутизаторы с MLDv2 слушают статус хоста

получателя для записи и хранения информации о хостах, соединяющих группы многоадресной рассылки IPv6 в локальном сегменте сети.

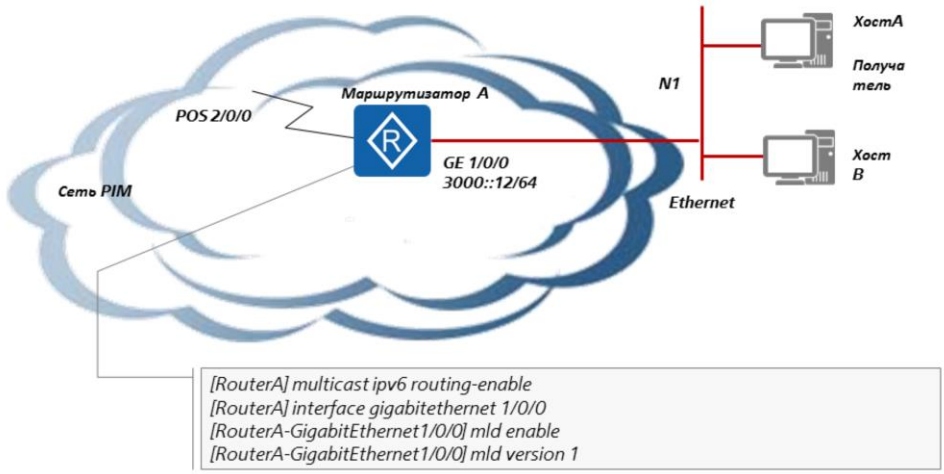
Пример конфигурации MLD



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Получатели получают видео по запросу (VoD) в режиме многоадресной рассылки. Получатели различных организаций образуют граничные сети. Каждая граничная сеть имеет один или несколько хостов-получателей.
- Хост A и Хост C являются получателями многоадресной рассылки в двух граничных сетях. Маршрутизатор A в сети PIM подключается к граничной сети N1 через GE 1/0/0 и другому устройству в сети PIM через POS 2/0/0. Маршрутизаторы B и C подключаются к граничной сети N2 через соответствующие интерфейсы GE 1/0/0 и другим устройствам в сети PIM через интерфейсы POS 2/0/0.
- Протокол MLDv1 настроен между маршрутизатором A и граничной сетью N1.
- Протокол MLDv2 настроен между маршрутизаторами B/C и граничной сетью N2.

Конфигурирование маршрутизатора A

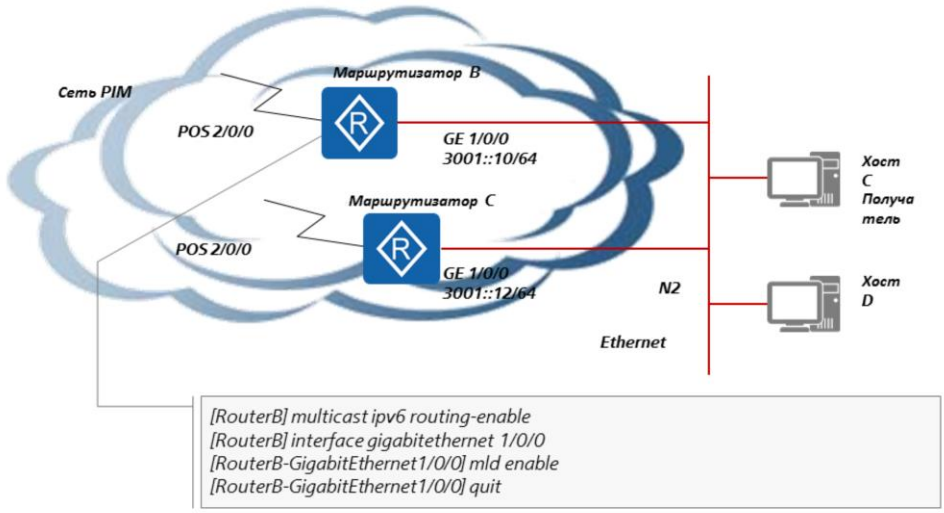


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Перейдите в режим командного интерфейса system view.
  - **system-view**
- Включите многоадресную IP-маршрутизацию.
  - **multicast ipv6 routing-enable**
- Перейдите в режим interface view.
  - **interface** *interface-type interface-number*
- Включите MLD.
  - **mld enable**
  - Протокол MLD должен быть включен на интерфейсе маршрутизатора с MLD для прослушивания всех групповых адресов IPv6.
  - Включите протокол MLD на интерфейсах, которые должны создавать и поддерживать членство в группах многоадресных рассылок.
  - Генератор запросов периодически посылает сообщения MLD Query в напрямую подключенный сетевой сегмент для поддерживания информации о многоадресной рассылке. При получении сообщения Report от члена группы, многоадресный маршрутизатор обновляет информацию участника группы.
- Перейдите в режим MLD view.
  - **mld**
- Установите версию MLD глобально.
  - **version** { **1** | **2** }
- Перейдите в режим interface view.
  - **interface** *interface-type interface-number*
- Сконфигурируйте на интерфейсе версию MLD.
  - **mld version** { **1** | **2** }
  - Эта конфигурация опциональна. По умолчанию используется MLDv2.
  - Если на интерфейсе не сконфигурирована версия MLD, то по умолчанию используется версия MLD,

сконфигурированная в режиме MLD view. Если на интерфейсе сконфигурирована версия MLD, предпочтение отдается версии MLD, сконфигурированной в режиме interface view.

Конфигурирование маршрутизатора B




```
[RouterB] multicast ipv6 routing-enable
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] mld enable
[RouterB-GigabitEthernet1/0/0] quit
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- По умолчанию используется протокол MLDv2.
- Конфигурация маршрутизатора C аналогична конфигурации маршрутизатора B.
- В сети необходимо выбрать генератор запросов. Какой маршрутизатор будет выбран в качестве генератора запросов?

Отображение информации о генераторе запросов

```
[RouterB] display mld interface gigabitethernet 1/0/0
  GigabitEthernet1/0/0(FE80::200:5EFF:FE66:5100):
    MLD is enabled
    Current MLD version is 2
    MLD group policy: none
    Value of query interval for MLD(in seconds): 125
    Value of other querier timeout for MLD(in seconds): 0
    Value of maximum query response time for MLD(in seconds): 10
    Querier for MLD: FE80::200:5EFF:FE66:5100 (this router)
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Вывод команды показывает, что маршрутизатор B является генератором запросов, так как адрес IPv6 маршрутизатора B GE 1/0/0 в одном сегменте сети меньше.

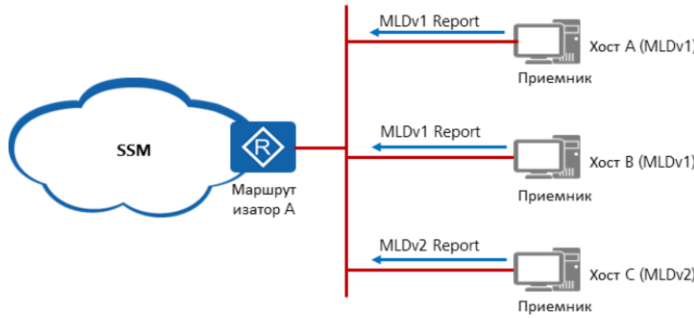
Содержание

1. Обзор MLD
2. MLDv1
3. MLDv2
4. **SSM Mapping**

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

MLD SSM Mapping

- Многоадресная передача от источника (SSM) требует, чтобы маршрутизаторы знали источники многоадресной рассылки, которые указывают хосты при присоединении к группе многоадресной рассылки. Хост с MLDv2 может указать адреса источников многоадресной рассылки в сообщениях MLDv2 Report. Некоторые хосты могут работать только в протоколе MLDv1. Для того, чтобы такие хосты могли использовать сервис SSM, маршрутизаторы должны предоставить функцию MLD SSM mapping.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- При конфигурировании SSM mapping Маршрутизатор A проверяет IPv6-адрес группы многоадресной рассылки G в каждом полученном сообщении MLDv1 Report и обрабатывает сообщение на основе результатов проверки:
  - Если адрес G находится за пределами диапазона адресов IPv6 группы SSM, маршрутизатор A предоставляет сервис ASM.
  - Если адрес G находится в диапазоне адресов IPv6 группы SSM:
  - Если у маршрутизатора нет записи MLD SSM mapping, соответствующей G, он не предоставляет сервис SSM и отбрасывает сообщение Report.
  - Если у маршрутизатор есть запись MLD SSM mapping, соответствующая G, он преобразует информацию (*, G) в сообщение Report (G, INCLUDE, (S1, S2...)) и предоставляет сервис SSM хостам. SSM mapping позволяет хостам с MLDv1 получать пакеты данных SSM без обновления версии MLD. Данная функция не влияет на хосты с MLDv2.
- Политика сопоставления может быть сконфигурирована несколько раз для сопоставления информации одной группы с несколькими источниками. Маршрутизатор передает только сообщения Group-Source-Specific Query в таблице сопоставления.

Конфигурирование MLD SSM Mapping (1)

- Перед конфигурированием SSM mapping выполните следующие действия:
  - Сконфигурируйте протокол одноадресной маршрутизации, чтобы обеспечить доступность всего домена многоадресной маршрутизации.
  - Включите многоадресную маршрутизацию IPv6.
- Подготовка данных
  - Для конфигурирования SSM mapping требуется следующая информация.

№	Данные
1	Интерфейсы, на которых необходимо включить SSM mapping
2	Имя политики IPv6 SSM mapping
3	Адрес и маска группы многоадресной рассылки; адрес источника многоадресной рассылки и маска

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Конфигурирование MLD SSM Mapping (2)

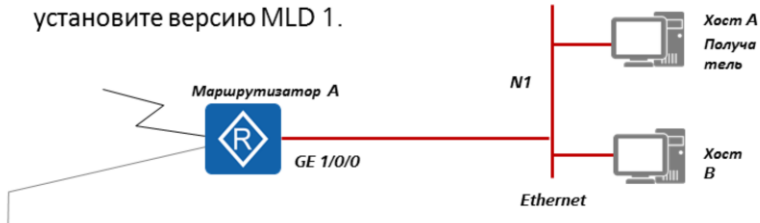
- Выполните команду **system-view** для входа в system view.
- Выполните команду **interface** *interface-type interface-number* для перехода в режим interface view.
- Выполните команду **mld enable** для включения MLD.
- Выполните команду **mld version 2** для установки версии MLD 2. Чтобы хосты с любой версией MLD в сетевом сегменте могли получать сервисы SSM, рекомендуется сконфигурировать MLDv2 на интерфейсе.
- Выполните команду **mld ssm-mapping enable** для включения SSM mapping.

- Выполните команду **system-view** для входа в system view.
- Выполните команду **mld** для входа в MLD view.
- Выполните команду **ssm-mapping** *ipv6-group-address ipv6-group-mask-length ipv6-source-address* для конфигурирования отображения из группы многоадресной рассылки в источник. Чтобы сопоставить группу многоадресной рассылки с несколькими источниками, выполните команду несколько раз.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Пример конфигурации MLD SSM Mapping

- Включите многоадресную передачу и включите MLD на интерфейсе со стороны хоста.
- #Включите многоадресную передачу на Маршрутизаторе A, включите MLD на GE 1/0/0 и установите версию MLD 1.



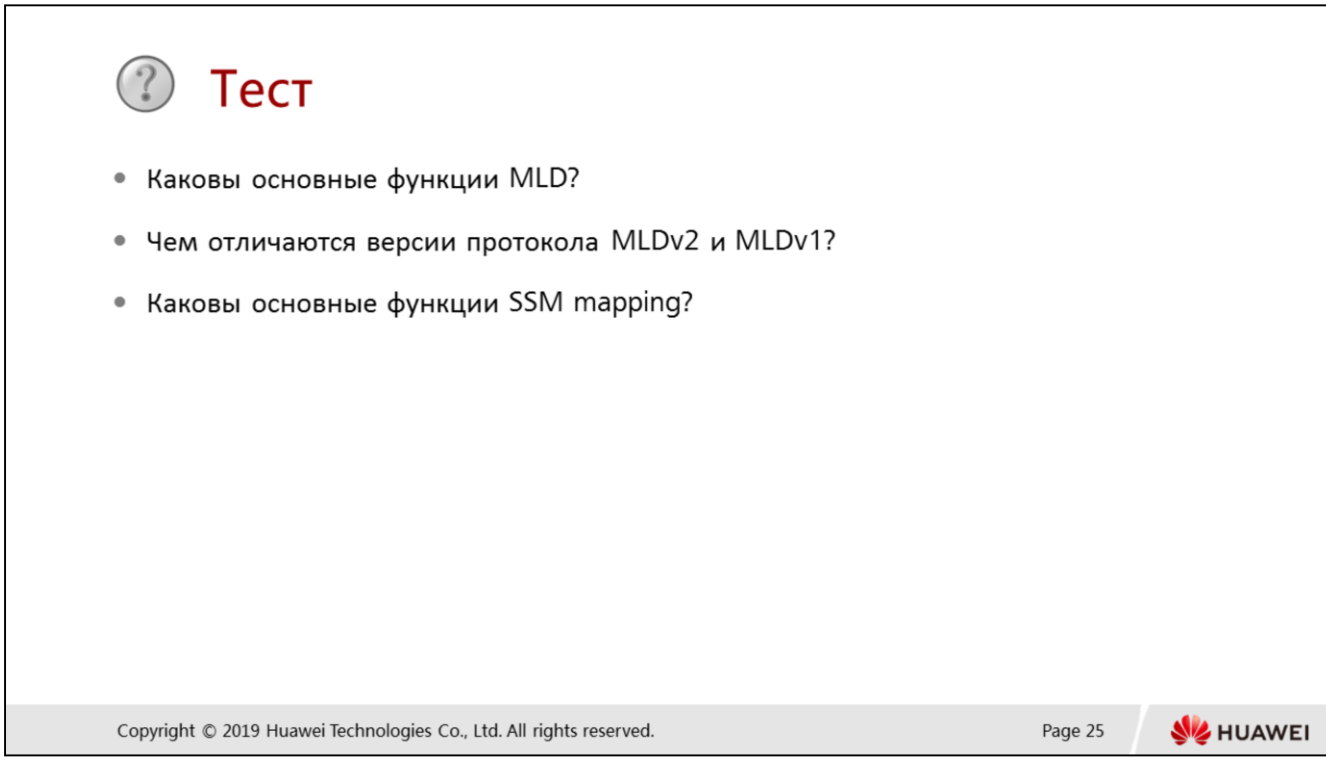

```
<RouterA> system-view
[RouterA] multicast ipv6 routing-enable
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] mld enable
[RouterA-GigabitEthernet1/0/0] mld version 2
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] mld ssm-mapping enable
```

```
[RouterA] mld
[RouterA-mld] ssm-mapping ff35::1 128 2000::1
```

Указывает адрес IPv6 и маску группы многоадресной рассылки, сконфигурированной с SSM mapping.

Указывает адрес IPv6 источника многоадресной рассылки

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.



- Каковы основные функции MLD?
  - Протокол MLD управляет членами группы многоадресной рассылки IPv6, а его принципы работы и функции аналогичны функциям IGMP. MLD обеспечивает обнаружение слушателей многоадресной рассылки (т.е. узлов, ожидающих получения многоадресных данных) каждым маршрутизатором IPv6 в сети, к которой они подключены напрямую, и идентифицировать адреса многоадресной рассылки, в которых заинтересованы соседние узлы. Сообщения затем предлагаются протоколу многоадресной маршрутизации, используемому маршрутизатором, чтобы данные многоадресной рассылки пересылались на все каналы, в которых существуют получатели.
- Чем отличаются версии протокола MLDv2 и MLDv1?
  - Версия MLDv2 совместима с версией MLDv1. Принципы работы MLDv2 аналогичны принципам работы MLDv1. MLDv2 поддерживает списки источников и режимы фильтрации. Вы можете указать адреса источников для присоединения к группе многоадресной рассылки с SSM.
- Каковы основные функции SSM mapping?
  - Хосты, отправляющие сообщения MLDv1 Report, не могут получать пакеты данных в диапазоне групп SSM. SSM mapping позволяет хостам с MLDv1 получать пакеты данных SSM без обновления версии MLD. Данная функция не влияет на хосты, использующие MLDv2.

Краткое содержание

- Функции протокола MLD
- Принципы работы MLDv1
- Улучшение в версии MLDv2
- Функции SSM Mapping

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Рекомендации

- Веб-сайт Huawei E-Learning:
  - http://support.huawei.com/learning/en/newindex.html
- Библиотека примеров Huawei:
  - http://support.huawei.com/enterprise/en/knowledge/enterprises-common-pid-8221819

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Спасибо!

www.huawei.com

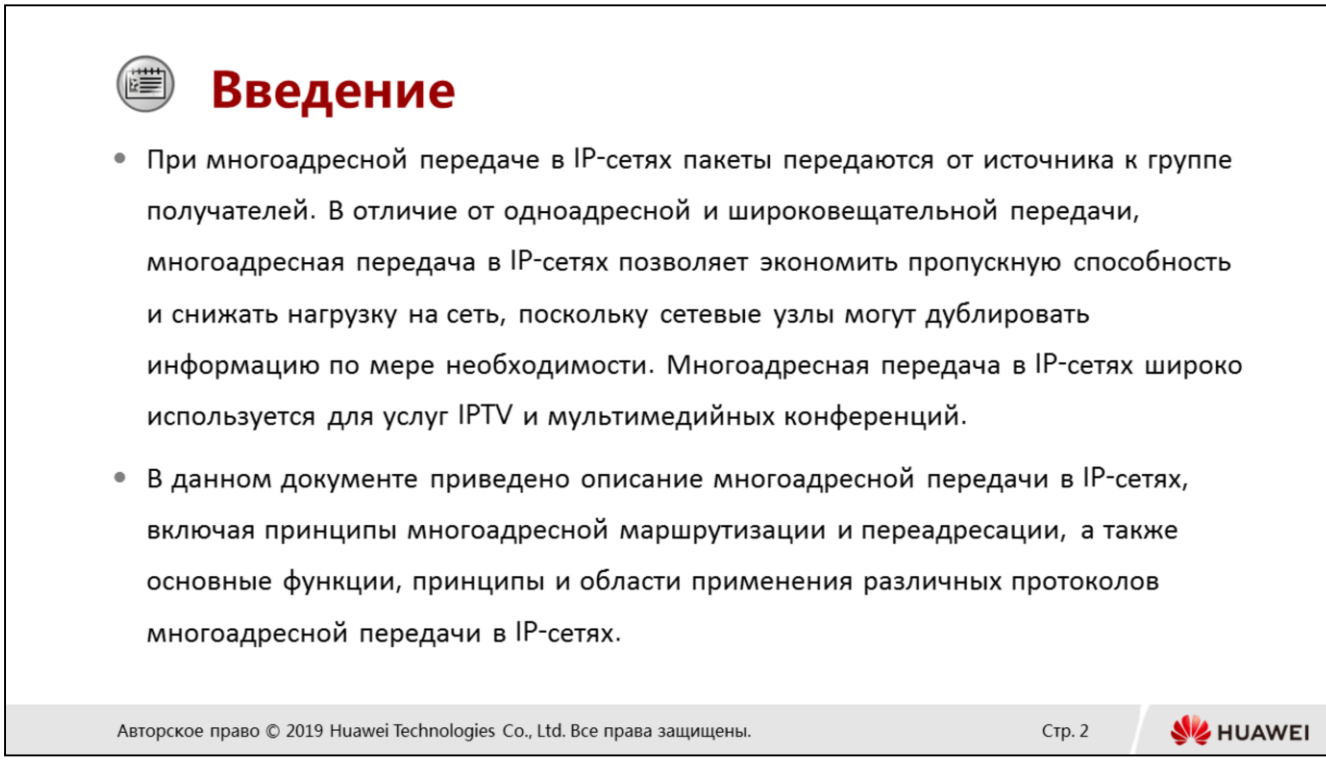
HCIE-R&S

PIM

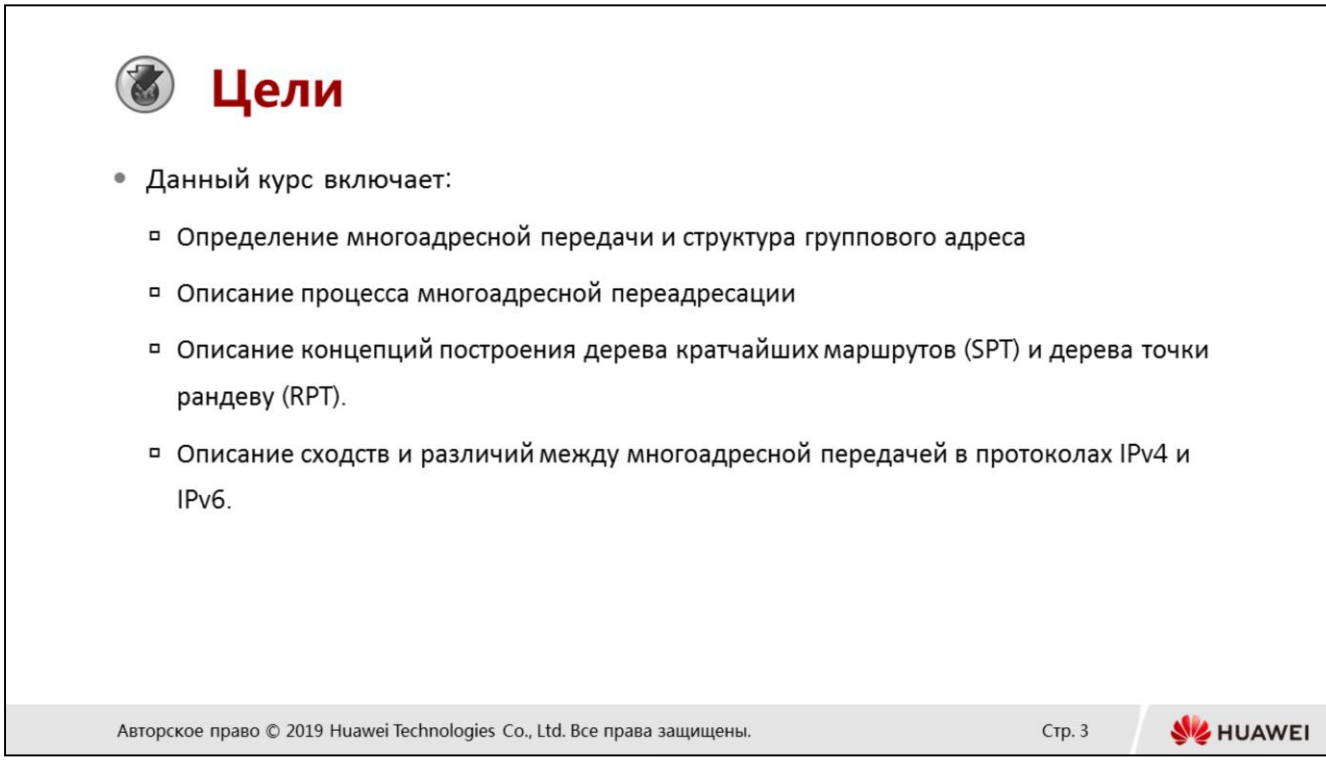
www.huawei.com

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI



- В современных технологиях передачи данных по сети уделяется большое внимание следующим двум целям:
  - Обнаружение ресурсов
  - Передача данных через многоточечное соединение
- Существует три решения для достижения этих двух целей: одноадресная, широковещательная и многоадресная передача.
- При сравнении этих трех способов можно сделать вывод, что многоадресная рассылка больше подходит для многоточечной передачи данных в IP-сетях.



- По завершении этого курса вы будете знать отличия между режимами многоадресной, одноадресной и широковещательной передачи, будете знать структуру адреса многоадресной рассылки, процесс переадресации многоадресных пакетов и связанные понятия, такие как as SPT и RPT.

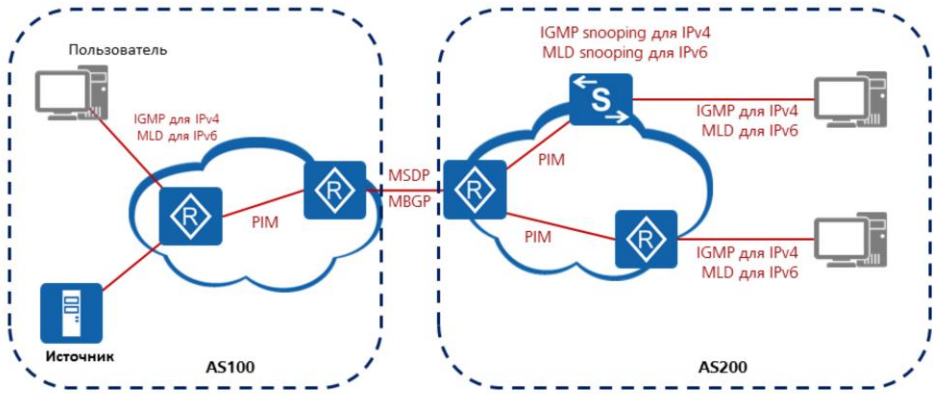
Содержание

- **Механизм PIM-SM**
- Конфигурация IPv6 PIM-SM
- Основные принципы IPv6 PIM-SSM
- Управление многоадресным маршрутом
- Типичные области применения многоадресной передачи IPv6

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Протоколы многоадресной передачи

- К протоколам многоадресной передачи относятся протоколы управления группами многоадресной передачи для регистрации хоста и протоколы многоадресной маршрутизации для маршрутизации и пересылки.



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- К протоколам многоадресной передачи относятся протоколы управления группами многоадресной передачи для регистрации хоста и протоколы многоадресной маршрутизации для маршрутизации и пересылки. На рисунке показаны различные многоадресные протоколы, используемые в сети.
- IGMP (Internet Group Management Protocol — протокол управления группами Интернета) используется между хостами получателей и многоадресными маршрутизаторами, и определяет механизм вступления в многоадресные группы и обмена информацией о членстве в таких группах между хостами и маршрутизаторами.
- Протоколы многоадресной маршрутизации, настроенные между маршрутизаторами, используются для установления и поддержания многоадресных маршрутов, а также для правильной и эффективной пересылки многоадресных данных.
- В модели ASM маршруты подразделяются на внутридоменные и междоменные.
  - Протоколы внутридоменной многоадресной маршрутизации позволяют обнаруживать источники многоадресной передачи и создавать деревья многоадресной рассылки в автономной системе (AS), чтобы доставлять информацию получателям. К протоколам внутридоменной маршрутизации относятся: протокол многоадресной маршрутизации по вектору расстояния (DVMRP), многоадресный протокол доступного кратчайшего маршрута (MOSPF) и группа многоадресных протоколов маршрутизации PIM.
    - DVMRP – это протокол плотного режима. Он определяет ограничение количества узлов в маршруте до 32.
    - MOSPF – это расширенный протокол OSPF. Он определяет новые LSA-пакеты для поддержки многоадресной рассылки.
    - PIM является типичным протоколом внутридоменной многоадресной маршрутизации и может работать в плотном режиме (DM) или в разреженном режиме (SM). Плотный режим применяется в случае высокой концентрации получателей в сети, а разреженный режим – когда по сети рассредоточено небольшое количество получателей. Протокол PIM должен взаимодействовать с протоколом одноадресной маршрутизации.
  - Протоколы междоменной многоадресной маршрутизации используются для передачи многоадресной информации между AS.
    - Протокол обнаружения источника многоадресной передачи (MSDP) позволяет передавать информацию об источнике многоадресной передачи среди AS.

- Multiprotocol BGP (MP-BGP) – это расширение протокола BGP, которое позволяет передавать многоадресные маршруты среди AS.

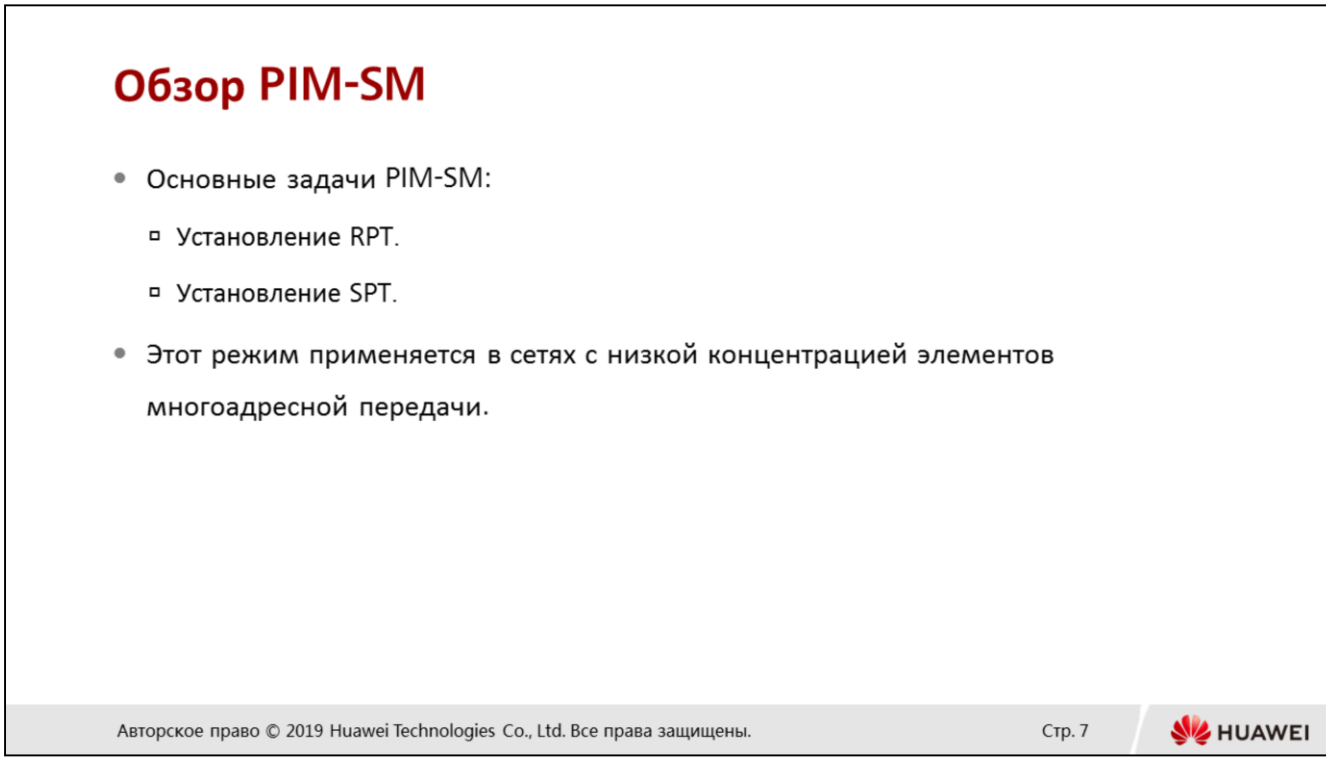
Протоколы, используемые в сети многоадресной передачи

Протокол	Место развертывания	Функция
IGMP для IPv4 MLD для IPv6	Между многоадресными маршрутизаторами и хостами	Протокол IGMP/MLD позволяет хостам динамически присоединяться и выходить из групп многоадресной рассылки на стороне хоста. На стороне маршрутизатора IGMP/MLD обменивается информацией с протоколами многоадресной маршрутизации верхнего уровня, а также управляет и поддерживает связь между участниками группы многоадресной рассылки.
PIM	Все интерфейсы на всех многоадресных маршрутизаторах	Обеспечивает многоадресную маршрутизацию и пересылку, а также поддерживает актуальность таблицы многоадресной маршрутизации в соответствии с изменениями топологии сети.
IGMP snooping для IPv4 MLD snooping для IPv6	Сети VLAN на уровне 2 выполняют переключение между многоадресными маршрутизаторами и хостами	Прослушивание сообщений IGMP/MLD, которыми обмениваются маршрутизаторы и хосты, для создания таблицы многоадресной маршрутизации 2-го уровня. Таким образом многоадресные данные пересылаются в сети 2-го уровня.
MSDP только для IPv4 MBGP	Пограничный маршрутизатор AS	При передаче информации об источнике многоадресной передачи через домены PIM требуется MSDP. При создании многоадресных маршрутов через AS требуется MBGP.

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- В модели SSM нет деления на междоменную и внутридоменную маршрутизацию. Получатели знают местоположение домена-источника многоадресной рассылки; следовательно, каналы многоадресной передачи могут быть установлены с помощью функций PIM-SM.
- Между доменами PIM-SM необходимо развернуть протокол MSDP, чтобы между доменами можно было настроить многоадресную рассылку. Между доменами PIM-SM устанавливаются отношения соседства MSDP, и соседи MSDP обмениваются сообщениями SA, чтобы получить данные многоадресной рассылки друг друга. После этого хосты получателя в одном домене PIM-SM смогут получать данные от источника многоадресной передачи, расположенного в другом домене PIM-SM. Протокол MSDP применяется только в сетях IPv4 и пригоден только в модели ASM. В PIM-домене протокол IGMP управляет членством в группах, а PIM-SM поддерживает маршруты многоадресной пересылки.
- PIM пересылает многоадресные данные на основе таблицы одноадресной маршрутизации. Поэтому пути многоадресной и одноадресной передачи совпадают. Когда источник и получатели многоадресной передачи расположены в разных AS, между AS необходимо настроить дерево многоадресной рассылки. В этом сценарии можно использовать протокол MBGP для создания таблицы многоадресной маршрутизации, независимой от таблицы одноадресной маршрутизации. После чего многоадресные данные будут передаваться на основе таблицы многоадресной маршрутизации.

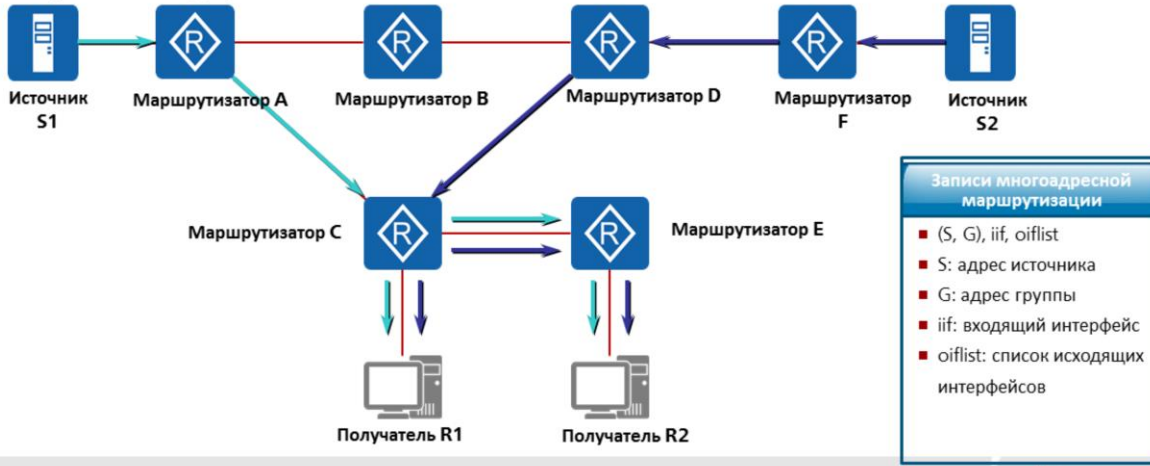


- По сравнению с PIM-DM, в котором используется модель распространения трафика push, в PIM-SM для пересылки многоадресных пакетов используется модель pull. Протокол PIM-SM предполагает, что члены группы разбросаны по сети, и большинство сегментов сети не имеет участников группы. Многоадресные маршруты для пересылки данных в сегмент сети создаются только тогда, когда в этом сегменте появляются участники группы. PIM-SM обычно используется для сетей с большим количеством рассредоточенных участников группы.
- Устройства в сети PIM-SM имеют следующие функции:
  - Точка рандеву (Rendezvous Point, RP) – важный маршрутизатор PIM, который предоставляет услуги участникам группы или многоадресным источникам, которые могут появиться в любое время. Все маршрутизаторы PIM в сети знают местоположение RP.
  - Когда устройство пользователя присоединяется к многоадресной группе G через протокол IGMP, последний маршрутизатор отправляет сообщение Join на RP. Запись (*, G) создается последовательно, от узла к узлу. Затем генерируется RPT с RP в качестве корневого узла.
  - Когда источник многоадресной рассылки отправляет первый многоадресный пакет группе многоадресной рассылки G, первый маршрутизатор инкапсулирует многоадресные данные в сообщение Register и отправляет его RP в режиме одноадресной передачи. Затем RP-маршрутизатор создает запись (S, G) и регистрирует информацию об источнике многоадресной рассылки.
- PIM-SM использует функции обнаружения соседнего узла, выбора DR-маршрутизатора, обнаружения RP, настройки RPT, регистрации источника многоадресной передачи, переключения SPT и механизмы подтверждения. Вы можете настроить загрузочный

маршрутизатор (BSR) для точного управления передачей в одном домене PIM-SM. Механизмы обнаружения и подтверждения соседних узлов в PIM-SM аналогичны механизмам, используемым в PIM-DM.

Дерево кратчайшего пути (SPT)

- Между каждым источником и получателем многоадресной рассылки настраивается дерево SPT.



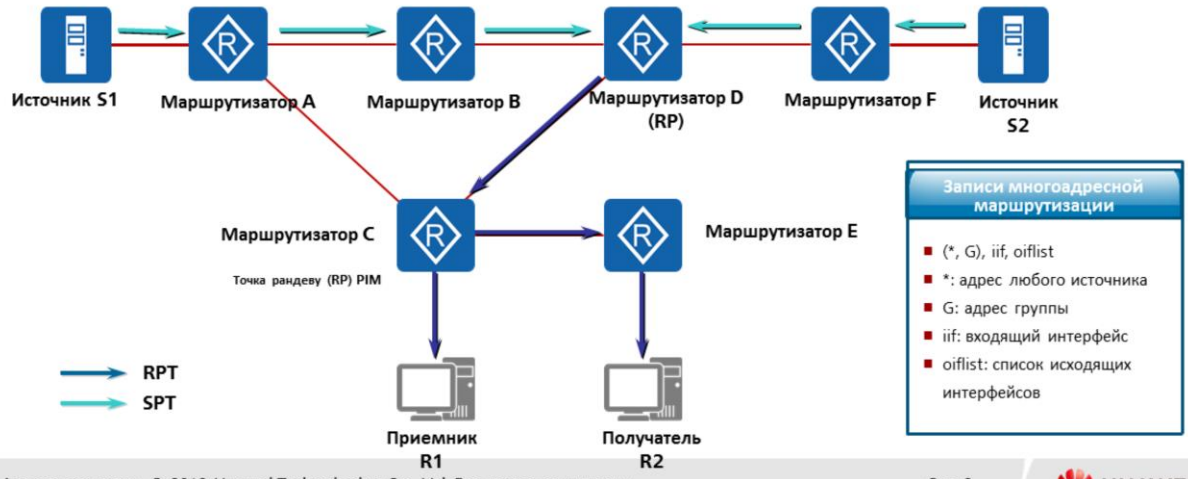
Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Корнем SPT является источник многоадресной передачи. Дерево SPT объединяет кратчайшие пути от источника к получателям.
- В случае с многоадресной группой, маршрутизаторы создают дерево SPT от каждого источника многоадресной рассылки, который отправляет пакеты в группу.
- В этом примере показаны два источника (S1 и S2) и два получателя (R1 и R2). В сети настроено два дерева SPT.
- S1 – Маршрутизатор A – Маршрутизатор C (R1) – Маршрутизатор E (R2)
- S2 – Маршрутизатор F – Маршрутизатор D – Маршрутизатор C (R1) – Маршрутизатор E (R2)

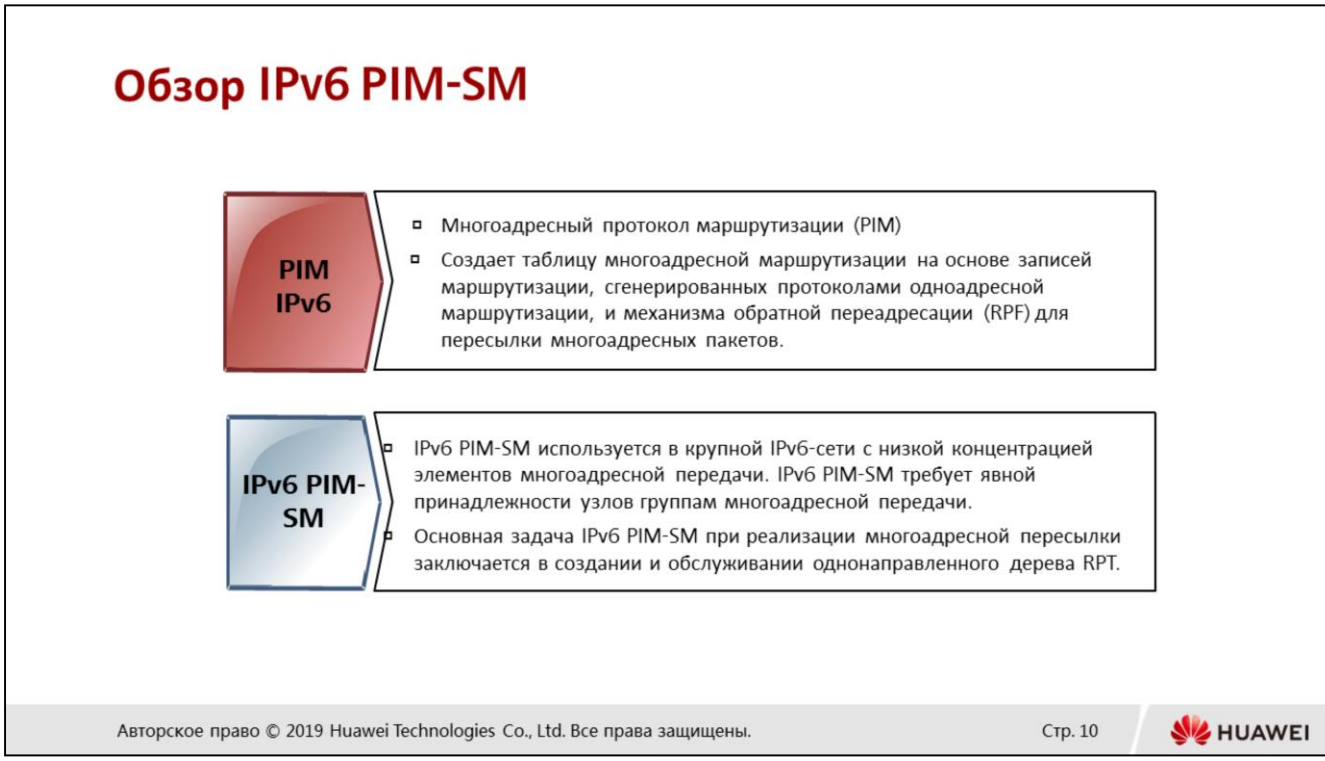
Дерево с корнем в точке рандеву (RPT)

- Для каждой группы многоадресной рассылки настраивается только одно дерево RPT.



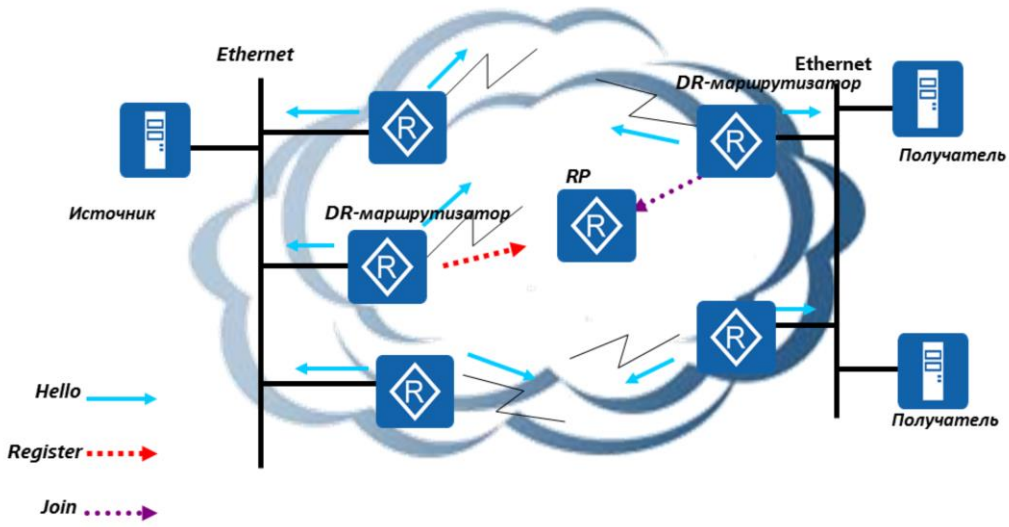
Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Корнем дерева RPT является точка рандеву (RP). Дерево RPT объединяет кратчайшие пути от RP до всех получателей. Для каждой группы многоадресной рассылки настраивается только одно дерево RPT. Все источники и получатели группы отправляют и получают многоадресные пакеты данных через дерево RPT. Сначала источник многоадресной рассылки отправляет пакеты данных на RP, которая затем пересылает пакеты всем получателям.
- В этом примере многоадресные источники S1 и S2 совместно используют одно дерево RPT: Маршрутизатор D (RP) – Маршрутизатор C (R1) – Маршрутизатор E (R2)



- PIM IPv6 – это протокол многоадресной маршрутизации, независимый от протоколов одноадресной маршрутизации IPv6, таких как статические маршруты, RIPng, OSPFv3, IS-ISv6 и BGP4+. Для пересылки многоадресных пакетов данный протокол создает таблицу многоадресной маршрутизации на основе записей маршрутизации, сгенерированных протоколами одноадресной маршрутизации, и механизмом RPF. Домен PIM IPv6 – это сеть, состоящая из многоадресных маршрутизаторов, поддерживающих PIM IPv6.
- В настоящее время существует две модели многоадресной рассылки: многоадресная рассылка из произвольного источника (ASM) и многоадресная рассылка из определенного источника (SSM). В IPv6-сети модель ASM действует на базе протоколов IPv6 PIM-DM и IPv6 PIM-SM. Модель SSM реализуется с помощью протокола MLDv2 и некоторых механизмов IPv6 PIM-SM.
- IPv6 PIM-SM применяется в крупной IPv6-сети, где участники группы рассредоточены. IPv6 PIM-SM требует явной принадлежности узлов группам многоадресной передачи. По умолчанию IPv6 PIM-SM считает, что не все узлы в сети должны получать многоадресные пакеты. Вышестоящие узлы пересылают многоадресные данные только после получения сообщений Join от нижестоящих узлов.
- В IPv6 PIM-SM RP-маршрутизатор передает многоадресную информацию только в нисходящих направлениях, в которых есть получатели, что позволяет снизить загрузку каналов пакетами данных и пакетами управления, а также снизить объем обработки заголовков маршрутизаторами.
- Если хост хочет получить данные из определенной группы многоадресной рассылки, маршрутизатор, подключенный к хосту, отправляет сообщение Join на RP в группе. Дерево RPT, корнем которого является RP, создается вдоль пути. Дерево RPT позволяет использовать этот общий путь, когда разные источники многоадресной рассылки пересылают данные в одну и ту же группу.
- Когда источник многоадресной рассылки отправляет данные в группу многоадресной рассылки, DR-маршрутизатор, подключенный к источнику, инкапсулирует данные многоадресной рассылки в сообщение Register и отправляет его RP в режиме одноадресной передачи. Когда RP-маршрутизатор получает сообщение Register, он декапсулирует данные и отправляет их получателю через дерево RPT. Когда передача данных, отправленных в сообщениях Register, достигает определенной скорости, RP отправляет сообщение Join источнику многоадресной рассылки, чтобы создать дерево многоадресной рассылки между источником многоадресной рассылки и RP.Затем RP отправляет сообщение Register-Stop DR-маршрутизатору на стороне источника, в котором указывает DR-маршрутизатору отправлять многоадресные данные напрямую в режиме без инкапсуляции в соответствии с информационной базой многоадресной пересылки (MFIB).

Выбор DR-маршрутизатора



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Выбор DR-маршрутизатора осуществляется в сегменте общей сети с помощью сообщений Hello. DR-маршрутизатор является единственным узлом, пересылающим многоадресные данные в сегменте сети. DR-маршрутизатор выбирается в общей сети, которая соединяет источник с получателями. DR-маршрутизатор на стороне получателя отправляет сообщение Join RP-маршрутизатору, а DR-маршрутизатор на стороне источника отправляет сообщение Register RP-маршрутизатору.

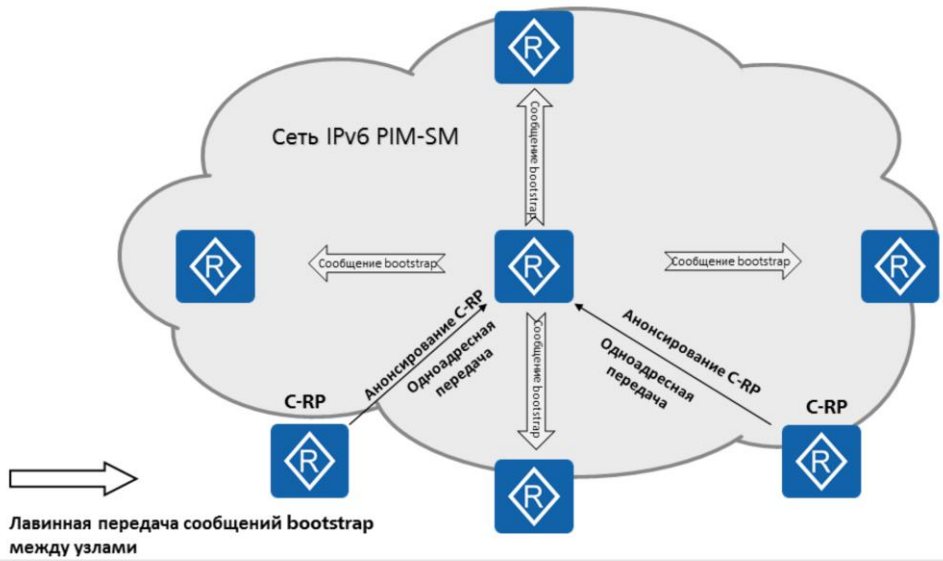
- Процедура выбора DR-маршрутизатора:
  - Маршрутизаторы в сегменте общей сети отправляют друг другу сообщения Hello с приоритетом DR.
  - В качестве DR-маршрутизатора в сегменте сети выбирается маршрутизатор с наивысшим приоритетом. Если у маршрутизаторов одинаковый приоритет, то в качестве DR-маршрутизатора выбирается маршрутизатор с наибольшим IPv6-адресом.
- В случае неисправности DR-маршрутизатора другие маршрутизаторы не смогут получать от него сообщения Hello. После истечения срока действия DR-маршрутизатора в сегменте общей сети запускается новый раунд выбора.
- Если хотя бы один маршрутизатор в сети не разрешит сообщениям Hello передавать приоритет DR, то в качестве DR-маршрутизатора будет использоваться маршрутизатор с наибольшим IPv6-адресом link-local.



- Как найти точку RP? В небольшой сети RP достаточно передать информацию по сети, и ее местоположение будет определено. Вы можете вручную указать IP-адрес RP на DR-маршрутизаторе, конечных маршрутизаторах и всех маршрутизаторах, через которые проходят потоки многоадресных данных. Однако в большинстве областей применения сеть IPv6 PIM-SM является крупной, и через RP необходимо пересылать большой объем многоадресного трафика. Поэтому у каждой многоадресной группы должна быть своя RP. Чтобы избежать настройки нескольких статических RP и улучшить адаптацию сети к изменениям в реальном времени, для динамического выбора RP применяется механизм Bootstrap.
- Механизм BSR является ключевым механизмом управления сети IPv6 PIM-SM. BSR собирает сообщения Advertisement от каждого RP-кандидата (C-RP) и выбирает подходящие C-RP для формирования информации RP-Set групп многоадресной рассылки. RP-Set – это база данных для каждой многоадресной группы и соответствующий C-RP. BSR сообщает всей сети IPv6 PIM-SM информацию RP-Set с помощью сообщения bootstrap. После получения C-RP для каждой многоадресной группы все маршрутизаторы, включая DR-маршрутизатор, вычисляют уникальную точку RP для каждой многоадресной группы на основе алгоритма хеширования.
- В сети (или домене управления) может быть только один BSR, но несколько кандидатов BSR (C-BSR). В случае неисправности BSR, выбирается новый BSR из C-BSR с помощью механизма Bootstrap, чтобы предотвратить прерывание обслуживания. В домене IPv6 PIM-SM можно настроить несколько C-RP. BSR собирает и отправляет информацию RP-Set каждой группы многоадресной рассылки.
- Рекомендации по настройке RP:
    - В небольших и средних сетях настройте статическую точку RP, так как такие сети отличается стабильностью и низкими требованиями к сетевым устройствам.
    - Если существует только один источник многоадресной рассылки, используйте маршрутизатор, напрямую подключенный к источнику многоадресной рассылки, в качестве статической точки RP, чтобы DR-маршрутизатору источника не нужно был регистрироваться в RP.
    - Если вы используете статическую точку RP, то на всех маршрутизаторах, включая RP в одном домене, должна быть настроена одинаковая информация и одинаковый диапазон групп многоадресной рассылки.
    - В крупных сетях рекомендуется использовать динамическую точку RP, поскольку она обладает высокой надежностью и проста в обслуживании.

- В случае плотного расположения нескольких источников многоадресной рассылки в сети, настройте основные маршрутизаторы вблизи источников многоадресной рассылки в качестве C-RP. Если несколько участников группы плотно расположены в сети, настройте основные маршрутизаторы, распложенные вблизи от участников группы, в качестве C-RP.

Выбор RP



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Механизм BSR: подходящие маршрутизаторы в сети настраиваются в качестве C-BSR. Каждый C-BSR имеет приоритет. После выполнения настройки маршрутизатора в качестве C-BSR запускается таймер (по умолчанию 150 с) для отслеживания сообщений bootstrap в сети. Первое сообщение bootstrap, отправленное с C-BSR, содержит приоритет и IPv6-адрес C-BSR. После получения сообщения bootstrap C-BSR сравнивает свой приоритет с приоритетом, указанным в сообщении. Если приоритет в сообщении выше, C-BSR сбрасывает свой таймер и продолжает прослушивать сообщения bootstrap. Если C-BSR обнаруживает, что его собственный приоритет выше, он отправляет сообщение bootstrap, чтобы объявить, что он является BSR. Если приоритеты одинаковы, C-BSR начинает сравнивать адреса IPv6. C-BSR с большим IPv6-адресом выбирается в качестве BSR. Адрес назначения каждого сообщения bootstrap – FF02::13, а TTL имеет значение 1. Все маршрутизаторы PIM IPv6 могут получать сообщение и отправлять его со всех интерфейсов, поддерживающих PIM IPv6, чтобы все устройства PIM IPv6 в сети могли получить сообщение bootstrap.
- Точки RP необходимо сконфигурировать на устройствах вручную. Сначала настройте C-RP, включая IPv6-адреса RP, приоритеты и группы, которые будут обслуживаться этими C-RP. Как упоминалось выше, RP может предоставлять услуги для некоторых или всех групп многоадресной рассылки IPv6. После получения сообщения bootstrap каждый C-RP узнает BSR в сети. Затем C-RP одноадресно передает группы многоадресной рассылки, которые он может обслуживать, в BSR в сообщении Candidate-RP-Advertising. Таким образом, BSR собирает информацию обо всех C-RP в сети и сортирует информацию в RP-Set. Затем BSR отправляет информацию RP-Set всем маршрутизаторам во всей сети в сообщении bootstrap.
- Правила выбора RP:
  - Если в RP-Set имеется только один C-RP для группового адреса IPv6, то DR-маршрутизатор выберет C-RP в качестве RP.
  - Если в RP-Set имеется несколько C-RP для группового адреса IPv6, то DR-маршрутизатор выберет C-RP с наивысшим приоритетом (меньшее значение указывает на более высокий приоритет) в качестве RP.
  - Если приоритеты одинаковы, DR-маршрутизатор запускает алгоритм хеширования и использует групповые адреса, хеш-маски и адреса C-RP в качестве входных параметров. DR-маршрутизатор

выводит номер каждого C-RP и выбирает C-RP с более высоким номером в качестве RP группы.

- Если результаты хеширования также совпадают, то в качестве RP группы будет выбран C-RP с наибольшим IPv6-адресом.



- С механизмом embedded RP маршрутизатор может получать адрес RP из адреса многоадресной рассылки IPv6, чтобы заменить RP на статическую RP или на RP, динамически рассчитанную маршрутизатором BSR.
- Диапазон адресов многоадресной рассылки в сценарии со встроенным адресом RP - от FF7*x*::/16 до FFF*x*::/16, где x обозначает любое шестнадцатеричное число в диапазоне от 0 до F.
- На стороне получателя:
  - Хост получателя отправляет сообщение MLD Report, чтобы присоединиться к многоадресной группе.
  - DR-маршрутизатор на стороне получателя извлекает адрес RP, содержащийся в адресе многоадресной рассылки, и отправляет сообщение Join IPv6 PIM-SM на адрес RP.
- На стороне источника:
  - После того как источник многоадресной рассылки узнал адрес многоадресной рассылки, он отправляет пакеты в группу многоадресной рассылки.
  - DR-маршрутизатор на стороне источника извлекает адрес RP, содержащийся в адресе многоадресной рассылки, и отправляет сообщение Register IPv6 PIM-SM на адрес RP в режиме одноадресной передачи.

Адрес многоадресной рассылки, в котором содержится адрес RP

- Как включить 128-разрядный адрес RP в 128-разрядный адрес многоадресной рассылки IPv6?
- Специальный адрес многоадресной рассылки настраивается следующим образом:



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

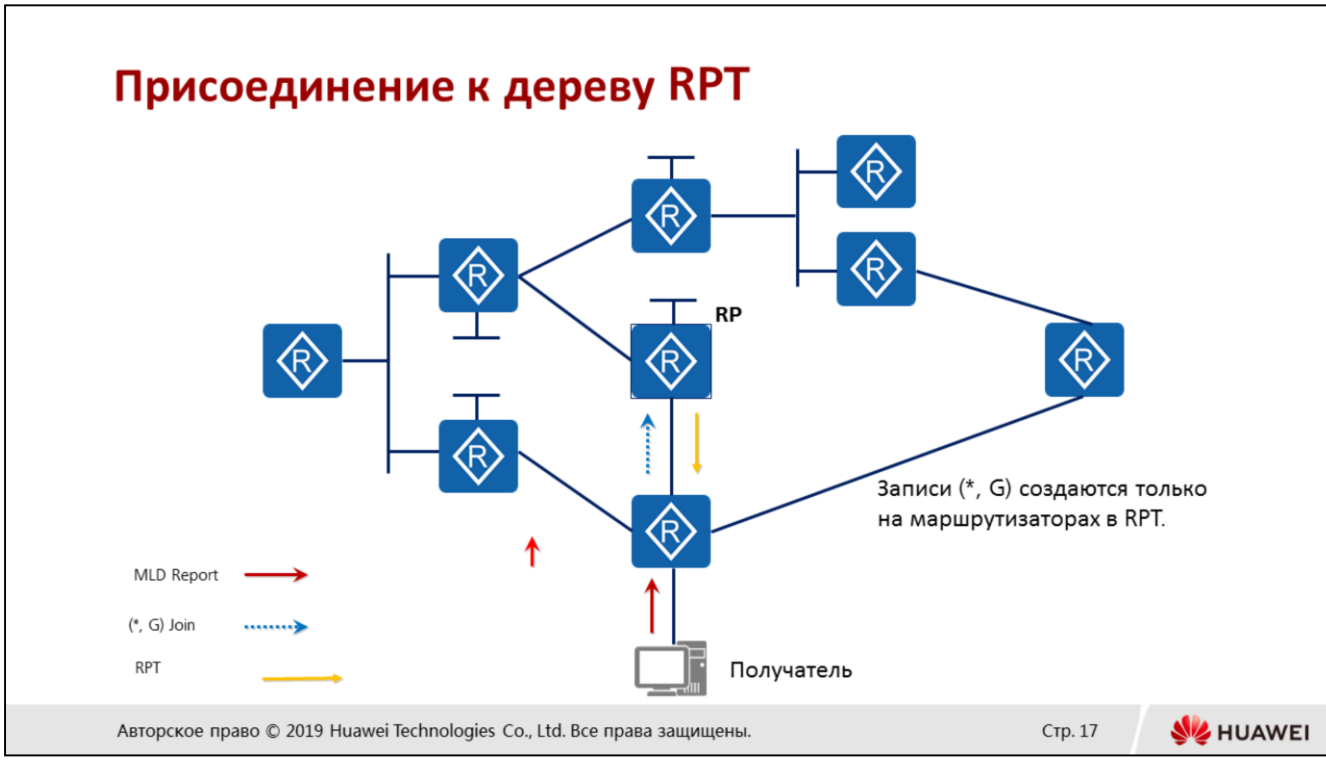
- Первые 8 бит – это FF, означающий адрес многоадресной рассылки IPv6.
- Диапазон значений поля Flags – от 7 до F. Поле указывает на адрес многоадресной рассылки IPv6, в котором содержится адрес RP.
- RIID: идентификатор интерфейса RP, который заполняется последними 4 битами адреса RP.
- Plen: длина префикса адреса RP, которая после перевода в десятичную систему не может быть равна 0 или превышать 64.
- Network Prefix: префикс адреса RP.

Преобразование адреса RP

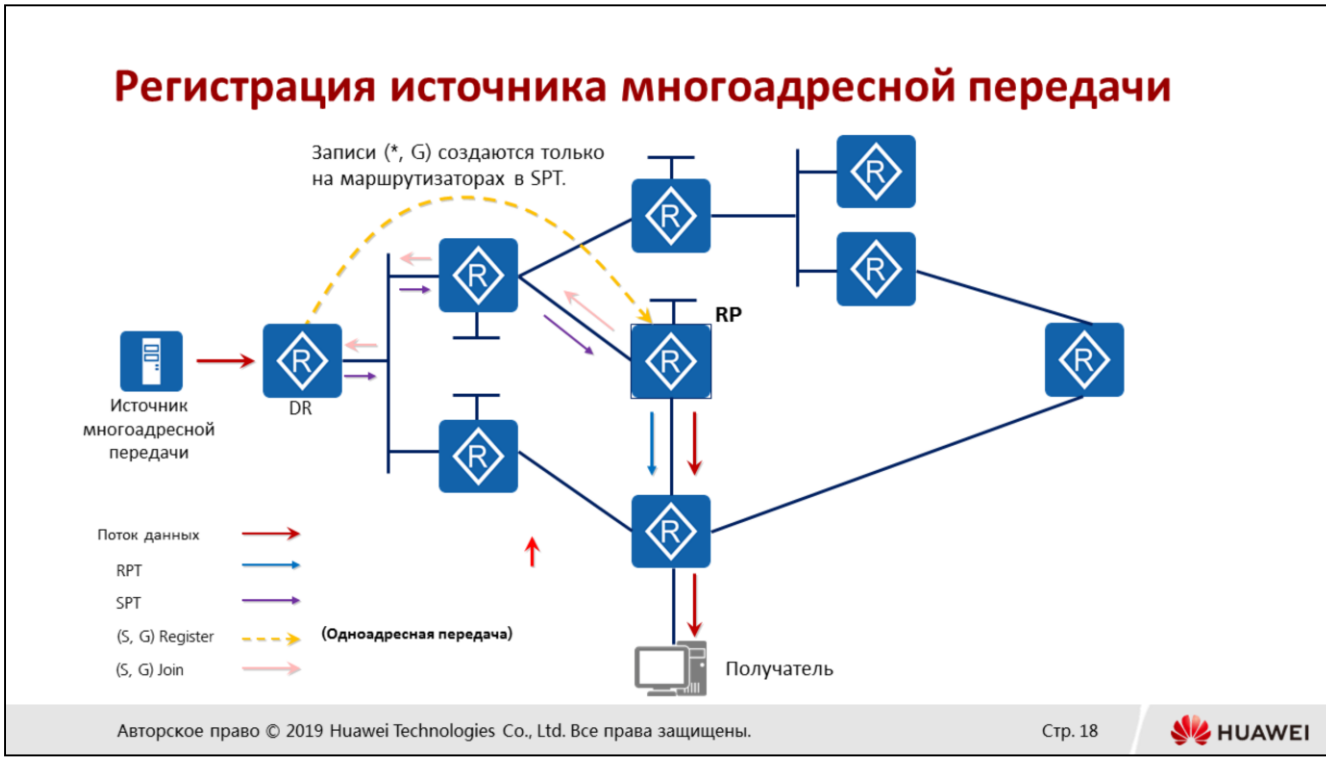
- Как получить адрес RP из адреса многоадресной передачи?
  - Извлеките поле Plen и преобразуйте его в десятичное число.
  - Извлеките первые 8 бит поля Network Prefix, которые являются префиксом адреса RP.
  - Извлеките поле RIID в качестве последних 4 битов идентификатора интерфейса адреса RP и укажите нули в других частях идентификатора интерфейса.
- Пример встроенного адреса RP
  - Если адрес многоадресной передачи имеет значение FF70:140:2001:DB8:BEEF:FEED::/96, то адрес RP, полученный из адреса многоадресной передачи будет равен 2001:DB8:BEEF:FEED::1/64.

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI



- Когда хост получателя присоединяется к многоадресной группе G, он отправляет сообщение MLD на конечный маршрутизатор, напрямую подключенный к хосту. Конечный маршрутизатор хранит информацию о получателе группы многоадресной рассылки G и последовательно, от узла к узлу, отправляет сообщение Report через восходящие узлы на RP.
- Каждый маршрутизатор, через который проходит сообщение от конечного маршрутизатора до RP, создает (*, G) записи в таблице пересылки. Эти маршрутизаторы составляют ветвь RPT. Запись (*, G) представляет информацию от любого источника до многоадресной группы G. Дерево RPT использует точку RP и получателя в качестве корневого узла и конечного узла соответственно.
- Когда пакеты от источника S до группы G проходят через RP, то, прежде чем поступить на хост получателя, пакеты поступают на конечный маршрутизатор по установленному дереву RPT.
- Когда получателю больше не интересна информация из группы многоадресной рассылки G, маршрутизатор многоадресной рассылки, непосредственно подключенный к получателю, последовательно, от узла к узлу, отправляет сообщение Prune точке RP группы в направлении, обратном дереву RPT. После получения сообщения первый вышестоящий маршрутизатор удаляет интерфейс, подключенный к нисходящему маршрутизатору, из своего списка интерфейсов и проверяет, есть ли в нем получатель многоадресной рассылки. Если нет, вышестоящий маршрутизатор пересылает сообщение Prune своему вышестоящему маршрутизатору.

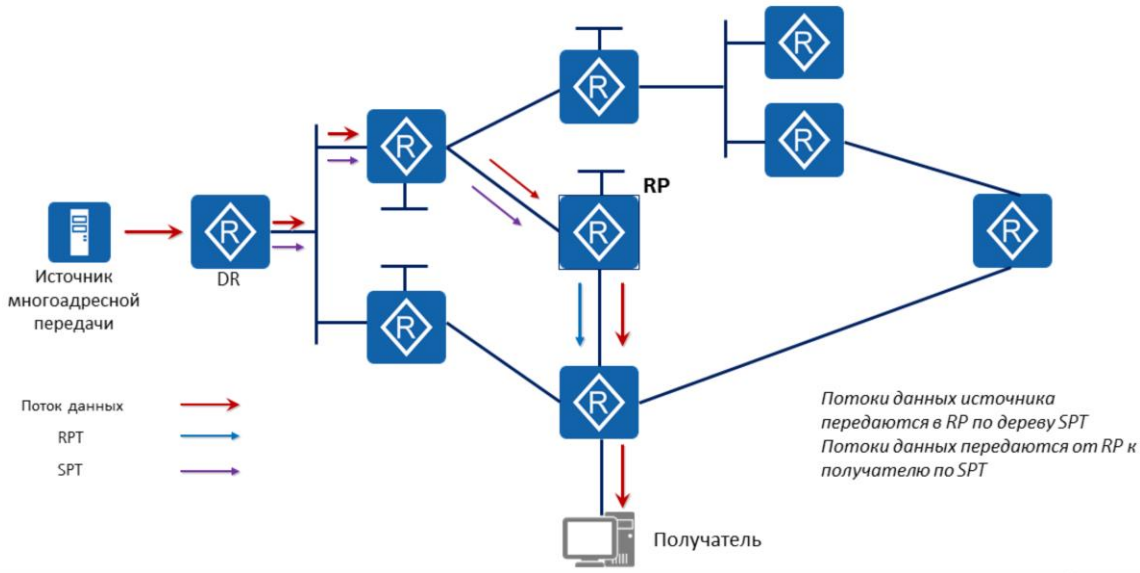


- Если источник многоадресной передачи S отправляет пакет многоадресной передачи группе G, маршрутизатор, непосредственно подключенный к S, инкапсулирует пакет в сообщение Register PIM IPv6 после получения пакета и передает сообщение точке RP в режиме одноадресной передачи.
- После получения сообщения Register от источника S, RP декапсулирует сообщение Register и передает информацию многоадресной передачи получателю по RPT. Кроме того, точка RP последовательно, от узла к узлу, передает сообщение Join (S, G) источнику S многоадресной передачи, так что все маршрутизаторы между RP и источником S генерируют записи (S, G). Маршрутизаторы внутри пути образуют ветвь дерева SPT. Дерево SPT использует источник многоадресной передачи S и RP в качестве корневого узла и пункта назначения соответственно.



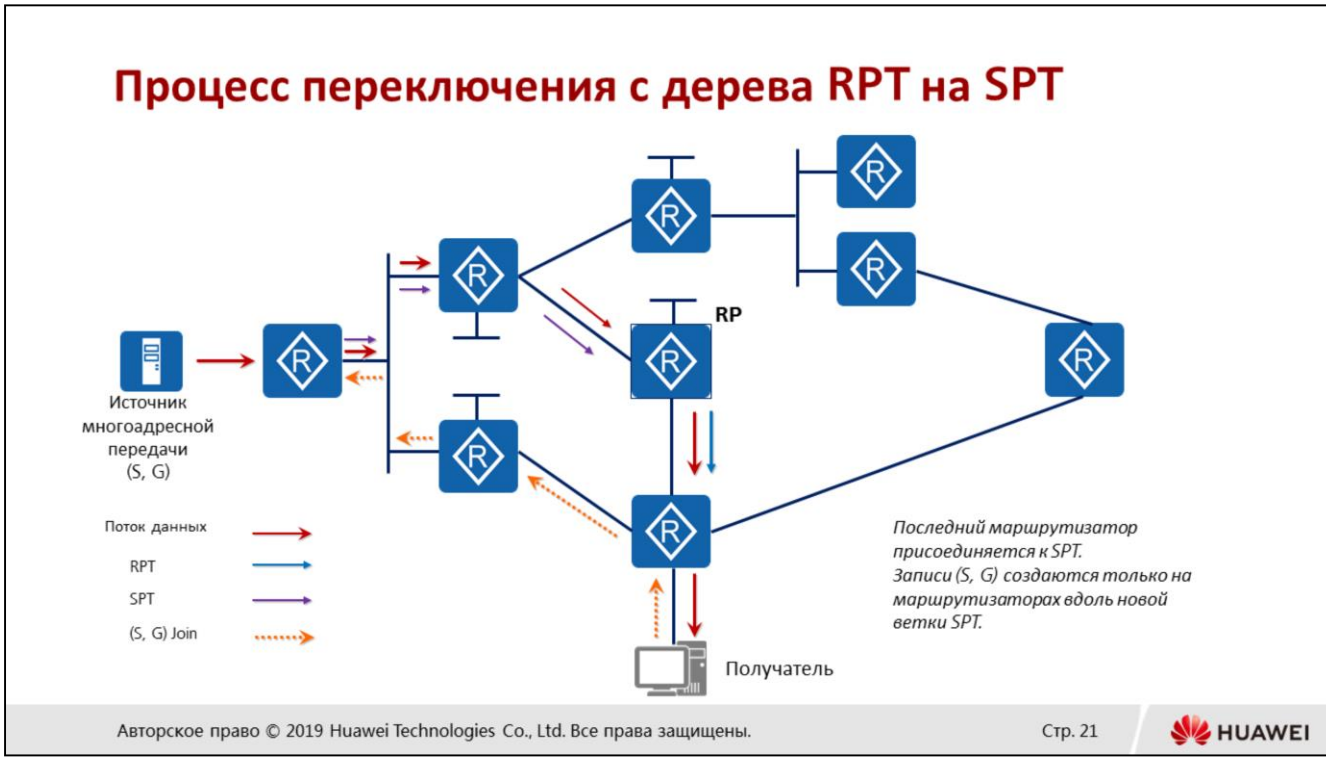
- Информация многоадресной передачи, отправленная источником S, поступает на точку RP по настроенному дереву SPT, после чего RP пересылает информацию по дереву RPT. После получения информации многоадресной рассылки, передаваемой по SPT, точка RP в режиме одноадресной передачи передает сообщение Register-Stop маршрутизатору, который напрямую подключен к источнику многоадресной передачи S. На этот момент регистрация источника многоадресной передачи считается выполненной.

Процесс переадресации многоадресного трафика



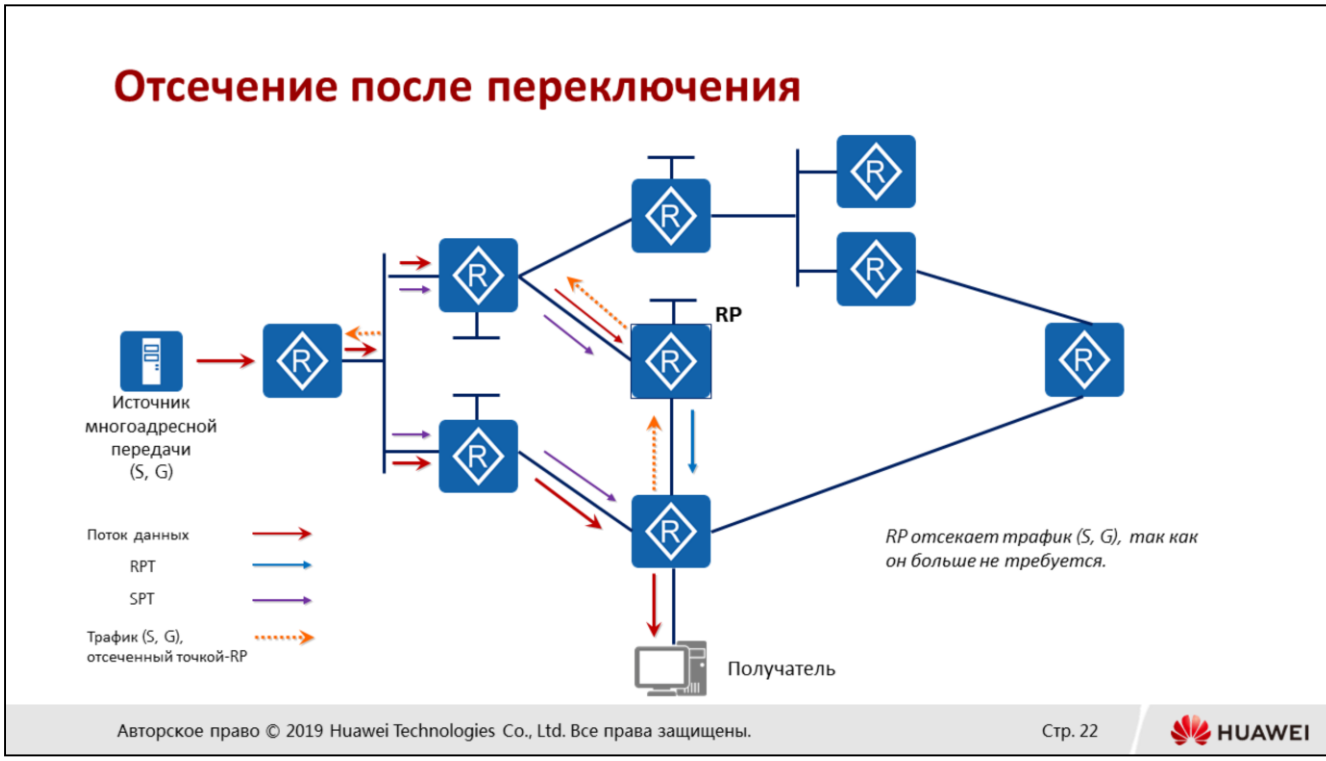
Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Потоки данных источника передаются в точку RP по дереву SPT, затем точка RP передает их получателю по дереву RPT.



- PIM-SM указывает пороговое значение для скорости передачи многоадресных пакетов из определенного источника и, тем самым, позволяет последнему маршрутизатору (DR-маршрутизатору на стороне получателя) переключаться с дерева RPT на дерево SPT. Когда последний маршрутизатор обнаруживает, что скорость передачи многоадресных пакетов от RP в группу многоадресной передачи G превышает пороговое значение, он отправляет сообщение Join (S, G) следующему маршрутизатору источника S на основе таблицы одноадресной маршрутизации. Сообщение Join последовательно, через каждый узел, доходит до первого маршрутизатора. Когда все маршрутизаторы в пути формируют запись (S, G), создается ветка дерева SPT.
- DR-маршрутизатор на стороне получателя периодически проверяет скорость передачи многоадресных пакетов. Если DR-маршрутизатор обнаруживает, что скорость многоадресных пакетов, отправленных RP в группу G, превышает пороговое значение, он инициирует переключение на дерево SPT.
    - DR-маршрутизатор на стороне получателя отправляет сообщение Join (S, G) DR-маршрутизатору на стороне источника и создает запись (S, G). Сообщение Join передается от узла к узлу, и все маршрутизаторы вдоль пути создают соответствующую запись (S, G). В итоге создается дерево SPT от DR-маршрутизатора на стороне источника до DR-маршрутизатора на стороне получателя.
    - Дерево SPT создано, и DR-маршрутизатор на стороне получателя отправляет сообщение Prune на RP. Сообщение Prune передается от узла к узлу по дереву RPT. После получения сообщения Prune маршрутизаторы в RPT преобразуют запись (*, G) в запись (S, G) и отсекают свои нисходящие интерфейсы. После завершения действия Prune, RP прекращает пересылку многоадресных пакетов по дереву RPT.
    - Поскольку дерево SPT не проходит через точку RP, точка RP продолжает отправлять сообщения Prune по дереву RPT DR-маршрутизатору на стороне источника, который затем удаляет нисходящий интерфейс, подключенный к RP, из записи (S, G). После завершения действия Prune, DR-маршрутизатор на стороне источника прекращает пересылку многоадресных пакетов по дереву SPT в RP.
- В соответствии с конфигурацией VRP по умолчанию, маршрутизаторы, подключенные к получателям, присоединяются к дереву SPT сразу после получения первого пакета данных

многоадресной передачи от источника многоадресной передачи, выполняя переключение с дерева RPT на дерево SPT.



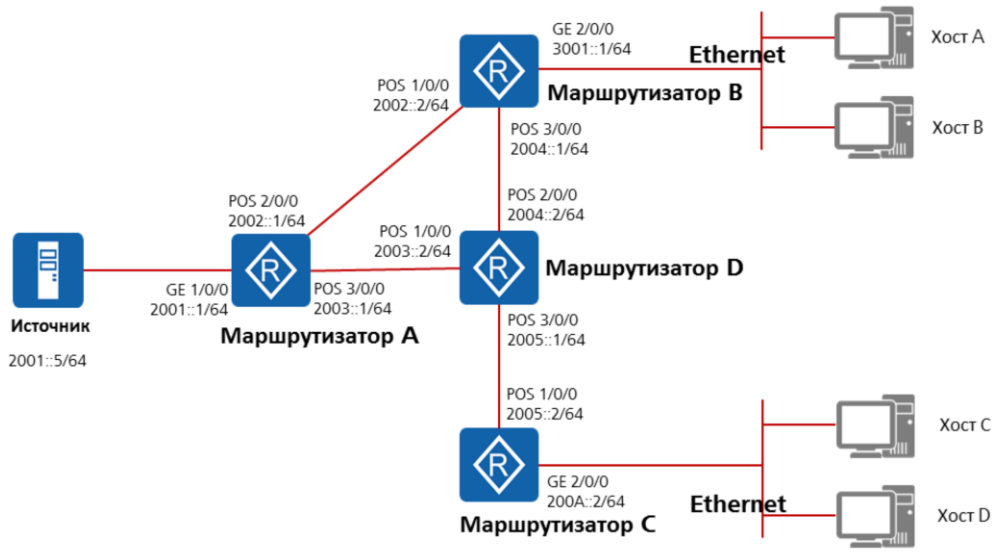
- Когда маршрутизатор получает одни и те же данные многоадресной передачи по деревьям RPT и SPT на разных интерфейсах, он отбрасывает данные, полученные по дереву RPT, и последовательно, от узла к узлу, отправляет сообщение Prune на RP. После получения сообщения Prune RP обновляет статус переадресации и прекращает переадресацию многоадресного трафика (S, G) по дереву RPT. RP также отправляет сообщение Prune источнику многоадресной рассылки, чтобы удалить или обновить запись (S, G). Таким образом происходит переключение передачи многоадресных данных с дерева RPT на дерево SPT.

Содержание

- Механизм IPv6 PIM-SM
- **Конфигурация IPv6 PIM-SM**
- Основные принципы IPv6 PIM-SSM
- Управление многоадресным маршрутом
- Типичные области применения многоадресной передачи IPv6

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

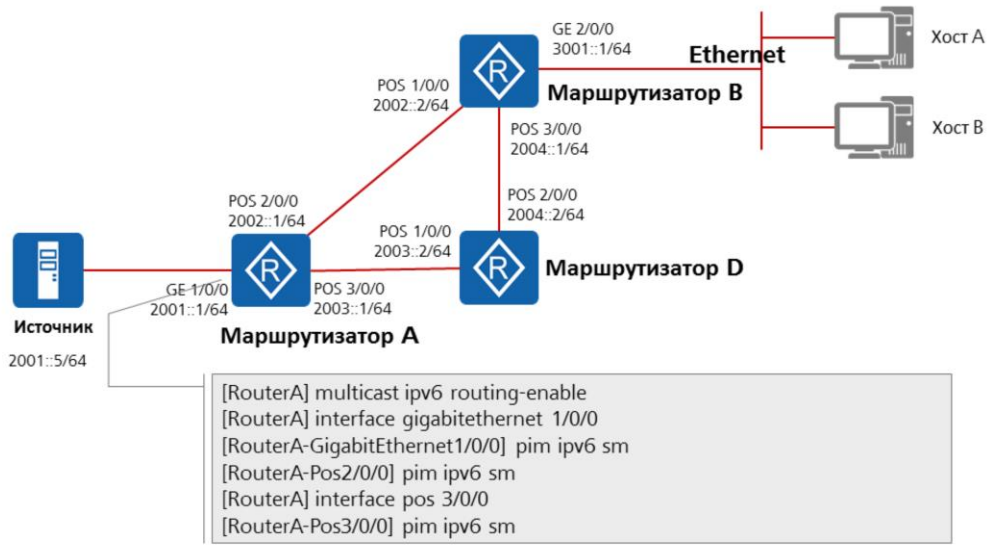
Пример настройки IPv6 PIM-SM



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Хост A и хост C являются получателями многоадресной рассылки в двух конечных (leaf) сетях. Эти получатели подключаются к источнику многоадресной рассылки через Маршрутизатор A, Маршрутизатор B, Маршрутизатор C и Маршрутизатор D.
- Порядок конфигурации:
  - Настрйте IPv6-адрес для каждого интерфейса и протокол одноадресной маршрутизации IPv6.
    - Настройте IPv6-адрес и маску для каждого интерфейса маршрутизатора.
    - Настройте OSPFv3 на каждом маршрутизаторе и установите для идентификатора процесса значение 1, а для идентификатора области – 0, чтобы Маршрутизатор A, Маршрутизатор B, Маршрутизатор C и Маршрутизатор D могли обмениваться данными на уровне сети.
  - Включите многоадресную передачу IPv6 на каждом маршрутизаторе, включите IPv6 PIM-SM на каждом интерфейсе маршрутизатора и настройте MLD на интерфейсах, подключенных к хостам (по умолчанию используется версия 2).
  - Настойте C-BSR и C-RP (в данном примере глобальные одиночные адреса IPv6 для C-BSR и C-RP оба имеют значение 2004::2 на Маршрутизаторе D).
  - Проверьте конфигурацию.

Конфигурация маршрутизатора A

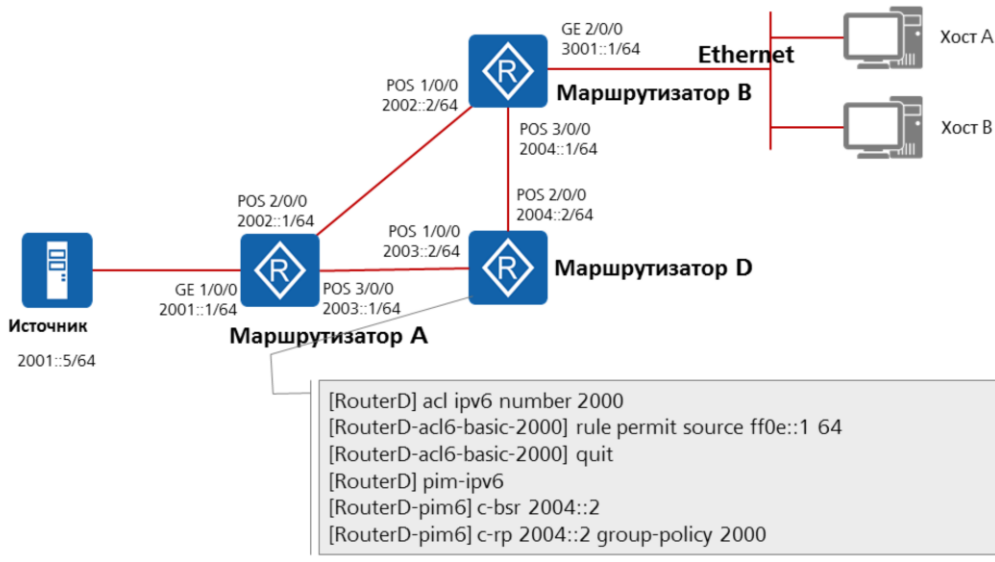


Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Войдите в режим системы.
  - **system-view**
- Включите многоадресную маршрутизацию IPv6.
  - **multicast ipv6 routing-enable**
- Войдите в режим интерфейса.
  - **interface** *interface-type interface-number*
- Включите IPv6 PIM-SM.
  - **pim ipv6 sm**
- Протокол IPv6 PIM-SM можно настроить только после включения многоадресной рассылки IPv6. После настройки IPv6 PIM-SM на интерфейсе маршрутизатор начинает периодически отправлять сообщения Hello для обнаружения соседних узлов PIM IPv6 и обработки сообщений от соседних узлов. Когда маршрутизатор присоединяется к домену IPv6 PIM-SM, рекомендуется включить IPv6 PIM-SM на всех интерфейсах маршрутизатора, не являющегося пограничным.
- IPv6 PIM-SM и IPv6 PIM-DM не могут быть включены на интерфейсе одновременно. Режимы PIM IPv6 всех интерфейсов на маршрутизаторе должны быть одинаковыми.
- Конфигурации Маршрутизатора B, Маршрутизатора C и Маршрутизатора D аналогичны конфигурации Маршрутизатора A.
- На маршрутизаторе, подключенном к получателям, необходимо включить MLD.

Конфигурация маршрутизатора D



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- В домене PIM можно настроить один или несколько C-BSR. BSR, выбранный из C-BSR, собирает и анонсирует информацию C-RP. BSR и другие устройства в домене обмениваются большим количеством информации, и поэтому между C-BSR и другими устройствами в домене должна быть зарезервирована полоса пропускания достаточного объема. Маршрутизаторы в магистральной сети используются в качестве C-BSR.
- Когда вы указываете адрес интерфейса в качестве адреса C-BSR, вы должны включить IPv6 PIM-SM на интерфейсе. Процесс выбора BSR из C-BSR:
  - Сначала каждый C-BSR рассматривает себя как BSR в домене PIM-SM и использует свой IPv6-адрес интерфейса в качестве адреса BSR для отправки сообщений bootstrap.
  - Когда C-BSR получает сообщение bootstrap от другого маршрутизатора, он сравнивает адрес BSR в сообщении с собственным адресом BSR. Сравниваются приоритеты и адреса BSR. Если приоритеты совпадают, то C-BSR с большим адресом BSR является предпочтительным. То есть, если C-BSR устанавливает, что адрес BSR, одержащийся в сообщении bootstrap больше, чем его собственный адрес BSR, C-BSR заменит собственный адрес BSR адресом BSR из сообщения и больше не будет рассматривать себя в качестве BSR. Если же C-BSR определяет, что адрес BSR, содержащийся в полученном сообщении bootstrap, не больше его адреса BSR, то C-BSR продолжает рассматривать себя в качестве BSR.
- Войдите в режим PIM IPv6.
  - **pim-ipv6**
- Настройте адрес интерфейса в качестве адреса C-BSR.
  - **c-bsr** ipv6-address [hash-length] [priority-value]
- Настройте C-RP.
  - **c-rp** *ipv6-address* [**priority** *priority*]
- Настройте статическую точку RP.

    - **static-rp** *rp-address* [*basic-acl6-number*] [**preferred**]
- Настройте встроенный адрес RP.
    - **embedded-rp [** *basic-acl6-number* **]**

- Команда **c-bsr** позволяет настроить адрес интерфейса в качестве адреса C-BSR на маршрутизаторе, который хочет стать BSR.
  - *ipv6-address*: определяет глобальный одиночный адрес IPv6 для C-BSR.
  - *hash-length*: определяет длину маски хеш-функции для расчета RP. Значение является целым числом в диапазоне от 0 до 128.
- Команда **pim ipv6 bsr-boundary** позволяет настроить интерфейс в качестве границы BSR. После запуска данной команды на интерфейсе сообщения bootstrap не смогут проходить через данный интерфейс, однако другие пакеты PIM смогут.
- Команда **c-rp** позволяет настроить маршрутизатор, чтобы он уведомлял BSR о том, что он является C-RP. Между маршрутизатором, настроенным в качестве C-RP, и другими устройствами необходимо зарезервировать большую полосу пропускания.
  - *ipv6-address*: определяет глобальный одиночный адрес IPv6 для C-RP.
  - Если в сети имеется только один динамический RP, то настройка статической точки RP позволит предотвратить прерывания связи, вызванные единичным отказом RP. Если для пересылки многоадресных данных используется статическая точка RP, то на всех маршрутизаторах в домене IPv6 PIM-SM необходимо настроить одну команду **static-rp**.

- Команда **static-rp** позволяет настроить статическую точку RP.
  - *rp-address*: определяет адрес статической RP. Этот адрес должен быть действительным глобальным одиночным IPv6-адресом.
  - *basic-acl6-number*: определяет количество базовых списков ACL для управления диапазоном многоадресных групп, которые обслуживает статическая RP. Диапазон значений от 2000 до 2999.
  - **preferred**: отдает предпочтение настроенной статической точке RP, если данная RP отличается от RP, выбранной механизмом BSR. Если данный параметр не определен, то RP, выбранная механизмом BSR, является предпочтительной.
- Чтобы заменить статическую или динамическую точку RP, выбранную с помощью механизма BSR, маршрутизатор использует механизм embedded RP, чтобы получить адрес RP из группового адреса. Диапазон групповых адресов в сценарии embedded RP – от FF7*x*::/16 до FFF*x*::/16, где *x* означает любое шестнадцатеричное число в диапазоне от 0 до F.

Отображение конфигураций PIM и информации о выборе BSR на интерфейсах

```
[RouterB] display pim ipv6 interface
Vpn-instance: public net
Interface    NbrCnt HelloInt  DR-Pri     DR-Address
Pos1/0/0     1      30        1          FE80::A01:10E:1(local)
GEth2/0/0    0      30        1          FE80::200:AFF:FE01:10E(local)
Pos3/0/0     1      30        1          FE80::9D62:0:FDC5:2
```

```
[RouterB] display pim ipv6 bsr-info
  Vpn-instance: public net
    Elected BSR Address: 2004::2
      Priority: 0
      Hash mask length: 126
      State: Accept Preferred
      Uptime: 00:04:22
      Expires: 00:01:46
```

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Отображение информации PIM IPv6 на интерфейсах.
  - **display pim ipv6 interface** [*interface-type interface-number*]
- Отображение информации о BSR в домене IPv6 PIM-SM.
  - **display pim ipv6 bsr-info**
  - BSR в сети – POS 2/0/0 маршрутизатора D.

Отображение информации RP

```
[RouterB] display pim ipv6 rp-info
  Vpn-instance: public net
   PIM-SM BSR RP information:
   Group/MaskLen: FF0E::1/64
     RP: 2004::2
     Priority: 0
     Uptime: 00:05:19
     Expires: 00:02:11
```

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Отображение информации RP в домене IPv6 PIM-SM.
  - **display pim ipv6 rp-info** [ipv6-group-address]
- RP в сети – это POS 2/0/0 маршрутизатора D.

Отображение информации многоадресной маршрутизации IPv6 - DR на стороне источника

```
[RouterA] display pim ipv6 routing-table
Vpn-instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry
 (2001::5, FF0E::1)
    RP: 2004::2
    Protocol: pim-sm, Flag: SPT LOC ACT
    UpTime: 00:02:15
    Upstream interface: GigabitEthernet1/0/0
       Upstream neighbor: FE80::200:AFF:FE01:10D
       RPF prime neighbor: FE80::200:AFF:FE01:10D
    Downstream interface(s) information:
    Total number of downstreams: 3
       1: Registration
          Protocol: pim-sm, UpTime: 00:02:15, Expires:  -
       2: Pos2/0/0
          Protocol: pim-sm, UpTime: 00:02:15, Expires: 00:03:15
       3: Pos3/0/0
          Protocol: pim-sm, UpTime: 00:02:15, Expires: 00:03:15
```

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Предположим, что хост A присоединяется к группе многоадресной рассылки G (FF0E :: 1). Между маршрутизатором D и маршрутизатором B создается дерево RPT, и на маршрутизаторе D и маршрутизаторе B в RPT генерируется запись (*, G). После того, как источник многоадресной передачи S (2001 :: 5) отправляет пакет группе многоадресной рассылки G, маршрутизатор A и маршрутизатор D в SPT генерируют запись (S, G).

Отображение информации многоадресной маршрутизации IPv6 - RP

```
[RouterD] display pim ipv6 routing-table
Vpn-instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, FF0E::1)
    RP: 2004::2 (local)
    Protocol: pim-sm, Flag: WC
    UpTime: 00:16:56
    Upstream interface: Register
       Upstream neighbor: NULL
       RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 2
       1: Pos2/0/0
          Protocol: pim-sm, UpTime: 00:16:56, Expires: 00:02:34
       2: Pos3/0/0
          Protocol: pim-sm, UpTime: 00:07:56, Expires: 00:02:35
```

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Отображение информации многоадресной маршрутизации IPv6 - RP (продолжение)

```
3.13.5 FF0E                1
  RP: 2004::2 (local)
  Protocol: pim-sm, Flag: SWT ACT
  UpTime: 00:02:54
  Upstream interface: Register
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 2
    1: Pos2/0/0
      Protocol: pim-sm, UpTime: 00:02:54, Expires:  -
    2: Pos3/0/0
      Protocol: pim-sm, UpTime: 00:02:54, Expires: 00:02:36
```

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.



Содержание

- Механизм PIM-SM
- Конфигурация IPv6 PIM-SM
- **Основные принципы работы IPv6 PIM-SSM**
- Управление многоадресным маршрутом
- Типичные области применения многоадресной передачи IPv6

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

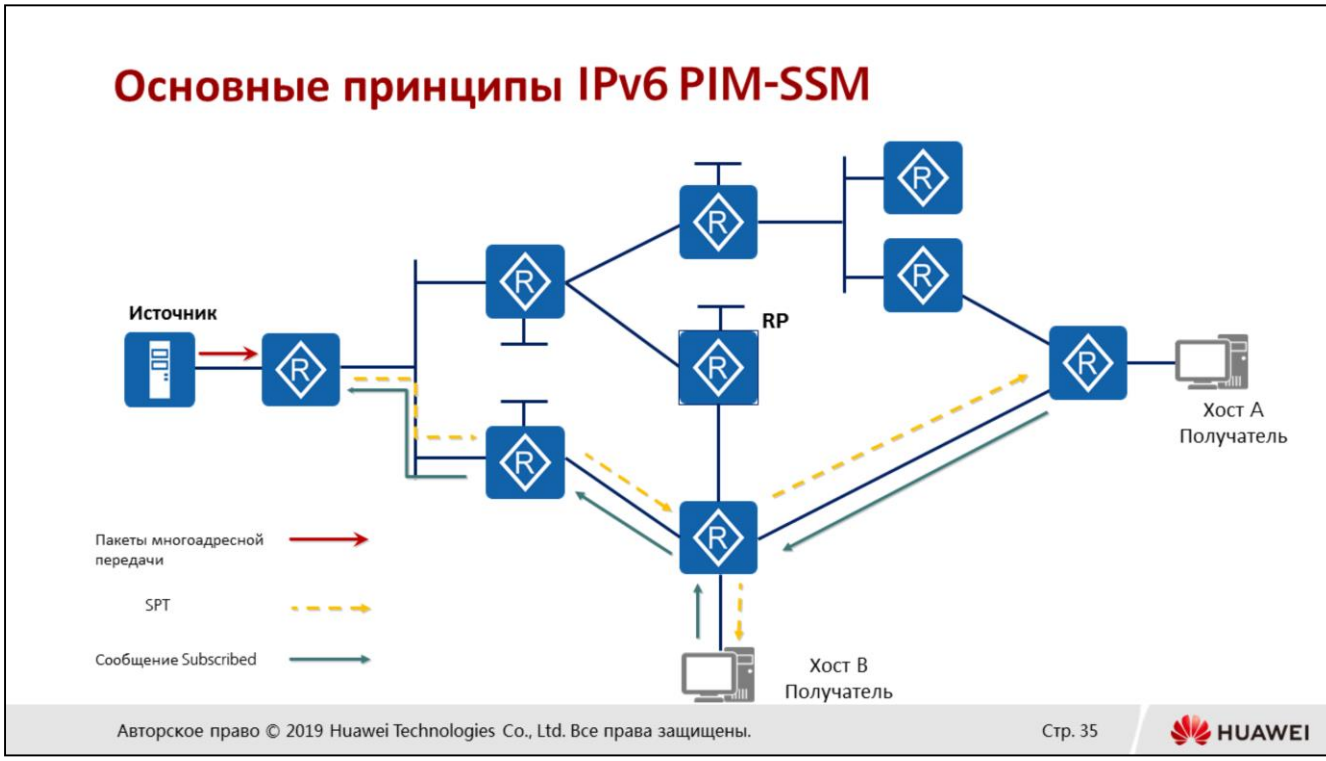
Обзор протокола IPv6 PIM-SSM

- Модель SSM – это многоадресная рассылка с настройкой источника, для реализации которой используется протокол MLDv2 и некоторые механизмы IPv6 PIM-SM. Последний маршрутизатор уже знает адрес источника многоадресной рассылки благодаря протоколу MLDv2. Таким образом, маршрутизатор может инициировать процесс присоединения к группе, чтобы создать дерево SPT от источника многоадресной рассылки до получателей в сети SSM.
  - Определяется специальный адрес многоадресной рассылки FF3x::/32, и проблемы с обнаружением источника не возникают.
  - Протокол IPv6 PIM-SSM должен взаимодействовать с протоколом MLDv2.
  - По сравнению с PIM-SM, PIM-SSM не включает в себя такие сложные механизмы, как RP, BSR, генерация RPT и регистрация источника.
  - Для создания междоменной многоадресной рассылки создается дерево SPT создается на основе одноадресного маршрута источника многоадресной рассылки.

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

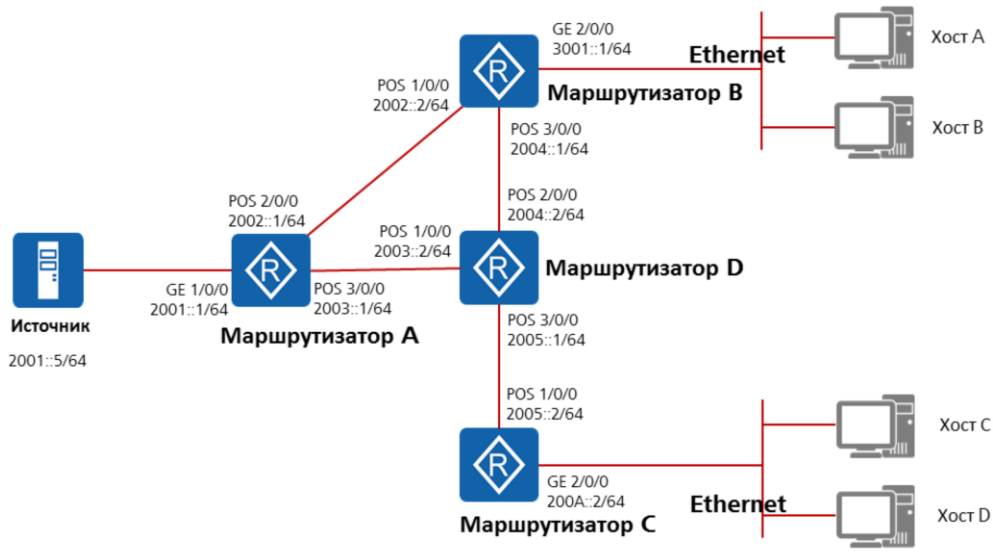
HUAWEI

- Протокол IPv6 PIM-SSM включает функции обнаружения соседнего узла, выбора DR-маршрутизатора и создания дерева SPT.
  - По аналогии с IPv6 PIM-SM, IPv6 PIM-SSM выполняет обнаружение соседнего узла и выбор DR с помощью сообщений Hello, передаваемых между маршрутизаторами.
  - PIM-SSM также использует механизм PIM-SM. Последний маршрутизатор определяет, какое дерево создавать – RPT или SPT – в зависимости от того, находится ли групповой адрес в диапазоне адресов группы SSM.



- В модели SSM канал определен как (S, G), а сообщение Subscribed используется как сообщение Join.
- Если пользователю A и пользователю B нужно получить информацию от источника многоадресной рассылки S, они отправляют сообщение Report с пометкой (include S, G) на ближайший генератор запросов через MLDv2. Если пользователю A и пользователю B не нужно получать информацию от источника многоадресной рассылки S, они отправляют сообщение Report с пометкой (exclude S, G) или другими источниками многоадресной передачи. Источник многоадресной рассылки S определен для получателей независимо от того, какое сообщение Report используется.
- После получения сообщения Report генератор запросов проверяет, находится ли групповой адрес, содержащийся в сообщении, в диапазоне адресов группы SSM. Если да, то маршрутизатор создает дерево многоадресной рассылки на основании модели SSM, а затем последовательно, от узла к узлу, отправляет сообщение Subscribed (также называемое сообщением Join) на определенный источник. Все маршрутизаторы в пути создают записи (S, G), тем самым создавая дерево SPT с источником S в качестве корня и получателей в качестве конечных узлов. В модели SSM дерево SPT используется в качестве пути передачи данных.
- Если генератор запросов обнаруживает, что адрес многоадресной рассылки выходит за пределы диапазона адресов группы SSM, он создает дерево многоадресной рассылки на основе протокола IPv6 PIM-SM.

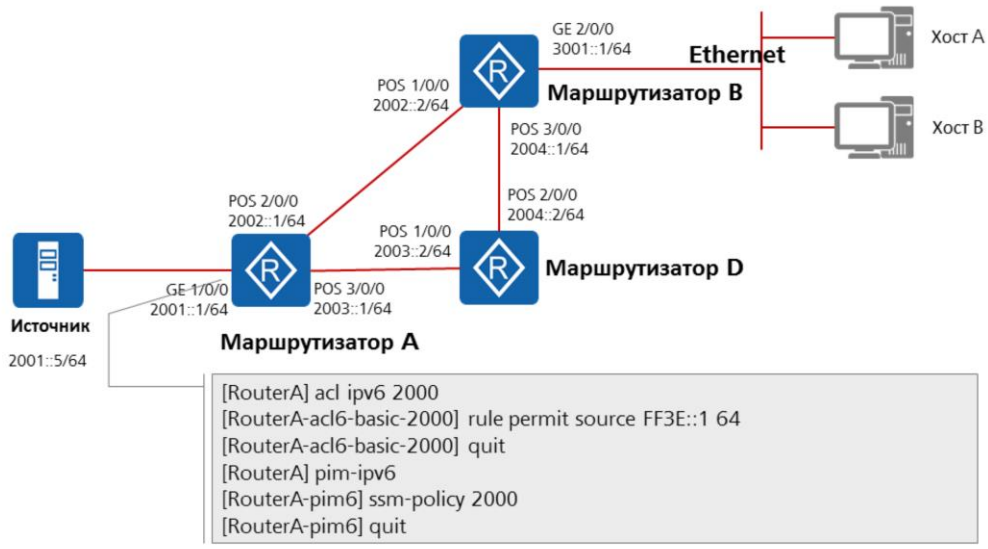
Пример конфигурации IPv6 PIM-SSM



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Хост A и хост C являются получателями многоадресной рассылки в двух конечных сетях. Эти получатели подключаются к многоадресному источнику через маршрутизатор A, маршрутизатор B, маршрутизатор C и маршрутизатор D.
- Протокол MLDv2 должен работать на интерфейсах, подключенных к хостам между маршрутизатором B и N1 и между маршрутизатором C и N2.
- Порядок конфигурации:
  - Настройте IPv6-адрес для каждого интерфейса маршрутизатора и протокол одноадресной маршрутизации IPv6.
    - Настройте IPv6-адрес и маску для каждого интерфейса маршрутизатора.
    - Настройте OSPFv3 на каждом маршрутизаторе и установите для идентификатора процесса значение 1, а для иднетификатора области – значение 0, чтобы гарантировать, что маршрутизатор A, маршрутизатор B, маршрутизатор C и маршрутизатор D смогут обмениваться данными на сетевом уровне.
  - Включите многоадресную маршрутизацию IPv6 на каждом маршрутизаторе и IPv6 PIM-SM на каждом интерфейсе маршрутизатора.
  - Настройте диапазон адресов многоадресной рассылки IPv6 PIM-SSM на каждом маршрутизаторе.
  - Настройте MLDv2 на интерфейсах, соединяющих маршрутизаторы и хосты.
  - Проверьте конфигурацию.

Конфигурация маршрутизатора A



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- На маршрутизаторе A установите значение FF3E::1 для диапазона групповых адресов IPv6 PIM-SSM.
- Настройки маршрутизатора B, маршрутизатора C и маршрутизатора D аналогичны настройкам маршрутизатора A.
- В модели SSM используется протокол IPv6 PIM-SM. На всех маршрутизаторах в сети необходимо включить IPv6 PIM-SM. Сконфигурируйте диапазон адресов группы SSM. По умолчанию используется диапазон адресов группы SSM, определенный IANA.
- Если вы хотите получить информацию из указанного источника S или из других источников, необходимо отправить сообщение MLDv2 Report, содержащее информацию канала (S, G). После получения сообщения DR-маршрутизатор на стороне получателя проверяет, находится ли групповой адрес G, содержащийся в сообщении, в диапазоне адресов группы SSM. Если да, то DR-маршрутизатор отправляет сообщение Join многоадресному источнику S и создает запись (S, G) на кадом маршрутизаторе в пути, чтобы создать дерево SPT. Модель SSM настроена. Если групповой адрес G не принадлежит диапазону адресов группы SSM или адрес источника S не указан явно, DR-маршрутизатор запускает процедуру настройки модели ASM на базе IPv6 PIM-SM.
- Модель SSM реализована с помощью протокола IPv6 PIM-SM. Маршрутизаторы с активированным протоколом IPv6 PIM-SM могут работать с рассылкой SSM. Маршрутизатор периодически отправляет сообщение Hello для обнаружения соседних узлов PIM IPv6 и обработки сообщений от соседних узлов. Когда маршрутизатор присоединяется к домену IPv6 PIM-SSM, рекомендуется включить IPv6 PIM-SSM на всех интерфейсах маршрутизатора, не являющегося пограничным маршрутизатором.
- Передача информации источника многоадресной рассылки получателям в режиме IPv6 PIM-SSM или IPv6 PIM-SM зависит от того, находится ли групповой адрес канала (S, G) в пределах диапазона адресов группы SSM. В режиме IPv6 PIM-SSM информация об адресе группы очень важна.
- Если диапазон адресов группы SSM не определен, система использует сегмент сети FF3x::/12, зарезервированный IANA для SSM в качестве диапазона адресов по умолчанию.
- Войдите в режим системы.
  - **system-view**
- Включите многоадресную маршрутизацию IPv6.
  - **multicast ipv6 routing-enable**
- Войдите в режим интерфейса.
  - **interface** *interface-type interface-number*
- Включите IPv6 PIM-SSM.
  - **pim ipv6 sm**
- Войдите в режим PIM IPv6.

    - **pim-ipv6**
- Настройте диапазон адресов группы IPv6 PIM-SSM.
    - **ssm-policy** *basic-acl6-number*

Отображение информации многоадресной маршрутизации IPv6

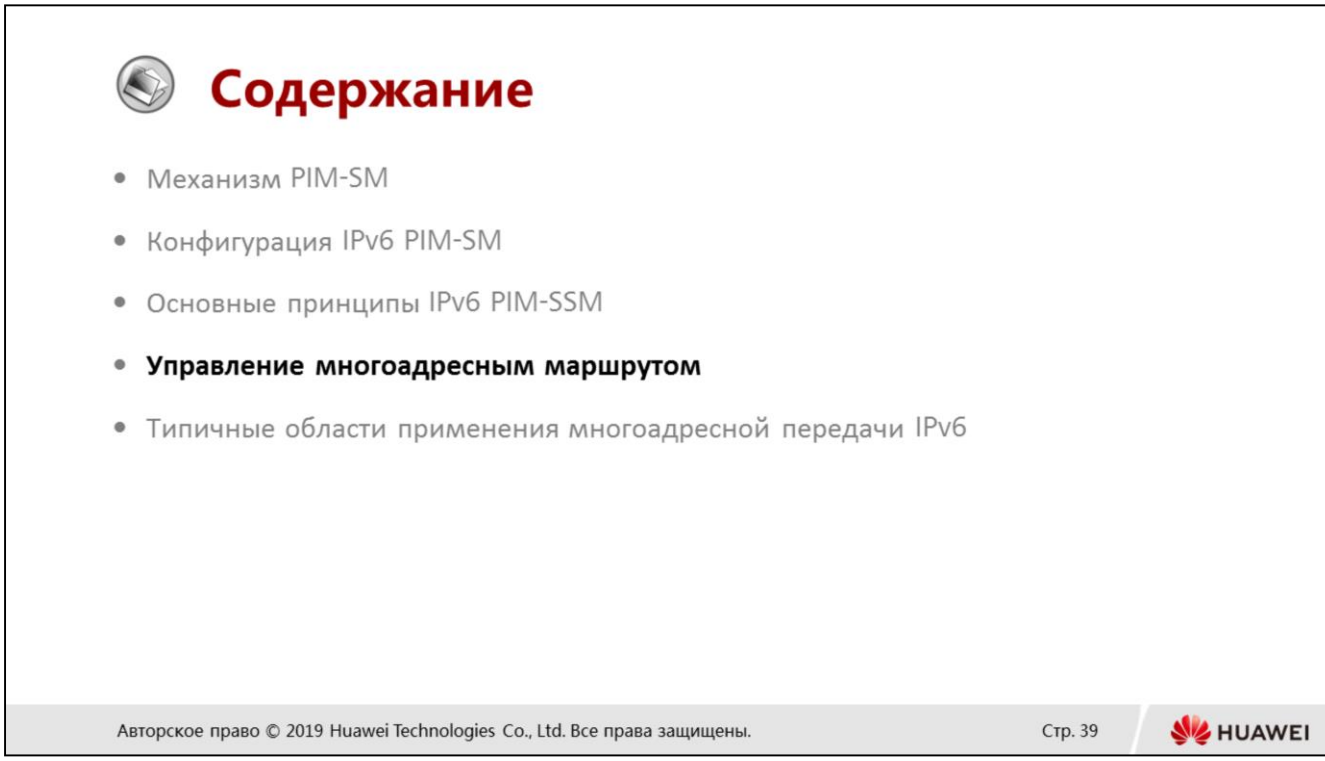
```
[RouterA] display pim ipv6 routing-table
Vpn-instance: public net
Total 1 (S, G) entry

 (2001::5, FF3E::1)
     Protocol: pim-ssm, Flag: LOC
    UpTime: 00:00:11
    Upstream interface: GigabitEthernet1/0/0
        Upstream neighbor: FE80::200:AFF:FE01:10D
        RPF prime neighbor: FE80::200:AFF:FE01:10D
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Pos2/0/0
            Protocol: pim-ssm, UpTime: 00:00:11, Expires: 00:03:19
```

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Если хосту A нужно получить информацию от многоадресного источника S (2001::5) в группе G (FF3E::1), маршрутизатор B настраивает дерево SPT к источнику. Маршрутизатор A и маршрутизатор B в дереве SPT генерируют запись (S, G). На маршрутизаторе D за пределами SPT запись (S, G) отсутствует.



- Управление многоадресными маршрутами – это управление пересылкой многоадресных пакетов за счет создания или изменения многоадресных маршрутов, а также проверки и обслуживания маршрутов многоадресной пересылки.

Управление многоадресным маршрутом (IPv6)

- В таблице описаны функции управления многоадресными маршрутами, которые позволяют создавать и поддерживать пути многоадресной переадресации.

Функция	Описание
Проверка RPF	Гарантирует, что данные многоадресной рассылки передаются по правильным маршрутам.
Распределение многоадресной нагрузки	Распределяет данные многоадресной рассылки по нескольким маршрутам с одинаковой стоимостью, чтобы снизить нагрузку на отдельные пути.

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Управление многоадресными маршрутами обеспечивает эффективную пересылку пакетов многоадресной рассылки по корректным маршрутам. При многоадресной маршрутизации и пересылке каждый протокол многоадресной маршрутизации создает и поддерживает собственную таблицу маршрутизации. Информация о маршрутизации из этих таблиц используется для создания общей таблицы многоадресной маршрутизации. Маршрутизаторы используют эту общую таблицу для выбора оптимальных маршрутов в соответствии с политиками многоадресной маршрутизации и пересылки. Информация об оптимальном маршруте затем доставляется в базу данных MFIB, которая управляет пересылкой многоадресных данных.
- Базы данных MFIB сетевых устройств поддерживают дерево многоадресной пересылки для всей сети, в котором источник многоадресной рассылки является корнем, а членами группы являются конечными устройствами. Управление осуществляется с помощью ряда функций для создания и поддержания маршрутов многоадресной пересылки.

Таблица маршрутизации протокола многоадресной маршрутизации IPv6

- Протоколы многоадресной маршрутизации поддерживают собственные таблицы маршрутизации для управления многоадресными маршрутами. Пример таблицы маршрутизации PIM:

```
<HUAWEI> display pim ipv6 routing-table
VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry

(FC00::2, FF3E::1)
    Protocol: pim-sm, Flag: SPT LOC ACT
    UpTime: 00:04:24
    Upstream interface: Vlanif20
        Upstream neighbor: FE80::A01:100:1
        RPF prime neighbor: FE80::A01:100:1
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlanif10
            Protocol: pim-sm, UpTime: 00:04:24, Expires: 00:02:47
```

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- **(FC00::2, FF3E::1)**: запись (S, and G).
- **Protocol: pim-sm**: тип протокола. Первое поле Protocol в записи указывает на протокол, который генерирует запись, а второе поле – на протокол, который генерирует нисходящие интерфейсы.
- **Flag: SPT LOC ACT**: флаг записи маршрутизации PIM.
- **UpTime: 00:04:24**: первое поле UpTime в записи означает время существования записи, а второе поле – время существования нисходящего интерфейса.
- **Upstream interface: Vlanif20**: восходящий интерфейс.
- **Upstream neighbor: FE80::A01:100:1**: восходящий соседний узел. Значение NULL указывает на то, что восходящий соседний узел недоступен.
- **RPF prime neighbor: FE80::A01:100:1**: соседний узел RPF. Значение NULL указывает на то, что соседний узел RPF недоступен.
- **Downstream interface(s) information**: информация о нисходящем интерфейсе.
- **Total number of downstreams: 1**: количество нисходящих интерфейсов.
- **Expires: 00:02:47**: время старения нисходящего интерфейса.

Таблица маршрутизации многоадресной передачи IPv6

- Модуль управления многоадресными маршрутами на маршрутизаторе генерирует и поддерживает таблицу многоадресной маршрутизации. Если маршрутизатор поддерживает несколько многоадресных протоколов, то его таблица многоадресной маршрутизации будет содержать оптимальные маршруты, выбранные из таблиц маршрутизации этих протоколов.

```
<HUAWEI> display multicast ipv6 routing-table
IPv6 multicast routing table
 Total 1 entry

 00001. (FC00::2, FF3E::1)
      Uptime: 00:00:14
      Upstream Interface: Vlanif10
      List of 1 downstream interface
        1: Vlanif20
```

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- **00001. (FC00::2, FF3E::1)**: запись 00001 в формате (S, G).
- **Uptime: 00:00:14**: время обновления записи многоадресной маршрутизации.
- **Upstream Interface: Vlanif10**: восходящий интерфейс.
- **List of 1 downstream interface**: список нисходящих интерфейсов.

База данных MFIB

- Модуль управления маршрутизацией генерирует базу MFIB в соответствии с таблицей многоадресной маршрутизации. MFIB используется для пересылки данных. MFIB имеет те же функции, что и FIB в одноадресной передаче.

```
<HUAWEI> display multicast ipv6 forwarding-table
IPv6 Multicast Forwarding Table
Total 2 entries, 2 matched

00001. (FC00:1::3, FF1E::1)
    MID: 10, Flags: ACT
    Uptime: 02:54:43, Timeout in: 00:02:27
    Incoming interface: Vlanif10
    List of 1 outgoing interfaces:
      1: LoopBack0
        Activetime: 00:23:15
    Matched 0 packets(0 bytes), Wrong If 0 packets
    Forwarded 0 packets(0 bytes)
```

Данные многоадресной рассылки передаются в соответствии с MFIB. Каждая запись многоадресной пересылки содержит статистику о пакетах, которые пересылаются в соответствии с записью.

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

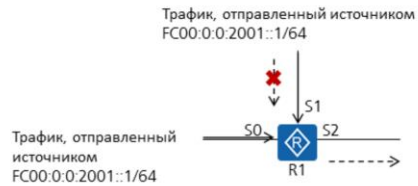
HUAWEI

- **00001. (FC00:1::3, FF1E::1)**: запись 00001 в формате (S, G).
- **MID: 10**: используется для быстрого поиска MFIB.
- **Flags: ACT**: флаг записи многоадресной пересылки.
- **UpTime: 02:54:43**: время существования записи многоадресной пересылки.
- **Timeout in: 00:03:26**: период ожидания записи многоадресной пересылки.
- **Incoming interface: Vlanif10**: входящий интерфейс записи.
- **List of 1 outgoing interfaces**: список исходящих интерфейсов записи.
- **Activetime: 00:23:15**: время существования исходящего интерфейса.
- **Matched 38264 packets(1071392 bytes)**: количество пакетов, соотвествующих записи.
- **Wrong If 0 packets**: количество пакетов из неправильного интерфейса.
- **Forwarded 38264 packets(1071392 bytes)**: количество переадресованных пакетов.

Проверка RPF

- Проверка RPF
  - Гарантирует передачу многоадресного трафика по правильному пути для предотвращения петель.
  - Работает на основе таблицы одноадресной маршрутизации.
  - Процесс проверки:
    - Маршрутизатор пересылает пакеты многоадресной передачи только из своего интерфейса, подключенного к источнику многоадресной рассылки, и отбрасывает пакеты, полученные другим путем.

Таблица маршрутизации IPv6	
Сегмент	Интерфейс
FC00:0:0:2001::1/64	S0
FC00:0:0:3001::1/64	S1
FC00:0:0:4001::1/64	S2



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Принципы проверки RPF
  - Когда маршрутизатор получает пакет многоадресной рассылки, он ищет в таблице одноадресной маршрутизации маршрут к адресу источника пакета. Когда маршрут найден, маршрутизатор проверяет, совпадает ли исходящий интерфейс для маршрута с входящим интерфейсом пакета. Если они совпадают, маршрутизатор считает, что пакет был получен из правильного интерфейса. Это гарантирует корректность путей переадресации пакетов.
  - Если маршруты с одинаковой стоимостью находятся в одной таблице маршрутизации, маршрутизатор выбирает маршрут с наибольшим адресом следующего узла в качестве маршрута RPF.
  - Проверки RPF могут выполняться на основе одноадресной передачи, протокола MBGP или статических многоадресных маршрутов. Приоритет маршрутов: статические многоадресные маршруты > маршруты MBGP > одноадресные маршруты.

- Описание топологии
  - Многоадресный трафик, отправленный из источника FC00:0:0:2001::1/64, поступает на интерфейс S1 маршрутизатора. Маршрутизатор проверяет таблицу маршрутизации и обнаруживает, что многоадресный трафик из этого источника должен поступить на интерфейс S0. Проверка RPF не пройдена, и маршрутизатор отбрасывает многоадресный поток.
  - Многоадресный трафик, отправленный из источника FC00:0:0:2001::1/64, поступает на интерфейс S0 маршрутизатора. Маршрутизатор проверяет таблицу маршрутизации и обнаруживает, что интерфейс RPF также является S0. Проверка RPF выполнена, и многоадресный трафик перенаправляется в правильном напрвлении.

- Протоколы многоадресной маршрутизации определяют вышестоящие и нижестоящие соседние узлы и создают записи многоадресной маршрутизации на основе одноадресных маршрутов. Механизм проверки RPF позволяет передавать многоадресные потоки данных по дереву распространения многоадресного трафика и предотвратить возникновение петель в маршрутах переадресации.
- Если маршрутизатор выполняет поиск в таблице одноадресной маршрутизации, чтобы проверить RPF для каждого полученного пакета многоадресных данных, потребуется большое количество системных ресурсов. Для экономии ресурсов маршрутизатор сначала выполняет поиск соответствующей записи (S, G) после получения пакета данных, отправленного из источника в группу.
- Если соответствующая запись (S, G) не найдена, маршрутизатор выполняет проверку RPF, чтобы найти интерфейс RPF для данного пакета. Затем маршрутизатор создает многоадресный маршрут с интерфейсом RPF в качестве восходящего интерфейса и передает маршрут в информационную базу многоадресной передачи (MFIB). Если проверка RPF пройдена, входящий интерфейс пакета является интерфейсом RPF, и маршрутизатор пересылает пакет на все нисходящие интерфейсы, содержащиеся в записи. Если проверка RPF не пройдена, пакет был переадресован по неверному пути, поэтому маршрутизатор отбрасывает такой пакет.
- Если соответствующая запись (S, G) найдена и входящий интерфейс пакета совпадает с восходящим интерфейсом в записи, маршрутизатор дублирует данный пакет на все нисходящие интерфейсы, указанные в записи.

- Если соответствующая запись (S, G) найдена, но входящий интерфейс пакета отличается от восходящего интерфейса в записи, маршрутизатор выполняет проверку RPF для пакета. В зависимости от результатов проверки RPF маршрутизатор обрабатывает пакет следующим образом:
    - Если интерфейс RPF совпадает с восходящим интерфейсом в записи, запись (S, G) является правильной, и пакет был переадресован по неверному пути.
    - Если интерфейс RPF отличается от восходящего интерфейса в записи, запись (S, G) устарела, и маршрутизатор изменяет интерфейс восходящего потока в записи, чтобы он был таким же, как интерфейс RPF. Затем маршрутизатор сравнивает интерфейс RPF с входящим интерфейсом пакета. Если входящий интерфейс является интерфейсом RPF, маршрутизатор дублирует пакет на все нисходящие интерфейсы, указанные в записи (S, G).

Разделение нагрузки многоадресной передачи (load splitting)

- Разделение нагрузки отличается от балансировки нагрузки.
- Разделение нагрузки – это распределение потоков данных к одному пункту назначения по нескольким маршрутам с одинаковой стоимостью. Нагрузка может распределяться неравномерно.
- Балансировка нагрузки – это особая форма разделения нагрузки, при которой нагрузка распределяется равномерно по нескольким маршрутам с одинаковой стоимостью.

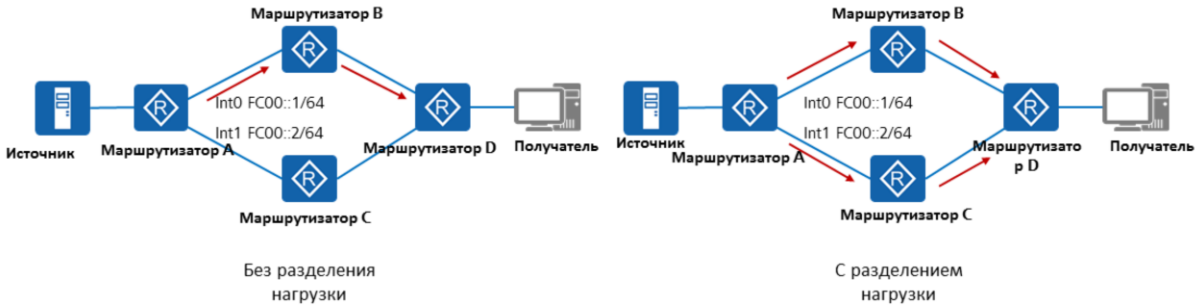
Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Если при пересылке пакетов многоадресной рассылки существует несколько маршрутов с одинаковой стоимостью, маршрутизатор по умолчанию выбирает в качестве маршрута RPF маршрут с наибольшим адресом следующего узла только из таблицы маршрутизации IGP.

Многоадресная пересылка без разделения и с разделением нагрузки

- Разделение нагрузки позволяет маршрутизатору распределять многоадресный трафик по нескольким маршрутам с одинаковой стоимостью вместо того, чтобы выбирать только один маршрут на основе политики проверки RPF.



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Источник многоадресной передачи отправляет потоки многоадресного трафика в группу G. Маршрутизатор A и Маршрутизатор D запускают протокол внутреннего шлюза (IGP), например OSPF, для реализации взаимодействия IP. Доступны два пути одинаковой стоимости: Маршрутизатор A -> Маршрутизатор B -> Маршрутизатор D и Маршрутизатор A -> Маршрутизатор C -> Маршрутизатор D.
- На основе политики проверки RPF по умолчанию потоки многоадресного трафика пересылаются через интерфейс Int1 маршрутизатора A, поскольку Int1 имеет больший IP-адрес, чем Int0. После настройки разделения многоадресной нагрузки на маршрутизаторе A он не выбирает маршруты переадресации путем сравнения IP-адресов следующих узлов. Вместо этого потоки многоадресного трафика пересылаются по обоим маршрутам с равной стоимостью.

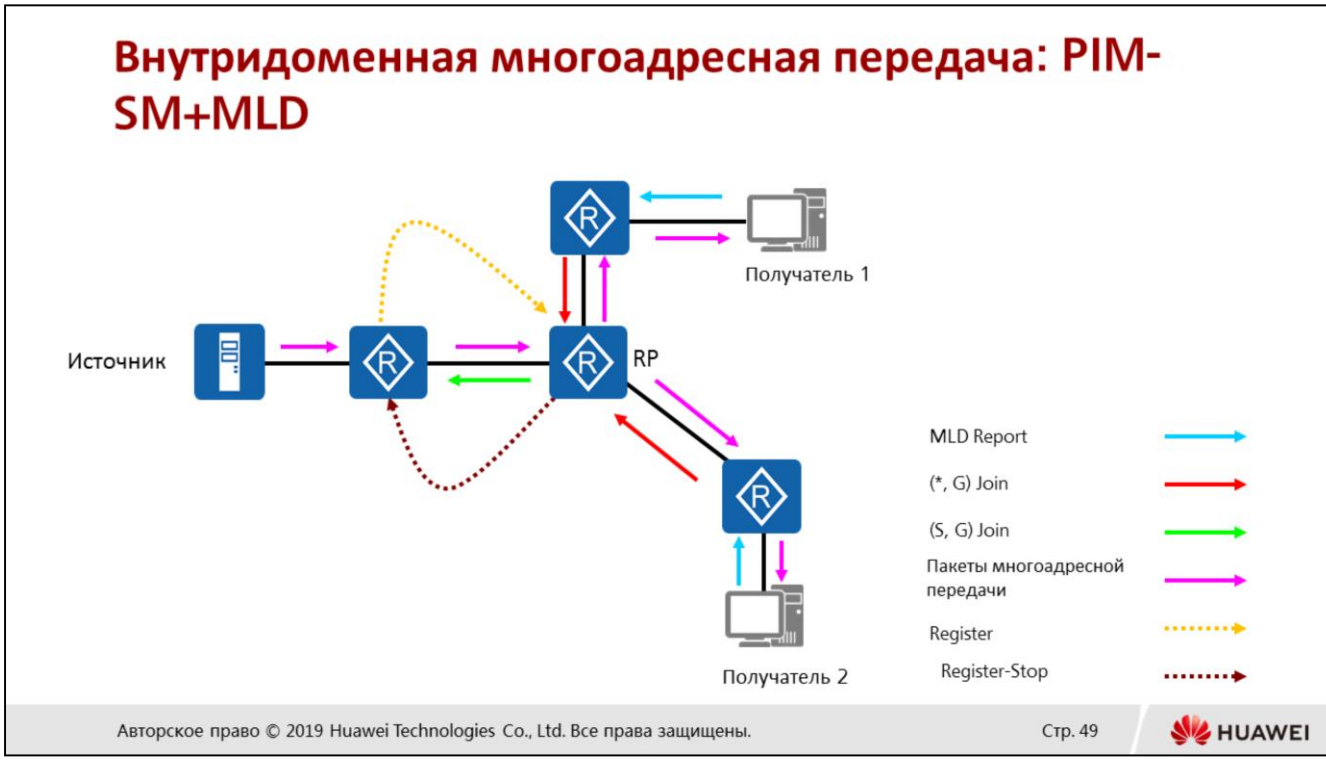


Содержание

- Механизм PIM-SM
- Конфигурация IPv6 PIM-SM
- Основные принципы IPv6 PIM-SSM
- Управление многоадресным маршрутом
- **Типичные области применения многоадресной передачи IPv6**

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI



- Как показано на рисунке, маршрутизаторы в домене используют PIM-SM, а интерфейсы, подключенные к получателям, – MLDv1. Протокол MLDv1 для многоадресной передачи IPv6 эквивалентен IGMPv2 для многоадресной передачи IPv4 и используется для получения информации о членах группы многоадресной рассылки и уведомления протоколов верхнего уровня.
- Все маршрутизаторы в домене получают информацию RP посредством статической конфигурации, динамического выбора (BSR) или автоматического обнаружения.
- Предпоследний маршрутизатор, подключенный к получателю IPv6, получает сообщение MLD Report от получателя и отправляет сообщение (*, G) Join вышестоящим маршрутизаторам через соседей RPF, пока RP не получит сообщение (*, G) Join. Все маршрутизаторы в пути создают запись (*, G) и автоматически создают дерево RPT с RP в качестве корневого узла.
- Источник многоадресной рассылки отправляет данные многоадресной рассылки. Первый маршрутизатор отправляет сообщение PIM Register на RP. После получения сообщения RP отправляет сообщение Register-Stop.
- RP отправляет сообщение (S, G) Join первому маршрутизатору через соседей RPF. Маршрутизаторы в пути создают запись (S, G), и автоматически создают дерево SPT с первым маршрутизатором в качестве корневого узла.
- Данные многоадресной рассылки поступают на RP по дереву SPT и пересылаются на основе записи (*, G). Маршрутизаторы вдоль пути генерируют запись (S, G), и данные доходят до получателя.

Краткое содержание раздела

- Механизм PIM-SM
- Конфигурация IPv6 PIM-SM
- Основные принципы IPv6 PIM-SSM
- Управление многоадресным маршрутом
- Типичные области применения многоадресной передачи IPv6

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.



Тест

- Чем отличаются протоколы IPv6 PIM-SM и IPv4 PIM-SM?
- В чем заключается принцип работы IPv6 PIM-SSM?

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Чем отличаются протоколы IPv6 PIM-SM и IPv4 PIM-SM?
  - Адреса различаются, но принципы действия протоколов аналогичны.
- В чем заключается принцип действия IPv6 PIM-SSM?
  - Реализация IPv6 PIM-SSM включает механизмы обнаружение соседа, выбора DR-маршрутизатора и создания дерева SPT.
    - По аналогии с IPv6 PIM-SM, IPv6 PIM-SSM выполняет обнаружение соседа и выбор DR-маршрутизатора с помощью сообщений Hello, передаваемых между маршрутизаторами.
    - PIM-SSM также использует PIM-SM. Последний маршрутизатор определяет, какое дерево нужно создавать – RPT или SPT –в зависимости от того, находится ли адрес многоадресной рассылки в диапазоне адресов группы SSM.

Спасибо!

www.huawei.com

HCIE-R&S

— Варианты MPLS BGP VPN между автономными системами (AS)

www.huawei.com

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Введение

- MPLS гармонично сочетает в себе гибкость IP-маршрутизации и простоту переключения меток в асинхронном режиме передачи (ATM). В IP-сети без установления соединения технология MPLS обеспечивает ориентированную на установление соединения плоскость управления, предоставляя дополнительные средства управления и эксплуатации IP-сети. Таким образом, операторы связи, высоко оценив преимущества VPN (или MPLS VPN), в которых IP-сети MPLS используются в качестве магистральных сетей, стали применять их для предоставления дополнительных видов обслуживания.
- В данном документе приводятся теоретические основы и конфигурации Варианта A, Варианта B и Варианта C для VPN между автономными системами (AS).

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Цели

- По окончании данного курса Вы получите представление о теоретических основах и конфигурациях:
  - Варианта A VPN между AS
  - Варианта B VPN между AS
  - Варианта C VPN между AS

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

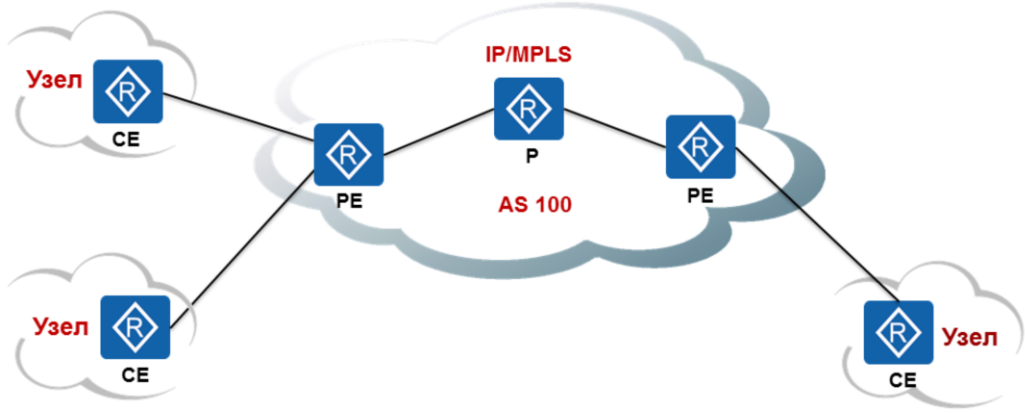
Содержание

- **Общие сведения**
- Теоретические основы
- Конфигурации

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Общие сведения о решении MPLS BGP VPN между AS (1/3)

- Традиционное решение MPLS BGP VPN



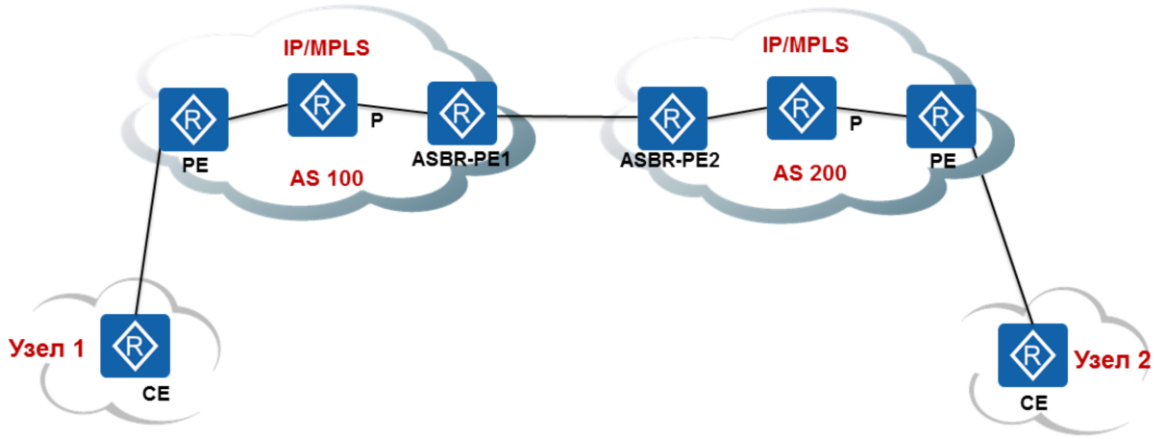
© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Введение

- Благодаря широкому применению решений MPLS VPN, филиальные сети крупных предприятий или сети совместных предприятий объединяют несколько AS.
- Например:
- Как правило, архитектура MPLS VPN используется внутри AS, в которой информация о маршрутизации экземпляра VPN лавинным образом рассылается по требованию. При этом информация о маршрутизации VPN внутри AS не может лавинно рассылаться в другие AS.
- В сети, показанной на этом слайде, VPN на основе MPLS соединяет различные ветви частной сети, образуя единую сеть. Кроме того, она обеспечивает контроль взаимодействия разных VPN. CE (Customer Edge) — граничное клиентское устройство. PE (Provider Edge) — маршрутизатор провайдера услуг, расположенный на границе магистральной сети. P (Provider) — магистральный маршрутизатор в сети провайдера услуг, который не имеет прямого подключения к CE.

Общие сведения о решении MPLS BGP VPN между AS (2/3)



© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

- Можно ли использовать для развертывания услуг традиционное решение MPLS BGP VPN, если два узла одной VPN расположены в разных AS?
- Ответ — нет. В этом случае PE с одинаково настроенным экземпляром VPN не могут устанавливать отношения соседства IBGP или отношения соседства с RR. Вместо этого PE требуются отношения соседства EBGP для передачи маршрутов VPNv4.
- Чтобы обеспечить обмен маршрутами VPN между различными AS, используется модель Inter-AS MPLS VPN. Эта модель является расширением существующего протокола и стандарта MPLS VPN. Ее использование позволяет анонсировать префикс маршрута и информацию о метке по каналам между различными AS.

Общие сведения о решении MPLS BGP VPN между AS (3/3)

- Данная презентация познакомит Вас с тремя следующими решениями VPN между AS:
  - Вариант A магистральных сетей между интернет-провайдерами (Inter-AS VPN Option A): экземпляры VPN, охватывающие несколько AS, имеют привязку к выделенным интерфейсам ASBR для управления своими собственными маршрутами VPN. Также это решение называется «VRF-to-VRF».
  - Вариант B магистральных сетей между интернет-провайдерами (Inter-AS VPN Option B): ASBR обмениваются маркированными маршрутами VPN-IPv4 друг с другом посредством MP-EBGP. Это решение также называется перераспределением EBGP маркированных маршрутов VPN-IPv4.
  - Вариант C магистральных сетей между интернет-провайдерами (Inter-AS VPN Option C): PE или RR обмениваются маркированными маршрутами VPN-IPv4 друг с другом посредством многоузлового MP-EBGP. Также это решение называется многоузловым перераспределением EBGP маркированных маршрутов VPN-IPv4.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Содержание

- Общие сведения
- **Теоретические основы**
  - Вариант A
  - Вариант B
  - Вариант C
- Конфигурации

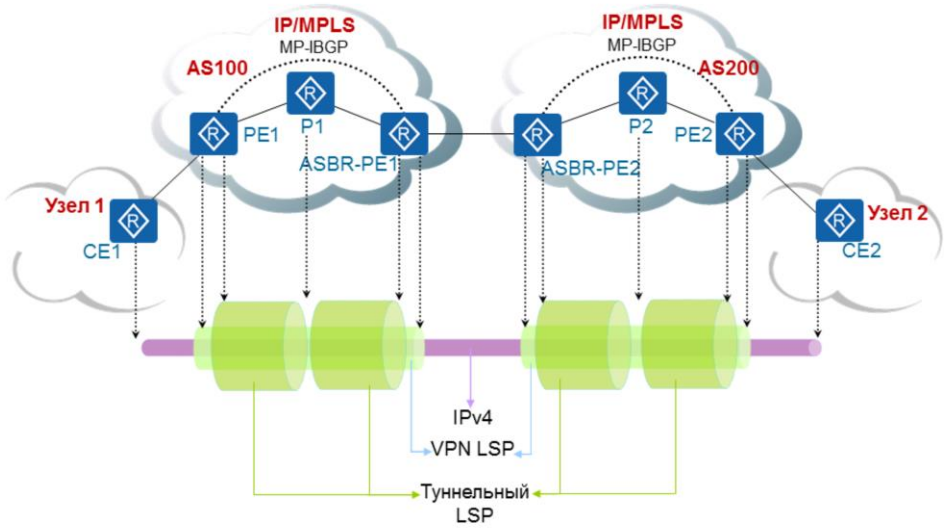
© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Вариант A магистральных сетей между интернет-провайдерами

- При использовании в качестве базового приложения BGP/MPLS IP VPN между автономными системами Вариант A не требует специального конфигурирования. Кроме того, между ASBR не требуется реализация MPLS. В этом режиме ASBR двух AS взаимодействуют напрямую, выполняя функции PE в собственных AS. Каждый ASBR воспринимает равноправный ASBR в качестве своего CE и передает ему маршруты IPv4 посредством EBGP.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Вариант A магистральных сетей между интернет-провайдерами — Топология

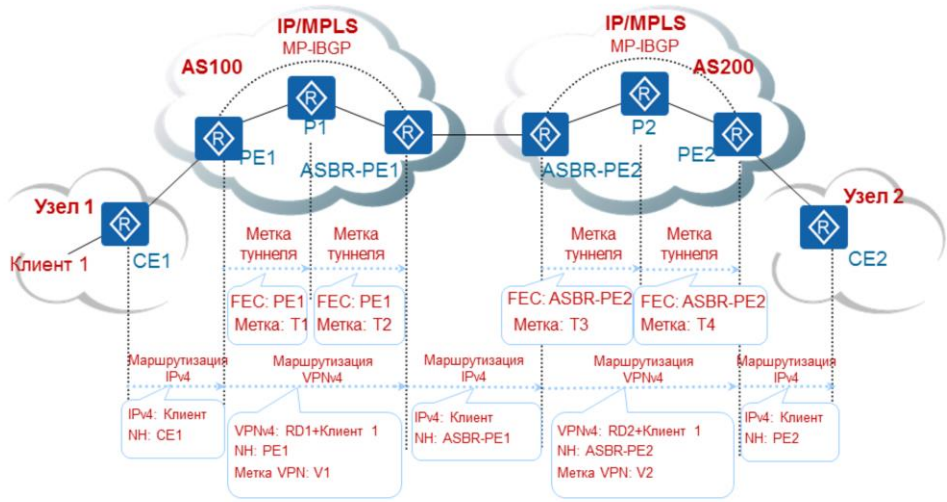


© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

- В этом решении ASBR-PE связаны напрямую. Два ASBR-PE взаимодействуют друг с другом через несколько интерфейсов, включая субинтерфейсы. Каждый интерфейс имеет привязку к VPN, и каждый ASBR-PE воспринимает своего соседа как CE. Следовательно, интерфейсы (включая субинтерфейсы), которые участвуют в соединении ASBR-PE, должны иметь привязку к VRF. Кроме того, маршрутам VPNv4 требуется преобразование в стандартные маршруты IPv4 для рассылки их от одной AS к другой посредством отношений соседства EBGP. Включение MPLS на подключенных ASBR-PE не требуется. Это решение не обеспечивает расширение сервисных атрибутов в MPLS BGP VPN.

Вариант A магистральных сетей между интернет-провайдерами — Плоскость управления



© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

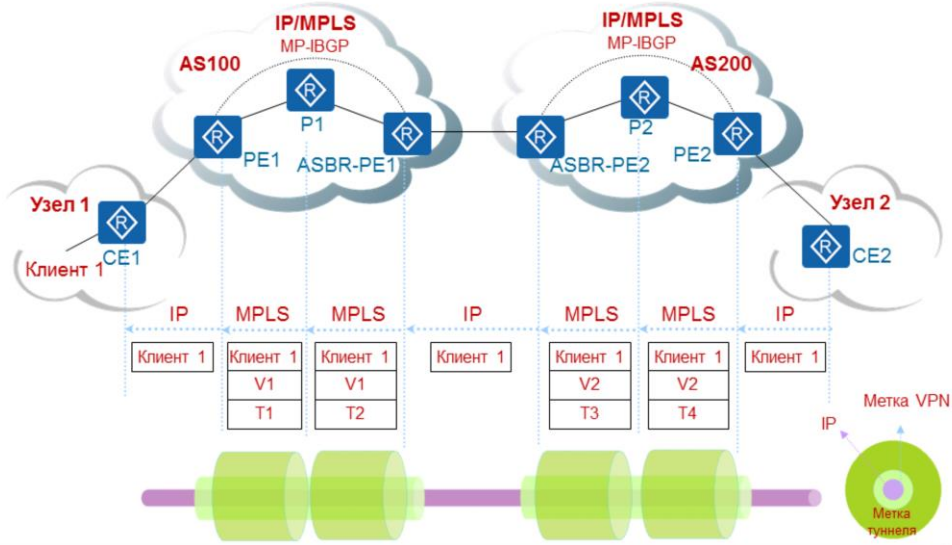
HUAWEI

- Рассмотрим в качестве примера анонсирование маршрутов в одном направлении в плоскости управления. Предположим, что на Узле 1 имеется хост, который называется Клиент 1. Необходимо реализовать анонсирование маршрута к Клиенту 1 от CE1 до CE2 через AS100 и AS200.
  - В AS100 PE1 использует LDP для назначения P1 метки внешнего туннеля T1, привязанной к маршруту до PE1.
  - В AS100 P1 использует LDP для назначения ASBR-PE1 метки внешнего туннеля T2, привязанной к маршруту до PE1.
  - В AS200 ASBR-PE2 использует LDP для назначения P2 метки внешнего туннеля T3, привязанной к маршруту до ASBR-PE2.
  - В AS200 P2 использует LDP для назначения PE2 метки внешнего туннеля T4, привязанной к маршруту до ASBR-PE2.
  - CE1 анонсирует PE1 маршрут, предназначенный для Клиента 1, где следующим узлом маршрута является адрес интерфейса CE1.
  - PE1 инкапсулирует полученный маршрут IPv4 к Клиенту 1 в маршрут VPNv4, меняет данные следующего узла на PE1 в соответствующем сообщении MP-BGP, присваивает метку VPN V1 для маршрута, а затем анонсирует маршрут в ASBR-PE1.
  - ASBR-PE1 выполняет обратное преобразование полученного маршрута VPNv4 в маршрут IPv4 и анонсирует его ASBR-PE2, указывая ASBR-PE1 в качестве следующего узла.
  - ASBR-PE2 инкапсулирует полученный маршрут IPv4 к Клиенту 1 в маршрут VPNv4, меняет данные следующего узла на ASBR-PE2 в соответствующем сообщении MP-BGP,

присваивает метку VPN V2 для маршрута, а затем анонсирует маршрут в PE2.

- PE2 выполняет обратное преобразование полученного маршрута VPNv4 в маршрут IPv4 для Клиента 1 и анонсирует его CE2, указывая PE2 в качестве следующего узла.

Вариант A магистральных сетей между интернет-провайдерами — Плоскость передачи



© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

- Теперь давайте рассмотрим передачу пакетов в плоскости передачи. В качестве примера используем процесс пакетной передачи от CE2 к CE1.
  - CE2 отправляет IP-пакет, предназначенный для Клиента 1, в PE2.
  - После получения PE2 инкапсулирует IP-пакет с меткой VPN V2, затем присваивает пакету внешнюю метку T4 и передает пакет в P2.
  - P2 меняет внешнюю метку T4 на T3 и передает IP-пакет в ASBR-PE2.
  - ASBR-PE2 удаляет обе метки из полученного пакета и перенаправляет немаркированный IP-пакет в ASBR-PE1.
  - ASBR-PE1 инкапсулирует полученный IP-пакет с меткой VPN V1, присваивает ему внешнюю метку T2 и передает пакет в P1.
  - P1 меняет внешнюю метку T2 на T1 и пересылает пакет в PE1.
  - PE1 удаляет обе метки из полученного пакета и перенаправляет немаркированный IP-пакет в CE1.

Особенности варианта A магистральных сетей между интернет-провайдерами

- Простота конфигурирования: конфигурирование MPLS не требуется между ASBR, а также не требуются специальные настройки соединений между AS.
- Низкая масштабируемость: всеми маршрутами VPN должны управлять ASBR, и для каждой VPN требуется конфигурирование экземпляра VPN. В результате на ASBR создается огромное количество маршрутов VPN-IPv4. Кроме того, поскольку между ASBR выполняется обычная IP-переадресация, то каждому экземпляру VPN между AS требуется привязка к определенному интерфейсу AC. Это значительно повышает требования к PE. Если VPN охватывает несколько AS, то промежуточные AS должны поддерживать сервисы VPN. Это усложняет процесс конфигурирования и существенно влияет на работу промежуточных AS. Таким образом, Вариант A рекомендуется к применению только, если между AS используется небольшое количество экземпляров VPN.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Содержание

- Общие сведения
- **Теоретические основы**
  - Вариант A
  - Вариант B
  - Вариант C
- Конфигурации

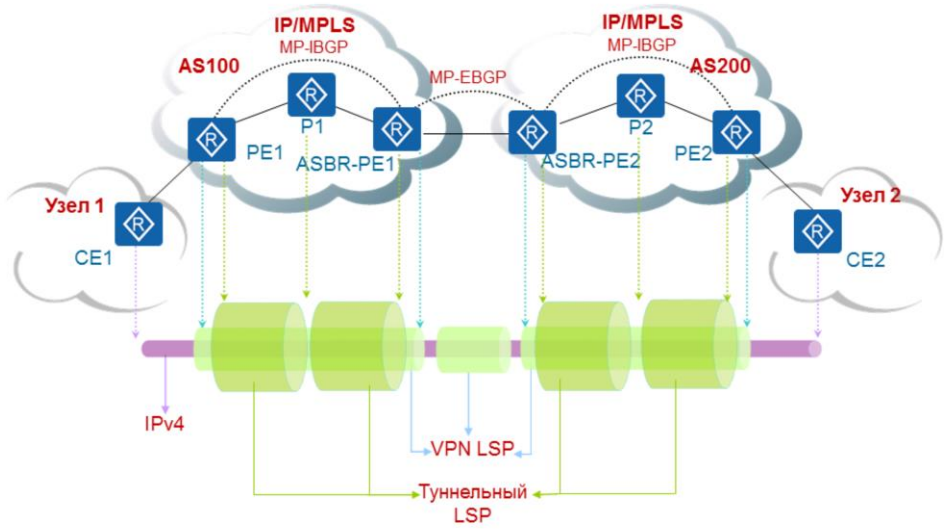
© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Вариант B магистральных сетей между интернет-провайдерами

- В Варианте B два ASBR для обмена маркированными маршрутами VPN-IPv4, полученными от PE в собственных AS, используют MP-EBGP.
- В Варианте B ASBR анонсирует все маршруты VPN-IPv4, полученные от внешней AS, в свою локальную AS. Кроме того, он анонсирует все маршруты VPN-IPv4, полученные от других устройств в одной AS, во внешнюю AS. В базовой реализации MPLS VPN PE хранит только те маршруты VPN, которые соответствуют объектам назначения VPN определенного экземпляра VPN, сконфигурированного на PE. Фильтрацию маршрутов на основе RT в ASBR, которые анонсируют маршруты, можно отключить. Таким образом, пользователю не нужно создавать экземпляры VPN на ASBR или настраивать привязку экземпляров VPN к интерфейсам.
- Для передачи VPN-маршрутов со стороны пользователя в сети развертываются RR.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Вариант B магистральных сетей между интернет-провайдерами — Топология

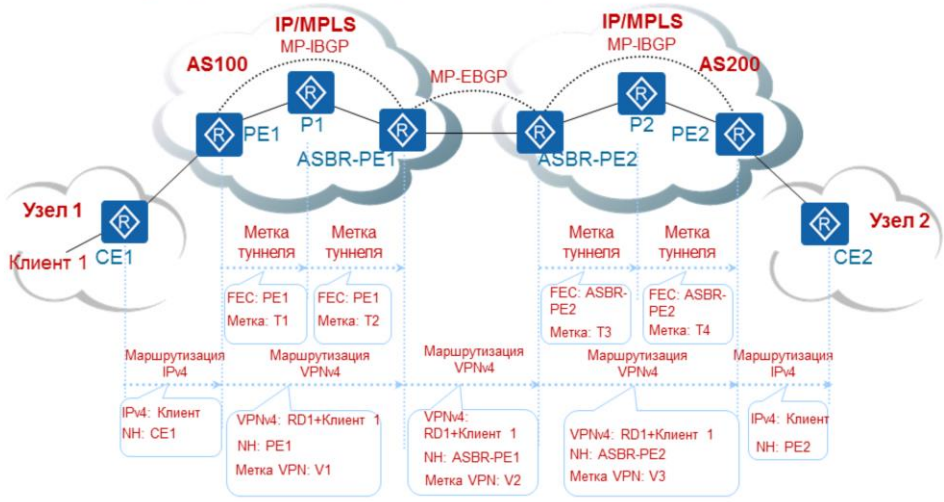


© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

- В решении Варианта B каждый PE анонсирует маршруты VPNv4 своему подключенному ASBR-PE или VPN RR посредством MP-IBGP. ASBR-PE является клиентским устройством PE. ASBR-PE в одной AS анонсирует маршруты VPNv4 в ASBR-PE другой AS посредством MP-EBGP. После получения ASBR-PE анонсирует маршруты VPNv4 в PE той же AS.

Вариант B магистральных сетей между интернет-провайдерами — Плоскость управления (без RR)



© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

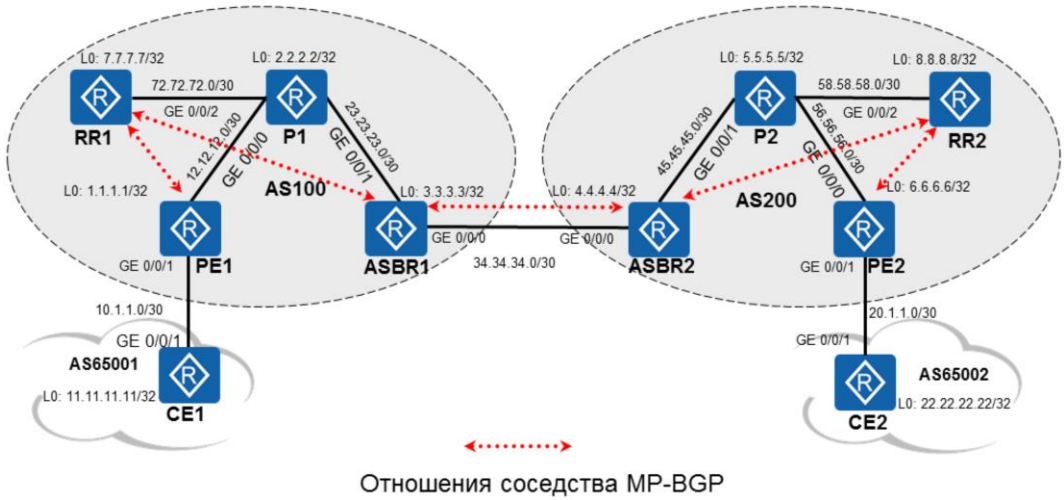
HUAWEI

- Рассмотрим в качестве примера анонсирование маршрутов в одном направлении в плоскости управления. Предположим, что на Узле 1 имеется хост, который называется Клиент 1.
- 1. В AS100 PE1 использует LDP для назначения P1 метки внешнего туннеля T1, привязанной к маршруту до PE1.
- 2. В AS100 P1 использует LDP для назначения ASBR-PE1 метки внешнего туннеля T2, привязанной к маршруту до PE1.
- 3. В AS200 ASBR-PE2 использует LDP для назначения P2 метки внешнего туннеля T3, привязанной к маршруту до ASBR-PE2.
- 4. В AS200 P2 использует LDP для назначения PE2 метки внешнего туннеля T4, привязанной к маршруту до ASBR-PE2.
- 5. CE1 анонсирует PE1 маршрут, предназначенный для Клиента 1, где следующим узлом маршрута является адрес интерфейса CE1.
- 6. PE1 инкапсулирует полученный маршрут IPv4 к Клиенту 1 в маршрут VPNv4, меняет данные следующего узла на PE1 в соответствующем сообщении MP-IBGP, присваивает метку VPN V1 для маршрута, а затем анонсирует маршрут в ASBR-PE1.
- 7. ASBR-PE1 анонсирует маршрут VPNv4, предназначенный для Клиента 1, в ASBR-PE2 посредством MP-EBGP, меняет следующий узел маршрута на ASBR-PE1 и присваивает маршруту новую метку VPN V2.
- 8. ASBR-PE2 анонсирует полученный маршрут VPNv4 в PE2 посредством MP-IBGP, меняет следующий узел маршрута на свой собственный адрес и присваивает маршруту

новую метку VPN V3.

- 9. PE2 выполняет обратное преобразование полученного маршрута VPNv4 в маршрут IPv4 для Клиента 1 и анонсирует его CE2, указывая PE2 в качестве следующего узла.

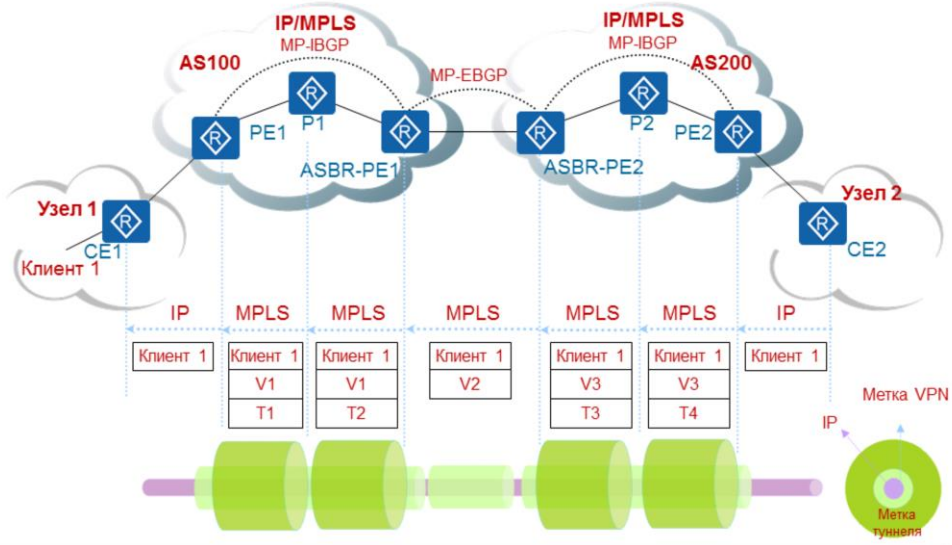
Вариант B магистральных сетей между интернет-провайдерами — Плоскость управления (с RR)



© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

- При необходимости использования большого количества экземпляров VPN рекомендуется развертывание независимых RR. Как показано на этом рисунке, PE и ASBR в каждой AS устанавливают отношения соседства MP-BGP только с RR. RR в каждой AS отражает маршруты, что исключает необходимость устанавливать отношения соседства BGP между PE и ASBR.
- RR передает только маршруты VPNv4 в плоскости управления и не передает трафик данных в плоскости передачи.

Вариант B магистральных сетей между интернет-провайдерами — Плоскость передачи



© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

- В качестве примера для иллюстрации процесса в плоскости передачи используем процесс пакетной передачи от CE2 к CE1.
  - CE2 отправляет IP-пакет, предназначенный для Клиента 1, в PE2.
  - После получения PE2 инкапсулирует IP-пакет с меткой VPN V3, затем присваивает пакету внешнюю метку T4 и передает пакет в P2.
  - P2 меняет внешнюю метку T4 на T3 и передает IP-пакет в ASBR-PE2.
  - ASBR-PE2 удаляет внешнюю метку из полученного пакета, меняет метку VPN V3 на V2 и пересылает пакет, содержащий только метку VPN V2, в ASBR-PE1.
  - После получения пакета ASBR-PE1 меняет метку VPN V2 на V1, добавляет метку внешнего туннеля T2, а затем пересылает пакет в P1.
  - P1 меняет внешнюю метку T2 на T1 и пересылает пакет в PE1.
  - PE1 удаляет обе метки из полученного пакета и перенаправляет немаркированный IP-пакет в CE1.

Особенности Варианта B магистральных сетей между интернет-провайдерами

- В отличие от Варианта A Вариант B не имеет ограничений в отношении количества каналов между ASBR.
- ASBR осуществляют хранение и передачу информации о маршрутизации VPN. При наличии большого количества VPN-маршрутов возникает перегрузка ASBR, что приводит к сбою в работе. ASBR, которые устанавливают отношения соседства MP-EBGP, только хранят информацию о маршрутизации VPN и не передают IP-пакеты в сеть общего пользования.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Содержание

- Общие сведения
- Теоретические основы
  - Вариант A
  - Вариант B
  - Вариант C
- Конфигурации

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

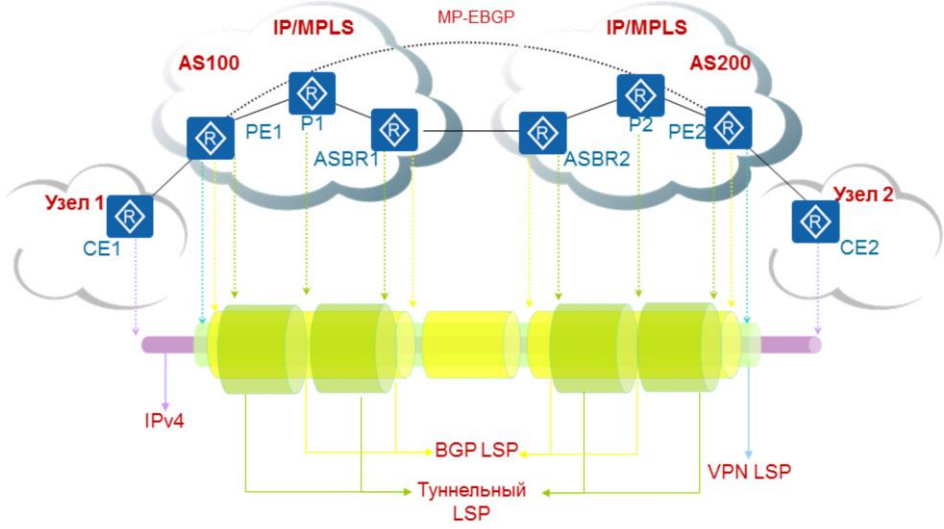
Вариант C магистральных сетей между интернет-провайдерами — Решение 1

- В Варианте C ASBR в каждой AS анонсирует маркированные маршруты IPv4 в подключенный к нему PE посредством MP-IBGP, а также анонсирует маркированные маршруты IPv4, полученные от подключенного PE, в равноправный ASBR другой AS. ASBR в транзитной AS также анонсирует маркированные маршруты IPv4. Таки образом, между входным PE и выходным PE устанавливается BGP LSP.
- PE в разных AS устанавливают многоузловое соединение EBGP друг с другом для обмена маршрутами VPNv4.
- ASBR не хранят маршруты VPN-IPv4 и не анонсируют маршруты VPNv4 друг другу.
- Для передачи маршрутов на стороне пользователя в крупномасштабной сети развертываются RR. В частности, PE и RR устанавливают отношения соседства MP-IBGP. RR1 и RR2 устанавливают отношения соседства MP-EBGP. Маршруты передаются по пути PE1 <-> RR1 <-> RR2 <-> PE2. Между PE установление отношения соседства BGP не требуется. При наличии большого количества VPN маршрутизаторы RR помогают снизить нагрузку на PE.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Вариант C магистральных сетей между интернет-провайдерами — Топология



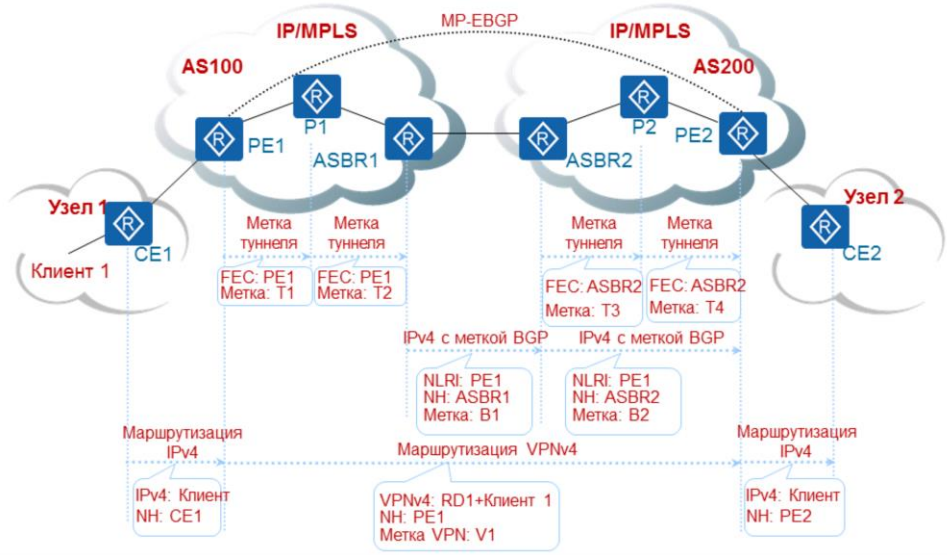
© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

- В решении Варианта C ASBR не хранят и не анонсируют маршруты VPNv4. Поэтому маршрутизаторы ASBR-PE заменяются на ASBR, как показано на рисунке. ASBR обеспечивает только хранение всех маркированных маршрутов до PE и использует EBGP для анонсирования этих маркированных маршрутов равноправному узлу в другой AS. ASBR в транзитной AS также должны использовать EBGP для анонсирования маркированных маршрутов IPv4. Таким образом, между PE в разных AS устанавливается BGP LSP, который обеспечивает многоузловое соединение MP-EBGP для анонсирования этими PE маршрутов VPNv4.
- Наличие на маршрутизаторе P информации о маршрутах до PE в другой AS упрощает передачу данных. Однако, если на маршрутизаторе P нет информации о маршрутах, PE добавляет метку уровня 3 к данным VPN, полученным от CE. Внутренней меткой является метка VPN, ассоциированная с маршрутом VPN и присваиваемая равноправному PE. Промежуточной меткой является метка, назначаемая ASBR и ассоциированная с маршрутом до равноправного PE. Внешней меткой является метка, ассоциированная с маршрутом до ASBR следующего узла.
- Для повышения производительности в будущем между VPN RR в разных AS можно установить многоузловой сеанс MP-EBGP. VPN RR не меняют атрибут Next_Hop при анонсировании маршрутов VPNv4. В каждой AS PE устанавливает сеанс MP-IBGP только с VPN RR.
- Примечание: для наглядности в данном примере используется симметричный LSP, как показано на рисунке. Однако структуры LSP в разных AS не являются симметричными. Более подробная информацию приводится на следующих

слайдах.

Вариант C магистральных сетей между интернет-провайдерами — Плоскость управления (без RR)

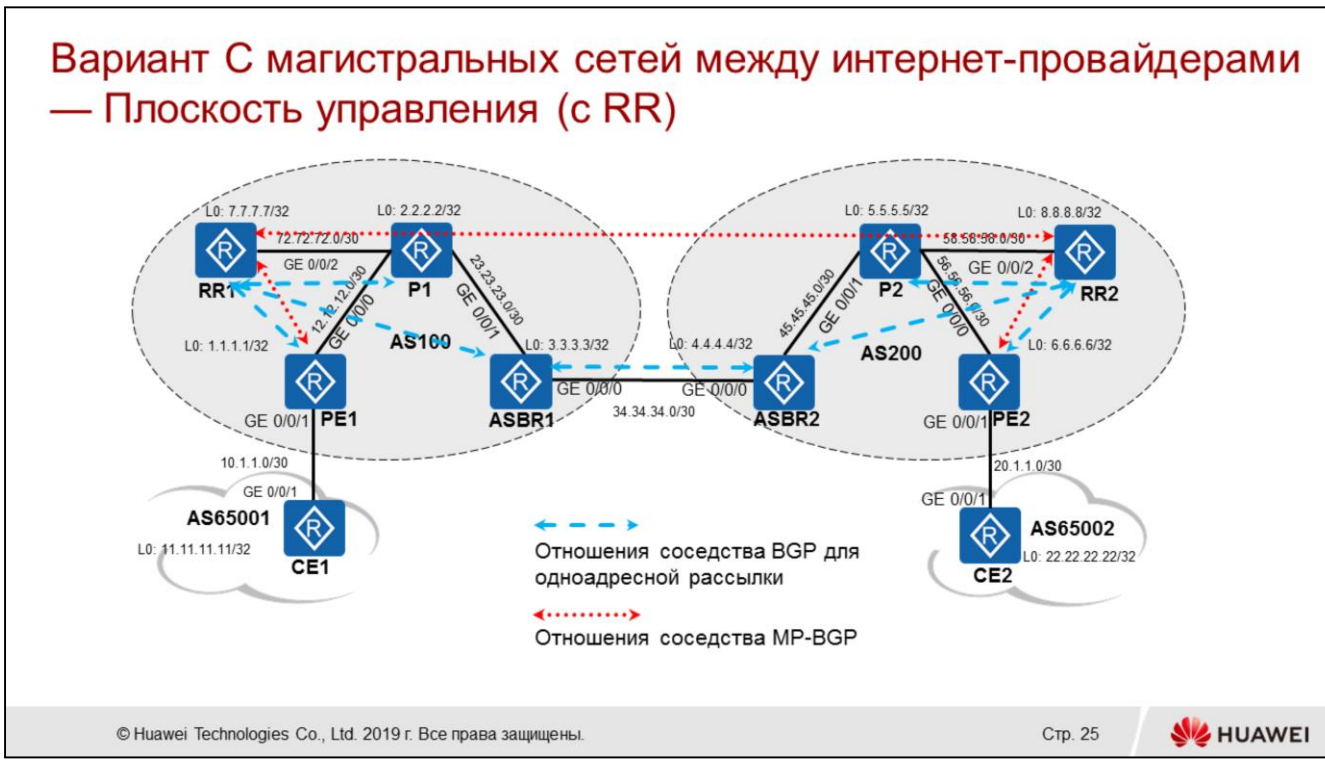


© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

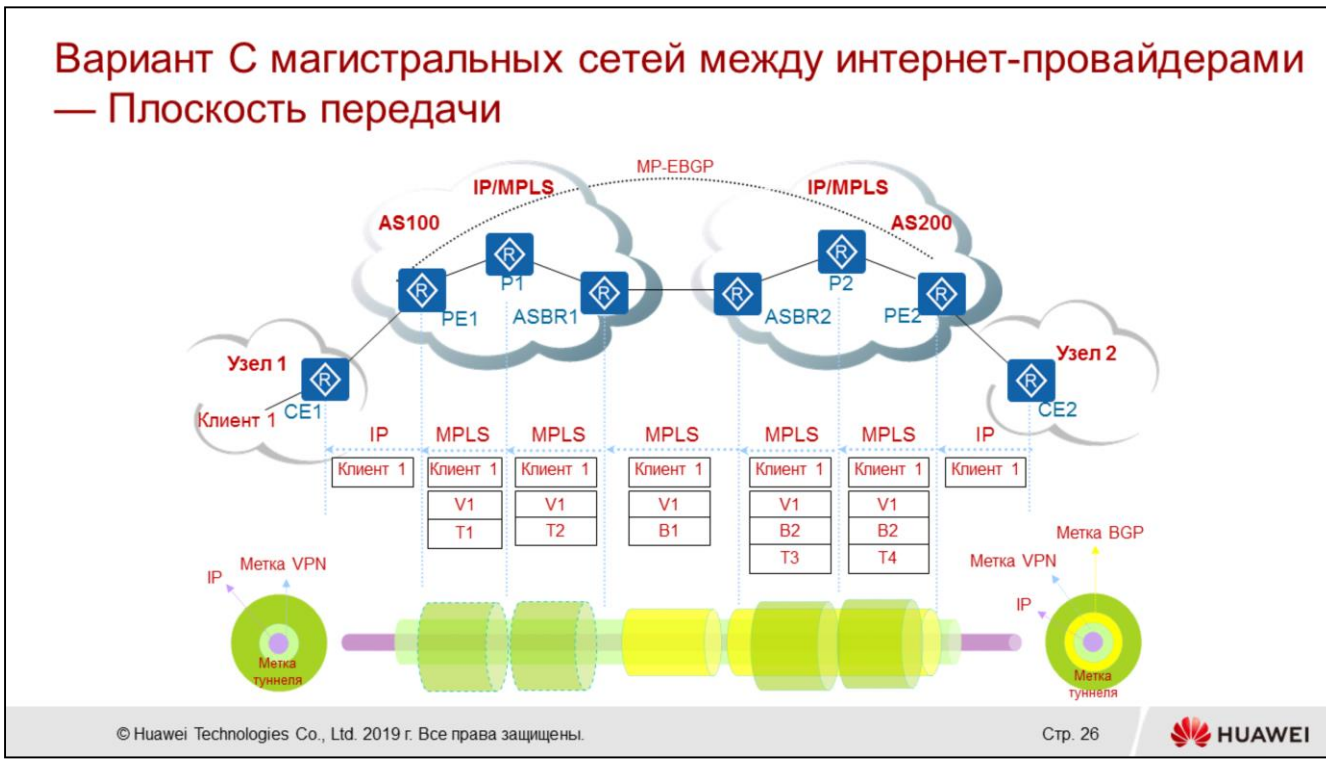
HUAWEI

- Рассмотрим в качестве примера анонсирование маршрутов в одном направлении в плоскости управления. Предположим, что на Узле 1 имеется хост, который называется Клиент 1. Маршрутизатор P каждой AS не имеет маршрутов к равноправному PE в другой AS.
  - В AS100 PE1 использует LDP для назначения P1 метки внешнего туннеля T1, привязанной к маршруту до PE1.
  - В AS100 P1 использует LDP для назначения ASBR-PE1 метки внешнего туннеля T2, привязанной к маршруту до PE1.
  - В AS200 ASBR-PE2 использует LDP для назначения P2 метки внешнего туннеля T3, привязанной к маршруту до ASBR-PE2.
  - В AS200 P2 использует LDP для назначения PE2 метки внешнего туннеля T4, привязанной к маршруту до ASBR-PE2.
  - ASBR1 анонсирует ASBR2 маркированный маршрут IPv4 до PE1 посредством сеанса EBGP. Следующим узлом является ASBR1, а метка является меткой BGP со значением B1.
  - ASBR2 анонсирует PE2 маркированный маршрут IPv4 до PE1 посредством сеанса BGP. Следующим узлом является ASBR2, а метка является меткой BGP со значением B2.
    - Примечание: Предположим, что маршрутам до PE2 и ASBR1 присвоены метки туннеля (или метки сети общего пользования), и осуществляется анонсирование маркированных маршрутов до PE2.
  - PE1 и PE2 устанавливают между собой сеанс MP-EBGP.
  - CE1 анонсирует PE1 маршрут, предназначенный для Клиента 1, где следующим узлом маршрута является адрес интерфейса CE1.
  - PE1 инкапсулирует полученный маршрут IPv4 к Клиенту 1 в маршрут VPNv4, меняет данные следующего узла на PE1 в соответствующем сообщении MP-EBGP, присваивает метку VPN V1 для маршрута, а затем анонсирует маршрут в PE2.
  - PE2 выполняет обратное преобразование полученного маршрута VPNv4 в маршрут

IPv4 для Клиента 1 и анонсирует его CE2, указывая PE2 в качестве следующего узла.



- Отношения соседства VPNv4:
  - PE устанавливает отношения соседства VPNv4 только с RR в одной с ним AS. Локальный RR устанавливает отношения соседства VPNv4 с равноправным RR для передачи маршрутов VPN между AS.
- ASBR, P и PE в одной AS устанавливают отношения соседства IPv4 для одноадресной передачи BGP с RR в той же AS.
  - Локальный ASBR выясняет loopback-маршрут до RR от равноправного ASBR посредством отношений соседства IPv4 и анонсирует loopback-маршрут локальному RR, чтобы локальный RR мог установить отношения соседства VPNv4 с равноправным RR.
  - Локальный ASBR выясняет loopback-маршруты равноправного RR и PE от равноправного ASBR посредством отношений соседства IPv4 и анонсирует их локальному RR. Далее локальный RR отражает loopback-маршруты в локальный маршрутизатор P для рекурсивного поиска маршрутов BGP между AS.
  - Локальный ASBR выясняет loopback-маршруты равноправного RR и PE от равноправного ASBR посредством отношений соседства IPv4 и анонсирует их локальному RR. Затем локальный RR отражает loopback-маршруты в локальный PE, чтобы PE в разных AS могли устанавливать BGP LSP.
- RR отражают маршруты IPv4 и передают маршруты VPNv4 в плоскости управления, но не передают трафик в плоскости передачи.



- В качестве примера для иллюстрации процесса в плоскости передачи используем процесс пакетной передачи от CE2 к CE1.
  - CE2 отправляет IP-пакет, предназначенный для Клиента 1, в PE2.
  - Сначала PE2 инкапсулирует полученный IP-пакет с меткой VPN V1. Поскольку PE1 следующего узла пакета не является напрямую подключенным соседним устройством, PE2 выполняет поиск по таблице маршрутизации, находит маркированный маршрут BGP до PE1, а затем добавляет в пакет метку BGP B2 в качестве промежуточной метки. Поскольку ASBR2 следующего узла маршрута до PE1 также не является напрямую подключенным соседним устройством, PE2 выполняет поиск по таблице маршрутизации и находит метку T4, ассоциированную с маршрутом до ASBR2. В результате PE2 добавляет в пакет внешнюю метку T4.
  - P2 меняет внешнюю метку T4 на T3 и передает IP-пакет в ASBR-PE2.
  - ASBR2 удаляет внешнюю метку из полученного пакета, меняет метку BGP B2 на B1 и пересылает пакет в ASBR1.
  - После получения пакета ASBR1 находит назначенную им метку B1, удаляет ее и выполняет поиск по таблице маршрутизации. ASBR1 находит метку T2, ассоциированную с маршрутом до PE1, добавляет метку T2 к вершине стека, а затем пересылает пакет в P1.
  - P1 меняет внешнюю метку T2 на T1 и пересылает пакет в PE1.
  - PE1 удаляет обе метки из полученного пакета и перенаправляет

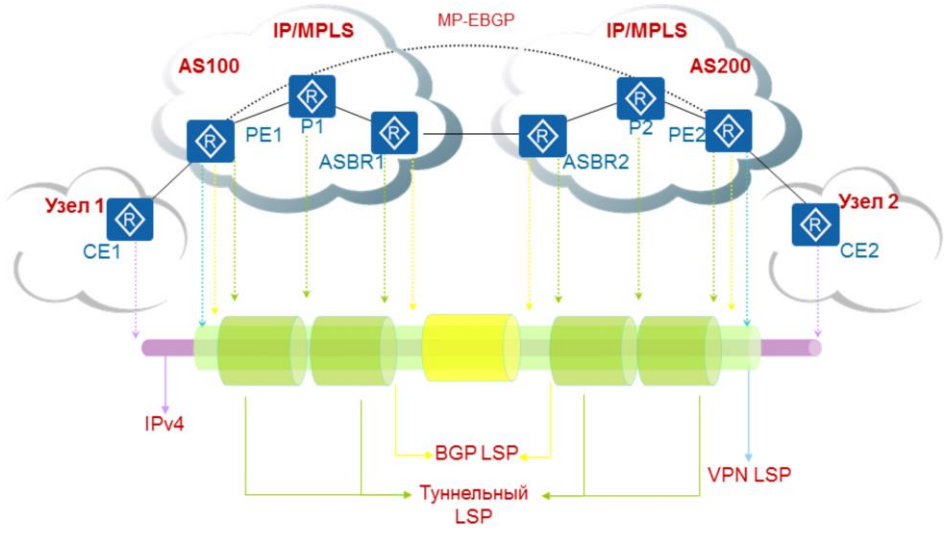
немаркированный IP-пакет в CE1.

Вариант C магистральных сетей между интернет-провайдерами — Решение 2

- Решение 2 аналогично решению 1.
- В решении 1 для передачи трафика используются три метки (VPN, BGP LSP и туннеля LSP), тогда как в решении 2 используются только две метки (VPN и туннеля).
- В решении 1 для генерирования новой метки требуется конфигурирование политики на локальном ASBR. После получения маркированного маршрута BGP от равноправного ASBR локальный ASBR присваивает новую метку для маршрута BGP и анонсирует маршрут PE или RR в той же AS, чтобы можно было установить полный LSP BGP. В решении 2 для присвоения меток маркированным маршрутам BGP требуется конфигурирование MPLS на ASBR. На PE в одной AS с ASBR можно установить LDP LSP до равноправного PE вместо BGP LSP.
- Развертывание RR поддерживается как для решения 1, так и для решения 2.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Вариант C магистральных сетей между интернет-провайдерами — Топология

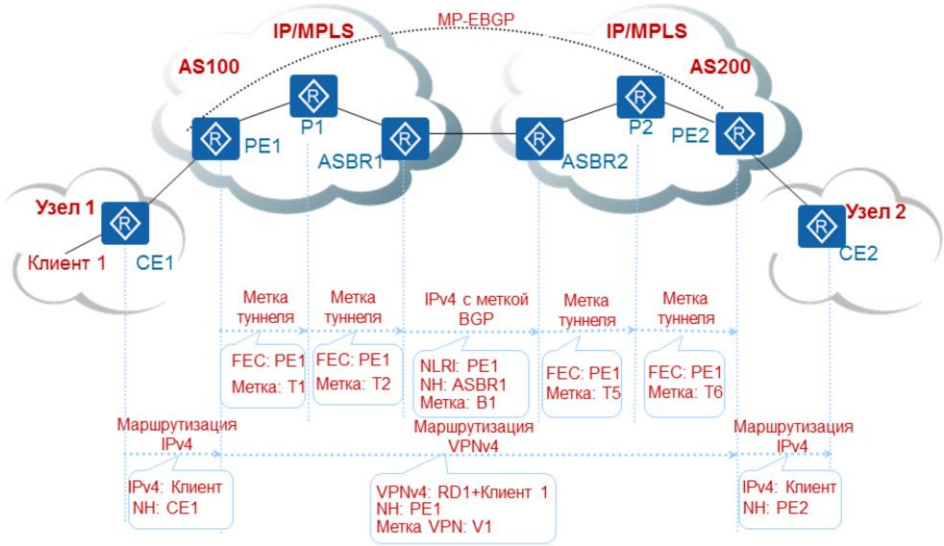


© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

- В данном решении ASBR не хранят и не анонсируют маршруты VPNv4. ASBR обеспечивает только хранение всех маркированных маршрутов до PE и использует EBGP для анонсирования этих маркированных маршрутов равноправному ASBR.
- После получения маркированного маршрута BGP, MPLS LDP на равноправном ASBR запускает генерирование метки для маркированного маршрута BGP и передает метку на соседний узел LDP в AS. Таким образом, на локальном PE можно установить LSP LDP до равноправного PE.
- Для повышения производительности в будущем между VPN RR в разных AS можно установить многоузловой сеанс MP-EBGP. PE в локальной AS должен установить отношения соседства MP-IBGP только с RR в той же AS. VPN RR анонсируют маршруты VPNv4 без изменения атрибута Next_Hop маршрутов, чтобы равноправный PE мог выполнять рекурсивный поиск маршрутов до нужного туннеля во время пересылки трафика.

Вариант C магистральных сетей между интернет-провайдерами — Плоскость управления (без RR)



© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

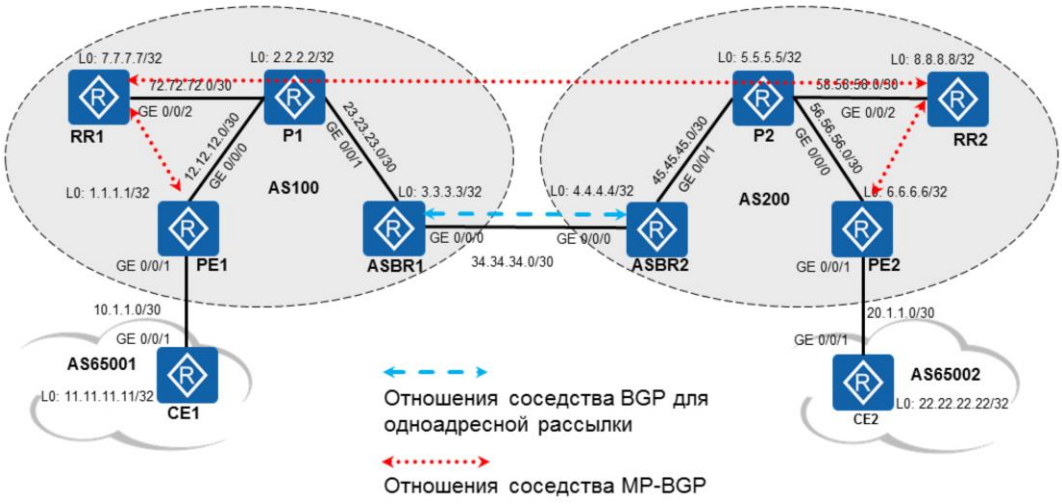
HUAWEI

- Рассмотрим в качестве примера анонсирование маршрутов в одном направлении в плоскости управления. Предположим, что на Узле 1 имеется хост, который называется Клиент 1. Маршрутизатор P каждой AS не имеет маршрутов к равноправному PE в другой AS.
    - В AS100 PE1 использует LDP для назначения P1 метки внешнего туннеля T1, привязанной к маршруту до PE1.
    - В AS100 P1 использует LDP для назначения ASBR1 метки внешнего туннеля T2, привязанной к маршруту до PE1.
    - В AS200 ASBR2 использует LDP для назначения P2 метки внешнего туннеля T3, привязанной к маршруту до ASBR2.
    - В AS200 P2 использует LDP для назначения PE2 метки внешнего туннеля T4, привязанной к маршруту до ASBR2.
    - ASBR1 анонсирует ASBR2 маркированный маршрут IPv4 до PE1 посредством сеанса EBGP. Следующим узлом является ASBR1, а метка является меткой BGP со значением B1.
    - ASBR2 устанавливает LSP для маркированного маршрута BGP и присваивает метку LDP T5 для P2. Затем P2 присваивает метку LDP T6 для PE2.
    - PE1 и PE2 устанавливают между собой сеанс MP-EBGP.
    - CE1 анонсирует PE1 маршрут, предназначенный для Клиента 1, где следующим узлом маршрута является адрес интерфейса CE1.
    - PE1 инкапсулирует полученный маршрут IPv4 к Клиенту 1 в маршрут VPNv4, меняет данные следующего узла на PE1 в соответствующем сообщении MP-EBGP, присваивает

метку VPN V1 для маршрута, а затем анонсирует маршрут в PE2.

- PE2 выполняет обратное преобразование полученного маршрута VPNv4 в маршрут IPv4 для Клиента 1 и анонсирует его CE2, указывая PE2 в качестве следующего узла.

Вариант C магистральных сетей между интернет-провайдерами — Плоскость управления (с RR)

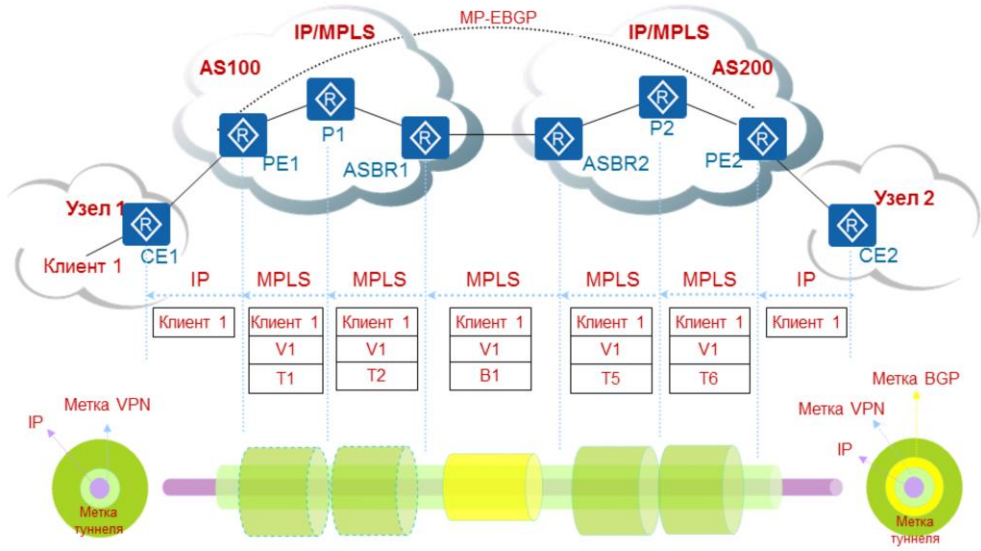


© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

- Отношения соседства VPNv4:
  - PE устанавливает отношения соседства VPNv4 только с RR в одной с ним AS. Локальный RR устанавливает отношения соседства VPNv4 с равноправным RR для передачи маршрутов VPN между AS.
- RR передает только маршруты VPNv4 в плоскости управления и не передает трафик в плоскости передачи.

Вариант C магистральных сетей между интернет-провайдерами — Плоскость передачи



© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

- В качестве примера для иллюстрации процесса в плоскости передачи используем процесс пакетной передачи от CE2 к CE1.
  - CE2 отправляет IP-пакет, предназначенный для Клиента 1, в PE2.
  - Сначала PE2 инкапсулирует полученный IP-пакет с меткой VPN V1. Поскольку PE1 следующего узла пакета не является напрямую подключенным соседним устройством, PE2 выполняет поиск по таблице маршрутизации, находит метку T6, ассоциированную с маршрутом до PE1, а затем добавляет в пакет метку T6.
  - P2 меняет внешнюю метку T6 на T5 и пересылает пакет в ASBR2.
  - ASBR2 удаляет внешнюю метку из полученного пакета, меняет метку T5 на B1 и пересылает пакет в ASBR1.
  - После получения пакета ASBR1 находит назначенную им метку B1, удаляет ее и выполняет поиск по таблице маршрутизации. ASBR1 находит метку T2, ассоциированную с маршрутом до PE1, добавляет метку T2 к вершине стека, а затем пересылает пакет в P1.
  - P1 меняет внешнюю метку T2 на T1 и пересылает пакет в PE1.
  - PE1 удаляет обе метки из полученного пакета и перенаправляет немаркированный IP-пакет в CE1.

Особенности Варианта C магистральных сетей между интернет-провайдерами

- Входной PE и выходной PE напрямую обмениваются маршрутами VPN. Для хранения или передачи маршрутов требуются промежуточные устройства.
- PE обеспечивают только обмен информацией о маршрутизации VPN, тогда как P и ASBR только передают пакеты. Промежуточные устройства должны поддерживать только передачу MPLS, а не сервисов MPLS VPN. ASBR больше не являются проблемными элементами в сети. Таким образом, Вариант C подходит для VPN, которая охватывает несколько AS.
- Кроме того, Вариант C отличается простотой балансирования нагрузки MPLS VPN.
- Недостаток этого режима заключается в том, что управление сквозными соединениями между PE обходится слишком дорого.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Содержание

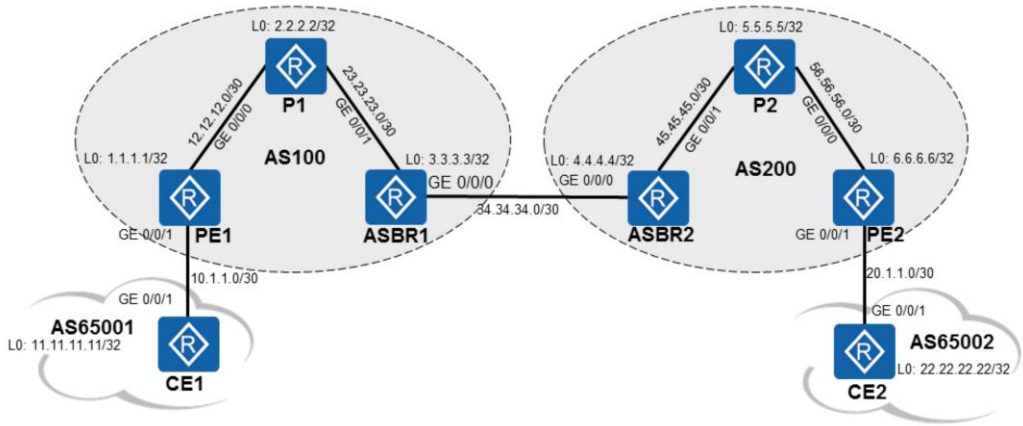
- Общие сведения
- Теоретические основы
- **Конфигурации**
  - Конфигурация решения Варианта A
  - Конфигурация решения Варианта B
  - Конфигурация решения 1 Варианта C
  - Конфигурация решения 2 Варианта C

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Топология Варианта A магистральных сетей между интернет-провайдерами

- Задача конфигурирования: сконфигурировать решение Варианта A для реализации взаимного доступа между CE1 и CE2.

  Примечание: в данном примере в AS используется OSPF.



© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

- В сети, показанной на рисунке, AS100 и AS200 используются для ISP, тогда как две другие AS используются для клиентов. PE1 и ASBR1 принадлежат к AS100, а PE2 и ASBR2 принадлежат к AS200. CE1 и CE2 принадлежат к одной VPN. CE1 подключен к PE1 в AS100, а CE2 подключен к PE2 в AS200.
- В этой топологии показаны IP-адреса, запланированные на каждом маршрутизаторе.

Процедура конфигурирования Варианта A магистральных сетей между интернет-провайдерами

Шаг	Описание	Справочная информация и команды
1	Назначение IP-адреса и маски каждому интерфейсу.	См. раздел «Основные настройки IPv4» в руководстве по соответствующему продукту.
2	Настройка параметров OSPF на каждом PE, P и ASBR через сеть общего пользования.	См. раздел «Настройка основных функций OSPF» в руководстве по соответствующему продукту.
3	Настройка параметров MPLS и LDP на каждом PE, P и ASBR через сеть общего пользования.	mpls mpls lsr-id lsr-id mpls ldp
4	Настройка отношений соседства IBGP между PE1 и ASBR1, а также между PE2 и ASBR2. Настройка отношений соседства MP-IBGP между PE1 и ASBR1, а также между PE2 и ASBR2.	См. раздел «Настройка основных функций BGP» в руководстве по соответствующему продукту. ipv4-family vpnv4 peer { group-name | ipv4-address | ipv6-address } enable
5	Настройка экземпляра VPN с RD и несколькими RT на каждом PE и ASBR.	ip vpn-instance vpn-instance-name route-distinguisher route-distinguisher vpn-target vpn-target [both |export-extcommunity | importextcommunity]
6	Настройка привязки интерфейса AC к экземпляру VPN на каждом PE и ASBR.	ip binding vpn-instance vpn-instance-name
7	Настройка отношений соседства EBGP для экземпляра VPN на каждом PE и ASBR.	См. раздел «Настройка основных функций BGP» в руководстве по соответствующему продукту.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Пример конфигурирования Варианта A магистральных сетей между интернет-провайдерами (1)

1. Определение топологии и настройка IP-адресов.
   - Выберите тестовую топологию на основании сетевых требований и настройте IP-адреса.
2. Настройка OSPF.
   - Настройте параметры OSPF на PE1, P1, ASBR1, PE2, P2 и ASBR2.
3. Настройка параметров MPLS и LDP на каждом PE, P и ASBR через сеть общего пользования.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

- Задайте топологию, показанную на предыдущем слайде, и настройте IP-адреса интерфейсам на основе топологии.
  - На CE1 настройте IP-адреса интерфейсам Loopback 0 и GE 0/0/1.
  - На PE1 настройте IP-адреса интерфейсам Loopback 0 и GE 0/0/0.
  - На P1 настройте IP-адреса интерфейсам Loopback 0, GE 0/0/0 и GE 0/0/1.
  - На ASBR1 настройте IP-адреса интерфейсам Loopback 0 и GE 0/0/1.
  - На ASBR2 настройте IP-адреса интерфейсам Loopback 0 и GE 0/0/1.
  - На P2 настройте IP-адреса интерфейсам Loopback 0, GE 0/0/0 и GE 0/0/1.
  - На PE2 настройте IP-адреса интерфейсам Loopback 0 и GE 0/0/0.
  - На CE2 настройте IP-адреса интерфейсам Loopback 0 и GE 0/0/1.
- Настройте параметры OSPF на PE1, P1, ASBR1, PE2, P2 и ASBR2.
  - Включите для PE1 анонсирование маршрутов в сетевые сегменты 1.1.1.1/32 и 12.12.12.0/30.
  - Включите для P1 анонсирование маршрутов в сетевые сегменты 2.2.2.2/32, 12.12.12.0/30 и 23.23.23.0/30.
  - Включите для ASBR1 анонсирование маршрутов в сетевые сегменты 3.3.3.3/32 и 23.23.23.0/30.
  - Включите для ASBR2 анонсирование маршрутов в сетевые сегменты 4.4.4.4/32 и 45.45.45.0/30.
  - Включите для P2 анонсирование маршрутов в сетевые сегменты 5.5.5.5/32,

45.45.45.0/30 и 56.56.56.0/30.

- Включите для PE2 анонсирование маршрутов в сетевые сегменты 6.6.6.6/32 и 56.56.56.0/30.

Пример конфигурирования Варианта A магистральных сетей между интернет-провайдерами (2)

3. Настройка параметров MPLS и LDP на каждом PE, P и ASBR через сеть общего пользования.

```
<PE1>system-view
[PE1]mpls lsr-id 1.1.1.1
[PE1]mpls
Info: Mpls starting, please wait... OK!
[PE1-mpls]mpls ldp
[PE1-mpls-ldp]quit
[PE1]interface GigabitEthernet0/0/0
[PE1-GigabitEthernet0/0/0]mpls
[PE1-GigabitEthernet0/0/0]mpls ldp
[PE1-GigabitEthernet0/0/0]quit
```

- Выполните такие же действия для P1, P2, PE2, ASBR1 и ASBR2.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Пример конфигурирования Варианта A магистральных сетей между интернет-провайдерами (3)

- После завершения настроек между P и PE, а также между P и ASBR в одной AS установятся сеансы LDP на равноправной основе. Выполните команду **display mpls ldp session** на каждом P. Результаты выполнения команды свидетельствуют о том, что сеанс имеет статус **Operational**.
- Далее в качестве примера приведены результаты выполнения команды на P1:

```
[P1]display mpls ldp session
 LDP Session(s) in Public Network
 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
 A '*' before a session means the session is being deleted.
 ------------------------------------------------------------------------------
 PeerID            Status      LAM  SsnRole  SsnAge       KASent/Rcv
 ------------------------------------------------------------------------------
 1.1.1.1:0         Operational DU   Active   0000:02:21   568/568
 3.3.3.3:0         Operational DU   Passive  0000:02:21   567/567
 ------------------------------------------------------------------------------
 TOTAL: 2 session(s) Found.
```

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Пример конфигурирования Варианта A магистральных сетей между интернет-провайдерами (4)

4. Настройка отношений соседства IBGP и MP-IBGP между PE1 и ASBR1, а также между PE2 и ASBR2.

```
[PE1]bgp 100
[PE1-bgp]peer 3.3.3.3 as-number 100
//Настройка отношений соседства IBGP между PE1 и ASBR1.
[PE1-bgp]peer 3.3.3.3 connect-interface loopback 0
//Настройка интерфейса Loopback 0, используемого для установления отношений соседства.
[PE1-bgp]ipv4-family vpnv4
//Переход в режим BGP VPNv4.
[PE1-bgp-af-vpnv4]peer 3.3.3.3 enable
//Настройка отношений соседства MP-IBGP между PE1 и ASBR1.
[PE1-bgp-af-vpnv4]quit
```

- Выполните такие же действия для PE2, ASBR1 и ASBR2.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Пример конфигурирования Варианта A магистральных сетей между интернет-провайдерами (5)

- Проверка настроек:

```
[PE1] display bgp vpnv4 all peer
BGP local router ID : 1.1.1.1
Local AS number : 100 Total number of peers : 1
Peers in established state : 1
Peer            V    AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv
3.3.3.3         4   100        3        7     0 00:01:36  Established       0
```

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Пример конфигурирования Варианта A магистральных сетей между интернет-провайдерами (6)

5. Настройка экземпляра VPN на каждом PE и ASBR.

```
[PE1]ip vpn-instance huawei
[PE1-vpn-instance-huawei]route-distinguisher 100:1
[PE1-vpn-instance-huawei]vpn-target 100:1 both
[PE1-vpn-instance-huawei]quit
```

```
[ASBR1]ip vpn-instance huawei
[ASBR1-vpn-instance-huawei]route-distinguisher 100:1
[ASBR1-vpn-instance-huawei]vpn-target 100:1 both
[ASBR1-vpn-instance-huawei]quit
```

- Настройте PE2 аналогично PE1, а также настройте ASBR2 аналогично ASBR1.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Пример конфигурирования Варианта A магистральных сетей между интернет-провайдерами (7)

6. Настройка привязки интерфейса AC к экземпляру VPN на каждом PE и ASBR.

```
[PE1]interface GigabitEthernet0/0/1
[PE1-GigabitEthernet0/0/1]ip binding vpn-instance huawei
[PE1-GigabitEthernet0/0/1]ip address 10.1.1.2 30
[PE1-GigabitEthernet0/0/1]quit
```

```
[ASBR1] interface GigabitEthernet0/0/0
[ASBR1-GigabitEthernet0/0/0]ip binding vpn-instance huawei
[ASBR1-GigabitEthernet0/0/0]ip address 34.34.34.1 30
[ASBR1-GigabitEthernet0/0/0]quit
//Настройка привязки экземпляра VPN к интерфейсу, который подключается к ASBR2 (ASBR1 считает ASBR2 своим CE).
```

- Настройте PE2 аналогично PE1, а также настройте ASBR2 аналогично ASBR1.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Пример конфигурирования Варианта A магистральных сетей между интернет-провайдерами (8)

7. Настройка отношений соседства EBGP для экземпляра VPN на каждом PE и ASBR.

```
[PE1]bgp 100
[PE1-bgp]ipv4-family vpn-instance huawei
[PE1-bgp-huawei]peer 10.1.1.1 as-number 65001
//Настройка отношений соседства EBGP между PE1 и CE1.
```

```
[CE1]bgp 65001
[CE1-bgp]peer 10.1.1.2 as-number 100
[CE1-bgp]network 11.11.11.11 32
```

```
[ASBR1]bgp 100
[ASBR1-bgp]ipv4-family vpn-instance huawei
[ASBR1-bgp-huawei]peer 34.34.34.2 as-number 200
//Настройка отношений соседства EBGP между ASBR1 и ASBR2.
```

- Настройте PE2 аналогично PE1, CE2 аналогично CE1, а также ASBR2 аналогично ASBR1.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Пример конфигурирования Варианта A магистральных сетей между интернет-провайдерами (9)

- Проверка настроек:

```
[PE1]display bgp vpnv4 vpn-instance huawei peer
BGP local router ID : 1.1.1.1
Local AS number : 100
Total number of peers : 1
Peers in established state : 1
Peer       V  AS  MsgRcvd  MsgSent  OutQ  Up/Down     State       PrefRcv
10.1.1.1   4 65001       10         10     0 00:07:10 Established       0
```

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Проверка результатов конфигурирования Варианта A магистральных сетей между интернет-провайдерами (1)

- После завершения приведенных выше настроек CE1 и CE2 определяют маршруты к loopback-интерфейсам друг друга и успешно осуществляют проверку связи с помощью команды ping.
  - Далее в качестве примера приведены результаты выполнения команды на CE1:

```
[CE1]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 6        Routes : 6

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

10.1.1.0/30         Direct  0    0           D   10.1.1.1        GigabitEthernet0/0/1
10.1.1.1/32         Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
11.11.11.11/32      Direct  0    0           D   127.0.0.1       LoopBack0
22.22.22.22/32      EBGP    255  0           D   10.1.1.2        GigabitEthernet0/0/1
127.0.0.0/8         Direct  0    0           D   127.0.0.1       InLoopBack0
127.0.0.1/32        Direct  0    0           D   127.0.0.1       InLoopBack0
```

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Проверка результатов конфигурирования Варианта A магистральных сетей между интернет-провайдерами (2)

- Выполните команду **display ip routing-table vpn-instance** на ASBR, чтобы проверить таблицу VPN-маршрутизации.

```
[ASBR1]dis ip routing-table vpn-instance huawei
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: huawei
         Destinations : 4        Routes : 4

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

11.11.11.11/32      IBGP    255  0           RD  1.1.1.1         GigabitEthernet0/0/1
22.22.22.22/32      EBGP    255  0           D   34.34.34.2      GigabitEthernet0/0/0
34.34.34.0/30       Direct  0    0           D   34.34.34.1      GigabitEthernet0/0/0
34.34.34.1/32       Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/0
```

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Проверка результатов конфигурирования Варианта A магистральных сетей между интернет-провайдерами (3)

- Выполните команду **display bgp vpnv4 all routing-table** на ASBR для проверки маршрутов VPNv4.

```
[ASBR1]dis bgp vpnv4 all routing-table

 BGP Local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total number of routes from all PE: 2
 Route Distinguisher: 100:1
        Network            NextHop      MED      LocPrf    PrefVal      Path/Ogn

 *>i  11.11.11.11/32      1.1.1.1        0         100         0         65001i
 *>   22.22.22.22/32      34.34.34.2                           0         200 65002i

 VPN-Instance huawei, Router ID 3.3.3.3:
 Total Number of Routes: 2
        Network            NextHop      MED      LocPrf    PrefVal      Path/Ogn
 *>i  11.11.11.11/32      1.1.1.1        0         100         0         65001i
 *>   22.22.22.22/32      34.34.34.2                           0         200 65002i
```

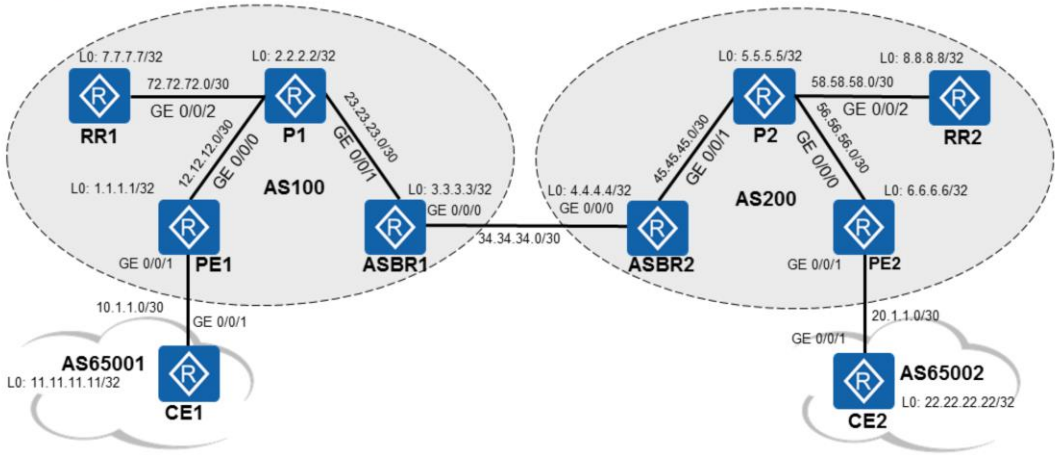
© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Содержание

- Общие сведения
- Теоретические основы
- **Конфигурации**
  - Конфигурация решения Варианта A
  - Конфигурация решения Варианта B
  - Конфигурация решения 1 Варианта C
  - Конфигурация решения 2 Варианта C

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Топология Варианта B магистральных сетей между интернет-провайдерами



- Задача конфигурирования: сконфигурировать решение Варианта B для реализации взаимного доступа между CE1 и CE2.

  Примечание: в данном примере в AS используется OSPF.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

- В этом примере RR1 и RR2 работают в AS100 и AS200 соответственно. В каждой AS PE и ASBR устанавливают отношения соседства BGP с RR, а RR отражает маршруты VPN.

Процедура конфигурирования Варианта B магистральных сетей между интернет-провайдерами (1)

Шаг	Описание	Справочная информация и команды
1	Назначение IP-адреса и маски каждому интерфейсу.	См. раздел «Основные настройки IPv4» в руководстве по соответствующему продукту.
2	Настройка параметров OSPF на каждом PE, P, ASBR и RR через сеть общего пользования.	См. раздел «Настройка основных функций OSPF» в руководстве по соответствующему продукту.
3	Настройка параметров MPLS и LDP на каждом PE, P и ASBR через сеть общего пользования.	mpls mpls lsr-id lsr-id mpls ldp
4	Настройка отношений соседства IBGP между PE и RR, а также между ASBR и RR в каждой AS. Включение отношений соседства MP-IBGP в режиме VPNv4 на каждом PE, RR и ASBR.	См. раздел «Настройка основных функций BGP» в руководстве по соответствующему продукту. ipv4-family vpnv4 peer { group-name | ipv4-address | ipv6-address } enable
5	Включение функции отражения маршрутов VPN на RR1 и RR2.	ipv4-family vpnv4 peer { group-name | ipv4-address | ipv6-address } reflect-client
6	Настройка экземпляра VPN с RD и несколькими RT на каждом PE.	ip vpn-instance vpn-instance-name route-distinguisher route-distinguisher vpn-target vpn-target [both |export-extcommunity | importextcommunity]

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Процедура конфигурирования Варианта B магистральных сетей между интернет-провайдерами (2)

Шаг	Описание	Справочная информация и команды
7	Настройка привязки интерфейса AC к экземпляру VPN на каждом PE.	ip binding vpn-instance vpn-instance-name
8	Настройка отношений соседства EBGP с подключенным CE в экземпляре VPN на каждом PE.	См. раздел «Настройка основных функций BGP» в руководстве по соответствующему продукту.
9	Включение MPLS на интерфейсах, обеспечивающих соединение с ASBR1 и ASBR2.	mpls
10	Настройка отношений соседства MP-EBGP между ASBR1 и ASBR2 в режиме VPNv4.	ipv4-family vpnv4 peer { group-name | ipv4-address | ipv6-address } enable undo policy vpn-target
Примечания	1. Включите MPLS вместо LDP на ASBR1 и ASBR2. 2. Вариант B требует соответствия объектов назначения VPN экземпляров VPN на PE в разных AS друг другу. 3. Настройка экземпляров VPN и привязки их к интерфейсам на ASBR1 и ASBR2 не требуется. 4. На ASBR1, ASBR2, RR1 и RR2 необходимо выполнить следующие специальные настройки: выполните команду **undo policy vpn-target** в режиме VPNv4 address family.	

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Пример конфигурирования Варианта B магистральных сетей между интернет-провайдерами (1)

- Шаги 1–4 аналогичны шагам 1–4 в Варианте A.

5. Включение на каждом RR функции отражения маршрутов VPN и отключение на каждом RR функции фильтрации полученных маршрутов VPN на основе объектов назначения VPN.

```
[RR1-bgp]ipv4-family vpnv4
[RR1-bgp-af-vpnv4]undo policy vpn-target
[RR1-bgp-af-vpnv4]peer 1.1.1.1 reflect-client
[RR1-bgp-af-vpnv4]peer 3.3.3.3 reflect-client
```

6. Настройка экземпляра VPN с RD (100:1) и несколькими RT (100:1) на каждом PE.

```
[PE1]ip vpn-instance huawei
[PE1-vpn-instance-huawei]route-distinguisher 100:1
[PE1-vpn-instance-huawei]vpn-target 100:1 both
[PE1-vpn-instance-huawei]quit
```

- Настройте RR2 аналогично RR1, а также настройте PE2 аналогично PE1.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Пример конфигурирования Варианта B магистральных сетей между интернет-провайдерами (2)

7. Настройка привязки интерфейса AC к экземпляру VPN на каждом PE.

```
[PE1]interface GigabitEthernet0/0/1
[PE1-GigabitEthernet0/0/1]ip binding vpn-instance huawei
[PE1-GigabitEthernet0/0/1]ip address 10.1.1.2 30
[PE1-GigabitEthernet0/0/1]quit
```

- Настройте PE2 аналогично PE1.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Пример конфигурирования Варианта B магистральных сетей между интернет-провайдерами (3)

8. Настройка отношений соседства EBGP с подключенным CE в экземпляре VPN на каждом PE.

```
[PE1]bgp 100
[PE1-bgp]ipv4-family vpn-instance huawei
[PE1-bgp-huawei]peer 10.1.1.1 as-number 65001
//Настройка отношений соседства EBGP между PE1 и CE1.
```

```
[CE1]bgp 65001
[CE1-bgp]peer 10.1.1.2 as-number 100
[CE1-bgp]network 11.11.11.11 32
```

- Настройте PE2 аналогично PE1, а также настройте CE2 аналогично CE1.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Пример конфигурирования Варианта B магистральных сетей между интернет-провайдерами (4)

9. Включение MPLS на интерфейсах, обеспечивающих соединение с ASBR1 и ASBR2.

```
[ASBR1]interface GigabitEthernet0/0/0
[ASBR1-GigabitEthernet0/0/0]ip address 34.34.34.1 24
[ASBR1-GigabitEthernet0/0/0]mpls
//Включение MPLS на интерфейсе ASBR1, который обеспечивает соединение с ASBR2.
```

- Настройте ASBR2 аналогично ASBR1.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Пример конфигурирования Варианта B магистральных сетей между интернет-провайдерами (5)

10. Настройка отношений соседства MP-EBGP между двумя ASBR в режиме VPNv4.

```
[ASBR1]bgp 100
[ASBR1-bgp]peer 34.34.34.2 as-number 200
[ASBR1-bgp]ipv4-family vpnv4
[ASBR1-bgp-af-vpnv4]peer 34.34.34.2 enable
//Установление отношений соседства MP-EBGP с ASBR2.
[ASBR1-bgp-af-vpnv4]undo policy vpn-target
//Отключение на ASBR фильтрации полученных маршрутов VPNv4 на основе объектов назначения VPN.
```

- Настройте ASBR2 аналогично ASBR1.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Проверка результатов конфигурирования Варианта B магистральных сетей между интернет-провайдерами (1)

- После завершения приведенных выше настроек CE1 и CE2 определяют маршруты к loopback-интерфейсам друг друга и успешно осуществляют проверку связи с помощью команды ping.
- Далее в качестве примера приведены результаты выполнения команды на CE1:

```
[CE1]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 6        Routes : 6

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

10.1.1.0/30         Direct  0    0           D   10.1.1.1        GigabitEthernet0/0/1
10.1.1.1/32         Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
11.11.11.11/32      Direct  0    0           D   127.0.0.1       LoopBack0
22.22.22.22/32      EBGP    255  0           D   10.1.1.2        GigabitEthernet0/0/1
127.0.0.0/8         Direct  0    0           D   127.0.0.1       InLoopBack0
127.0.0.1/32        Direct  0    0           D   127.0.0.1       InLoopBack0
```

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Проверка результатов конфигурирования Варианта B магистральных сетей между интернет-провайдерами (2)

- Выполните команду **display bgp vpnv4 all routing-table** на ASBR для проверки маршрутов VPNv4.

```
[ASBR1]dis bgp vpnv4 all routing-table
 BGP Local router ID is 23.23.23.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total number of routes from all PE: 2
 Route Distinguisher: 100:1

        Network         NextHop        MED        LocPrf    PrefVal     Path/Ogn
*>i   11.11.11.11/32     1.1.1.1         0          100        0         65001i
*>    22.22.22.22/32     34.34.34.2                             0         200 65002i
```

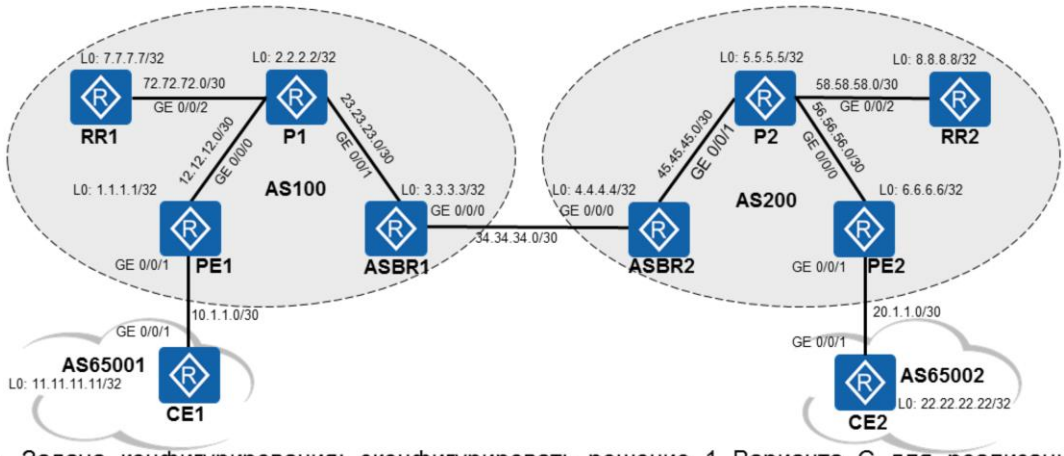
© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Содержание

- Общие сведения
- Теоретические основы
- **Конфигурации**
  - Конфигурация решения Варианта A
  - Конфигурация решения Варианта B
  - Конфигурация решения 1 Варианта C
  - Конфигурация решения 2 Варианта C

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Топология Варианта C магистральных сетей между интернет-провайдерами (Решение 1)



- Задача конфигурирования: сконфигурировать решение 1 Варианта C для реализации взаимного доступа между CE1 и CE2.
- Примечание: в данном примере в AS используется OSPF.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

- В сети, показанной на рисунке, AS100 и AS200 используются для ISP, тогда как две другие AS используются для клиентов. PE1, P1, RR1 и ASBR1 принадлежат к AS100. PE2, P2, RR2 и ASBR2 принадлежат к AS200. CE1 и CE2 принадлежат к одной VPN. CE1 подключен к PE1 в AS100, а CE2 подключен к PE2 в AS200.
- В этой топологии показаны IP-адреса, запланированные на каждом маршрутизаторе.
- В качестве примера используется решение 1 Варианта C. PE1 и PE2 могут устанавливать отношения соседства MP-EBGP друг с другом для передачи VPN-маршрутов между AS без привлечения RR. В противном случае RR1 и RR2 устанавливают отношения соседства MP-EBGP для передачи VPN-маршрутов между AS. В этом случае отношения соседства MP-IBGP устанавливаются между PE1 и RR1, а также между PE2 и RR2. В этом примере для реализации решения 1 Варианта C используются RR.

Процедура конфигурирования решения 1 для Варианта C магистральных сетей между интернет-провайдерами (1)

Шаг	Описание	Справочная информация и команды
1	Назначение IP-адреса и маски каждому интерфейсу.	См. раздел «Основные настройки IPv4» в руководстве по соответствующему продукту.
2	Настройка параметров OSPF на каждом PE, P, RR и ASBR через сеть общего пользования.	См. раздел «Настройка основных функций OSPF» в руководстве по соответствующему продукту.
3	Настройка параметров MPLS и LDP на каждом PE, P и ASBR через сеть общего пользования.	mpls mpls lsr-id lsr-id mpls ldp
4	Настройка отношений соседства IBGP между каждым PE, P и ASBR с RR, а также настройка PE, P и ASBR в качестве клиентов RR в каждой AS.	См. раздел «Настройка основных функций BGP» в руководстве по соответствующему продукту.
5	Настройка отношений соседства EBGP между ASBR1 и ASBR2.	См. раздел «Настройка основных функций BGP» в руководстве по соответствующему продукту.
6	Настройка экземпляра VPN с RD (100:1) и несколькими RT (100:1) на каждом PE.	ip vpn-instance vpn-instance-name route-distinguisher route-distinguisher vpn-target vpn-target [both |export-extcommunity | importextcommunity]
7	Настройка привязки интерфейса AC к экземпляру VPN на каждом PE.	ip binding vpn-instance vpn-instance-name
8	Настройка отношений соседства EBGP с подключенным CE в экземпляре VPN на каждом PE.	См. «Конфигурирование BGP».
9	Настройка многоузловых отношений соседства MP-EBGP между RR1 и RR2 в режиме VPNv4. Настройка отношений соседства MP-IBGP между PE1 и RR1 в режиме VPNv4. Настройка отношений соседства MP-IBGP между PE2 и RR2 в режиме VPNv4. Отключение на каждом RR функции изменения атрибута Next_Hop в анонсируемых маршрутах.	peer { group-name | ipv4-address | ipv6-address } ebgp-max-hop [hop-count] ipv4-family vpnv4 peer { group-name | ipv4-address | ipv6-address } enable peer next-hop-invariable

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Процедура конфигурирования решения 1 для Варианта C магистральных сетей между интернет-провайдерами (2)

Шаг	Описание	Справочная информация и команды
10	Включение функции обмена маркированными маршрутами IPv4 между PE и RR в каждой AS, между RR и ASBR в каждой AS и между ASBR в разных AS.	peer { group-name | ipv4-address } label-route-capability
11	Создание политики маршрутизации и применение ее к маршрутам, предназначенным для анонсирования локальным ASBR удаленному ASBR, и маршрутам, предназначенным для анонсирования локальным ASBR локальному RR.	route-policy route-policy-name { permit | deny } node node peer { group-name | ipv4-address | ipv6-address } route-policy route-policy-name { import | export }
Примечания	1. Включите MPLS на ASBR1 и ASBR2. Использование LDP по усмотрению. 2. Настройка экземпляров VPN и привязки их к интерфейсам на ASBR1 и ASBR2 не требуется. 3. Настройте параметры обмена маркированными маршрутами IPv4: Между PE1 и RR1 Между RR1 и ASBR1 Между PE2 и RR2 Между RR2 и ASBR2 Между ASBR1 и ASBR2 4. Убедитесь, что покальный RR не меняет атрибут Next_Hop маршрутов VPN при анонсировании их удаленному RR. Также убедитесь, что удаленный RR не меняет атрибут Next_Hop полученных маршрутов VPN при анонсировании их в PE той же AS. 5. Настройте политику маршрутизации на каждом ASBR1 и ASBR2, чтобы обеспечить, что: Локальный ASBR может присваивать метки MPLS маршрутам, полученным от RR в той же AS, при анонсировании их в ASBR равноправной AS. ASBR может присваивать новые метки MPLS маркированным маршрутам IPv4 при анонсировании их RR в той же AS.	

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Пример конфигурирования решения 1 для Варианта C магистральных сетей между интернет-провайдерами (1)

- Шаги 1–3 аналогичны шагам 1–3 в Варианте A.

4. Настройка отношений соседства IBGP между каждым PE, P и ASBR с RR, а также настройка PE, P и ASBR в качестве клиентов RR в каждой AS.

```
[RR1-bgp]peer 1.1.1.1 as-number 100
[RR1-bgp]peer 1.1.1.1 connect-interface Loopback0
[RR1-bgp]peer 1.1.1.1 reflect-client
[RR1-bgp]peer 2.2.2.2 as-number 100
[RR1-bgp]peer 2.2.2.2 connect-interface Loopback0
[RR1-bgp]peer 2.2.2.2 reflect-client
[RR1-bgp]peer 3.3.3.3 as-number 100
[RR1-bgp]peer 3.3.3.3 connect-interface Loopback0
[RR1-bgp]peer 3.3.3.3 reflect-client
```

5. Настройка отношений соседства EBGP между ASBR1 и ASBR2.

```
[ASBR1-bgp]peer 34.34.34.2 as-number 200
```

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

- На шаге 4 настройте RR2 аналогично RR1. Более подробная информация о настройке PE, P и ASBR приводится в разделе «Настройка основных функций BGP» в руководстве по соответствующему продукту.
- На шаге 5 настройте ASBR2 аналогично ASBR1.
- Установите отношения соседства EBGP для одноадресной передачи между ASBR, чтобы локальный ASBR мог анонсировать маршруты до адресов loopback-интерфейсов локального RR и PE в равноправный ASBR.
- При анонсировании маршрутов до адресов loopback-интерфейсов RR1 и PE1 в ASBR2 локальный ASBR присваивает метки MPLS этим маршрутам. При анонсировании маршрутов до адресов loopback-интерфейсов RR1 и PE1 в RR2 ASBR2 присваивает новые метки MPLS этим маршрутам.
- После установления отношений соседства IBGP между ASBR и RR, а также между PE и RR в одной AS включите функцию обмена метками на равноправных узлах IBGP.
- В той же AS установите отношения соседства IPv4 между каждым ASBR, P и PE с RR.
  - Локальный ASBR выясняет loopback-маршрут до RR от равноправного ASBR посредством отношений соседства IPv4 и анонсирует loopback-маршрут локальному RR, чтобы локальный RR мог установить отношения соседства VPNv4 с равноправным RR.
  - Локальный ASBR выясняет loopback-маршруты равноправного RR и PE от равноправного ASBR посредством отношений соседства IPv4 и анонсирует их локальному RR. Далее локальный RR отражает loopback-маршруты в локальный маршрутизатор P для рекурсивного поиска маршрутов BGP.
  - Локальный ASBR выясняет loopback-маршруты равноправного RR и PE от

равноправного ASBR посредством отношений соседства IPv4 и анонсирует их локальному RR. Затем локальный RR отражает loopback-маршруты в локальный PE, чтобы PE в разных AS могли устанавливать BGP LSP.

Пример конфигурирования решения 1 для Варианта C магистральных сетей между интернет-провайдерами (2)

6. Настройка экземпляра VPN с RD (100:1) и несколькими RT (100:1) на каждом PE.

```
[PE1]ip vpn-instance huawei
[PE1-vpn-instance-huawei]route-distinguisher 100:1
[PE1-vpn-instance-huawei-af-ipv4]vpn-target 100:1 both
```

7. Настройка привязки интерфейса AC к экземпляру VPN на каждом PE.

```
[PE1]interface GigabitEthernet0/0/1
[PE1-GigabitEthernet0/0/1]ip binding vpn-instance huawei
[PE1-GigabitEthernet0/0/1]ip address 10.1.1.2 30
[PE1-GigabitEthernet0/0/1]quit
```

- Настройте PE2 аналогично PE1.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Пример конфигурирования решения 1 для Варианта C магистральных сетей между интернет-провайдерами (3)

8. Настройка отношений соседства EBGP с подключенным CE в экземпляре VPN на каждом PE.

```
[PE1]bgp 100
[PE1-bgp]ipv4-family vpn-instance huawei
[PE1-bgp-huawei]peer 10.1.1.1 as-number 65001
//Настройка отношений соседства EBGP между PE1 и CE1.
```

```
[CE1]bgp 65001
[CE1-bgp]peer 10.1.1.2 as-number 100
[CE1-bgp]network 11.11.11.11 32
```

- Настройте PE2 аналогично PE1, а также настройте CE2 аналогично CE1.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Пример конфигурирования решения 1 для Варианта C магистральных сетей между интернет-провайдерами (4)

9. Настройка отношений соседства MP-EBGP между RR1 и RR2 в режиме VPNv4 и отключение на RR функции изменения атрибута Next_Hop анонсируемых маршрутов VPN.

```
[RR1]bgp 100
[RR1-bgp]peer 8.8.8.8 as-number 200
[RR1-bgp]peer 8.8.8.8 connect-interface LoopBack 0
[RR1-bgp]peer 8.8.8.8 ebgp-max-hop 10
[RR1-bgp]ipv4-family vpnv4
[RR1-bgp-af-vpnv4]peer 8.8.8.8 enable
[RR1-bgp-af-vpnv4]peer 8.8.8.8 next-hop-invariable
[RR1-bgp-af-vpnv4]undo policy vpn-target
```

- В каждой AS настройте отношения соседства MP-IBGP между PE и RR в режиме VPNv4 и отключите на RR функцию изменения атрибута Next_Hop анонсируемых маршрутов VPN.

```
[RR1]bgp 100
[RR1-bgp]peer 1.1.1.1 as-number 100
[RR1-bgp]peer 1.1.1.1 connect-interface LoopBack 0
[RR1-bgp]ipv4-family vpnv4
[RR1-bgp-af-vpnv4]peer 1.1.1.1 enable
[RR1-bgp-af-vpnv4]peer 1.1.1.1 next-hop-invariable
```

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

- Более подробная информация об установлении отношений соседства MP-IBGP между PE2 и RR2 приводится в разделе «Конфигурация между PE1 и RR1».
- Выполнение команды **undo policy vpn-target** в Варианте C аналогично выполнению данной команды в Варианте B. В обоих случаях команда отключает на RR функцию фильтрации маршрутов на основе RT.
- Выполнение команды **peer** *X.X.X.X* **next-hop-invariable** обеспечивает, что соседний PE сможет осуществлять рекурсивный поиск маршрутов до BGP LSP, выделенного для локального PE в процессе передачи трафика.
- Установите отношения соседства MP-EBGP между RR в режиме VPNv4 и отключите на локальном RR функцию изменения атрибута Next_Hop маршрутов, анонсируемых соседнему RR. Таким образом, следующим узлом маршрута VPNv4, который получит PE, будет являться локальный PE.
- Установите отношения соседства MP-IBGP между RR и PE в режиме VPNv4 и отключите на RR функцию изменения атрибута Next_Hop маршрутов, анонсируемых локальному RR. Таким образом, следующим узлом маршрута VPNv4, который получит PE, будет являться равноправный PE.
- PE устанавливает отношения соседства VPNv4 только с RR в одной с ним AS. Локальный RR устанавливает отношения соседства VPNv4 с равноправным RR для передачи маршрутов VPN между AS.

Пример конфигурирования решения 1 для Варианта C магистральных сетей между интернет-провайдерами (5)

10. Включение функции обмена маркированными маршрутами IPv4 между PE и RR в каждой AS, между RR и ASBR в каждой AS и между ASBR в разных AS.

```
[PE1]bgp 100
[PE1-bgp]peer 7.7.7.7 as-number 100
[PE1-bgp]peer 7.7.7.7 label-route-capability
```

```
[RR1]bgp 100
[RR1-bgp]peer 1.1.1.1 as-number 100
[RR1-bgp]peer 1.1.1.1 label-route-capability
[RR1-bgp]peer 3.3.3.3 as-number 100
[RR1-bgp]peer 3.3.3.3 label-route-capability
```

```
[ASBR1]bgp 100
[ASBR1-bgp]peer 7.7.7.7 as-number 100
[ASBR1-bgp]peer 7.7.7.7 label-route-capability
[ASBR1-bgp]peer 34.34.34.2 as-number 200
[ASBR1-bgp]peer 34.34.34.2 label-route-capability
```

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

- Настройки PE2, RR2 и ASBR2 приведены в конфигурациях для PE1, RR1 и ASBR1 соответственно.

Пример конфигурирования решения 1 для Варианта C магистральных сетей между интернет-провайдерами (6)

11. Создание политики маршрутизации и применение ее к маршрутам, предназначенным для анонсирования локальным ASBR удаленному ASBR, и маршрутам, предназначенным для анонсирования локальным ASBR локальному RR.

```
[ASBR1]interface GigabitEthernet0/0/0
[ASBR1-GigabitEthernet0/0/0]ip address 34.34.34.1 30
[ASBR1-GigabitEthernet0/0/0]mpls
[ASBR1-GigabitEthernet0/0/0]quit
[ASBR1]route-policy policy1 permit node 10
[ASBR1-route-policy]apply mpls-label
//Присвоение меток MPLS маршрутам, которые соответствуют условиям фильтрации.
[ASBR1-route-policy]quit
[ASBR1]route-policy policy2 permit node 10
[ASBR1-route-policy]if-match mpls-label
[ASBR1-route-policy]apply mpls-label
//Присвоение меток MPLS маркированным маршрутам IPv4 для замены исходных меток MPLS новыми.
[ASBR1-route-policy]quit
//Создание двух политик маршрутизации на ASBR1.
```

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Пример конфигурирования решения 1 для Варианта C магистральных сетей между интернет-провайдерами (7)

```
[ASBR1]bgp 100
[ASBR1-bgp]peer 7.7.7.7 route-policy policy2 export
```
//Применение для ASBR1 политики маршрутизации к маршрутам, анонсируемым в RR1. Если анонсируемые маршруты являются маркированными маршрутами IPv4, ASBR1 присвоит им новые метки MPLS.

```
[ASBR1-bgp]peer 34.34.34.2 as-number 200
[ASBR1-bgp]peer 34.34.34.2 route-policy policy1 export
[ASBR1-bgp]peer 34.34.34.2 label-route-capability
[ASBR1-bgp]quit
```
//Применение для ASBR1 политики маршрутизации к маршрутам, анонсируемым в ASBR2.
При анонсировании в ASBR2 маршрутов, полученных от RR1, ASBR1 будет присваивать им метки MPLS.

```
[ASBR1]bgp 100
[ASBR1-bgp]network 1.1.1.1 32
[ASBR1-bgp]network 7.7.7.7 32
```
//Настройка на ASBR1 параметров анонсирования в ASBR2 маршрутов, предназначенных для loopback-интерфейсов PE1 и RR1, чтобы ASBR2 мог анонсировать маршруты в RR2 и PE2.
```
[ASBR1-bgp]quit
```

- Настройте ASBR2 аналогично ASBR1.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Проверка результатов конфигурирования решения 1 Варианта C магистральных сетей между интернет-провайдерами (1)

- После завершения приведенных выше настроек CE1 и CE2 определяют маршруты к loopback-интерфейсам друг друга и успешно осуществляют проверку связи с помощью команды ping.
- Далее в качестве примера приведены результаты выполнения команды на CE1:

```
[CE1]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 6        Routes : 6

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

10.1.1.0/30         Direct  0    0           D   10.1.1.1        GigabitEthernet0/0/1
10.1.1.1/32         Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
11.11.11.11/32      Direct  0    0           D   127.0.0.1       LoopBack0
22.22.22.22/32      EBGP    255  0           D   10.1.1.2        GigabitEthernet0/0/1
127.0.0.0/8         Direct  0    0           D   127.0.0.1       InLoopBack0
127.0.0.1/32        Direct  0    0           D   127.0.0.1       InLoopBack0
```

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Проверка результатов конфигурирования решения 1 Варианта C магистральных сетей между интернет-провайдерами (2)

- Выполните команду **display bgp routing-table label** на ASBR, чтобы проверить метки маршрутов.

```
[ASBR1]dis bgp routing-table label

 BGP Local router ID is 23.23.23.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 4
        Network          NextHop           In/Out Label

 *>     1.1.1.1           23.23.23.1        1080/NULL
 *>     6.6.6.6           34.34.34.2        1077/1071
 *>     7.7.7.7           23.23.23.1        1081/NULL
 *>     8.8.8.8           34.34.34.2        1076/1070
```

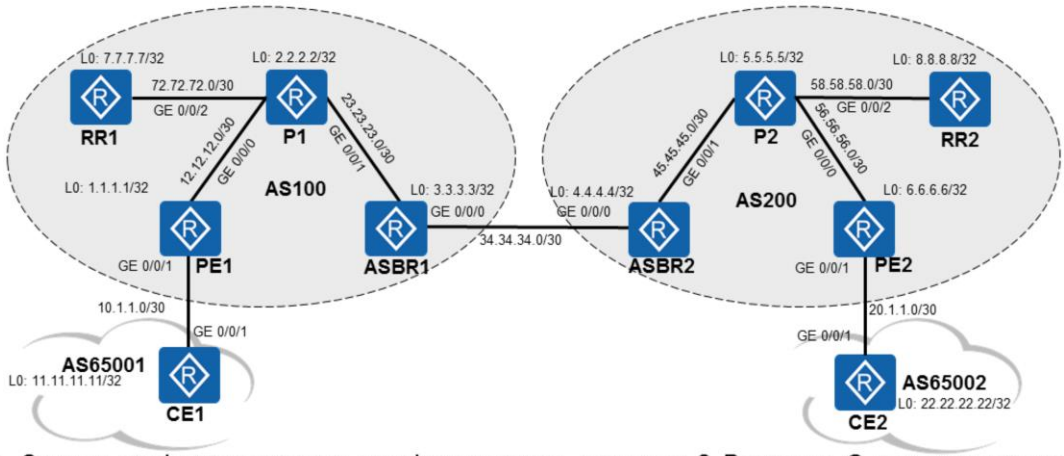
© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Содержание

- Общие сведения
- Теоретические основы
- **Конфигурации**
  - Конфигурация решения Варианта A
  - Конфигурация решения Варианта B
  - Конфигурация решения 1 Варианта C
  - Конфигурация решения 2 Варианта C

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Топология Варианта C магистральных сетей между интернет-провайдерами (Решение 2)



- Задача конфигурирования: сконфигурировать решение 2 Варианта C для реализации взаимного доступа между CE1 и CE2.
- Примечание: в данном примере в AS используется OSPF.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

- В сети, показанной на рисунке, AS100 и AS200 используются для ISP, тогда как две другие AS используются для клиентов. PE1, P1, RR1 и ASBR1 принадлежат к AS100. PE2, P2, RR2 и ASBR2 принадлежат к AS200. CE1 и CE2 принадлежат к одной VPN. CE1 подключен к PE1 в AS100, а CE2 подключен к PE2 в AS200.
- В этой топологии показаны IP-адреса, запланированные на каждом маршрутизаторе.
- В качестве примера используется решение 2 Варианта C. Реализация решения 2 аналогична реализации решения 1. Разница заключается в том, что при получении локальным ASBR маркированных маршрутов IPv4 от равноправного ASBR запускается LDP для присвоения меток маркированным маршрутам сети общего пользования BGP.

Процедура конфигурирования решения 2 для Варианта C магистральных сетей между интернет-провайдерами (1)

Шаг	Описание	Справочная информация и команды
1	Назначение IP-адреса и маски каждому интерфейсу.	См. раздел «Основные настройки IPv4» в руководстве по соответствующему продукту.
2	Настройка параметров OSPF на каждом PE, P, RR и ASBR через сеть общего пользования.	См. раздел «Настройка основных функций OSPF» в руководстве по соответствующему продукту.
3	Настройка параметров MPLS и LDP на каждом PE, P и ASBR через сеть общего пользования.	mpls mpls lsr-id lsr-id mpls ldp
4	Настройка отношений соседства EBGP между ASBR1 и ASBR2. Настройка на ASBR в каждой AS функции анонсирования маршрута до loopback-интерфейса локального RR и импортирования маршрута в процесс IGP.	См. раздел «Настройка основных функций BGP» в руководстве по соответствующему продукту. import-route bgp
5	Настройка экземпляра VPN с RD (100:1) и несколькими RT (100:1) на каждом PE.	ip vpn-instance vpn-instance-name route-distinguisher route-distinguisher vpn-target vpn-target [both |export-extcommunity | importextcommunity]
6	Настройка привязки интерфейса AC к экземпляру VPN на каждом PE.	ip binding vpn-instance vpn-instance-name
7	Настройка отношений соседства EBGP с подключенным CE в экземпляре VPN на каждом PE.	См. раздел «Настройка основных функций BGP» в руководстве по соответствующему продукту.
8	Настройка многоузловых отношений соседства MP-EBGP между RR1 и RR2 в режиме VPNv4. Настройка отношений соседства MP-IBGP между PE1 и RR1 в режиме VPNv4. Настройка отношений соседства MP-IBGP между PE2 и RR2 в режиме VPNv4. Отключение на каждом RR функции изменения атрибута Next_Hop в анонсируемых маршрутах.	peer { group-name | ipv4-address | ipv6-address } ebgp-max-hop [hop-count] ipv4-family vpnv4 peer { group-name | ipv4-address | ipv6-address } enable peer next-hop-invariable

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Процедура конфигурирования решения 2 для Варианта C магистральных сетей между интернет-провайдерами (2)

Шаг	Описание	Справочная информация и команды
9	Настройка параметров обмена маркированными маршрутами IPv4 между ASBR.	peer { group-name | ipv4-address } label-route-capability
10	Включение LDP на каждом ASBR для присвоения меток маркированным маршрутам сети общего пользования BGP.	lsp-trigger bgp-label-route
11	Применение политики маршрутизации к маршрутам, анонсируемым локальным ASBR в удаленный ASBR.	route-policy route-policy-name { permit | deny } node node peer { group-name | ipv4-address | ipv6-address } route-policy route-policy-name { import | export }
Примечания	1. Включите MPLS на ASBR1 и ASBR2. Использование LDP по усмотрению. 2. Настройка экземпляров VPN и привязки их к интерфейсам на ASBR1 и ASBR2 не требуется. 3. Настройте обмен маркированными маршрутами IPv4 на ASBR1 и ASBR2. 4. Убедитесь, что локальный RR не меняет атрибут Next_Hop маршрутов VPN при анонсировании их удаленному RR. Также убедитесь, что удаленный RR не меняет атрибут Next_Hop полученных маршрутов VPN при анонсировании их в PE той же AS. 5. Настройте политику маршрутизации на каждом ASBR1 и ASBR2, чтобы ASBR мог присваивать метки MPLS при анонсировании маршрутов до ASBR в равноправной AS. 6. Включите LDP на каждом ASBR для присвоения меток маркированным маршрутам сети общего пользования BGP.	

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Пример конфигурирования решения 2 для Варианта C магистральных сетей между интернет-провайдерами (1)

- Шаги 1–3 аналогичны шагам 1–3 в Варианте A.

4. Настройка отношений соседства EBGP между ASBR1 и ASBR2. Настройка на ASBR в каждой AS функции анонсирования маршрута до loopback-интерфейса локального RR и импортирования маршрута в процесс IGP.

```
[ASBR1]bgp 100
[ASBR1-bgp]peer 34.34.34.2 as-number 200
[ASBR1-bgp]network 7.7.7.7 255.255.255.255
[ASBR1-bgp]quit
[ASBR1]ospf
[ASBR1-ospf-1]import-route bgp
```

```
[ASBR2]bgp 200
[ASBR2-bgp]peer 34.34.34.1 as-number 100
[ASBR2-bgp]network 8.8.8.8 255.255.255.255
[ASBR2-bgp]quit
[ASBR2]ospf
[ASBR2-ospf-1]import-route bgp
```

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

- Импорт маршрутов BGP в процесс OSPF необходим для того, чтобы RR1 и RR2 могли устанавливать отношения соседства EBGP для передачи маршрутов VPN. Для обеспечения точности импортирования маршрутов BGP в процесс OSPF рекомендуется настроить политику маршрутизации. Это позволит предотвратить передачу нежелательных маршрутов в зону IGP.

Пример конфигурирования решения 2 для Варианта C магистральных сетей между интернет-провайдерами (2)

5. Настройка экземпляра VPN с RD (100:1) и несколькими RT (100:1) на каждом PE.

```
[PE1]ip vpn-instance huawei
[PE1-vpn-instance-huawei]route-distinguisher 100:1
[PE1-vpn-instance-huawei-af-ipv4]vpn-target 100:1 both
```

6. Настройка привязки интерфейса AC к экземпляру VPN на каждом PE.

```
[PE1]interface GigabitEthernet0/0/1
[PE1-GigabitEthernet0/0/1]ip binding vpn-instance huawei
[PE1-GigabitEthernet0/0/1]ip address 10.1.1.2 30
[PE1-GigabitEthernet0/0/1]quit
```

- Настройте PE2 аналогично PE1.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Пример конфигурирования решения 2 для Варианта C магистральных сетей между интернет-провайдерами (3)

7. Настройка отношений соседства EBGP с подключенным CE в экземпляре VPN на каждом PE.

```
[PE1]bgp 100
[PE1-bgp]ipv4-family vpn-instance huawei
[PE1-bgp-huawei]peer 10.1.1.1 as-number 65001
//Настройка отношений соседства EBGP между PE1 и CE1.
```

```
[CE1]bgp 65001
[CE1-bgp]peer 10.1.1.2 as-number 100
[CE1-bgp]network 11.11.11.11 32
```

- Настройте PE2 аналогично PE1, а также настройте CE2 аналогично CE1.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Пример конфигурирования решения 2 для Варианта C магистральных сетей между интернет-провайдерами (4)

8. Настройка отношений соседства MP-EBGP между RR1 и RR2 в режиме VPNv4 и отключение на RR функции изменения атрибута Next_Hop анонсируемых маршрутов VPN.

```
[RR1]bgp 100
[RR1-bgp]peer 8.8.8.8 as-number 200
[RR1-bgp]peer 8.8.8.8 connect-interface LoopBack 0
[RR1-bgp]peer 8.8.8.8 ebgp-max-hop 10
[RR1-bgp]ipv4-family vpnv4
[RR1-bgp-af-vpnv4]peer 8.8.8.8 enable
[RR1-bgp-af-vpnv4]peer 8.8.8.8 next-hop-invariable
[RR1-bgp-af-vpnv4]undo policy vpn-target
```

- В каждой AS настройте отношения соседства MP-IBGP между PE и RR в режиме VPNv4 и отключите на RR функцию изменения атрибута Next_Hop анонсируемых маршрутов VPN.

```
[RR1]bgp 100
[RR1-bgp]peer 1.1.1.1 as-number 100
[RR1-bgp]peer 1.1.1.1 connect-interface LoopBack 0
[RR1-bgp]ipv4-family vpnv4
[RR1-bgp-af-vpnv4]peer 1.1.1.1 enable
[RR1-bgp-af-vpnv4]peer 1.1.1.1 next-hop-invariable
```

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

- Более подробная информация об установлении отношений соседства MP-IBGP между PE2 и RR2 приводится в разделе «Конфигурация между PE1 и RR1».
- Выполнение команды **undo policy vpn-target** в Варианте C аналогично выполнению данной команды в Варианте B. В обоих случаях команда отключает на RR функцию фильтрации маршрутов на основе RT.
- Выполнение команды **peer** *X.X.X.X* **next-hop-invariable** обеспечивает, что соседний PE сможет осуществлять рекурсивный поиск маршрутов до BGP LSP, выделенного для локального PE в процессе передачи трафика.
- Установите отношения соседства MP-EBGP между RR в режиме VPNv4 и отключите на локальном RR функцию изменения атрибута Next_Hop маршрутов, анонсируемых соседнему RR. Таким образом, следующим узлом маршрута VPNv4, который получит PE, будет являться локальный PE.
- Установите отношения соседства MP-IBGP между RR и PE в режиме VPNv4 и отключите на RR функцию изменения атрибута Next_Hop маршрутов, анонсируемых локальному RR. Таким образом, следующим узлом маршрута VPNv4, который получит PE, будет являться равноправный PE.
- PE устанавливает отношения соседства VPNv4 только с RR в одной с ним AS. Локальный RR устанавливает отношения соседства VPNv4 с равноправным RR для передачи маршрутов VPN между AS.

Пример конфигурирования решения 2 для Варианта C магистральных сетей между интернет-провайдерами (5)

9. Настройка параметров обмена маркированными маршрутами IPv4 между ASBR.

```
[ASBR1]bgp 100
[ASBR1-bgp]peer 34.34.34.2 as-number 200
[ASBR1-bgp]peer 34.34.34.2 label-route-capability
```

```
[ASBR2]bgp 200
[ASBR2-bgp]peer 34.34.34.1 as-number 100
[ASBR2-bgp]peer 34.34.34.1 label-route-capability
```

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Пример конфигурирования решения 2 для Варианта C магистральных сетей между интернет-провайдерами (6)

10. Включение LDP на каждом ASBR для присвоения меток маркированным маршрутам сети общего пользования BGP.

```
[ASBR1]mpls
[ASBR1-mpls]lsp-trigger bgp-label-route
```

```
[ASBR2]mpls
[ASBR2-mpls]lsp-trigger bgp-label-route
```

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Пример конфигурирования решения 2 для Варианта C магистральных сетей между интернет-провайдерами (7)

11. Применение политики маршрутизации к маршрутам, анонсируемым локальным ASBR в удаленный ASBR.

```
[ASBR1]interface GigabitEthernet0/0/0
[ASBR1-GigabitEthernet0/0/0]ip address 34.34.34.1 30
[ASBR1-GigabitEthernet0/0/0]mpls
[ASBR1-GigabitEthernet0/0/0]quit
[ASBR1]route-policy policy1 permit node 10
[ASBR1-route-policy]apply mpls-label
//Присвоение меток MPLS маршрутам, которые соответствуют условиям фильтрации.
[ASBR1-route-policy]quit
[ASBR1]bgp 100
[ASBR1-bgp]peer 34.34.34.2 as-number 200
[ASBR1-bgp]peer 34.34.34.2 route-policy policy1 export
[ASBR1-bgp]network 1.1.1.1 32
```

- Настройте ASBR2 аналогично ASBR1.

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Проверка результатов конфигурирования решения 2 Варианта С магистральных сетей между интернет-провайдерами (1)

- После завершения приведенных выше настроек CE1 и CE2 определяют маршруты к loopback-интерфейсам друг друга и успешно осуществляют проверку связи с помощью команды ping.
- Далее в качестве примера приведены результаты выполнения команды на CE1:

```
[CE1]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 6        Routes : 6

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

10.1.1.0/30         Direct  0    0           D   10.1.1.1        GigabitEthernet0/0/1
10.1.1.1/32         Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
11.11.11.11/32      Direct  0    0           D   127.0.0.1       LoopBack0
22.22.22.22/32      EBGP    255  0           D   10.1.1.2        GigabitEthernet0/0/1
127.0.0.0/8         Direct  0    0           D   127.0.0.1       InLoopBack0
127.0.0.1/32        Direct  0    0           D   127.0.0.1       InLoopBack0
```

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Проверка результатов конфигурирования решения 2 Варианта C магистральных сетей между интернет-провайдерами (2)

- Выполните команду **display bgp routing-table label** на ASBR, чтобы проверить метки маршрутов.

```
[ASBR1]dis bgp routing-table label

 BGP Local router ID is 34.34.34.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 4
        Network            NextHop         In/Out Label

 *>     1.1.1.1            23.23.23.1        1047/NULL
 *>     6.6.6.6            34.34.34.2        NULL/1041
 *>     7.7.7.7            23.23.23.1        1043/NULL
 *>     8.8.8.8            34.34.34.2        NULL/1042
```

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

HUAWEI

Проверка результатов конфигурирования решения 2 Варианта C магистральных сетей между интернет-провайдерами (3)

- Выполните команду **display mpls lsp** на PE для проверки LDP LSP до равноправного PE.

```
[PE1]dis mpls lsp
------------------------------------------------
                LSP Information: BGP  LSP
------------------------------------------------
FEC                    In/Out Label    In/Out IF     Vrf Name
11.11.11.11/32         1042/NULL        -/-          huawei
------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------
FEC                    In/Out Label   In/Out IF      Vrf Name
2.2.2.2/32             NULL/3          -/GE0/0/0
2.2.2.2/32             1037/3          -/GE0/0/0
6.6.6.6/32             NULL/1033       -/GE0/0/0
6.6.6.6/32             1039/1033       -/GE0/0/0
.............
```

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Вопросы

- В каком из вариантов для хранения информации о маршрутизации на стороне CE не требуется ASBR? ( )
  - Вариант A
  - Вариант B
  - Вариант C
- В каком из вариантов применяются три метки при передаче пакетов, если для присвоения меток используется только LDP или BGP? ( )
  - Вариант A
  - Вариант B
  - Вариант C

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

1. C
2. C

Заключение

- Теоретические основы и конфигурации Варианта A
- Теоретические основы и конфигурации Варианта B
- Теоретические основы и конфигурации Варианта C

© Huawei Technologies Co., Ltd. 2019 г. Все права защищены.

Спасибо за внимание!

www.huawei.com

HCIE-R&S

— Безопасность

www.huawei.com

Авторское право © 2019 Huawei Technologies Co., Ltd.

HUAWEI

Введение

- Благодаря развитию Интернета стек протоколов TCP/IP стал самым популярным протоколом сетевого взаимодействия. Однако, поскольку данный стек протоколов изначально предназначался для небольшого числа доверенных групп пользователей в исследовательской среде, обеспечению безопасности сети было уделено мало внимания. В результате в протоколах существуют некоторые риски, связанные с безопасностью. В данном документе представлены основные технологии обеспечения безопасности сети.

Авторское право © 2019 Huawei Technologies Co., Ltd.

Цели

- После прохождения данного курса вы сможете:
  - Описать распространенные сетевые атаки
  - Использовать базовые технологии защиты от сетевых атак.

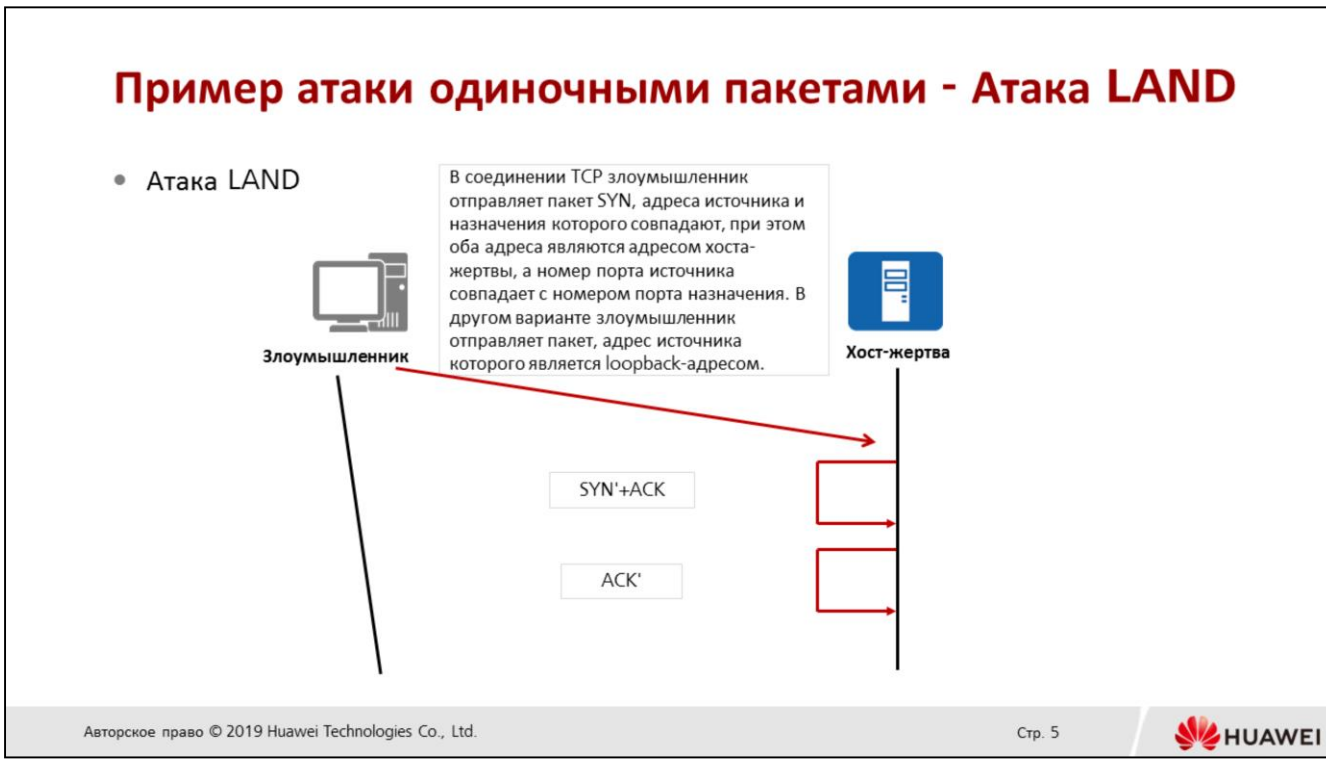
Авторское право © 2019 Huawei Technologies Co., Ltd.



Содержание

1. **Защита от атак одиночными пакетами**
2. Защита от flood-атак
3. Защита от подмены адреса источника (IP-спуфинг).
4. Защита от атак посредника
5. Защита передачи данных

Авторское право © 2019 Huawei Technologies Co., Ltd.



- Атаки одиночными пакетами являются разновидностью DoS-атак («Отказ в обслуживании») и подразделяются на следующие типы:
  - Атака сканирования может быть первым шагом в процессе взлома и не наносит прямого ущерба. Как правило, это действия в сети перед реальной атакой. Примерами таких атак являются сканирование IP-адресов и сканирование портов.
  - Атака некорректными пакетами: злоумышленник отправляет большое количество некорректных пакетов, чтобы вывести из строя хост или сервер, который обрабатывает такие пакеты. Примерами таких атак являются атаки LAND и Smurf.
  - Атака специально сконструированными пакетами: обычные пакеты используются для отслеживания структуры сети или атаки на систему или сеть, в результате чего возникает сбой системы или отключение сети. Примерами таких атак являются атаки слишком большими пакетами ICMP и атаки пакетами ICMP с использованием недостижимых адресов.
- Атаки LAND
  - Злоумышленник отправляет пакет SYN хосту-жертве, используя уязвимость механизма трехстороннего квитирования TCP. В этом пакете в качестве адреса источника и адреса назначения указан адрес хоста-жертвы, а номер порта источника совпадает с номером порта назначения. Когда хост-жертва получает такой пакет, он пытается установить TCP-соединение, где в качестве адреса источника и адреса назначения указан адрес самого хоста. При такой атаке хост-жертва создает большое количество недействительных TCP-соединений, в результате чего расходует большое

количество ресурсов и в конечном счете выходит из строя.

Пример атаки одиночными пакетами - Защита от атаки LAND

- Защита от атаки LAND
  - После включения защиты от атак некорректными пакетами устройство проверяет адреса источника и назначения пакетов TCP SYN, чтобы предотвратить атаки LAND. Если адрес источника и адрес назначения в пакете TCP SYN совпадают, он считается некорректным и отбрасывается.
  - Необходимо включить защиту от некорректных пакетов (режим системы):

anti-attack abnormal enable



Авторское право © 2019 Huawei Technologies Co., Ltd.

- Все функции защиты от атак, включая защиту от атак некорректными пакетами, можно включить с помощью команды **anti-attack enable** в режиме системы.



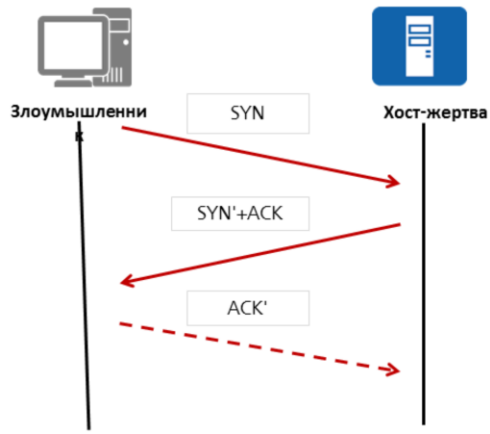
Содержание

1. Защита от атак одиночными пакетами
2. **Защита от flood-атак**
3. Защита от подмены адреса источника (IP-спуфинг).
4. Защита от атак посредника
5. Защита передачи данных

Авторское право © 2019 Huawei Technologies Co., Ltd.

Пример Flood-атаки — SYN flood

- Атака SYN



Авторское право © 2019 Huawei Technologies Co., Ltd.

- Flood-атака – это также одна из разновидностей DoS-атак.
- Атаки SYN в протоколе TCP
  - Атака SYN использует уязвимость механизма трехстороннего квитирования TCP. При трехстороннем квитировании TCP получатель получает первый пакет SYN от отправителя, затем отправляет пакет SYN+ACK отправителю и ожидает окончательный пакет ACK от отправителя. В этом процессе соединение всегда является полуоткрытым. Если получатель не получает окончательный пакет ACK, он повторно отправляет пакет SYN + ACK отправителю. Если отправитель по-прежнему не возвращает пакет ACK после нескольких попыток, получатель закрывает сеанс и обновляет сеанс в памяти. В течение этого периода злоумышленник может отправлять сотни тысяч пакетов SYN на открытый порт и не отвечать на пакеты SYN + ACK от получателя. В итоге получатель перегружается, перестает обрабатывать новые запросы на соединение и разрывает все активные соединения.

Пример защиты от Flood-атаки — Защита от атаки SYN flood

- Защита от атак SYN flood
  - После включения на устройстве защиты от атак SYN flood устройство ограничивает скорость получения пакетов SYN, чтобы избежать истощения ресурсов хоста.
  - Необходимо включить защиту от атак TCP SYN flood (режим системы):

```
anti-attack tcp-syn enable
anti-attack tcp-syn car cir cir
```



Авторское право © 2019 Huawei Technologies Co., Ltd.

- Команды защиты от Flood-атак
  - Команда **anti-attack tcp-syn enable** включает защиту от атак SYN flood.
  - Команда **anti-attack tcp-syn car** устанавливает ограничение скорости передачи пакетов для защиты от атак SYN flood. Если скорость приема пакетов SYN превышает установленное ограничение, устройство начинает отбрасывать избыточные пакеты, чтобы обеспечить корректную работу ЦП.



Содержание

1. Защита от атак одиночными пакетами
2. Защита от flood-атак
3. **Защита от подмены адреса источника (IP-спуфинг).**
4. Защита от атак посредника
5. Защита передачи данных

Авторское право © 2019 Huawei Technologies Co., Ltd.

Механизм URPF

- Подмена IP-адреса источника. Как правило, доверие к хостам в сети определяется на основе их IP-адреса. Подмена IP-адреса источника подразумевает использование поддельных адресов источников, чтобы завоевать доверие хоста с целью похищения сетевой информации или нарушение связи в системе.
- Механизм URPF (Unicast RPF)
  - Защищает от DoS-атак с использованием поддельных IP-адресов источника.
  - Режимы работы URPF:
    - Строгий (Strict)
    - Свободный (Loose)
  - **URPF** { **loose** | **strict** } [**allow-default-route**] [**acl** *acl-number*]



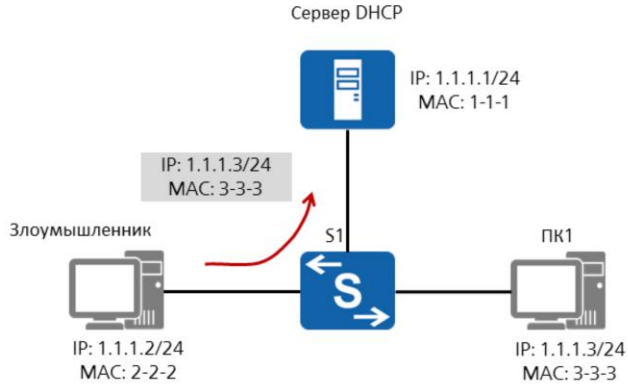
Авторское право © 2019 Huawei Technologies Co., Ltd.

- Режимы работы URPF:
  - Строгий (Strict)
    - В строгом режиме пакет проходит проверку URPF только тогда, когда у устройства есть маршрут к IP-адресу источника пакета в таблице FIB, и входящий интерфейс пакета совпадает с исходящим интерфейсом маршрута. На рисунке выше злоумышленник подделывает пакет с адресом источника 2.1.1.1, чтобы инициировать запрос к S1. После получения запроса S1 отправляет пакет реальному хосту (ПК1) с адресом 2.1.1.1. Подделанный пакет является атакой и на S1, и на ПК1. Если на S1 включена проверка URPF, то при получении пакета с адресом источника 2.1.1.1 S1 выполняет проверку URPF и устанавливает, что исходящий интерфейс, соответствующий адресу источника пакета, не соответствует интерфейсу, принимающему пакет, и отбрасывает такой пакет.
    - В среде с симметричными маршрутами рекомендуется использовать строгий режим URPF. Например, если между двумя оконечными устройствами сети существует только один путь, то для обеспечения максимальной безопасности сети может использоваться строгий режим URPF.

- Свободный (Loose)
  - В свободном режиме пакет проходит проверку, если у устройства есть маршрут к исходному IP-адресу пакета в таблице FIB, и при этом входящий интерфейс пакета не должен совпадать с исходящим интерфейсом маршрута.
  - В среде с несимметричными маршрутами рекомендуется использовать свободный режим URPF. Например, если между двумя граничными устройствами существует несколько маршрутов, то для повышения безопасности сети и предотвращения отбрасывания пакетов, передаваемых по правильному пути, может использоваться свободный режим URPF.

Функция защиты от подмены IP-адресов (IPSG)

- Защита от подмены IP-адресов
  - Функция IPSG сопоставляет IP-пакеты с таблицей динамических или статических привязок DHCP, чтобы предотвратить подмену IP-адреса источника.



Авторское право © 2019 Huawei Technologies Co., Ltd.

- Функция IPSG
  - IPSG сопоставляет IP-пакеты с таблицей статических привязок или таблицей динамических привязок DHCP. Перед пересылкой IP-пакета устройство сравнивает IP-адрес источника, MAC-адрес источника, номер порта и идентификатор VLAN в IP-пакете с информацией в таблице привязок. Если информация совпадает, пакет отправлен авторизованным пользователем и устройство разрешает прохождение такого пакета. В противном случае устройство рассматривает такой пакет как атаку и отбрасывает его. На рисунке выше на S1 настроена функция IPSG для проверки входящих IP-пакетов по таблице привязок. Информация о пакетах, отправленных авторизованными пользователями, совпадает с информацией в таблице привязок. Прохождение пакетов разрешено. Информация о поддельных пакетах

от злоумышленников не соответствует информации в таблице привязок. Пакеты отбрасываются.

- Команды IPSG
  - Существуют таблицы динамических привязок и таблицы статических привязок DHCP. Таблица статических привязок настраивается вручную с помощью команды **user-bind static**.
  - Команда **ip source check user-bind enable** включает функцию проверки IP-пакета.
  - Команда **ip source check user-bind check-item** настраивает элемент проверки IP-пакета по идентификатору VLAN или интерфейсу. Эта команда действует только для записей динамических привязок.



Содержание

1. Защита от атак одиночными пакетами
2. Защита от flood-атак
3. Защита от подмены адреса источника (IP-спуфинг).
4. **Защита от атак посредника**
5. Защита передачи данных

Авторское право © 2019 Huawei Technologies Co., Ltd.

HUAWEI

Защита от атак посредника — DAI

- Атака посредника: как следует из названия, злоумышленник находится между клиентом и сервером. При этом злоумышленник имитирует сервер для клиента и клиента для сервера.
- Динамическая проверка ARP (DAI)
  - Для защиты от атак посредника используется таблица привязок DHCP snooping. Когда устройство получает пакет ARP, оно сравнивает IP-адрес источника, MAC-адрес источника, идентификатор VLAN и информацию об интерфейсе в пакете ARP с данными в таблице привязок DHCP snooping. Если информация совпадает, устройство рассматривает такой пакет как пакет от авторизованного пользователя, и пропускает пакет. В противном случае устройство считает, что пакет получен от злоумышленника, и отбрасывает его.
  - Команда

Запись ARP ПК1

IP-адрес	MAC-адрес	Тип
10.1.1.3	3-3-3	Динамический

Обновленная запись ARP

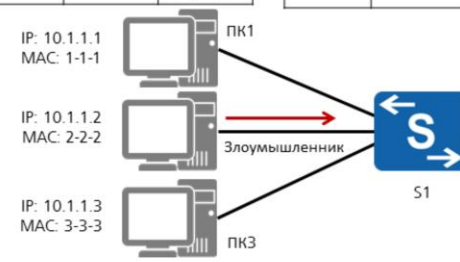
IP-адрес	MAC-адрес	Тип
10.1.1.3	2-2-2	Динамический

Запись ARP ПК3

IP-адрес	MAC-адрес	Тип
10.1.1.1	1-1-1	Динамический

Обновленная запись ARP

IP-адрес	MAC-адрес	Тип
10.1.1.1	2-2-2	Динамический



arp anti-attack check user-bind enable

Авторское право © 2019 Huawei Technologies Co., Ltd.

- На рисунке показана атака посредника. Злоумышленник выдает себя за ПК3 и отправляет поддельный пакет ARP на ПК1. В результате в таблице ARP ПК1 регистрируется неверное соответствие между IP-адресом и MAC-адресом ПК3. Злоумышленник легко получает данные, которые ПК1 отправляет на ПК3. Злоумышленник также может легко получить данные, которые ПК3 отправляет на ПК1. Следовательно, защитить информацию, передаваемую между ПК1 и ПК3, невозможно.
- Для защиты от атак посредника на S1 можно включить функцию DAI.
- Если после включения функции DAI на S1 злоумышленник, подключенный к S1, попытается отправить поддельные ARP-пакеты, S1 обнаружит атаку на таблицу привязок DHCP snooping и отбросит такие ARP-пакеты. Если на S1 также включена функция сигнализации на базе DAI, S1 отправит сигнал

администратору, когда количество ARP-пакетов, отброшенных из-за несоответствия записям таблицы привязки DHCP snooping, превысит пороговое значение.

- Команда DAI
  - Команда **arp anti-attack check user-bind enable** включает функцию DAI для интерфейса или VLAN. После выполнения этой команды выполняется сверка ARP-пакетов с записями таблицы привязок.

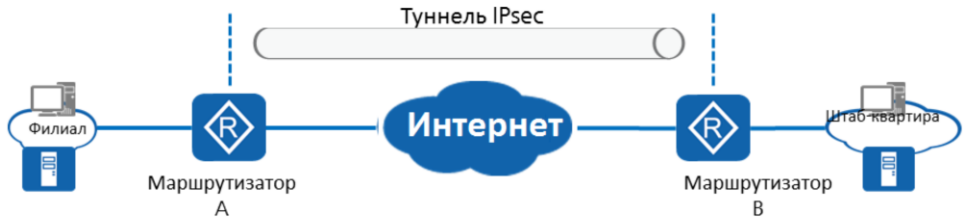
Содержание

1. Защита от атак одиночными пакетами
2. Защита от flood-атак
3. Защита от подмены адреса источника (IP-спуфинг).
4. Защита от атак посредника
5. **Защита передачи данных**

Авторское право © 2019 Huawei Technologies Co., Ltd.

Обзор IPsec VPN

- Internet Protocol Security (IPsec) – это простой в использовании набор протоколов для обеспечения защиты данных. Протокол IPSec обеспечивает прозрачные сервисы по защите передачи данных в IP-сетях на базе протокола TCP от прослушивания и взлома и эффективную защиту от сетевых атак.
- IPsec устанавливает двунаправленные безопасные ассоциации (SA) между узлами IPsec, чтобы построить туннель IPsec для безопасной передачи данных в Интернете.

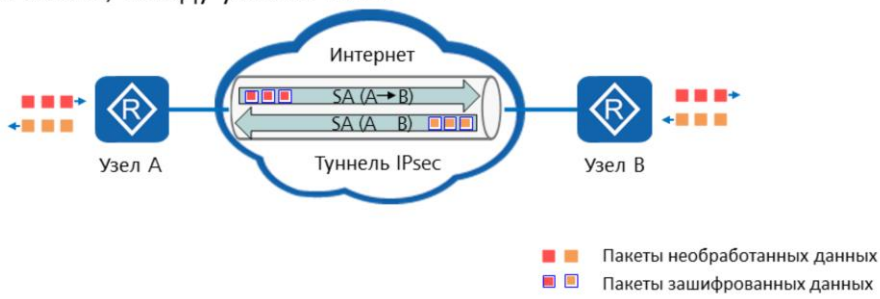


Авторское право © 2019 Huawei Technologies Co., Ltd.

- IPsec, развернутый в сети, может выполнять шифрование b проверку целостности и аутентификацию источника передаваемых данных, чтобы снизить риски утечки информации.

IPsec SA

- Прежде чем IPsec начнет безопасно передавать данные, необходимо установить безопасные ассоциации (SA) между одноранговыми узлами IPsec (двумя конечными точками туннеля IPsec).
- Соединение SA – это установление общих атрибутов безопасности (таких как алгоритмы и ключи) между узлами IPsec.



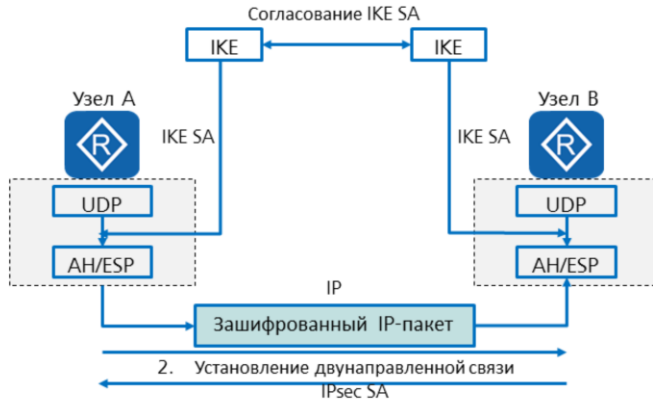
Пакеты необработанных данных
Пакеты зашифрованных данных

Авторское право © 2019 Huawei Technologies Co., Ltd.

- Для передачи данных узлы IPsec устанавливают общие атрибуты безопасности для соединения SA. К этим атрибутам относятся протокол безопасности, характеристики защищаемых потоков данных, режим инкапсуляции данных, алгоритм шифрования, алгоритм аутентификации, метод обмена ключами, IKE и время жизни SA.
- За аутентификацию SA отвечают три параметра: индекс параметров безопасности (SPI), IP-адрес назначения и идентификатор протокола безопасности (AH или ESP).

Протокол IKE для установления соединения SA

- Протокол IKE выполняет автоматическое согласование ключей для установления соединения SA.

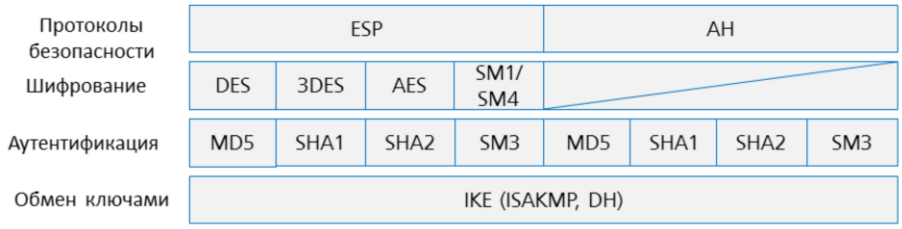


Авторское право © 2019 Huawei Technologies Co., Ltd.

- Протокол обмена ключами (IKE) работает на основе протокола ISAKMP. IKE – это протокол прикладного уровня на основе протокола UDP, который предоставляет ключи для шифрования данных. Это упрощает использование, управление, настройку и обслуживание IPsec.
- После установления соединения SA между узлами IPsec с помощью IKE для аутентификации и обмена ключами далее выполняется согласование пары SA-соединений на основе настроенных параметров, таких как протокол AH или ESP. После чего выполняется шифрование и передача данных между узлами в туннеле IPsec.

Протоколы безопасности IPsec

- IPsec обеспечивает защиту IP-пакетов за счет использования двух протоколов безопасности, а именно, протокола заголовка аутентификации (Authentication Header, AH) и протокола инкапсулирующей защиты содержимого (Encapsulating Security Payload, ESP).



Авторское право © 2019 Huawei Technologies Co., Ltd.

HUAWEI

- Протокол AH обеспечивает аутентификацию источника данных, проверку целостности данных и защиту от атак повторного воспроизведения, но не обеспечивает шифрование.
- Протокол ESP обеспечивает шифрование, аутентификацию источника данных, проверку целостности данных и защиту от атак повторного воспроизведения.
- Функции безопасности, предоставляемые протоколами AH и ESP, зависят от алгоритмов аутентификации и шифрования, используемых IPsec.
- Ключи, используемые для шифрования и аутентификации IPsec, могут настраиваться вручную или динамически согласовываться с использованием протокола IKE. В этом курсе приведено описание способа создания туннеля

IPsec вручную.

Режим инкапсуляции: транспортный режим

- В транспортном режиме между заголовком IP и заголовком протокола транспортного уровня (TCP/UDP/ICMP) добавляется заголовок AH или ESP для защиты полезной нагрузки TCP, UDP или ICMP.

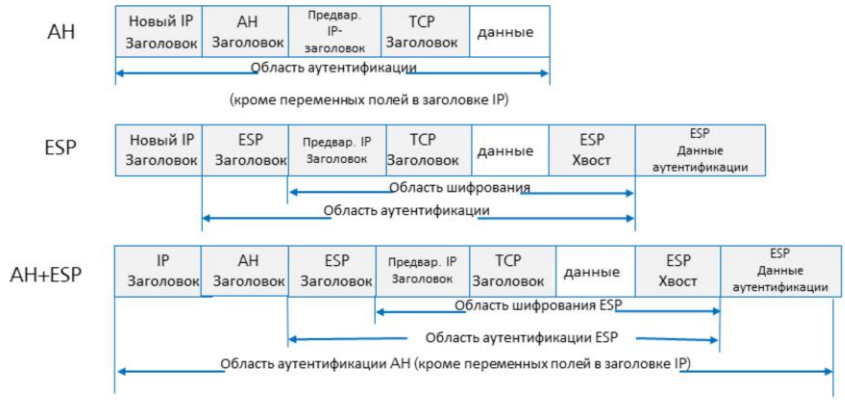


Авторское право © 2019 Huawei Technologies Co., Ltd.

- Транспортный режим не меняет заголовок IP, поэтому адреса источника и назначения туннеля IPsec должны совпадать с адресами в заголовке IP. Этот режим инкапсуляции применяется только для связи между двумя хостами или между хостом и шлюзом VPN.

Режим инкапсуляции: туннельный режим

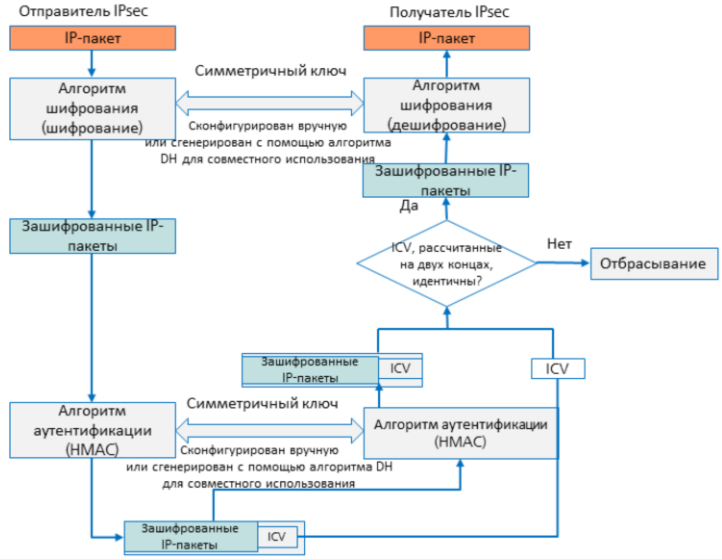
- В туннельном режиме заголовок AH или ESP добавляется перед предварительным IP-заголовком, а затем инкапсулируется в новый IP-пакет с новым IP-заголовком для защиты IP-заголовка и полезной нагрузки.



Авторское право © 2019 Huawei Technologies Co., Ltd.

- Туннельный режим применяется для связи между двумя VPN-шлюзами или между хостом и VPN-шлюзом.
- Отличие между двумя режимами инкапсуляции заключаются в следующем:
  - С точки зрения безопасности, туннельный режим является более безопасным по сравнению с транспортным режимом. Туннельный режим обеспечивает полную аутентификацию и шифрование исходных IP-пакетов. Он позволяет скрыть IP-адреса, типы протоколов и номера портов в исходных IP-пакетах.
  - С точки зрения производительности, туннельный режим занимает больше ресурсов полосы пропускания из-за дополнительного заголовка IP.

Шифрование, дешифрование и аутентификация IPsec



Авторское право © 2019 Huawei Technologies Co., Ltd.

- Для шифрования и дешифрования данных IPsec использует алгоритмы симметричного шифрования.
- IPsec предоставляет механизм аутентификации, позволяющий получателю данных проверить подлинность отправителя данных при IP-связи, и определяет, изменяются ли данные во время передачи.
- В IPsec для аутентификации используется код аутентификации сообщений, использующий хеш-функции (HMAC). Функция HMAC позволяет проверить целостность и подлинность пакетов данных путем сравнения цифровых подписей.



Тест

1. Когда IPsec использует протокол AH для инкапсуляции данных, он не поддерживает проверку целостности данных. ( )
   A. Верно
   B. Неверно
2. Какие из следующих атак являются DoS-атаками? ( )
   A. Атака некорректными пакетами
   B. Подмена IP-адреса источника
   C. Атака посредника
   D. Flood-атака

Авторское право © 2019 Huawei Technologies Co., Ltd.

HUAWEI

- Ответы:
  - B
  - A D

Краткое содержание

- Атаки одиночными пакетами и способы защиты
- Flood-атаки и способы защиты
- Атака подмены IP-адреса источника
- URPF
- IPSG
- DAI
- IPsec VPN

Авторское право © 2019 Huawei Technologies Co., Ltd.

Спасибо!

www.huawei.com

HCIE-R&S

— Высокая доступность и управление сетью

www.huawei.com

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Введение

- Помимо соответствия требованиям к соединениям, сеть должна обеспечивать непрерывность услуг. Для этого сеть должна быть высоконадежной и доступной, чтобы возникновение сбоя не влияло на оказание услуг и сбой был быстро обнаружен и устранен. В этом разделе описываются технологии высокой доступности сети (HA) и протоколы управления сетью, способные удовлетворить все описанные требования.

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Цели

- Данный курс включает:
  - Описание процессов развертывания технологий высокой доступности в соответствии со сценариями применения.
  - Описание процессов управления сетью и быстрого поиска сетевых отказов.

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Содержание

1. **Технологии высокой доступности**
   - Обзор высокой доступности
   - Протокол BFD
   - Технология NSF
   - Технология NSR
2. Протоколы управления сетью

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Обзор высокой доступности

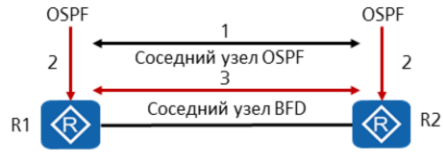
- Высокая доступность (High availability, HA)
  - Определение: высокая доступность – это характеристика продукта или системы.
  - Характеристики высокой доступности
    - Низкий уровень возникновения ошибок
    - Быстрое восстановление после возникновения отказов
  - Стандарты высокой доступности
    - MTBF – среднее время между отказами компонента или устройства.
    - MTTR – среднее время, необходимое компоненту или устройству для восстановления после сбоя.

$$\text{Доступность системы} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

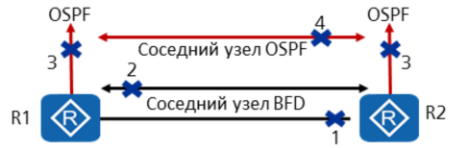
Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Протокол BFD – Рабочий процесс

- Протокол BFD (Bidirectional Forwarding Detection)
  - Протокол BFD позволяет быстро определять проблемы соединения каналов и IP-передачи.
- Установление сеанса BFD



- Обнаружение отказа BFD



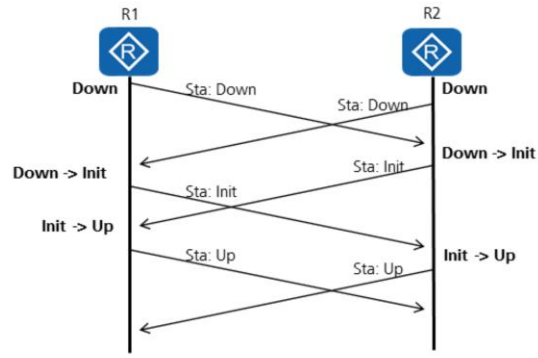
Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Основные понятия BFD
  - Два сетевых устройства устанавливают сеанс BFD, чтобы проверить путь между собой и предоставить обслуживание приложениям верхнего уровня. Протокол BFD не предоставляет функцию обнаружения соседних устройств. Вместо этого BFD получает информацию о соседях из приложений верхнего уровня, которые он обслуживает. После того, как два устройства устанавливают сеанс BFD, они начинают отправлять пакеты BFD через определенные промежутки времени. Если устройство не получает ответ в течение установленного срока, устройство считает, что путь передачи ошибочен. В этом случае BFD уведомляет об этом протокол верхнего уровня.
  - Управляющие пакеты BFD инкапсулируются с помощью UDP. Номер порта назначения - 3784, а номер порта источника - от 49152 до 65535.
- Установление сеанса BFD
  1. OSPF использует механизм Hello для обнаружения соседних устройств и устанавливает отношения соседства.
  2. OSPF передает BFD информацию о соседнем устройстве, включая адреса источника и назначения.
  3. BFD устанавливает сеанс BFD на основе принятой информации о соседнем устройстве.
  4. После того, как сеанс BFD установлен, BFD начинает отслеживать и быстро реагировать на неисправности канала.
- Обнаружение неисправности BFD
  1. Обнаружена неисправность канала.
  2. Считается, что сеанс BFD находится в состоянии Down.

3. BFD уведомляет локальный процесс OSPF о том, что соседнее устройство недоступно.
4. Локальный процесс OSPF завершает отношения соседства OSPF.

Протокол BFD – Управление сеансом

- Управление сеансом BFD
  - Сеанс BFD может находится востояних Down, Init, Up или AdminDown.
  - При установлении и отключении конечного автомата BFD используется механизм трехстороннего квитирования.



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Состояние сеанса BFD
  - Down: сеанс BFD находится в состоянии Down или был отправлен запрос.
  - Init: локальное конечное устройство может устанавливать связь с удаленным устройством и требует, чтобы сеанс перешел в состояние Up.
  - Up: сеанс BFD установлен.
  - AdminDown: сеанс BFD находится в состоянии AdminDown.
- Процесс миграции сеанса BFD
  - Протокол BFD, настроенный на R1 и R2, запускает конечные автоматы. Начальное состояние конечных автоматов BFD - Down. R1 и R2 отправляют контрольные пакеты BFD, в которых в поле State установлено значение Down.
  - После получения управляющего пакета BFD, в котором в поле State установлено значение Down, R2 переключает состояние сеанса на Init и отправляет управляющий пакет BFD, в котором в поле State установлено значение Init.
  - После того, как состояние локального сеанса BFD R2 изменяется на Init, R2 прекращает обрабатывать полученные управляющие пакеты BFD, в которых в поле State установлено значение Down.
  - Изменение состояния BFD R1 совпадает с изменением состояния R2.
  - После получения управляющего пакета BFD со значением Init, установленным в поле State, R2 изменяет состояние локального сеанса на Up.

- Изменение состояния BFD R1 совпадает с изменением состояния R2.

Протокол BFD – Сценарии применения

- Сценарии применения протокола BFD
  - BFD для IP-соединений
  - Связь между состоянием сеанса BFD и состоянием интерфейса
  - BFD для статических маршрутов
  - BFD для OSPF
  - BFD для IS-IS
  - BFD для BGP
  - BFD для MPLS LSP
  - BFD для VRRP
  - BFD для PIM

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Общие команды
  - Обнаружение IP-канала подразделяется на обнаружение через один интервал и через несколько интервалов.
    - Команда bfd включает BFD глобально в режиме системы и выводит на экран глобальный режим BFD.
    - Команда bfd bind peer-ip создает привязку BFD и устанавливает сеанс BFD.
    - Команда discriminator устанавливает локальный и удаленный дискриминаторы для текущего сеанса BFD.
    - Команда commit фиксирует конфигурацию сеанса BFD.
    - Существует два сценария в зависимости от того, поддерживает ли одноранговое устройство BFD: 1. Если одноранговое устройство поддерживает BFD, создайте сеанс BFD, который может быть установлен только тогда, когда параметры BFD согласованы на обоих концах и оба конца отправляют пакеты в MPU. 2. Если одноранговое устройство не поддерживает BFD, создайте однонаправленный эхо-сеанс BFD.
  - Связь между состоянием сеанса BFD и состоянием интерфейса
    - Команда bfd включает BFD глобально в режиме системы и отображает BFD глобально.
    - Команда bfd bind peer-ip default-ip создает привязку BFD для обнаружения физического состояния канала.
    - Команда discriminator устанавливает локальный и удаленный дискриминаторы для текущего сеанса BFD.
    - Команда process-interface-status ассоциирует сеанс BFD с интерфейсом, к которому привязан сеанс BFD.
    - Конфигурация связи состояния интерфейса аналогична конфигурации связи маршрутов, и поэтому не описывается в данном документе.

Технология NSF

- Технология NSF (Non-Stop Forwarding)
  - Если в системе происходит сбой, то при переключении между активным и резервным устройством услуги плоскости переадресации не прерываются.
  - Когда система восстанавливает конфигурации, устройство восстанавливает отношения соседства и получает информацию о маршрутизации от соседних устройств, чтобы перестроить таблицу маршрутизации.
- Механизм NSF должен соответствовать следующим требованиям:
  - Требования к аппаратному обеспечению: система имеет два MPU с дублированием RP.
  - Требования к программному обеспечению: активная и резервная платы синхронизированы.
  - Требование к протоколу: связанные сетевые протоколы поддерживают GR.

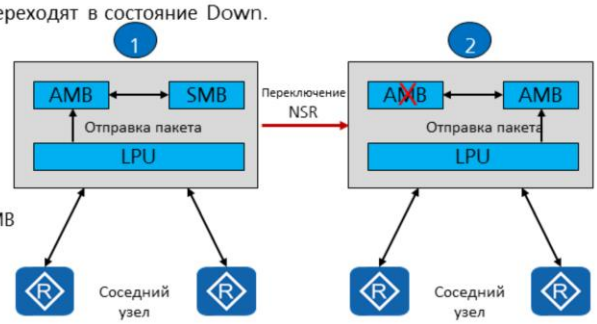
Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- В случае неисправности маршрутизатора соседние устройства на уровне протокола маршрутизации обнаруживают, что отношения соседства между ними находятся в состоянии Down, но через некоторе время снова переходят в состояние Up. Такие отношения являются нестабильными. Нестабильные отношения соседства приводят к нестабильности маршрута, что в свою очередь, приводит к возникновению маршрутов «в никуда» на перезапущенном маршрутизаторе или обходу перезапускающегося маршрутизатора трафиком данных с соседних устройств. Это снижает надежность сети. Цель технологии NSF состоит в решении проблемы нестабильности маршрутов. Необходимо соблюдать следующие требования:
  - Требования к аппаратному обеспечению: система имеет два MPU с дублированием RP: один - активный MPU, а другой - резервный MPU. В случае перезапуска активного MPU, резервный MPU становится активным. Используется распределенная структура, поэтому процессы передачи и управления данными разделены. Для передачи данных используются выделенные LPU (интерфейсные платы).
  - Требования к программному обеспечению: если активный MPU работает нормально, он синхронизирует информацию о конфигурации и состоянии интерфейса с резервным MPU. При переключении между активным и резервным MPU интерфейсы остаются в состоянии Up; LPU не сбрасывают и не удаляют записи переадресации.
  - Требования к протоколу: для связанных сетевых протоколов должен поддерживаться GR, например, для протоколов маршрутизации OSPF, IS-IS и BGP и других протоколов, например, LDP.

Технология NSR

- Технология NSR (Non-stopping routing) – это механизм резервного копирования протокола, который гарантирует отсутствие прерывания связи на уровне управления (маршрутизация) и уровне переадресации (услуги) во время переключения между активным и резервным устройством.
  - Во время переключения между устройствами обработка маршрута не прерывается, поскольку информация о соседях и топологии не теряется.
  - Отношения соседства не переходят в состояние Down.
- Процесс NSR

1. Пакетное резервное копирование
2. Резервное копирование в реальном времени
3. Переключение между AMB и SMB



1. Протокол маршрутизации на уровне управления выполняет резервное копирование информации о маршрутизации в режиме реального времени.
2. Аппаратный канал обнаруживает ошибку на AMB, SMB становится новым AMB, и LPU отправляют пакеты на новый AMB.

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Преимущества NSR
  - NSR не влияет на соседнее устройство и не зависит от него.
  - Скорость конвергенции маршрута NSR выше скорости конвергенции NSF.
- Процесс NSR
  1. Пакетное резервное копирование: после включения NSR и перезапуска SMB сервисный процесс на AMB получает сообщение о том, что SMB переходит в режим онлайн. После получения сообщения ACP выполняет резервное копирование своих данных на SCP в формате пакетов.
     - После выполнения пакетного резервного копирования устройство переходит в резервное состояние. В случае неисправности AMB, SMB становится новым AMB и восстанавливает данные.
     - В случае неисправности AMB перед пакетным резервным копированием, SMB не может взять на себя функции нового AMB. Неисправность может быть устранена после перезапуска устройства.
  2. После завершения пакетного резервного копирования устройство переходит в фазу резервного копирования в режиме реального времени. Если на AMB изменяется статус соседнего устройства или информация о маршрутизации, AMB резервирует обновленную информацию на SMB в режиме реального времени.
  3. Если происходит сбой программного или аппаратного обеспечения AMB, SMB обнаруживает сбой и автоматически становится новым AMB. Новый AMB использует данные резервного копирования для передачи трафика. LPU отправляет информацию, которая была обновлена во время переключения AMB/SMB, на новый AMB. Маршруты доступны, и во время переключения передача трафика не прерывается.
- Во время переключения AMB/SMB система поддерживает два типа защиты высокой доступности: NSR и GR, которые являются взаимоисключающими. То есть для конкретного протокола после

переключения системы может использоваться только один из процессов NSR и GR .



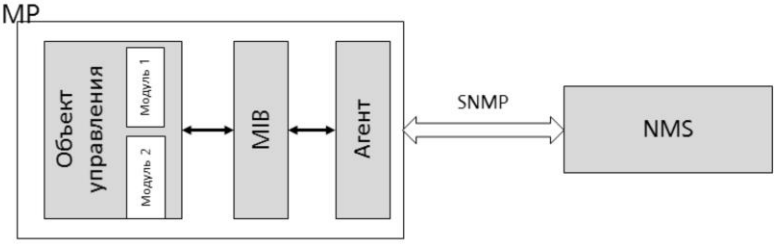
Содержание

1. Технологии высокой доступности
2. **Протоколы управления сетью**
   - SNMP
   - NTP

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Протокол SNMP – основные понятия

- Простой протокол управления сетью (SNMP)
  - Протокол SNMP использует центральный компьютер (станцию управления сетью), который запускает программное обеспечение управления сетью для управления устройствами.
- Версии SNMP
  - SNMPv1, SNMPv2c и SNMPv3
- Модель SNMP

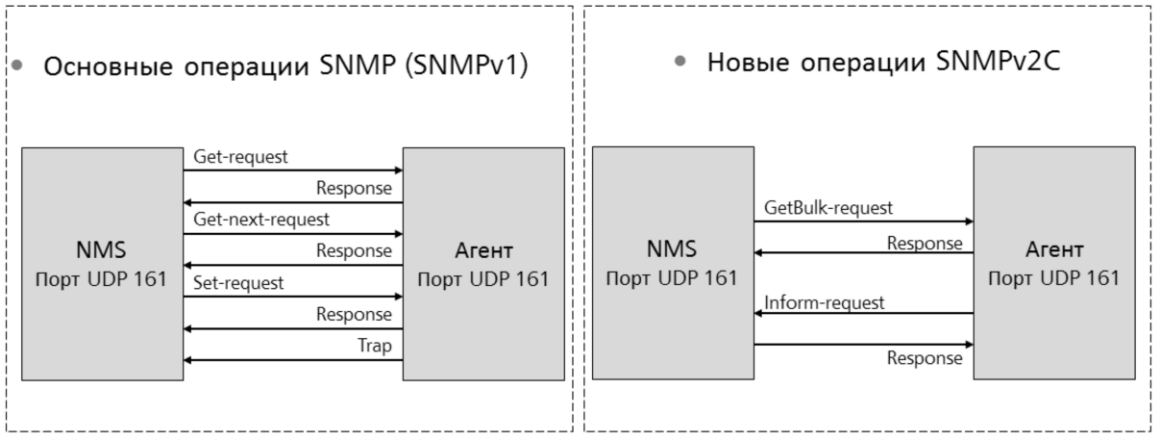


Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Модель SNMP
  - Система управления сетью (NMS): NMS обычно является независимым устройством, которое запускает приложения для управления сетью. Приложение управления сетью предоставляет как минимум один интерфейс человек-машина, через который администратор осуществляет управление сетью.
  - Агент SNMP: Агент - это программное обеспечение, установленное на управляемом устройстве. Он принимает и обрабатывает пакеты запросов от NMS и возвращает ответные пакеты в NMS. В некоторых срочных случаях агент отправляет пакет Trap в NMS.
  - Протокол SNMP: SNMP, являясь протоколом прикладного уровня в стеке TCP/IP, осуществляет обмен управляющей информацией между NMS и управляемым устройством.
  - База управляющей информации (MIB): MIB представляет собой набор управляемых объектов. MIB является мостом между NMS и агентом, позволяющий программному обеспечению NMS взаимодействовать с устройствами. Каждый агент поддерживает MIB. NMS считывает или устанавливает значение объекта, содержащегося в MIB.
  - MO – это объект, которым нужно управлять на сетевом устройстве. Управляемое устройство содержит несколько MO, например, аппаратный компонент (LPU) и набор параметров, сконфигурированных для аппаратного или программного обеспечения (протокол выбора маршрута).

Протокол SNMP – принципы работы SNMPv1/SNMPv2c

- Принципы работы SNMPv1, SNMPv2c и SNMPv3 в основном сходны.

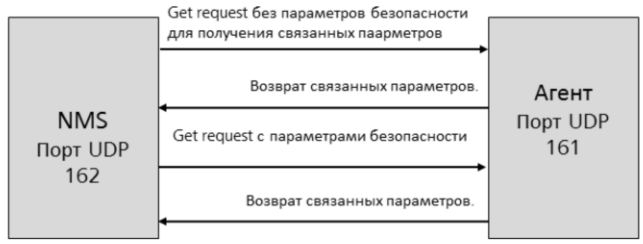


Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Основные операции:
  - get-request: NMS хочет получить один или несколько параметров из MIB агента.
  - get-next-request: NMS хочет получить следующий параметр из MIB агента.
  - set-request: NMS хочет установить один или несколько параметров из MIB агента.
  - get-response: возвращает один или несколько параметров. Генерируется агентом и передается в ответ на любую из предыдущих операций.
  - trap: отправляется агентом, чтобы проинформировать NMS о некоторых важных событиях.
- Новые операции SNMPv2C:
  - getbulk-request: запрашивает информацию об управляемых устройствах в пакетном режиме. Операция GetBulk равнозначна последующим операциям GetNext. Вы можете настроить количество операций GetNext, которые будут включены в одну операцию GetBulk.
  - Inform-request: управляемое устройство активно отправляет аварийные сигналы в NMS. После того, как управляемое устройство отправляет пакет Inform, NMS должна отправить пакет InformResponse на управляемое устройство.
- SNMPv1 и SNMPv2c слабо защищены.

Протокол SNMP – Принципы работы SNMPv3

- В SNMPv3 добавлены функции аутентификации и шифрования.

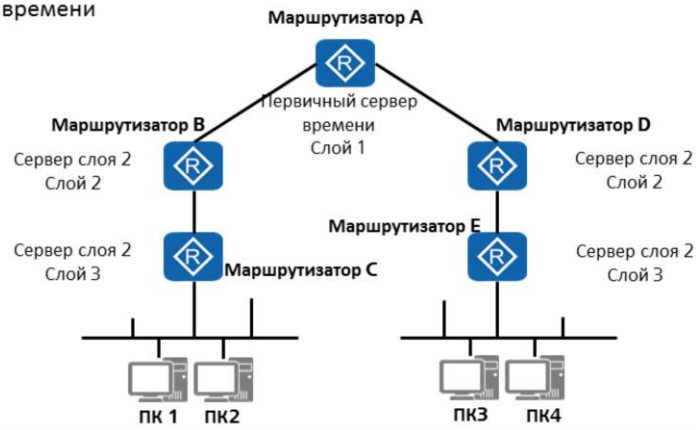


Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Принципы реализации SNMPv3 аналогичны принципам реализации SNMPv1 и SNMPv2c.
- Принципы работы SNMPv3
  - NMS отправляет сообщение Get request без параметров безопасности агенту и получает параметры безопасности (например, информацию об engine SNMP-сущности, имя пользователя, параметры аутентификации и параметры шифрования) от агента.
  - Агент отвечает на запрос от NMS и отправляет запрашиваемые параметры в NMS.
  - NMS отправляет сообщение Get request без параметров безопасности агенту (параметры безопасности - это параметры аутентификации, используемые для аутентификации личности, и параметры шифрования, используемые для шифрования пакетов. Данные параметры рассчитываются с помощью алгоритмов, настроенных в NMS).
  - Агент аутентифицирует сообщение и расшифровывает информацию сообщения. Затем он шифрует ответное сообщение и отправляет сообщение в NMS.

Протокол NTP – архитектура сети

- Архитектура сети NTP
  - Подсеть синхронизации
  - Первичный сервер времени
  - Сервер слоя 2
  - Слой

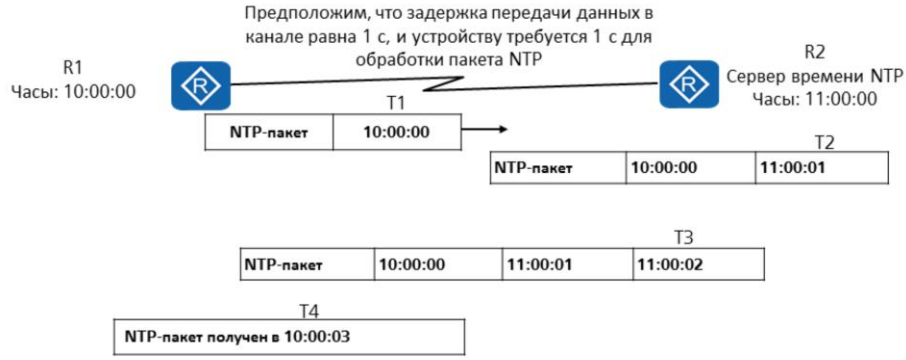


Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Основные понятия и функции NTP:
  - Подсеть синхронизации: состоит из первичного сервера времени, серверов времени слоя 2, ПК и взаимосвязанных путей передачи.
  - Первичный сервер времени: синхронизирует свои часы напрямую со стандартными эталонными часами по кабелю или радиосвязи. Как правило, стандартными эталонными часами является радиотаймер или система GPS.
  - Сервер времени слоя 2: синхронизирует свои часы с первичным сервером времени или другими серверами слоя 2 в сети. Сервер слоя 2 передает время другим узлам локальной сети (LAN) через NTP.
  - Слой: иерархический стандарт для синхронизации часов. Обеспечивает точность часов. Значение слоя колеблется от 1 до 16. Меньшее значение указывает на более высокую точность. Значение 1 указывает на самую высокую точность, а 16 указывает, что часы не синхронизированы.
- Как правило, в подсети синхронизации первичный сервер времени и серверы слоя 2 организованы в соотвествии с иерархической структурой активный/резервный. В данной структуре первичный сервер расположен на корневом узле, а серверы слоя 2 – вблизи конечных узлов. По мере увеличения слоя точность уменьшается. Низкая точность серверов слоя 2 зависит как от сетевого пути, так и от стабильности часов локального времени.

Протокол NTP – Принципы работы

- Протокол NTP
  - Синхронизирует время между серверами времени и клиентами.
  - NTP-пакеты передаются UDP через порт 123.



Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Процесс синхронизации NTP
  - R1 отправляет NTP-пакет на R2. Когда пакет покидает R1, он несет метку времени 10:00:00 (T1).
  - Когда NTP-пакет поступает на R2, R2 добавляет метку времени получения 11:00:01 (T2) в данный пакет.
  - Когда NTP-пакет покидает R2, R2 добавляет метку времени передачи 11:00:02 (T3) в данный пакет.
  - Когда R1 получает ответный пакет, он добавляет новую метку времени получения 10:00:03 (T4) в данный пакет. R1 использует полученную информацию для рассчета следующих значений:
    - Двухсторонняя задержка для NTP-пакета: задержка = (T4 - T1) - (T3 - T2)
    - Разница времени между R1 и R2: сдвиг = ((T2 - T1) + (T3 - T4))/2
  - После выполнения расчетов R1 получает информацию о том, что двухсторонняя задержка составляет 2 секунды, а сдвиг тактовой частоты равен 1 часу. В соответствии со значениями задержки и сдвига R1 настраивает собственные часы, чтобы синхронизироваться с часами R2.



Тест

1. Технологии NSF и NSR используются совместно для обесечения непрерывности услуг. ( )
   A. Верно
   B. Неверно

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Ответ:
  - B

Краткое содержание

- Технологии высокой доступности
  - Протокол BFD
  - Технология NSF
  - Технология NSR
- Технологии управления сетью
  - SNMP
  - NTP

Авторское право © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Спасибо!

www.huawei.com

HCIE-R&S

— QoS

www.huawei.com

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Введение

- По мере быстрого развития сетей сервисы в Интернете становятся все более разнообразными. Помимо традиционных областей применения, таких как WWW, электронная почта и протокол передачи файлов (FTP), появились другие сервисы, такие как IP-телефония, электронная торговля, мультимедийные игры, e-learning, телемедицина, видеотелефония, видеоконференции, видео по запросу (VOD) и стриминг фильмов. Кроме того, компании используют технологии виртуальной частной сети (VPN) для подключения своих филиалов в разных регионах, чтобы они имели доступ к корпоративным базам данных друг друга или управляли удаленными устройствами через Telnet.
- Разнообразие сервисов обогащает жизнь пользователей, но повышает вероятность перегрузок трафика в Интернете. В случае перегрузки сервисы могут столкнуться с длительными задержками или даже с потерей пакетов. В результате качество услуг сервисов ухудшается или сервисы становятся недоступными. Поэтому проблему перегрузки трафика в IP-сети необходимо срочно решить. Для этого была разработана технология QoS («качество обслуживания»), использующая политику для управления перегрузкой трафика с низкими затратами. В данном документе описываются расширенные функции QoS.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Цели

- После завершения этого курса вы будете знать:
  - Технологию классификации QoS по нескольким параметрам (multi-field).
  - Алгоритм маркерной корзины QoS.
  - Решение по развертыванию QoS в действующей сети.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.



Содержание

- **Конфигурация QoS MQC**
- Алгоритм маркерной корзины QoS
- Применение QoS

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Конфигурация QoS MQC

- Концепция MQC:
  - Модульный интерфейс командной строки QoS (MQC) позволяет классифицировать пакеты на основе характеристик и маркировать пакеты одного типа. Это позволяет предоставлять различным типам пакетов разные сервисы.
- Параметры MQC:
  - MQC включает три параметра: классификатор трафика, поведение трафика и политику трафика.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Классификатор трафика

- Правила классификации трафика 2 уровня
  - MAC-адрес источника, MAC-адрес назначения, идентификатор VLAN, MPLS EXP, поле протокола 2 уровня и поле правила ACL 4000–4999
- Правила классификации трафика 3 уровня
  - IP DSCP, IP-приоритетность, тип IP-протокола, номер порта RTP, поле правила ACL 2000–3999

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Классификатор трафика определяет группу правил сопоставления для классификации пакетов.

Конфигурация классификатора трафика

- **traffic classifier** *classifier-name* [**operator** { **and** | **or** }]
  - Параметр **and** указывает, что взаимосвязь между правилами в классификаторе трафика устанавливается следующим образом:
    - Если классификатор трафика содержит правила ACL, пакеты соответствуют классификатору трафика только тогда, когда пакеты соответствуют одному правилу ACL и всем правилам помимо ACL.
    - Если классификатор трафика не содержит правил ACL, пакеты соответствуют классификатору трафика только тогда, когда они соответствуют всем правилам в классификаторе.
  - Параметр **or** указывает на то, что взаимосвязь между правилами в классификаторе трафика устанавливается следующим образом: пакеты соответствуют классификатору трафика, если они соответствуют одному или нескольким правилам в классификаторе трафика.

  По умолчанию связь между правилами в классификаторе трафика устанавливается как OR.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- **traffic classifier** *classifier-name* [**operator** { **and** | **or** }]
  - ***classifier-name:*** определяет имя классификатора трафика.
  - **operator:** указывает на связь между правилами в классификаторе трафика. Если этот параметр не указан, отношения между правилами установлены как OR по умолчанию.
  - **and:** указывает, что взаимосвязь между правилами – AND.
  - **or:** указывает на то, что взаимосвязь между правилами – OR. При указании данного параметра пакеты соответствуют классификатору трафика, если они соответствуют одному или нескольким правилам.

Конфигурация поведения трафика

- Поведения трафика MQC включают:
  - Фильтрацию пакетов
  - Маркировку приоритетов
  - Перенаправление
  - Управление трафиком
  - Сбор статистики трафика
- Выполните команду **traffic behavior** *behavior-name* для создания поведения трафика.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

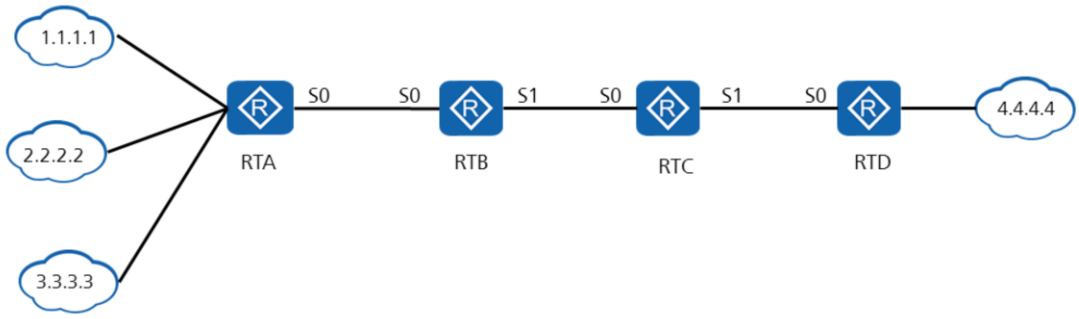
Конфигурация политики трафика

- Классификаторы трафика и поведение трафика могут быть связаны в политике управления трафиком.
  - Выполните команду **traffic policy** *policy-name*, чтобы создать политику управления трафиком и отобразите политику управления трафиком трафика.
  - Выполните команду **classifier** *classifier-name* **behavior** *behavior-name* [**precedence** *precedence-value*], чтобы связать классификатор трафика и поведение трафика.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Пример конфигурации MQC



- В RTA классифицируйте трафик по трем типам: AF11, AF21 и EF.
- В RTB отметьте трафик AF21 как трафик AF22.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Это пример конфигурации QoS на основе классов. Классификация трафика выполняется на RTA, и политики, такие как ограничение скорости и маркировка приоритетов, выполняются на RTB.

Конфигурация MQC на RTA

```
acl number 2001
 rule 0 permit source 1.1.1.1 0
acl number 2002
 rule 0 permit source 2.2.2.2 0
acl number 2003
 rule 0 permit source 3.3.3.3 0

traffic classifier Class_af11 operator and
 if-match acl 2001
traffic classifier Class_af21 operator and
 if-match acl 2002
traffic classifier Class_ef operator and
if-match acl 2003                          //Traffic classifier

traffic behavior Behavior_af11
 remark dscp af11
traffic behavior Behavior_af21
 remark dscp af21
traffic behavior Behavior_ef
remark dscp ef                             //Traffic behavior

traffic policy Mark
 classifier Class_af11 behavior Behavior_af11
 classifier Class_af21 behavior Behavior_af21
classifier Class_ef behavior Behavior_ef   //Traffic policy

interface Serial0
 ip address 12.12.12.1 255.255.255.252
 traffic-policy Mark outbound
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Классификация трафика выполняется на RTA, т.е. трафик помечается как трафик AF11, AF21 и EF на основе адреса источника.

Конфигурация MQC на RTB

```
traffic classifier Class_af21 operator and
if-match dscp af21                                  //Traffic classifier

traffic behavior Behavior_af21
remark dscp af22                                    //Traffic behavior

traffic policy dscp
classifier Class_af21 behavior Behavior_af21    //Traffic policy

interface Serial0
 ip address 23.23.23.1 255.255.255.252
 traffic-policy dscp inbound
```

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Для трафика, отмеченного разными маркерами на RTB, применяются различные политики QoS.

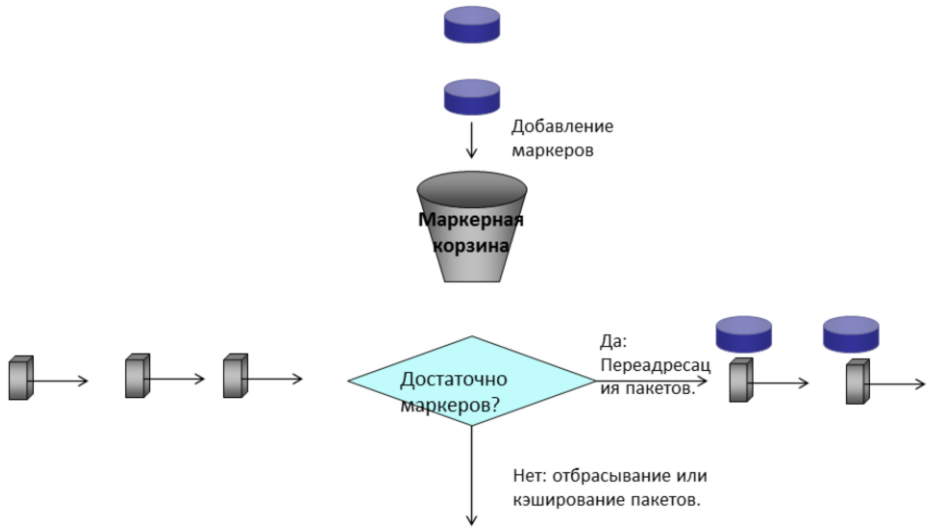


Содержание

- Конфигурация QoS MQC
- **Алгоритм маркерной корзины QoS**
- Применение QoS

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Маркерная корзина



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Для реализации управления трафиком требуется механизм для измерения трафика, проходящего через устройство. Маркерная корзина является широко используемым механизмом для измерения такого трафика.
- Когда пакеты достигают устройства, устройство получает достаточно маркеров из корзины для передачи пакетов. Если корзине недостаточно маркеров для отправки пакета, пакет ожидает накопления достаточного количества жетонов или отбрасывается. Эта функция ограничивает пакеты, которые должны быть отправлены со скоростью, меньшей или равной скорости, при которой генерируются маркеры.

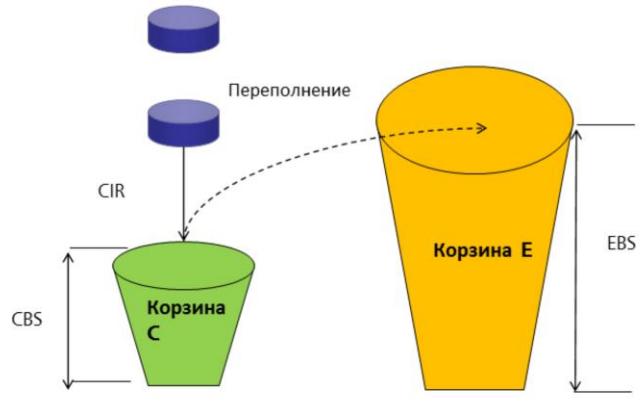
Параметры управления односкоростным трафиком

- Следующие параметры используются при управлении односкоростным трафиком:
  - Согласованная скорость передачи информации (CIR)
  - Согласованный размер всплеска (CBS)
  - Расширенный размер всплеска (EBS)

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Механизм управления односкоростным трафиком

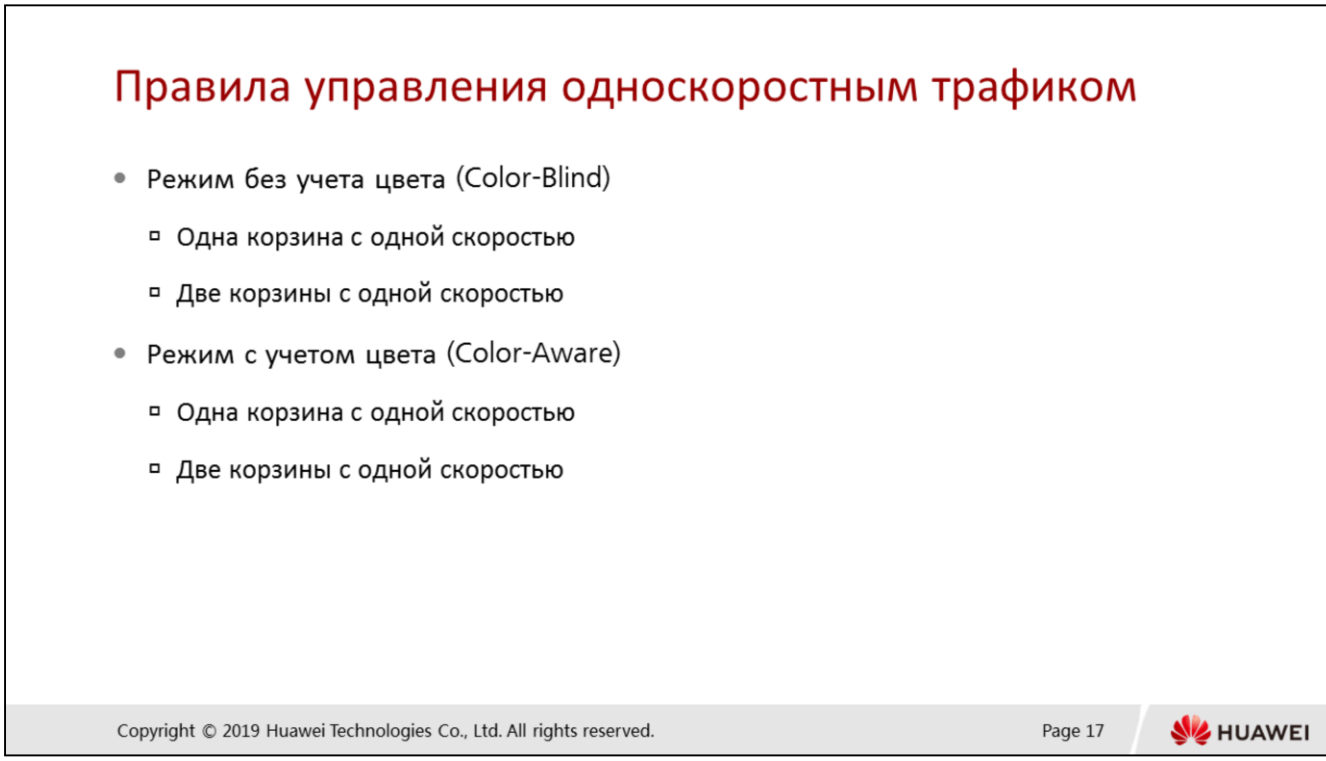
- Используются две маркерные корзины: C и E.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Маршрутизатор Huawei использует две маркерные корзины для управления односкоростным трафиком.
- Используются две маркерные корзины – C и E. Емкость корзины C – CBS, а емкость корзины E – EBS. Таким образом, общая емкость двух маркерных корзин – CBS + EBS. Чтобы предотвратить всплеск трафика, пользователи могут установить значение EBS на 0.
- Когда EBS не равен 0, управления односкоростным трафиком используются две маркерные корзины. Когда EBS равен 0, в корзину E не добавляются маркеры. Поэтому для управления односкоростным трафиком используется только корзина C. Когда используется только корзина C, пакеты помечаются как зеленые или красные.
- Что такое CIR, CBS и EBS?
  - CIR: указывает скорость, при которой интерфейс позволяет пропускать пакеты, а также скорость, при которой маркеры помещаются в маркерную корзину. Единица CIR – Кбит/с.
  - CBS: указывает согласованный объем трафика, который пропускает интерфейс, а также глубину маркерной корзины. Единица CBS – байты. CBS должен быть больше или равен размеру самого большого пакета, поступающего на устройство. Обратите внимание, что иногда один пакет может потреблять все маркеры в корзине. Чем больше CBS, тем больший всплеск трафика допустим.
  - EBS: указывает максимальный объем всплеска трафика, прежде чем скорость всего трафика превысит CIR.



- **Метод добавления маркеров для управления односкоростным трафиком**
  - При управлении односкоростным трафиком изначально обе корзины C и E заполнены маркерами. Маркеры помещаются в корзину C, а затем в корзину E, для возможного всплеска трафика со скоростью, превышающей CIR, после того как корзина C будет наполнена маркерами. После заполнения маркерами обеих корзин C и E последующие маркеры отбрасываются.
- **Правила управления односкоростным трафиком**
  - Когда пакет поступает на интерфейс, длина пакета сопоставляется с количеством маркеров в корзинах (как правило, для одного бита требуется один маркер). Если количество маркеров меньше длины пакета, пакет будет отброшен или буферизирован.
  - Tc и Te обозначают количество маркеров в корзинах C и E соответственно. Исходными значениями Tc и Te являются CBS и EBS соответственно.
  - В режиме без учета цвета применяются следующие правила, когда пакет размером B прибывает в момент t:
  - Когда маркерная корзина используется для управления односкоростным трафиком:
    - Если $Tc(t) - B \geq 0$, пакет помечается зеленым цветом, а Tc уменьшается на величину B.
    - Если $Tc(t) - B < 0$, пакет помечается красным цветом, а Tc остается неизменным.
  - Когда используется две маркерные корзины для управления односкоростным трафиком:
    - Если $Tc(t) - B \geq 0$, пакет помечается зеленым цветом, а Tc уменьшается на величину B

- Если Tc(t) – B < 0, но Te(t) – B ≥ 0, то пакет помечается желтым цветом, а Te уменьшается на величину B.
- Если Te(t) – B < 0, то пакет помечается красным цветом, и ни Tc, ни Te не уменьшаются.

- В режиме с учетом цвета применяются следующие правила, когда пакет размером B поступает в момент t:
- Когда маркерная корзина используется для управления односкоростным трафиком:
  - Если пакет помечен зеленым цветом, а Tc(t) – B ≥ 0, пакет повторно отмечается зеленым, а Tc уменьшается на величину B.
  - Если пакет помечен зеленым цветом, а Tc(t) – B < 0, цвет пакета меняется на красный, а Tc остается неизменным.
  - Если пакет помечен желтым или красным цветом, цвет пакета меняется на красный независимо от длины пакета. Значение Tc остается неизменным.
- Когда используется две маркерные корзины для управления односкоростным трафиком:
  - Если пакет помечен зеленым цветом, а Tc(t) – B ≥ 0, пакет повторно отмечается зеленым, а Tc уменьшается на величину B.

- Если пакет помечен зеленым цветом, а $Tc(t) - B < 0$, но $Te(t) - B \geq 0$, пакет отмечается желтым цветом, а Te уменьшается на величину B.
- Если пакет помечен желтым цветом и $Te(t) - B \geq 0$, то пакет повторно отмечается желтым, а Te уменьшается на величину B.
- Если пакет помечен желтым и $Te(t) - B < 0$, то цвет пакета меняется на красный, а Te остается неизменным.
- Если пакет помечен красным, пакет помечается красным цветом, независимо от длины пакета. Значения Tc и Te остаются неизменными.

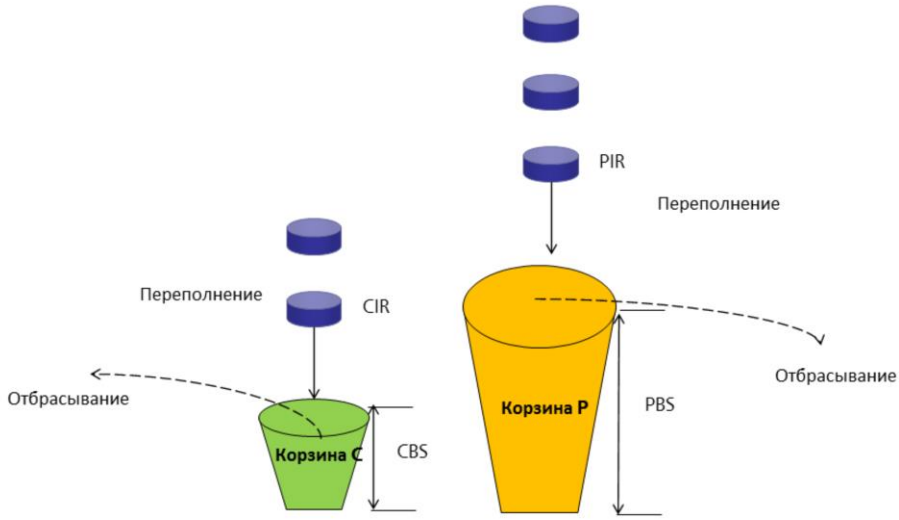
Параметры управления двухскоростным трафиком

- Согласованная скорость передачи информации (CIR)
- Согласованный размер всплеска (CBS)
- Пиковая скорость передачи информации (PIR)
- Размер пикового всплеска (PBS)

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- CIR – скорость, при которой интерфейс позволяет пропускать пакеты, а также скорость, при которой маркеры помещаются в маркерную корзину. Единица CIR – Кбит/с.
- CBS – согласованный объем трафика, который пропускает интерфейс, а также глубину маркерной корзины. Единица CBS – байты. CBS должен быть больше или равен размеру самого большого пакета, поступающего на устройство.
- PIR – максимальная скорость, при которой интерфейс пропускает пакеты, в Кбит/с. PIR должен быть больше или равен CIR.
- PBS – максимальный объем трафика, который интерфейс пропускает при всплеске трафика.

Механизм управления двухскоростным трафиком



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Двухскоростной трехцветный маркер используют две маркерные корзины и фокусируется на скорости всплеска трафика. Односкоростной трехцветный маркер переносит избыток маркеров из первой во вторую корзину, в то время как двухскоростной трехцветный маркер использует две маркерные корзины, которые хранят маркеры раздельно. Таким образом, двухскоростной трехцветный маркер определяет две скорости при которой маркеры кладутся в корзину. Эти две маркерные корзины обозначаются как C и P. Емкость корзины C равна CBS, а емкость корзины P – PBS. Маркеры со скоростью CIR помещаются в корзину C и в ведро P со скоростью PIR.
    - Маркер является двухскоростным, поскольку маркеры помещаются в две маркерные корзины в зависимости от одной из двух скоростей.
- **Метод добавления маркеров для двухскоростного управления трафиком**
    - Изначально корзины C и P заполнены маркерами. Маркеры помещаются в корзины C и P при скорости CIR и PIR соответственно. Корзины C и P работают отдельно. Когда одна корзина заполняется маркерами, любые последующие маркеры для корзины отбрасываются, но маркеры продолжают поступать в другую корзину, если она не заполнена.
- **Правила для двухскоростного управления трафиком**
    - Двухскоростной трехцветный маркер фокусируется на скорости всплеска трафика и проверяет соответствие скорости трафика спецификациям. Таким образом, трафик измеряется на основе параметров корзины P, а затем корзины C.
    - Двухскоростной трехцветный маркер работает в режимах с учетом и без учета цвета. Tc и Tp ссылаются на номера маркеров в корзинах C и P соответственно. Исходными значениями Tc и Tp являются CBS и PBS.
    - В режиме без учета цвета применяются следующие правила, когда пакет размером B прибывает в момент t:
        - Если $Tp(t) - B < 0$, то пакет отмечается красным цветом, а значения Tc и Tp остаются

неизменными.

- Если $Tp(t) - B \geq 0$, но $Tc(t) - B < 0$, пакет отмечается желтым цветом, а Tp уменьшается на величину B.

- Если Tc(t) – B ≥ 0, пакет отмечается зеленым цветом, а Tp и Tc уменьшаются на величину B.
- В режиме с учетом цвета применяются следующие правила, когда пакет размером B поступает в момент t:
  - Если пакет помечен зеленым цветом и Tp(t) – B < 0, то пакет обозначается красным цветом, и значения Tp и Tc не уменьшаются.
  - Если пакет помечен зеленым цветом и Tp(t) – B ≥ 0, но Tc(t) – B < 0, то пакет обозначается желтым цветом, Tp уменьшается на величину B, а Tc остается неизменным.
  - Если пакет помечен зеленым цветом, а Tc(t) – B ≥ 0, то пакет обозначается зеленым цветом, а Tp и Tc уменьшаются на величину B.
  - Если пакет помечен желтым цветом и Tp(t) – B < 0, то пакет обозначается красным цветом, и значения Tp и Tc не уменьшаются.
  - Если пакет помечен желтым цветом и Tp(t) – B ≥ , то пакет обозначается желтым цветом, а Tp уменьшается на величину B, Tc остается неизменным.
  - Если пакет помечен красным цветом, пакет помечается красным цветом независимо от длины пакета. Значения Tp и Tc остаются неизменными.

- Что такое CIR, CBS и EBS?
  - **cir** *cir-value* указывает на согласованную скорость трафика, которую пропускает интерфейс. Значение представляет собой целое число от 0 до 4294967295, в Кбит/с.
  - **pir** *pir-value* указывает на пиковую скорость трафика, которую пропускает

интерфейс. Значение представляет собой целое число от 0 до 4294967295, в Кбит/с. Значение *pir-value* должно быть больше или равно сконфигурированно

му значению *cir-value*.

- **cbs** *cbs-value* указывает согласованный объем трафика, который пропускает интерфейс, и глубину первой корзины (при

условии, что это корзина C). Значение представляет собой целое число от 0 до 4294967295, в байтах. Значение CBS должно быть больше значения CIR. Значение по

умолчанию изменяется в зависимости от значения *cir-value*.

- **pbs** *pbs-value* указывает на пиковый объем трафика, который пропускает интерфейс, и

глубину второй корзины (при условии, что это ведро P). Значение представляет собой целое число от 0 до 4294967295, в байтах. Значение по умолчанию зависит от значения *pir-*

value.



Содержание

- Конфигурация QoS MQC
- Алгоритм маркерной корзины QoS
- **Применение QoS**

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Применение QoS в действующей сети: планирование и развертывание

- Классификация трафика, маркировка трафика и ограничение скорости настраиваются на входящем пользовательском интерфейсе, а формирование трафика осуществляется на исходящем пользовательском интерфейсе (если речь идет о пакетах различных уровней, планирование очереди и предотвращение перегрузок настраиваются на исходящем пользовательском интерфейсе). Планирование очереди и предотвращение перегрузок настраиваются на исходящем сетевом интерфейсе.
- Рекомендуется настроить ограничения скорости для приоритетных очередей (PQS) на основе сервисных требований.
- Рекомендуется настроить классификацию трафика (классификацию multi-field) на границе сети (ближе к пользователям и источникам услуг) для упрощения последующей классификации трафика. Рекомендуется использовать классификацию Behavior aggregate на оборудовании на уровне агрегации или верхнему уровне, чтобы уменьшить нагрузку на оборудование.
- В целом, пакеты услуг с более низким приоритетом отбрасываются больше и раньше, чем пакеты услуг с более высоким приоритетом. Пакеты сервисов, предоставляемых в реальном времени, обрабатываются с помощью политики отбрасывания конца очереди. Пакеты протокола сигнализации не отбрасываются.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Применение QoS в действующей сети: планирование приоритета сервисов

- Сообщения управления: включают важные пакеты, такие как пакеты протоколов, используемые для связи с NMS и другими устройствами, и имеют чрезвычайно важное значение для действующей сети. Таким пакетам должно быть присвоено самое приоритетное значение.
- Поток речевых пакетов: требуется обеспечить малое время задержки, низкий уровень дрожания и низкий коэффициент потери пакетов. Такие пакеты должны быть помещены в очередь EF.
- Потоки видео в реальном времени (например, видеоконференции и видеовызовы): требуется обеспечить малое время задержки, низкий уровень дрожания и низкий коэффициент потери пакетов. Такие пакеты должны быть помещены в очередь EF.
- Офисные услуги: низкие требования к задержкам и дрожанию. Как правило, помещаются в очереди AF и BE.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Применение QoS в действующей сети: управление трафиком и формирование трафика

- Для трафика, отправленного с некоторых серверов NMS, уязвимых к вирусам, необходимо настроить контроль трафика, чтобы избежать атак на голосовые и видеосервисы. Трафик, отправленный с серверов NMS, имеет наивысший приоритет при организации очередей на основе приоритета.
- Чтобы предотвратить DDoS-атаки от офисных сервисов на другие сервисы из-за вируса или превышения полосы пропускания, сконфигурируйте управление трафиком (CAR) для каждого потока доступа на основе SLA. Задайте самый низкий приоритет избыточному трафику, чтобы он переадресовывался в оптимальном режиме вместо прямого отбрасывания. Эта конфигурация помогает сбалансированно использовать сетевые ресурсы и повышать уровень удовлетворенности клиентов.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Применение QoS в действующей сети: планирование очереди и политика отбрасывания пакетов

- Включите классификацию behavior aggregate для входящих пакетов на пограничных маршрутизаторах в магистральной сети, чтобы планирование очереди осуществлялось на основе приоритетов, переносимых пакетами на непограничных маршрутизаторах в магистральной сети. Соответствие между значениями IP DSCP/precedence и MPLS EXP обычно конфигурируется на пограничных маршрутизаторах сети MPLS, подключенных к IP-сети. Как правило, высокий приоритет имеют сообщения управления и пакеты голосовых вызовов, видеоконференций и видеовызовов, которые предпочтительно переадресовываются. Пакеты других услуг могут быть запланированы с использованием механизма взвешенной справедливой очереди (WFQ).
- Отбрасывание конца очереди используется для услуг с приоритетом в очереди (PQ), таких как голосовые и видеовызовы, чтобы переадресовывать пакеты PQ без отбрасывания. Пакеты теряются только при исчерпании ресурсов PQ. Чтобы предотвратить глобальную синхронизацию TCP, используется механизм WRED для планирования услуг WFQ. Задайте высокий порог отбрасывания пакетов для высокоприоритетного трафика и порог низкого уровня для низкоприоритетного трафика, чтобы у низкоприоритетного трафика была более высокая вероятность отбрасывания пакетов.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Спасибо!

www.huawei.com

HCIE-R&S

— SDN VXLAN

www.huawei.com

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Введение

- VXLAN – очень важная оверлейная технология. Она широко используется в программно-конфигурируемых сетях (SDN), например, для центров обработки данных (ЦОД) с интеграцией облака и сети и совместно с Cloud VPN.
- В этой презентации вы узнаете причины появления и основные понятия VXLAN.
- Анализируя сетевой трафик VXLAN, вы узнаете, как предоставляются комплексные услуги в сети SDN DCN.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Цели

- После прохождения этого курса вы будете знать:
  - Основные понятия SDN
  - Почему технология VXLAN необходима в сетях ЦОД
  - Основные понятия VXLAN
  - Процедуры обработки пакетов VXLAN
  - Применение VXLAN

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Содержание

- **Обзор SDN**
- Проблемы перехода к облачным сервисам для традиционных сетей ЦОД
- Основные понятия VXLAN
- Применение VXLAN
- Понятия и сценарии применения VXLAN в облачных ЦОД

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Происхождение SDN-сетей



Профессор Ник Макоуэн и его коллеги из Стэнфордского университета разработали протокол OpenFlow, в котором переадресацией данных в сети управляет контроллер.





Команда Ника Макоуэна, программа Clean Slate Program

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Технология SDN была создана для кампусных сетей в 2006 году. В 2012 году технология SDN был впервые использована в коммерческих целях. В 2012 году технология SDN оказалась в центре внимания в связи с развертыванием SDN-сетей компанией Google, в результате чего ее стали использовать в телекоммуникационных сетях.
- Далее описываются основные события, связанные с разработкой SDN (вам нужно знать только ключевые моменты).
- В 2006 году технология SDN была разработана в рамках программы Clean Slate Program Стэнфордского университета, финансируемой проектом GENI (США). Исследовательская группа под руководством профессора Ника Макоуэна из Стэнфордского университета предложила концепцию протокола OpenFlow, позволяющего работать с экспериментальными протоколами для проведения экспериментов и внедрения инновационных решений в кампусных сетях. Позже, благодаря характеристикам программируемости, которые протокол OpenFlow обеспечил сетям, появилась концепция SDN. Конечная цель программы Clean Slate Program состоит в том, чтобы переосмыслить архитектуру Интернета с целью изменения устаревшей сетевой инфраструктуры, которую сложно развивать.
- В 2007 году студент из Стэнфорда Мартин Касадо возглавил проект Ethane по сетевой безопасности и управлению. В проекте была предпринята попытка применения централизованного контроллера, с помощью которого сетевые администраторы могли определять политики управления безопасностью на основе сетевых потоков и применять эти политики к различным сетевым устройствам, тем самым реализуя контроль безопасности для всей сети.
- В 2008 году, вдохновленный проектом Ethane и предыдущим проектом Sane, профессор Ник Макоуэн и его команда предложили концепцию OpenFlow. В документе под названием «OpenFlow: поддержка инноваций в кампусных сетях», опубликованном в ACM SIGCOMM, Ник

Макоуэн впервые подробно представил концепцию OpenFlow. В дополнение к описанию того, как работает протокол OpenFlow, в этой статье перечислены несколько сценариев его применения.

- Опираясь на программируемость, которую OpenFlow предоставляет для сетей, Ник Макоуэн и его команда предложили концепцию программно-определяемой сети (SDN). В 2009 году технология SDN была включена в десятку самых передовых технологий по версии Technology Review. После этого технология была широко признана и стала использоваться в университетах и промышленности.
- В декабре 2009 года была выпущена версия OpenFlow 1.0 для использования в коммерческих продуктах. Наряду с этим были усовершенствованы такие функции, как плагин для получения заголовков пакетов OpenFlow в Wireshark, инструмент отладки OpenFlow (liboftrace), эмуляция виртуальной машины OpenFlow (OpenFlowVMS) и др. На данный момент представлены версии OpenFlow 1.1, 1.2, 1.3 и 1.4. Текущая версия OpenFlow – 1.5.1.
- В марте 2011 года благодаря профессору Нику Макоуэну был создан фонд Open Network Foundation (ONF) для содействия стандартизации и развитию архитектуры и технологий SDN. В ONF входят 96 членов, включая семь компаний-основателей: Google, Facebook, NTT, Verizon, Deutsche Telekom, Microsoft и Yahoo.
- В мае 2011 года компания NEC выпустила первый коммерческий коммутатор OpenFlow.
- В апреле 2012 года компания Google объявила, что ее магистральная сеть полностью работает на OpenFlow и подключена к 12 ЦОД по всему миру через сети 10 Гбит/с, в результате чего эффективность использования канала WAN повысилась с 30% до почти 100%.
- Это доказало, что OpenFlow уже не просто исследовательская модель, а готовая для коммерческого использования технология.
- В июле 2012 года компания VMware приобрела компанию Nicira, специализирующуюся на SDN и виртуализации сетей, за 1,26 миллиарда долларов. Nicira – это молодая компания, которая переосмысляет работу ЦОД. Она создала сетевую виртуальную платформу (NVP) на основе OpenFlow. OpenFlow – это проект с открытым исходным кодом, созданный Мартином Касадо во время его работы над докторской диссертацией в Стэнфорде. Он стал соучредителем Nicira вместе с двумя профессорами Стэнфордского университета, Ником Макоуэном и Скоттом Шенкером. Поглощение компанией VMware превратило технологические исследования Касадо, проводившиеся более десяти лет, в реальность. Сетевое программное обеспечение было удалено с аппаратных серверов, что также стало первым шагом выхода технологии SDN на рынок.
- В конце 2012 года компании AT&T, BT, Deutsche Telekom, Orange, Italy Telecom, Spain Telecom и Verizon совместно создали отраслевой альянс виртуализации сетевых функций (NFV) с целью внедрения технологии SDN в телекоммуникационную отрасль. Альянс состоит из 52 сетевых операторов, поставщиков телекоммуникационного оборудования, поставщиков ИТ-оборудования и поставщиков технологий.
- В апреле 2013 года Cisco и IBM совместно с Microsoft, Big Switch, Brocade, Citrix, Dell, Ericsson, Fujitsu, Intel, Juniper Networks, Microsoft, NEC, HP, Red Hat и Vmware создали проект Open Daylight. В сотрудничестве с Linux Foundation организация разработала контроллеры SDN и нисходящие и восходящие API-интерфейсы, стремясь разрушить монополию крупных поставщиков на сетевое оборудование, стимулировать инновации в области сетевых технологий, упростить управление сетью и снизить затраты на управление. В этой организации состоят только поставщики SDN, но нет пользователей SDN (интернет-пользователей и операторов). Проект Open Daylight занимается разработкой контроллеров SDN и расширением API. Они объявили о выпуске промышленного контроллера SDN с открытым исходным кодом.
- Дополнительная информация о создании SDN:

- Программа Clean Slate
  - Слабые места: постоянное исправление существующей сетевой архитектуры затрудняет решение фундаментальных проблем. Возможно, окончательным решением этой проблемы станет пересмотр сетевой архитектуры .
  - Конечная цель программы Clean Slate Program состоит в том, чтобы переосмыслить архитектуру Интернета с целью изменения устаревшей сетевой инфраструктуры, которую сложно развивать.
  - Программа Clean Slate:
    - В широком смысле включает различные проекты по разработке сетей следующего поколения (NGN).
    - В узком смысле подразумевает план лабораторных исследований под руководством профессора Ника Макоуэна из Стэнфордского университета (место создания технологии SDN).
- Проект Ethane (подпроект программы Clean Slate)
  - Ethane – это проект по сетевой безопасности и управлению, который возглавлял студент Стэнфорда Мартин Касадо. В проекте была предпринята попытка применения централизованного контроллера, с помощью которого сетевые администраторы могли определять политики управления безопасностью на основе сетевых потоков и применять эти политики к различным сетевым устройствам, тем самым реализуя контроль безопасности для всей сети.
  - Вдохновленные этим проектом, Мартин и его наставник Ник Макоуэн предложили концепцию OpenFlow.

Определение SDN

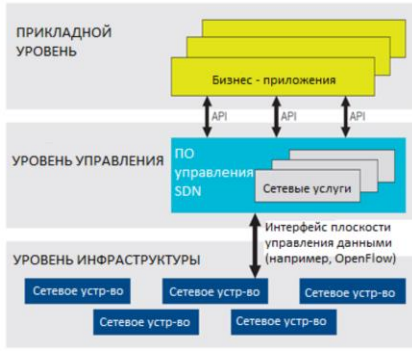
Программно-определяемая сеть (SDN) – это абсолютно новая сетевая архитектура, в которой плоскость управления отделена плоскости передачи данных для гибкого управления сетевым трафиком. Она обеспечивает отличную платформу для инноваций в базовой сети и приложениях.



Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Архитектура сети SDN, определенная ONF

Архитектура программно-определяемой сети



Источник: документ ONF, 13 апреля 2012 г.

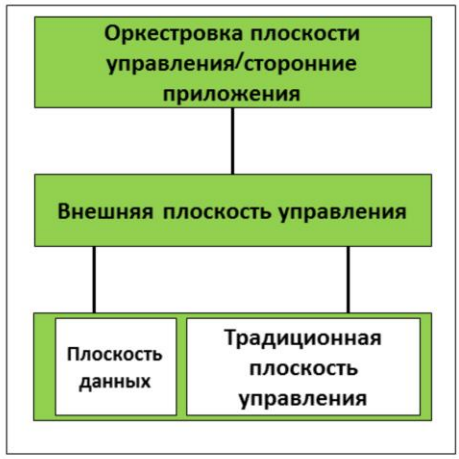


Организация ONF выполняет стандартизацию оборудования передачи для сетей SDN на базе протокола OpenFlow с разделением плоскостей управления и передачи данных. Ключевым моментом является стандартизация протокола OpenFlow.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Архитектура SDN для традиционных поставщиков телекоммуникационного оборудования

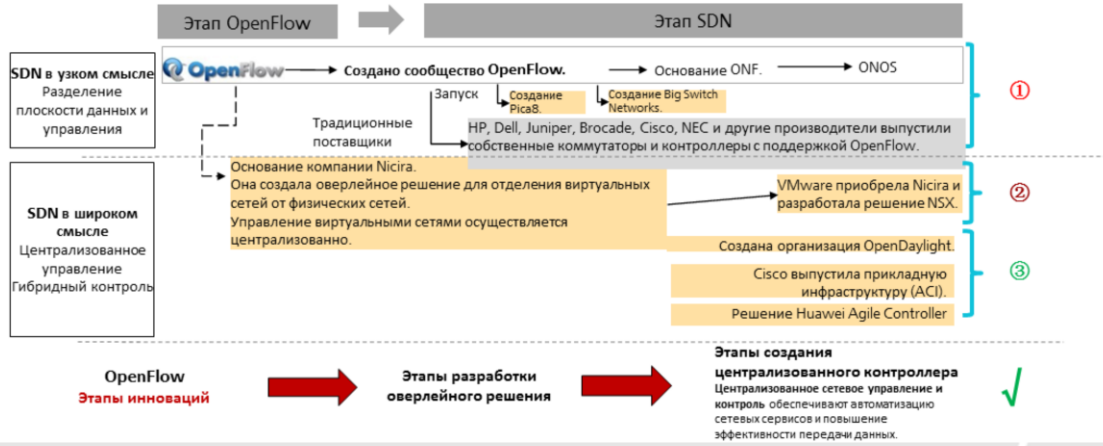




Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

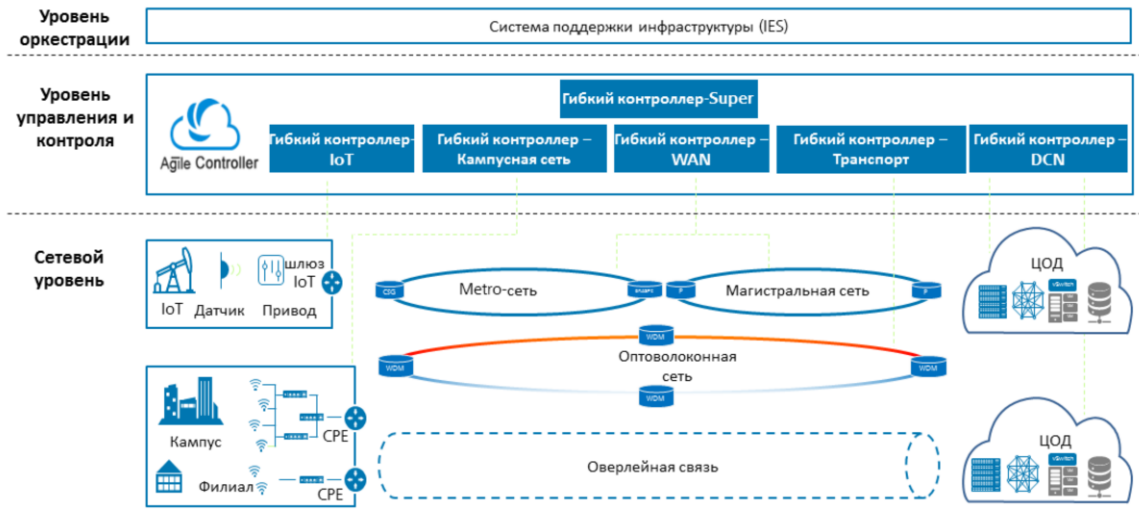
Основные этапы технического развития SDN

- В 2006 году Стэнфордский университет представил протокол OpenFlow. Этот протокол отделяет плоскость данных, в которой работают сетевые устройства, от плоскости управления. Плоскость управления может гибко управлять сетевым трафиком.
- В дополнение к умеренному разделению плоскостей управления и данных, основной особенностью SDN в ЦОД Huawei является разделение плоскостей управления и контроля для автоматического предоставления сетевых сервисов, в результате чего упрощается быстрое развертывание ЦОД.



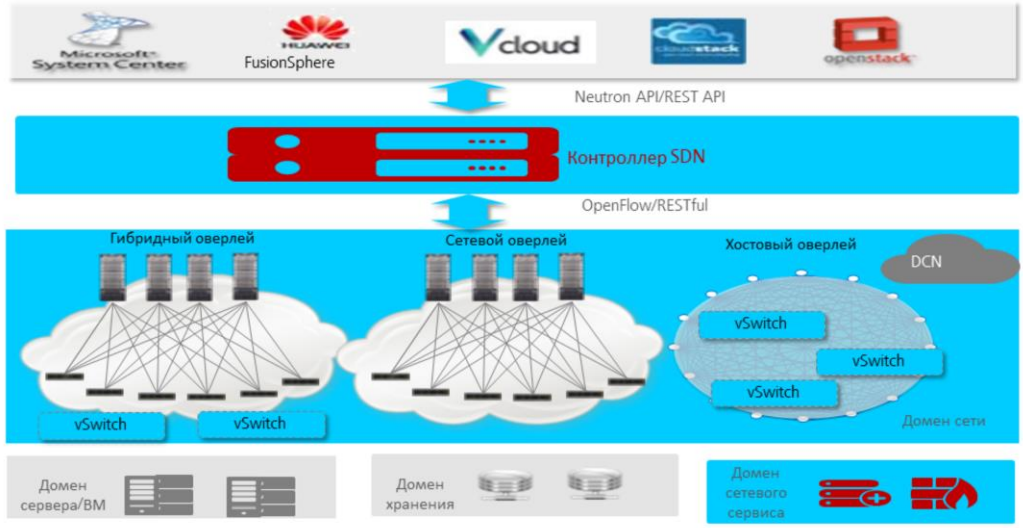
Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Решение SDN Huawei



Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Решение DCN SDN



Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

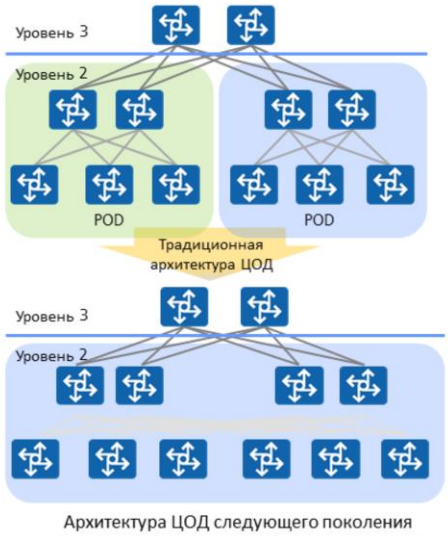
HUAWEI

Содержание

1. Обзор SDN
2. **Проблемы перехода к облачным сервисам для традиционных сетей ЦОД**
3. Основные понятия VXLAN
4. Применение VXLAN
5. Понятия и сценарии применения VXLAN в облачных ЦОД

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Тенденция развития ЦОД (1)



Архитектура ЦОД следующего поколения

Традиционная архитектура ЦОД

- В традиционных сетях ЦОД уровень 2 включает только коммутаторы доступа или агрегации, а виртуальные машины (ВМ) можно переносить только внутри домена уровня 2. Чтобы перенести виртуальные машины в другой домен уровня 2, необходимо изменить их IP-адреса и прервать работу сервисов на время переноса.

Архитектура ЦОД следующего поколения

- В эпоху облачной обработки данных операторам ЦОД требуется выполнять миграцию виртуальных машин в пределах более крупного домена, чтобы эффективнее использовать ресурсы ЦОД.
- Поскольку между серверами передается большой объем внутреннего трафика ЦОД, требуется использовать неблокирующую пересылку данных для полноценного использования ресурсов сетевого канала.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Размер ВМ ограничен спецификациями сети.
  - В крупномасштабной сети уровня 2 пакеты данных передаются на уровне 2 на основе MAC-адресов. Однако объем таблицы MAC-адресов ограничен, поэтому количество виртуальных машин также ограничено.

Тенденция развития ЦОД (2)



- Традиционные технологии для сетей 2 уровня, такие как STP и CSS + iStack, не подходят для построения крупномасштабной сети 2 уровня. Для построения таких сетей применяется технология VXLAN, которая поддерживает однородные сети fat tree с высокой загрузкой полосы пропускания.

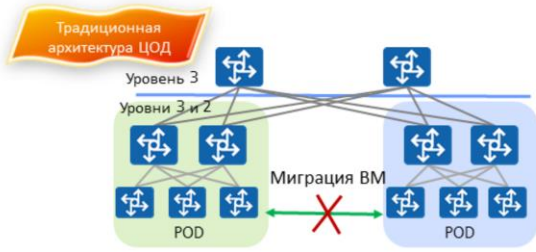
Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Ограничения возможностей изоляции сети:
  - В настоящее время для изоляции сети используются технологии VLAN или VPN. Поле Tag в сети VLAN, описанное в стандарте IEEE 802.1Q, имеет только 12 бит и может включать не более 4096 сетей VLAN. Это не удовлетворяет требованию к идентификации многочисленных групп пользователей в крупномасштабной сети уровня 2.
  - Сети VLAN и VPN в традиционных сетях 2 уровня не поддерживают динамическую настройку параметров сети.

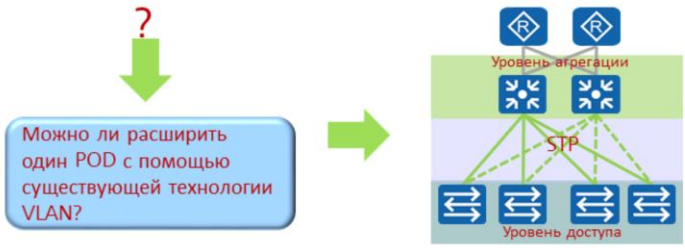


- Компания Google использует крупномасштабные серверные кластеры. Из-за большого объема взаимодействия между серверами требуется использовать неблокирующие сети.
- Количество серверов Google в одном кластере достигло 10 000.
- Интернет-провайдеры в Китае планируют разместить 20 000 серверов в одном кластере.
- Количество и емкость сетевых интерфейсов являются основными факторами, определяющими размер кластера.
- Межрегиональный серверный кластер улучшает возможности аварийного восстановления системы.
- Крупномасштабная сеть 2 уровня:
  - Требуется возможность неблокирующей передачи горизонтального сетевого трафика.

Почему традиционные сети не могут быть большими?



- **Сеть VLAN не может пересечь границу уровня 3.**
  Следовательно, в традиционных сетях ЦОД шлюзы создаются на агрегирующих коммутаторах, которые обмениваются данными друг с другом посредством базовых коммутаторов уровня 3. Виртуальные машины можно переносить только в пределах одного POD. Чтобы перенести виртуальные машины в другой POD внутри домена 2 уровня, необходимо изменить их IP-адреса и прервать работу сервисов на время миграции.



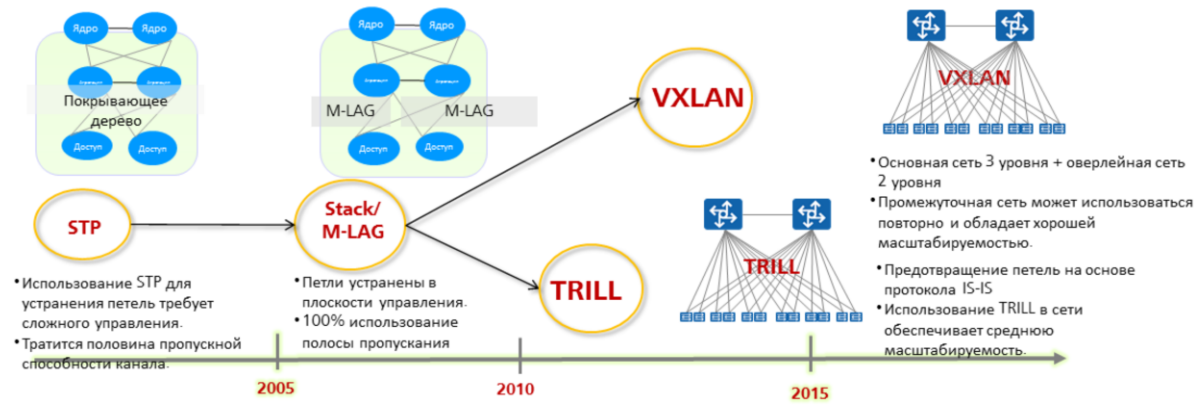
Технология STP решает проблему образования петель в сети, но имеет следующие недостатки:

- Конвергенция в протоколе STP занимает много времени. Она применяется только к сетям с макс. 50 сетевыми узлами и не подходит для крупномасштабных сетей облачных ЦОД.
- Когда протокол STP используется для построения сети без петель, необходимо заблокировать половину каналов, что снижает использование полосы пропускания.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Тенденции развития архитектуры сети ЦОД



- Использование стандарта TRILL решает проблемы протокола STP. С помощью усовершенствованного алгоритма маршрутизации на основе состояния канала TRILL обеспечивает расширение протокола IS-IS и позволяет создать сеть без петель для балансировки нагрузки множественных путей.
- Виртуальная расширяемая локальная сеть (VXLAN) обеспечивает лучшую доступность, масштабируемость и простоту эксплуатации и обслуживания, поэтому ее предпочитают поставщики ИТ и КТ.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Секторы ИТ и КТ объединяют усилия.
- TRILL – это революционная технология. VXLAN – это усовершенствованная технология.

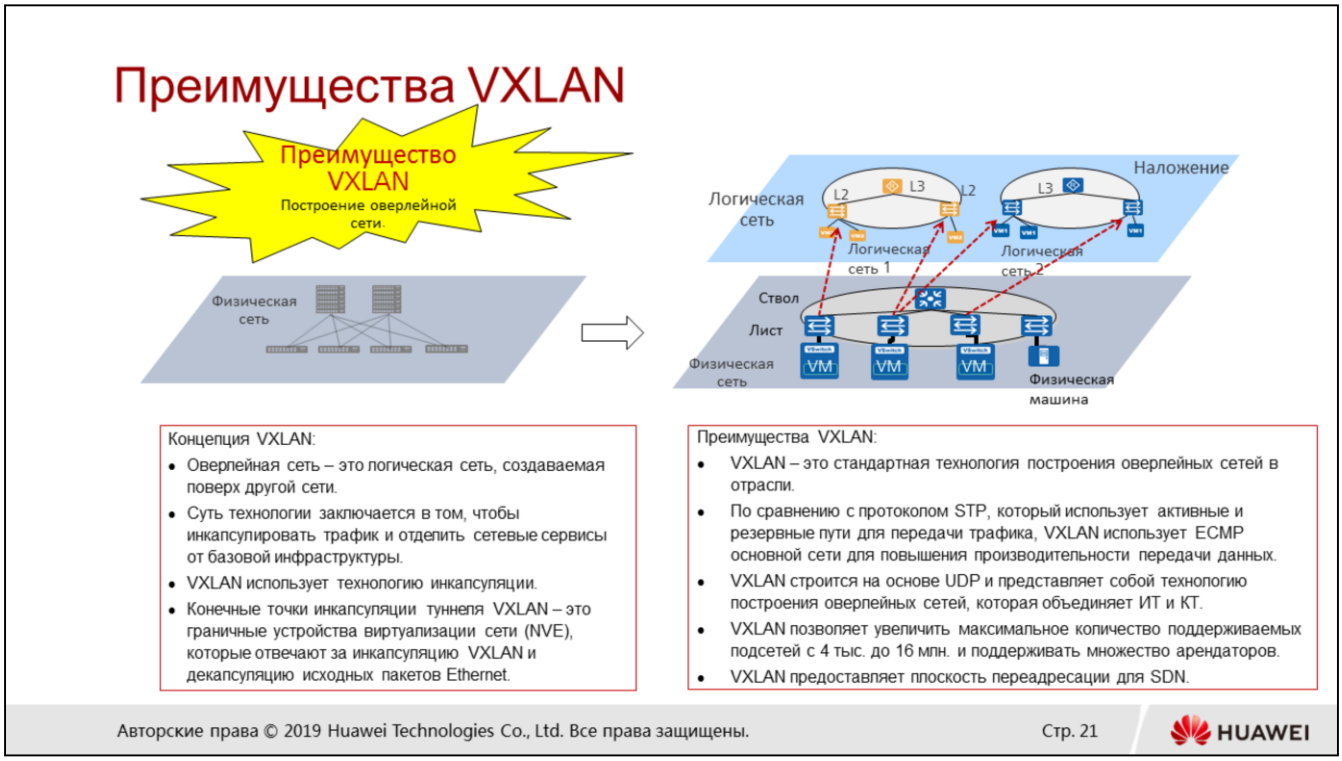
VXLAN – де-факто стандарт для построения оверлейных сетей в отрасли

Требования к высокопроизводительным сетям облачных ЦОД		VXLAN	CSS/SVF	TRILL
> 4 тыс. арендаторов	Арендуемый ЦОД должен обслуживать большое количество арендаторов.	**16 млн.**	4 тыс.	4 тыс. (последняя версия стандарта позволяет обслуживать 16 млн. арендаторов)
Сохранение существующих сетей	Новая сеть может быть построена на основе существующей сети.	**Существующая сеть должна поддерживать общие функции уровня 3.**	Требуется создать новую архитектуру.	Требуется создать новую архитектуру.
Возможности SDN	Можно легко обновить до сети SDN.	**Наложение является важным этапом развертывания SDN.**	Не поддерживается	Не поддерживается
Стандартный протокол	Позволяет различным поставщикам взаимодействовать друг с другом.	**Стандартный**	Определяется поставщиком	Стандартный
Возможности перекрестных соединений ЦОД	Крупномасштабная сеть 2 уровня может быть построена через IP WAN.	**Поддерживается**	Не поддерживается	Не поддерживается

- VXLAN обладает более широкими возможностями по поддержке технологии SDN и множества арендаторов. Поэтому VXLAN стала популярной технологией в отрасли.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI



- Физическая сеть
  - Физическая сеть обладает высокой пропускной способностью и большой производительностью.
  - Крупномасштабная сеть уровня 2 требует использования протокола STP для устранения петель.
  - Поддерживает изоляцию не более 4 тыс. сетей VLAN.
  - Миграция виртуальной машины не является гибкой и требует изменения конфигурации физической сети.
- Оверлейная сеть
  - Оверлейная сеть обладает большей мобильностью, потому что ее инфраструктура не привязана к географии и удовлетворяет требования к гибкости сетей уровня 2.
  - Оверлейная сеть поддерживает оказание услуг по требованию. Когда услуги меняются, вносить изменения в основной сети не требуется.
  - Оверлейная сеть отделена от физической сети.

Содержание

1. Обзор SDN
2. Проблемы перехода к облачным сервисам для традиционных сетей ЦОД
3. **Основные понятия VXLAN**
4. Применение VXLAN
5. Понятия и сценарии применения VXLAN в облачных ЦОД

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

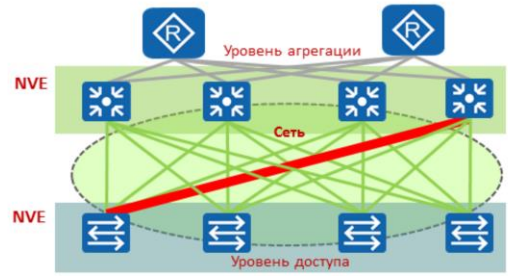
Основные понятия VXLAN

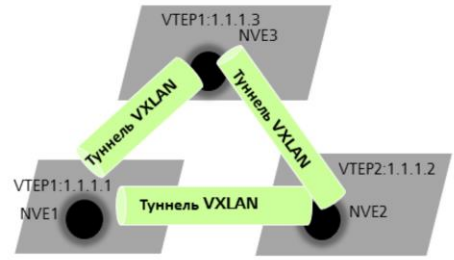
Организация сети 2 уровня на базе NVo3

Технологии NVO3 обеспечивают создание виртуальных сетей на основе оверлейных IP-сетей 3 уровня. Стандартные технологии NVO3 включают VXLAN, NVGRE и STT.
Устройство, работающее по технологии NVO3, называется граничным устройством виртуализации сети (NVE). Устройство NVE находится на границе оверлейной сети и реализует функции виртуализации уровня 2 и уровня 3.

VXLAN – самая влиятельная технология NVO3, в которой используется режим инкапсуляции пакетов MAC в пакеты UDP для создания виртуальных локальных сетей на основе IP-оверлеев.

- Точки VTEP используются для идентификации NVE в сети VXLAN.
- Каждое устройство NVE имеет по крайней мере одну точку VTEP, которая определяется IP-адресом NVE.
- Туннель VXLAN определяется по двум точкам VTEP.



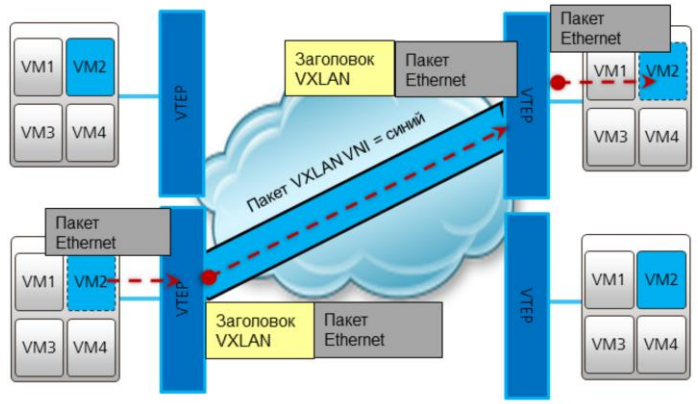


Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Понятие VXLAN — точка VTEP

- Точки VTEP используются для идентификации устройств NVE в сети VXLAN.
- У каждого устройства NVE есть как минимум одна точка VTEP, которая определяется IP-адресом NVE.
- По двум точкам VTEP определяется туннель VXLAN, который совместно используется всеми идентификаторами VXLAN (VNI) между двумя устройствами NVE.

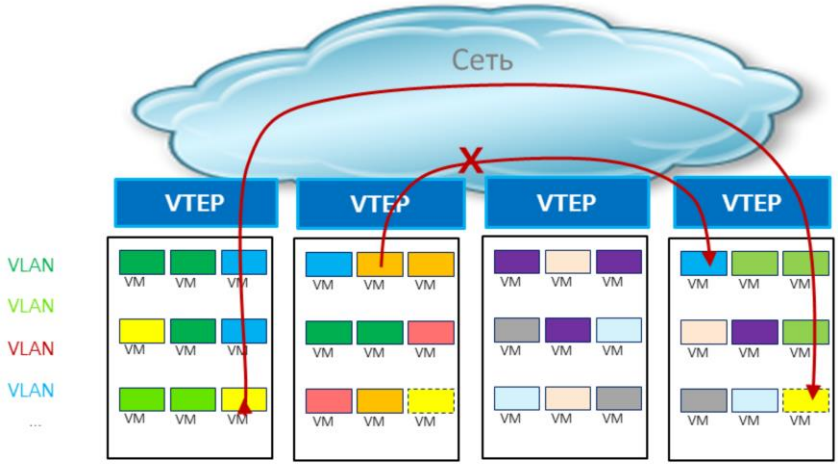


Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

VXLAN — идентификатор VNI

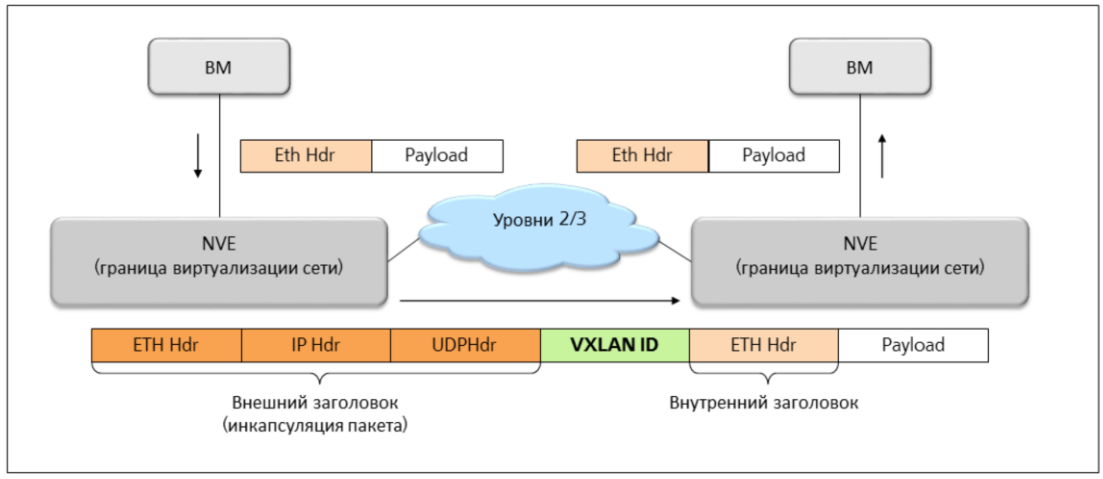
- VNI (24 бита) идентифицирует виртуальную сеть. Поле VNI поддерживает до 16 миллионов сетевых сегментов.



Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

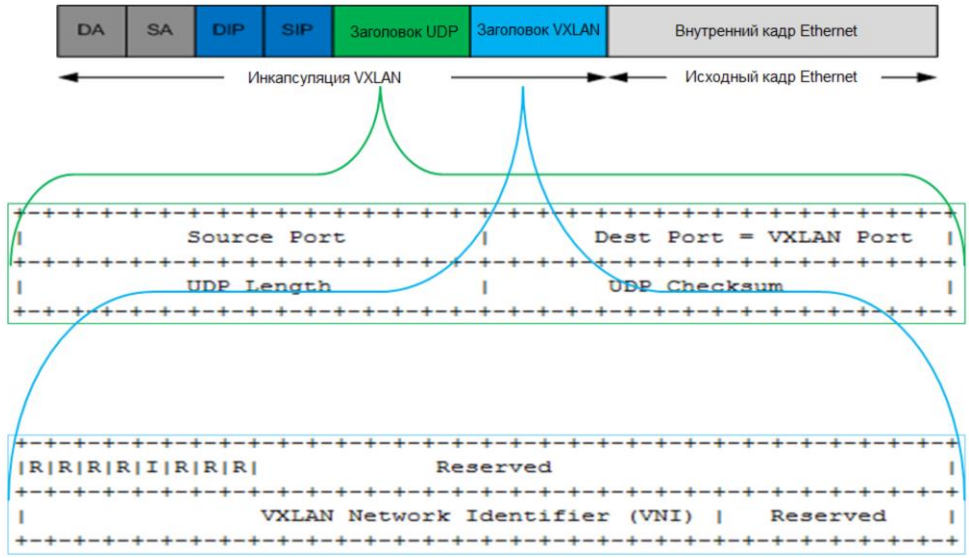
Формат пакета VXLAN (1)



Процес инкапсуляции пакета VXLAN

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

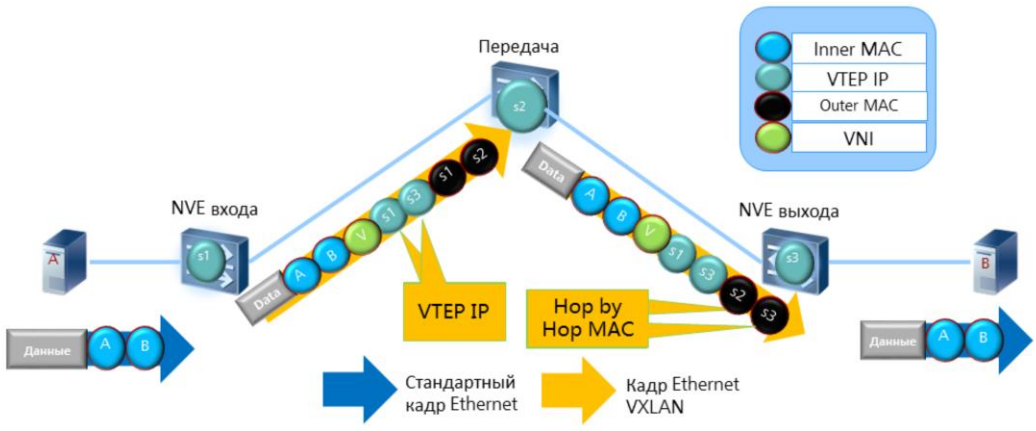
Формат пакета VXLAN (2)



Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

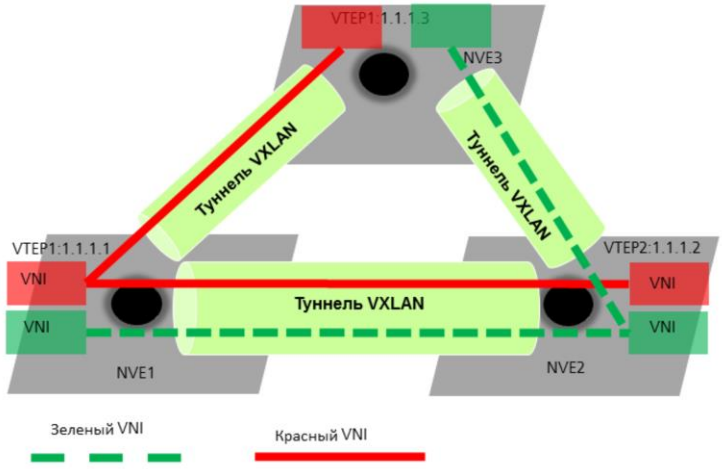
Инкапсуляция пересылаемых данных VXLAN



Пакеты сети 2 уровня могут поступать от исходного хоста на хост назначения через IP-сеть. Сеть VXLAN функционирует как мост для хостов.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Связь между туннелями и VNI

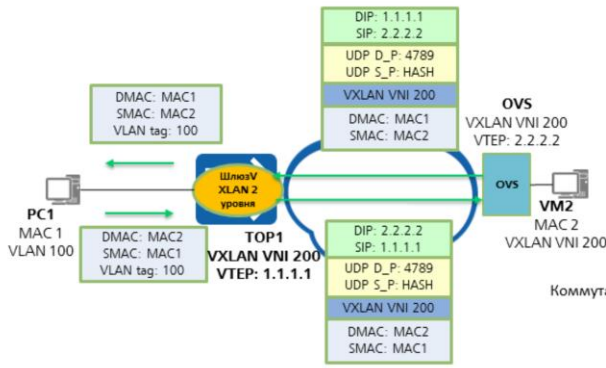


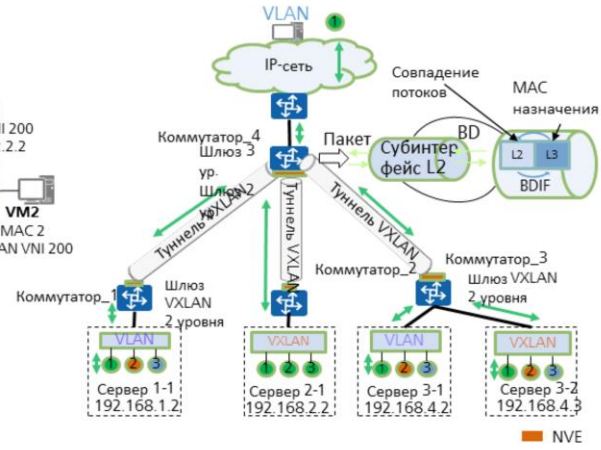
VNI

- VNI идентифицирует домен уровня 2 в сети VXLAN.
- Два VTEP определяют туннель VXLAN, который совместно используется всеми VNI между двумя NVE.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Шлюзы VXLAN





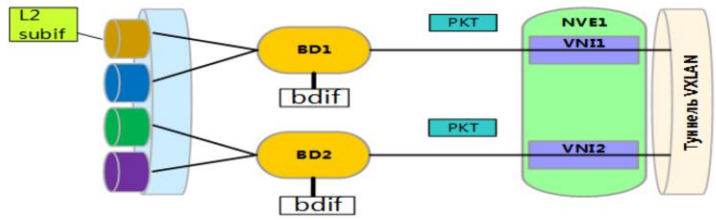
- **Шлюз VXLAN 2 уровня** обеспечивает арендаторам доступ к сети VXLAN для осуществления обмена трафиком внутри VXLAN.
- **Шлюз VXLAN 3 уровня** реализует прямой обмен трафиком между различными сетями VXLAN или между сетями VXLAN и прочими сетями.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Модель доступа к сервисам VXLAN (1)

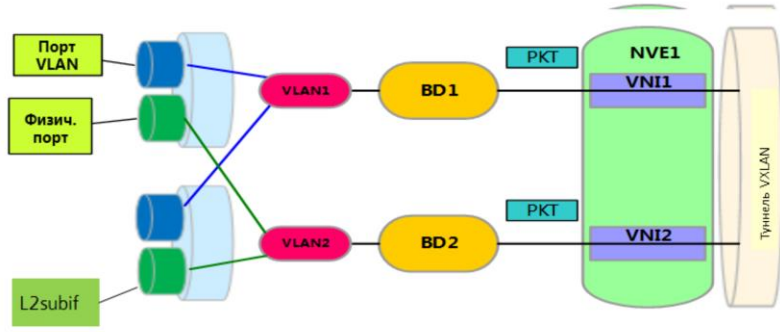
- Шлюз VXLAN использует виртуальное Ethernet-соединение (EVC) для услуг. EVC включает в себя мостовой домен (BD), VNI, NVE, субинтерфейс 2 уровня (subif L2) и туннель VXLAN.
  - Субинтерфейс 2 уровня (L2 subif) используется для доступа пользователя. Доступ на субинтерфейсе 2 уровня можно настроить с помощью одного тега VLAN или без тега.
  - Мостовой домен (BD) идентифицирует широковещательный домен 2 уровня и отображает VNI 1:1. Все широковещательные домены поддерживаются на основе мостовых доменов, таких как обучение MAC-адресам, поиск в таблице 2 уровня и репликация широковещательной рассылки.
  - NVE используется для управления локальным адресом VTEP, туннелем VXLAN и списком репликации на входе.
  - Туннель VXLAN используется для пересылки пакетов VXLAN и определяется по локальному адресу VTEP и удаленному адресу VTEP.
  - BDIF – это интерфейс маршрутизации 3 уровня мостового домена, который используется для передачи трафика 2 уровня в домен 3 уровня для пересылки на основе маршрутов.



Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

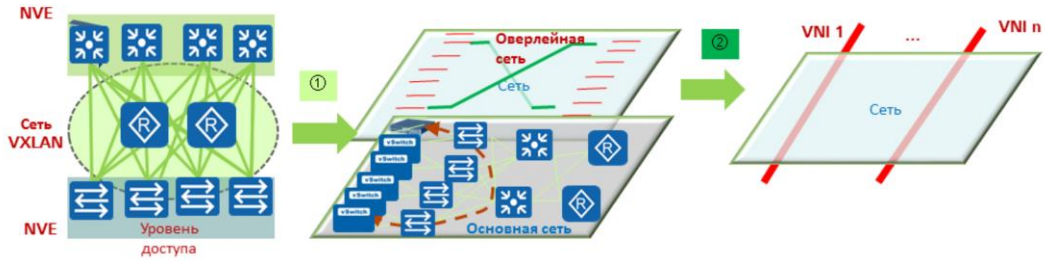
Модель доступа к сервисам VXLAN (2)

- Модель доступа к глобальной VLAN в основном используется для сервиса L2VPN. В этом сценарии сеть VLAN привязана к BD для связи традиционного порта и интерфейса VLAN к сети VXLAN. Субинтерфейс 2 уровня должен быть связан с BD.



Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Логика VXLAN



Упрощенное описание VXLAN: двойная виртуализация

1. Первая виртуализация: туннель соединяет пограничные устройства для прозрачной передачи пакетов 2 уровня. Сеть можно представить как сверхбольшой коммутатор локальной сети с большим количеством интерфейсов.
2. Вторая виртуализация: для виртуализации сверхбольшого коммутатора в несколько широковещательных доменов уровня 2, похожих на VLAN, используются идентификаторы VNI. VNI – это то же самое, что и VLAN ID. Поле VNI в заголовке VXLAN расширяет количество подсетей с 4 тысяч до 16 миллионов.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Преимущества VXLAN



Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

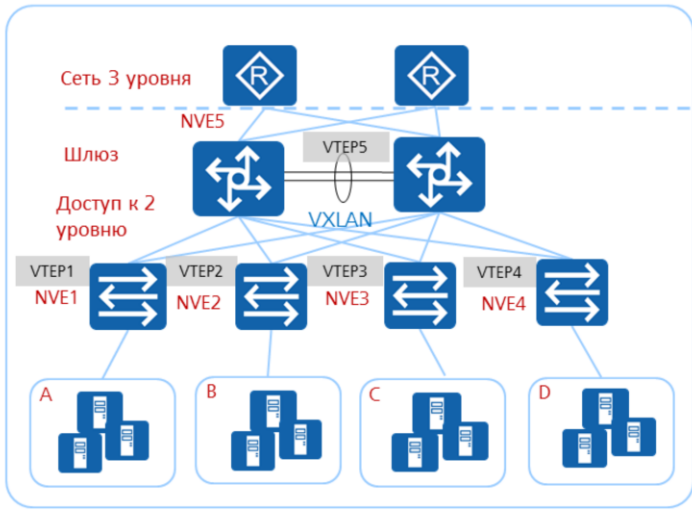
HUAWEI

Содержание

1. Обзор SDN
2. Проблемы перехода к облачным сервисам для традиционных сетей ЦОД
3. Основные понятия VXLAN
4. **Процесс передачи пакетов VXLAN**
5. Понятия и сценарии применения VXLAN в облачных ЦОД

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Процесс передачи пакетов VXLAN внутри подсети



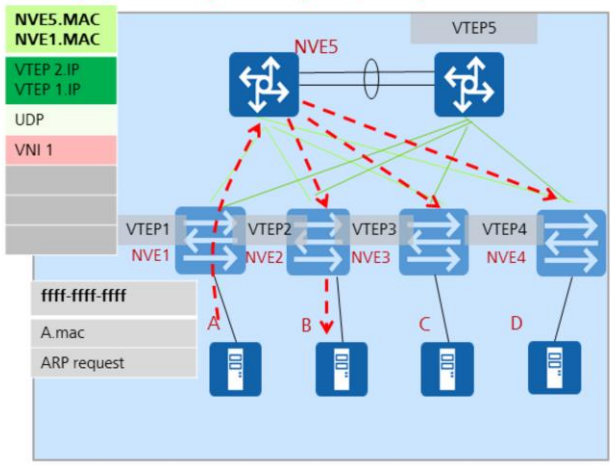
Процесс

- Хост A отправляет сообщение ARP Request на хост B.
- Хост B возвращает ответное сообщение ARP Reply на хост A.
- Хост A отправляет пакет данных в формате одноадресной передачи на хост B.
- Примечание. Хосты A, B, C и D принадлежат VNI 1. Подавление широковещательной передачи ARP отключено.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Поиск записей в таблице MAC-адресов для передачи данных на уровне 2 внутри одного сегмента сети (1)

Хост A отправляет сообщение ARP Request (в формате широковещания) хосту B.

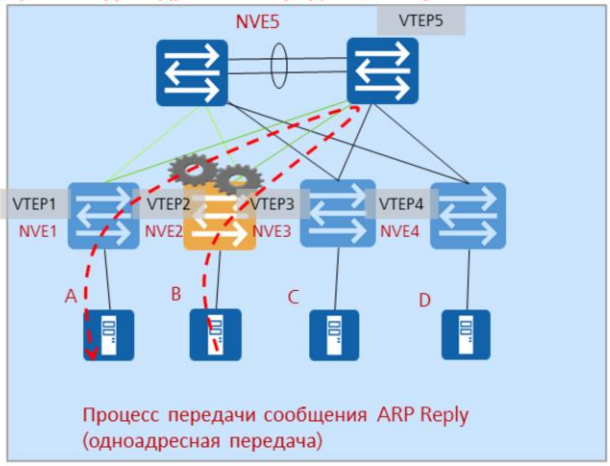


1. Когда устройство NVE1 обнаружит, что принятое сообщение ARP Request является широковещательным пакетом, оно передаст этот пакет в VNI 1 и инкапсулирует его в пакет VXLAN.
2. Промежуточные узлы прозрачно передают инкапсулированный пакет VXLAN.
3. После того, как NVE 2, 3, 4 и 5 получат пакет, они декапсулируют пакет и узнают MAC-адрес хоста A.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Поиск записей в таблице MAC-адресов для передачи данных на уровне 2 внутри одного сегмента сети (2)

Хост B возвращает ответное сообщение ARP Reply (в формате одноадресной передачи) хосту A.



Процесс передачи сообщения ARP Reply (одноадресная передача)

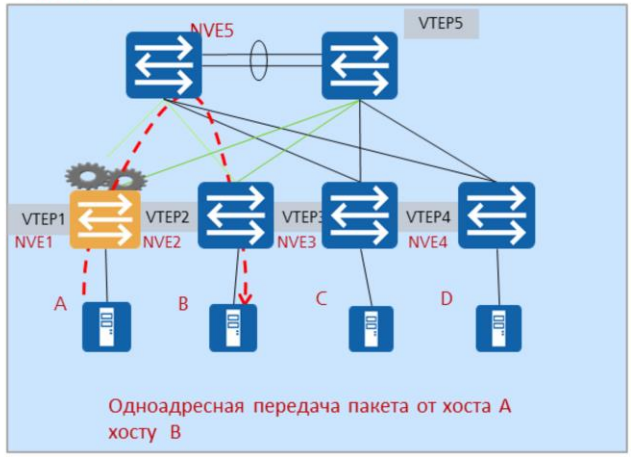
1. Устройство NVE2 ищет запись MAC-адреса хоста A и обнаруживает, что исходящий интерфейс – это туннельный интерфейс NVE2-NVE1. NVE2 затем инкапсулирует пакет в пакет VXLAN и отправляет его на уровне 3.
2. Промежуточные узлы прозрачно передают инкапсулированный пакет VXLAN.
3. После того, как NVE1 получает пакет, он декапсулирует и передает его локально. NVE1 узнает MAC-адрес хоста B.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Поиск записей в таблице MAC-адресов для передачи данных на уровне 2 внутри одного сегмента сети (3)

Одноадресная передача пакета данных от хоста A хосту B

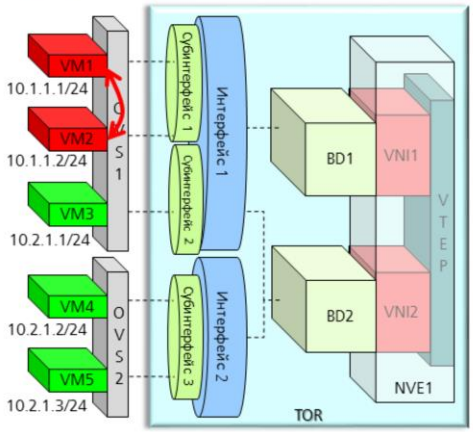


1. Устройства NVE1 и NVE2 распознали MAC-адреса хостов A и B.
   Когда они выполняют поиск записей в своих таблицах MAC-адресов, они находят совпадающие записи и передают пакет в порядке, аналогичном порядку передачи пакетов VLAN.
2. Единственное отличие состоит в том, что внешний уровень пакета данных инкапсулирован с заголовком VXLAN.
   Основная сеть по-прежнему передает пакеты на основе IP-маршрутов.

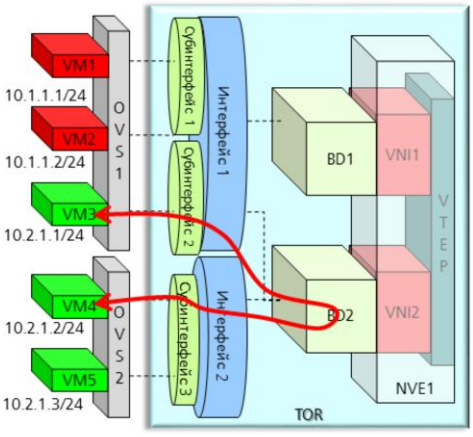
Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Модель передачи данных VXLAN: взаимный доступ между виртуальными машинами в одном сегменте сети (1)



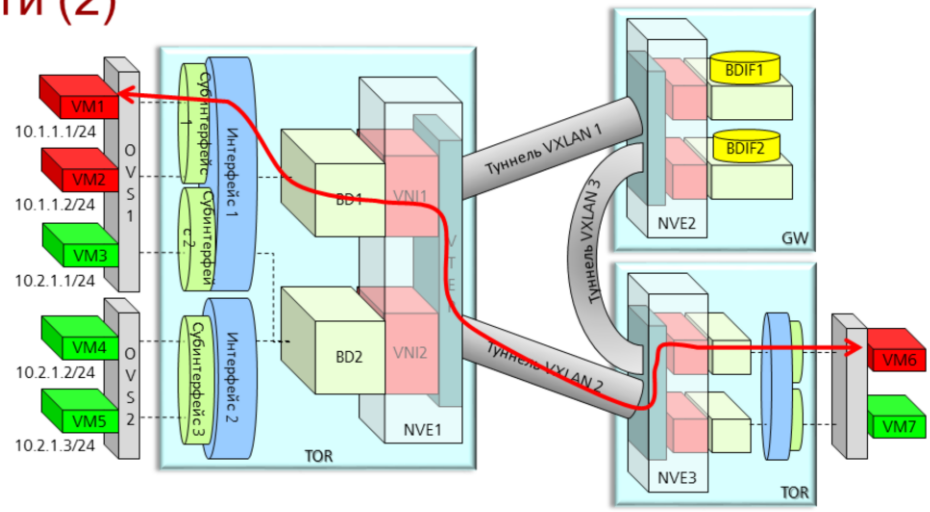
Сценарий 1: Обе виртуальные машины, расположенные на одном и том же коммутаторе vSwitch, подключены к одному и тому же TOR



Сценарий 2: Обе виртуальные машины, расположенные на разных коммутаторах vSwitch, подключены к одному и тому же TOR

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

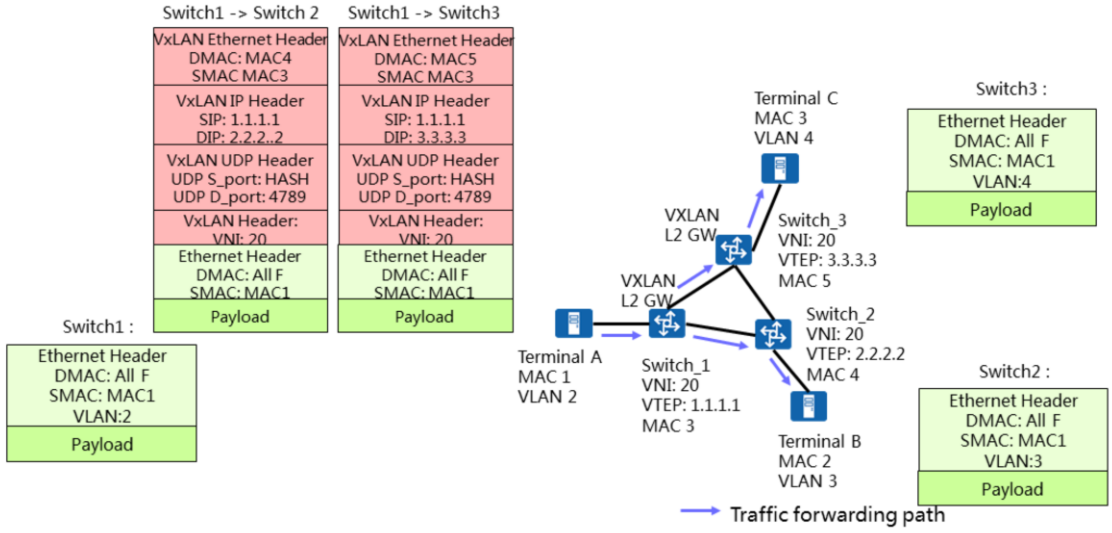
Модель передачи данных VXLAN: взаимный доступ между виртуальными машинами в одном сегменте сети (2)



Сценарий 3: Виртуальные машины, расположенные на разных коммутаторах vSwitch, подключены к разным TOR

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

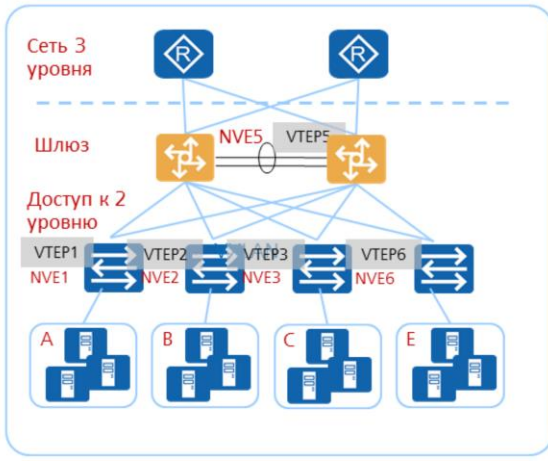
Процесс передачи пакетов BUM в сети VXLAN



Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Процесс передачи пакетов VXLAN между подсетями



Процесс

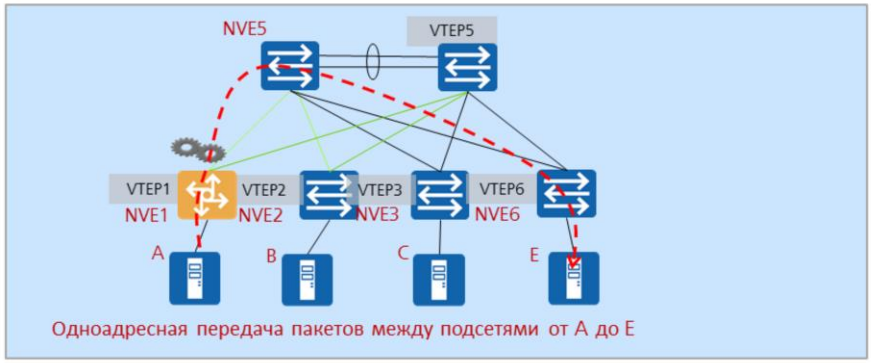
- Хост A отправляет пакет хосту E в формате одноадресной передачи.

Примечание: NVE5 функционирует как шлюз уровня 3. Хост A принадлежит VNI 1, а хост E принадлежит VNI 2. В этом примере предполагается, что хосты и шлюзы распознали MAC-адреса всех узлов посредством широковещательной передачи ARP.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Хост A отправляет пакет хосту E в формате одноадресной передачи.
- Примечание: NVE5 функционирует как шлюз уровня 3. Хост A принадлежит VNI 1, а хост E принадлежит VNI 2. В этом примере предполагается, что хосты и шлюзы распознали MAC-адреса всех узлов посредством широковещательной передачи ARP.

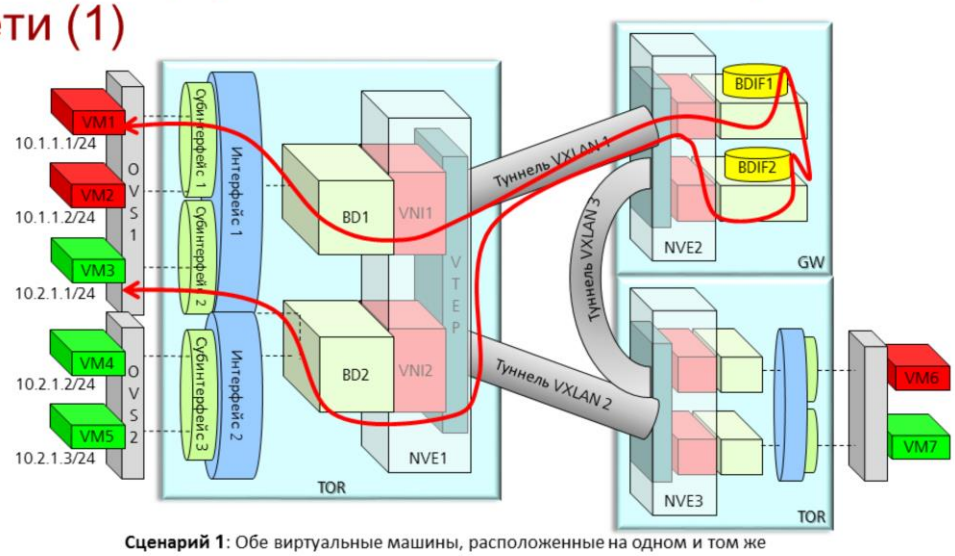
Одноадресная передача пакетов от A к E



1. Когда устройство NVE1 находит запись MAC-адреса своего шлюза, оно инкапсулирует пакет в пакет VXLAN с VNI 1 и отправляет пакет на шлюз.
2. После получения пакета шлюз декапсулирует пакет, ищет требуемый маршрут на основе внутреннего заголовка IP, заменяет внутренний заголовок Ethernet, инкапсулирует пакет в пакет VXLAN с VNI 2 и, наконец, отправляет пакет по туннелю VXLAN в NVE6.
3. После получения NVE6 декапсулирует пакет и отправляет внутренний пакет на MAC-адрес назначения.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

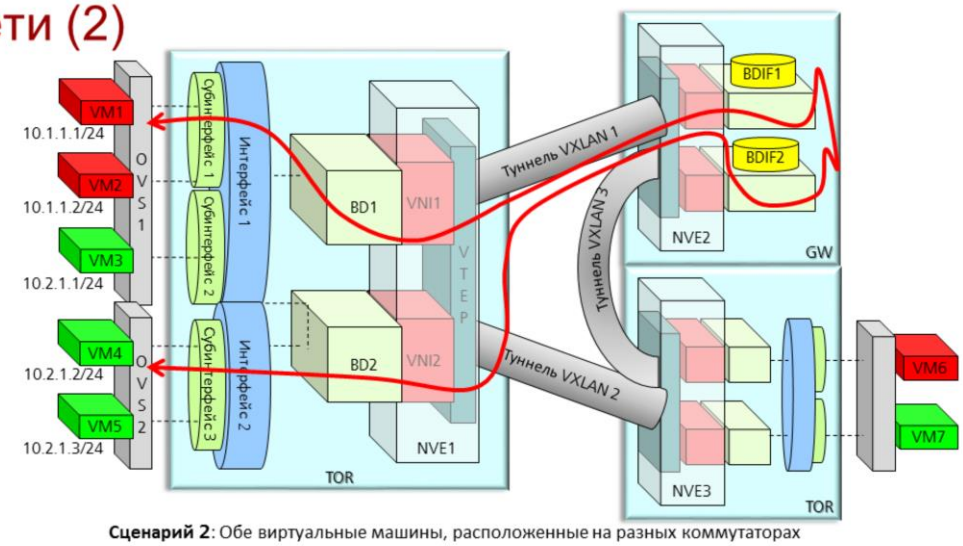
Модель передачи данных VXLAN: взаимный доступ между виртуальными машинами в разных сегментах сети (1)



Сценарий 1: Обе виртуальные машины, расположенные на одном и том же коммутаторе vSwitch, подключены к одному и тому же TOR

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

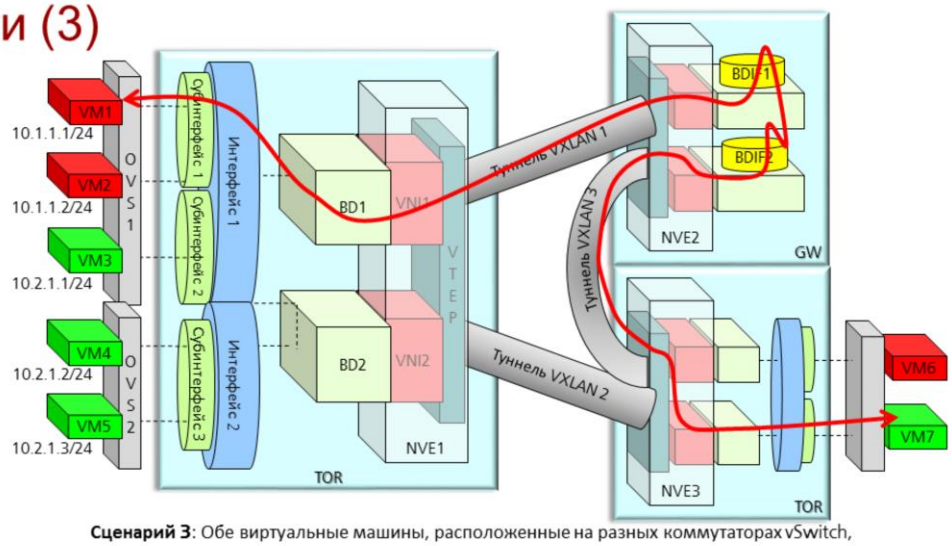
Модель передачи данных VXLAN: взаимный доступ между виртуальными машинами в разных сегментах сети (2)



Сценарий 2: Обе виртуальные машины, расположенные на разных коммутаторах vSwitch, подключены к одному и тому же TOR

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Модель передачи данных VXLAN: взаимный доступ между виртуальными машинами в разных сегментах сети (3)



Сценарий 3: Обе виртуальные машины, расположенные на разных коммутаторах vSwitch, подключены к разным TOR

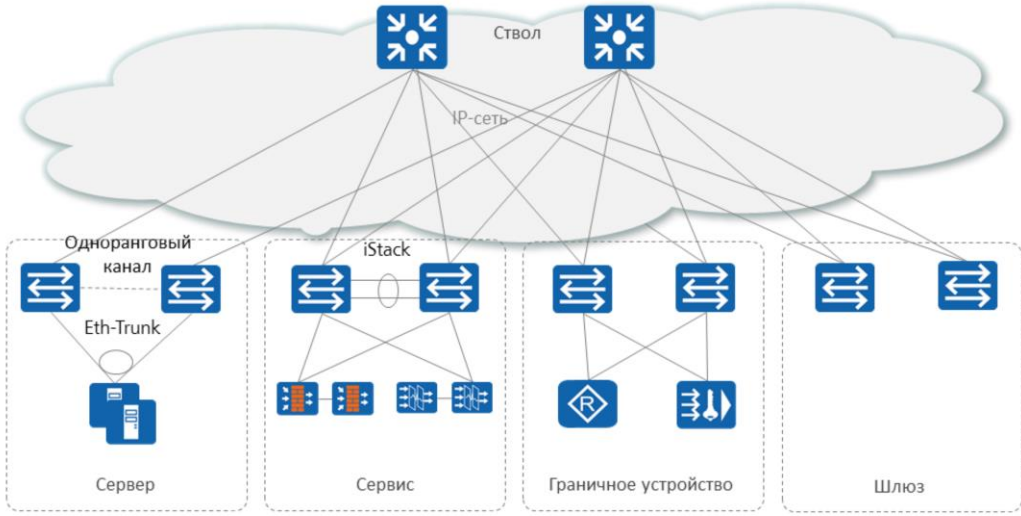
Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Содержание

1. Обзор SDN
2. Проблемы перехода к облачным сервисам для традиционных сетей ЦОД
3. Основные понятия VXLAN
4. Процесс передачи пакетов VXLAN
5. **Понятия и сценарии применения VXLAN в облачных ЦОД**

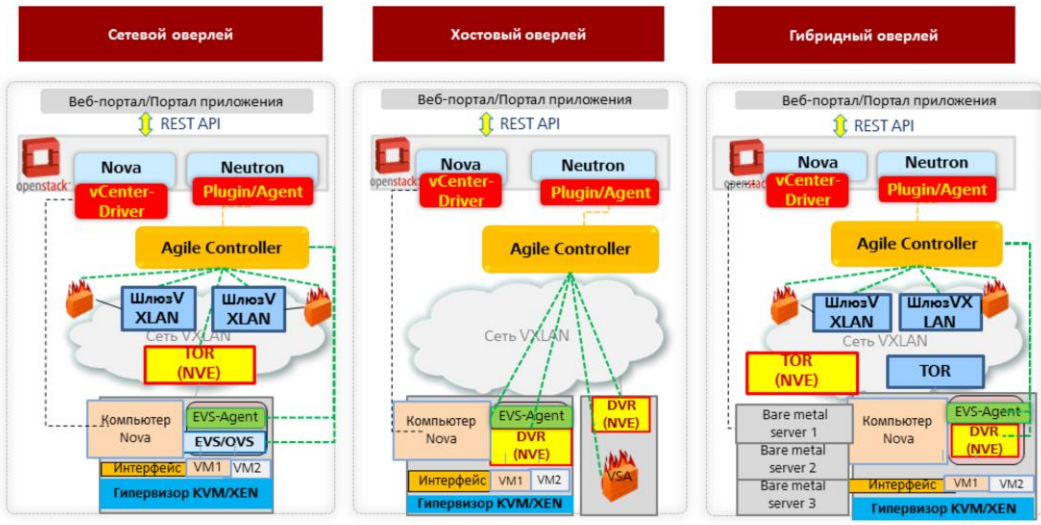
Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Сетевая архитектура «ствол и листья» (Spine-Leaf) для VXLAN



Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

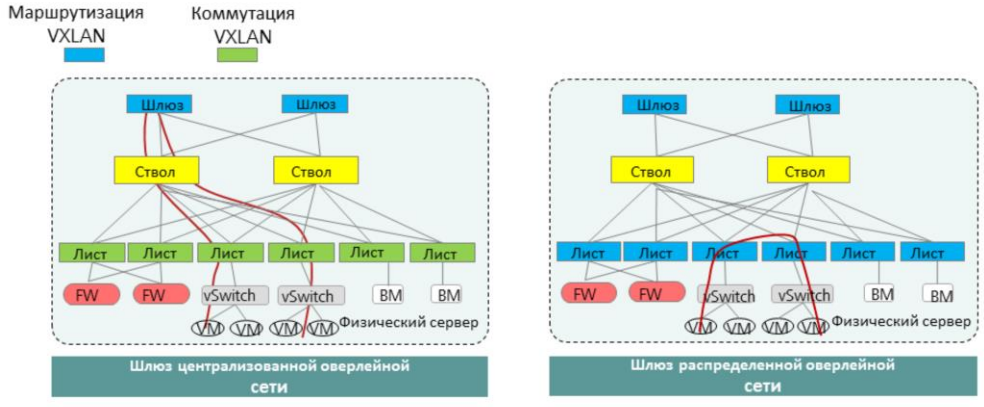
Три типа оверлейных сетей VXLAN



Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Хостовый оверлей
  - Логические сети 2-го уровня могут создаваться автоматически без необходимости перестроение и настройки физической сети. Это решение не зависит от аппаратных устройств.
- Сетевой оверлей
  - Для автоматического предоставления услуг через оверлейную сеть VXLAN требуется построить новую физическую сеть.
- Гибридный оверлей
  - SDN используется для настройки и управления виртуальными и физическими сетями, состоящими из коммутаторов, межсетевых экранов и балансировщиков нагрузки F5, а также для автоматизации предоставления услуг.

Распределенная и централизованная оверлейная сеть VXLAN



Шлюз централизованной оверлейной сети

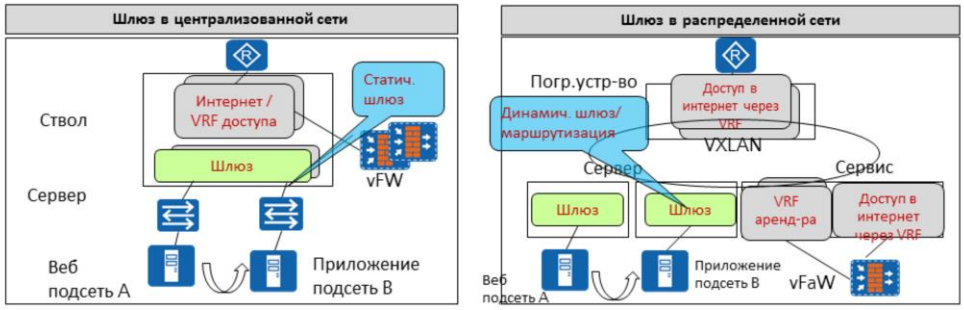
- Точки VTEP сети VXLAN 2 уровня находятся на конечных узлах (листьях)
- Шлюзы сети VXLAN 3 уровня находятся на основном уровне
- Ствол: общий маршрут

Шлюз распределенной оверлейной сети

- Конечные узлы (листья) выступают в качестве шлюзов сети VXLAN 3 уровня для горизонтального трафика и шлюзов VTEP сети VXLAN 2 уровня.
- Шлюз для горизонтального трафика находится на основном уровне.
- Ствол: общий маршрут

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

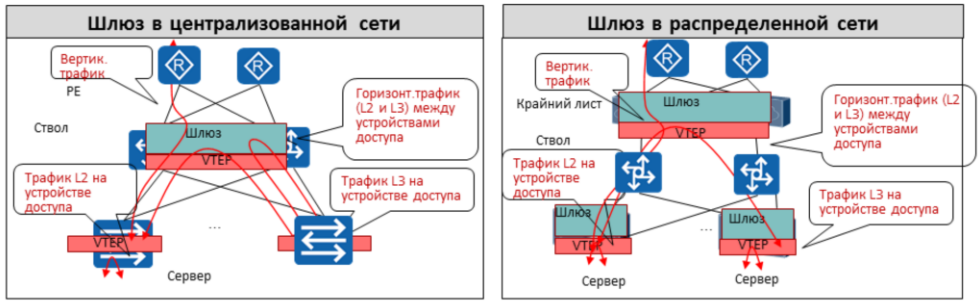
Сравнение вариантов размещения шлюзов



Пункт	Централизованная сеть	Распределенная сеть
Изменение местоположения шлюза при миграции виртуальной машины	Шлюз остается неизменным при миграции виртуальных машин.	Шлюз меняется при миграции виртуальных машин. В частности, удаляется шлюз для устройства доступа источника и создается новый шлюз для устройства доступа назначения.
Записи, затронутые при миграции виртуальных машин	Шлюз обновляет записи ARP. Устройства доступа обновляют записи MAC-адресов.	Все устройства обновляют маршруты хостов. Устройства доступа обновляют записи MAC-адресов.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

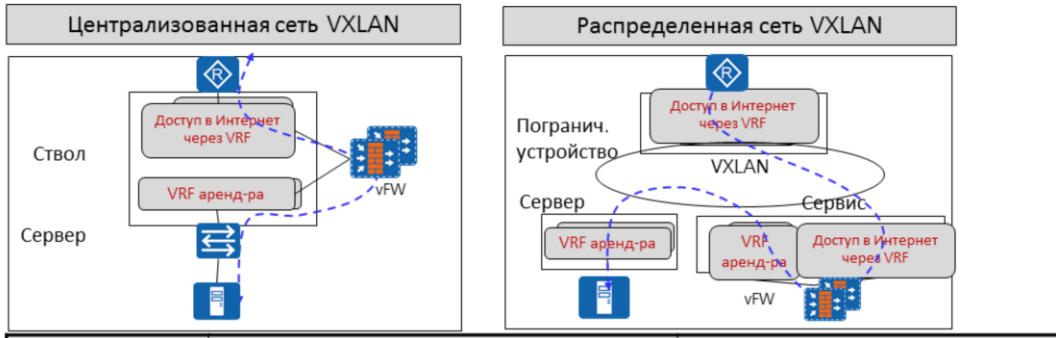
Сравнение путей передачи данных до и после оптимизации



Пункт	Централизованная сеть	Распределенная сеть
Вертикальный трафик (клиент-сервер)	Передача через основной уровень	Передача через основной уровень
Горизонтальный трафик (L2 и L3) между разными устройствами доступа	Передача через основной уровень	Передача через основной уровень
Горизонтальный трафик (L2) между хостами, подключенными к одному устройству доступа	Локальная передача	Локальная передача
Горизонтальный трафик (L3) между хостами, подключенными к одному устройству доступа	Передача через основной уровень	Локальная передача

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

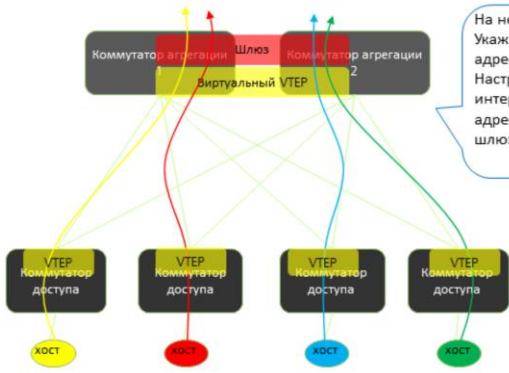
Сравнение процессов фильтрации трафика межсетевыми экранами



Пункт	Централизованная сеть	Распределенная сеть
Передача трафика на межсетевые экраны	Межсетевые экраны подключаются к шлюзу централизованной сети в режиме обхода. Политики развертываются на централизованном шлюзе для перенаправления трафика на межсетевые экраны.	Межсетевые экраны не связаны напрямую со шлюзами. Несколько шлюзов подключены к межсетевым экранам через туннели VXLAN. Политики развернуты на нескольких распределенных шлюзах.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Высоконадежный централизованный шлюз



На нескольких шлюзах:
Укажите в качестве loopback-адреса IP-адрес точки VTEP.
Настройте на одинаковых интерфейсах одинаковые IP-адреса и MAC-адреса на шлюзах.

1. Когда шлюз восстанавливается после сбоя, он объявляет маршруты с низким приоритетом (настроенные на контроллере), чтобы гарантировать передачу восходящего и нисходящего трафика на другие шлюзы. Когда записи ARP на шлюзе восстанавливаются, приоритеты маршрутов восстанавливаются, и шлюз снова участвует в балансировке нагрузки.
2. При сбое интерфейсов шлюза нисходящей связи схождение маршрутов выполняется в сети нижнего уровня.
3. Если все интерфейсы восходящей связи шлюза выходят из строя, OPS понижает приоритет адреса VTEP шлюза, так что восходящий трафик не будет отправляться на неисправный шлюз.

Таблица MAC-адресов и таблица IP-маршрутизации на устройстве доступа

MAC-адрес назначения	Удаленный VTEP
Виртуальный MAC шлюза	vVTEP

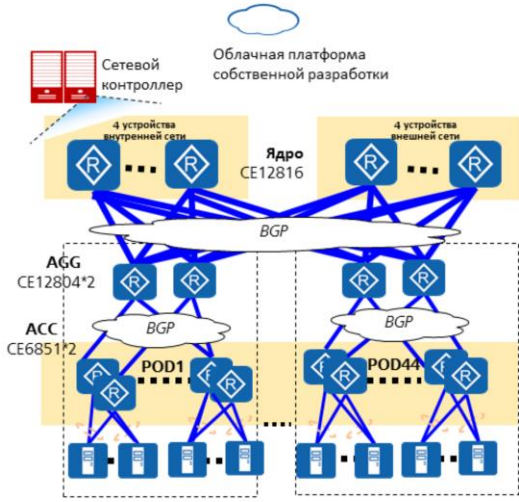
Маршрут назначения VTEP	Следующий узел
IP vVTEP	AGG1&AGG2

По сравнению с традиционными стековыми шлюзами или шлюзами, настроенными с VRRP, централизованный шлюз имеет следующие преимущества:
Шлюзам не нужно запускать какие-либо протоколы heartbeat на основе подсети, такие как VRRP и GLBP, в результате чего нагрузка на обработку пакетов сигнализации значительно снижается.
По сравнению со шлюзами VRRP уровня 3 балансировка нагрузки на основе потоков может быть реализована между физическими шлюзами, и число этих физических шлюзов может быть увеличено.
Объявление маршрутов можно контролировать на контроллере протокола маршрутизации vVTEP для расширения или улучшения пропускной способности шлюза без потерь.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Крупномасштабное общедоступное облако для интернет-компании A в Китае



Требования клиентов

- Большой масштаб, высокая производительность и низкий коэффициент превышения лимита
- Миграция по ЦОД
- Автоматические и усовершенствованные процедуры эксплуатации и техобслуживания на основе контроллера SDN

Решение

- Андерлейная сеть использует архитектуру spine-leaf, а оверлейная сеть использует VXLAN для крупномасштабного соединения уровня 2. VTEP развернуты на конечных коммутаторах.
- Шлюзы VXLAN уровня 3 в режиме «активный-активный» развернуты централизованно для балансировки нагрузки с целью повышения пропускной способности.
- Сетевой контроллер предоставляет настроенные северные API для подключения к частной облачной платформе с целью автоматического предоставления сетевых услуг.
- Сетевой контроллер используется для обеспечения визуализации пути и трафика для упрощения эксплуатации и обслуживания.

Преимущества для клиентов

- Мультиактивный централизованный аппаратный шлюз обеспечивает масштабирование и производительность сети, а также удовлетворяет требованиям к управлению и эксплуатации в традиционных ЦОД.

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Тест

1. Какие из следующих утверждений о VXLAN неверны?
   A. VXLAN использует режим инкапсуляции MAC-in-MAC.
   B. Аналогично передаче данных на основе меток MPLS, пакеты VXLAN передаются на основе VNI.
   C. VXLAN – это технология NVO3.
   D. В пакетах VXLAN номер исходного порта во внешнем заголовке UDP обычно рассчитывается с использованием алгоритма хеширования на основе внутреннего заголовка кадра Ethernet.
2. Какие из следующих решений являются решениями VXLAN?
   A. Сетевой оверлей
   B. Хостовый оверлей
   C. Гибридный оверлей

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Ответы
  - AB
  - ABC

Краткое содержание

- Требования и проблемы облачных ЦОД
- Основы VXLAN
- Процесс передачи пакетов VXLAN
- Общая организация сети VXLAN
- Сценарии применения

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Дополнительная информация

- Официальные веб-сайты Huawei:
  - Корпоративная платформа: http://enterprise.huawei.com/en/
  - Техническая поддержка: https://support.huawei.com/enterprise/en
  - Справочные материалы: http://learning.huawei.com/en/
- Инструмент документации:
  - HedEx Lite
- Симулятор:
  - eNSP

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Рекомендации

- Веб-сайт Huawei E-Learning:
  - http://support.huawei.com/learning/en/newindex.html
- Библиотека примеров службы поддержки Huawei:
  - http://support.huawei.com/enterprise/servicecenter?lang=en

Авторские права © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Спасибо за внимание!

www.huawei.com

HCIE-R&S

— BGP EVPN

www.huawei.com

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Введение

- В данной главе описывается технология Ethernet VPN (EVPN), которая используется для виртуализации сети (NVO). EVPN может использоваться совместно с технологией VXLAN для инкапсуляции туннеля через IP-уровень и управления маршрутами.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Цели

- После прохождения этого курса вы будете знать:
  - Происхождение и развитие технологии EVPN.
  - Принципы работы EVPN.
  - Совместное использование EVPN и VXLAN в Huawei.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Содержание

1. **Обзор EVPN**
2. Принципы работы EVPN
3. Применение EVPN в NVO

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

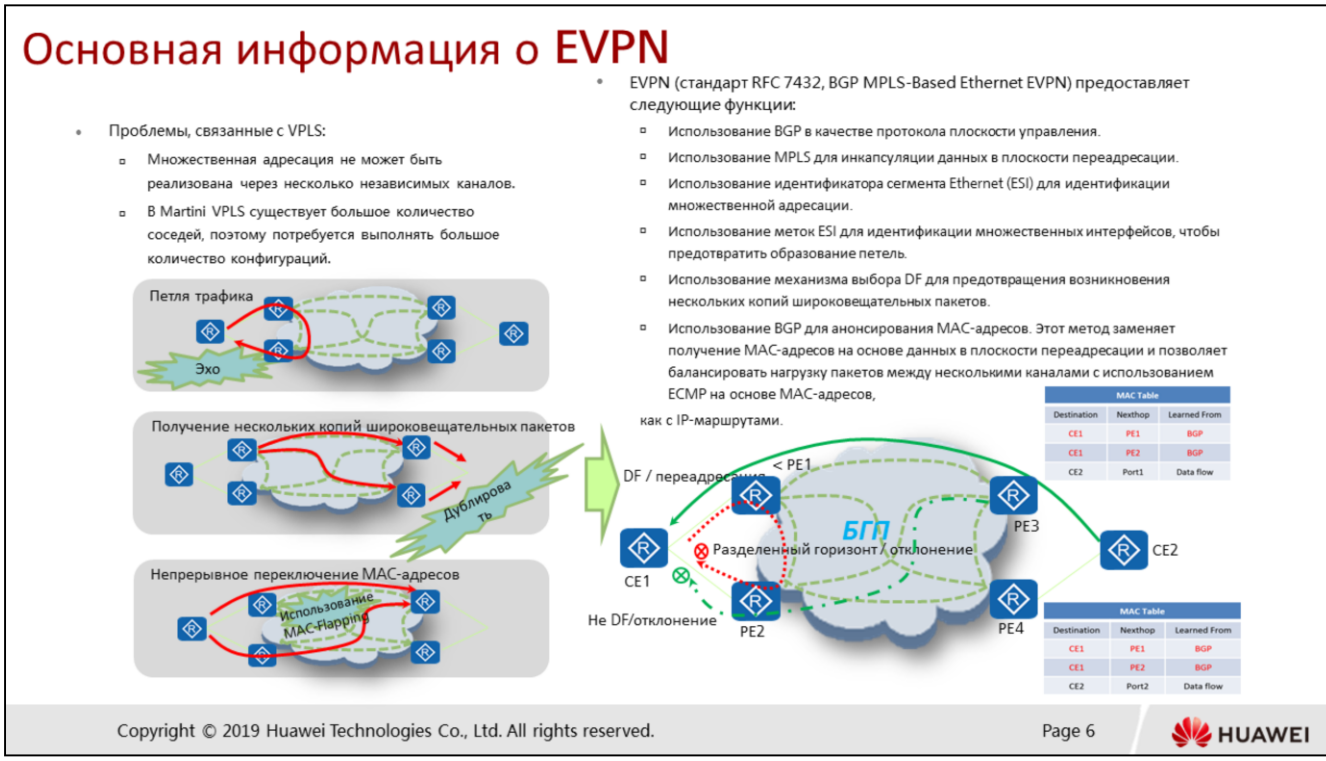
Ethernet L2VPN

- Сервисы Ethernet L2VPN широко применяются в сети. Например, шлюзы таких сервисов, как VoIP, высокоскоростной Интернет и телевещание, располагаются на маршрутизаторах широкополосного удалённого доступа (BRAS). Сети 2 уровня строятся поверх metro-сети между компаниями для создания связи между центрами обработки данных (ЦОД).
- VPLS широко используется в сетях для прозрачной передачи пакетов 2 уровня. Однако при применении VPLS возникают следующие ограничения и проблемы:
  - Множественная адресация
  - Оптимизация многоадресной рассылки
  - Сложная конфигурация
  - Решение Multi-tenant DCI
  - Быстрая сходимость
  - Подавление широковещания
- EVPN используется для решения этих проблем.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- HSI: высокоскоростной Интернет
- BTV: телевещание
- Множественная адресация: в настоящее время VPLS поддерживает множественную адресацию только в режиме резервирования single-active, вместо переадресации multi-path all-active.
- Оптимизация многоадресной рассылки: многоадресные LSP можно использовать совместно с VPLS, но только для LSP P2MP. VPLS не поддерживает MP2MP LSP.
- Сложная конфигурация: на данный момент VPLS обеспечивает односторонний доступ на основе BGP для автоматического обнаружения. В результате возникает большой объем работы по конфигурации Ethernet на стороне доступа.
- Multi-tenant DCI: помимо поддержки сетей уровня 2 между ЦОД каналы DCI требуют расширения сетей 2 уровня для арендаторов.



- Мы упомянули о недостатках VXLAN для новых протоколов плоскости управления. Давайте рассмотрим протокол EVPN. Определение протокола EVPN (Ethernet VPN) приводится в стандарте RFC 7432 и используется для решения некоторых проблем VPLS. Например, VPLS не поддерживает множественную адресацию через несколько независимых каналов. В некоторых случаях можно получить множество широковещательных пакетов или произойдет MAC address flapping. В Martini VPLS существует большое количество соседей, в результате чего необходимо выполнять большой объем конфигураций.
- EVPN использует протокол BGP в качестве протокола плоскости управления и MPLS для инкапсуляции данных плоскости передачи данных, чтобы решить проблемы петель, множества широковещательных пакетов и получения MAC-адресов в сценариях VPLS.

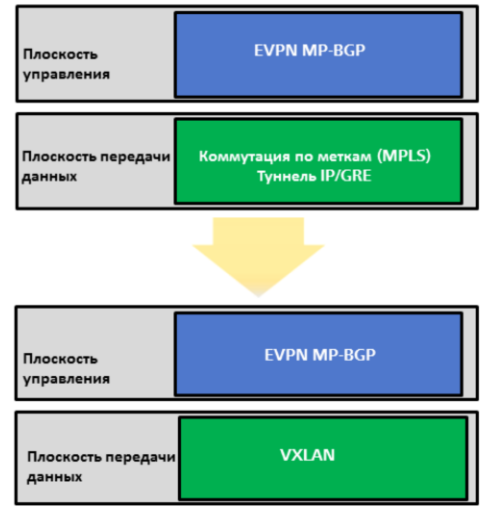
Разработка и применение протокола BGP-EVPN

Разработка EVPN

- Технология Ethernet VPN, описанная в стандарте RFC 7432, была создана для удовлетворения необходимости в высокой пропускной способности и выполнению комплексного контроля QoS в сетях VPN на базе MPLS. Протокол MP-BGP применяется в плоскости управления для внедрения концепции семейства адресов.
- Характеристики EVPN: плоскость управления и плоскость передачи данных отделяются и изолируются друг от друга. Плоскость управления MP-BGP передает маршруты MAC/IP. Существует несколько методов инкапсуляции в плоскости передачи данных.

EVPN для VXLAN

- Поскольку VXLAN не имеет плоскости управления, плоскость управления MP-BGP EVPN подходит для VXLAN.
- VXLAN расширяет действие стандарта EVPN.
- Проекты EVPN:
  - draft-ietf-bess-evpn-overlay
  - draft-ietf-bess-evpn-inter-subnet-forwarding
  - draft-ietf-bess-evpn-prefix-advertisement

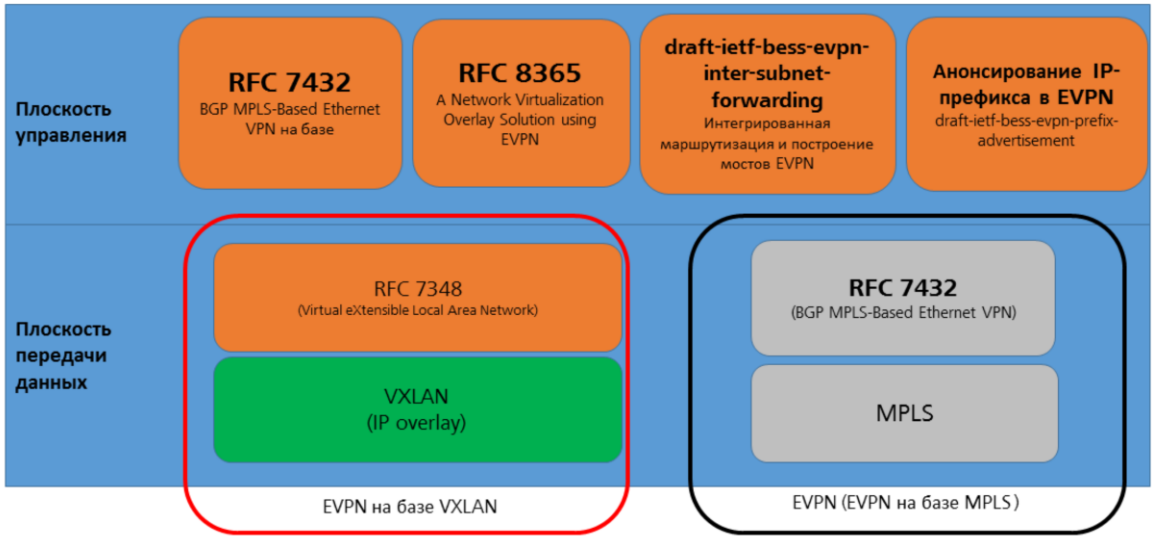


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- EVPN – это технология VPN, используемая для сетей 2 уровня. EVPN использует механизм, аналогичный механизму BGP/MPLS IP VPN. EVPN определяет новый тип информация сетевого уровня о доступности сети BGP (NLRI) под названием EVPN NLRI. EVPN NLRI определяет новые маршруты BGP EVPN для реализации определения MAC-адресов и анонсирования между точками в сети 2 уровня.
- Исходное решение по внедрению VXLAN не имело плоскости управления. Обнаружение VTEP и информация о хосте (включая IP-адрес, MAC-адрес, VNI и IP-адреса шлюзов VTEP) выполняются посредством лавинного распространения трафика в плоскости передачи данных. В результате в сети ЦОД будет много трафика. Для решения этой проблемы VXLAN использует EVPN в качестве плоскости управления. Для автоматического обнаружения VTEP и анонсирования информации хоста VTEP обмениваются маршрутами BGP EVPN обмениваются между, избегая лавинного распространения трафика .
- Помимо решения, описанного в стандарте RFC 7432, существует еще три проекта EVPN. Решение draft-ietf-bess-evpn-overlay стало стандартом RFC 8365 (NVO с использованием Ethernet VPN (EVPN)). Два других проекта станут стандартами в будущем.

Реализация EVPN



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- VXLAN используется в качестве плоскости передачи данных.

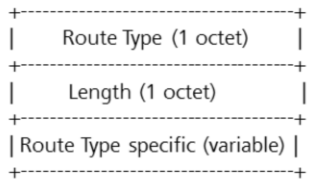
Содержание

1. Обзор EVPN
2. **Принципы работы EVPN**
3. Применение EVPN в NVO

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

EVPN NLRI

- В RFC 7432 протокол EVPN определяет новую информацию NLRI, которая называется EVPN NLRI. Формат EVPN NLRI выглядит следующим образом:

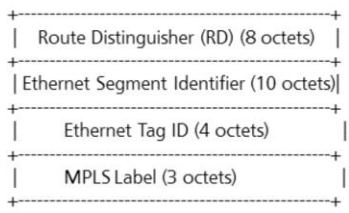


- RFC 7432 определяет четыре типа маршрутов:
  - 1 - Ethernet Auto-Discovery (A-D)
  - 2 - MAC/IP Advertisement
  - 3 - Inclusive Multicast Ethernet Tag
  - 4 - Ethernet Segment

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Тип 1: маршрут Ethernet Auto-Discovery

- Формат EVPN NLRI:



- Индексы префиксов:
  - Ethernet Segment Identifier
  - Ethernet Tag ID

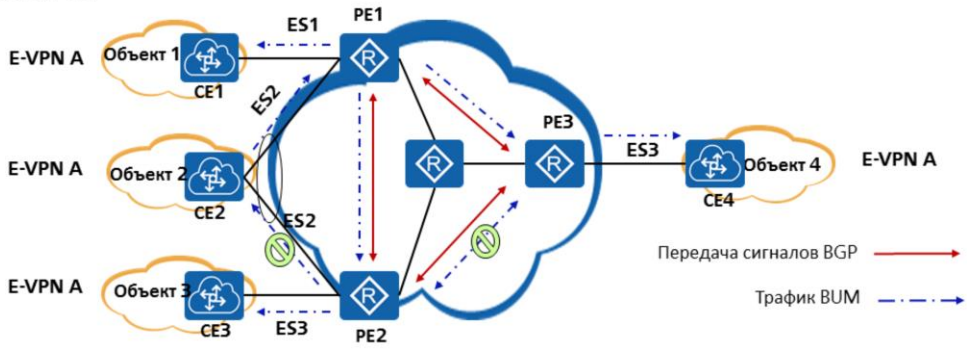
- Маршрут 1 типа также называется маршрутом Ethernet Auto-Discovery (A-D).
- Требуется только тогда, когда для реализации многоадресного доступа используется ESI.
- Функции:
  - Расщепление горизонта (Split horizon)
  - Быстрая сходимость
  - Aliasing

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Расщепление горизонта (назначение меток ESI)
- Быстрая сходимость (другие PE осуществляют быстрое пакетное переключение определенных маршрутов, например маршрутов анонсирования MAC на основании RT1-маршрутов.)
- Alias (Многоадресные PE могут анонсировать определенные маршруты, например маршруты анонсирования MAC. Другие PE могут формировать каналы ECMP ко всем PE с несколькими подключениями, основанным на маршрутах RT1)
- Для замены таких маршрутов можно использовать технологию M-LAG и технологию накопления в стеке.

Расщепление горизонта (split horizon)

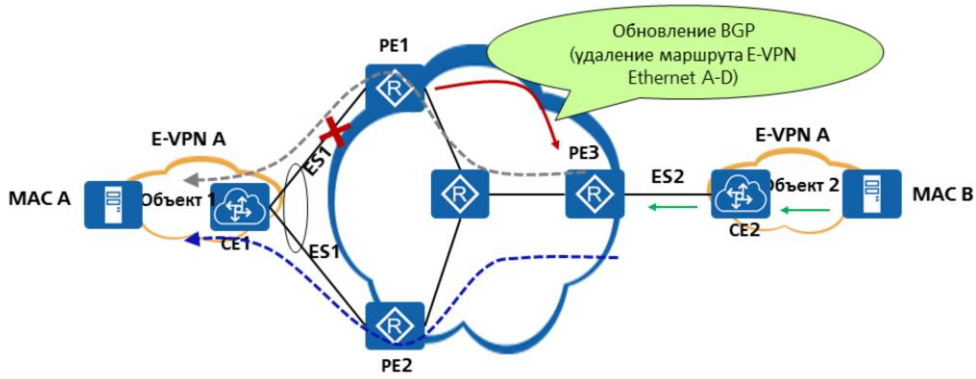
- Как показано на рисунке, CE2-маршрутизатор соединен с маршрутизаторами PE1 и PE2. После получения трафика BUM (широковещание, одноадресная и многоадресная передача) от CE2, PE1 дублирует и передает трафик PE2. PE2 не посылает полученные пакеты в CE2. Это предотвращает возникновение петлей на стороне CE. Аналогичным образом, трафик многоадресной рассылки, полученный PE2 от PE1, не передается на сторону PE, предотвращая возникновение петлей на стороне публичной сети.
- Функция расщепления горизонта осуществляется с помощью метки ESI, передаваемой в маршрутах Ethernet A-D per ES. Как показано на рисунке, PE2 назначает метку ESI для идентификации ES2 и анонсирует ее PE1 через маршруты Ethernet A-D. PE1 добавляет эту метку к трафику BUM перед его отправкой на PE2, а PE2 идентифицирует метку после получения трафика BUM. То есть, трафик BUM не переадресовывается ES2.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Быстрая сходимость

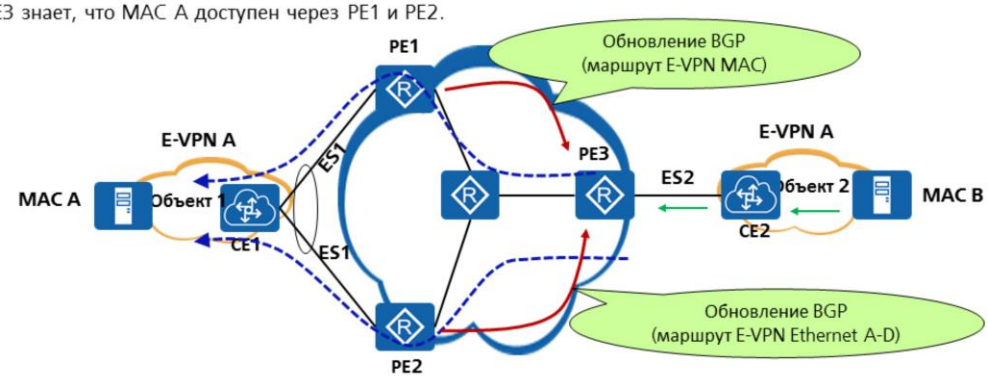
- Маршруты Ethernet A-D per ES используются для быстрого удаления MAC-маршрутов с целью обеспечения быстрой сходимости.
- Как показано на рисунке, CE1 подключен к PE1 и PE2. PE1 и PE2 узнают MAC-адрес CE1 и анонсируют MAC-маршруты к PE3. При сбое канала между CE1 и PE1, PE1 посылает PE3 сообщение об удалении маршрута Ethernet A-D per ES, чтобы PE3 мог быстро обновить MAC-маршруты ES1 и переключить трафик на PE2.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Aliasing

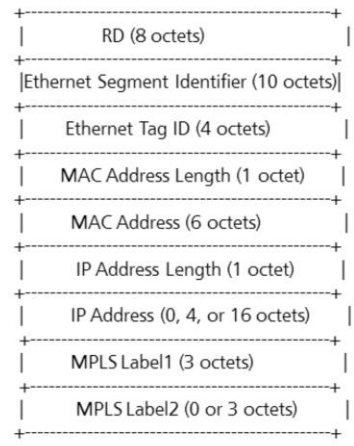
- В сценарии множественной адресации all-active CE некоторые PE могут не узнать MAC-адрес CE. Если эта проблема возникает, удаленные PE не будут участвовать в балансировке нагрузки или работать в качестве резервных устройств. Для решения этой проблемы EVPN вводит понятие aliasing через маршруты Ethernet A-D per EVI.
- Как показано на рисунке, CE1 подключен к PE1 и PE2. Предположим, что PE1 узнает MAC A и анонсирует MAC-маршруты к PE3. PE2 не узнает MAC A, но PE2 может анонсировать маршруты Ethernet A-D per EVI маршруты к PE3. PE3 знает, что MAC A доступен через PE1 и PE2.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Тип 2: маршрут MAC/IP Advertisement

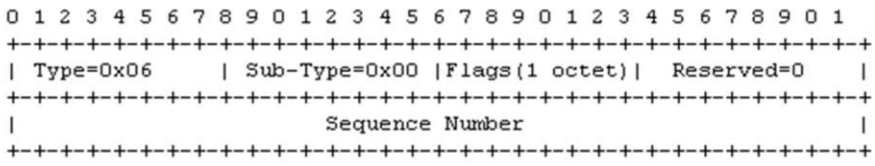
- Формат EVPN NLRI:
- Функции:
  - Управление переадресацией одноадресного трафика.
  - Переадресация MAC/IP-адресов виртуальных машин.
- Индексы префиксов:
  - Идентификатор метки Ethernet (Ethernet Tag ID), MAC-адрес и IP-адрес используются в качестве индексов префиксов. Метки ESI и MPLS используются в качестве атрибутов маршрутов.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Расширенный атрибут MAC Mobility Extended Community

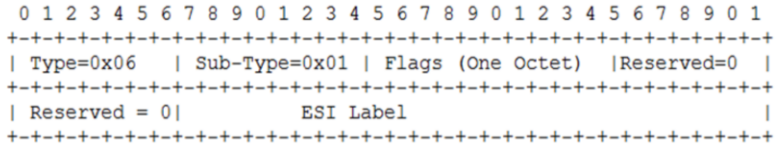
- Описание:
  - Этот расширенный атрибут является переходным атрибутом community со значением поля Type 0x06 и значением поля Sub-Type 0x00. Его можно анонсировать вместе с маршрутами MAC/IP Advertisement.
  - Флаги: младший бит. Значение 1 означает, что MAC-адрес статичен и не может перемещаться.
- Формат:



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Идентификатор ESI

- Формат:



- Описание:
  - Этот расширенный атрибут является переходным атрибутом community со значением поля Type 0x06 и значением поля Sub-Type 0x01. Его можно анонсировать вместе с маршрутами Ethernet A-D.
  - Флаги: наименьший значимый бит. Значение 0 означает режим резервирования all-active, а значение 1 означает режим резервирования single-active.
  - Метка ESI: это 3-байтовое поле метки ESI используется для разделения горизонта (split horizon). В режиме резервирования single-active значение этого поля равно 0.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

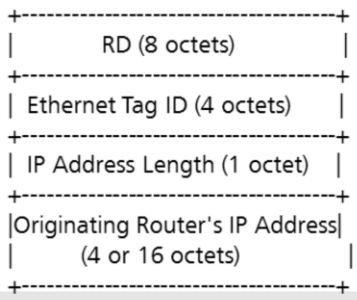
Режимы резервирования

- Режим резервирования Single-active:
  - Если поле Flags Ethernet-сегмента имеет статус Single-Active в наборе маршрутов Ethernet A-D per ES, полученных PE, PE работает в режиме резервирования Single-active. В этом случае трафик может передаваться только через основной PE.
  - Если в основном PE возникает ошибка, маршруты Ethernet A-D per ES можно удалить, а удаленный PE переключит трафик на другой PE в группе.
- Режим резервирования All-active:
  - Если поле Flags Ethernet-сегмента имеет статус All-Active в наборе маршрутов Ethernet A-D per ES, полученных PE, PE работает в режиме резервирования all-active. В этом случае трафик может передаваться через любой PE.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Тип 3: маршрут Inclusive Multicast Ethernet Tag

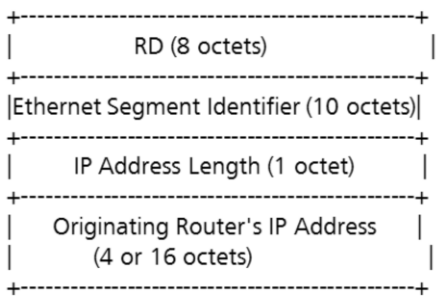
- Маршрут типа 3 также называется маршрутом Inclusive Multicast Ethernet Tag.
- Он используется для автоматического создания туннеля и автоматического присоединения широковещательных элементов VNI.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Тип 4: маршрут Ethernet Segment

- Формат NLRI:

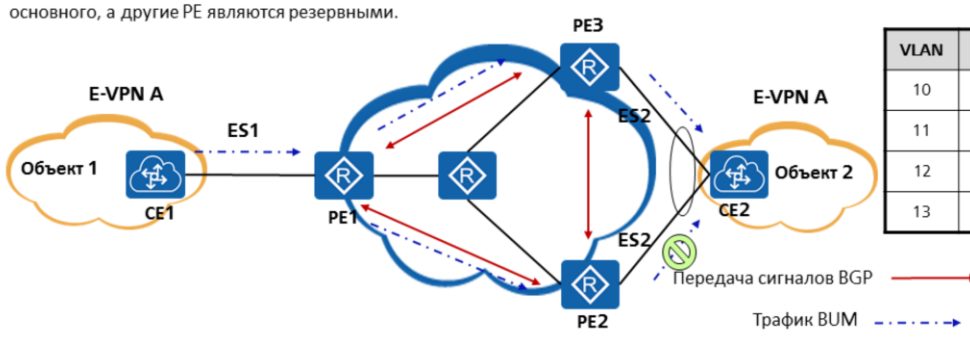


- Этот тип маршрута требуется только в сценариях многоадресного доступа и может использоваться для выбора DF между многоадресными каналами.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Выбор DF

- Когда CE многоадресно подключен к нескольким PE, только один PE должен переадресовать трафик BUM в CE. Процесс выбора PE называется выбором DF.
- Как показано на рисунке, CE2 подключен к PE2 и PE3. Пакеты BUM, исходящие из CE1, будут отправлены на PE2 и PE3. Выбор DF выполняется между PE2 и PE3. Если PE3 выбран в качестве основного PE и PE2 в качестве резервного PE, PE2 не передает трафик BUM в CE2.
- Выбор DF осуществляется через ES-маршруты. Когда истекает таймер DF (3 секунды по умолчанию), каждый PE делает выбор согласно ES-маршрутам EVI. Алгоритм выбора выглядит следующим образом: одни и те же маршруты ES сортируются в соответствии с IP-адресом отправителя в порядке возрастания. После создания списка PE выполняется операция по модулю на основе количества PE в VLAN. Если значение модуля соответствует положению PE в списке PE, то PE выбирается в качестве основного, а другие PE являются резервными.



VLAN	PE2	PE3
10	DF	
11		DF
12	DF	
13		DF

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.



Содержание

1. Обзор EVPN
2. Основы EVPN
3. **Применение EVPN в NVO**

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Общая информация о маршрутах 5 типа

- BGP EVPN определяет четыре типа маршрутов и обеспечивает гибкую плоскость управления для обеспечения взаимодействия на уровне 3 в одном сегменте сети. В некоторых случаях системы с несколькими арендаторами должны напрямую подключаться к сети без взаимодействия протоколов.
- EVPN определяет маршруты 5 типа для анонсирования маршрутов IP-префиксов.
- Маршруты IP-префиксов используются для связи между подсетями и доступа хоста к внешним сетям.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Более подробную информацию см в проекте стандарта RFC "IP Prefix Advertisement in EVPN."
- draft-ietf-bess-evpn-prefix-advertisement-11

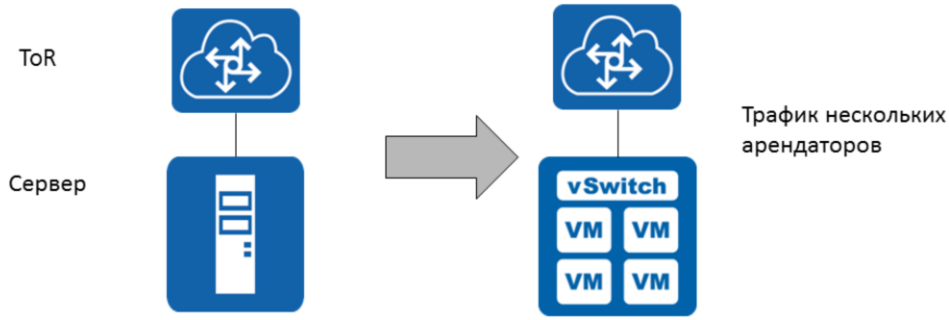
Применение EVPN в маршрутизаторах Huawei

- EVPN – это новая технология. Текущие стандарты RFC описывают маршруты 1-4 типа и поддерживают MPLS LSP в плоскости передачи данных.
- Huawei применяет технологию EVPN к более широким IP-сетям и использует ее совместно с технологией IP-туннелирования.
- IP-туннели создаются на базе технологии VXLAN. BGP EVPN выполняет роль плоскости управления, а VXLAN-туннель – плоскости переадресации. BGP EVPN используется в сценариях NVO.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

NVO

- Технология виртуализации используется в облачном ЦОД, чтобы один хост включал несколько виртуальных машин (ВМ), и каждая ВМ принадлежала разным арендаторам (tenant). Это создает новые требования к сети. Для решения этой проблемы внедряется NVO.

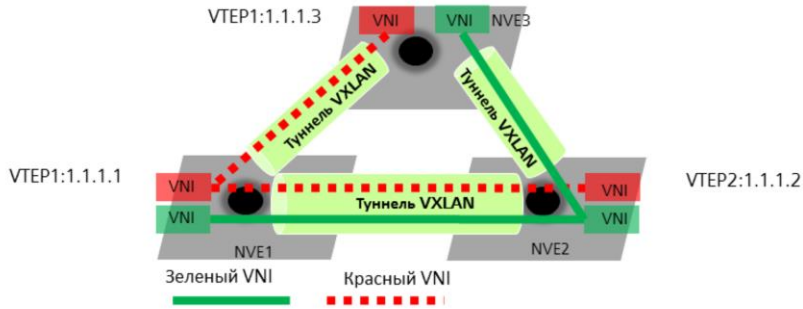


Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- NVO позволяет передавать трафик каждого арендатора через независимый оверлейный туннель.
- Несколько оверлейных туннелей могут работать в нижележащей сети.

Инкапсуляция VXLAN

- В настоящее время основными технологиями NVO являются VXLAN, NVGRE и MPLS over GRE.
- VXLAN обеспечивает возможность инкапсуляции в плоскости передачи данных, которая обеспечивает пакетную передачу данных между двумя граничными устройствами сетевой виртуализации (NVE) в общей IP-сети.
- Инкапсуляция VXLAN основана на протоколе UDP и предоставляет 8-байтовый заголовок VXLAN рядом с заголовком UDP. Идентификатор VNI состоит из 24 бит. Каждый VNI идентифицирует арендатора. Кадры данных, инкапсулированные на входной точке VTEP, не содержат внутренних тегов VLAN. Выходная точка VTEP отбрасывает кадры, несущие внутренний тег VLAN.



Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

EVPN и NVO (1)

- Использование технологии NVO решает проблему с несколькими арендаторами, но применима только к арендаторам в плоскости передачи данных.
- EVPN используется в качестве плоскости управления NVO. BGP-сеть расширяется, чтобы определить информацию NLRI на основе EVPN, которая используется для передачи сигналов управления поверх переадресации данных.
- Комбинированное использование EVPN и VXLAN отвечает следующим требованиям:
  - Обеспечивается изоляция сети с несколькими арендаторами.
  - Поддерживаются крупные арендаторы.
  - Сеть арендаторов поддерживает масштабные соединения 2 уровня в физических сетях.
  - Сети BM можно мигрировать по физическим сетям.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

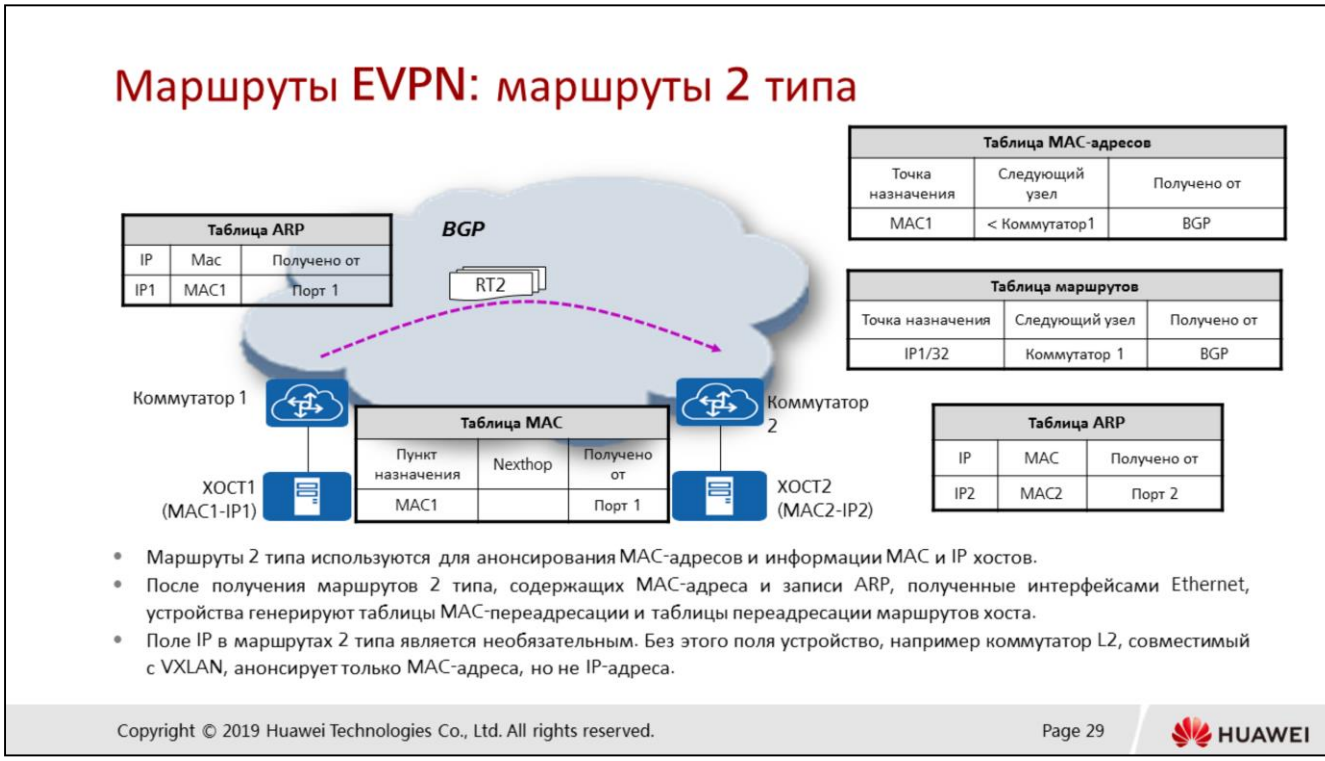
HUAWEI

- Сеть VXLAN не имеет плоскости управления, и трафик распространяется в плоскости передачи данных для обнаружения точек VTEP и информации хоста (IP и MAC-адресов, идентификаторов VNI и IP-адреса шлюза VTEP), что приводит к высокому объему трафика в ЦОД. Для решения этой проблемы VXLAN использует EVPN в качестве плоскости управления. Между точками VTEP происходит обмен маршрутами BGP EVPN для автоматического обнаружения VTEP и анонсирования информации хоста, за счет чего предотвращается высокий объем трафика.

EVPN и NVO (2)

- EVPN используется для решения следующих проблем:
  - BGP распределяет плоскость управления, а широковещательные и многоадресные пакеты реплицируются общим деревом или входом.
  - Механизм MAC learning реализуется в плоскости управления.
  - Отражение маршрутов заменяет полное соединение.
- Поскольку NVO требует создания миллионов экземпляров на физическом устройстве, масштабируемость плоскости управления очень важна. EVPN и его расширенные функции созданы для выполнения этого требования.
- Huawei сочетает EVPN с VXLAN, в основном используя маршруты 2, 3 и 5 типа.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

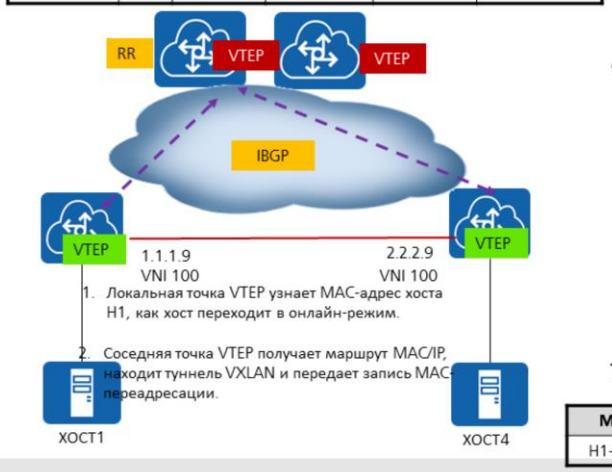


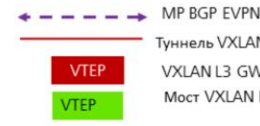
- Технология EVPN позволяет определить несколько типов маршрутов BGP EVPN, которые можно использовать для передачи адресов VTEP и информации о хосте. EVPN применяется к сети VXLAN, чтобы перенести функции обнаружения VTEP и получения информации о хосте с плоскости передачи данных на плоскость управления. Теперь познакомимся ближе с маршрутами BGP EVPN.
- VXLAN использует маршруты 2 типа (также называемые маршрутами MAC/IP Advertisement), указанные протоколом EVPN для анонсирования MAC-адреса или MAC и IP адресов хоста. BGP EVPN позволяет преобразовывать MAC-адреса и записи ARP, полученные интерфейсами Ethernet, в маршруты 2 типа. После объявления маршрутов 2 типа другим устройствам эти устройства генерируют таблицы MAC-переадресации и таблицы переадресации маршрутов хоста.
- Как правило, MAC learning запускается пакетами. BGP-EVPN

использует маршруты 2 типа, которые переносят информацию MAC для анонсирования MAC-адресов, благодаря чему экономится много трафика ARP.

EVPN VXLAN — Анонсирование маршрутов MAC/IP

Тип маршрута	RD	MAC	Метка	Тип туннеля	Следующий узел
2	1:1	H1-MAC	L2 VNI:100	8(VXLAN)	L2 VTEP: 1.1.1.9





- EVPN определяет маршруты MAC/IP для анонсирования MAC-адресов хоста, сокращая поток трафика в сети VXLAN.
  - Локальная точка VTEP считывает MAC-адрес локального хоста, преобразует его в маршрут EVPN MAC/IP и отправляет маршрут на удаленную VTEP через плоскость управления EVPN.
  - После получения маршрута MAC/IP соседняя точка VTEP передает маршрут в нужный экземпляр EVPN и находит туннель VXLAN на основе адреса следующего узла в маршруте. Если туннель доступен, VTEP передает запись MAC-переадресации.

Таблица MAC-адресов

MAC	VNI	DIP
H1-MAC	100	1.1.1.9

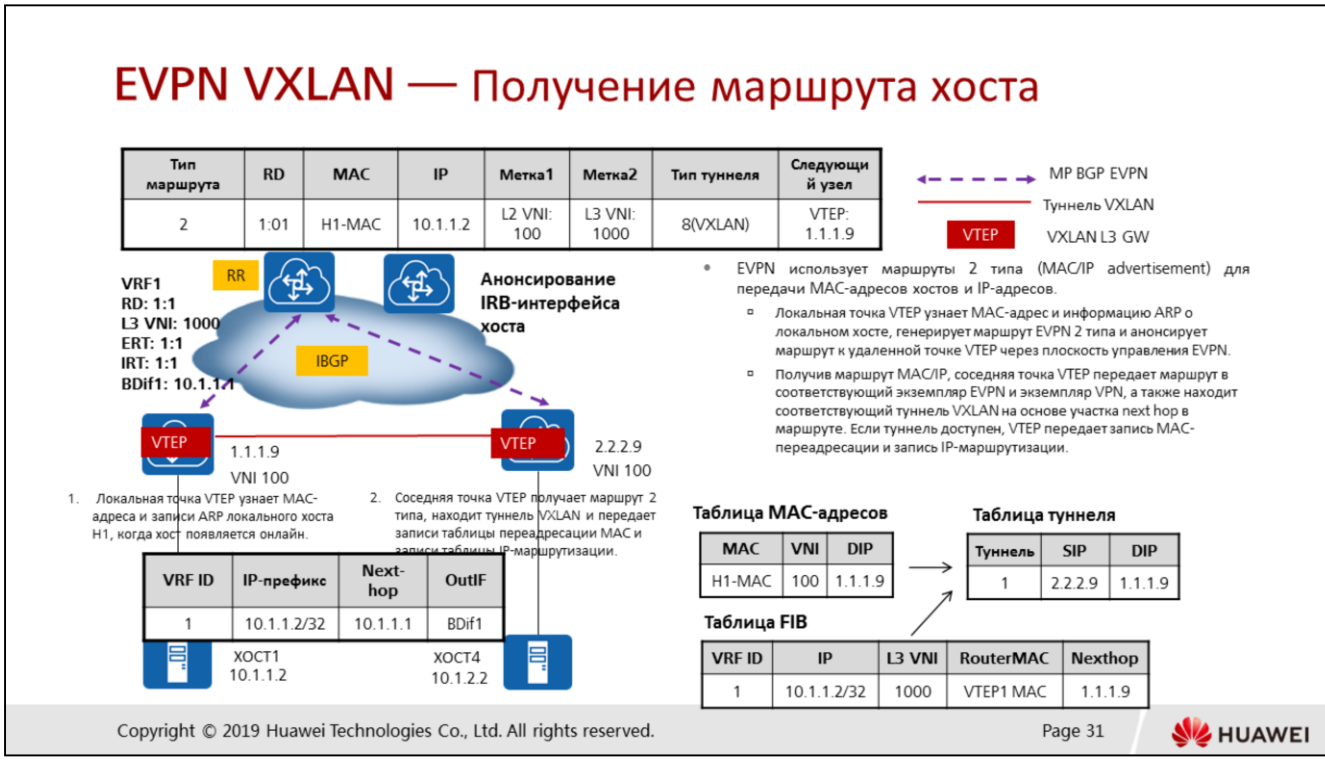
Таблица туннелей

Туннель	SIP	DIP
1	2.2.2.9	1.1.1.9

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

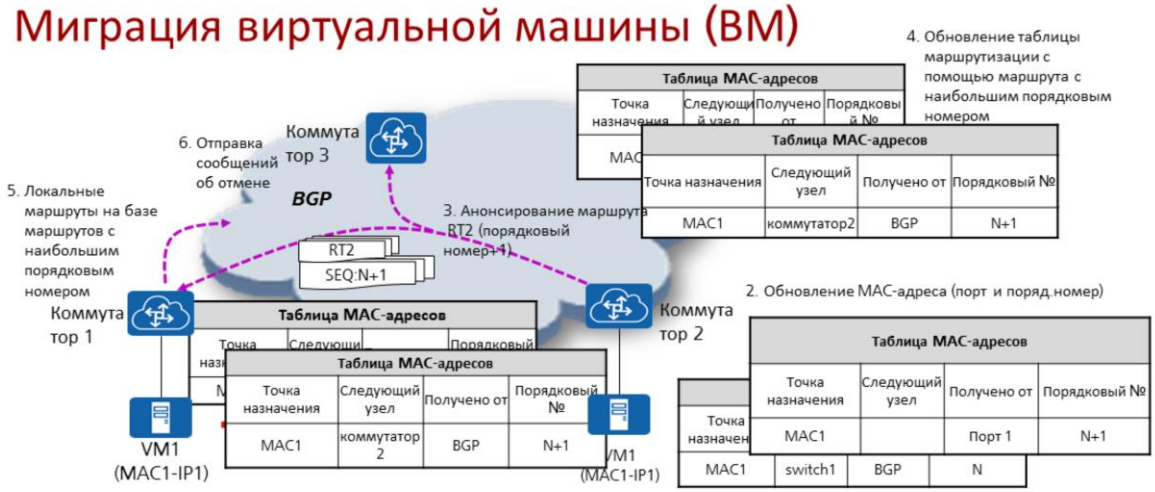
HUAWEI

- Сценарии применения маршрутов 2 типа.
  - Во-первых, анонсирование MAC-маршрутов. В этом примере мы видим, что после того, как локальный хост H1 переходит в режим онлайн, локальное устройство NVE узнает MAC-адрес хоста и отправляет MAC-адрес на удаленное устройство через BGP EVPN.
  - После получения маршрута MAC/IP соседняя точка VTEP передает маршрут в нужный экземпляр EVPN и находит туннель VXLAN на основе адреса следующего узла в маршруте. Если туннель доступен, VTEP передает запись MAC-переадресации.



- Маршруты 2 типа также называются маршрутами MAC/IP advertisement. Когда локальный хост H1 появляется онлайн, локальная точка VTEP узнает MAC-адрес и запись ARP хоста и генерирует маршруты EVPN 2 типа, и маршруты отправляются на удаленное устройство через BGP EVPN.
- После получения маршрутов MAC/IP advertisement соседняя точка VTEP передает маршруты в нужный экземпляр EVPN и находит туннель VXLAN на основании адреса следующего узла в маршрутах. Если туннель доступен, VTEP передает таблицу переадресации MAC и таблицу IP-маршрутизации.

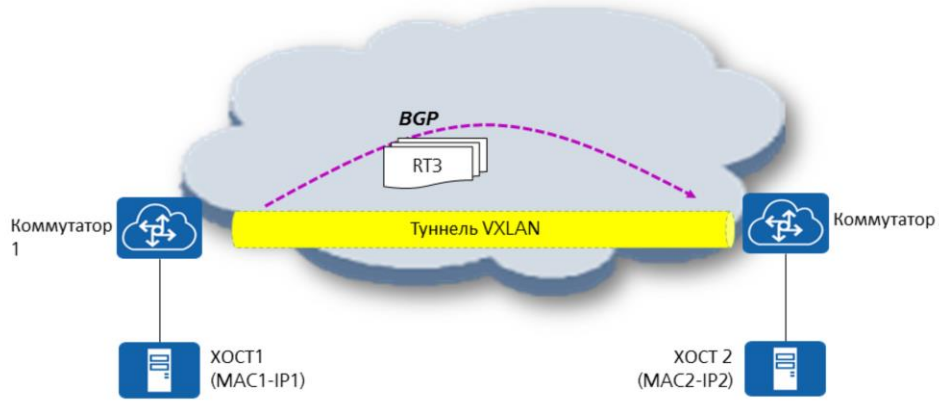
Миграция виртуальной машины (BM)



- Расширенные атрибуты EVPN содержат порядковые номера. Последний маршрут определяется путем миграции расширенных атрибутов.
- После миграции порядковый номер в маршруте увеличивается на 1 на устройстве назначения, и маршрут затем анонсируется соседнему устройству.
- Устройство, получающее этот маршрут, определяет последний маршрут на основе порядкового номера в маршруте.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Маршруты EVPN — маршруты 3 типа



- Маршруты Inclusive Multicast Ethernet Tag:
  - Маршруты 3 типа используются для автоматического создания туннелей и автоматического присоединения к широковещательным элементам VNI.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

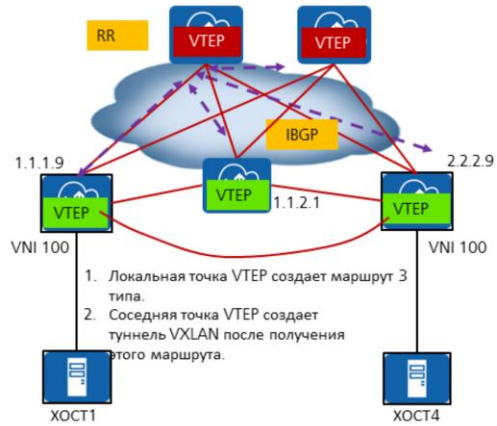
- Маршруты 3 типа также называются маршрутами Inclusive Multicast Ethernet Tag. Данный тип маршрута состоит из префиксов и атрибутов PMSI, которые используются для автоматического создания туннелей и автоматического присоединения к широковещательным элементам VNI.
- Данный тип маршрута используется для автоматического обнаружения VTEP и динамического создания туннеля VXLAN на плоскости управления VXLAN. После установления отношений соседства BGP EVPN между точками VTEP они обмениваются многоадресными маршрутами для передачи VNI уровня 2 и IP-адресов VTEP друг другу.
- Поля Originating Router IP Address и MPLS Label, передаваемые в маршрутах, указывают IP-адрес локальной точки VTEP и VNI 2 уровня соответственно. Если маршрут к IP-адресу соседней точки VTEP доступен, туннель VXLAN устанавливается от локальной точки

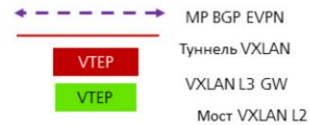
VTEP к соседней точке VTEP. Кроме того, если локальный и соседний идентификатор VNI совпадают, для последующей переадресации пакетов BUM создается список репликации входов.

EVPN VXLAN: создание туннеля

Тип маршрута	RD	Исходный IP-адрес	Метка	ID туннеля
3	1:01	1.1.1.9	L2 VNI: 100	L2 VTEP: 1.1.1.9

Инклюзивный маршрут





- Маршруты Inclusive multicast Ethernet Tag используются для передачи VNI 2 уровня и VTEP-адресов уровня 2 и динамического создания туннелей VXLAN уровня 2.
  - После конфигурирования адресов BD, L2 VNI и VTEP на локальной точке VTEP, генерируются маршруты Inclusive multicast Ethernet Tag и отправляются удаленной точке VTEP.
  - После получения маршрутов Inclusive multicast Ethernet Tag удаленная точка VTEP сравнивает параметры в маршрутах с локальными BD и L2 VNI. Если параметры одинаковы, точки VTEP устанавливают туннель VXLAN и список репликации входов для него.

Таблица туннеля

Туннель	SIP	DIP
1	2.2.2.9	1.1.1.9

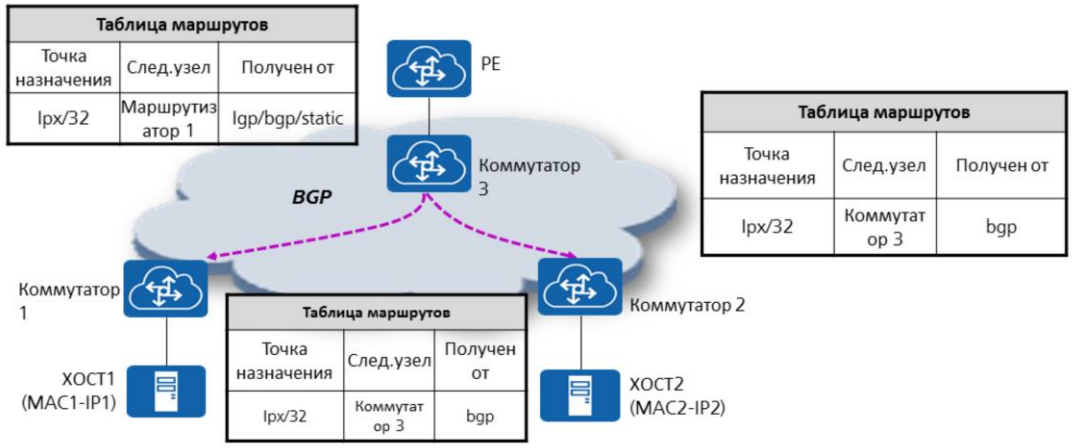
Список репликации входов туннеля VXLAN

VNI	Сосед
100	1.1.1.9

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

- Вы можете создать туннель VXLAN вручную, указав адреса VTEP и VNI в обоих концах. В динамическом BGP EVPN туннель VXLAN создается с помощью маршрутов 3 типа. Адрес локальной точки VTEP и VNI содержатся в маршрутах 3 типа, отправленных удаленной точке VTEP. После того, как удаленная точка VTEP получает маршруты, она создает туннель VXLAN с локальной точкой VTEP и список репликации входов туннеля VXLAN.

Маршруты EVPN: маршруты 5 типа



- Маршруты 5 типа также называются маршрутами IP Prefix.
  - Данный тип маршрута используется для импорта подсетей за пределами EVPN в EVPN и анонсирования маршрутов хостов.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

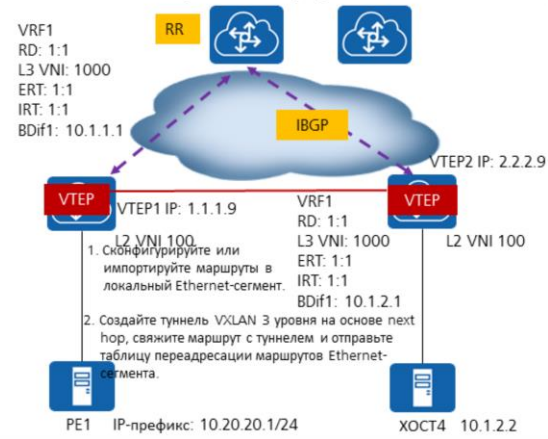
- Маршруты 5 типа также называются маршрутами IP Prefix. Данный тип маршрута используется для импорта подсетей за пределами EVPN в EVPN . Маска подсети может быть 32 бита. Маршруты 5 типа используются для анонсирования маршрутов хостов.

EVPN VXLAN — получение маршрута сегмента сети

Тип маршрута	RD	IP-префикс	Метка	Тип туннеля	Next Hop	MAC маршрутизатора	ERT
5	1:1	10.20.20.1/24	L3 VNI : 1000	8(VXLAN)	VTEP: 1.1.1.9	VTEP1 MAC	1:1

MP BGP EVPN
Туннель VXLAN
VTEP
VXLAN L3 GW

Анонсирование IP-префикса сегмента сети



- EVPN использует маршруты 5 типа для передачи VNI 3 уровня и IP-маршрутов сетевого сегмента:
  ① Локальная точка VTEP суммирует маршруты локального сегмента IP-сети и отправляет маршруты своим соседям через EVPN. Эти маршруты переносят VNI 3 уровня соответствующего VRF, адрес локальной точки VTEP в качестве next hop и MAC-адрес маршрутизатора локального NVE.
  ② После получения маршрута сетевого сегмента удаленная точка VTEP добавляет маршрут к соответствующему экземпляру VPN, создает динамический туннель VXLAN 3 уровня в соответствии с next hop, указанным в маршруте, связывает маршрут VPN с туннелем и передает таблицу переадресации маршрутов.

Таблица IP-маршрутизации

VRF ID	IP-префикс	L3 VNI	MAC маршрутизатора	Next Hop
1	10.20.20.1/24	1000	VTEP1 MAC	1.1.1.9

Таблица туннеля

Туннель	SIP	DIP
1	2.2.2.9	1.1.1.9

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Маршруты типа 5 можно использовать для передачи IP-маршрутов сегмента сети и передачи L3 VNI соответствующего VRF.
- Их также можно использовать для передачи VNI 3 уровня, представляющего VRF. Что такое L3 VNI?
  - В среде распределенных шлюзов подсети, которые должны поддерживать связь, представляют собой поле виртуального маршрута (VRF). Однако пакет не содержит информацию VRF. Таким образом, VNI сопоставляется с VRF через определенный идентификатор VNI. Такой VNI называется L3 VNI.
  - После получения маршрута сетевого сегмента удаленная точка VTEP добавляет маршрут к соответствующему экземпляру VPN, создает динамический туннель VXLAN 3 уровня в соответствии с следующим узлом, указанным в маршруте, и отправляет таблицу маршрутизации.



Тест

1. Какие типы маршрутов используются для BGP EVPN + VXLAN? ()
   A. Тип 1
   B. Тип 2
   C. Тип 3
   D. Тип 4
   E. Тип 5
2. Кратко опишите функции маршрутов типа 2.

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Ответ:
  - B, C, E
  - Маршруты 2 типа также называются маршрутами MAC/IP advertisement и используются для миграции BM в среде распределенных шлюзов.

Краткое содержание

- Обзор EVPN
- Принципы работы EVPN
- Применение EVPN в NVO

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Дополнительная информация

- https://datatracker.ietf.org/doc/rfc8365 /
- https://datatracker.ietf.org/doc/rfc7209 /
- https://datatracker.ietf.org/doc/rfc7432 /

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Рекомендации

- Huawei E-learning
  - http://support.huawei.com/learning/Index!toTrainIndex
- Библиотека примеров на сайте технической поддержки Huawei
  - http://support.huawei.com/enterprise/servicecenter?lang=zh

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

Спасибо!

www.huawei.com

Обучение и сертификация Huawei по маршрутизации и коммутации

– Проектирование сетей и продукты

www.huawei.com

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Предисловие

- IP-сети стали неотъемлемой частью жизни людей.
- Проектирование IP-сетей для предприятий в соответствии с их потребностями является актуальной темой.
- Этот курс знакомит с принципами и передовыми методами проектирования корпоративных IP-сетей.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Цели

- По окончании этого курса вы сможете:
  - Описать основные принципы проектирования корпоративных сетей.
  - Описать основной процесс проектирования корпоративной сети.
  - Проанализировать общие требования к проектированию корпоративных сетей.
  - Описать передовые методы проектирования корпоративных сетей.
  - Описать типы продуктов Huawei для корпоративных сетей.
  - Проектировать стандартные корпоративные сети.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Содержание

1. **Принципы проектирования корпоративных сетей**
2. Обзор процесса проектирования корпоративных сетей
3. Общая информация о продуктах для корпоративных сетей
4. Анализ примеров проектирования корпоративных сетей

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Платформа корпоративной сети



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Корпортивная сеть является платформой для поддержки корпоративных сервисов и информационным центром для предприятий.
  - У предприятия может быть много сервисов, таких как офис, производство, мониторинг и обслуживание клиентов (колл-центр).
  - Различные сервисы связаны через сетевую платформу предприятия для эффективной работы предприятия.
  - Сеть является основной платформой, поддерживающей корпоративные сервисы.
  - Проектирование корпоративных сетей очень важно для работы корпоративных сервисов.



- Планирование. Помощь компаниям в планировании корпоративных сетей, обеспечении информационной безопасности, унификации коммуникации и планировании ИТ-систем на основе долгосрочных целей предприятий, за счет эффективного управления и отслеживания рисков и системных проблем.
- Проектирование. Основываясь на понимании существующей сети, системы и приложений, разработать детальный проект, чтобы удовлетворить требования корпоративных пользователей к текущим технологиям и услугам, а также поддерживать возможности, надежность, безопасность, масштабируемость и производительность предприятий в области ИТ и сервисов.
- Внедрение. Помощь компании в разработке, установке и тестировании сервисов, сетей и ИТ-систем на основе проектных спецификаций, чтобы удовлетворить требования клиентов к сервисам и техническим характеристикам.
- Эксплуатация. Помощь компании в поддержке непрерывной исправной работы сервисов, активный мониторинг и управление системой, а также максимальное повышение производительности, емкости, доступности, надежности и безопасности системных устройств и прикладных систем.
- Улучшение. Помощь компании в постоянном улучшении качества обслуживания, регулярном обновлении и усовершенствовании услуг в соответствии с требованиями клиентов, а также внедрении целевых политик и операций для улучшения качества обслуживания.

Основные принципы проектирования сетей



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Основные принципы проектирования сети:
  - Надежность: при возникновении сбоя в сети сетевые услуги не прерываются.
  - Масштабируемость: сеть может поддерживать увеличение объема услуг и пропускной способности.
  - Функциональность: сеть должна поддерживать множество услуг и иметь безопасную многоуровневую гарантию качества услуг.
  - Управляемость: сеть должна поддерживать стандартные методы управления для облегчения мониторинга и обслуживания.
- Кроме того, при проектировании сети должна быть учтена стоимость. Мы должны выбрать наиболее выгодное решение при проектировании с учетом требований к обслуживанию.

Процесс проектирования корпоративной сети



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Проектирование сети включает в себя множество модулей. Потребность в модулях определяется в соответствии с требованиями обслуживания предприятия.

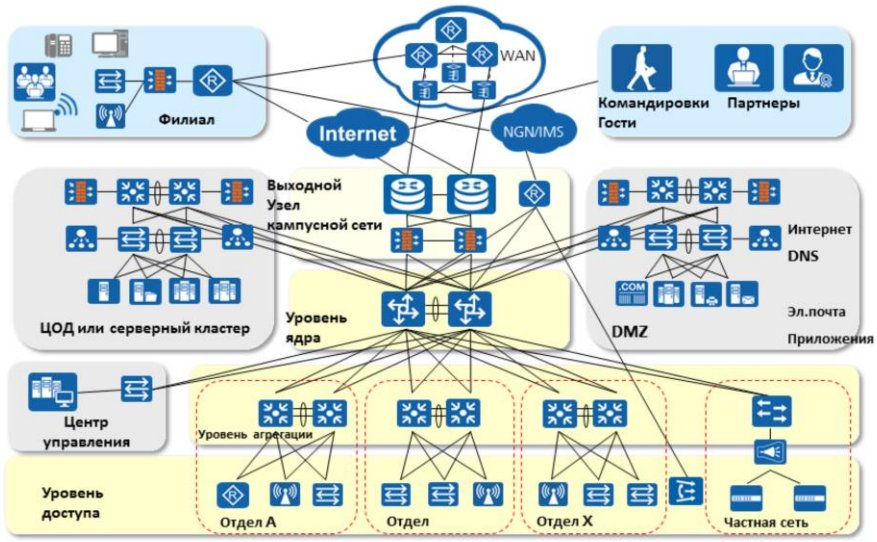
Методы и подходы к проектированию сети



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Общие методы и подходы к проектированию сети:
  - Метод модульного проектирования
  - Метод иерархического проектирования
  - Подход к проектированию «сверху вниз»
  - Подход к проектированию «снизу вверх»

Модульное проектирование сети

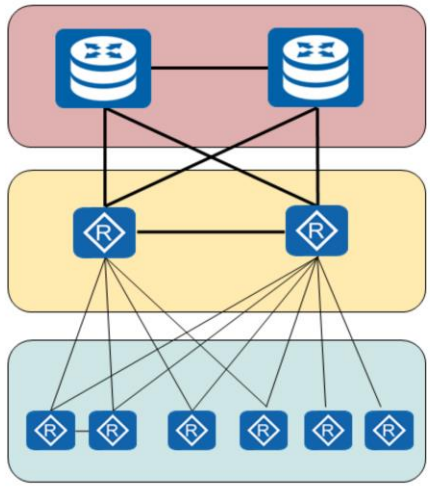


© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Большая корпоративная сеть может быть разделена на различные модули в зависимости от функций. Различные модули имеют разные требования и функции. Общая классификация выглядит следующим образом:
  - Кампусная сеть: все локальные сети головного офиса предприятия
  - Демилитаризованная зона (DMZ)
  - WAN
  - Сеть ЦОД
  - Сеть филиала
  - Сеть удаленных пользователей
- Модульная конструкция сети имеет следующие преимущества:
  - Функции не зависят друг от друга. Каждый модуль может быть спроектирован отдельно.
  - Облегчает расширение возможностей. Например, добавление модуля не влияет на работу всей сети.
  - Простота управления. Например, для разных модулей определены разные политики безопасности.
- При фактическом развертывании выходной маршрутизатор кампусной сети часто интегрируется с функцией IP PBX.

Иерархическое проектирование сети



- Уровень ядра
  - Высокоскоростная передача данных
  - Высокая надежность
- Уровень агрегации
  - Суммирование маршрутов
  - Конвергенция трафика
- Уровень доступа
  - Доступ терминальных устройств
  - Контроль доступа

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Иерархическое проектирование сети дает следующие преимущества:
  - Устройства могут использоваться на разных уровнях для снижения затрат.
  - Простота понимания: функции иерархической сети дифференцированы.
  - Модульный дизайн: иерархическая архитектура также является модульной конструкцией, которая облегчает проектирование, управление и расширение сети.
  - Изоляция неисправностей: многоуровневая структура способствует эффективному контролю над последствиями неисправностей.

Подход к проектированию «сверху-вниз»



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Проектирование «сверху-вниз» выполняется на основе прикладного уровня модели OSI. Сеть должна поддерживать приложения верхнего уровня.
- Проектирование «сверху-вниз» состоит в том, чтобы сначала проанализировать требования к прикладному уровню, а затем спроектировать архитектуру сети и базовые сервисы на основе этих требований.
  - Например, если предприятию необходимо развернуть систему видеоконференций (с помощью многоадресной передачи), при проектировании сети необходимо планировать топологию сети, многоадресную передачу и QoS.

Походы «сверху-вниз» и «снизу-вверх»

Подход к проектированию	Преимущества	Недостатки	Сценарий использования
Сверху-вниз	• Требования к приложениям хорошо поддерживаются с точки зрения приложений. • Текущие и будущие требования могут быть удовлетворены с точки зрения всей сети.	• Проектировщикам сетей требуется вкладывать больше времени и сил в проектирование.	• Крупномасштабная новая сеть
Снизу-вверх	• Проектирование осуществляется на основе опыта • Быстрая реализация	• Общие требования не учитываются. • Долгосрочные требования могут быть не удовлетворены.	• Небольшая новая сеть • Реконструкция сети

- Подходы к проектированию «сверху-вниз» и «снизу-вверх» не противоречат друг другу:
  - Они применяются в разных сценариях.
  - Их применение можно рассматривать для одного сетевого проекта.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Подход «сверху-вниз» соответствует подходу «снизу-вверх».
- В подходе к проектированию «снизу-вверх» не анализируются конкретные требования приложений с точки зрения сервисов. Проектирование сетей осуществляется на основе опыта.
  - Например, при расширении офисной сети архитектура сети остается неизменной. Добавляются только коммутаторы доступа.

Содержание

1. Принципы проектирования корпоративных сетей
2. **Процесс проектирования корпоративных сетей**
   - Анализ требований пользователей
   - Проектирование топологии сети
   - Проектирование LAN
   - Проектирование WAN
   - Выбор сетевых устройств
   - Планирование IP-адресов и наименование устройств
   - Планирование маршрутизации

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Почему необходимо анализировать требования пользователей?



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Для обычных предприятий корпоративная сеть является технической платформой, на базе которой разрабатываются корпоративные услуги.
- Следовательно, сеть должна разрабатываться в соответствии с услугами компании.

Процедура анализа требований пользователей



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Первым шагом в анализе требований пользователей является определение состояния сети следующими методами:
  - Запрос документов
  - Консультирование сторон
  - Мониторинг сети
  - Анализ трафика
- Вторым этапом анализа требований пользователей является определение целей организации. Без учета таких целей проект сети не имеет смысла. Стандартные организационные цели:
  - Повышение удовлетворенности клиентов
  - Добавление сервисов
  - Повышение конкурентоспособности
  - Снижение затрат
- Определение организационных ограничений имеет важное значение, поскольку они напрямую влияют на проект сети. Стандартные организационные ограничения :
  - Бюджет
  - Трудовые ресурсы
  - Политика
  - Временные рамки



- Общие цели с технической точки зрения:
  - Увеличить пропускную способность сети.
  - Сократить время перерывов в обслуживании.
  - Упростить управление сетью.
  - Повысить безопасность сети.
  - Повысить надежность ключевых услуг.
- Технические ограничения:
  - Кабели в действующей сети не поддерживают новые технологии.
  - Пропускная способность действующей сети не обеспечивает поддержку новых приложений.
  - Сеть должна быть совместима со старыми устройствами.
  - Старые приложения должны поддерживаться.

Содержание

1. Принципы проектирования корпоративных сетей
2. **Процесс проектирования корпоративных сетей**
   - Анализ требований пользователей
   - Проектирование топологии сети
   - Проектирование LAN
   - Проектирование WAN
   - Выбор сетевых устройств
   - Планирование IP-адресов и наименование устройств
   - Планирование маршрутизации

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Принципы проектирования топологии сети

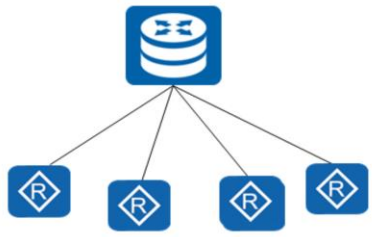


© 2019 Huawei Technologies Co., Ltd. Все права защищены.

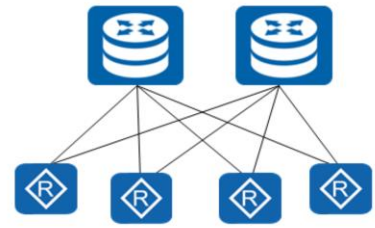
HUAWEI

- Модульность
  - Как упоминалось ранее, модульная конструкция упрощает проектирование сети, а также управление сетью и ее расширение.
- Иерархичность
  - Иерархическая топология позволяет снизить затраты и изолировать неисправности в сети.
- Надежность
  - Повышение надежности сети позволяет снизить воздействие отказов сети, вызванных неисправностью одного элемента, реализовать балансировку нагрузки и повысить производительность сети.
  - Однако повышение надежности сети часто увеличивает сложность и стоимость сети.
- Безопасность
  - Базовые маршрутизаторы, граничные точки, коммутаторы и серверы должны быть защищены.
  - Межсетевой экран защищает сеть от внешних атак.
- Высокая производительность
  - В топологии сети отсутствуют узкие места производительности.
- Экономичность
  - Учитывается стоимость сети.

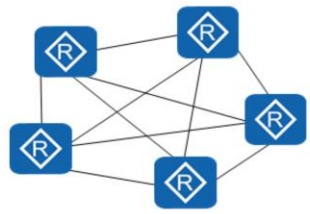
Стандартные топологии сети



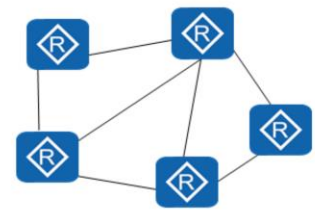
Топология «звезда»



Топология «двойная звезда»



Топология «сетка»

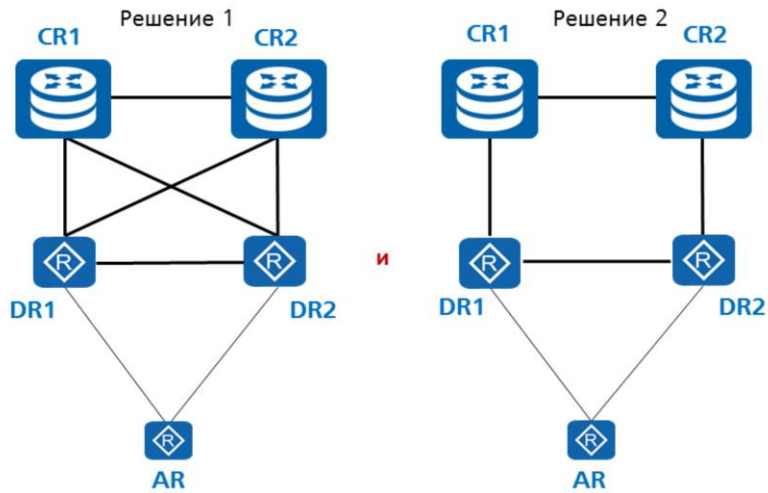


Частичная сеточная топология

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Немногие корпоративные сети используют только одну структуру топологии. В большинстве случаев используется несколько топологий.
  - Топология «звезда» используется, когда сеть нижнего уровня подключена к сети верхнего уровня.
  - В случае сетевого соединения на одном уровне используется топология сетки или частичная сеточная топология.

Пример: какая топология лучше?



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Для связи устройств агрегации с основными устройствами существуют две популярные топологии.
  - Решение 1:
    - Маршрутизатор агрегации подключен к двум основным маршрутизаторам, но два маршрутизатора агрегации не соединены между собой.
  - Решение 2:
    - Маршрутизатор агрегации подключен к основному маршрутизатору и другому маршрутизатору агрегации.
- Два решения гарантируют, что на маршрутизаторе доступа не возникнет сбоя. Какое решение лучше?
- С технической точки зрения:
  - Если узел или канал в сети неисправны, является ли путь передачи данных от уровня доступа к уровню ядра оптимальным?
  - Решение 1: независимо от того, в какой точке происходит сбой, данные передаются с уровня доступа на уровень ядра через три узла.
  - Решение 2: если канал между CR1 и DR1 неисправен, данные могут достигнуть уровня ядра через четыре узла (AR -> DR1 -> DR2 -> CR2).
  - С технической точки зрения решение 1 лучше.
- С точки зрения затрат:
  - Если уровень ядра находится далеко от уровня агрегации, затраты на решение 1 вдвое превышают затраты на решение 2.
  - С точки зрения затрат решение 2 лучше.
- Сравнение:
  - В сети LAN стоимость канала низкая. Можно использовать решение 1 или комбинацию двух решений.

- В сети WAN рекомендуется использовать решение 2, поскольку стоимость канала высокая. Кроме того, при разработке маршрутов следует избегать использования субоптимальных маршрутов.

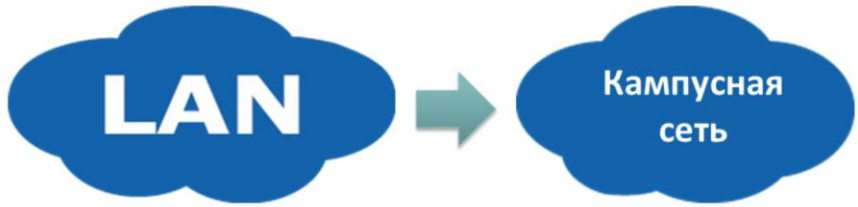
Содержание

1. Принципы проектирования корпоративных сетей
2. **Обзор процесса проектирования корпоративных сетей**
   - Проектирование топологии сети
   - Проектирование LAN
   - Проектирование WAN
   - Выбор сетевых устройств
   - Планирование IP-адресов и наименование устройств
   - Планирование маршрутизации
   - PBR и политика маршрутизации

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Сеть LAN и кампусная сеть



С технической точки зрения, локальная сеть (LAN) – это вычислительная сеть, покрывающая небольшую область.

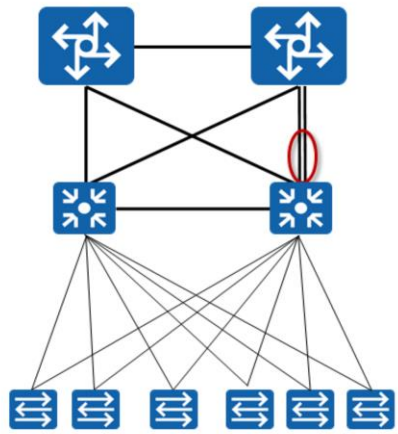
С точки зрения обслуживания, кампусная сеть – это вычислительная сеть внутри кампуса предприятия.
Кампусная сеть также является локальной сетью.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- С технической точки зрения LAN – это вычислительная сеть, покрывающая небольшую область.
  - Современные сети LAN часто используют только технологию одного канального уровня, то есть технологию Ethernet.
  - Поэтому технология Ethernet является признанным стандартом для технологии LAN.
- С точки зрения сервиса, кампусная сеть – это вычислительная сеть внутри кампуса предприятия.
  - Кампусная сеть – это также локальная сеть или комбинация нескольких локальных сетей.
  - Поэтому LAN и кампусная сеть описываются вместе.

Применение технологий в иерархической сети



Маршрутизация 3 уровня:
- Кросс-соединение
- Агрегация каналов

Коммутационная сеть 2 уровня
- VLAN
- Протокол STP, Smart Link, CSS и iStack
- VRRP

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Оптимальный метод на уровне доступа
  - Не подключайте к сетям VLAN коммутаторы доступа. Подключите одинаковые сервисы к одному коммутатору доступа и используйте одну сеть VLAN.
  - Используйте RSTP или MSTP для предотвращения петель и включите функцию пограничного порта на порту, подключенному к хостам.
  - Подключите интерфейс доступа к хосту, подключите интерфейс соединительной линии к коммутатору агрегации и настройте интерфейс соединительной линии так, чтобы он разрешал проходить пакетам из указанной VLAN (не разрешайте всем сетям VLAN проходить через интерфейс).
  - Для топологии с двумя восходящими линиями связи может использоваться технология Smart Link.
- Оптимальный метод на уровне агрегации
  - Используйте VRRP для дублирования шлюзов для хостов.
  - Разверните маршруты уровня 3 между основными устройствами агрегации для распределения нагрузки и быстрой конвергенции.
  - Агрегирующие и основные устройства используют топологию «полная сетка», но не квадратную топологию.
  - Когда коммутатор агрегации объявляет маршруты, сначала выполните суммирование маршрутов.

- Между устройствами агрегации и доступа используется соединение уровня 2.
- Используйте технологию агрегации каналов для важных каналов, чтобы увеличить пропускную способность и улучшить резервирование каналов.

Стандартные локальные сети

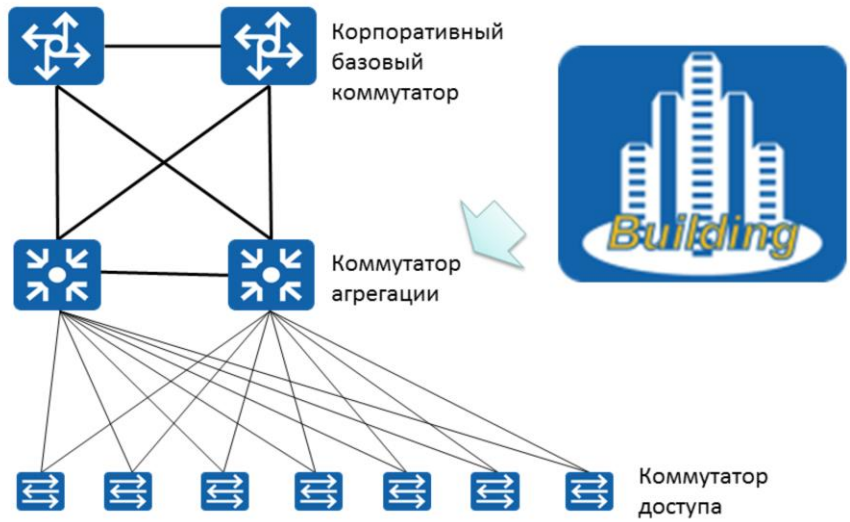
- Сети LAN зданий
- Кампусные сети
- Сети LAN ЦОД
- Сети LAN среднего размера
- Сети LAN малого размера

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Выше приведено описание распространенных локальных сетей.

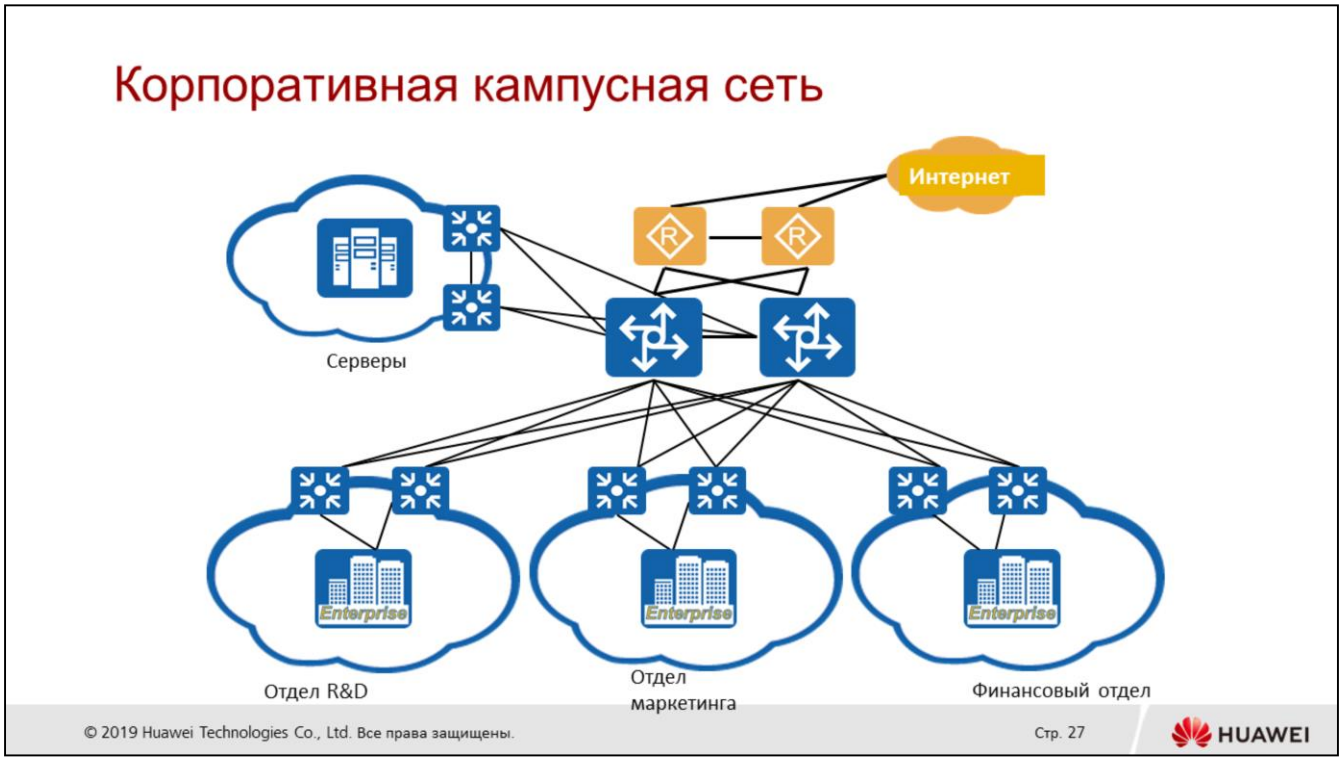
Сети LAN зданий



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

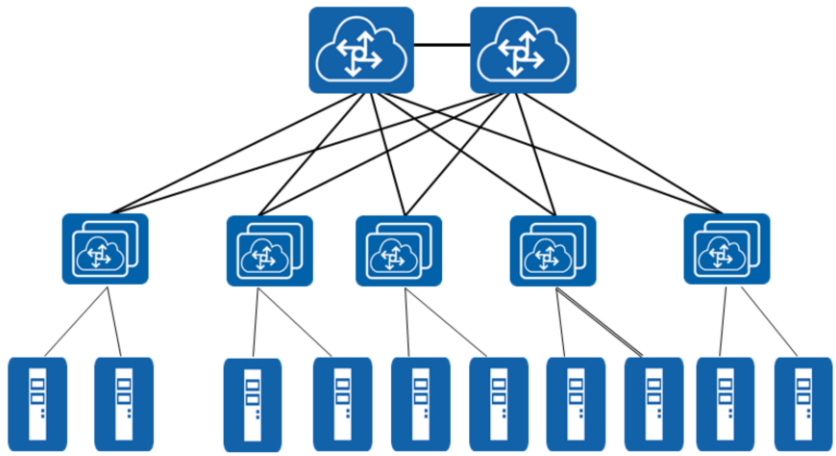
HUAWEI

- Сеть LAN здания является наиболее типичной сетью LAN.
  - Как правило, LAN зданий делится по этажам или отделам.
  - Коммутаторы доступа подключаются к одному или нескольким этажам или отделам.
  - Коммутатор агрегации подключен к нескольким коммутаторам доступа.
  - Коммутатор агрегации здания связан с другими модулями (например, центрами обработки данных) в кампусной сети предприятия через базовые коммутаторы.
  - В большинстве случаев для снижения затрат между уровнем доступа и уровнем агрегации используется соединение уровня 2 .
  - Как правило, коммутатор доступа имеет резервируемое подключение к двум коммутаторам агрегации. RSTP или MSTP используются для предотвращения петель.
  - Соединение уровня 3 используется между уровнем агрегации и уровнем ядра для быстрой конвергенции и балансировки нагрузки.
  - Для управления маршрутами на коммутаторе агрегации могут использоваться политики.
  - В небольших зданиях уровень ядра и уровень агрегации могут быть объединены.



- Корпоративная кампусная сеть может рассматриваться как соединение между несколькими локальными сетями зданий.
  - В корпоративной кампусной сети используются высокоскоростные соединения. Если сеть новая, рекомендуется использовать каналы с пропускной способностью 10 Гбит/с и выше.
  - Физическое расстояние между сетями небольшое (обычно в пределах нескольких километров), поэтому обычно компании сами строят инфраструктуру, например каналы связи.
  - В кампусной сети коммутаторы агрегации во всех зданиях могут быть подключены к двум основным коммутаторам, которые поддерживают друг друга.
  - Крупная кампусная сеть может иметь более двух основных устройств. Уровень ядра использует кольцевую топологию, топологию с частичной или полной сеткой.
  - При планировании адресов в здании используется сегмент смежных IP-адресов для упрощения агрегации маршрутов.
  - На уровне доступа необходимо планировать механизмы обеспечения безопасность. Рекомендуется использовать NAC для аутентификации и авторизации доступа пользователей.

Сеть LAN ЦОД

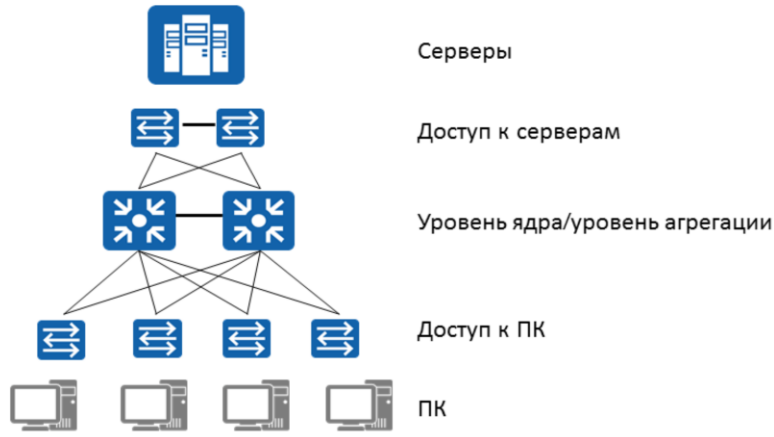


© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Различия между локальной сетью ЦОД и обычной локальной сетью заключаются в следующем:
  - Поскольку ЦОД является информационным центром компании, в его сеть LAN поступает большой объем внешнего трафика. Поэтому в таких сетях используются высокопроизводительные коммутаторы.
  - В связи с использованием таких технологий, как серверные кластеры и виртуальные машины, объем внутреннего трафика в LAN ЦОД большой. Следовательно, общая полоса пропускания постепенно снижается от уровня доступа до уровня агрегации и уровня ядра. Однако ЦОД не требуется конвергенция.
  - Для реализации таких функций, как балансировка нагрузки и резервирование каналов, серверы предоставляют несколько сетевых адаптеров, а коммутаторы доступа должны поддерживать такие функции, как связывание каналов.
  - Некоторые новые технологии, такие как FCoE, требуют поддержки коммутаторов.
  - Для удовлетворения требований приложений, таких как миграция виртуальных машин, ЦОД использует сети уровня 2.
  - Для предотвращения возникновения петель в крупномасштабной сети уровня 2 можно использовать технологии виртуализации коммутации, такие как CSS, стекирование, M-LAG и SVF.

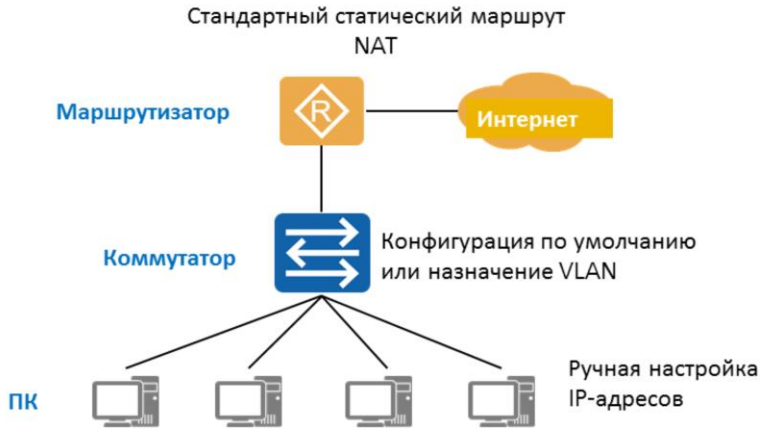
Сеть LAN среднего размера



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Архитектура локальной сети среднего размера аналогична архитектуре локальной сети здания.
  - Локальная сеть среднего размера имеет небольшой размер. Функции уровня ядра и уровня агрегации объединены в группе устройств.

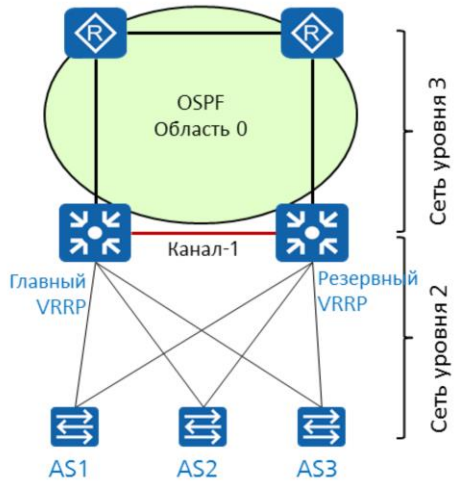
Сеть LAN малого размера



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Сеть LAN малого размера имеет простейшую архитектуру.
  - Как правило, коммутаторы 2 уровня подключаются к хостам нисходящей линии связи и выходному маршрутизатору восходящей линии связи.

Пример: организация сети VRRP+STP



Вопрос:
Сеть 3 уровня развернута между основными устройствами и устройствами агрегации. С учетом стоимости, основные устройства и устройства агрегации подключены в режиме квадрата, используется протокол OSPF, а маршруты сегментов сервисной сети анонсируются путем импорта маршрутов.
Если сеть 2 уровня развернута между устройствами агрегации и доступа, является ли канал 1 каналом 2 уровня или каналом 3 уровня?

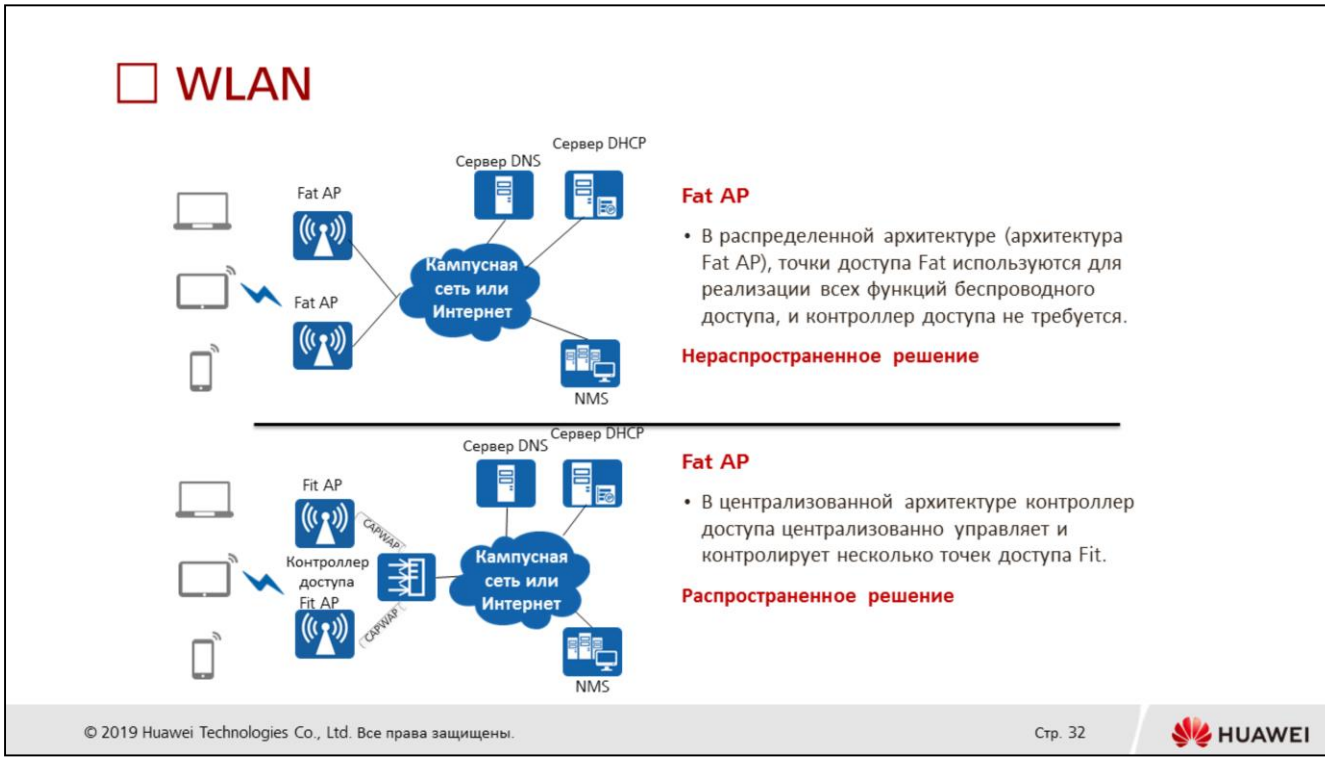
Что будет, если канал 1 является каналом 3 уровня?
Что будет, если канал 1 является каналом 2 уровня?
Существует ли хорошее комплексное решение?

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Что будет, если канал 1 является каналом 3 уровня?
  - В качестве корневого коммутатора и вспомогательного корневого коммутатора STP настраиваются главный и резервный коммутатор соответственно. Если канал 1 является каналом 3 уровня, STP не будет блокировать все интерфейсы коммутатора доступа (определить этот коммутатор сложно, например, AS1). Однако один интерфейс на других коммутаторах доступа будет заблокирован STP.
  - Таким образом, AS1 становится ключевым узлом в сети, и весь трафик VRRP проходит через AS1. Если AS1 неисправен, вся сеть ниже уровня конвергенции закрывается.
- Что будет, если канал 1 является каналом 2 уровня?
  - Аналогично, d качестве корневого коммутатора и вспомогательного корневого коммутатора STP настраиваются главный и резервный коммутатор соответственно. Если канал 1 является каналом 2 уровня и разрешает все VLAN, используемые уровнем доступа, все интерфейсы коммутаторов доступа, подключенных к резервному коммутатору, блокируются STP.
  - Однако, если канал 1 является чистым каналом 2 уровня, сеть 3 уровня между уровнем ядра и уровнем агрегации является топологией типа «цепочка». Любые сбои устройства или канала могут привести к разделению области 0 OSPF.
- Комплексное решение:
  - Канал 1 – это канал уровня 2, который разрешает все VLAN, используемые уровнем доступа.
  - Включите VLAN и создайте интерфейс VLANIF на двух коммутаторах агрегации для установления отношений OSPF между ними. Таким образом, сеть уровня 3 использует кольцевую архитектуру и обладает избыточностью.
  - Учитывая важность канала 1, для повышения надежности может использоваться связывание каналов.
  - Вы также можете использовать MSTP и развернуть главные устройства нескольких групп

VRRP для балансировки нагрузки.



- Fat AP
  - В распределенной архитектуре (также называемой архитектурой FAT AP) точки доступа Fat AP используются для реализации всех функций беспроводного доступа, и контроллер доступа не требуется.
  - Раньше распределенная архитектура широко применялась в сетях WLAN. С увеличением числа точек доступа такие задачи управления, как настройка точки доступа и обновление программного обеспечения, сопряжены с высокими затратами. Поэтому эта архитектура применяется реже.
  - Это нераспространенное решение.
- Fit AP
  - В централизованной архитектуре (также называемой архитектурой Fit AP) контроллер доступа централизованно управляет несколькими точками Fit AP.
  - В централизованной архитектуре контроллер доступа и точки доступа реализуют беспроводной доступ. Централизованная архитектура является основной архитектурой корпоративных WLAN и WLAN провайдеров, поскольку она обеспечивает централизованное управление, аутентификацию и управление безопасностью. Это решение является общим решением для корпоративной сети.
  - Это распространенное решение.
- Проектирование WLAN требует профессиональных знаний и инструментов. У нас есть профессиональный курс по проектированию сети WLAN.

Содержание

1. Принципы проектирования корпоративных сетей
2. **Процесс проектирования корпоративных сетей**
   - Проектирование LAN
   - Проектирование WAN
   - Выбор сетевых устройств
   - Планирование IP-адресов и наименование устройств
   - Планирование маршрутизации
   - PBR и политика маршрутизации
   - Подключение к сети Интернет

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Корпоративная сеть WAN



- Корпоративная глобальная сеть (WAN) – это частная сеть предприятия, которая использует арендованные каналы связи или самостоятельно построенные каналы для соединения узлов, таких как головной офис, ЦОД, филиалы, офисы и мобильные офисы.
- Корпоративная глобальная сеть представляет собой частную сеть предприятия, построенную предприятием, или созданную на основе арендованных каналов.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Корпоративная сеть WAN = граница выхода корпоративной сети + канал WAN, арендованный у оператора или построенный компанией самостоятельно.

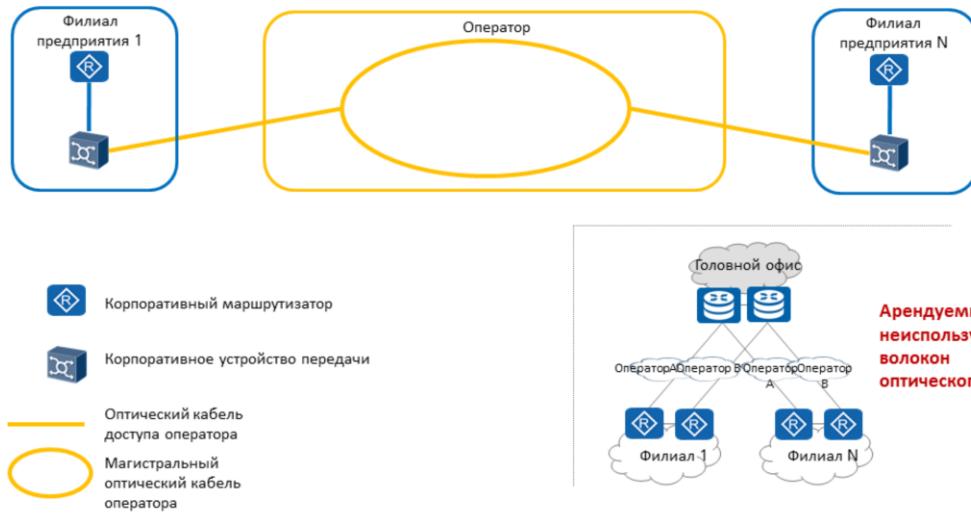
Этапы проектирования сети WAN

- Многоуровневая корпоративная сеть WAN
  - Многоуровневая структура управления на предприятиях определяет многоуровневую структуру корпоративных сетей WAN. Передача данных сервисов, модель топологии и режим доступа между узлами сети на разных уровнях могут быть одинаковыми или разными.
- Различные модели сетевой топологи
  - Различные модели топологии применяются к различным моделям трафика.
- Режимы передачи данных сервисов
  - Доступны режимы IP и VPN и используются различные политики взаимодействия или изоляции WAN.
- Этапы создания решения WAN
  - Доступны технические и отраслевые решения. Техническое решение фокусируется на создании WAN между двумя уровнями сетевых узлов. Отраслевое решение предназначено для конкретных отраслей (например, электроэнергетика и правительство) или сценариев (например, для крупных предприятий).
  - Техническое решение: сценарии классифицируются на основе технологий межсетевого соединения WAN, например, сценарии частной линии SDH/MSTP/WDM.
  - Отраслевое решение: сценарии классифицируются по отраслям. Технологии, используемые в различных отраслевых решениях, могут быть одинаковыми.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Технология развертывания сети WAN – аренда неиспользуемых волокон оптического кабеля



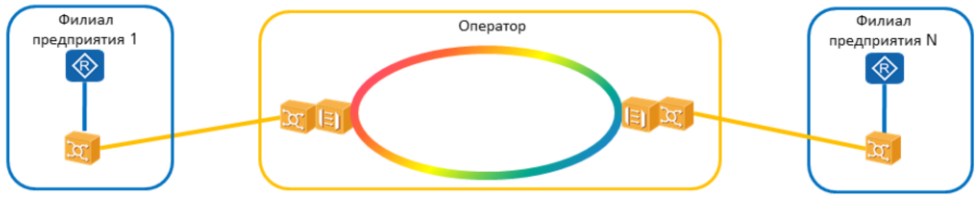


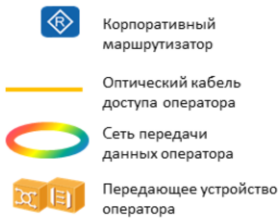
Арендуемые неиспользуемых волокон оптического кабеля

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Типы частных каналов классифицируются на основе диапазона аренды.

Технология развертывания сети WAN – аренда частных линий связи SDH/MSTP/WDM







Аренда частных линий связи SDH/MSTP/WDM

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- В данном случае MSTP означает мультисервисную транспортную платформу.

Архитектура на основе частной линии связи SDH/MSTP/WDM

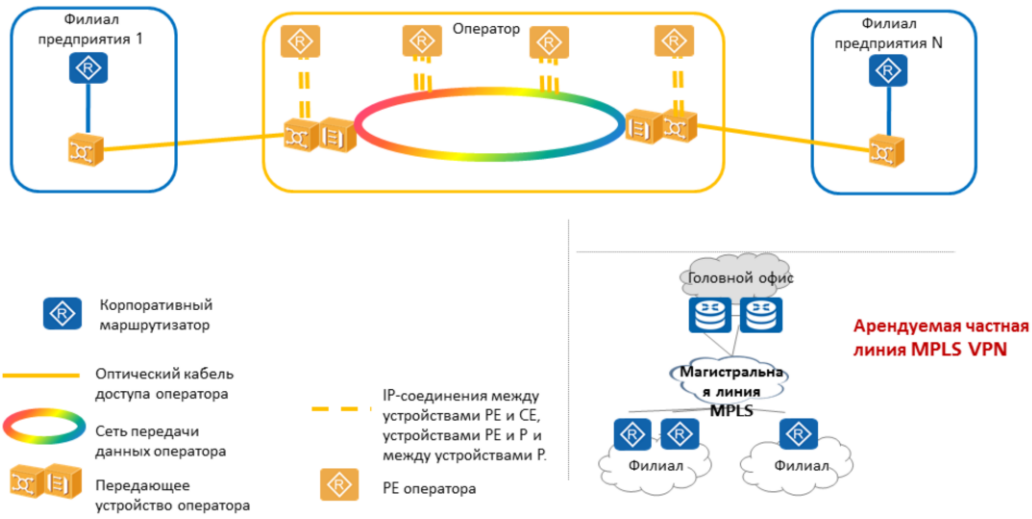


- Сценарий применения
  - Предприятия, требующие высокого качества линий WAN
  - Предприятия, предъявляющие высокие требования к безопасности и конфиденциальности связи
  - Предприятия, которые хотят иметь независимые магистральные сети, но не имеют возможностей для построения собственных сетей
- Преимущества
  - Частная линия делится на физические временные интервалы. Малая задержка и хорошая конфиденциальность.
  - Высокое качество услуг и QoS
  - Точная полоса пропускания (удлинение сетевого кабеля)
- Недостатки
  - Стоимость частной линии SDH/MSTP/WDM высокая, но ниже, чем у неиспользуемых волокон оптического кабеля.
  - Долгий период предоставления.
- Ситуация
  - Сеть передачи данных WAN крупных предприятий широко используется в Китае.
  - Финансовые предприятия широко используют частные линии связи SDH/MSTP/WDM.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Технология развертывания сети WAN – Аренда частных линий связи MPLS VPN



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Мультисервисная транспортная платформа (MSTP)
- Использовать передающие устройства оператора в аппаратных предприятия необязательно. Определите, следует ли развертывать решение на основе оптических кабелей доступа и сервисного доступа к аппаратной предприятия.

Архитектура на основе частных линий связи MPLS VPN



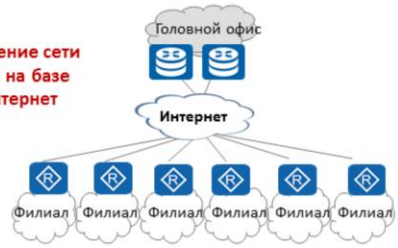
- Сценарий применения
  - Низкие требования к качеству линии WAN
  - Высокоскоростной доступ к частной линии между головным офисом и филиалами
  - Высокая стоимость частных линий SDH/MSTP/WDM
- Преимущества
  - VPN 3 уровня операторов изолированы, и предприятиям не нужно обращать внимание на развертывание маршрутов.
  - Гибкий взаимный доступ или контроль изоляции между объектами
  - Стоимость намного ниже, чем у неиспользуемых волокон оптического кабеля и частных линий SDH/MSTP/WDM.
- Недостатки
  - Услуга VPN оператора арендуется. Различные предприятия изолированы друг от друга на уровне 3. Оператор контролирует отношения взаимного доступа, и конфиденциальность зависит от оператора.
  - Предоставление QoS зависит от операторов.
- Ситуация
  - Практически все операторы могут предоставлять услуги частной линии MPLS VPN.
  - Количество частных линий MPLS VPN быстро увеличивается.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Развертывание и применение корпоративных сетей WAN

Построение сети DSVPN на базе сети Интернет





Высоконадежная сеть: частная линия SDH/MSTP/WDM + резервная оверлейная сеть VPN

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- На этой странице приведены абстрактные топологии WAN.

Сеть DSVPN на базе сети Интернет



- Сценарий применения
  - Большое количество филиалов. Требуется расширение.
  - Множество взаимодействий по сервисам между филиалами.
  - Низкие требования к качеству каналов
  - Требуется экономия затрат на эксплуатацию и обслуживание сети
- Характеристики решения
  - Обмен трафиком между головным офисом и филиалами осуществляется на основе интернет-решения DSVPN.
  - Филиалу не нужно иметь статический общедоступный IP-адрес.
  - Количество филиалов легко расширять, а сеть головного офиса легко развертывать.
- Ситуация
  - Корпоративные клиенты мало знают о DSVPN.
  - DSVPN становится все более широко используемой оверлейной технологией VPN.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Высоконадежная сеть: частная линия SDH/MSTP/WDM + резервная оверлейная сеть VPN



- Сценарий применения
  - Предприятия, которым требуются активные/резервные каналы
  - Предприятия, предъявляющие высокие требования к качеству основного канала с хорошей системой защиты конфиденциальности
  - Головной офис и филиалы могут иметь доступ к Интернету.
- Характеристики решения
  - Частная линия SDH/MSTP/WDM обеспечит высококачественный частный основной канал передачи данных. В дополнение к требованиями к доступу в Интернет, в качестве резервного канала используется оверлейный VPN-туннель на базе интернет-канала.
  - Оверлейной сеть VPN включает DSVPN, IPSec VPN и GRE VPN.
  - Такая комбинация обеспечивает полноценную работу сети на выгодных условиях.
- Ситуация
  - Широко используемое решение

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Содержание

1. Принципы проектирования корпоративных сетей
2. **Процесс проектирования корпоративных сетей**
   - Проектирование WAN
   - Выбор сетевых устройств
   - Планирование IP-адресов и наименование устройств
   - Планирование маршрутизации
   - PBR и политика маршрутизации
   - Подключение к сети Интернет
   - Планирование QoS

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Стандартные сетевые устройства

- К стандартным сетевым устройствам относятся маршрутизаторы, коммутаторы, концентраторы и межсетевые экраны.
- Выбор устройства здесь означает выбор типов, но не моделей устройств, например, маршрутизаторов, коммутаторов 2 уровня и коммутаторов 3 уровня.


Маршрутизатор


Коммутатор


Концентратор


Межсетевой экран

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Стандартные сетевые устройства
  - Коммутатор является основным устройством в локальной сети.
  - Маршрутизатор обеспечивает соединение WAN корпоративной сети и функционирует как граничное устройство.
  - Концентратор не используется.
  - Межсетевые экраны играют важную роль в пограничных областях сети предприятия и важных зонах.
  - Кроме того, существуют такие устройства, как LB и IPS, которые выполняют определенные функции, и их развертывание не связано с изменением топологии сети. Поэтому эти устройства здесь не описаны.
- Тенденция
  - Конвергенция маршрутизации и коммутации: коммутатор уровня 3 обеспечивает функцию маршрутизации, а коммутирующий маршрутизатор поддерживает модуль коммутации.
  - Интеграция функций VAS: все больше сетевых устройств поддерживают дополнительные функции, например функции межсетевых экранов. Например, маршрутизаторы Huawei AR G3 поддерживают функции межсетевого экрана, а коммутаторы S7700 поддерживают функции межсетевого экрана и контроллера доступа за счет плат.

Сравнение сетевых устройств

Устройство	Описание	Цена	Применение
Маршрутизатор	Это устройство 3 уровня, которое использует архитектуру ЦП, передает пакеты на основе таблицы маршрутизации и поддерживает различные типы интерфейсов.	Высокая	Граница WAN и LAN
Коммутатор 3 уровня	Это устройство уровня 2 или уровня 3. Трафик уровня 2 передается на основе таблицы MAC-адресов, а трафик уровня 3 передается на основе таблицы маршрутизации. Оно поддерживает только Ethernet.	Средняя	Уровень агрегации и уровень ядра LAN
Коммутатор 2 уровня	Это устройство уровня 2, которое передает пакеты на основе таблицы MAC-адресов. Оно поддерживает только Ethernet.	Низкая	Уровень доступа LAN
Межсетевой экран	Это устройство уровня 4, которое передает пакеты на основе таблиц сеансов. Оно может работать в режиме уровня 2 или уровня 3. Оно поддерживает только Ethernet.	Высокая	Граница сети и граница зоны сети

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Устройства выбираются на основе требований к обслуживанию с учетом функций и цены.
  - Коммутаторы 2 уровня используются на уровне доступа корпоративной сети.
  - Коммутаторы 3 уровня используются на уровне агрегации и уровне ядра.
  - Маршрутизаторы используются в сети WAN корпоративной сети.
  - Маршрутизатор или межсетевой экран используются на выходе корпоративной сети.

Модель сетевого устройства

Устройство	Описание	Применение	Пример
Фиксированные устройства	Тип и количество интерфейсов не изменяется. Как правило, размер устройств небольшой. Пользователи могут выбирать устройства разных моделей по мере необходимости.	Уровень доступа к сети Уровень ядра или уровень агрегации небольших сетей	Коммутаторы серии S3700
Модульные устройства	Устройство состоит из шасси и дополнительных модулей. Размер устройств большой. Пользователи могут выбирать модули (тип интерфейса, количество интерфейсов и поддерживаемые функции) в зависимости от требований объекта.	Уровень агрегации или уровень ядра	Коммутаторы серии S7700



Коммутаторы серии S3700



Коммутаторы серии S7700

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Устройства делятся на фиксированные и модульные.
  - В стек могут быть добавлены фиксированные устройства (например, коммутатор Huawei S5700) для увеличения пропускной способности интерфейса, упрощения управления и повышения надежности.
  - Модульные коммутаторы (например, коммутатор Huawei S9700) также могут использоваться в кластере с помощью CSS.
  - Модульные коммутаторы можно виртуализировать в несколько логических устройств через VS (например, коммутаторы Huawei CE12800).

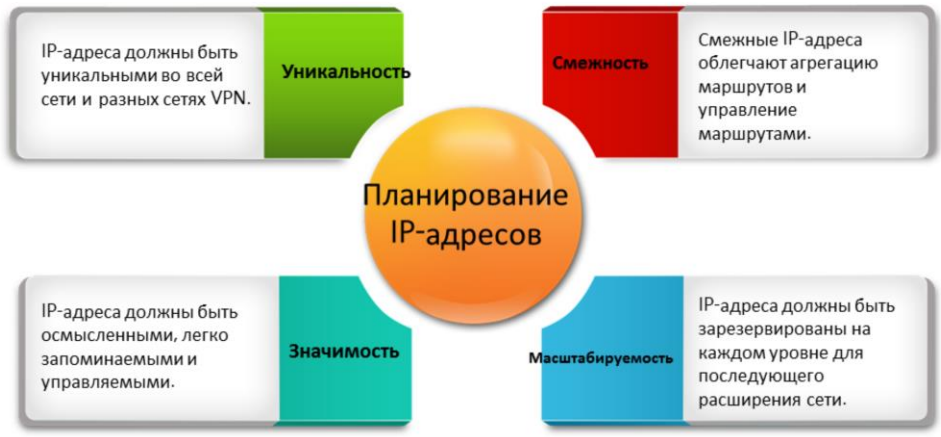
Содержание

1. Принципы проектирования корпоративных сетей
2. **Обзор процесса проектирования корпоративных сетей**
   - Выбор сетевых устройств
   - Планирование IP-адресов и наименование устройств
   - Планирование маршрутизации
   - PBR и политики маршрутизации
   - Подключение к сети Интернет
   - Планирование QoS
   - Развертывание системы сетевой безопасности

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Правила планирования IP-адресов



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Уникальность:
  - Хосты в IP-сети должны использовать уникальные IP-адреса. Выделите хостам разные IP-адреса, даже если они поддерживают совпадение адресов MPLS VPN.
- Смежность:
  - Маршруты со смежными IP-адресами легко объединять в иерархическую сеть. За счет этого уменьшается размер таблицы маршрутизации и ускоряется вычисление маршрута и сходимость маршрутов.
- Масштабируемость:
  - IP-адреса должны быть зарезервированы на каждом уровне, чтобы обеспечить наличие адресов при расширении сети.
- Значимость:
  - Хорошо спланированный IP-адрес обозначает роль устройства, которому он принадлежит. Планирование IP-адресов – это искусство. Идеальный способ – использовать формулу, а также соответствующие параметры и коэффициенты для расчета каждого IP-адреса.

Рекомендации по планированию важных IP-адресов



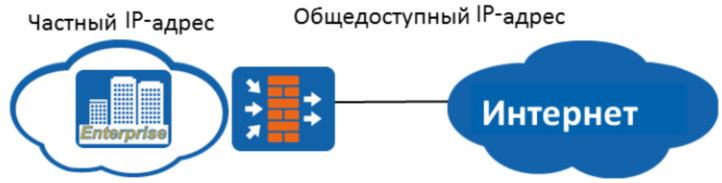
© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Как правило, при планировании IP-адресов используются стандартные типы IP-адресов, приведенные выше. Хотя обязательного стандарта нет, в отрасли существует ряд практик, описанных выше.

Общедоступные и частные IP-адреса

- В Интернете становится недостаточно общедоступных IP-адресов.
  - Доступные адреса IPv4 были распределены.
  - Предприятия должны платить за использование общедоступных IP-адресов.
- Частные IP-адреса могут использоваться случайным образом внутри предприятия.



Сервер NAT используется для предоставления сервисов для внешних устройств. Исходящий сервер NAT используется для того, чтобы предоставить пользователям внутренней сети доступ в Интернет.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Частный IP-адрес
  - Предприятие обычно использует частные IP-адреса, то есть адреса в сегментах сети 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16.
  - Хотя частные IP-адреса могут использоваться случайным образом, они должны быть запланированы.
- Общедоступный IP-адрес
  - Если предприятие не предоставляет услуги внешним устройствам, но нуждается в доступе к Интернету, оно может использовать динамический общедоступный IP-адрес, выделенный оператором.
  - Если предприятие предоставляет услуги внешним устройствам (например, собственный сервис WWW), предприятие должно подать заявку на получение фиксированных общедоступных IP-адресов.
  - Фиксированные общедоступные IP-адреса стоят дорого. Для экономии затрат может использоваться технология сервера NAT для использования одного общедоступного IP-адреса для предоставления нескольких услуг.
  - В долгосрочной перспективе в IT-системе предприятия должен быть учтен переход с IPv4 на IPv6.

Наименование устройств

- Наименование устройств облегчает управление сетью.
- Наименование устройства включает в себя следующее:
  - Имя устройств (sysname)
  - Идентификаторы логических интерфейсов, VLAN и ACL
  - Описание интерфейсов, VLAN и ACL

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Имя устройства включает в себя имя устройства, описание конфигурации, а также идентификаторы интерфейсов и VLAN.
- Наименование устройства кажется неважным. На самом деле, это важно для работы и обслуживания сети. Использование правил наименования устройств значительно повышает эффективность управления сетью.
- Предприятие должно установить свои собственные правила наименования устройств и строго соблюдать их.

Наименование устройств

- Наименование устройств не влияет на работу устройств.
- Предприятия должны использовать единые спецификации для наименования устройств, чтобы облегчить управление сетью.
- A-B-C-D-E, например: HQ-CS-HW-S7706-1
  - A: географическое местоположение устройства. Например, HQ означает, что устройство находится в головном офисе предприятия.
  - B: расположение устройства в логической сети. Например, CS указывает, что устройство является основным коммутатором.
  - C: производитель устройства. Например, HW указывает, что производителем устройства является компания Huawei.
  - D: модель устройства, например, S7706.
  - E: Идентификатор устройства, например, 1 или 2.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Для наименования сетевых устройств не существует отраслевых стандартов и правил.
- Предприятия могут определять правила наименования на основании требований к обслуживанию.

Нумерация логических конфигураций

Конфигурация	Рекомендация	Пример
Субинтерфейсы Ethernet	Номер субинтерфейса аналогичен идентификатору VLAN.	Ethernet 0/0/1.10 привязан к VLAN 10.
Интерфейс группы MP	Первые две цифры в идентификаторе интерфейса группы MP указывают на идентификатор слота и идентификатор дополнительной платы. Последние две цифры в идентификаторе интерфейса группы MP одинаковы для двух устройств в группе MP.	–
Идентификатор VLAN	Идентификаторы VLAN должны планироваться и использоваться по сегментам.	VLAN 10 – VLAN 100 используются для сетевого соединения. VLAN 101 – VLAN 200 используются для производственных услуг.
Номер ACL	Используйте имена ACL. Номера ACL должны планироваться и использоваться по сегментам.	ACL 3000–3100 используются для политик маршрутизации. ACL 3101–3200 используются для фильтрации пакетов.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Нумерация логических конфигураций устройства не влияет на работу устройства. Использование правил упорядоченной нумерации облегчает управление сетью.

Добавление описания конфигурации

Конфигурация	Рекомендация	Пример
Интерфейс	Опишите интерфейс, подключенный к соседнему устройству, с помощью имени и номера порта соседнего устройства.	Интерфейс, подключенный к GE1/0/1 базового коммутатора 1 в головном офисе: To_HQ-CS-HW-S7706-1_GE1/0/1
Идентификатор VLAN	Опишите VLAN на основе услуг, оказываемых с помощью VLAN.	VLAN используется для офисных услуг отдела маркетинга: MKT-OA Интерфейс VLANIF, используемый для соединения устройств на уровне 3 (описывается на основе локального интерфейса, соседнего устройства и соседнего интерфейса): Ge0/0/1_to_HQ-CS-HW-S7706-1_GE1/0/1
Номер ACL	Опишите использование ACL.	ACL используется для политики маршрутизации **rp1**: For_RP_rp1

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Описания конфигурации не участвуют ни в каких процессах вычисления протокола. Описания значительно улучшают читаемость конфигураций устройств и позволяют новым сетевым администраторам быстро ознакомиться с конфигурациями устройств.

Содержание

1. Принципы проектирования корпоративных сетей
2. **Процесс проектирования корпоративных сетей**
   - Планирование IP-адресов и наименование устройств
   - Планирование маршрутизации
     - PBR и политика маршрутизации
     - Подключение к сети Интернет
     - Планирование QoS
     - Развертывание системы сетевой безопасности
     - Планирование сетевого управления

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Протоколы маршрутизации

Протокол маршрутизации	Алгоритм	Скорость конвергенции	Развертывание	Сценарий применения
Прямой маршрут	Генерируется протоколами канального уровня	–	–	По умолчанию
Статический маршрут	Настраивается администраторами вручную	–	Простое	Небольшая сеть (менее 3 маршрутизаторов) Дополнение к протоколам динамической маршрутизации
OSPF	Алгоритм состояния канала. Стоимость маршрута измеряется на основе пропускной способности.	Быстрая	Довольно простое	Сети среднего и крупного размера (сотни маршрутизаторов)
IS-IS	Алгоритм состояния канала. Стоимость маршрутов измеряется на основе нескольких параметров, таких как пропускная способность и задержка.	Очень быстрая	Довольно простое	Сети среднего и крупного размера (сотни маршрутизаторов)
BGP	Алгоритм вектора пути. Стоимость маршрутов измеряется на основе нескольких атрибутов маршрута.	Средняя	Довольно простое	Сверхкрупная сеть (более 1000 маршрутизаторов) BGP MPLS VPN

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- В дополнение к прямым и статическим маршрутам большинство предприятий используют протокол IGP.
  - Из-за проблем с эффективностью и масштабом сети лишь немногие предприятия используют протокол RIP.
  - В области корпоративных сетей все больше сетевых инженеров использует протокол OSPF.
  - Поэтому большинство предприятий используют протокол OSPF в качестве IGP.
- Некоторые предприятия используют BGP в следующих ситуациях:
  - Протокол IGP не может обрабатывать все маршруты в крупной сети.
  - Сеть должна использовать большое количество сложных политик маршрутизации.
  - Развернута сеть MPLS VPN.
- В сложной сетевой среде может использоваться несколько протоколов маршрутизации.

Планирование статического маршрута

- Статическая маршрутизация является обязательным режимом маршрутизации для корпоративных сетей. Как правило, стандартные статические маршруты:
  - Применяются на выходе корпоративной сети
  - Используются устройствами, которые не поддерживают протоколы динамической маршрутизации
  - Используются для простого соединения разных сетей



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Статическая маршрутизация является самым простым режимом маршрутизации, но ее также необходимо планировать при использовании статических маршрутов.
  - Как правило, в корпоративных сетях следует избегать использования статических маршрутов. В обычных случаях устройства узнают требуемые маршруты, используя протоколы динамической маршрутизации. Настроенные статические маршруты не являются предпочтительными, но мешают устранению неполадок.
  - Стандартные статические маршруты в основном используется на выходе корпоративной сети. Они анонсируются во внутренней сети через протокол динамической маршрутизации.
  - Некоторые устройства младших моделей не поддерживают протоколы динамической маршрутизации, но устройства, которыми может управлять NMS, обычно поддерживают статические маршруты.
  - Динамическая маршрутизация рекомендуется для простого сетевого соединения.
  - Статические маршруты не реагируют на изменения в сети. Можно использовать BFD и NQA для связывания статических маршрутов с интерфейсами и каналами, чтобы статические маршруты могли реагировать на изменения в сети.

Протоколы OSPF и ISIS

- Сходства
  - OSPF и IS-IS основаны на алгоритме состояния канала.
  - OSPF и IS-IS поддерживают быструю конвергенцию маршрутов.
  - OSPF и IS-IS могут быть развернуты в крупных сетях.
- Отличия
  - IS-IS обладает более высокой масштабируемостью для поддержки IPv6.
  - Инженеры корпоративных сетей лучше знают протокол OSPF.
- Заключение
  - Протоколы OSPF и IS-IS являются популярными протоколами IGP.
  - Рекомендуется использовать протокол OSPF в корпоративных сетях.
  - Рекомендуется использовать протокол IS-IS тогда, когда IPv4 и IPv6 развертываются одновременно.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- OSPF и IS-IS используют схожие алгоритмы и обеспечивают одинаковую производительность.
- По разным причинам все больше предприятий внедряют OSPF, и многие инженеры, специализирующиеся на корпоративных сетях, лучше знакомы с OSPF.
  - На рынке операторских сетей все больше клиентов используют IS-IS.

Планирование внедрения протокола BGP

- Когда рекомендуется использовать протокол BGP для предприятий?
  - Масштаб сети большой, и протокол IGP не может обрабатывать маршруты.
  - Для распределения и фильтрации трафика в сети требуется большое количество сложных политик маршрутизации.
  - В сети необходимо развернуть MPLS VPN.
- На каких устройствах может использоваться протокол BGP?
  - BGP не генерирует маршруты, но управляет маршрутами и анонсирует их.
  - BGP не потребляет большое количество ресурсов устройства.
  - При правильном планировании все устройства могут работать с BGP.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Как правило, крупные предприятия используют протокол BGP. При необходимости любое предприятие может использовать протокол BGP.
- В отличие от IGP, BGP не генерирует маршруты, но управляет маршрутами и анонсирует их. Поэтому BGP не требует использования устройств с высокой производительностью. Следовательно, BGP может работать на любом устройстве при условии правильного планирования.

Содержание

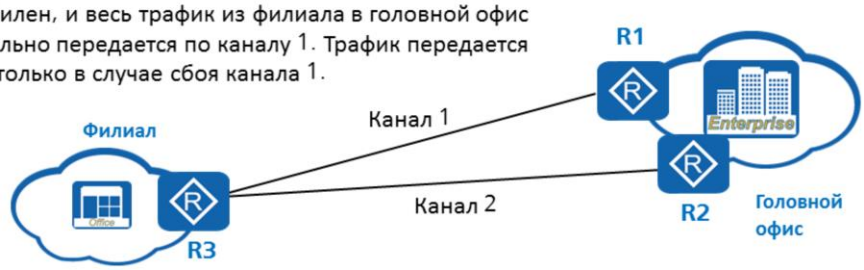
1. Принципы проектирования корпоративных сетей
2. **Процесс проектирования корпоративных сетей**
   - Планирование IP-адресов и наименование устройств
   - Планирование маршрутизации
   - PBR и политика маршрутизации
   - Подключение к сети Интернет
   - Планирование QoS
   - Развертывание системы сетевой безопасности
   - Планирование сетевого управления

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Пример планирования политики маршрутизации

Требование:
Канал 1 стабилен, и весь трафик из филиала в головной офис предпочтительно передается по каналу 1. Трафик передается по каналу 2 только в случае сбоя канала 1.



- Политики маршрутизации влияют на вычисление маршрутов и, следовательно, изменяют таблицу маршрутизации.
  - Общая политика маршрутизации состоит в том, чтобы отфильтровать маршруты, которые не анонсируются. Значения метрик маршрутов могут быть скорректированы для изменения последовательности выбора маршрута.
  - В протоколах маршрутизации используются разные инструменты политики маршрутизации.
  - Политика маршрутизации должна рассматриваться глобально.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Для удовлетворения вышеупомянутого требования необходимо выполнить планирование следующим образом:
  - Предположим, что R1, R2 и R3 находятся в одной области OSPF.
  - Отрегулируйте стоимость канала 2 между R2 и R3 до большего значения.
  - Тогда OSPF будет предпочитать канал 1 с более низкой стоимостью.

Пример планирования PBR

Требование:
Весь HTTP-трафик из филиала предприятия поступает в головной офис по каналу 1, а другой трафик поступает в головной офис по каналу 2. В случае сбоя одного из каналов трафик переключается на другой канал.



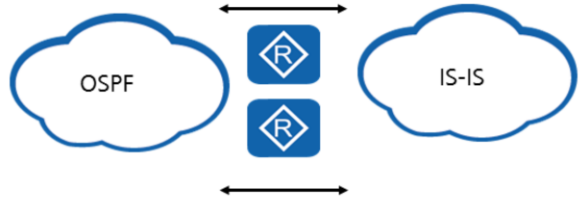
- Механизм PBR напрямую применяется к плоскостям передачи устройств, но не влияет на таблицу маршрутизации.
  - Обычный механизм PBR предназначен для изменения следующего узла для передачи данных.
  - Основывается на разных адресах источников
  - Основывается на других условиях

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Для удовлетворения вышеупомянутого требования необходимо выполнить планирование следующим образом:
  - Настройте значение стоимости (политику маршрутизации), чтобы весь трафик филиалов предприятия поступал в головной офис по каналу 2.
  - Настройте PBR на R3. Определите HTTP-трафик (номер порта TCP = 80) и укажите R1 в качестве следующего узла для HTTP-трафика.
  - Используйте аналогичную политику на R1 и R2, чтобы разрешить передачу трафика HTTP на R3 по каналу 1.

Политика импорта маршрутов



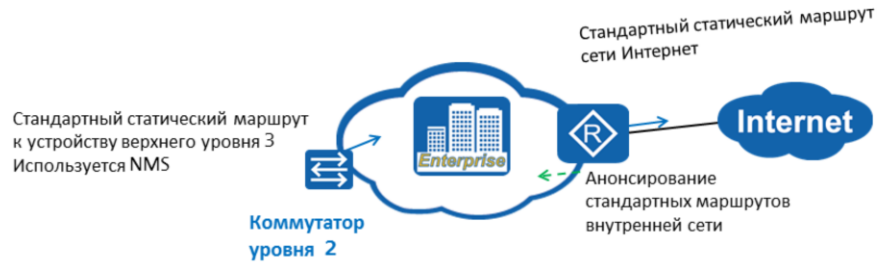
- Ключевые особенности импорта маршрутов
  - Перед импортом маршрутов добавьте политику управления маршрутизацией, чтобы предотвратить импорт всех маршрутов.
  - Стандартный маршрут не может быть импортирован и должен быть анонсирован в специальном режиме.
  - Когда два протокола динамической маршрутизации на двух устройствах импортируют маршруты друг от друга, могут возникнуть петли маршрутизации.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- В сети статические и прямые маршруты импортируются для анонсирования статических и прямых маршрутов.
  - Как правило, стандартные статические маршруты не могут быть импортированы протоколами динамической маршрутизации.
  - Для стандартных протоколов динамической маршрутизации доступны специальные команды для импорта и анонсирования стандартных маршрутов.
  - Если политика маршрутизации не настроена, все маршруты одного типа импортируются по умолчанию при импорте стандартных маршрутов. В результате возникают некоторые проблемы, например петли маршрутизации.
  - Когда два протокола динамической маршрутизации импортируют маршруты друг к другу, существует более высокая вероятность возникновения петель маршрутизации.
  - Поэтому перед импортом маршрутов необходимо добавить политику маршрутизации, чтобы отфильтровать маршруты, которые не нужно анонсировать, или добавить некоторые идентификаторы (например, теги) для облегчения последующего управления маршрутами.

Использование стандартных маршрутов



- Стандартные маршруты играют важную роль в сети.
  - Настройте стандартный статический маршрут на выходе из сети.
  - Анонсируйте стандартный статический маршрут во внутреннюю сеть через протокол динамической маршрутизации.
  - Не рекомендуется настраивать стандартные статические маршруты в корпоративной внутренней сети (кроме устройств уровня 2).

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

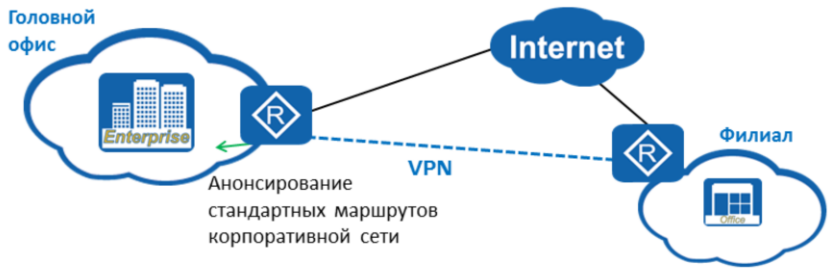
- Не рекомендуется использовать стандартные статические маршруты во внутренней сети.
  - Во внутренней сети предприятия существуют только маршруты, полученные с помощью протоколов динамической маршрутизации (включая стандартные маршруты).
  - Если во внутренней сети настроены стандартные статические маршруты, в ней могут возникнуть петли маршрутизации, и ошибки не будут обнаружены. (Почему?)
  - Стандартные статические маршруты могут использоваться для временных чрезвычайных ситуаций. В особых случаях, например, при сбое протоколов динамической маршрутизации, вы можете настроить такие маршруты.

Содержание

1. Принципы проектирования корпоративных сетей
2. **Процесс проектирования корпоративных сетей**
   - Планирование IP-адресов и наименование устройств
   - Планирование маршрутизации
   - PBR и политики маршрутизации
   - Подключение к сети Интернет
   - Планирование QoS
   - Развертывание системы сетевой безопасности
   - Планирование сетевого управления

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Корпоративная сеть и сеть Интернет



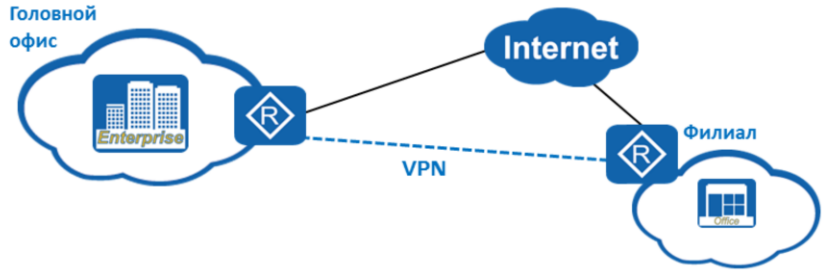
- Почти все корпоративные сети подключены к Интернету.
  - Корпоративные пользователи должны иметь доступ к Интернету.
  - Предприятия предоставляют услуги доступа в Интернет (такие как веб-услуги и услуги электронной почты).
  - Корпоративные филиалы настраивают VPN для подключения к головному офису через Интернет.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- В настоящее время немногие корпоративные сети не имеют подключения к Интернету (за исключением конфиденциальных сетей).
- Корпоративным пользователям необходим доступ в Интернет, предприятиям необходимо предоставлять доступ в Интернет, и корпоративным VPN-сетям также необходимо подключаться к Интернету.
- Проектирование выхода в Интернет корпоративных сетей также очень важно.
- Корпоративная внутренняя сеть должна распознавать только маршруты, направленные к выходным устройствам, но не должна распознавать конкретные маршруты, направленные в Интернет.

Устройство выхода в Интернет

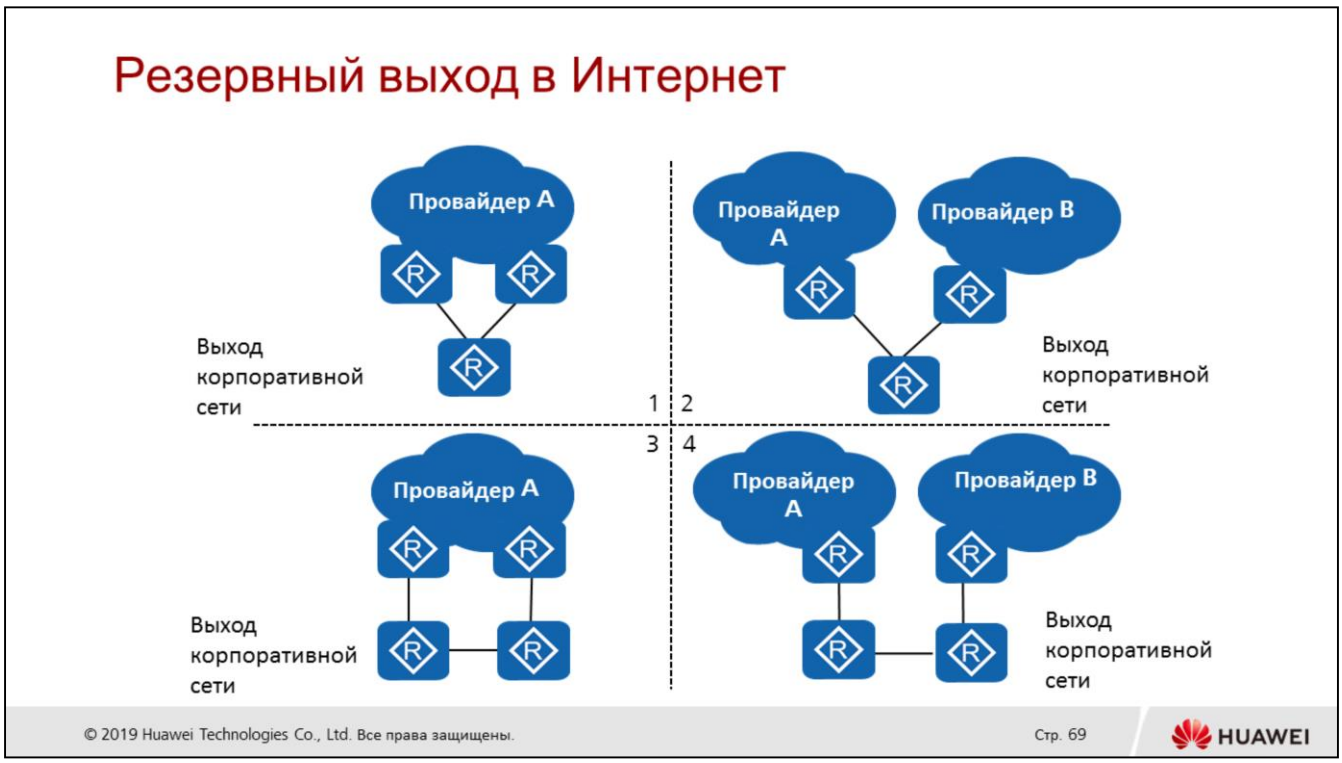


- Устройства корпоративных сетей для выхода в Интернет должны поддерживать следующие функции:
  - Функции NAT и сервера NAT
  - Функция маршрутизации (соединение с провайдерами)
  - Функции обеспечения безопасности (защита от атак и VPN)

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

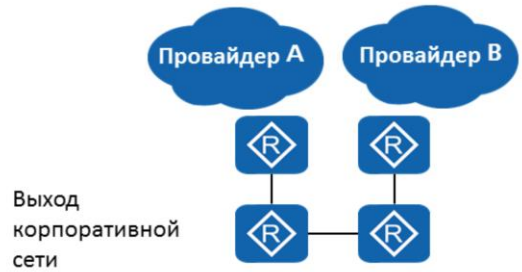
HUAWEI

- В качестве выходного устройства корпоративной сети может выступать высокопроизводительный маршрутизатор, прозрачный межсетевой экран или межсетевой экран, поддерживающий функцию маршрутизации.
- Устройства VPN могут быть маршрутизаторами или межсетевыми экранами, а также могут быть внедрены отдельно.
  - Многие маршрутизаторы или межсетевые экраны поддерживают функцию VPN.
  - Если на предприятии имеется большое количество филиалов или пользователей VPN, рекомендуется использовать специальные устройства VPN.



- Выходные интернет-соединения являются критически важными для корпоративных сетей. Следовательно, при проектировании выхода в Интернет необходимо учитывать резервные выходы.
  - В решении 1 резервируются выходные каналы.
  - В решении 2 резервируются выходные каналы и провайдеры.
  - В решении 3 резервируются выходные устройства и выходные каналы.
  - В решении 4 резервируются выходные устройства, выходные каналы и провайдеры.
- Предприятия должны выбирать подходящие решения для резервирования выхода в Интернет на основе требований к надежности обслуживания и бюджета.

Несколько выходов в Интернет



- При развертывании нескольких выходов в Интернет следует определить:
  - Исходящий интерфейс трафика доступа в Интернет, отправляемого пользователями внутренней сети
  - Входящий интерфейс трафика, отправляемого пользователями внешней сети для доступа к внутренним серверам

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Определение исходящего интерфейса трафика доступа в Интернет, отправляемого пользователями интрасети:
  - Использование протокола BGP между корпоративными сетями и сетями провайдера является оптимальным способом. Однако протоколы динамической маршрутизации не работают между сетями провайдеров и корпоративными сетями.
  - При использовании одного провайдера предприятия могут настроить статические выходные маршруты на выходных маршрутизаторах для решения проблемы.
  - Когда существует несколько выходов, предприятиям необходимо настроить конкретные статические маршруты на основе сегментов Интернета, охватываемых различными провайдерами, и анонсировать эти статические маршруты, по крайней мере, между выходными маршрутизаторами.
  - Таким образом, корпоративные пользователи получают более высокие скорости доступа в Интернет, и обеспечивается резервирование каналов.
- Определение входящего интерфейса трафика, отправляемого пользователями внешней сети для доступа к внутренним серверам
  - На самом деле эта проблема не может быть решена на уровне сети. Если предприятие объявляет только один общедоступный IP-адрес, внешние пользователи могут получить доступ к внутренним серверам только через интерфейс, с которого объявляется общедоступный IP-адрес.
  - Эта проблема может быть решена на прикладном уровне. Обычно пользователи используют доменные имена вместо IP-адресов для доступа к интернет-сервисам. Корпоративная сеть может использовать два общедоступных IP-адреса для предоставления интернет-услуг и связывать общедоступные IP-адреса с одним доменным именем. Вы можете установить некоторые параметры на DNS-сервере, чтобы запросы доменного имени, отправленные из разных сетей, могли получать разные IP-адреса.



Содержание

1. Принципы проектирования корпоративных сетей
2. **Процесс проектирования корпоративных сетей**
   - Планирование IP-адресов и наименование устройств
   - Планирование маршрутизации
   - PBR и политика маршрутизации
   - Подключение к сети Интернет
   - Планирование QoS
   - Развертывание системы сетевой безопасности
   - Планирование сетевого управления

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Анализ требований QoS

- Политики QoS должны разрабатываться и применяться на основе прикладных требований.
- Области применения для предприятий сильно различаются. Данные обычно подразделяются на следующие типы:
  - Аудио
  - Видео
  - Офис
  - Информация управления сетью
  - Прочее

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Далее мы проанализируем различные типы данных.

Развертывание технологии QoS



- При развертывании приложений в сети WAN соблюдайте осторожность из-за небольшой пропускной способности и высокой стоимости.
- Учитывайте приоритет обслуживания при разработке политик QoS.
- Скорость интерфейса WAN может отличаться от фактической пропускной способности канала WAN.

- Типы данных определены и отмечены на границе сети.
- Можно настраивать простые политики QoS, если в сетях LAN редко происходит перегрузка.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- К разным данным добавляются различные теги. Затем устройства применяют различные политики QoS к данным в соответствии с тегами.

Содержание

1. Принципы проектирования корпоративных сетей
2. **Процесс проектирования корпоративных сетей**
   - Планирование IP-адресов и наименование устройств
   - Планирование маршрутизации
   - PBR и маршрутизации
   - Подключение к сети Интернет
   - Планирование QoS
   - Развертывание сетевой безопасности
   - Планирование сетевого управления

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Угрозы сетевой безопасности



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Сети находятся под влиянием различных угроз, таких как кабельное соединение, идентификация личности и угрозы уязвимости системы. Понятие сетевой безопасности применяется к любому объекту в сети, который может быть подвержен атаке или использован для атаки на других. В системе не существует абсолютной безопасности. Поэтому вам необходимо оценить риски и найти уязвимости для улучшения безопасности.
- IP-сети в основном строятся на основе стека протоколов TCP/IP. Поэтому наш анализ также основан на стеке протоколов TCP/IP.

Возможности безопасности

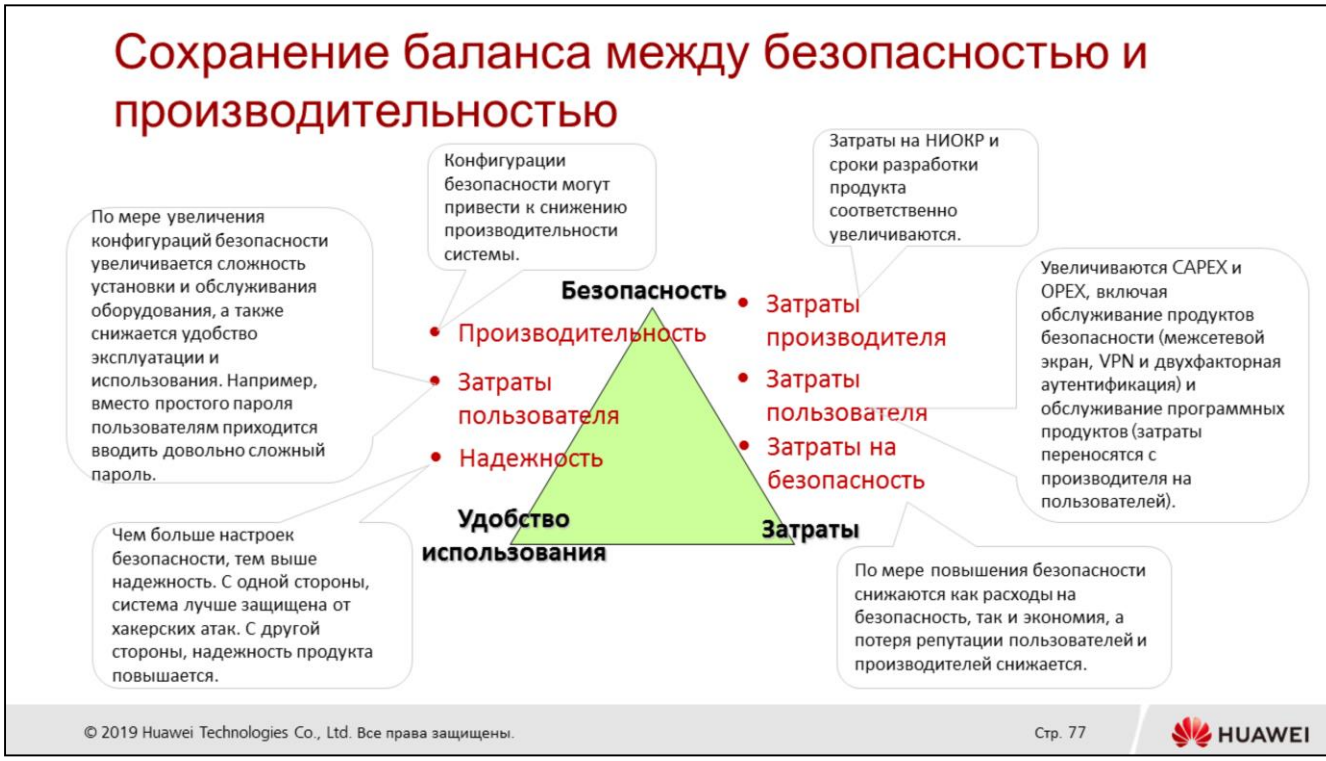


© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Проблемы безопасности неизбежно затрагивают людей. Если мы поместим секретные объекты на Марс, они будут в полной безопасности. В текущей среде средства управления безопасностью особенно важны, потому что вся информация обрабатывается людьми. Если в отношении лиц, которые могут получить доступ к информации, не применяется строгая политика управления безопасностью, любая технология становится неэффективной. При поддержке стратегий и политик управления безопасностью можно использовать соответствующие технические средства для расширения возможностей обеспечения безопасности. Средства безопасности подразделяются на шесть типов:

- Защита, обнаружение, реагирование, восстановление, контратака и предупреждение. Эти средства также называются PDRRCW.
- В настоящее время защита, обнаружение, реагирование, восстановление (PDRR) применяются более широко и фокусируются на пассивной защите от атак. Средства PDRRCW включают в себя еще два элемента, «Контратака» и «Предупреждение», и в некоторой степени предоставляют более мощные средства обеспечения безопасности.



- Безопасность, удобство использования и затраты образуют треугольник. По мере повышения безопасности снижается удобство использования системы и увеличиваются затраты на обслуживание. Однако, если безопасность не улучшена, могут возникнуть проблемы с безопасностью, что приведет к дополнительным затратам.
- Гарантия безопасности – трудоемкая и ресурсоемкая задача. Чтобы обеспечить безопасные услуги оптимального качества, вы должны соблюдать баланс между безопасностью, удобством использования и затратами.

Иерархическая комплексная структура обеспечения безопасность



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- NAC: контроль доступа к сети
  - Проверяет личность пользователей и контролирует права доступа к сети, тем самым защищая безопасность корпоративной сети.
  - Следит за трафиком в сети, предотвращая атаки через посредника
  - Использует методы защиты от внешних сетевых атак для обеспечения безопасности доступа внешних пользователей и осуществления безопасной и надежной передачи данных.



Содержание

1. Принципы проектирования корпоративных сетей
2. **Процесс проектирования корпоративных сетей**
   - Планирование IP-адресов и наименование устройств
   - Проектирование маршрутизации
   - Политика PBR и маршрутизации
   - Подключение к сети Интернет
   - Проектирование QoS
   - Развертывание сетевой безопасности
   - Планирование сетевого управления

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Общие режимы управления сетью

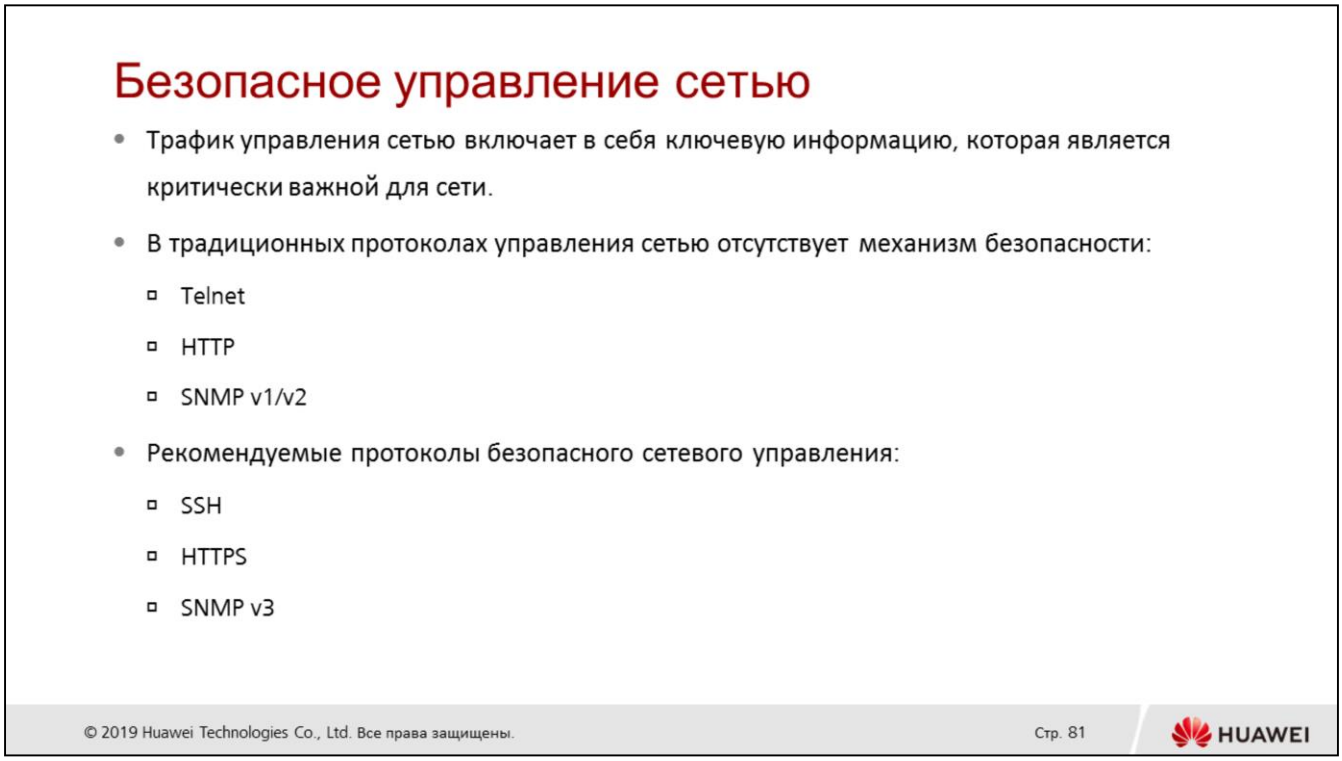
- Для управления сетью используется несколько режимов.

Режим	Описание	Применение
CLI	• Управляет отдельными устройствами посредством командных строк. • Отсутствует возможность управления всей сетью. • Требуется, чтобы администратор был знаком с командной строкой. • Обеспечивает высокую эффективность, но не прост в использовании.	• Начальная конфигурация устройства • Сложная конфигурация • Решение сложных проблем
Веб	• Управляет отдельными устройствами на веб-странице. • Отсутствует возможность управления всей сетью. • Прост в использовании и применим для простых и многократных конфигураций.	• Наблюдение за состоянием устройства • Простая конфигурация
SNMP	• Управляет устройствами во всей сети посредством SNMP. • Управляет сетевыми устройствами, каналами и даже услугами. • Предоставляет графический интерфейс пользователя (GUI) и прост в освоении и использовании. • Отсутствует возможность решения некоторых сложных проблем.	• Управление сетевыми устройствами, каналами и услугами • Используется с CLI и веб-режимами

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

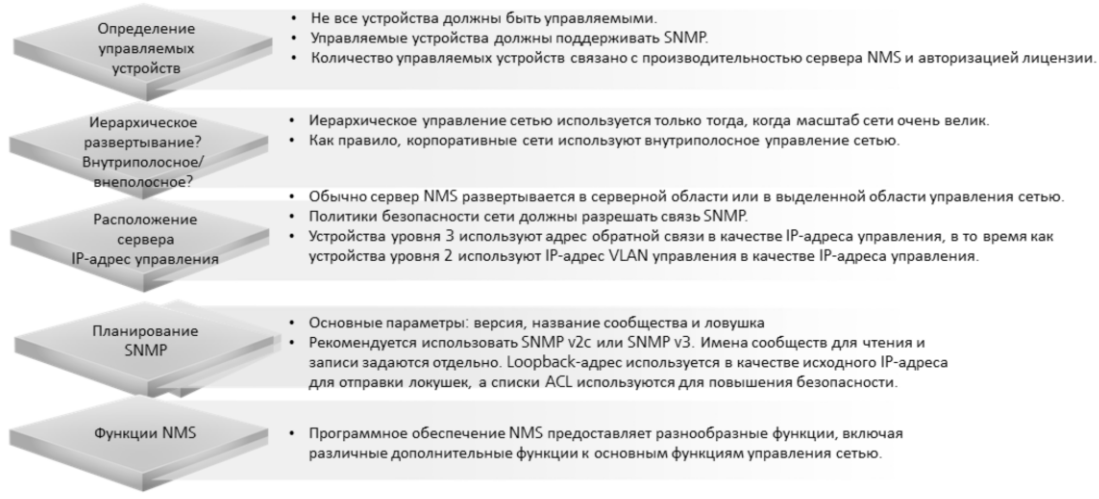
HUAWEI

- CLI и веб-режимы являются режимами управления на основе устройств.
  - Некоторые устройства предоставляют только один из этх режимов, а некоторые – оба.
  - Как для CLI, так и для веб-управления, команды или страницы операций для устройств разных производителей или устройств разных моделей от одного поставщика могут отличаться.
- SNMP – это стандартный протокол управления сетью.
  - Большинство сетевых устройств поддерживают SNMP.
  - SNMP управляет различными устройствами одинаково.



- Трафик управления сетью включает в себя ключевую информацию, которая является критически важной для сети.
  - Пароль администратора приведен в качестве примера.
- Ввиду специальных целей и ограничений ранних сетей многие протоколы управления передают данные в виде открытого текста, что не может обеспечить безопасность. С проникновением сетей в различные области деятельности безопасность сети становится все более важной. Традиционные протоколы управления, которые передают данные в виде открытого текста, не могут отвечать требованиям безопасности. Поэтому разработаны протоколы управления, которые передают данные в зашифрованном виде:
  - Telnet -> SSH
  - HTTP -> HTTPS
  - SNMP v1/v2 -> SNMP v3

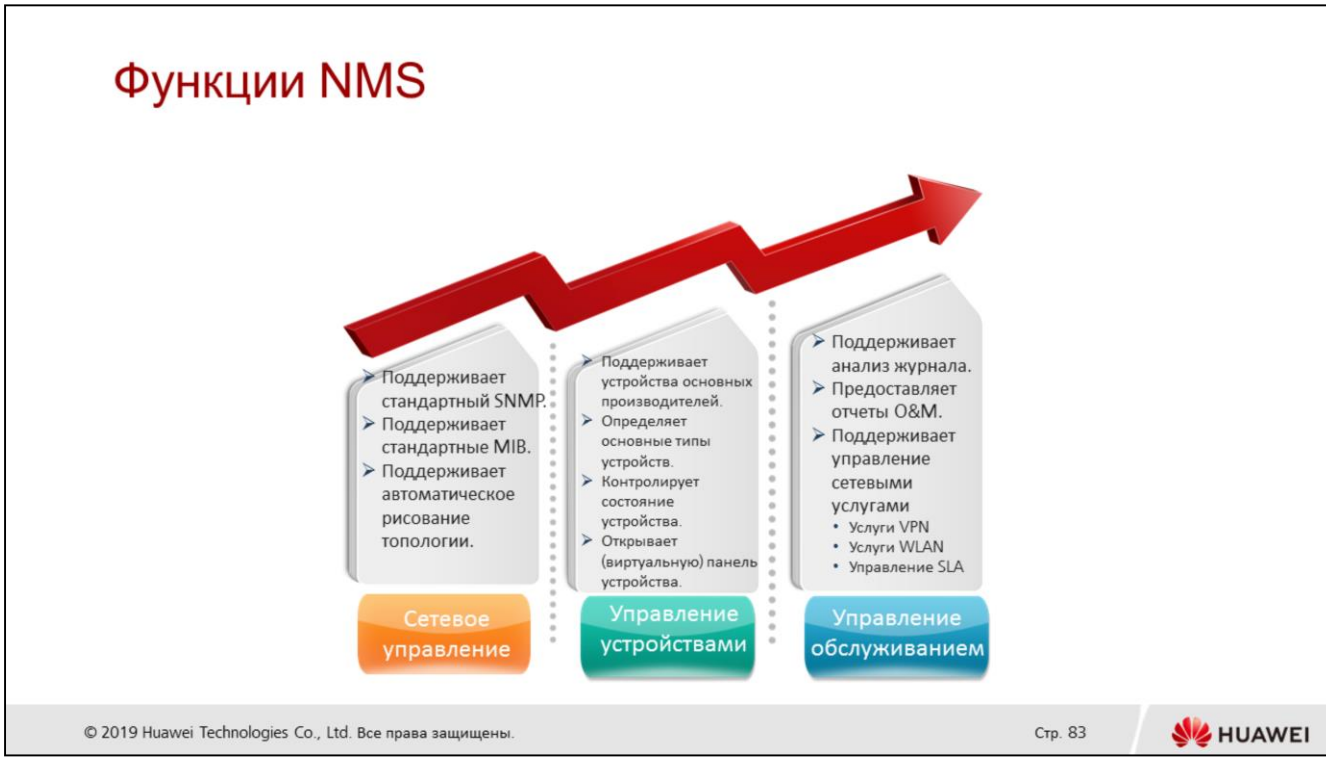
Планирование NMS



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- NMS: система сетевого управления
  - Программное обеспечение является основным компонентом NMS.
  - С развитием технологий функции программного обеспечения NMS изменились с простого управления сетью на управление полным спектром услуг ИКТ.



- Сетевое управление
  - Управление сетью является основной функцией NMS.
  - NMS должна поддерживать стандартные SNMP и стандартные MIB.
  - NMS может автоматически обнаруживать и рисовать топологии сети.
- Управление устройствами
  - Управление устройством – удобная функция для пользователей. Однако, управление устройствами от разных поставщиков предъявляет более высокие требования к NMS.
  - NMS должна быть в состоянии идентифицировать основные типы устройств основных поставщиков.
  - NMS может отслеживать состояние этих устройств.
  - NMS может открывать (виртуальные) панели этих устройств.
- Управление обслуживанием
  - Являясь сетевым инструментом O&M, NMS должна уметь анализировать журналы и генерировать отчеты.
  - Кроме того, NMS должна иметь возможность управлять сетевыми службами, такими как VPN, WLAN и SLA.

Содержание

1. Принципы проектирования корпоративных сетей
2. Процесс проектирования корпоративных сетей
3. **Выбор продукта**
   - Как выбирать продукты
   - Маршрутизаторы серии AR G3
   - Коммутаторы серии Sx700
   - Другие продукты
4. Проектирование корпоративной сети на примерах

© 2019 Huawei Technologies Co., Ltd. Все права защищены.



- Примите во внимание все возможные факторы, такие как технология, цена и обслуживание, чтобы выбрать наиболее подходящий продукт, а не лучший.
  - Удовлетворение требований к обслуживанию по-прежнему является основным фактором при выборе устройства.
  - Исходя из требований обслуживания, выбирайте продукты с передовыми технологиями, отличным сервисом и разумными ценами.

Содержание

1. Принципы проектирования корпоративных сетей
2. Процесс проектирования корпоративных сетей
3. **Выбор продукта**
   - Как выбирать продукты
   - Маршрутизаторы серии AR G3
   - Коммутаторы серии Sx700
   - Другие продукты
4. Проектирование корпоративной сети на примерах

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

VRP Huawei

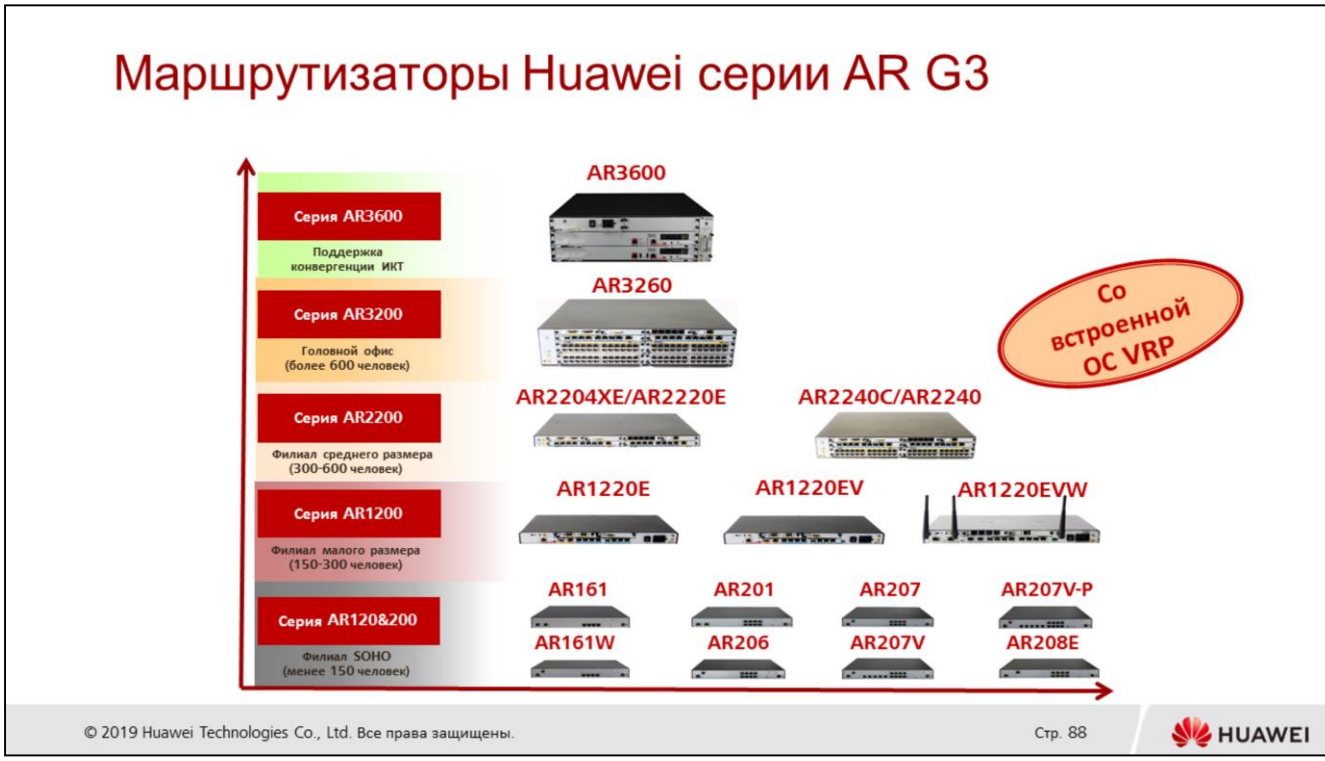


Универсальная платформа маршрутизации (VRP)

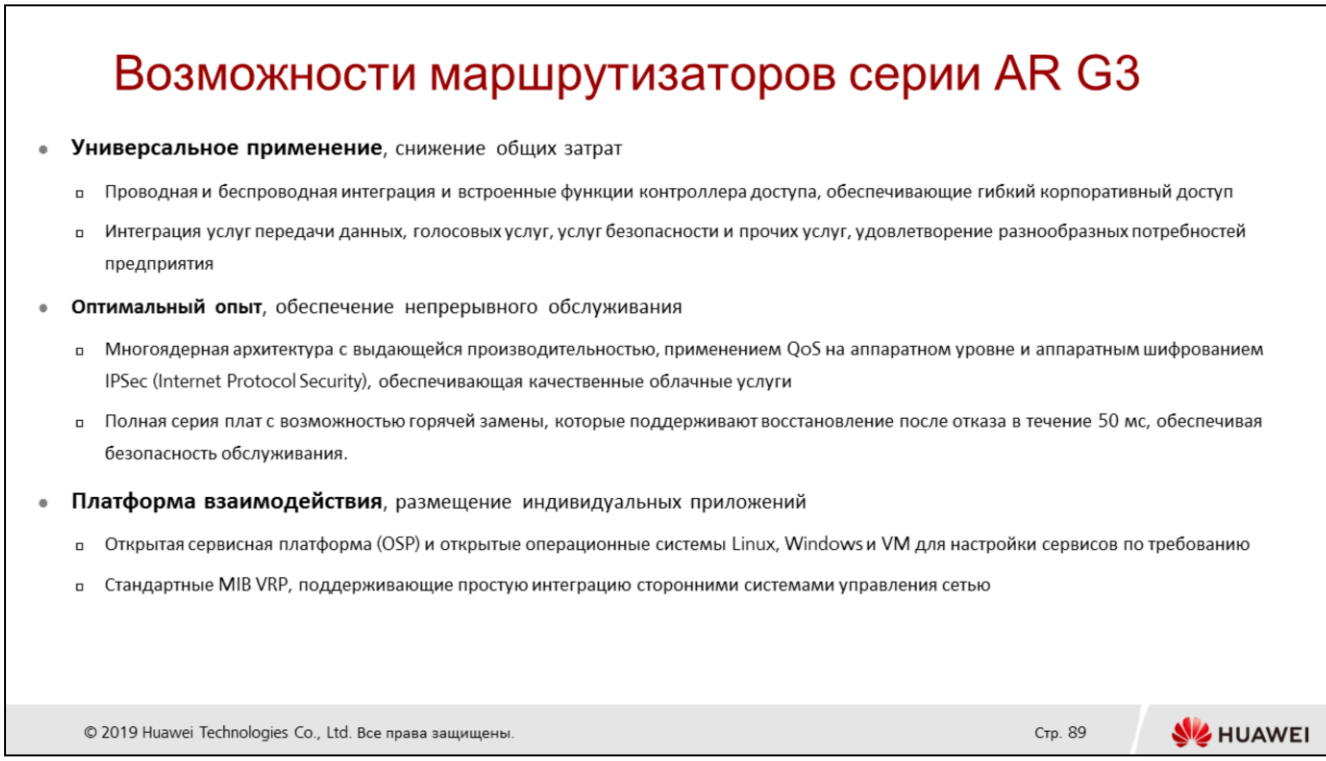
© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- VRP – это сетевая операционная система, используемая устройствами передачи данных Huawei. Сетевая операционная система – это системное программное обеспечение, которое работает на определенных устройствах и обеспечивает доступ к сети и услуги взаимодействия. VRP является базовым механизмом маршрутизаторов Huawei, коммутаторов Ethernet и сервисных шлюзов. Он обеспечивает унифицированный пользовательский интерфейс и интерфейс управления, реализует функции плоскости управления и определяет спецификации интерфейса плоскости пересылки для реализации взаимодействия между плоскостью пересылки каждого продукта и плоскостью управления VRP. Он также реализует уровень сетевого интерфейса, чтобы скрыть различия между канальным уровнем каждого продукта и сетевым уровнем.



- Маршрутизаторы серии AR G3 – это маршрутизаторы корпоративного класса следующего поколения на основе Huawei VRP. Компания Huawei разработала маршрутизаторы серии AR G3 с использованием технологий, накопленных в областях передачи данных, беспроводной связи, сети доступа и опорной сети. Маршрутизаторы AR G3 объединяют функции маршрутизации, коммутации, WLAN, 3G/LTE, голосовой связи и безопасности. Они используют многоядерный ЦП и неблокирующую коммутационную структуру и обеспечивают лучшую в отрасли производительность и расширяемость системы, удовлетворяя разнообразные требования разработки приложений предприятий в будущем. Эти маршрутизаторы предоставляют интегрированное решение для корпоративных сетей, ускоряют предоставление мультисервисных услуг и защищают инвестиции клиентов.



- Корпоративные маршрутизаторы серии AR используют многоядерный ЦП и неблокирующую коммутационную структуру и обеспечивают лучшую в отрасли производительность системы, отвечая требованиям расширения сети и требованиям развития услуг предприятий и филиалов.
- Маршрутизаторы AR G3 поддерживают сетевые режимы 3G и LTE, а также гибкий доступ через оптоволокно и медные кабели.
- Маршрутизаторы серии AR соединяются со сторонними ИТ-системами ведущих производителей с помощью OSP, чтобы предоставить корпоративным пользователям унифицированные услуги связи. Клиенты, агенты, сторонние поставщики и производители могут разрабатывать и использовать маршрутизаторы серии AR для создания наилучших систем.
- Маршрутизаторы серии AR предоставляют различные голосовые функции для корпоративных сетей передачи данных, позволяя предприятиям гибко и эффективно взаимодействовать.
- Во время предоставления услуг маршрутизаторы серии AR обеспечивают безопасность корпоративных сетей. Они предоставляют полный набор механизмов защиты, включая управление доступом пользователей, обнаружение пакетов и проактивную защиту от атак. Эти механизмы максимизируют инвестиции клиентов.
- Таким образом достигается интеллектуальное развертывание услуг и простое управление.

Внешний вид маршрутизаторов серии AR2200



Вид спереди
AR2204-27GE

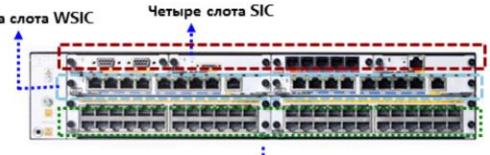


Вид спереди
AR2220E



3GE (комбинация 2GE)

Вид спереди
AR2240



Вид сзади AR2240

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Маршрутизаторы серии AR2200 используют встроенную аппаратную технику шифрования и поддерживают процессор цифровой обработки сигналов (DSP), функции межсетевого экрана, обработку вызовов, голосовую почту и различные прикладные программы. Маршрутизаторы серии AR2200 поддерживают различные режимы проводного и беспроводного доступа, такие как E1/T1, xDSL, xPON, CPOS, 3G и LTE.
- Маршрутизаторы серии AR2200 включают следующие модели: AR2204-27GE, AR2204-27GE-P, AR2204-51GE, AR2204-51GE-P, AR2204E, AR2220E, AR2240C, AR2240 и AR2204XE.

Характеристики маршрутизаторов серии AR2200

Характеристика	AR2220E	AR2240
Производительность передачи	9 млн. пакетов в секунду	10–25 млн. пакетов в секунду
Производительность межсетевого экрана	3 Гбит/с	5,5–15 Гбит/с
Порты	3*GE (1*Combo)	3*GE (2*Combo)/4*GE Combo + 2*GE SFP/4*GE Combo + 2*10GE SFP+
Слот SIC	4	4
Слот WSIC	2	4
Слот XSIC	0	4
Слот ESIC	0	1
Слот DSP	1	3
Память	1 ГБ	4 ГБ
Флэш-память (по умолчанию/макс.)	512 МБ/4 ГБ	2 ГБ/8 ГБ
Карта Micro SD (по умолчанию/мин.)	2 ГБ/4 ГБ	2 ГБ/4 ГБ
Порт USB	2	2
Размеры (Ш x Г x В)	442 мм x 420 мм x 44,5 мм	442 мм x 470 мм x 88,2 мм

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- AR2240 поддерживает несколько подключаемых SRU. SRU отличаются по производительности передачи и функциям управления трафиком. SRU обеспечивают аппаратное управление трафиком и аппаратный механизм H-QoS.
- Маршрутизаторы серии AR2200 поддерживают несколько типов интерфейсных плат, включая интерфейсные платы Ethernet, интерфейсные платы E1/T1/PRI/VE1, синхронные/асинхронные интерфейсные платы, интерфейсные платы ADSL2+/G.SHDSL, платы голосовых услуг FXS/FXO, интерфейсные платы ISDN, интерфейсные платы CPOS, интерфейсные платы EPON/GPON и интерфейсные платы 3G/LTE. Платы подразделяются на платы SIC, WSIC и XSIC в зависимости от типа слота.

Внешний вид маршрутизаторов серии AR3200



SRU80 – высокопроизводительные SRU. V200R003 не поддерживает двойные SRU.

Вид спереди AR3260



Вид сзади AR3260

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Маршрутизаторы серии AR3200 используют встроенную аппаратную технику шифрования и поддерживают голосовой DSP. Они также поддерживают функции межсетевого экрана, обработку вызовов, голосовую почту и различные прикладные программы. Маршрутизаторы серии AR3200 поддерживают различные режимы проводного и беспроводного доступа, такие как E1/T1, xDSL, xPON, CPOS и 3G.

Характеристики маршрутизаторов серии AR3200

Характеристика	AR3260
Производительность передачи	10–40 млн. пакетов в секунду
Возможности передачи услуг	1–5,5 Гбит/с
Возможности коммутации системы	640 Гбит/с
Слот SIC	4
Слот WSIC	4
Слот XSIC	6
Порты	3*GE (2*Combo)/4*GE Combo + 2*GE SFP/4*GE Combo + 2*10GE SFP+
Слот DSP	3
Память	4 ГБ
Флэш-память	8 ГБ
Слот ESIC	1
Порт USB	2
Размеры (Ш x Г x В)	442 мм x 470 мм x 130,5 мм

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- AR3260 поддерживает несколько типов подключаемых SRU. SRU отличаются по производительности передачи и функциям управления трафиком. SRU обеспечивают аппаратное управление трафиком и аппаратный механизм H-QoS.
- Маршрутизаторы серии AR3200 поддерживают несколько типов интерфейсных плат, включая интерфейсные платы Ethernet, интерфейсные платы E1/T1/PRI/VE1, синхронные/асинхронные интерфейсные платы, интерфейсные платы ADSL2+/G.SHDSL, платы голосовых услуг FXS/FXO, интерфейсные платы ISDN, интерфейсные платы CPOS, интерфейсные платы EPON/GPON и интерфейсные платы LTE. Платы подразделяются на платы SIC, WSIC и XSIC в зависимости от типа слота.

Характеристики SRU40, SRU60 и SRU80



SRU40/SRU60/SRU80

Характеристики SRU:

Название SRU	Производительность	Функция
SRU40	8-ядерный ЦП, частота 600 МГц	Не поддерживает управление трафиком.
SRU60	8-ядерный ЦП, частота 600 МГц	Не поддерживает управление трафиком.
SRU80	12-ядерный ЦП, частота 750 МГц	Поддерживает управление трафиком.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- SRU объединяет функции контроля и управления и обеспечивает плоскость контроля, плоскость управления и плоскость коммутации системы. Плоскость контроля: предоставляет такие функции, как обработка протокола, обработка услуг, расчет маршрута, управление передачей, планирование услуг, сбор статистики трафика и безопасность системы.
- Плоскость управления: обеспечивает такие функции, как мониторинг системы, мониторинг среды, обработка журналов и аварийных сигналов, загрузка системного программного обеспечения и обновление системы.
- Плоскость коммутации: обеспечивает высокоскоростные неблокирующие каналы данных для сервисного переключения между сервисными модулями.

Характеристики SRU100, SRU200, SRU400 и SRUX5



SRU100



SRU200



SRU400



SRUX5

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- SRU объединяет функции контроля и управления и обеспечивает плоскость контроля, плоскость управления и плоскость коммутации системы. Плоскость контроля: предоставляет такие функции, как обработка протокола, обработка услуг, расчет маршрута, управление передачей, планирование услуг, сбор статистики трафика и безопасность системы.
- Плоскость управления: обеспечивает такие функции, как мониторинг системы, мониторинг среды, обработка журналов и аварийных сигналов, загрузка системного программного обеспечения и обновление системы.
- Плоскость коммутации: обеспечивает высокоскоростные неблокирующие каналы данных для сервисного переключения между сервисными модулями.



- Два слота SIC можно объединить в один слот WSIC, удалив направляющую между ними.
- Два слота SIC и слот WSIC под ними можно объединить в один слот XSIC, удалив направляющие.
- Два слота XSIC можно объединить в один слот EXSIC, удалив направляющую между ними.
- Слоты могут быть объединены в один, но один слот не может быть разделен на несколько слотов.
- Новым идентификатором слота будет набольший между двумя исходными идентификаторами слотов.
- В V200R002C00 и более поздних версиях плату WSIC можно вставить в слот XSIC в нижней части слота и использовать идентификатор слота XSIC в качестве собственного идентификатора слота.
- MFS расшифровывается как Multiple Function Slot – многофункциональный слот.

Объединение интерфейсных плат на маршрутизаторах серии AR G3

Маршрутизаторы серии AR G3 со стандартной конструкцией поддерживают гибкое объединение различных сервисных плат, полностью используя ресурсы слотов и защищая инвестиции.

SIC: Smart Interface Card – Интеллектуальная интерфейсная плата

WSIC: Wide SIC – Расширенная плата SIC

XSIC: Extended WSIC – Расширенная плата WSIC

EXSIC: Extra-Extended XSIC – Экстра-расширенная плата XSIC



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Слоты могут быть объединены в один, но один слот не может быть разделен на несколько слотов.
- Новым идентификатором слота является набольший между двумя исходными идентификаторами слотов.

Интерфейсные модули WAN, поддерживаемые маршрутизаторами серии AR G3 (1/2)

Плата SIC E1:



1E1/T1-M

1/2-портовый канальный мультифункциональный интерфейсный модуль E1/T1/PRI/VE1



2E1/T1-M

Он получает, отправляет и обрабатывает потоки данных на интерфейсах E1. Этот модуль может быть настроен с интерфейсами VE1 для передачи голосовых услуг и данных, а также факсимильных сигналов.



1E1-F



2E1-F

1/2-портовый неканальный мультифункциональный интерфейсный модуль E1/T1

Плата SIC Ethernet



2FE

2-портовый модуль электрического интерфейса WAN 10M/100M



1GEC

1-портовый комбинированный интерфейсный модуль GE Ethernet WAN

Синхронная/асинхронная плата SIC



1SA

1-портовый улучшенный модуль синхронного/асинхронного последовательного интерфейса

Поддерживаются следующие протоколы: V.24, V.35, X.21, RS-449 и RS-530.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- 1/2: один или два интерфейса E1: интерфейс E1 T1: интерфейс T1 M: магистральный интерфейс первичной скорости (PRI): интерфейс первичной скорости ISDN
- VE1: голосовой интерфейс E1

Интерфейсные модули WAN, поддерживаемые маршрутизаторами серии AR G3 (2/2)

Плата ADSL2+ SIC:



1ADSL-A/M — 1-портовый интерфейсный модуль ADSL по POTS, поддерживающий ANNEX A/M



1ADSL-B/M — 1-портовый интерфейсный модуль ADSL over ISDN, поддерживающий ANNEX B

Плата 4G.SHDSL SIC:



4G.SHDSL — 1-портовый 4-парный интерфейсный модуль G.SHDSL

Плата PON SIC:



1PON — 1-портовая интерфейсная плата EPON/GPON

Плата CPOS SIC:



1CPOS — 1-портовый интерфейсный модуль 155M CPOS

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- 4G.SHDSL обеспечивает 4-канальный доступ G.SHDSL и независимый ЦП, а также интерфейсы управления.
- 1PON – это модуль автоматического определения EPON/GPON, используемый на маршрутизаторе AR. Он работает с SRU и поддерживает два интерфейса восходящей линии связи PON SFP.
- 1CPOS-155M (1-портовая канальная интерфейсная плата POS): **C** означает канализацию; **POS** означает пакет по SDH/SONET; **155M** означает, что скорость составляет 155,52 Мбит/с.

Интерфейсные модули коммутации Ethernet, поддерживаемые маршрутизаторами серии AR G3

Плата WSIC коммутации Ethernet:



8FE/1GE

Модуль электрического интерфейса Ethernet с 8 портами 100M (RJ45) и 1 портом 1000M (RJ45)-L2/L3. Он поддерживает линейную скорость передачи данных уровня 2 и уровня 3. Каждый интерфейс поддерживает автоматическое распознавание и может работать в полудуплексном или полнодуплексном режиме.

Плата XSIC коммутации Ethernet:



24GE

24-портовая электрическая интерфейсная плата 1000M (RJ45)-L2/L3 Ethernet. Поддерживает передачу данных уровня 2 и уровня 3. Каждый интерфейс поддерживает автоматическое распознавание и может работать в полудуплексном или полнодуплексном режиме.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- 8FE1GE можно установить в слот WSIC на шасси AR1200, AR2200 и AR3260. На AR1200 и AR2204 два слота SIC необходимо объединить в один слот WSIC.
- 24GE можно установить в слот XSIC на шасси AR2220, AR2240 и AR3260. На AR2220 два слота WSIC необходимо объединить в один слот XSIC.



- Интерфейсы Foreign Exchange Station (Внешняя станция; FXS) являются стандартными интерфейсами RJ-11. Интерфейсы FXS подключаются к таким устройствам, как обычные телефоны и факсимильные аппараты, через телефонные линии и обмениваются сигналами с устройствами посредством изменения уровня оконечных и кольцевых линий для обеспечения сигналов вызова, напряжения и тонов набора.
- Обменный пункт (FXO) – это двухпроводная магистральная петля. Интерфейс FXO представляет собой интерфейс RJ-11 и подключает локальный вызов к центральному офису телефонной сети общего пользования (PSTN) или небольшому абонентскому коммутатору (PBX) через телефонную линию. Подобно интерфейсам FXS, интерфейсы FXO также обмениваются сигналами посредством изменения уровня и кольцевых линий. Интерфейсы FXO могут подключаться только к другим интерфейсам FXS.

- 2BST – это модуль доступа к услугам ISDN для маршрутизаторов серии AR. Он обеспечивает два интерфейса ISDN S/T для передачи голосовых услуг.
- 2BST предлагает функцию ISDN BRI и обеспечивает полосу пропускания двух каналов B и одного канала D:
- Канал B является каналом голосовых услуг и обеспечивает полосу пропускания 64 кбит/с.
- Канал D является каналом сигнализации и обеспечивает полосу пропускания 16 кбит/с.
- Общая полоса пропускания двух каналов B и одного канала D составляет 144 кбит/с.
- Интерфейс S/T на 2BST обеспечивает линейную скорость 192 кбит/с, включая 144 кбит/с для передачи данных (два канала B и один канал D) и 48 кбит/с для передачи информации о

техническом обслуживании.

Электрические интерфейсы Ethernet на маршрутизаторах серии AR G3

- Электрический интерфейс Ethernet
  - Тип интерфейса: RJ45
  - Кабель: UTP/STP
  - Скорость: 10 Мбит/с, 100 Мбит/с, 1 Мбит/с
  - Протокол связи: Ethernet
  - Плата:
    - 8FE1GE
    - 24GE
    - 2FE



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Сетевые кабели соединяют сетевые устройства друг с другом, чтобы устройства могли обмениваться данными или обеспечивать локальное обслуживание и удаленный доступ.

Оптические интерфейсы Ethernet на маршрутизаторах серии AR G3

- Оптический интерфейс Ethernet
  - Тип интерфейса: LC/PC
  - Кабель: одномодовый и многомодовый
  - Скорость: 100 Мбит/с, 1 Гбит/с
  - Протокол связи: Ethernet
  - Плата
    - SRU
    - 1GEC





Модуль оптического интерфейса SFP



Сетевой распределитель LC/PC

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Одномодовое оптическое волокно и многомодовое оптическое волокно имеют одинаковый внешний вид, но разные цвета. Одномодовое оптическое волокно – желтое, а многомодовое оптическое волокно – оранжевое.
- Типы оптических модулей:
- Оптический модуль многооборотного режима должен быть подключен к многомодовому оптическому волокну.
- Оптический модуль с одной продольной или несколькими продольными модами должен быть подключен к одномодовому оптическому волокну.

Интерфейсы E1/T1 на маршрутизаторах серии AR G3

- Интерфейс E1/T1
  - Тип интерфейса: DB9
  - Кабель: магистральный кабель
  - Скорость: 2,048 Мбит/с, 1,544 Мбит/с
  - Протокол связи: PPP/HDLC
  - Плата:
    - 1E1T1-M
    - 2E1T1-M



Несимметричный коаксиальный кабель E1 с сопротивлением 75 Ом



Симметричный кабель «витая пара» E1 с сопротивлением 120 Ом или T1 с сопротивлением 100 Ом

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Кабели E1 подразделяются на следующие виды:
- Несимметричный коаксиальный кабель с сопротивлением 75 Ом (DB9 до BNC), который подключается следующим способом:
  - Один конец имеет разъем DB9.
  - Другой конец имеет два разъема BNC.
- Симметричный кабель «витая пара» с сопротивлением 120 Ом (DB9 до RJ45), который подключается следующим способом:
  - Один конец имеет разъем DB9.
  - Другой конец имеет разъем RJ45.
- Магистральный кабель T1 представляет собой сбалансированную витую пару на 100 Ом. Его внешний вид такой же, как у симметричной витой пары E1.

Интерфейсы xDSL на маршрутизаторах серии AR G3

- Интерфейс xDSL
  - Тип интерфейса: RJ11/RJ45 (4G.SHDSL)
  - Кабель: обычный телефонный кабель
  - Скорость: 5,696 Мбит/с, 8 Мбит/с, 12 Мбит/с, 24 Мбит/с
  - Протокол связи: аналоговая модуляция и демодуляция
  - Плата:
    - ADSL-A/M
    - ADSL-B
    - 4G.SHDSL



Кабель 4G.SHDSL

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Кабель 4G.SHDSL подключается следующим образом:
  - Один конец имеет разъем RJ45.
  - Другой конец имеет четыре разъема RJ11.

Синхронные/асинхронные последовательные интерфейсы на маршрутизаторах серии AR G3

- Синхронный/асинхронный последовательный интерфей
  - Тип интерфейса: DB28
  - Кабель: DCE/DTE
  - Скорость: 64 кбит/С до 2,048 Мбит/с
  - Протокол связи: Protocol/Flow
  - Плата:
    - 1SA



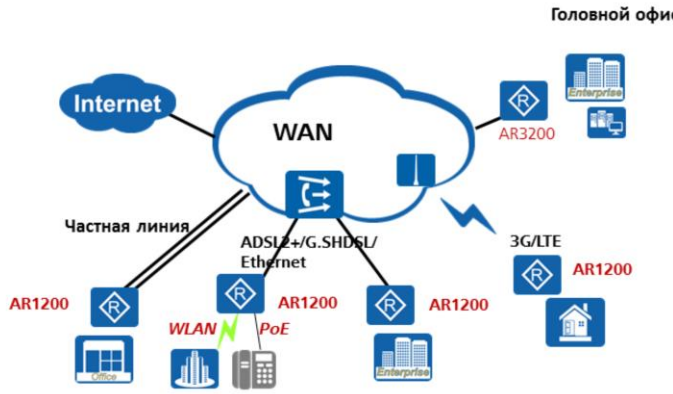
Кабель V.35 DCE



Кабель V.35 DTE

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

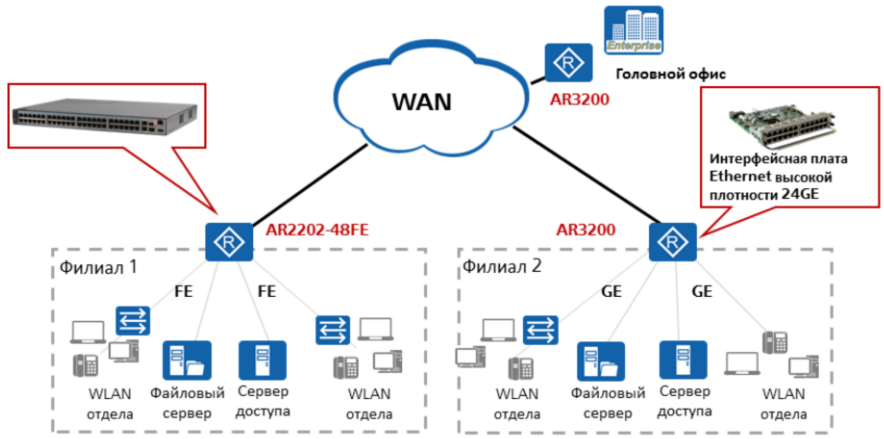
Сценарии широкополосного доступа корпоративных маршрутизаторов



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Корпоративные маршрутизаторы серии AR G3 функционируют в качестве выходных маршрутизаторов в сетях филиалов предприятия и предоставляют гибкие режимы доступа для реализации удаленного сетевого взаимодействия.
- Маршрутизаторы серии AR отвечают различным требованиям доступа, включая частную линию, Ethernet, xDSL, 3G и WLAN. Это экономит затраты на развертывание, эксплуатацию и обслуживание и предоставляет больше преимуществ для клиентов.
- Интерфейсы Ethernet 100M AR1220V и AR1220W (V200R001C01) поддерживают функцию PoE в соответствии с IEEE 802.3af и 802.3at; следовательно, эти маршрутизаторы могут обеспечивать питание PoE для устройств с удаленным питанием (PD), таких как IP-телефоны. Интерфейс 802.3at обеспечивает мощность более 30 Вт, отвечая требованиям по питанию для мощных PD.

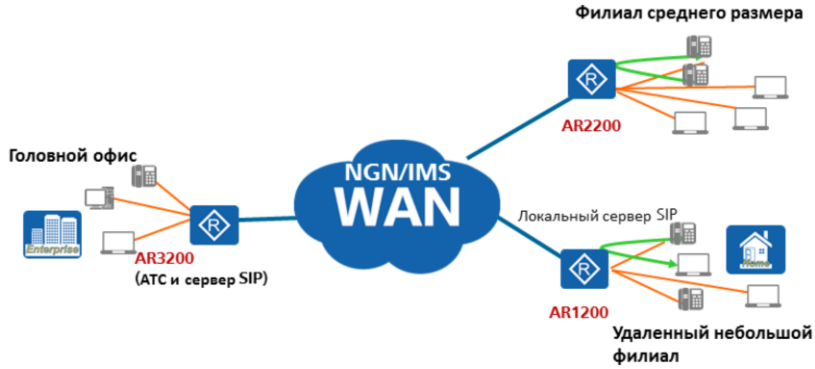
Интеграция функций доступа, маршрутизации и коммутации для филиалов предприятия



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Корпоративные маршрутизаторы серий AR2200 и AR3200 предоставляют платы с восемью портами FE и одним комбинированным портом GE, а также платы с двадцатью четырьмя портами GE для реализации межплатных коммутаций VLAN, зеркалирования, связующего дерева и связывания каналов, а также обмена данными уровня 2 и уровня 3.

Корпоративная связь VoIP



- Маршрутизатор AR имеет встроенную АТС и предоставляет услуги голосовой связи, такие как коммутационный узел, IVR и запрос счета.
- Маршрутизатор AR имеет встроенный сервер SIP, который обеспечивает надежность корпоративных голосовых услуг.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Маршрутизаторы серии AR G3 имеют встроенную АТС и предоставляют услуги голосовой связи, такие как коммутационный узел, IVR и запрос счетов, для улучшения имиджа предприятия и повышения эффективности связи на предприятии.
- Если сервер SIP в главном офисе недоступен, встроенный сервер SIP маршрутизатора AR реализует связь между филиалами и между филиалами и NGN/IMS. Это обеспечивает надежность голосовых услуг.
- Примечание: маршрутизаторы серии AR2200 и AR3200 версии V200R001C01 поддерживают корпоративную связь VoIP.

Сценарий корпоративного VPN-шлюза



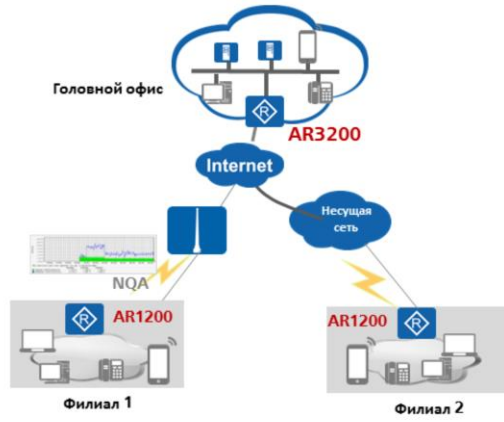
- Корпоративные маршрутизаторы серии AR G3 предоставляют туннели безопасности GRE VPN и IPSec VPN для обеспечения безопасного доступа и передачи данных, а также быстрого развертывания туннелей и аутентификации туннелей для филиалов.
- Маршрутизаторы серии AR G3 могут быть развернуты в филиалах как PE в сети MPLS. Различные сервисы изолированы MPLS VPN уровня 3, реализуя виртуализированную работу корпоративных сервисов.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Корпоративные маршрутизаторы серии AR G3 предоставляют множество функций безопасного доступа, включая туннели безопасности GRE VPN и IPSec VPN, для реализации безопасного доступа к данным и их передачи, а также быстрого развертывания туннелей и аутентификации туннелей для филиалов. Через удаленный туннельный доступ партнеры могут получить доступ к внутренним ресурсам предприятия. Поддерживается безопасность аутентификации и авторизации для пользователей.
- Маршрутизаторы серии AR G3 также могут быть развернуты в филиалах как PE в сети MPLS. Различные сервисы изолированы MPLS VPN уровня 3 для реализации гибкого развертывания, быстрой пересылки и безопасной передачи услуг VPN, реализуя виртуализированную работу корпоративных сервисов.

Сценарий беспроводного доступа 3G/LTE



- Маршрутизаторы серии AR G3 соответствуют стандартам 3G и LTE, включая CDMA2000 EV-DO, WCDMA и TD-SCMDA, LTE FDD и LTE TDD, удовлетворяя требованиям беспроводной связи между филиалами, а также между головным офисом и филиалами.
- Как правило, беспроводной доступ является резервным для проводного доступа.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Корпоративные маршрутизаторы серии AR G3 обеспечивают функции беспроводного доступа 3G и LTE и поддерживают стандарты 3G, включая CDMA2000 EV-DO, WCDMA и TD-SCDMA, отвечая требованиям беспроводного соединения между филиалами предприятия, а также между штаб-квартирой и филиалами. Кроме того, беспроводные каналы передачи данных могут использоваться в качестве резервной копии для проводных каналов с целью защиты восходящих каналов xDSL, FE / GE, GPON и POS. Резервирование каналов повышает стабильность сети и снижает стоимость строительства сети. Маршрутизаторы серии AR G3 используют технологию NQA для определения качества каналов 3G и LTE в режиме реального времени, обеспечивая SLA.

Содержание

1. Принципы проектирования корпоративных сетей
2. Процесс проектирования корпоративных сетей
3. **Выбор продукта**
   - Как выбирать продукты
   - Маршрутизаторы серии AR G3
   - Коммутаторы серии Sx700
   - Другие продукты
4. Проектирование корпоративной сети на примерах

© 2019 Huawei Technologies Co., Ltd. Все права защищены.



- Линейка интеллектуальных коммутаторов Huawei Sx700 нового поколения предназначена для кампусных сетей предприятий. Гибкие устройства развертываются на уровне ядра, агрегации и доступа, отвечая требованиям различных компаний к организации сети.
- В линейку Sx700 включены следующие серии:
  - Терабитные маршрутизирующие коммутаторы уровня ядра серии S9700
  - Интеллектуальные маршрутизирующие коммутаторы серии S7700
  - Коммутаторы 10GE серии S6700 для центров обработки данных
  - Корпоративные гигабитные коммутаторы серии S5700
  - Корпоративные коммутаторы 100M уровня 3 серии S3700
  - Корпоративные коммутаторы 100M уровня 2 серии S2700
  - Коммутаторы серии S1700 для предприятий среднего и малого бизнеса

Коммутаторы серии S3700 (1/4)

- **S3700-28TP-EI-24S-AC**



- **S3700-28TP-PWR-EI**



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Коммутаторы серии S3700 (2/4)

S3700-26C-HI



- 22 порта 10/100BASE-TX, 2 комбинированных порта GE (10/100/1000BASE-T или 100/1000BASE-X) и 2-портовый модуль 100BASE-X (опционально)
- Двойные съемные модули питания, питание от источника переменного тока или источника постоянного тока
- Скорость передачи пакетов: 9,3 млн пакетов в секунду
- Емкость коммутации: 64 Гбит/с

S3700-28TP-SI/EI



- 24 порта 10/100BASE-TX, 2 порта 1000BASE-X SFP и 2 комбинированных порта GE (10/100/1000BASE-T или 100/1000BASE-X)
- Питание от источника переменного тока или постоянного тока
- Скорость передачи пакетов: 9,6 млн пакетов в секунду
- Емкость коммутации: 64 Гбит/с

S3700-28TP-EI-MC-AC



- 24 порта 10/100BASE-TX, 2 порта 1000BASE-X SFP и 2 комбинированных порта GE (10/100/1000BASE-T или 100/1000BASE-X)
- Питание от источника переменного тока
- Скорость передачи пакетов: 9,6 млн пакетов в секунду
- Емкость коммутации: 64 Гбит/с

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Коммутаторы серии S3700 (3/4)

S3700-28TP-PWR-EI



- 24 порта 10/100BASE-TX, 2 порта 1000BASE-X SFP и 2 комбинированных порта GE (10/100/1000BASE-T или 100/1000BASE-X)
- Питание от источника переменного тока
- Питание PoE+
- Скорость передачи пакетов: 9,6 млн. пакетов в секунду
- Емкость коммутации: 64 Гбит/с

S3700-28TP-EI-24S-AC



- 24 порта 100BASE-FX SFP, 2 порта 1000BASE-X SFP и 2 комбинированных порта GE (10/100/1000BASE-T или 100/1000BASE-X)
- Питание от источника переменного тока
- Скорость передачи пакетов: 9,6 млн. пакетов в секунду
- Емкость коммутации: 64 Гбит/с

S3700-52P-SI-AC



- 48 портов 10/100BASE-TX, 2 порта 100/1000BASE-X SFP и 2 порта 1000BASE-X SFP
- Питание от источника переменного тока
- Скорость передачи пакетов: 13,2 млн. пакетов в секунду
- Емкость коммутации: 64 Гбит/с

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Коммутаторы серии S3700 (4/4)

S3700-52P-EI



- 48 портов 10/100BASE-TX, 2 порта 100/1000BASE-X SFP и 2 порта 1000BASE-X SFP
- Питание от источника переменного тока или постоянного тока
- Скорость передачи пакетов: 13,2 млн. пакетов в секунду
- Емкость коммутации: 64 Гбит/с

S3700-52P-PWR-EI



- 48 портов 10/100BASE-TX, 2 порта 100/1000BASE-X SFP и 2 порта 1000BASE-X SFP
- Питание от источника переменного тока
- Питание PoE+
- Скорость передачи пакетов: 13,2 млн. пакетов в секунду
- Емкость коммутации: 64 Гбит/с

S3700-52P-EI-48S



- 48 портов 100BASE-FX SFP, 2 порта 100/1000BASE-X SFP и 2 порта 1000BASE-X SFP
- Питание от источника переменного тока или постоянного тока
- Скорость передачи пакетов: 13,2 млн. пакетов в секунду
- Емкость коммутации: 64 Гбит/с

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Коммутаторы серии S5700 (1/4)

- **S5700-24TP-SI-AC**



- **S5700-48TP-PWR-SI**



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Высота шасси устройств S5700 —1 U (1 U = 44,45 мм).
- Габаритные размеры (Ш x Г x В) шасси моделей S5700-24TP-SI-AC, S5700-24TP-SI-DC, S5700-28C-HI и S5700-28C-HI-24S — 442,0 мм × 220,0 мм × 43,6 мм.
- Габаритные размеры (Ш x Г x В) шасси модели S5700-6TP-LI-AC — 250,0 мм × 180,0 мм × 43,6 мм.
- Габаритные размеры (Ш x Г x В) шасси остальных моделей — 442,0 мм × 420,0 мм × 43,6 мм.
- Коммутаторы серии S5700-EI поддерживают платы восходящей связи, которые предоставляют гибкие порты восходящей связи GE/10GE высокой плотности.
- Коммутатор S5710-EI предоставляет четыре порта фиксированной связи 10GE SPF+. Комбинируя платы восходящей связи, можно реализовать следующие конфигурации портов: 64*GE+4*10GE, 48*GE+8*10GE или 56*GE+6*10GE. Таким образом, это оптимальный вариант, подходящий под текущие потребности в пропускной способности и учитывающий будущее обновление, который эффективно защитит инвестиции клиентов.

Коммутаторы серии S5700 (2/4)

S5700-24TP-SI



- 20 портов 10/100/1000BASE-T и 4 комбинированных порта 100/1000BASE-X GE
- Питание от источника переменного тока или источника постоянного тока, поддержка (резервный источник 12 В)
- Порт USB
- Скорость передачи пакетов: 36 млн. пакетов в секунду
- Емкость коммутации: 256 Гбит/с

S5700-24TP-PWR-SI



- 20 портов 10/100/1000BASE-T и 4 комбинированных порта 100/1000BASE-X GE
- Два съемных модуля питания переменного тока
- Питание PoE+
- Порт USB
- Скорость передачи пакетов: 36 млн. пакетов в секунду
- Емкость коммутации: 256 Гбит/с

S5700-48TP-SI



- 24 порта 10/100/1000BASE-T и 4 комбинированных порта 100/1000BASE-X GE
- Питание от источника переменного тока или источника постоянного тока, поддержка (резервный источник 12 В)
- Порт USB
- Скорость передачи пакетов: 72 млн. пакетов в секунду
- Емкость коммутации: 256 Гбит/с

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Коммутаторы серии S5700 (3/4)

S5700-48TP-PWR-SI



- 24 порта 10/100/1000BASE-T и 4 комбинированных порта 100/1000BASE-X GE
- Питание от источника переменного тока
- Питание PoE+
- Порт USB
- Скорость передачи пакетов: 72 млн. пакетов в секунду
- Емкость коммутации: 256 Гбит/с

S5700-28C-SI



- 20 портов 10/100/1000BASE-T, 4 комбинированных порта 100/1000BASE-X GE, 4-портовый модуль 1000BASE-X SFP, 2-портовый модуль 10GE SFP+ и 4-портовый модуль 10GE SFP+
- Два съемных модуля питания
- Порт USB
- Скорость передачи пакетов: 96 млн. пакетов в секунду
- Емкость коммутации: 256 Гбит/с

S5700-28C-EI



- 24 порта 10/100/1000BASE-T, 4-портовый модуль 1000BASE-X SFP, 2-портовый модуль 10GE SFP+ и 4-портовый модуль 10GE SFP+
- Два съемных модуля питания
- Скорость передачи пакетов: 96 млн. пакетов в секунду
- Емкость коммутации: 256 Гбит/с

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Коммутаторы серии S5700 (4/4)

S5700-28C-EI-24S



- 20 портов 100/1000BASE-X, 4 комбинированных порта 10/100/1000BASE-T GE, 4-портовый модуль 1000BASE-X SFP, 2-портовый модуль 10GE SFP+ и 4-портовый модуль 10GE SFP+
- Два съемных модуля питания
- Скорость передачи пакетов: 96 млн пакетов в секунду
- Емкость коммутации: 256 Гбит/с

S5700-28C-PWR-EI



- 24 порта 10/100/1000BASE-T, 4-портовый модуль 1000BASE-X SFP, 2-портовый модуль 10GE SFP+ и 4-портовый модуль 10GE SFP+
- Два съемных модуля питания переменного тока
- Питание PoE+
- Скорость передачи пакетов: 96 млн. пакетов в секунду
- Емкость коммутации: 256 Гбит/с

S5700-52C-SI

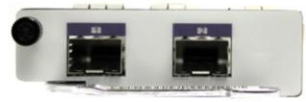


- 28 портов 10/100/1000BASE-T, 4-портовый модуль 1000BASE-X SFP, 2-портовый модуль 10GE SFP+ и 4-портовый модуль 10GE SFP+
- Два съемных модуля питания
- Порт USB
- Скорость передачи: 132 млн. пакетов в секунду
- Емкость коммутации: 256 Гбит/с

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Платы, поддерживаемые коммутаторами серии S3700



Тип платы	Описание	Модель устройства
Передняя плата	G2S: 2-портовый оптический SFP-модуль GE	S3700-26C-HI

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Плата G2S предоставляет два оптических порта 1000M SFP для подключения каналов передачи данных и коммутации на линейной скорости.
- Плата G2S управляется главной платой управления устройства S3700-HI. Поддерживает функции: управление включением и выключением питания, определение нормальной установки платы в слоте, PHY, управление оптическими портами. Предусмотрены также такие расширенные функции, как OAM и BFD.
- Плату G2S можно вставлять в слот, предназначенный для передних плат коммутатора S3700-HI, и заменять ее можно в горячем режиме.

Платы, поддерживаемые коммутаторами серии S5700



E2XX: 2-портовый оптический XFP-модуль 10GE



E2XY: 2-портовый оптический модуль SFP+ 10GE



E4XY: 4-портовый оптический модуль SFP+ 10GE



X4SA: 4-портовый оптический модуль SFP GE или SFP+ 10G



E4GF/E4GFA: 4-портовый оптический модуль GE

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

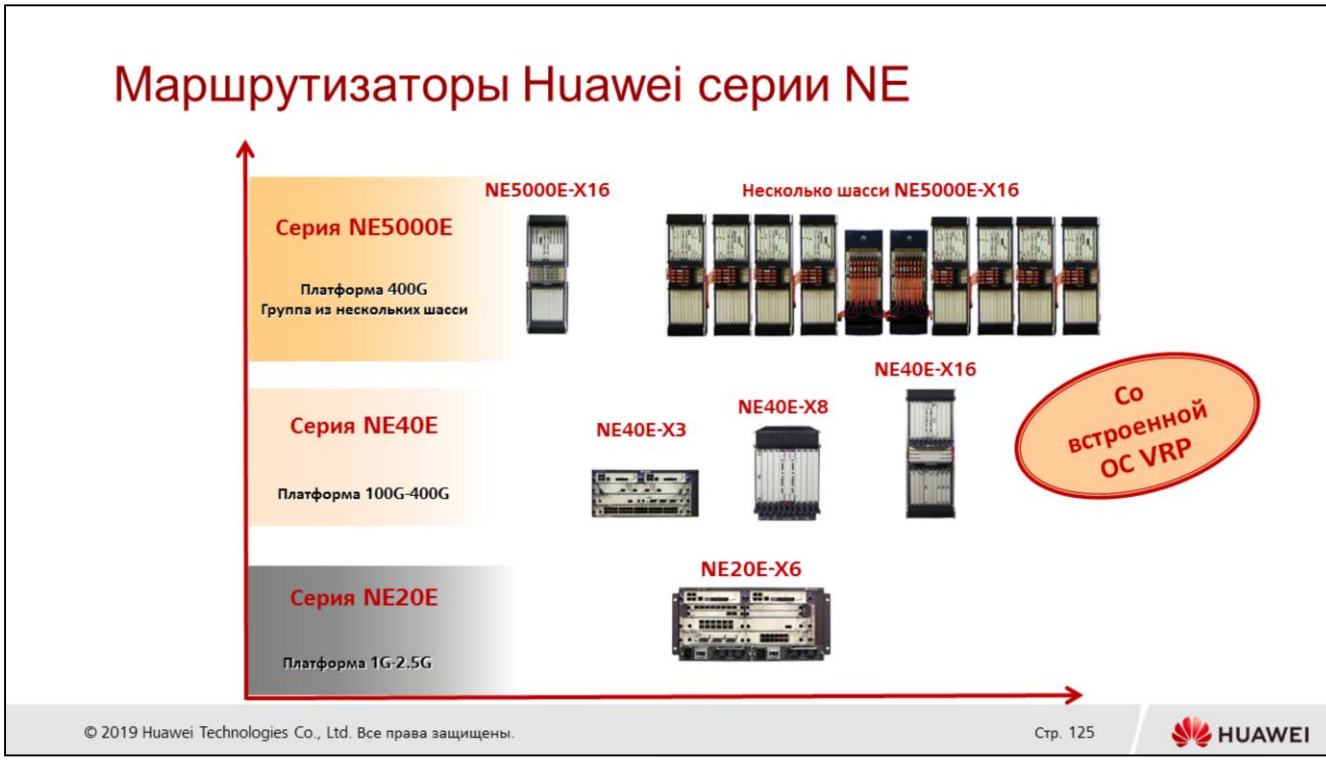
HUAWEI

- Плата E2XX используется в моделях S5700-28C-EI, S5700-52C-EI, S5700-28C-EI-24S, S5700-28C-SI, S5700-52C-SI и S5700-28C-PWR-EI.
- Плата E2XY используется в модели S5700-52C-PWR-EI.
- Плата E4XY используется в моделях S5700-28C-EI, S5700-52C-EI, S5700-28C-EI-24S, S5700-28C-SI и S5700-52C-SI.
- Плата E4GFA используется в модели S5700SI.
- Плата E4GF используется в модели S5700EI.
- В серии S5700C платы с горячей заменой поддерживаются только моделями S5700-28C-HI, S5700-28C-HI-24S, S5710-28C-EI и S5710-52C-EI.

Содержание

1. Принципы проектирования корпоративных сетей
2. Процесс проектирования корпоративных сетей
3. **Выбор продукта**
   - Как выбирать продукты
   - Маршрутизаторы серии AR G3
   - Коммутаторы серии Sx700
   - Другие продукты
4. Проектирование корпоративной сети на примерах

© 2019 Huawei Technologies Co., Ltd. Все права защищены.



- Сверхбыстрый кластерный маршрутизатор NetEngine5000E (сокращенно NE5000E) разработан компанией Huawei для магистральных интернет-узлов, узлов уровня ядра сети MAN, узлов DCI и узлов транспортного уровня Интернет. В данном устройстве применяются разработанные компанией Huawei чипы Solar, передовая архитектура коммутации и распределенная масштабируемая программная платформа. Маршрутизатор отличается большой емкостью коммутации и сверхвысокой скоростью передачи, отвечая современным требованиям к интернет-устройствам нового поколения — высокая пропускная способность, высокое качество обслуживания и функциональность.
- Универсальные сервисные маршрутизаторы серии NetEngine40E (сокращенно NE40E) — это профессиональные сетевые устройства разработки Huawei. Данные устройства развертываются, как правило, на границах магистральных IP-сетей, IP MAN и других крупномасштабных сетей IP. Использование устройств NE40E, NE5000E и ME60 в комбинации позволяет получить полное решение для иерархической IP-сети.
- Сервисный маршрутизатор NetEngine20E-X6 профессионального уровня (сокращенно NE20E-X6) предназначен для применения в различных отраслях — финансовыми и энергетическими компаниями, государственными и образовательными организациями. Данные устройства, обладающие высокой надежностью и доступностью, можно устанавливать в сетях доступа и агрегации.



- Высокопроизводительные облачные коммутаторы Huawei серии CloudEngine предназначены для центров обработки данных нового поколения и высокопроизводительных кампусных сетей. Флагман этой серии, коммутатор уровня ядра CloudEngine 12800, обладает самой высокой производительностью в мире, а высокопроизводительные фиксированные коммутаторы CloudEngine 6800 и 5800 предназначены для организации доступа 10GE/GE. В устройствах CloudEngine применяется программная платформа Huawei нового поколения — VRP8, поддерживающая расширенные сервисные функции для сетей центров обработки данных и кампусных сетей.
- Данные коммутаторы в комбинации с продуктами передачи, маршрутизации, обеспечения безопасности и сетевого управления стали основой для создания компанией Huawei решения CloudFabric для облачных центров обработки данных нового поколения. Используя данное решение, клиенты смогут построить стабильную сетевую архитектуру с перспективой развития на ближайшие 10 лет.



- Свою линейку точек беспроводного доступа 802.11n нового поколения компания Huawei разработала для корпоративных пользователей. Устройства совместимы со стандартами 802.11a, 802.11b и 802.11g. В линейку вошли серия высокопроизводительных устройств, серия недорогих экономичных устройств и серия устройств, отличающихся передовыми технологиями. Любая компания, сможет подобрать подходящую модель, соответствующую ее размеру и деятельности.
    - В точках беспроводного доступа высокотехнологичной серии применяются современные технологии WLAN, обеспечивающие высочайшую скорость передачи услуг WLAN в условиях высокой плотности пользователей средних и крупных предприятий.
    - В точках беспроводного доступа высокопроизводительной серии применяется новейшая архитектура чипов нового поколения, которые обеспечат поддержку различных сервисов в средних и крупных предприятиях.
    - Серия недорогих устройств обеспечит доступом 802.11n к базовым сервисам небольшие и средние компании, а также филиалы компаний.
- Huawei предлагает два типа контроллеров точек доступа: в виде отдельного устройства и в виде платы. Устройства можно применять в различных архитектурах проводных сетей крупных кампусов, филиалов предприятий и небольших компаний. Контроллеры безопасны, надежны, эффективны и просты в управлении.

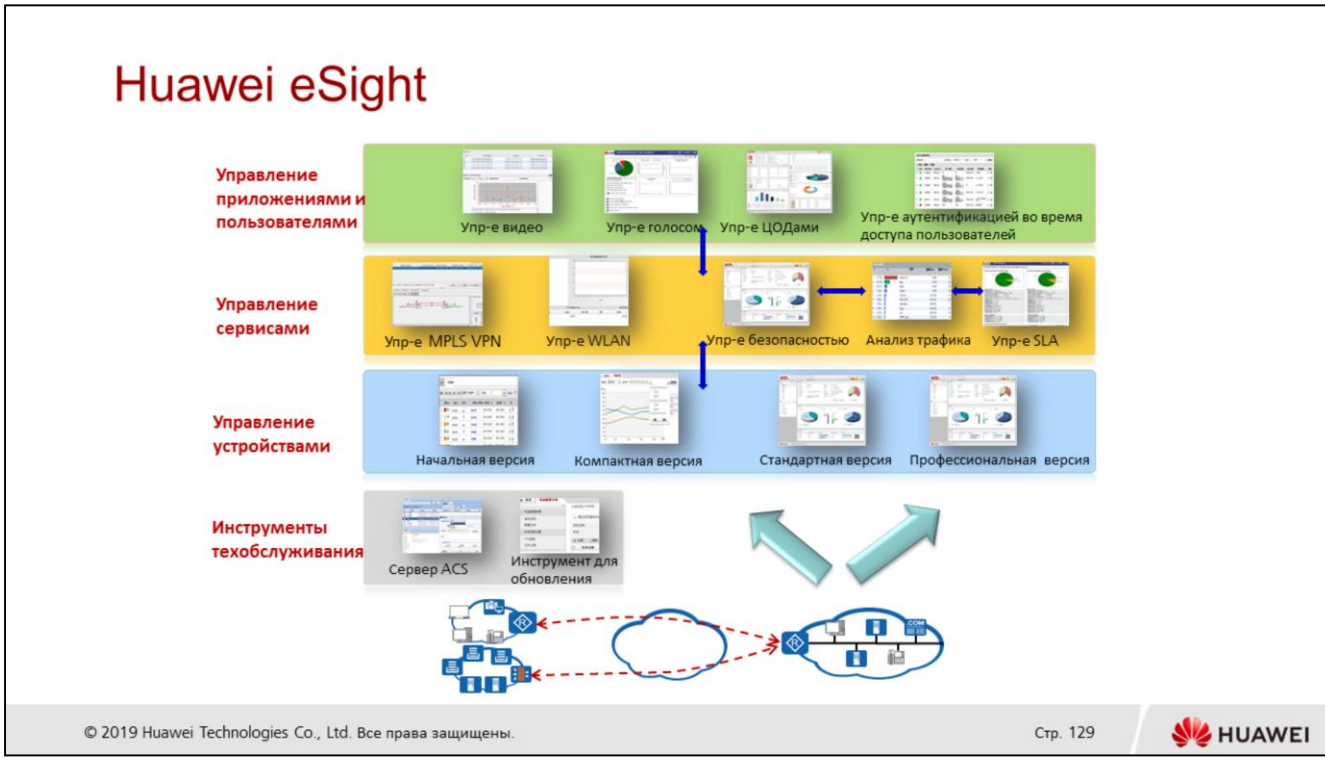
Продукты обеспечения сетевой безопасности Huawei



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Углубленная проверка пакетов (DPI): продукты серии SIG
- Системы обнаружения и предотвращения вторжений и хакерских атак (IDS и IPS): продукты серии NIP
- Продукты защиты от атак DDoS: Eudemon 1000E-I/D и Eudemon 8000E-X
- UTM и межсетевой экран: Eudemon 200E-X Eudemon 1000E-X и Eudemon 8000E-X
- SSL VPN: продукты серии SVN
- Управление безопасностью терминалов: TSM и DSM
- Управление безопасностью: eLog, VSM, UMA и iSOC



- eSight — это решение компании Huawei для унифицированной эксплуатации и техобслуживания IP- и IT-сетей нового поколения. Решение, разработанное в соответствии со стандартами ITIL, реализует централизованное управление корпоративными ресурсами, сервисами и пользователями. С этим решением различные предприятия и компании-партнеры получат интегрированную и открытую платформу O&M.

Содержание

1. Принципы проектирования корпоративных сетей
2. Процесс проектирования корпоративных сетей
3. Выбор продукта
4. **Проектирование корпоративной сети на примерах**

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Развитие компании A



Корпоративная сеть стимулирует быстрый рост компании.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Когда компания A была небольшим предприятием...

- Компания A со штатом в 20 человек арендовала офисное помещение.
- Каждый сотрудник выполнял свои обязанности, используя ПК. Сотрудникам приходилось часто обмениваться файлами, искать информацию в Интернете.
- Петр отвечал за администрирование сети и работал на полставки.



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Особенности небольших и средних компаний
  - Один вид сервиса
    - Небольшие и средние компании обычно предлагают один вид сервиса или набор нескольких сервисов.
  - Отсутствие изоляции
    - Если компания предоставляет один вид сервиса, изоляция сервисов не требуется.
    - Кроме того, сотрудники таких предприятий обычно выполняют разные обязанности, поэтому изоляция сервисов невозможна.
  - Централизованные сервисы
    - Персонал и основные средства небольших и средних компаний часто сосредоточены на небольшой территории, например в офисе или одном здании.
  - Простые требования
    - В связи с необходимостью организации только базовых видов сервисов требования, которые такие компании предъявляют к сетям, достаточно просты.

Решение Петра



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Архитектура сети небольшой компании проста.
- Как правило, это офисная сеть.
  - Из сетевых устройств может потребоваться только один маршрутизатор и один коммутатор или устройство, совмещающее функции маршрутизации и коммутации (например, AR G3).
  - Для подключения к Интернет на маршрутизаторе настраивается один стандартный статический маршрут и NAT.
  - Коммутатор использует конфигурацию по умолчанию или обеспечивает простое назначение VLAN.
  - QoS не гарантируется.
  - Количество ПК небольшое, поэтому их IP-адреса можно настроить вручную.
  - Отдельные сотрудники по техобслуживанию сети не предусмотрены.

Когда компания A стала расширяться...

- С развитием бизнеса компании требования к сети стали расти.
- В целях быстрой адаптации к потребностям компании Петр начал постепенно расширять сеть.
- Однако по достижении определенного масштаба в сети начали появляться проблемы.

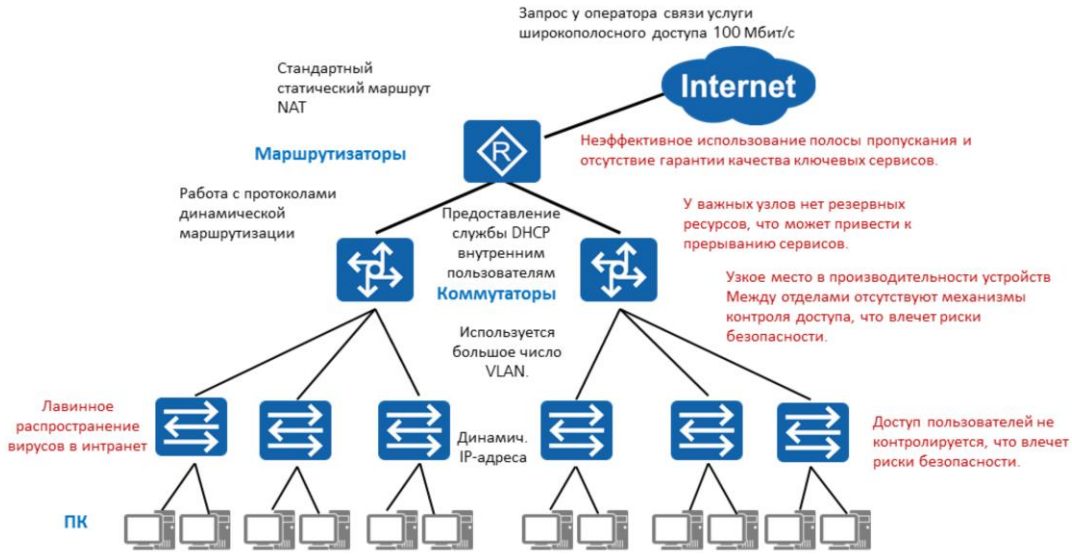


Петр

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Для увеличения количества пользователей на раннем этапе развития сети удобно просто добавлять устройства и кабели к существующей сети.
- Но с дальнейшим расширением сети постепенно появляются те или иные проблемы.

Состояние существующей сети



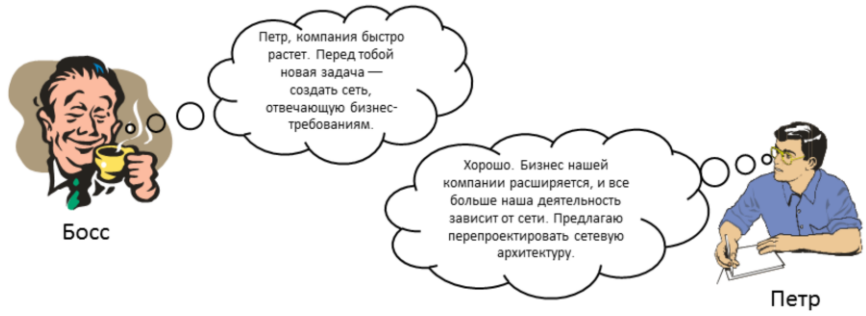
© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Развитие сети — это не просто добавление устройств и подключение кабелей. Если крупную сеть создавать на базе структуры небольшой сети, возникнет множество проблем.

Когда компания A стала предприятием среднего размера

- Новая корпоративная сеть значительно повысила эффективность работы компании. Компания A в результате быстро выросла в предприятие среднего размера с несколькими сотнями сотрудников.
- Петр переконструировал сеть, но она так и не отвечала требованиям развития бизнеса компании. Таким образом, изменение сетевой архитектуры стало просто необходимым условием.

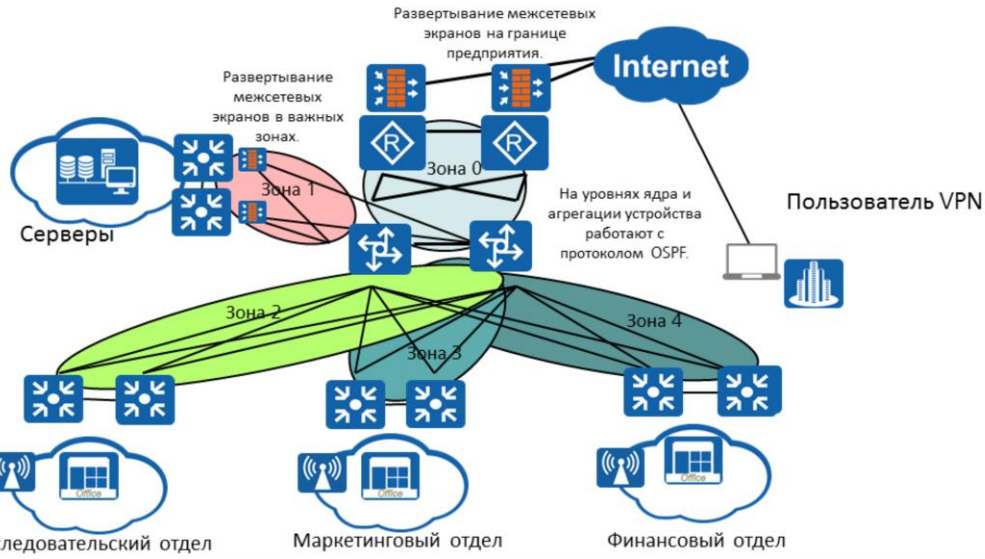


© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Новая корпоративная сеть значительно повысила эффективность работы компании. Компания A в результате быстро выросла в предприятие среднего размера с несколькими сотнями сотрудников.
- Петр изменил архитектуру сети следующим образом:
  - С увеличением количества пользователей доступа Петр добавил в сеть большое число коммутаторов уровня 2.
  - Из-за большого числа коммутаторов доступа Петру пришлось установить коммутаторы агрегации и назначить VLAN.
  - В связи с увеличением объема сервисов был модернизирован выходной маршрутизатор и выделена более широкая полоса пропускания.
- Однако сеть так и не отвечала требованиям развития бизнеса компании.

Решение Петра

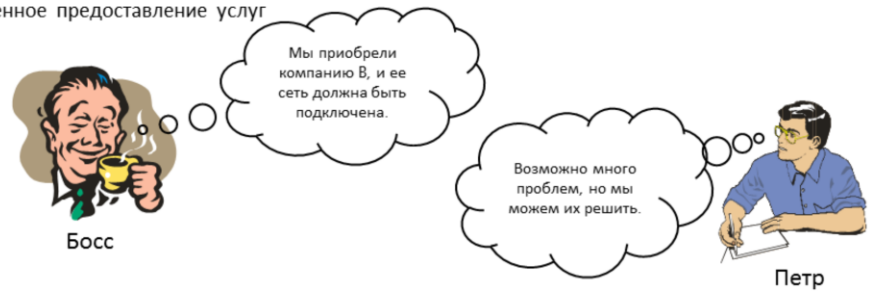


© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Различные отделы и службы предприятия могут находиться в разных кампусах. Каждый кампус представляет собой сеть небольшого или среднего размера, имеющую следующие особенности:
  - В сети установлено большое число коммутаторов.
  - Сеть имеет понятную иерархическую структуру, и каждая подсеть имеет иерархическую структуру.
  - Поскольку структура сети сложная, и статические маршруты не отвечают требованиям, используется протокол динамической маршрутизации (OSPF).
  - Различные сервисы распределяются по различным зонам, и для изоляции этих зон применяются межсетевые экраны.
  - С повышением важности ИТ-системы для компании была создана отдельная серверная зона.
  - Поскольку от сети зависит работа сервисов предприятия, важные узлы были продублированы.
  - На границах корпоративной сети и в важных серверных зонах были установлены межсетевые экраны.
  - Для реализации мобильного офиса в офисной зоне была развернута WLAN на базе точек беспроводного доступа Fit. Центральное управление этими точками доступа осуществляет контроллер.
  - Для техобслуживания сети выделены отдельные сотрудники.

Долгосрочное использование

- При развитии компании A корпоративная сеть также столкнулась с большими проблемами.
  - Более сложные политики контроля
  - Более строгие политики безопасности
  - Более подробные политики QoS
  - Ускоренное предоставление услуг



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Открытое обсуждение:
  - Какие проблемы могут возникнуть при объединении двух сетей?
  - Как мы можем решить эти проблемы?

Резюме

- Корпоративные сети должны проектироваться на основе корпоративных услуг.
- Проектирование корпоративной сети должно соответствовать общим правилам.
- При проектировании корпоративных сетей необходимо учитывать будущие тенденции и возможности расширения.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Спасибо за внимание!

www.huawei.com

HCIE-R&S
— диагностика и устранение отказов на примерах

www.huawei.com

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Предисловие

- В данном разделе приводится описание процедуры и методов диагностики и устранения проблем, связанных с работой протоколов IP-маршрутизации маршрутизаторов.
- В презентации разбираются и детально анализируются примеры общих проблем OSPF, IS-IS, BGP и MPLS VPN. Эта информация поможет в дальнейшем диагностировать и устранять отказы, связанные с протоколами маршрутизации.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Цели

- По завершении данного курса обучающиеся научатся:
  - Описывать стандартные методы диагностики работы OSPF, IS-IS, BGP и MPLS BGP VPN.
  - Описывать план действий при проведении диагностики OSPF, IS-IS, BGP и MPLS BGP VPN.
  - Анализировать и устранять проблемы, связанные с протоколами OSPF, IS-IS, BGP и MPLS BGP VPN.

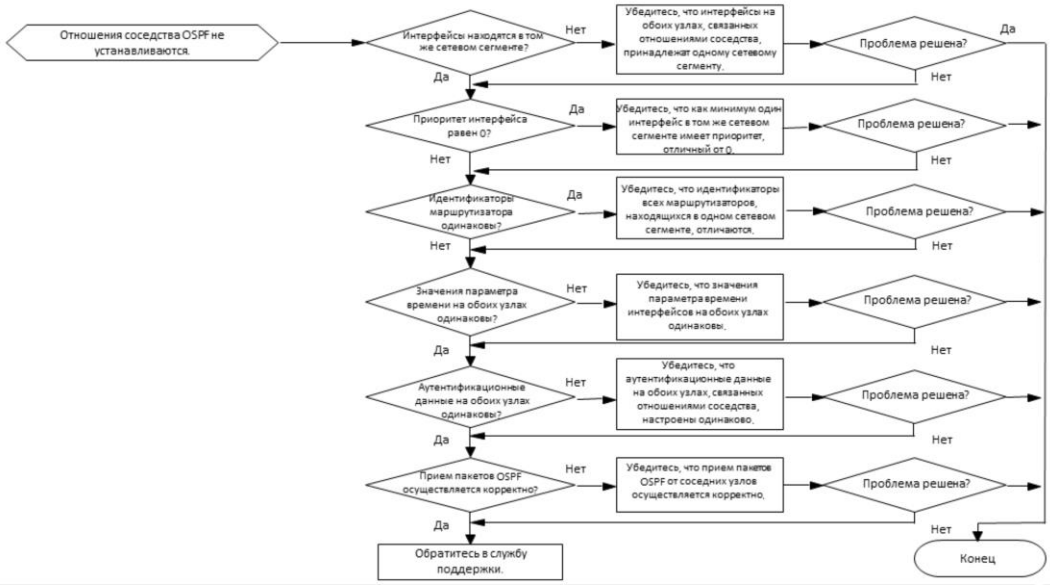
© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Содержание

1. **Диагностика OSPF**
   - Стандартная процедура диагностики OSPF
   - Диагностика OSPF на примерах
2. Диагностика IS-IS
3. Диагностика BGP
4. Диагностика MPLS BGP VPN

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Процесс диагностики и устранения отказов



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Проблемы установления отношений соседства OSPF считаются наиболее общими проблемами OSPF.
- Если после настройки маршрутизаторов не удается установить отношения соседства OSPF, выполните диагностику, следуя процедуре, приведенной на схеме.

Процедура диагностики и устранения отказов



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Шаг 1. Убедитесь, что интерфейсы находятся в одном сетевом сегменте.
  - Для установления отношений соседства OSPF необходимо проверить интерфейсы NBMA и широковещания — они должны принадлежать одному сетевому сегменту. Два межсетевых экрана должны успешно проверять достижимость друг друга командой ping. Интерфейсы должны иметь одинаковые значения идентификатора и типа зоны — area ID и area type (включая NSSA, Stub и Normal Area).
- Шаг 2. Убедитесь, что имеется интерфейс, приоритет которого не равен 0.
  - В широковещательных и NBMA-сетях как минимум один интерфейс должен иметь приоритет, отличный от 0. Это гарантирует корректный выбор выделенного маршрутизатора (DR). Иначе отношения соседства смогут достигнуть только состояния двухстороннего соединения (two-way state). Для проверки приоритета каждого интерфейса выполните команду **display ospf interface**.
- Шаг 3. Убедитесь, что каждый маршрутизатор имеет уникальный идентификатор (ID).
  - Идентификаторы разных маршрутизаторов в одной автономной системе (AS) должны отличаться. Иначе возникает непредвиденное явление нестабильности (flapping) маршрутов. Для проверки идентификатора каждого маршрутизатора выполните команду **display ospf brief**.

- Шаг 4. Убедитесь, что значения параметра Timer интерфейсов совпадают.
  - Командой **ospf timer hello** настройте интервал отправки интерфейсами пакетов Hello. На интерфейсе широковещания и интерфейсе Point-to-Point (P2P) по умолчанию стоит значение, равное 10 секундам. На интерфейсе NBMA и интерфейсе Point-to-Multipoint (P2MP) по умолчанию стоит значение, равное 30 секундам.
  - Командой **ospf timer dead** установите для отношений соседства OSPF значение периода dead interval, по прохождению которого, сосед будет считаться недоступным при отсутствии пакета Hello. На интерфейсе широковещания и интерфейсе Point-to-Point (P2P) по умолчанию стоит значение 40 секунд, а на интерфейсе NBMA и интерфейсе Point-to-Multipoint (P2MP) — 120 секунд.
  - Перед настройкой отношений соседства OSPF убедитесь, что значения интервалов на указанных интерфейсах совпадают, иначе установление соседства будет невозможно. Для проверки интервала выполните команду **display ospf interface verbose**.
- Шаг 5. Убедитесь, что аутентификационные данные интерфейсов настроены одинаково.
  - Аутентификационные данные настраиваются для определенной зоны или определенного интерфейса.
  - Основные принципы аутентификации OSPF:
    - Данные аутентификации вступают в силу после их настройки на интерфейсе.
    - Если на интерфейсе будет установлено значение Null, интерфейс не будет проходить аутентификацию.
    - Если аутентификация не будет сконфигурирована на интерфейсе (значение authentication mode — Null), будет

применена процедура аутентификации зоны.

- Если аутентификация не будет сконфигурирована ни для интерфейса, ни для зоны, процедура аутентификации не будет выполняться.

- Во время установления отношений соседства OSPF переход в состояние Full для таких отношений будет возможен, только если настройки аутентификации на обоих узлах согласованы.

- Шаг 6. Убедитесь, что прием пакетов OSPF осуществляется корректно.
  - В процессе получения пакетов OSPF могут возникать проблемы. В этом случае необходимо в первую очередь проверить подключение на канальном уровне. Выполните команду **debugging ospf packet** and **debugging ospf event** и проверьте процессы отправки и получения пакетов OSPF. Для просмотра статистики ошибок OSPF используется также команда **display ospf error**.
  - Если все пакеты OSPF в норме, проверьте правильность настройки GTSM на интерфейсе. Если настроена только политика пропуска пакетов частной сети (private policy) или сети общего пользования (public policy), и по умолчанию пакеты, не отвечающие политике GTSM, пропускаются, пакеты OSPF других экземпляров могут по ошибке отбрасываться.
  - Выполните команду **debugging ip packet**. В появившейся информации отладки передачи IP-пакетов проверьте и убедитесь, что данный процесс нормально выполняется. Информацию отладки можно отфильтровать, применив фильтр ACL Filter.



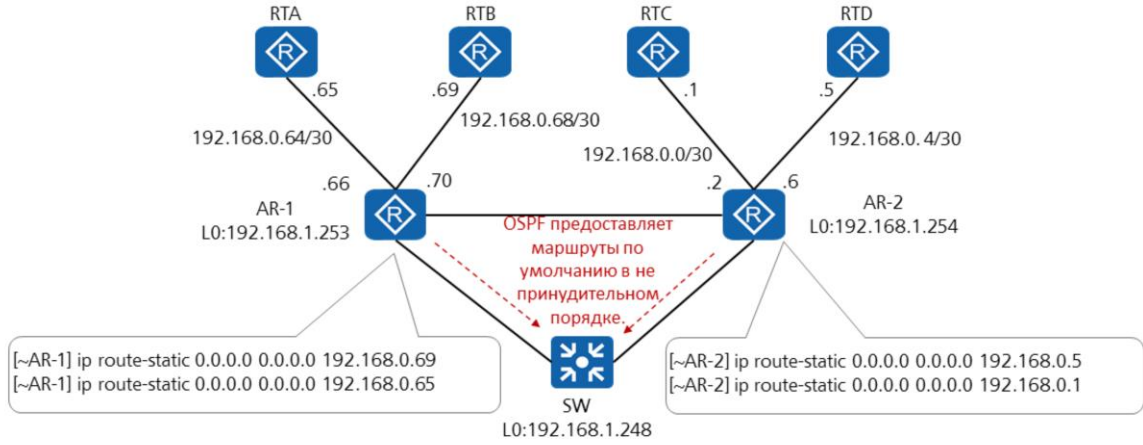
Содержание

1. **Диагностика OSPF**
   - Стандартная процедура диагностики OSPF
   - Диагностика OSPF на примерах
2. Диагностика IS-IS
3. Диагностика BGP
4. Диагностика MPLS BGP VPN

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Топология



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- AR-1 и AR-2 — это выходные маршрутизаторы в корпоративной сети. Для передачи восходящего трафика оба устройства имеют два восходящих интерфейса GE и два маршрута по умолчанию.
- Каждый маршрутизатор с помощью OSPF предоставляет маршруты по умолчанию в не принудительном порядке коммутатору агрегации SW.

Описание отказа 1

- В обычном режиме коммутатор (SW) имеет два внешних маршрута OSPF по умолчанию, направленных к двум маршрутизаторам AR.
- В следующей ситуации на SW имеется только один маршрут OSPF по умолчанию, направленный к одному из двух маршрутизаторов AR:
  - Маршрут по умолчанию к следующему транзитному узлу с адресом 192.168.0.69 на устройстве AR-1 удален, а у маршрутизатора AR-1 есть только один маршрут по умолчанию к следующему транзитному узлу с адресом 192.168.0.65. У маршрутизатора AR-2 все еще имеются два статических маршрута по умолчанию для передачи восходящего трафика.

```
[~AR-1]undo ip route-static 0.0.0.0 0.0.0.0 192.168.0.69
```

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Описание отказа 2

- Маршрут по умолчанию к следующему транзитному узлу с адресом 192.168.0.65 на устройстве AR-1 удален, а у маршрутизатора AR-1 есть только один маршрут по умолчанию к следующему транзитному узлу с адресом 192.168.0.69. У маршрутизатора AR-2 все еще имеются два статических маршрута по умолчанию для передачи восходящего трафика. В этом случае предыдущая проблема не возникает. На устройстве SW все еще имеются два маршрута по умолчанию, направленных к двум маршрутизаторам AR.
- Таким же образом, если будет удален маршрут по умолчанию к следующему транзитному узлу с адресом 192.168.0.5 на устройстве AR-2, и останется только один маршрут по умолчанию к следующему транзитному узлу с адресом 192.168.0.1 на устройстве AR-2, а у маршрутизатора AR-1 все еще будут два статических маршрута по умолчанию для передачи восходящего трафика, то на устройстве SW будет только один маршрут OSPF по умолчанию, направленный к одному из двух маршрутизаторов AR.

  ```
  [~AR-2]undo ip route-static 0.0.0.0 0.0.0.0 192.168.0.5
  ```

- Если будет удален маршрут по умолчанию к следующему транзитному узлу с адресом 192.168.0.1 на устройстве AR-2, и останется только один маршрут по умолчанию к следующему транзитному узлу с адресом 192.168.0.5 на устройстве AR-2, а у маршрутизатора AR-1 все еще будут два статических маршрута по умолчанию для передачи восходящего трафика, предыдущая проблема не возникнет. На устройстве SW все еще имеются два маршрута по умолчанию, направленных к двум маршрутизаторам AR.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Анализ отказа 1

- Проверьте функцию изучения маршрутов устройства SW, просмотрев базу данных состояний канала (LSDB). Проверьте на SW-устройстве LSA-записи маршрутов OSPF по умолчанию.

```
[~SW]display ospf lsdb ase
            OSPF Process 1 with Router ID 192.168.1.248
                 Link State Database
 Type       : External
 Ls id      : 0.0.0.0
 Adv rtr    : 192.168.1.254
 Ls age     : 482
 Len        : 36
 Options    :  E
 seq#       : 80000004
 chksum     : 0xeb78
 Net mask   : 0.0.0.0
 TOS 0  Metric: 1
 E type     : 2
 Forwarding Address : 0.0.0.0
 Tag        : 1
 Priority   : Low
```

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Анализ отказа 2

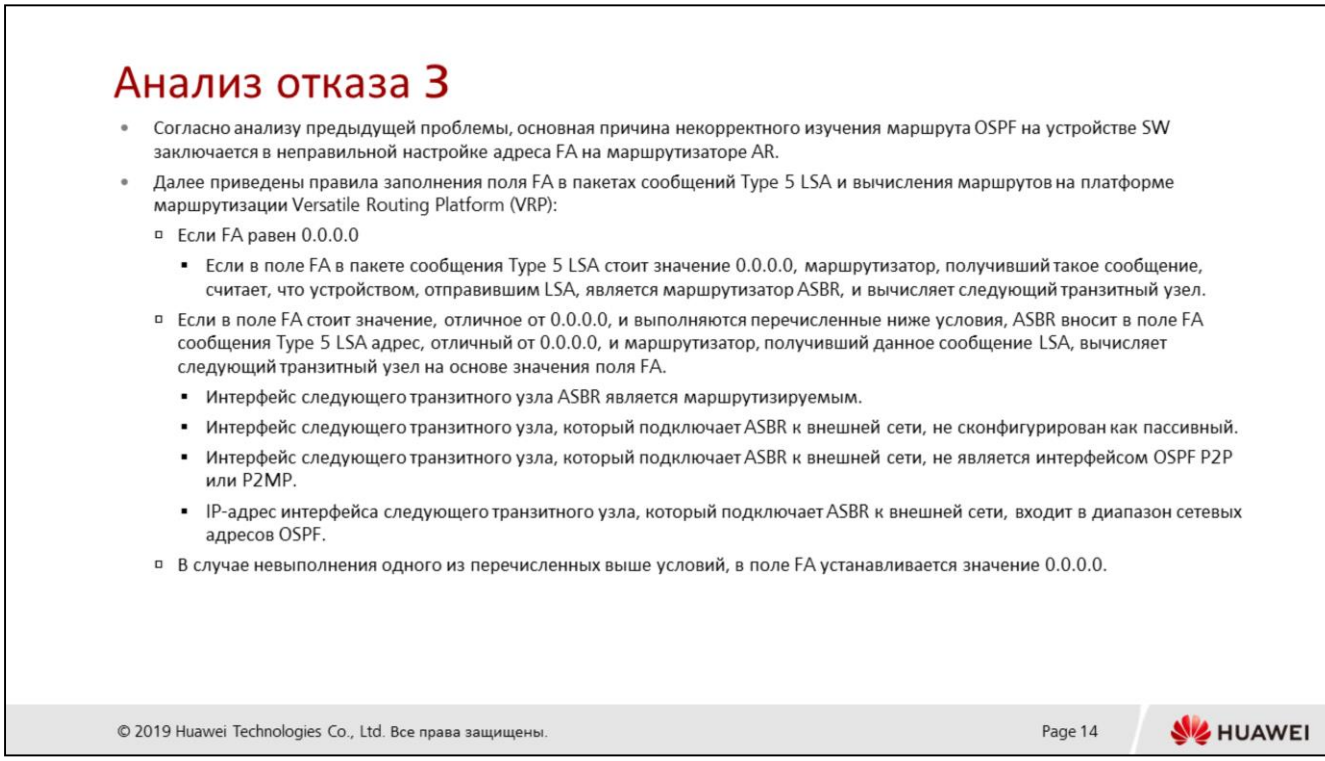
- Проверьте на SW-устройстве LSA-записи маршрутов OSPF по умолчанию.
- В приведенном командном выводе можно увидеть, что на устройстве AR-1 неправильно настроен адрес пересылки (FA). В этом случае на SW будет существовать только один маршрут OSPF по умолчанию, направленный к устройству AR-2 (IP-адрес: 192.168.1.254). Если объявления Type 5 LSA — AS-external (ASE) — имеют одинаковые значения параметров стоимости и типа внешних маршрутов (E), сравниваются стоимости внутренних маршрутов зоны, содержащиеся в данных LSA. При выборе предпочтение отдается маршруту внутри зоны с самой низкой стоимостью.

```
Type        : External
Ls id       : 0.0.0.0
Adv rtr     : 192.168.1.253
Ls age      : 149
Len         : 36
Options     :  E
seq#        : 8000000b
chksum      : 0xa50e
Net mask    : 0.0.0.0
TOS 0  Metric: 1
E type      : 2
Forwarding Address : 192.168.0.65
Tag         : 1
Priority    : Low
```

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Согласно правилам выбора маршрутов, приведенным в рекомендациях RFC 2328, если объявления Type 5 LSA — AS-external (ASE) — имеют одинаковые значения параметров стоимости и типа внешних маршрутов (E), сравниваются стоимости внутренних маршрутов зоны. В частности сравниваются стоимости маршрутов OSPF к пограничному маршрутизатору автономной системы (ASBR) или узлу с адресом пересылки (FA). Если FA равен 0, маршрут вычисляется в направлении к ASBR. Если FA не равен 0, маршрут вычисляется в направлении к узлу с данным FA. При выборе предпочтение отдается маршруту внутри зоны с самой низкой стоимостью, даже если его стоимость не будет добавлена к стоимости в таблице маршрутизации.



- Согласно анализу предыдущей проблемы, основная причина некорректного изучения маршрута OSPF на устройстве SW заключается в неправильной настройке адреса FA на маршрутизаторе AR.
- Далее приведены правила заполнения поля FA в пакетах сообщений Type 5 LSA и вычисления маршрутов на платформе маршрутизации Versatile Routing Platform (VRP):
    - Если FA равен 0.0.0.0
        - Если в поле FA пакета сообщения Type 5 LSA стоит значение 0.0.0.0, маршрутизатор, получивший такое сообщение, считает, что устройством, отправившим LSA, является объявляющий маршрутизатор (то есть ASBR), и вычисляет следующий транзитный узел.
- Если в поле FA стоит значение, отличное от 0.0.0.0, и выполняются перечисленные ниже условия, ASBR вносит в поле FA сообщения Type 5 LSA адрес, отличный от 0.0.0.0, и маршрутизатор, получивший данное сообщение LSA, вычисляет следующий транзитный узел на основе значения поля FA.
    - На интерфейсе следующего транзитного узла, который подключает ASBR к внешней сети, включен OSPF.
    - Интерфейс следующего транзитного узла, который подключает ASBR к внешней сети, не сконфигурирован как пассивный.
    - Интерфейс следующего транзитного узла, который подключает ASBR к внешней сети, не является интерфейсом OSPF P2P или P2MP.
    - IP-адрес интерфейса следующего транзитного узла, который подключает ASBR к

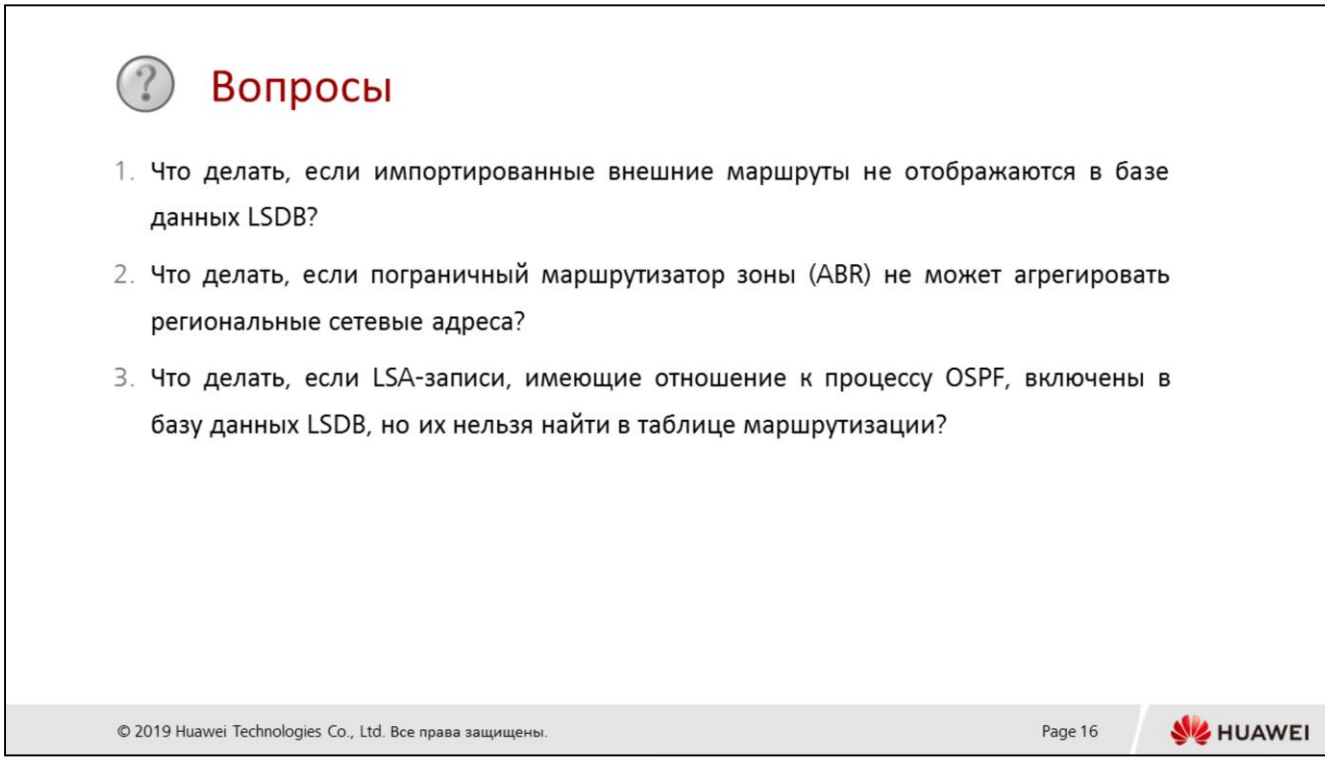
внешней сети, входит в диапазон сетевых адресов OSPF.

- В случае невыполнения одного из перечисленных выше условий, в поле FA устанавливается значение 0.0.0.0.

Диагностика и устранение отказа

- Теперь мы найдем причину неполучения ожидаемого результата вычисления маршрута OSPF, а также узнаем о правилах заполнения поля FA в пакете сообщения Type 5 LSA. Простым решением этой проблемы является устранение условий, являющихся причиной заполнения поля FA адресом, отличным от 0.0.0.0. Для этого есть три метода:
  1. Данные, сконфигурированные на AR-1 (IP-адрес: 192.168.1.253), указывают на то, что командой **network** настроен интерфейс, который запускает процесс OSPF в сетевом сегменте 192.168.0.65/30, а не в сегменте 192.168.0.68/30. Аналогично, данные, сконфигурированные на AR-2 (IP-адрес: 192.168.1.254), указывают на то, что командой **network** настроен интерфейс, который запускает процесс OSPF в сетевом сегменте 192.168.0.0/30, а не в сегменте 192.168.0.4/30. Поэтому выполните команду **undo network**, которая удалит интерфейсы, запускающие процесс OSPF в сетевых сегментах 192.168.0.65/30 и 192.168.0.4/30.
  2. В этом методе не требуется выполнять команду **undo network**, а конфигурацию в представлении OSPF не требуется изменять. Выполните команду **ospf network-type p2p** на интерфейсах AR, запускающих процесс OSPF, и на интерфейсах соседей.
  3. Настройте на устройствах AR соответствующие интерфейсы в режим молчания или сконфигурируйте на SW маршруты, направленные по адресам интерфейсов восходящей связи AR.
- После применения одного из выше перечисленных методов функция вычисления маршрутов OSPF по умолчанию на устройстве SW начнет работать в нормальном режиме.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.



- Вопрос 1. Что делать, если импортированные внешние маршруты не отображаются в базе данных LSDB?
- Ответ. Выполните следующие действия:
  - Выполните команду display ospf interface для проверки интерфейса OSPF. Убедитесь, что интерфейс не находится в состоянии Down.
  - Выполните команду display ospf brief, которая проверит маршрутизатор, импортирующий внешние маршруты, на принадлежность тупиковой зоне (Stub).
  - Если изучение внешних маршрутов осуществляется от соседних узлов, выполните команду display ospf peer, которая проверит статус соседнего узла, возможно значением является Full.
  - Проверьте, возможно сконфигурирована команда lsdb-overflow-limit, а общее число внешних маршрутов превышает максимальное значение, заданное параметром Over-Flow-Limit.
  - Выполните команду display ospf asbr-summary, которая проверит условие настройки команды asbr-summary, агрегирующей внешние маршруты.
- Вопрос 2. Что делать, если пограничный маршрутизатор зоны (ABR) не может агрегировать региональные сетевые адреса?
- Ответ. Выполните следующие действия:
  - Выполните команду display current configuration для проверки адресов

сетевого сегмента данной зоны на предмет непрерывности.

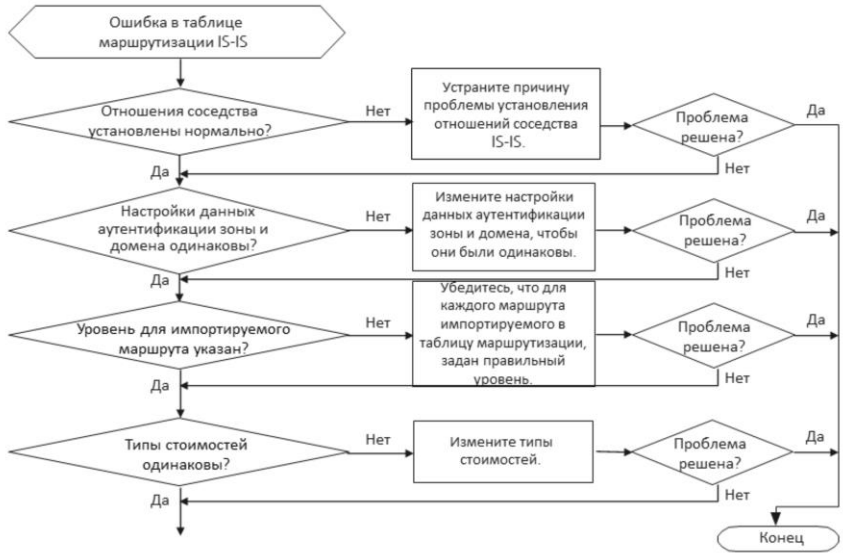
    - Если последовательность адресов прерывная, разбейте их на несколько групп, в которые будут входить непрерывные блоки сетевых адресов.
    - Выполните команду abr-summary для объединения каждой группы непрерывных сетевых адресов в единую сеть на пограничном маршрутизаторе зоны (ABR).
    - Выполните команду filter {acl | ip-prefix prefix | route-policy route-policy-name} {import | export} в представлении зоны и убедитесь, что LSA, агрегированные маршрутизатором ABR, не отфильтрованы.
- Вопрос 3. Что делать, если LSA-записи, имеющие отношение к процессу OSPF, включены в базу данных LSDB, но их нельзя найти в таблице маршрутизации?
- Ответ. Выполните следующие действия:
    - Проверьте правильность настройки IP-адреса.
    - Убедитесь, что адрес FA известен.
    - Проверьте правильность суммирования или повторного распределения маршрутов.
    - Убедитесь, что списки маршрутов объявляются.
    - Проверьте магистральную зону на предмет прерывания.

Содержание

1. Диагностика OSPF
2. **Диагностика IS-IS**
   - Стандартная процедура диагностики IS-IS
   - Диагностика IS-IS на примерах
3. Диагностика BGP
4. Диагностика MPLS BGP VPN

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

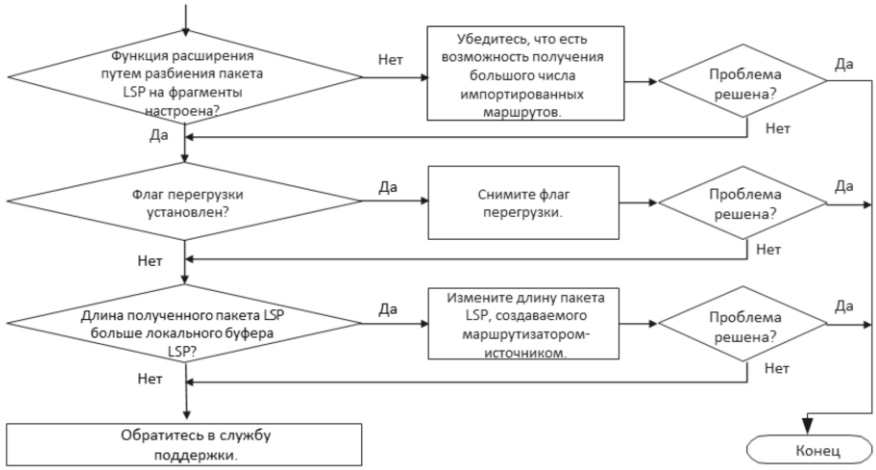
Алгоритм диагностики и устранения отказов 1



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- IS-IS и OSPF относятся к протоколам внутренних шлюзов (Interior Gateway Protocol; IGP), но IS-IS обладает очевидными преимуществами в плане масштабируемости (например, поддерживается адресация IPv6). Поэтому протокол IS-IS нашел широкое применение.
- Подробнее о процессе диагностики проблем IS-IS см. схему процесса.

Алгоритм диагностики и устранения отказов 2



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- IS-IS и OSPF относятся к протоколам внутренних шлюзов (Interior Gateway Protocol; IGP), но IS-IS обладает очевидными преимуществами в плане масштабируемости (например, поддерживается адресация IPv6). Поэтому протокол IS-IS нашел широкое применение.
- Подробнее о процессе диагностики проблем IS-IS см. схему процесса.

Процедура диагностики и устранения отказов 1

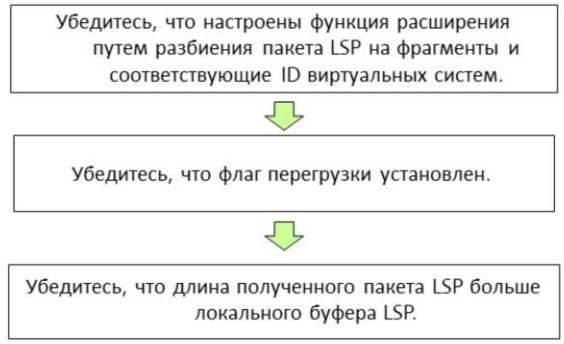


© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Шаг 1. Убедитесь, что отношения соседства установлены (состояние Up).
  - Для этого выполните команду display isis peer.
  - Если результат выполнения команды показывает, что отношения соседства находятся в состоянии Down, устраните проблему установления отношений соседства IS-IS, обратившись к инструкции.
- Шаг 2. Убедитесь, что данные аутентификации зоны и домена всех маршрутизаторов настроены одинаково.
  - Выполните команду display isis lsdb для сравнения контента баз данных LSDB двух соседних узлов.
  - Если базы LSDB не синхронизированы, убедитесь, что настройки аутентификации зоны и домена одинаковы.
- Шаг 3. Убедитесь, что для каждого маршрута импортируемого в таблицу маршрутизации, указан уровень.
  - Если маршруты импортируются в таблицу маршрутизации уровня 1 или уровня 1-2, выполните команду display this в представлении IS-IS и убедитесь, что для маршрута указан уровень.
- Шаг 4. Убедитесь, что маршрутизаторы в данной сети используют один тип стоимости.

Процедура диагностики и устранения отказов 2



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Шаг 5. Убедитесь, что настроены функция расширения путем разбиения пакета LSP на фрагменты и соответствующие ID виртуальных систем.
  - Выполните команду display isis statistics для получения количества фрагментов пакета LSP, используемых в исходной системе. Если количество достигло значения 256, необходимо сконфигурировать функции расширения путем разбиения пакета LSP на фрагменты и соответствующие ID виртуальных систем.
- Шаг 6. Убедитесь, что флаг перегрузки установлен.
  - Если данный флаг установлен, пакет LSP, генерируемый устройством, будет содержать информацию, оповещающую остальные устройства о переполнении базы данных этого устройства и невозможности пересылки пакетов. Остальные устройства не будут, в таком случае, посылать пакеты, требующие пересылки перегруженным устройством, на это устройство, если только адрес назначения пакетов не является адресом интерфейса, напрямую подключенного к устройству.
  - Флаг перегрузки снимается командой undo set-overload.
- Шаг 7. Убедитесь, что длина полученного пакета LSP больше локального буфера LSP.
  - Если длина пакетов LSP, отправленных соседом, превысит значение локального буфера LSP, локальный узел IS-IS отбросит такие пакеты.
  - Выполните команду lsp-length для изменения длины генерируемых пакетов

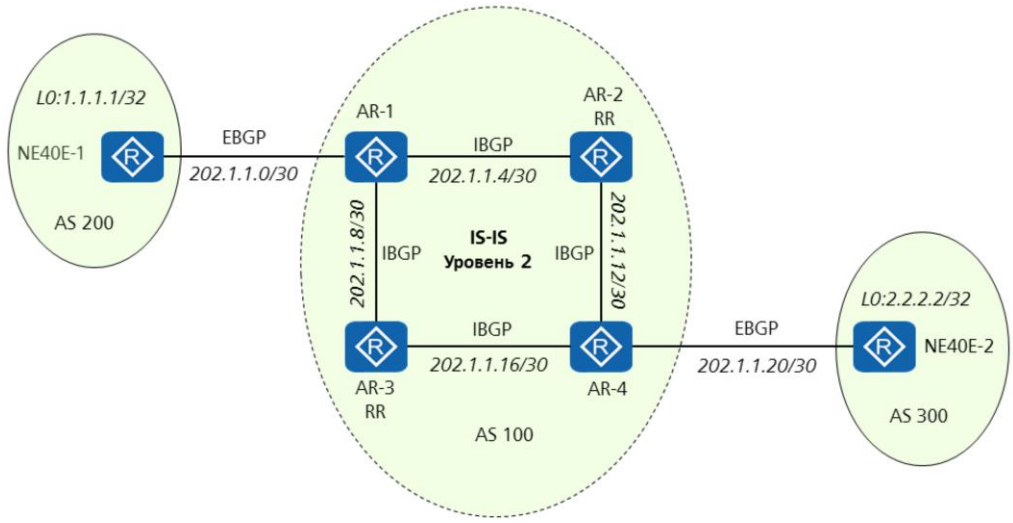
LSP или длины получаемых пакетов LSP.

Содержание

1. Диагностика OSPF
2. **Диагностика IS-IS**
   - Стандартная процедура диагностики IS-IS
   - Диагностика IS-IS на примерах
3. Диагностика BGP
4. Диагностика MPLS BGP VPN

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Топология



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

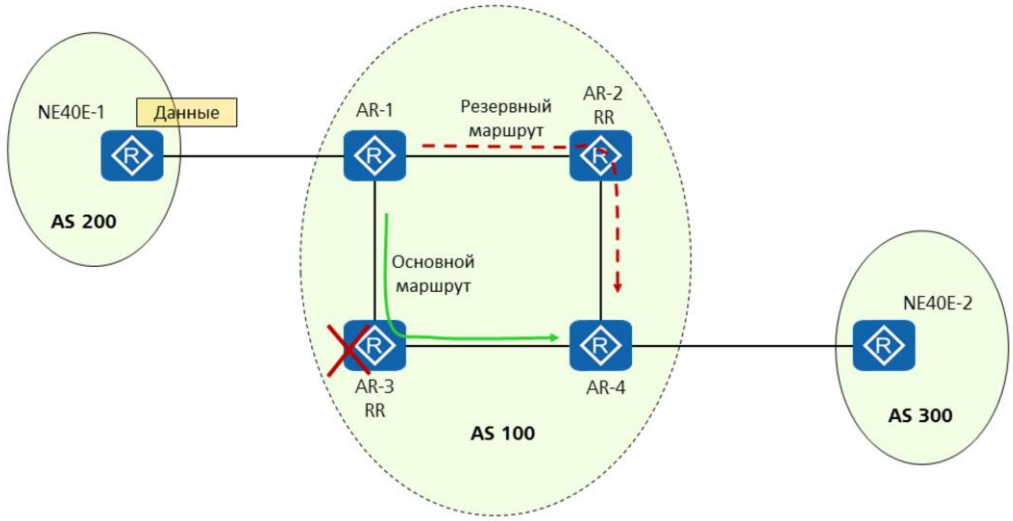
- На данной схеме изображена крупная корпоративная кампусная сеть.
- NE40E-1 принадлежит автономной системе AS 200, NE40E-2 принадлежит системе AS 300.
- Между четырьмя маршрутизаторами в системе AS 100 установлены отношения соседства IBGP. AR-2 и AR-3 являются устройствами-отражателями маршрутов (RR) BGP, выполняющими функции отражения маршрутов для устройств AR-1 и AR-4.
- Между AR-1 и AR-4 нет прямого маршрута, и пакеты BGP данных устройств должны пересылать отражатель RR.
- NE40E-1 в автономной системе AS 200 посылает данные на устройство назначения NE40E-2 по основному маршруту AR-1 – AR-3 – AR-4.
- Маршрут AR-1 – AR-2 – AR-4 является резервным.
- Настройте значение стоимости IGP таким образом, чтобы при передаче трафика BGP предпочтение отдавалось маршруту AR-1 – AR-3 – AR-4.

Описание отказа

- После возникновения проблемы устройство AR-3 перезапустилось. Сходимость маршрутов IS-IS прошла быстро, и устройство AR-1 передало пакеты BGP устройству AR-2.
- После перезапуска AR-3 передача трафика, идущего от AR-1 к AR-4, была остановлена и через несколько минут возобновлена.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Моделирование отказа



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Анализ отказа 1

- Если на устройстве AR-3 обновлены сервисы, проверьте таблицу маршрутизации AR-1. Согласно информации командного вывода, AR-1 выбирает резервный маршрутизатор IS-IS — устройство AR-2 (IP-адрес: 202.1.1.6).

```
[~AR-1]display ip routing-table 2.2.2.2 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1

  Destination: 2.2.2.2/32
     Protocol: BGP             Process ID: 0
   Preference: 255                   Cost: 0
      NextHop: 10.1.1.4        Neighbour: 10.1.1.2
        State: Active Adv Relied      Age: 00h00m01s
          Tag: 0                 Priority: low
        Label: NULL              QoSInfo: 0x0
   IndirectID: 0x2
RelayNextHop: 202.1.1.6        Interface: Ethernet0/0/0
     TunnelID: 0x0                 Flags: RD
```

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Анализ отказа 2

- После выполнения перезапуска AR-3 проверьте таблицу маршрутизации AR-1 еще раз. Согласно информации командного вывода, AR-1 выбирает активный маршрутизатор IS-IS — устройство AR-3 (IP-адрес: 202.1.1.10).

```
[~AR-1]display ip routing-table 2.2.2.2 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1

Destination: 2.2.2.2/32
    Protocol: BGP              Process ID: 0
  Preference: 255                  Cost: 0
     NextHop: 10.1.1.4         Neighbour: 10.1.1.2
       State: Active Adv Relied      Age: 00h04m34s
         Tag: 0                  Priority: low
       Label: NULL               QoSInfo: 0x0
  IndirectID: 0x2
RelayNextHop: 202.1.1.10       Interface: Ethernet0/0/4
    TunnelID: 0x0                  Flags: RD
```

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Анализ отказа 3

- Однако сходимость трафика BGP на устройстве AR-3 не выполнена. В результате пакеты данных этим устройством отбрасываются.

```
[~AR-3]display isis peer

                    Peer information for ISIS(1)

System Id          Interface   Circuit Id                State  HoldTime Type    PRI
------------------------------------------------------------------------------
0001.0001.0001  Eth0/0/2  0003.0003.0003.01 Up   2s         L2       64
0004.0004.0004  Eth0/0/3  0003.0003.0003.02 Up   1s         L2       64

                                                                  Total Peer(s): 2

                                                                <AR-3>display bgp peer

 BGP local router ID : 10.1.1.3
 Local AS number : 100
 Total number of peers : 2              Peers in established state : 0

  Peer        V   AS  MsgRcvd  MsgSent  OutQ  Up/Down      State PrefRcv

  10.1.1.1  4   100     0              0              0  00:00:26      Idle      0
  10.1.1.4  4   100     0              0              0  00:00:26      Idle      0
```

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

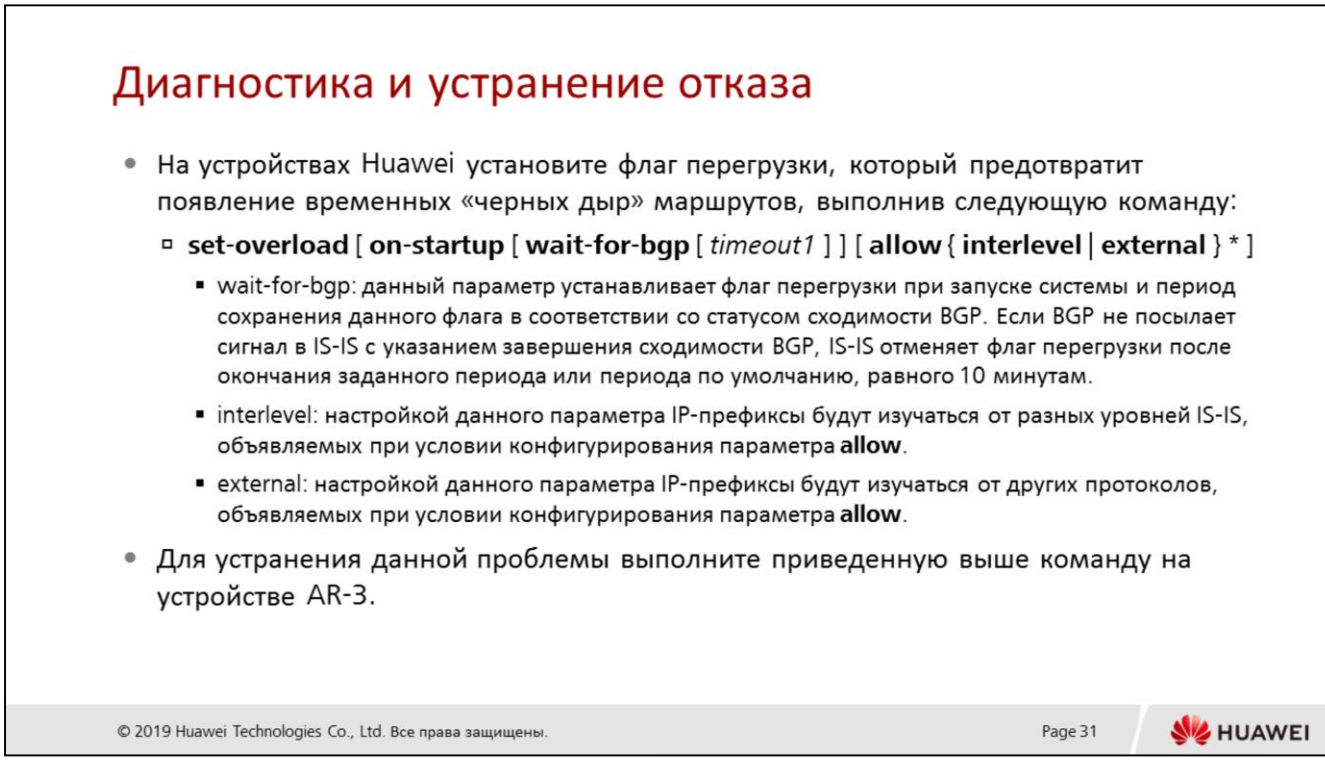
Анализ отказа 4

- Причина отказа следующая:
  - После перезапуска и восстановления работы AR-3 (в течение нескольких секунд) между устройствами AR-1, AR-4 и AR-3 были установлены отношения соседства IS-IS, и в течение нескольких секунд была выполнена синхронизация данных. Далее была обновлена информационная база пересылки (FIB) устройства AR-1, и трафик, отправленный устройству NE40E-2, был передан маршрутизатору AR-3 устройством AR-1. Однако сходимость маршрутов BGP выполнялась настолько медленно, что маршрутизатор AR-3 не смог изучить информацию о маршруте BGP к устройству NE40E-2. В результате маршрутизатор AR-3 отбросил пакеты, предназначенные устройству NE40E-2, и была создана временная «черная дыра» маршрута.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- После восстановления работы AR-3 между устройствами AR-1, AR-4 и AR-3 были установлены отношения соседства IS-IS, и за несколько секунд была выполнена синхронизация данных. Далее была обновлена информационная база пересылки (FIB) устройства AR-1, и трафик, отправленный устройству NE40E-2, был передан маршрутизатору AR-3 устройством AR-1. Однако сходимость маршрутов BGP выполнялась настолько медленно, что маршрутизатор AR-3 не смог изучить информацию о маршруте BGP к устройству NE40E-2. В результате маршрутизатор AR-3 отбросил пакеты, предназначенные устройству NE40E-2, и была создана временная «черная дыра» маршрута.



- На устройствах Huawei установите флаг перегрузки, который предотвратит появление временных «черных дыр» маршрутов, выполнив следующую команду: set-overload [on-startup [wait-for-bgp [timeout1]] [allow { interlevel | external } *]
  - wait-for-bgp: данный параметр устанавливает флаг перегрузки при запуске системы и период сохранения данного флага в соответствии со статусом сходимости BGP. Если BGP не посылает сигнал в IS-IS с указанием завершения сходимости BGP, IS-IS отменяет флаг перегрузки после окончания заданного периода или периода по умолчанию, равного 10 минутам.
  - interlevel: настройкой данного параметра IP-префиксы будут изучаться от разных уровней IS-IS, объявляемых при условии конфигурирования параметра allow.
  - external: настройкой данного параметра IP-префиксы будут изучаться от других протоколов, объявляемых при условии конфигурирования параметра allow.
- Для устранения данной проблемы выполните приведенную выше команду на устройстве AR-3.



Вопросы

1. Маршрутизатор соединен с другими маршрутизаторами физическими каналами. Однако в результатах выполнения команды **display isis peer** отсутствует информация о соседнем узле. Как решить такую проблему?
2. Маршрутизатор уровня 1 не может создать маршруты по умолчанию, направленные в другие зоны. Как проанализировать проблему?
3. Протокол IS-IS некорректно изучает маршруты. Каковы возможные причины?

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Вопрос 1. Маршрутизатор соединен с другими маршрутизаторами физическими каналами. Однако в результатах выполнения команды display isis peer отсутствует информация о соседнем узле. Как решить такую проблему?
- Ответ. Возможные причины: проблема установления соседства может быть вызвана тем, что маршрутизаторы на противоположных узлах работают на разных уровнях, или у них настроены разные идентификаторы зон, типы аутентификации интерфейсов или пароли. Проблема может возникнуть, даже если у них один ID системы.
- Вопрос 2. Маршрутизатор уровня 1 не может создать маршруты по умолчанию, направленные в другие зоны. Как проанализировать проблему?
- Ответ. Маршрутизатор уровня 1 может создавать маршрут в другие зоны только после установления отношений соседства уровня 1 с маршрутизатором уровня 1-2, находящимся в локальной зоне. Если маршрутизатор уровня 1-2 на границе зоны имеет соседей уровня 2 в других зонах, в генерируемом пакете LSP устанавливается флаг Attachment (ATT). Это означает, что маршрутизатор уровня 1-2 подключен к другим зонам и имеет маршруты в такие зоны. Получив пакет LSP, все маршрутизаторы уровня 1 в той же зоне создают маршрут по умолчанию, направленный по адресу 0.0.0.0 0.
- Вопрос 3. Протокол IS-IS некорректно изучает маршруты. Каковы возможные причины?
- Ответ. Возможные причины:
  - Проблема установления отношений соседства.
  - Отличаются типы стоимости, используемые противоположными узлами.
  - Отсутствует следующий транзитный узел по причине различия топологий IPv4 и IPv6.
  - Маршрут отфильтровывается политикой маршрутизации, и его нельзя добавить в таблицу одноадресной маршрутизации (Unicast Routing Table; URT).
  - LSP-ID использован, что приводит к потере Neighbor TLV. Если количество импортируемых маршрутов слишком большое, а число использованных фрагментов LSP достигло 255, необходимо сконфигурировать функцию расширения путем разбиения пакета LSP на фрагменты.

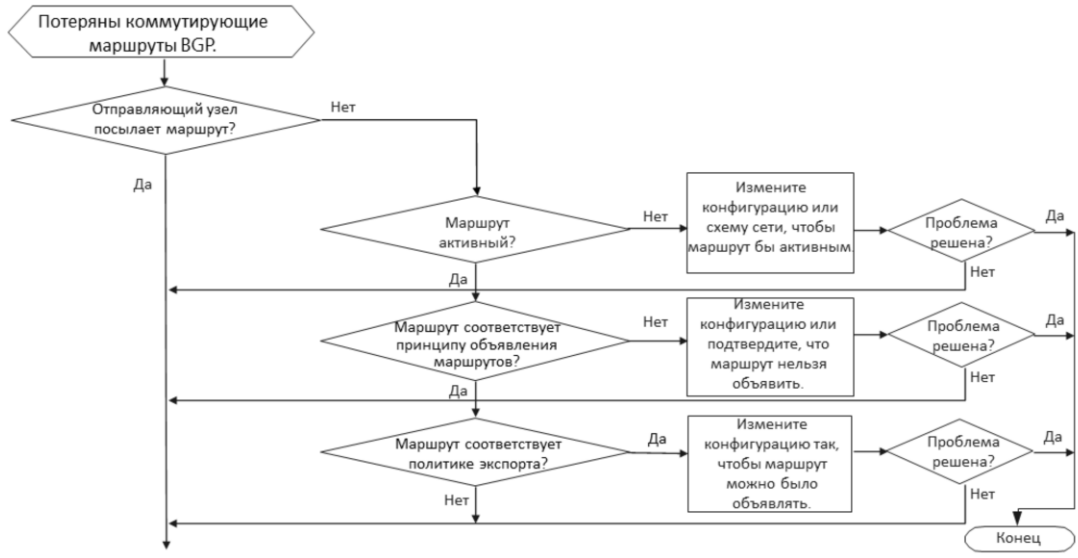
- Настроенные на маршрутизаторе домен и зона не могут пройти процедуру аутентификации. В результате база LSDB не синхронизирована.

Содержание

1. Диагностика OSPF
2. Диагностика IS-IS
3. **Диагностика BGP**
   - Стандартная процедура диагностики BGP
   - Диагностика BGP на примерах
4. Диагностика MPLS BGP VPN

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Алгоритм диагностики и устранения отказов 1



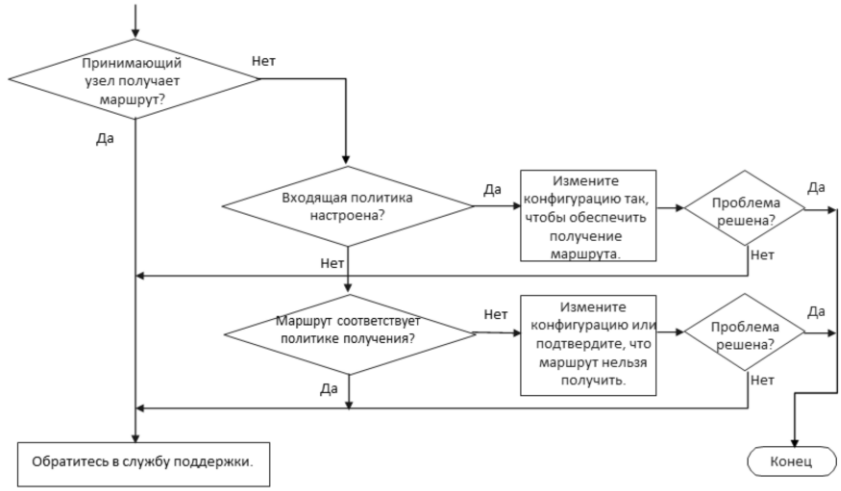
© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- BGP — это протокол динамической маршрутизации, используемый между AS-системами. BGP обеспечивает обмен информацией о достижимых маршрутах между AS-системами. BGP имеет следующие преимущества перед IGP:
  - Как протокол внешнего шлюза, BGP выбирает оптимальные маршруты между AS-системами и объявляет данные маршруты.
  - BGP гибко фильтрует и выбирает маршруты, применяя различные политики маршрутизации.
  - BGP предотвращает нестабильность (flapping) маршрутов, что повышает устойчивость интернет-сети.
  - BGP легко расширяется, что позволяет адаптироваться в условиях развития сетей.

- Проблемы BGP классифицируются на проблемы, связанные с соседством BGP, и проблемы, связанные с изучением маршрутов BGP. На схеме показан процесс изучения маршрутов BGP.
  - BGP — это протокол, управляющий процессом передачи информации о маршруте. Проблемы, связанные с изучением маршрута, можно разделить на проблемы посылки маршрута и проблемы получения маршрута.
  - Если отправляющее устройство работает нормально, проверьте принимающее устройство.

Алгоритм диагностики и устранения отказов 2

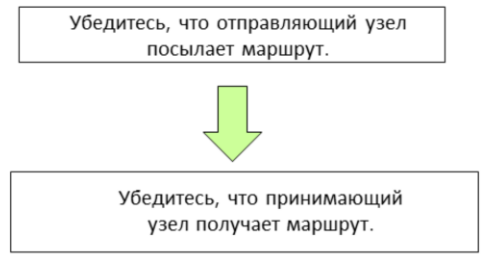


© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Если оба устройства — отправляющее и принимающее — работают нормально, но изучение маршрутов BGP так и не происходит, обратитесь в службу техподдержки Huawei.

Процедура диагностики и устранения отказов



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Шаг 1. Убедитесь, что отправляющий узел посылает маршрут.
  - Для этого выполните команду display bgp routing-table peerpeer-addressadvertised-routes.
  - Если маршруты с отправителя не посылаются, выполните следующие операции:
    - Убедитесь, что локальный маршрут находится в активном состоянии. Для этого выполните команду display bgp routing-table. То есть проверьте наличие тега *> у данного маршрута. Если локальный маршрут находится в неактивном состоянии, следующий транзитный узел недостижим, или же на локальном узле существуют другие приоритетные маршруты.
    - Проверьте, возможно не соблюдается принцип объявления маршрутов. Маршруты, подавляемые в результате процедуры сходимости, не освобождаются внешне. Результат выполнения команды display bgp routing-table показывает, что у маршрутов имеется тег s. Маршруты, подавляемые в результате заморозки (Dampening), также не освобождаются внешне. Результат выполнения команды display bgp routing-table показывает, что у маршрутов имеется флаг d. Маршруты, изучаемые от соседнего узла IBGP, не передаются на такой узел.
    - Убедитесь, что для фильтрации объявляемых маршрутов настроена политика экспорта. BGP может использовать следующие фильтры: IP-Prefix List (фильтр списка префиксов), AS_Path Filter (фильтр списка маршрутов), Community Filter и Route-Policy (фильтры списка атрибутов

сообщества). Данные фильтры применимы к маршрутной информации, получаемой от соседей IBGP или объявляемых соседям IBGP.

- Выполните команду display current-configuration configuration bgp для просмотра конфигурационной информации.

- Выполните команду display current-configuration configuration bgp для просмотра конфигурационной информации.
- Шаг 2. Убедитесь, что принимающий узел получает маршрут.
    - Для этого выполните команду **display bgp routing-table peer** *peer-address* **received-routes**.
    - Если принимающий узел не получает ни одного маршрута, выполните следующие операции:
        - Убедитесь, что для фильтрации получаемых маршрутов настроена политика импорта. Выполните команду **display current-configuration configuration bgp** для просмотра конфигурационной информации.
        - Проверьте, возможно не соблюдается принцип получения маршрутов. Отбрасываются маршруты в следующих случаях: 1. Команда **peer allow-as-loop** не сконфигурирована, и номер локальной автономной системы включен в атрибуты AS_Path получаемого маршрута. 2. Команда **peer allow-as-loop [~** *number* **]** сконфигурирована. Число повторов номера AS в атрибутах AS_Path превышает заданное значение (по умолчанию: 1). 3. Номер первой AS в атрибутах AS_Path, полученных от соседа EBGP, не является номером AS соседнего узла. 4. Идентификаторы Originator_ID и local Router-ID совпадают или имеют недействительное значение 0.0.0.0. 5.

Список кластеров (Cluster-List) маршрута, полученного от отражателя, содержит идентификатор локального кластера (local Cluster-ID). 6. Агрегатор имеет недействительное значение 0.0.0.0. 7. Адресом следующего транзитного узла (Next_Hop) является адрес локального интерфейса. 8. Адрес следующего транзитного узла (Next_Hop) маршрута, полученного от прямого соседа EBGP, недостижим. 9. При применении команды **peer route-limit alert-only** все получаемые маршруты будут отбрасываться, как только будет достигнуто пороговое значение.

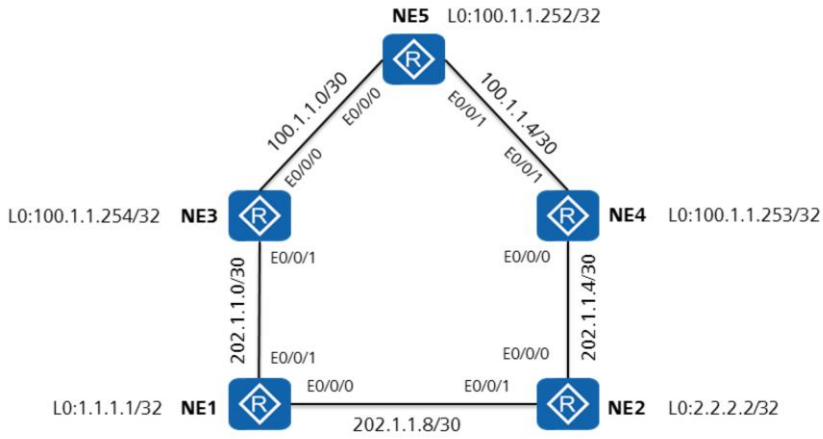
- Если проблема не будет устранена после выполнения выше описанных операций, обратитесь в службу технической поддержки Huawei.

Содержание

1. Диагностика OSPF
2. Диагностика IS-IS
3. **Диагностика BGP**
   - Стандартная процедура диагностики BGP
   - Диагностика BGP на примерах
4. Диагностика MPLS BGP VPN

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Топология



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- На схеме изображена сетевая топология, включающая граничные маршрутизаторы в сети IP MAN или магистральной сети. NE1 и NE2 — это граничные маршрутизаторы в автономной системе AS 200 в сети IP MAN, а NE3, NE4 и NE5 в системе AS 100 являются граничными маршрутизаторами региональной магистральной сети. NE1 и NE2 с помощью команды network объявляют маршруты своим соседям EBGP — маршрутизаторам NE3 и NE4. NE3 и NE4 устанавливают отношения соседства IBGP с маршрутизатором NE5. NE5 функционирует как отражатель маршрутов (RR), а устройства NE3 и NE4 являются его клиентами. Настройте виртуальный адрес 202.105.0.5 следующего транзитного узла на NE3 и NE4, чтобы данные устройства изменили следующий транзитный узел маршрутов на узел с адресом 202.105.0.5, перед тем, как начнут объявлять маршруты своему соседу IBGP — маршрутизатору NE5.

Описание отказа

- Если соединение между NE1 и NE3 прерывается, между устройствами NE3 и NE5 возникает петля.

```
[~NE3]tracert 202.1.1.11
traceroute to  202.1.1.11(202.1.1.11), max hops: 30 ,packet length: 40
1 100.1.1.2 40 ms  30 ms  50 ms
2 100.1.1.5 60 ms 100.1.1.1 50 ms  50 ms
3 100.1.1.2 60 ms  60 ms  80 ms
4 * * *
5  *  * 100.1.1.2 90 ms
6 100.1.1.1 80 ms  90 ms  100 ms
7 100.1.1.2 110 ms  110 ms  *
```

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Если соединение между NE1 и NE3 прерывается, то при попытке устройства NE3 получить доступ к узлу с IP-адресом в сетевом сегменте 202.1.1.0/24 возникает петля. Предположим, NE3 получает доступ к 202.1.1.11, последовательность будет выглядеть так, как представлена на рисунке.

Анализ отказа 1

- Проверьте на устройстве настройки BGP, связанные с изучением маршрутов и передачей этой информации.
- Проверьте конфигурацию устройства NE1. В результате проверки может выясниться, что NE1 объявляет маршрут своему соседу EBGP — устройству NE3 — используя маршрут «черная дыра» и режим network. Настройки на устройстве NE2 такие же, как и на NE1.

```
[~NE1]display  current-configuration  configuration bgp
bgp 200
 ……
 ipv4-family unicast
  undo synchronization
  network 202.1.1.0
  peer 2.2.2.2 enable
  peer 2.2.2.2 next-hop-local
  peer 202.1.1.1 enable

[~NE1]display current-configuration  | include  route-static
 ip route-static 202.1.1.0 255.255.255.0 NULL0
```

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- 202.1.1.0/24 — это смоделированный пул адресов пользователей в сетевом сегменте.

Анализ отказа 2

- Проверьте конфигурацию BGP устройства NE3.

```
[~NE3]display current-configuration  configuration bgp
#
bgp 100
 peer 100.1.1.252 as-number 100
 peer 100.1.1.252 connect-interface LoopBack0
 peer 202.1.1.2 as-number 200
 #
 ipv4-family unicast
  undo synchronization
  peer 100.1.1.252 enable
  peer 100.1.1.252 route-policy vir-add-bgp export
  peer 202.1.1.2 enable
#
Return
```

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Анализ отказа 3

- На устройстве NE3 сконфигурирована политика, которая принудительно заменяет адрес следующего транзитного узла BGP виртуальным адресом 202.105.0.5.

```
[~NE3] display  route-policy  vir-add-bgp
Route-policy : vir-add-bgp
  permit : 10
    Apply clauses :
      apply ip-address next-hop 202.105.0.5
[~NE3]display  this
#
 sysname NE3
isis 1
Import-route static
preference 100
……
 ip route-static 202.105.0.5 255.255.255.255 100.1.1.2
```

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Адресом следующего узла после виртуального является IP-адрес 100.1.1.2 взаимосвязи устройств NE5 и NE3.

Анализ отказа 4

- Проверьте таблицу маршрутизации на устройстве NE3.

```
[~NE3]display ip routing-table 202.1.1.0 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1

Destination: 202.1.1.0/24
    Protocol: BGP              Process ID: 0
  Preference: 255                    Cost: 0
     NextHop: 202.105.0.5      Neighbour: 100.1.1.252
       State: Active Adv Relied      Age: 00h00m00s
         Tag: 0                  Priority: low
       Label: NULL               QoSInfo: 0x0
  IndirectID: 0x5
RelayNextHop: 100.1.1.2          Interface: Ethernet0/0/1
    TunnelID: 0x0                Flags: RD
```

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Поскольку соединение между NE1 и NE3 прервано, маршруты на NE3 объявляются устройством NE4, отражаются RR-отражателем и имеют исходящий интерфейс на NE5.

Анализ отказа 5

- Проверьте таблицу маршрутизации на устройстве NE5. Из таблицы видно, что у NE5 есть маршрут, направленный к NE3. Поэтому возникает маршрутная петля.

```
[~NE5]display  ip routing-table 202.1.1.0
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

        202.1.1.0/24  BGP    255  0           RD  202.105.0.5     Ethernet0/0/0
                      BGP    255  0           RD  202.105.0.5     Ethernet0/0/1
[~NE5]display  ip routing-table  202.105.0.5
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
Destination/Mask  Proto  Pre  Cost      Flags NextHop         Interface

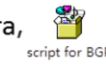
     202.105.0.5/32  ISIS     15   74          D   100.1.1.5       Ethernet0/0/0
                     ISIS     15   74          D   100.1.1.1       Ethernet0/0/1
```

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Проверьте на устройстве NE5 маршруты, направленные к NE3. Из информации командного вывода видно, что следующим транзитным узлом данных маршрутов является узел с виртуальным IP-адресом 202.105.0.5. Проверьте на устройстве NE5 маршруты, исходящие из узла с адресом 202.105.0.5. Из информации командного вывода видно, что существуют два маршрута равной стоимости, направленные на устройства NE3 и NE4.
- у NE3 есть маршрут, направленный к NE5, а у NE5 есть маршрут, направленный к NE3. Поэтому возникает маршрутная петля.

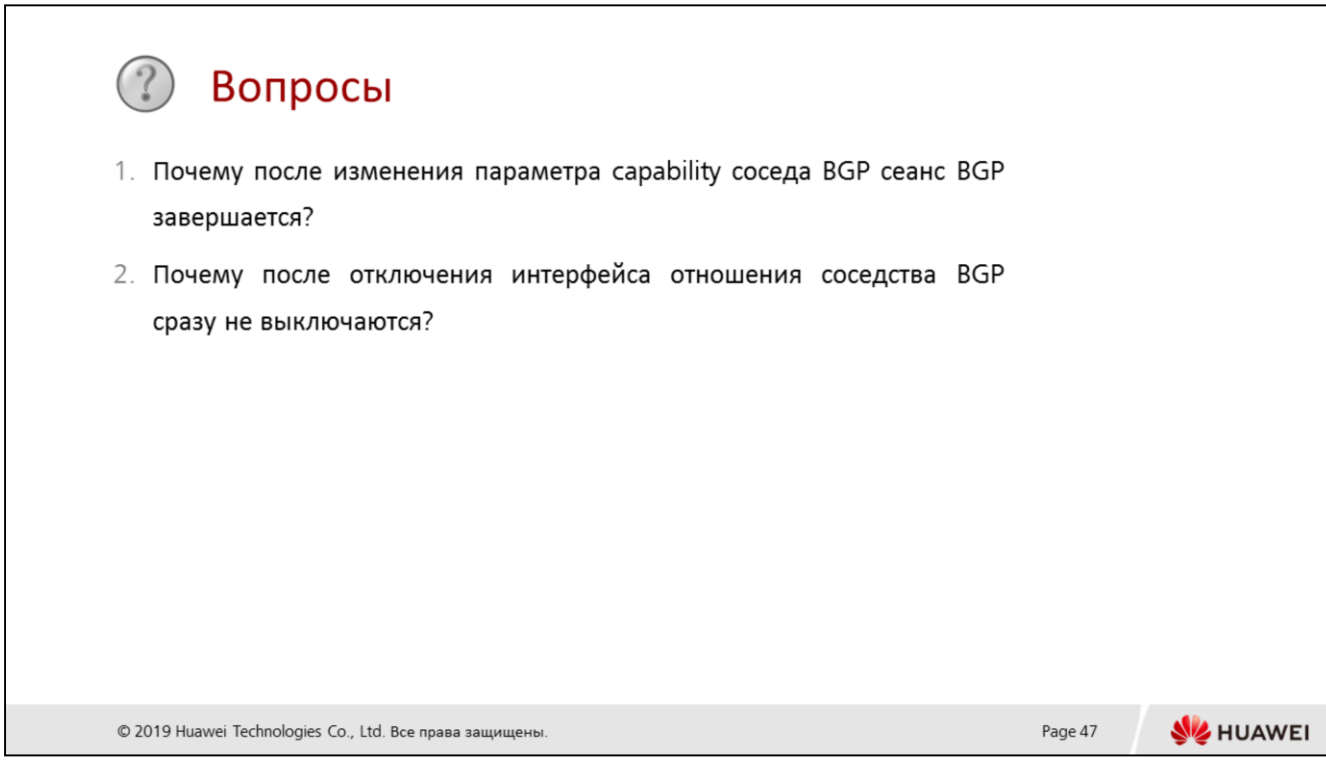
Диагностика и устранение отказа

1. Согласно маршрутной информации на устройствах, основная причина возникновения петли заключается в том, что статический маршрут, направленный по виртуальному адресу 202.105.0.5, объявляется устройством NE3 через IS-IS маршрутизатору NE5.
2. Если на NE3 сконфигурирован статический маршрут, адресом следующего транзитного узла будет 100.1.1.2. Поэтому статический маршрут будет импортироваться в IS-IS, даже если интерфейс Ethernet0/0/0 данного канала перейдет в состояние DOWN.
3. Измените адрес следующего транзитного узла статического маршрута, направленного по виртуальному адресу 202.1.1.2 на NE3.




```
[~NE3]ip route-static 202.105.0.5 255.255.255.255 202.1.1.2
```

© 2019 Huawei Technologies Co., Ltd. Все права защищены.



- Вопрос 1. Почему после изменения параметра capability соседа BGP сеанс BGP завершается?
- Ответ. Сеанс BGP завершается автоматически после изменения настроек параметра capability BGP. Это происходит потому, что BGP не поддерживает динамический режим согласования возможностей (capability). Возможности соседнего узла согласуются в этом случае повторно. Сеанс BGP завершается автоматически после выполнения следующих действий:
  - Включение или выключение параметра Label-Route-Capability.
  - Активация или деактивация соседа BGP в семействе адресов. Например, если в отношении семейства адресов VPNv4 применяется команда **peer enable/undo peer enable**, сеанс BGP с соседом из другого семейства адресов завершается автоматически.
  - Включение параметра capability GR.
- Вопрос 2. Почему после отключения интерфейса отношения соседства BGP сразу не выключаются?
- Ответ. Отношения соседства EBGP отключаются сразу же после выключения интерфейса, только если соседи EBGP подключены напрямую, и в представлении BGP применена команда **ebgp-interface-sensitive**. Данная команда используется по умолчанию. В противном случае, отношения соседства BGP не перейдут в состояние down, пока не истечет время ожидания.

Содержание

1. Диагностика OSPF
2. Диагностика IS-IS
3. Диагностика BGP
4. **Диагностика MPLS BGP VPN**
   - Диагностика MPLS BGP VPN
   - Диагностика MPLS BGP VPN на примерах

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

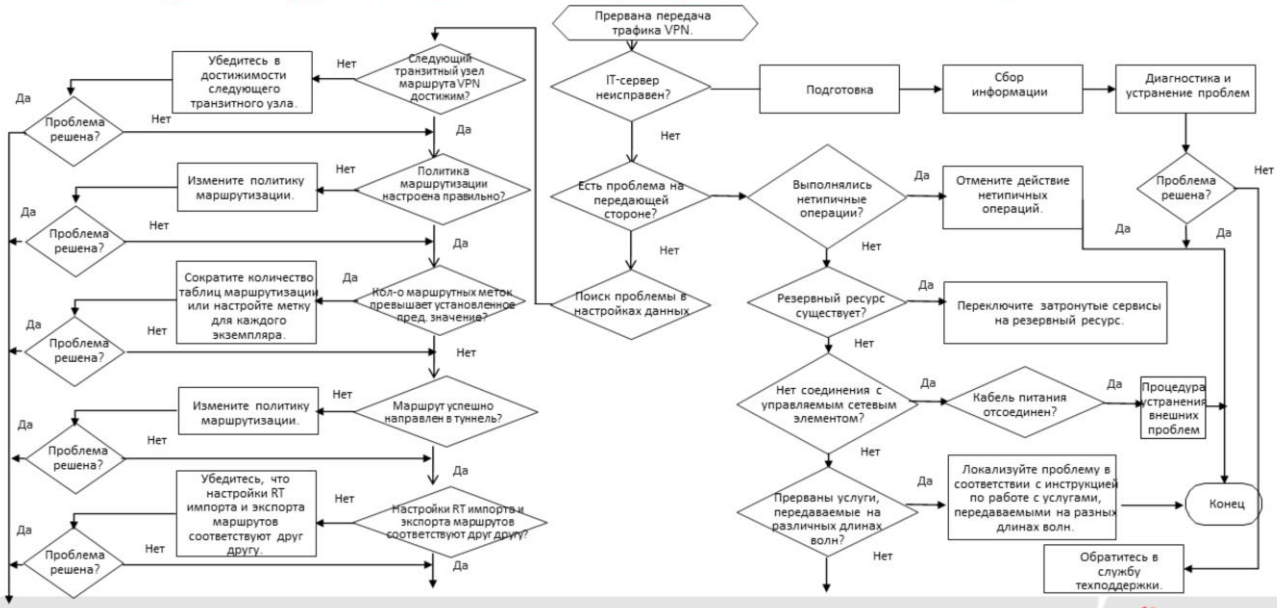
Причины общих проблем

- Маршруты неактивны, поскольку их следующие транзитные узлы недостижимы.
- Проблемы объявления или получения маршрутов связаны с неправильной настройкой политик маршрутизации.
- Проблемы объявления маршрутов VPN связаны с превышением количеством меток установленного верхнего предельного значения.
- Маршруты VPN неактивны, поскольку их невозможно направить к туннелям.
- Проблемы добавления маршрутов в таблицу маршрутизации VPN связаны с несоответствием настроек RT импорта маршрутов настройкам RT экспорта маршрутов.
- Проблема отбрасывания полученных маршрутов связана с верхним предельным значением, устанавливаемым для количества маршрутов, которые может получить устройство.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

Алгоритм диагностики и устранения отказов



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Алгоритм диагностики и устранения отказов



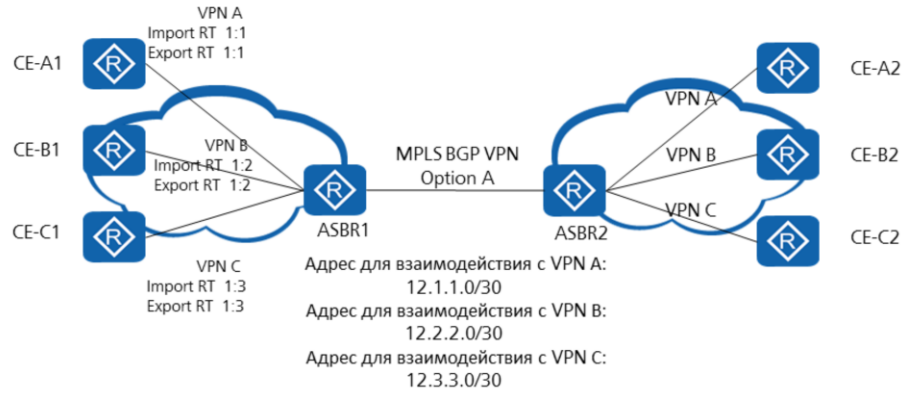
© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Содержание

1. Диагностика OSPF
2. Диагностика IS-IS
3. Диагностика BGP
4. **Диагностика MPLS BGP VPN**
   - Диагностика MPLS BGP VPN
   - Диагностика MPLS BGP VPN на примерах

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

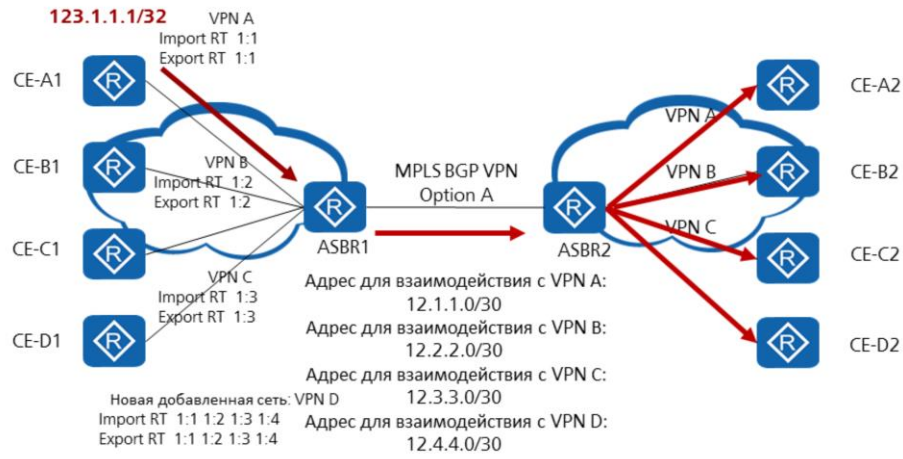
Топология



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- В сети одной компании есть три экземпляра L3 VPN: VPN A, VPN B и VPN C. Идентификаторами маршрутов (Route Distinguisher) данных экземпляров являются 1:1, 1:2 и 1:3 соответственно, а идентификаторами правил импорта и экспорта маршрутов VPN (Route Target) являются 1:1, 1:2 и 1:3 соответственно. Три сети VPN, таким образом, изолированы друг от друга и не могут взаимодействовать друг с другом.
  Согласно схеме, CE-A1, CE-B1 и CE-C1 подключены к VPN A, VPN B и VPN C маршрутизатора ASBR1 соответственно. CE-A2, CE-B2 и CE-C2 подключены к VPN A, VPN B и VPN C маршрутизатора ASBR2 соответственно. Между маршрутизаторами ASBR1 и ASBR2 сконфигурирован режим подключения Inter-AS MPLS BGP VPN Option A. В этом случае только CE-A2 может получать маршруты, объявляемые CE-A1, чем достигается изоляция между экземплярами VPN.

Описание отказа



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- В связи с расширением сервисов компания решила сконфигурировать в сети новую VPN D. Необходимо было сохранить изолированность VPN A, VPN B и VPN C по отношению друг к другу, но при этом обеспечить возможность взаимодействия VPN D с каждой из этих виртуальных сетей. Поэтому параметр Route Distinguisher сети VPN D установлен в значение 1:4, а параметр Route Target VPN — в значения 1:1 1:2 1:3 1:4. Между маршрутизаторами ASBR1 и ASBR2 сконфигурирован режим подключения Inter-AS MPLS BGP VPN Option A.
  Однако в этом случае CE-B2 и CE-C2 смогут также изучать маршруты от CE-A1. В действительности, после настройки режима Inter-AS MPLS BGP VPN Option A у каждой VPN появилась возможность изучать маршруты от других VPN. Настроенная ранее изоляция этих виртуальных сетей стала недействительной.

Анализ отказа (1/6)

- Выберите неисправный маршрут (123.1.1.1/32) и убедитесь, что на устройстве ASBR1 локальное пересечение маршрута находится в нормальном состоянии.

```
<~ASBR1>display bgp vpnv4 all routing-table 123.1.1.1 32
 BGP local router ID : 1.1.1.1
Local AS number : 100
Total routes of Route Distinguisher(1:1): 1
BGP routing table entry information of 123.1.1.1/32:
From: 10.1.1.1 (10.1.1.1)
Route Duration: 00h02m09s
Direct Out-interface: Ethernet0/0/0
Original nexthop: 10.1.1.1
Qos information : 0x0
Ext-Community:RT <1 : 1>
AS-path 1000, origin igp, MED 0, pref-val 0, valid, external, best, select, pre
255
Not advertised to any peer yet
VPN-Instance vpna, Router ID 1.1.1.1:
Total Number of Routes: 1
BGP routing table entry information of 123.1.1.1/32:
From: 10.1.1.1 (10.1.1.1)
.....
```

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Анализ отказа (2/6)

```
Route Duration: 00h15m07s
 Direct Out-interface: Ethernet0/0/0
 Original nexthop: 10.1.1.1
 Qos information : 0x0
 AS-path 1000, origin igp, MED 0, pref-val 0, valid, external, best, select, act
ive, pre 255
 Advertised to such 2 peers:
   10.1.1.1
   12.1.1.2        // Маршрут объявляется устройству ASBR2 через соседа Option A (12.1.1.2) виртуальной сети VPN A.
VPN-Instance vpnd, Router ID 1.1.1.1:
Total Number of Routes: 1
BGP routing table entry information of 123.1.1.1/32:
From: 10.1.1.1 (10.1.1.1)
Route Duration: 00h15m07s
Direct Out-interface: Ethernet0/0/0
Original nexthop: 10.1.1.1
Qos information : 0x0
Ext-Community:RT <1 : 1>
AS-path 1000, origin igp, MED 0, pref-val 0, valid, external, best, select, act
ive, pre 255
 Advertised to such 2 peers:
   40.1.1.1
   12.4.4.2        // Маршрут объявляется устройству ASBR2 через соседа Option A (12.4.4.2) виртуальной сети VPN D.
```

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Идентификатор export RT виртуальной сети VPN A равен 1:1, а идентификатор import RT виртуальной сети VPN D — 1:1. Поэтому маршруты могут локально пересекаться в VPN D. Сосед ASBR1-устройства — маршрутизатор ASBR2 с подключением Option A — эквивалентен устройству на стороне клиента (CE), поэтому маршрут, локально пересекающий VPN D, может быть объявлен маршрутизатору ASBR2 через соседа Option A (12.4.4.2) виртуальной сети VPN D.

Анализ отказа (3/6)

- Проверьте процесс передачи маршрута 123.1.1.1/32 на устройстве ASBR2.

```
<~ASBR2>display bgp vpnv4 all routing-table 123.1.1.1 32
 BGP local router ID : 2.2.2.2
Local AS number : 200
Total routes of Route Distinguisher(1:1): 1
BGP routing table entry information of 123.1.1.1/32:
From: 12.1.1.1 (1.1.1.1)
Route Duration: 00h19m33s
Direct Out-interface: GigabitEthernet0/0/1
Original nexthop: 12.1.1.1
Qos information : 0x0
Ext-Community:RT <1 : 1>
AS-path 100 1000, origin igp, pref-val 0, valid, external, best, select, pre 255
Not advertised to any peer yet
Total routes of Route Distinguisher(1:4): 1
BGP routing table entry information of 123.1.1.1/32:
From: 12.4.4.1 (1.1.1.1)
Route Duration: 00h12m23s
Direct Out-interface: GigabitEthernet0/0/3
Original nexthop: 12.4.4.1
```

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Анализ отказа (4/6)

```
Qos information : 0x0
 Ext-Community:RT <1 : 1>, RT <1 : 2>,
           RT <1 : 3>, RT <1 : 4>
 AS-path 100 1000, origin igp, pref-val 0, valid, external, best, select, pre 25
5
 Not advertised to any peer yet
 VPN-Instance vpna, Router ID 2.2.2.2:
 Total Number of Routes: 2
 BGP routing table entry information of 123.1.1.1/32:
 From: 12.1.1.1 (1.1.1.1)
 Route Duration: 00h19m33s
 Direct Out-interface: GigabitEthernet0/0/1
 Original nexthop: 12.1.1.1
 Qos information : 0x0
 AS-path 100 1000, origin igp, pref-val 0, valid, external, best, select, active
, pre 255
 Advertised to such 2 peers:
   10.1.2.1              // Маршрут объявляется устройству CE-A2.
   12.1.1.1
```

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- ASBR2 изучает маршрут VPN A по адресу 123.1.1.1/32, получая информацию от соседа Option A (12.1.1.1) виртуальной сети VPN A, и объявляет этот маршрут устройству CE-A2.

Анализ отказа (5/6)

```
BGP routing table entry information of
123.1.1.1/32:
 From: 12.4.4.1 (1.1.1.1)
 Route Duration: 00h12m24s
 Direct Out-interface: GigabitEthernet0/0/3
 Original nexthop: 12.4.4.1
 Qos information : 0x0
 Ext-Community:RT <1 : 1>, RT <1 : 2>,
               RT <1 : 3>, RT <1 : 4>
// Маршрут VPN D локально пересекает
VPN A.
 AS-path 100 1000, origin igp, pref-val 0, valid,
external, pre 255, not preferred for peer type
 Not advertised to any peer yet
```

```
 VPN-Instance vpnd, Router ID 2.2.2.2:

 Total Number of Routes: 2
 BGP routing table entry information of
123.1.1.1/32:
 From: 12.4.4.1 (1.1.1.1)
 Route Duration: 00h11m08s
 Direct Out-interface: GigabitEthernet0/0/3
 Original nexthop: 12.4.4.1
 Qos information : 0x0
 AS-path 100 1000, origin igp, pref-val 0,
valid, external, best, select, active
, pre 255
 Advertised to such 1 peers:
    40.1.2.1 // Маршрут объявляется
устройству CE-D2.
```

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- ASBR2 изучает маршрут VPN D 123.1.1.1/32, получая информацию от соседа Option A (12.4.4.1) виртуальной сети VPN D. Маршрут локально пересекает VPN A (не приоритетна), CE-B2, CE-C2 и CE-D2.

Анализ отказа (6/6)

VPN-Instance vpnb, Router ID 2.2.2.2:

Total Number of Routes: 1
BGP routing table entry information of
123.1.1.1/32:
From: 12.4.4.1 (1.1.1.1)
Route Duration: 00h11m08s
Direct Out-interface: GigabitEthernet0/0/3
Original nexthop: 12.4.4.1
Qos information : 0x0
Ext-Community:RT <1 : 1>, RT <1 : 2>,
RT <1 : 3>, RT <1 : 4>// Маршрут
VPN D локально пересекает VPN B.
AS-path 100 1000, origin igp, pref-val 0, valid,
external, best, select, active
, pre 255
Advertised to such 2 peers:
20.1.2.1 // Маршрут объявляется
устройству CE-B2.
12.2.2.1

VPN-Instance vpnc, Router ID 2.2.2.2:

Total Number of Routes: 1
BGP routing table entry information of
123.1.1.1/32:
From: 12.4.4.1 (1.1.1.1)
Route Duration: 00h11m08s
Direct Out-interface: GigabitEthernet0/0/3
Original nexthop: 12.4.4.1
Qos information : 0x0
Ext-Community:RT <1 : 1>, RT <1 : 2>,
RT <1 : 3>, RT <1 : 4>
// Маршрут локально пересекает VPN C.
AS-path 100 1000, origin igp, pref-val 0, valid,
external, best, select, active
, pre 255
Advertised to such 2 peers:
30.1.2.1 // Маршрут объявляется
устройству CE-C2.
12.3.3.1

© 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- ASBR2 изучает маршрут VPN D 123.1.1.1/32, получая информацию от соседа Option A (12.4.4.1) виртуальной сети VPN D. Маршрут локально пересекает VPN A (не приоритетна), CE-B2, CE-C2 и CE-D2.

Диагностика и устранение отказа

- Параметр export RT виртуальной сети VPN D равен 1:1 1:2 1:3 1:4. Параметр import RT виртуальной сети VPN A равен 1:1, import RT виртуальной сети VPN B равен 1:2, import RT виртуальной сети VPN C равен 1:3. Таким образом, локальное пересечение неисправного маршрута 123.1.1.1/32 в норме. Маршруты, локально пересекающие VPN B и VPN C, объявляются устройствам CE-B2 и CE-C2. Процесс объявления проходит нормально.
- Процессы пересечения маршрутов и объявления таблицы маршрутизации на устройствах ASBR1 и ASBR2 осуществляются нормально. Проблема заключается в том, что VPN D может взаимодействовать с остальными тремя VPN. В результате маршруты, изучаемые устройством ASBR2 от VPN D, пересекают эти три VPN. В этих условиях маршруты от любой из четырех VPN могут пересекать любую другую VPN. То есть каждая VPN может изучать маршруты от других VPN, и поэтому настроенная ранее изоляция этих виртуальных сетей стала недействительной.



© 2019 Huawei Technologies Co., Ltd. Все права защищены.

Решение 1

- Решение 1. Сконфигурируйте на устройстве ASBR1 политику экспорта для соседа Option A виртуальной сети VPN D маршрутизатора ASBR2.

```
ip extcommunity-filter 1 permit rt 1:4
ip extcommunity-filter 2 permit rt 1:1 rt 1:2 rt 1:3
#
route-policy rp-asbr2-vpnd permit node 10
 if-match extcommunity-filter 1
#
route-policy rp-asbr2-vpnd deny node 20
 if-match extcommunity-filter 2
#
route-policy rp-asbr2-vpnd permit node 100
#
bgp 100
  peer 12.4.4.2 route-policy rp-asbr2-vpnd export
#
```

- Выполните такие же настройки на ASBR2.
- Примечание. В сценариях локальных пересечений с отсутствием устройств на стороне провайдера (PE) настройку **route-policy rp-asbr2-vpnd** и **extcommunity-filter 1** на **node 10** можно пропустить.

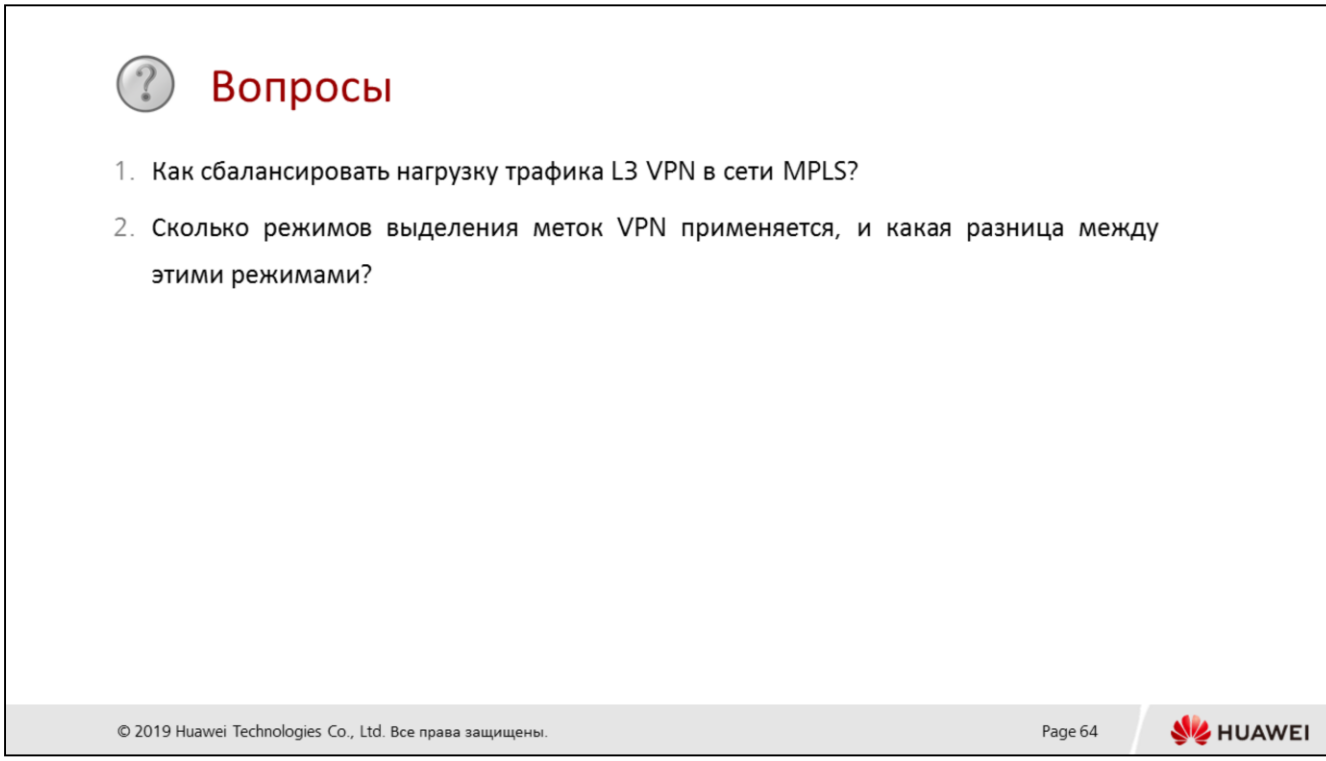
© 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Сконфигурируйте на устройстве ASBR1 политику экспорта для соседа Option A виртуальной сети VPN D. Объявляются только маршруты, исходящие от VPN D (включая маршруты VPNv4, пересекающие VPN D через import RT 1:4, и маршруты, получаемые от других соседей VPN D). Маршруты, исходящие от остальных VPN (включая маршруты VPNv4, пересекающие VPN D через import RT 1:1, 1:2 или 1:3, и маршруты, локально пересекающие VPN D и идущие от других экземпляров VPN) не объявляются. В этом случае ASBR2 не получит маршрут от устройства CE-A1 через соседа Option A виртуальной сети VPN D, и поэтому через него не пройдет маршрут, направленный к остальным экземплярам VPN.
- Маршруты, исходящие от VPN D устройства ASBR1, включают маршруты VPNv4, пересекающие VPN D через import RT 1:4 (передавая атрибут extcommunity <1:4>) и маршруты, получаемые от других соседей VPN D.

Решение 2

- Решение 2. Сконфигурируйте режим подключения Inter-AS MPLS BGP VPN Option B, в котором устройства ASBR будут объявлять маршруты через соседей VPNv4. В этом случае, если ASBR1 будет объявлять маршруты, полученные от CE-A1, устройству ASBR2, будут объявляться только маршруты VPNv4 с атрибутом extcommunity 1:1. Также данные маршруты не будут объявляться через VPN, являющуюся соседом VPN D. Поэтому, не получая маршруты VPN от VPN D, устройство ASBR2 будет получать только маршруты VPNv4 с атрибутом extcommunity 1:1. Согласно политикам импорта маршрутов (import RT), данные маршруты могут пересечь только VPN A и VPN D.

© 2019 Huawei Technologies Co., Ltd. Все права защищены.



- Вопрос 1. Как сбалансировать нагрузку трафика L3 VPN в сети MPLS?
- Ответ. По умолчанию трафик L3 VPN в сети MPLS не сбалансирован. Для балансировки нагрузки применяются следующие команды:
  - **tunnel select-seq** { **cr-lsp** | **lsp** } * **load-balance-number** *количество туннелей для балансировки нагрузки*
- Вопрос 2. Сколько режимов выделения меток VPN применяется, и какая разница между этими режимами?
- Ответ. Метки VPN выделяются одним из двух способов:
  - Apply-label per-route (режим по умолчанию)
  - Apply-label per-instance
- Разница:
  - Метод выделения меток на основе маршрута (режим по умолчанию) занимает большое число ресурсов устройства. Выделение меток большому количеству маршрутов может привести к перегрузке устройства и стать причиной ошибки передачи.
  - Второй метод на основе экземпляра отличается эффективностью использования ресурсов устройства.
- В целом, оба режима демонстрируют один результат, но рекомендуется второй метод.

Спасибо за внимание!

www.huawei.com