

Содержание

Архитектуры базовых корпоративных сетей	1
Введение в среды передачи данных	9
Интернет фреймирование	22
IP-адресация	42
Протокол межсетевых управляющих сообщений (ICMP)	69
Протокол определения адреса (ARP)	84
Транспортный уровень	99
Сценарий пересылки данных	115
Основы VRP	132
Навигация по CLI	147
Навигация и управление в файловой системе	165
Управление образами операционной системы VRP	184
Создание единой коммутируемой сети	198
Протокол остовного дерева (STP)	209
Быстрый протокол разворачивающегося дерева (RSTP)	241
Базовые знания IP-маршрутизации	267
Маршруты статических IP	280
Дистанционно-векторная маршрутизация с протоколом маршрутной информации (RIP)	296
Маршрутизация по состоянию канала с помощью OSPF	323
Принципы DHCP протокола	352
Принципы FTP протокола	369
Принципы Telnet протокола	380

Архитектуры базовых корпоративных сетей

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

Требования коммерческого предприятия подчеркивают необходимость в сетях, способных адаптироваться к постоянно меняющимся требованиям бизнеса в условиях его роста и развития услуг. Поэтому необходимо понимать принципы того, что представляет собой корпоративная сеть, и как она формируется и адаптируется под потребности бизнеса в реальном мире.

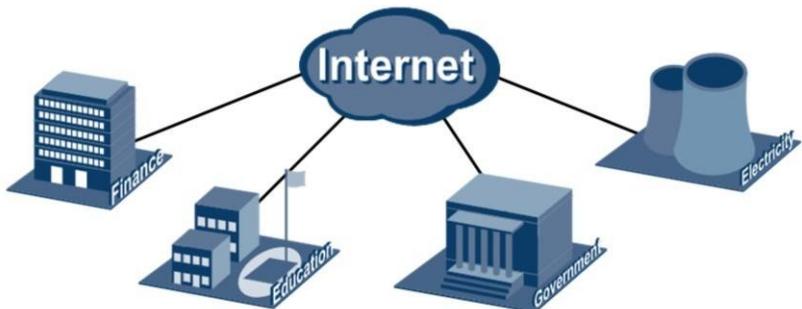


Цели

По завершении этого раздела проходящие обучение смогут:

- Объяснять, из чего состоит корпоративная сеть.
- Описывать типы архитектур популярных корпоративных сетей.
- Описывать некоторые из решений, которые часто применяются внутри корпоративных сетей с целью поддержки бизнес-операций.

Реальные корпоративные сети



- Корпоративные сети существуют во многих известных индустриях.
- Сети варьируются от офисов до крупных промышленных платформ.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

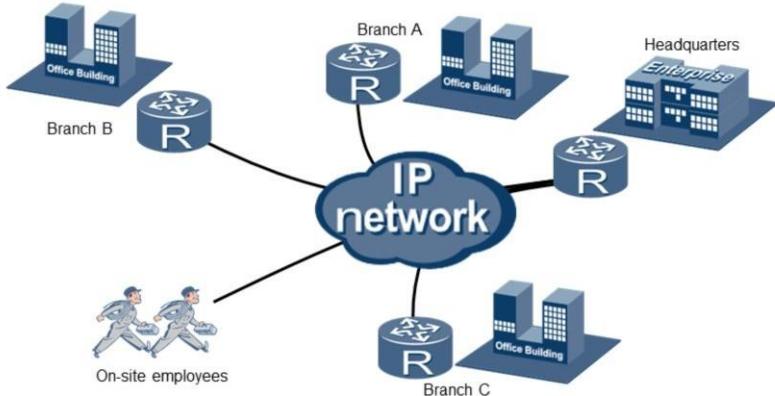
Page 4



В своей основе корпоративная сеть представляет собой взаимосвязь систем, принадлежащих к определенной функциональной группе или организации, с целью, в первую очередь, обеспечить совместное использование ресурсов, таких как принтеры и файловые серверы, поддержку связи такими средствами, как электронная почта, а также переход к приложениям, обеспечивающим совместную работу пользователей. Сегодня корпоративные сети присутствуют в различных отраслях промышленности от офисной среды до больших энергетических, финансовых и правительственные отраслей, которые зачастую состоят из корпоративных сетей, соединяющих различные физические местоположения.

Появление Интернета в качестве общественного сетевого домена позволило расширить существующую корпоративную сеть, через которую теперь могут быть соединены географически разрозненные сети, принадлежащие одной организации или предприятию, в результате чего возникает ряд новых проблем, связанных с установлением взаимосвязи между географически разрозненными корпоративными сетями при сохранении конфиденциальности и безопасности данных, принадлежащих отдельному предприятию.

Удаленные корпоративные сети



- Корпоративные сети могут охватывать большие площади

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

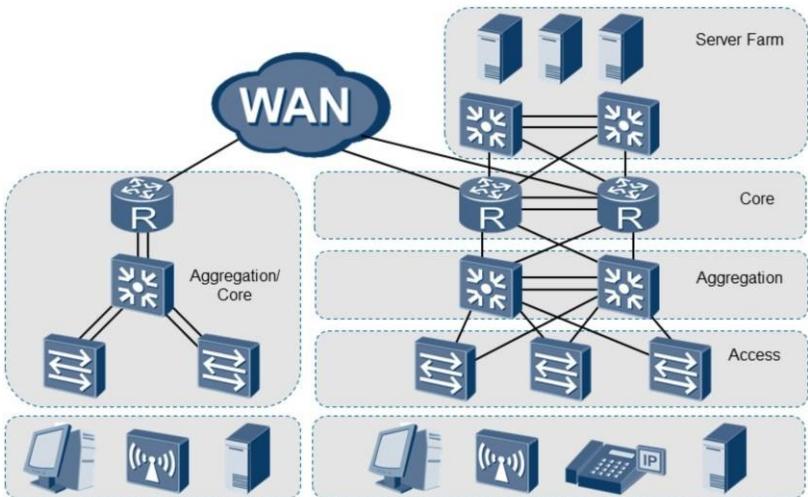
Page 5



Различные проблемы влияют на сегодняшние отрасли промышленности в плане предоставления решений для установления взаимосвязи между удаленными локациями, которыми часто оказываются региональными филиалами и головными офисами, а также сотрудниками, которые представляют собой нефиксированный объект в корпоративной сети, часто находясь в местах за пределами границ предприятия. Проблемы в отраслях промышленности создали спрос на повсеместные сети, которые позволяют корпоративной сети быть доступной из любого места и в любое время, чтобы обеспечить доступ к ресурсам и инструментам, которые позволяют эффективно оказывать поддержку и услуги отраслевым партнерам и клиентам.

Развитие корпоративных решений наряду с развитием технологий, которые устанавливают частные сетевые соединения через инфраструктуру общедоступной сети, позволило публичным и сторонним IP-сетям обеспечить связь отдельных частей в любом месте в любое время, с целью расширить дистанционные возможности корпоративной сети за пределы физических границ предприятия, позволяя удаленному офису и пользователям образовывать единый корпоративный домен, который охватывает большие географические расстояния.

Базовая архитектура корпоративной сети



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 6



Архитектурные решения корпоративной сети существенно различаются в зависимости от требований отрасли и организации. Небольшие предприятия часто могут иметь очень ограниченное требование с точки зрения сложности и спроса, предпочитая внедрять плоскую сеть, главным образом из-за размера организации, которая часто ограничивается одним географическим местоположением или в пределах нескольких мест, поддерживая доступ к общим ресурсам, обеспечивая при этом гибкость внутри организации для поддержки небольшого числа пользователей. Затраты на внедрение и обслуживание таких сетей значительно снижаются, однако сеть часто подвержена сбоям из-за отсутствия избыточности, а производительность может варьироваться в зависимости от ежедневных операций и нагрузки на сеть.

Более крупные корпоративные сети внедряют решения для обеспечения минимального сбоя сети, контролируемого доступа и предоставления различных сервисов для поддержки повседневной деятельности организации. Многоуровневая архитектура предназначена для оптимизации трафика, применения политик управления трафиком и контролируемого доступа к ресурсам, а также для поддержания доступности сети и стабильной работы за счет эффективной избыточности сети. Многоуровневая конструкция сети также предполагает легкое расширение, а вместе с модульным проектированием, обеспечивающим эффективную изоляцию и обслуживание компонентов, позволяет, в случае, если в сети возникает проблема, не затронуть всю сеть.



Итог

- Какие основные отличия между небольшими и средними по размеру корпоративными сетями?
- Каковы некоторые основные соображения архитектуры, которые нужно учитывать для небольших и средних по размеру корпоративных сетей?

1. Небольшие корпоративные сети, реализующие плоскую сетевую архитектуру, могут ограничить возможности масштабирования сети в случае роста числа пользователей. В тех случаях, когда ожидается, что необходимо будет поддерживать большее число пользователей, следует рассмотреть иерархический подход к корпоративным сетям. Сети среднего размера, как правило, поддерживают большее число пользователей и, как правило, реализуют иерархическую сетевую инфраструктуру, позволяющую сети расти и поддерживать требуемую базу пользователей.
2. Небольшие и средние корпоративные сети должны учитывать производительность сети, а также поддерживать избыточность в случае сбоя сети для обеспечения доступности сервиса всем пользователям. По мере роста сети растет угроза безопасности сети, что также может угрожать сервисам.



Thank you

www.huawei.com

Введение в среды передачи данных

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

Создание корпоративной сети требует фундаментального понимания основных сетевых концептов. Эти концепты включают знания о том, чем определяется сеть, а также основные стандарты технологий и физических компонентов, которые используются для построения корпоративных сетей. Понимание основных сетевых коммуникаций и влияния, которые они оказывают на сеть, также первостепенно для эффективной реализации сети.

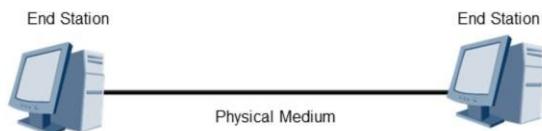


Цели

По завершении этого раздела проходящие обучение смогут:

- Объяснять, из чего состоит сеть.
- Распознавать базовые компоненты сети.
- Описывать главные механизмы связи по сети.

Простые двухточечные Ethernet сети



- Сети состоят из минимум двух конечных устройств и физической среды передачи данных

Под сетью понимается возможность взаимодействия двух или более объектов через данную среду передачи информации. Разработка любой сети основывается на этом же принципе для установления связи. Обычно объекты в сети, которые отвечают за передачу и прием данных, называются конечными устройствами, а средства, с помощью которых обеспечивается связь, называются средой передачи. В корпоративной сети среда передачи может быть представлена в различных формах - от физического кабеля до радиоволн.

Коаксиальная линия передачи



Standard	Cables	Maximum Transmission Distance
10Base2	Thin coaxial	185m
10Base5	Thick coaxial	500m

- Медные коаксиальные кабели обычно используются для поддержки пользователей в общей сети

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 5



Коаксиальный кабель представляет собой довольно старую среду передачи, которая сегодня ограниченно используется в корпоративной сети. В качестве среды передачи коаксиальный кабель имеет два стандарта: формы 10Base2 и 10Base5, которые известны как Thinnet или Thinwire, Thicknet или Thickwire соответственно.

Оба стандарта поддерживают пропускную способность 10 Мбит/с в виде сигналов основной полосы частот на расстояния 185 и 500 метров соответственно. В современных корпоративных сетях пропускная способность крайне ограничена в каком-либо значительном применении. Коннектор Bayonet Neill-Concelman (BNC) является обычной формой разъема, используемого для тонких коаксиальных кабелей 10Base2, в то время как разъем типа N был применен к более толстому кабелю 10Base5.

Ethernet



Standard	Physical Medium	Distance
10Base-T	Two pairs of Category 3/4/5 twisted pair cables	100m
100Base-TX	Two pairs of Category 5 twisted pair cables	100m
1000Base-T	Four pairs of Category 5e twisted pair cables	100m

- Основная физическая среда передачи данных, используемая в корпоративных сетях

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 6



Кабель Ethernet стал стандартом для многих корпоративных сетей, обеспечивая среду передачи, которая поддерживает гораздо более высокую пропускную способность. Среда поддерживает четыре пары медных проводов, находящихся в оболочке, которые могут быть защищены или не защищены от внешних электрических помех. Емкость передачи определяется в основном категорией кабеля, где категория 5 (CAT5) поддерживает передачу Fast Ethernet до 100 Мбит/с, а более высокую пропускную способность Gigabit Ethernet обеспечивает расширенный стандарт категории 5 (CAT5e) и выше.

Передача данных через Ethernet в качестве физической среды также подвержена затуханию, что приводит к ограничению дистанции передачи до 100 метров. Разъем RJ-45 используется для обеспечения возможности подключения проводной пары, при этом требует определенного порядка контактов в разъеме RJ-45, для обеспечения правильной передачи и приема конечными устройствами через среду передачи.

Оптоволокно



Standard	Physical Medium	Distance
10Base-F	Two strand fiber	2000m
100Base-FX	Two strand multi-mode fiber	2000m
1000Base-LX	Single-mode fiber or multi-mode fiber	316 - 5000m
1000Base-SX	Multi-mode fiber	275 - 550m

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 7



Оптические среды передачи используют свет как средство передачи сигнала, а не электрические сигналы, как в Ethernet и коаксиальных средах. Оптоволоконная среда поддерживает такие стандарты передачи данных, как 10 Мбит/с, 100 Мбит/с, 1 Гбит/с и даже 10 Гбит/с (10GBASE). Одномодовое или многомодовое оптоволокно определяет использование оптической среды передачи для распространения света. Одномодовое волокно предполагает передачу одной моды и обычно используется для высокоскоростной передачи на большие расстояния.

Многомодовое волокно поддерживает распространение нескольких мод, которые восприимчивы к затуханию в результате рассеяния света вдоль оптической среды и, следовательно, не способно поддерживать передачу на большие расстояния. Этот режим часто применяется в локальных сетях, которые охватывают гораздо меньший диапазон передачи. Существует множество стандартов оптоволоконного разъема, самые распространенные из которых разъем ST, разъем LC и SC или защелкивающийся разъем.

Последовательный интерфейс



Standard	Speed
RS-232	Standards define up to 20000bps, but can reach 1Mbit/s
RS-422	100Kbit/s ~ 10Mbit/s+

- Последовательный интерфейс представляет собой устаревший способ передачи данных.
- Стандарты продолжают развиваться в таких формах, как USB.

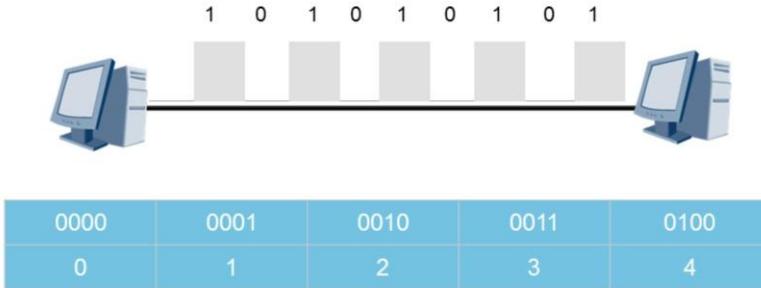
Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 8



Последовательный интерфейс представляет собой стандарт, разработанный более 50 лет назад для обеспечения надежной передачи между устройствами, за это время произошло много изменений стандарта. Последовательное соединение предназначено для передачи данных в виде последовательного потока бит. Обычно применяемый стандарт обозначается как (Recommended Standard) RS-232, однако он ограничен как расстоянием, так и скоростью. Оригинальные стандарты RS-232 определяют, что поддерживаемые скорости связи не должны превышать 20 Кбит/с, исходя из длины кабеля 50 футов (15 метров), несмотря на это скорость передачи для последовательного порта вряд ли будет ниже 115 Кбит/с. Обычно для последовательного интерфейса по мере увеличения длины кабеля поддерживаемая скорость передачи будет уменьшаться, например, если кабель длиной около 150 метров, что в 10 раз превышает стандарт, поддерживаемая скорость передачи бит будет уменьшена вдвое. Другие стандарты последовательного интерфейса имеют возможность достигать гораздо больших диапазонов передачи, например, в стандартах RS-422 и RS-485, которые охватывают расстояния до 4900 футов (1200 метров) и часто используются с разъемами V.35, которые устарели в конце 1980-х годов, но которые все еще часто встречаются и поддерживаются сегодня для таких технологий, как Frame Relay и ATM, где они применяются. Сам RS-232 не определяет стандарты разъема, однако два похожих разъема, поддерживающие стандарт RS-232 - DB-9 и DB-25. Более новые стандарты были разработаны для замены значительной части существующей последовательной технологии RS-232, включая стандарты FireWire и универсальной последовательной шины (USB), последний из которых становится обычным явлением во многих новых продуктах и устройствах.

Кодирование данных сигнала



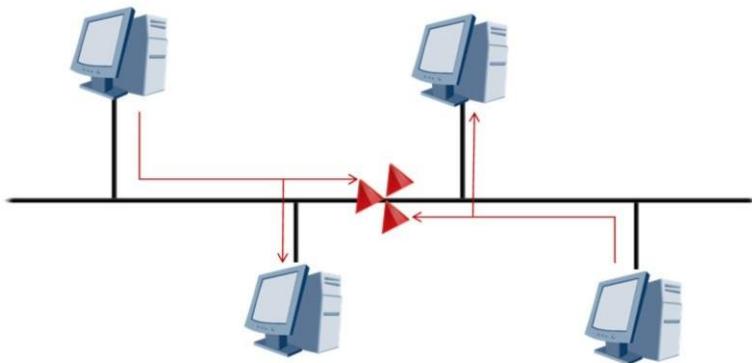
- Для дешифровки данных используются схемы сигналов.
- Кодирование используется для синхронизации передачи данных.

Для обеспечения связи по физическим каналам сигналы должны передаваться между передающим и принимающим устройствами. Этот сигнал будет меняться в зависимости от используемой среды передачи, как в случае оптической и беспроводной передачи. Основная цель сигнала - обеспечить синхронизацию (или тактовую синхронизацию) между отправителем и получателем в физическом среде, а также обеспечить передачу сигнала данных в такой форме, которая может быть распознана как отправителем, так и получателем.

Форма сигнала обычно определяется как свойство линейного кодирования, где напряжение переводится в двоичное представление из 0 и 1, которое может быть переведено обратно принимающим устройством. Существуют различные стандарты линейного кодирования, например 10Base Ethernet поддерживают такой стандарт линейного кодирования, как Манчестерское кодирование. Fast Ethernet с частотным диапазоном 100 МГц позволяет достичь более высокой частоты, чем при использовании Манчестерского кодирования.

Поэтому используется альтернативная форма линейного кодирования, известная как NZRI, которая сама по себе, зависит от физической среды передачи, тем самым поддерживая MLT-3 для 100Base-TX и 100Base-FX вместе с расширенным линейным кодированием, известным как кодирование 4B/5B с целью решения потенциальных проблем тактовой синхронизации. Например, 100Base-T4 использует другую форму кодирования, известную как расширенное линейное кодирование 8B/6T. Gigabit Ethernet поддерживает линейное кодирование 8B/10B, за исключением стандарта 1000Base-T, который основывается на сложной блочной кодировке, называемой 4D-PAM5.

Домены коллизий



- Сигналы в общей сети подвержены коллизиям.
- Для обнаружения коллизий используется механизм распознавания коллизий.

Ethernet представляет собой сеть с множественным доступом, в которой два или более конечных устройства совместно используют общую среду передачи для пересылки данных. Такая сеть, однако, подвержена коллизиям передачи, когда данные персылаются конечными устройствами одновременно по общей среде передачи. Сегмент, где такие события возможны, называется общим доменом коллизии.

Конечные устройства в таком домене коллизии конкурируют за передачу данных назначенному адресату. Такое конкурентное поведение требует от каждого конечного устройства осуществлять мониторинг входящих данных в сегменте, прежде чем делать попытку передачи, данный процесс называется «Множественный доступ с прослушиванием несущей и обнаружением коллизий» (Carrier Sense Multiple-Access Collision Detection (CSMA/CD)). Однако даже после принятия таких мер предосторожности вероятность возникновения коллизий в результате одновременной передачи двумя конечными устройства остается весьма большой.

Дуплексные режимы



- Дуплексные режимы поддерживают одновременную и неодновременную передачу в обе стороны

Режимы передачи определяются как полу- и полнодуплексные, чтобы обозначить поведение, связанное с передачей данных по физической среде.

Полудуплексный режим относится к связи двух или более устройств через общую физическую среду, в которой существует домен коллизии, поэтому для обнаружения таких столкновений требуется CSMA/CD. Начинается процесс с того, что конечное устройство прослушивает входящий трафик на своем собственном интерфейсе, и тогда, когда его нет в течение определенного периода времени, оно приступит к передаче своих данных. Если произойдет коллизия, передача прекратится, затем включится алгоритм задержки для предотвращения дальнейшей передачи, пока не истечет таймер со случайным значением, после произойдет повторная попытка передачи данных.

Полнодуплексный режим определяет одновременную двустороннюю связь через выделенные пары двухточечных проводов, гарантируя отсутствие возможности возникновения коллизий, и, следовательно, ликвидируя необходимость в CSMA/CD.



Итог

- Какие способы кабельного соединения могут быть использованы для поддержки Gigabit Ethernet в корпоративной сети?
- Что такое домен коллизии?
- Каково назначение CSMA/CD?

1. Передача Gigabit Ethernet поддерживается категорией кабеля САТ 5е и выше, а также любой вид оптоволокна 1000Base или выше.
2. Домен коллизии — это сегмент сети, в котором используется одна и та же физическая среда передачи для двусторонней связи. Данные, передаваемые одновременно между хостами в одной и той же среде общей сети, подвержены коллизии сигналов еще до того, как эти сигналы достигнут назначенного адресата. Обычно это приводит к получению адресатом искаженных сигналов, также известных как карлики и гиганты, которые больше или меньше допустимого размера для передачи (64 байта - 1500 байт).
3. CSMA/CD — это механизм для обнаружения и минимизации вероятности коллизий, которые могут возникнуть в общей сети. CSMA требует, чтобы передающий хост сначала прослушивал сигналы в общей среде перед тем, как начать передачу. Если никакой передачи данных в среде не обнаружено, хост может начать передачу своих данных. В случае, когда сигналы передаются одновременно и происходит коллизия, применяются механизмы обнаружения коллизий с целью прекращения передачи в течение локально устанавливаемого периода времени, чтобы позволить среде очиститься от коллизии и избежать дальнейших коллизий между передающими хостами.



Thank you

www.huawei.com

Ethernet фреймирование

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

Передача по физической среде требует правил, которые определяют поведение во время связи. Управление передачей в сетях, основанных на Ethernet, контролируется стандартами IEEE 802, определенных для технологии передачи данных Ethernet. Фундаментальные знания этих стандартов необходимо для полного понимания работы связи на канальном уровне в сетях, основанных на Ethernet.



Цели

По завершении этого раздела проходящие обучение смогут:

- Объяснять применение эталонных моделей к сетям.
- Описывать, как строятся фреймы.
- Объяснять функцию MAC-адресации на канальном уровне.
- Описывать передачу Ethernet фреймов и последующее поведение.

Управление передачей в сети



- Сети в основном управляются протоколами верхнего и нижнего уровней

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

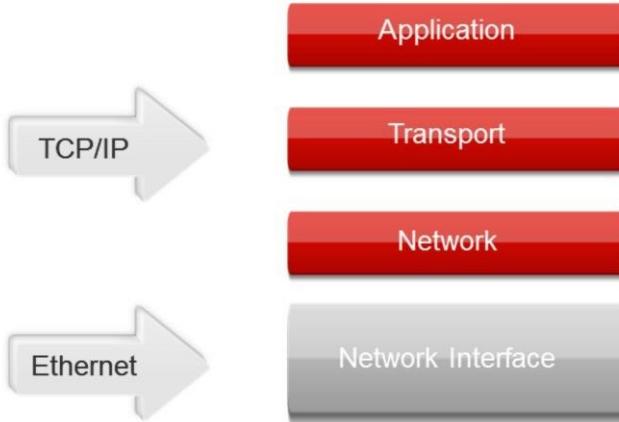
Page 4



Связь в сетях основана на применении правил, которые определяют, как данные передаются и обрабатываются, способом, понятным как отправляющим, так и получающим объектам. В результате с течением времени были разработаны несколько стандартов, и некоторые стали широко распространены и применимы. Тем не менее существует четкое различие между стандартами, которые управляют физическим потоком данных, и стандартами, ответственными за логическую пересылку и доставку трафика.

Стандарты IEEE 802 представляют собой универсальный стандарт для управления физической передачей данных по физической сети и состоят из стандартов, включая Ethernet 802.3, для физической передачи по локальным сетям. Существуют альтернативные стандарты для передачи по глобальным сетям, работающим с последовательными интерфейсами, включая Frame Relay, HDLC и более старые стандарты, такие как ATM. TCP/IP широко используется в качестве набора протоколов, определяющих стандарты верхнего уровня, регулирующие правила (протоколы) и поведение, связанное с управлением логической пересылкой и доставкой между конечными устройствами.

Многоуровневые модели – TCP/IP



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 5



Эталонная модель TCP/IP в основном касается основных принципов набора протоколов, которые можно понимать, как логическую передачу и доставку трафика между конечными устройствами. Таким образом, эталонная модель протокола TCP/IP дает четырехуровневое представление сети, оставляя поведение физической передачи под управлением уровня сетевого интерфейса (network interface layer), поскольку работа нижнего уровня не связана с набором протоколов TCP/IP.

Основной фокус остается на сетевом (или интернет-) уровне (network layer), который управляет тем, как трафик логически пересыпается между сетями, и на транспортном (или межхостовый) уровне (transport layer), который управляет сквозной доставкой трафика, обеспечивая надежность передачи между исходным и конечным устройствами. Прикладной уровень (application layer) представляет собой интерфейс со множеством протоколов, которые позволяют применять сервисы к процессам приложений конечного пользователя.

Многоуровневые модели – OSI



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

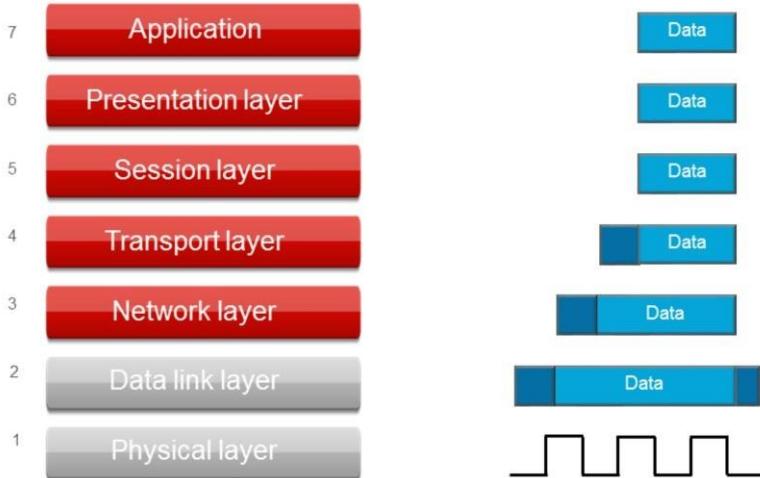
Page 6



Хотя эталонная модель TCP/IP в основном поддерживается как стандартная модель, основанная на наборе протоколов TCP/IP, данная модель четко не разделяет и не отличает функциональные возможности при переходе к физической передаче нижнего уровня.

В свете этого эталонная модель OSI (the open systems interconnection) часто признается в качестве эталонной модели для стандартов IEEE 802 благодаря четкому различию и описанию поведения нижних уровней, которая почти полностью соответствует стандартам эталонной модели LAN/MAN, которые определены как часть документированных стандартов IEEE 802-1990 для локальных и городских сетей. Кроме того, модель, которая почти полностью относится к набору протоколов ISO, обеспечивает расширенное разделение процессов верхнего уровня.

Инкапсуляция



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

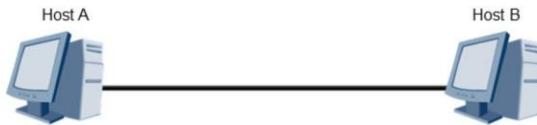
Page 7



Поскольку данные приложения верхнего уровня передаются по сети из конечной системы, к данным перед успешной отправкой применяется ряд процессов и инструкций. Этот процесс добавления (как перед самими данными, так и после них, то есть заголовки и концевики соответственно) инструкций к данным называется инкапсуляцией, и каждый слой эталонной модели предназначен для этого процесса.

По мере добавления инструкций к данным, общий размер данных увеличивается. Дополнительные инструкции представляют собой добавки к существующим данных и определяются в качестве инструкций только для того уровня, на котором они были применены. Для других слоев инкапсулированные инструкции не отличаются от исходных данных. Окончательное добавление инструкций выполняется в рамках стандартов протокола нижнего уровня (например, стандарта Ethernet IEEE 802.3) перед передачей в виде закодированного сигнала через физическую среду.

Связь между двумя конечными устройствами



- Фреймы канального уровня используются для управления передачей по коммуникационной среде

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

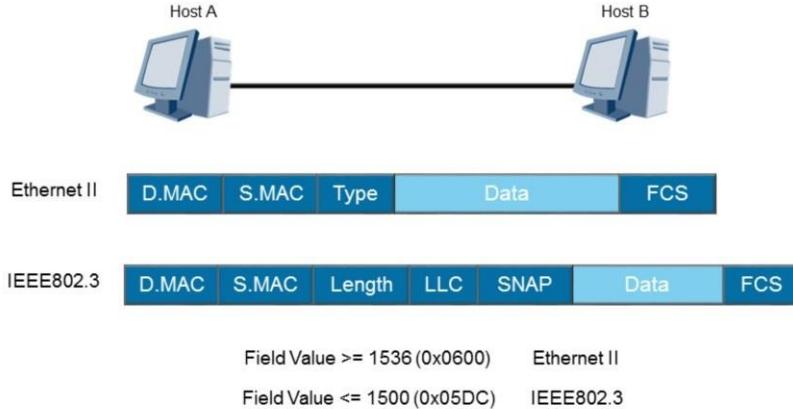
Page 8



В рамках стандарта Ethernet IEEE 802.3 данные инкапсулируются инструкциями в виде заголовка и концевика, прежде чем его можно будет передать по физической среде с поддержкой Ethernet. Каждый этап инкапсуляции работает с так называемым блоком данных протокола (Protocol Data Unit – PDU), который на канальном уровне называется фреймом.

Ethernet фреймы содержат инструкции, которые определяют, каким образом и могут ли данные передаваться через среду передачи между двумя или более точками. Фреймы Ethernet имеют два основных формата, выбор которых сильно зависит от протоколов, которые были определены перед процессом инкапсуляции фреймов.

Форматы фреймов



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 9

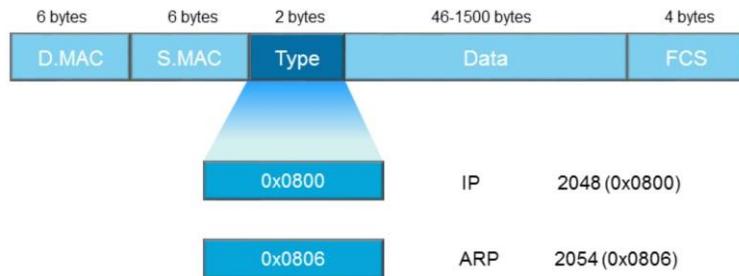


В качестве стандарта для сетей на основе Ethernet признаны два формата фреймов. Стандарт типа DIX версии 2 был первоначально разработан в начале 1980-х годов, но сегодня он называется, как тип фрейма Ethernet II. Впоследствии Ethernet II был принят и интегрирован в стандарты IEEE 802 как часть раздела 3.2.6 документации по стандартам IEEE 802.3x-1997. Стандарт Ethernet IEEE 802.3 был первоначально разработан в 1983 году с некоторыми ключевыми различиями между форматами фреймов, включая изменение поля типа (type field), которое предназначено для идентификации протокола, на который данные должны быть отправлены после того, как будут обработаны инструкции фрейма. В формате Ethernet IEEE 802.3 оно представлено как поле длины (length field) для идентификации протокола пересылки, которое опирается на расширенный набор инструкций, называемых 802.2 LLC.

Ethernet II и IEEE 802.3 связаны с протоколами верхнего уровня, которые отличаются диапазоном значений поля типа, где протоколы, поддерживающие значение, меньшее или равное 1500 (или 05DC в шестнадцатеричной СС), будут использовать тип фрейма Ethernet IEEE 802.3 на канальном уровне. Протоколы, у которых значение поля типа больше или равно 1536 (или 0600 в шестнадцатеричной СС), будут использовать стандарт Ethernet II, которому соответствует большинство всех фреймов в сетях на основе Ethernet.

Другие поля внутри фрейма включают в себя поля MAC-адреса получателя и отправителя, которые идентифицируют отправителя и предполагаемого получателя(-ей), а также поле контрольной суммы фрейма (frame check sequence), которое используется для подтверждения целостности фрейма во время передачи.

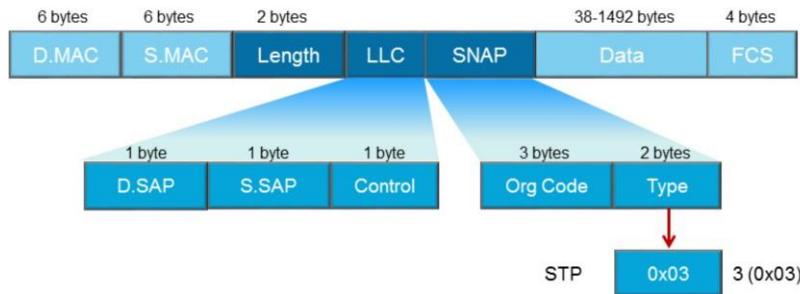
Фрейм Ethernet II



- Тип фрейма Ethernet II связан с протоколами, у которых значение поля типа больше 1536 (0x600)

Фрейм Ethernet II ссылается на шестнадцатеричное значение, которое идентифицирует протокол верхнего уровня. Одним из распространенных примеров этого является протокол IP (Internet Protocol), который представлен шестнадцатеричным значением 0x0800. Поскольку это значение превышает 0x0600, то во время инкапсуляции должен применяться тип фрейма Ethernet II. Другим распространенным протоколом, который использует тип фрейма Ethernet II на канальном уровне, является ARP и представлен он шестнадцатеричным значением 0x0806.

Фрейм IEEE802.3



- Тип фрейма IEEE802.3 связан с протоколами, у которых значение поля типа меньше 1500 (0x05DC)

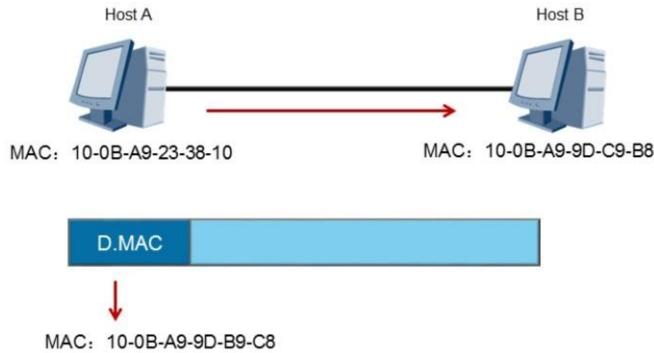
Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 11



Для типа фрейма IEEE 802.3 поле типа содержится как часть заголовка расширения SNAP и обычно не применяется к протоколам в сегодняшних сетях, частично из-за необходимости дополнительных инструкций, которые приводят к дополнительным служебным данным для каждого фрейма. Некоторые старые протоколы, которые существовали в течение многих лет, но которые все еще применяются для поддержки сетей Ethernet, зачастую используют тип кадра IEEE 802.3. Ярким примером этого может являться протокол распределенного связующего дерева (Spanning Tree Protocol - STP), который представлен значением 0x03 в поле типа в заголовке SNAP.

Пересылка фреймов



- Контроль доступа к среде передачи (Media Access Control – MAC) обеспечивает передачу данных на канальном уровне

Сети на основе Ethernet обеспечивают связь между двумя конечными устройствами в локальной сети с использованием адресации контроля доступа к среде передачи (Media Access Control - MAC), которая позволяет различать конечные системы в сети множественного доступа. MAC-адрес – это физический адрес, который записан в карту сетевого интерфейса, к которой подключена физическая среда передачи. Этот же MAC-адрес извлекается и используется отправителем в качестве MAC-адреса назначения предполагаемого получателя, прежде чем фрейм будет передан на физический уровень для пересылки по подключенной среде передачи.

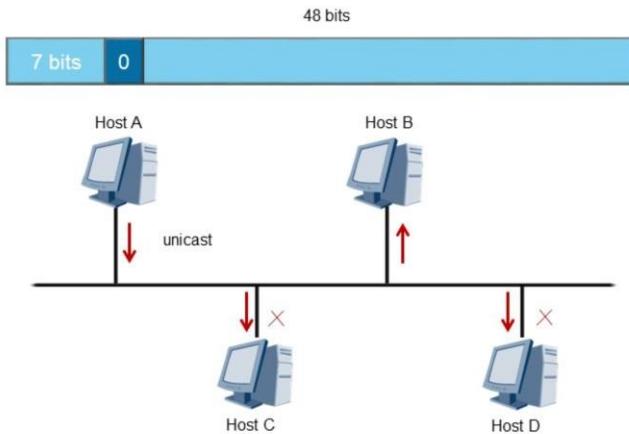
Ethernet MAC-адрес



- MAC-адреса состоят из уникального идентификатора организации (organizationally unique identifier – OUI) и присваиваемого компанией-изготовителем значения адреса

Каждый MAC-адрес представляет собой 48-битное значение, обычно представленное в шестнадцатеричном формате и состоящее из двух частей, которые должны гарантировать, что каждый MAC-адрес является глобально уникальным. Это достигается путем определения OUI (organizationally unique identifier), уникального для каждого производителя, на основе которого можно проследить происхождение продукта вплоть до его производителя на основе первых 24 бит MAC-адреса. Остальные 24 бита MAC-адреса представляют собой значение, которое увеличивается и уникально назначается каждому продукту (примером может служить, сетевая интерфейсная карта или аналогичные продукты, поддерживающие интерфейсы портов, для которых требуется MAC).

Пересылка одноадресатных фреймов



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

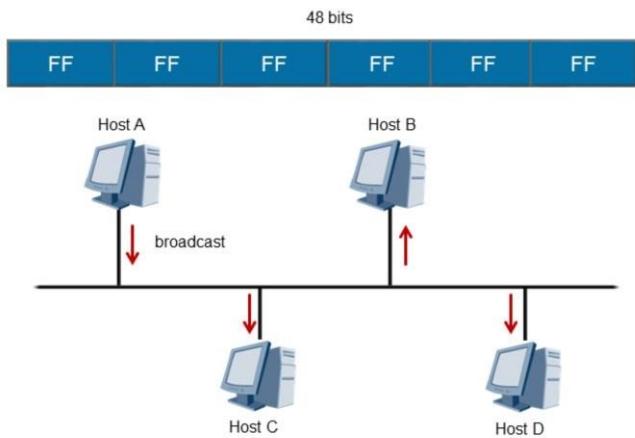
Page 14



Передача кадров в локальной сети осуществляется с помощью одного из трех методов маршрутизации, первый из них - одноадресатный и относится к передаче из одного источника в один пункт назначения. Каждый интерфейс хоста представлен уникальным MAC-адресом, содержащим OUI, в котором 8-й бит наиболее значимого октета (или первого байта) в поле MAC-адреса определяет тип адреса. Этот 8-й бит всегда установлен в 0, если MAC-адрес является MAC-адресом хоста и означает, что любой фрейм, содержащий этот MAC-адрес в поле MAC-адреса назначения, предназначен только для одного адресата.

Если хосты находятся в общем домене коллизии, все подключенные хосты получат такую одноадресатную передачу, но фрейм будет проигнорирован всеми узлами, у которых MAC-адрес не соответствует MAC-адресу в поле MAC-адреса назначения фрейма, и только хост назначения примет и обработает переданные данные. Одноадресатные передачи пересылаются к назначенному конечному хосту только с одного физического интерфейса, даже если есть несколько интерфейсов.

Широковещательная пересылка фреймов



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

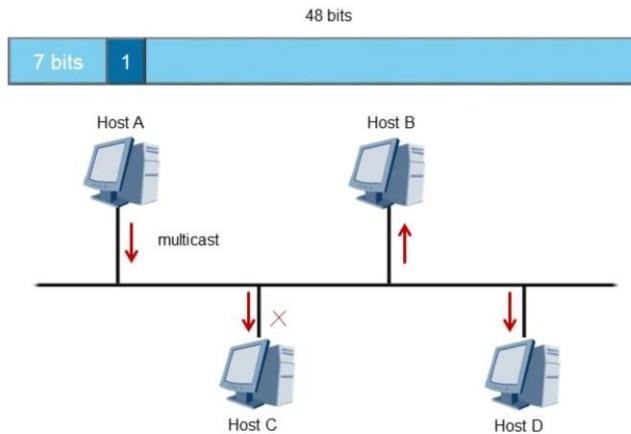
Page 15



Широковещательная передача представляет собой метод пересылки, который позволяет разослать фреймы из одного источника, и получить их во всех узлах в локальной сети. Чтобы разрешить отправку всем хостам в локальной сети, поле MAC-адреса назначения фрейма заполняется значением, которое в шестнадцатеричном виде определено как FF:FF:FF:FF:FF и которое указывает, что все получатели фрейма с указанным адресом должны принять этот фрейм и обработать его заголовок и концевик.

Широковещательные передачи используются протоколами для облегчения ряда важных сетевых процессов, включая обнаружение и поддержку работы сети, однако они также генерируют чрезмерный трафик, который часто вызывает прерывания в конечных системах и перегрузку полосы пропускания, из-за чего может снижаться общая производительность сети.

Многоадресатная пересылка фреймов



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 16

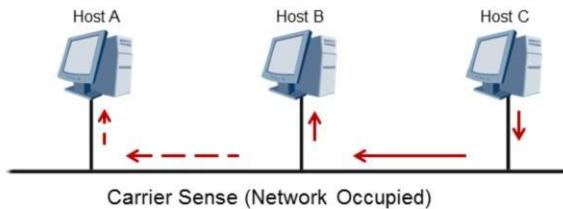


Более эффективной альтернативой широковещательной передаче является многоадресатный фрейм, который начал заменять широковещательные передачи во многих новых технологиях. Многоадресатная пересылка может пониматься как форма избирательной широковещательной передачи, которая позволяет выбирать хостов, чтобы прослушивать специальный MAC-адрес многоадресатной передачи в дополнение к одноадресатному MAC-адресу, который связан с хостом, и обрабатывать любые фреймы, содержащие MAC-адрес многоадресатной передачи в MAC-адресе назначения поля фрейма.

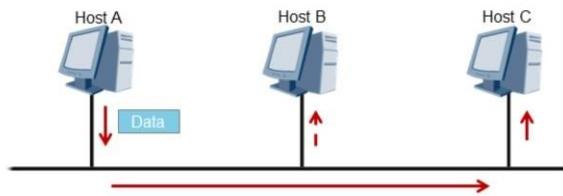
Поскольку нет взаимного различия между форматами одноадресатных MAC-адресов и многоадресатных MAC-адресов, адрес многоадресатной рассылки изменен с использованием 8-го бита первого октета. Если значение этого бита равно 1, оно показывает, что адрес является частью диапазона MAC-адресов многоадресатной передачи, в отличие от одноадресатных MAC-адресов, где это значение всегда равно 0.

В локальной сети истинные возможности многоадресатной передачи на канальном уровне ограничены, поскольку маршрутизация остается аналогичной широковещательному фрейму, где прерывания распространены по всей сети. Единственное явное отличие от технологии широковещания заключается в выборочной обработке данных на конечных устройствах. По мере расширения сети для поддержки нескольких локальных сетей, настоящее преимущество многоадресатной технологии как эффективного средства передачи становится более очевидным.

Контроль несущей



Carrier Sense (Network Occupied)



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

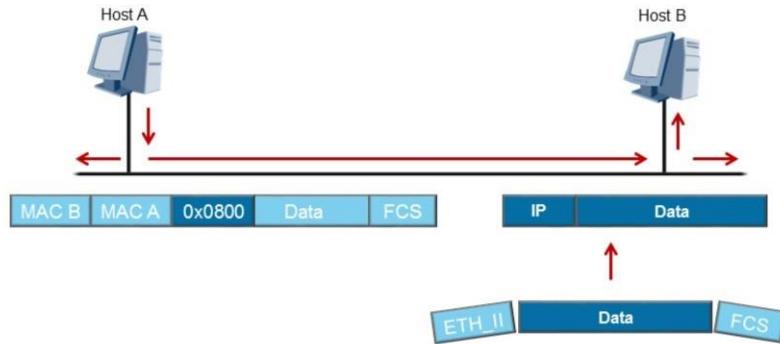
Page 17



По мере того, как трафик подготавливается к пересылке по физической сети, хостам в общих доменах коллизии необходимо определить, занимает ли какой-либо трафик в настоящее время среду передачи. Средства передачи, например, в случае 10Base2, обеспечивают общую среду передачи, в которой должен быть применен CSMA/CD для обеспечения обработки коллизий, если они произойдут. Если в канале будет обнаружена передача фрейма, хост задержит пересылку своих собственных фреймов до тех пор, пока канал не станет доступен, после чего хост начнет пересылать фреймы с физического интерфейса в направлении назначенного адресата.

Если два хоста подключены через среду передачи, поддерживающую полнодуплексную передачу, как в случае, например, с 10BaseT, считается, что передаваемые фреймы не могут пострадать от коллизий, поскольку передача и прием фреймов происходит по отдельным проводам, и поэтому нет необходимости в CSMA/CD.

Обработка фреймов



- Получение, обработка и отбрасывание инструкций канального уровня (для фрейма)

Как только фрейм отправлен с физического интерфейса хоста, он переносится по среде к его пункту назначения. В случае общей сети фрейм может быть принят несколькими хостами, которые будут оценивать, предназначен ли фрейм им, путем анализа MAC-адреса назначения в заголовке фрейма. Если MAC-адрес назначения и MAC-адрес хоста не совпадают, или MAC-адрес назначения не является широковещательным или многоадресатным MAC-адресом, который прослушивается хостом, то фрейм будет проигнорирован и отброшен.

Для назначенного адресата фрейм будет принят и обработан после подтверждения, что фрейм предназначен для физического интерфейса данного хоста. Хост должен также подтвердить, что во время передачи целостность фрейма была сохранена, взяв значение поля контрольной суммы фрейма (FCS) и сравнив это значение со значением, определяемым принимающим хостом. Если значения не совпадают, фрейм будет считаться поврежденным и впоследствии будет отброшен.

Для действительных фреймов хост затем должен будет определить следующий этап обработки, проанализировав поле типа заголовка фрейма и определив протокол, для которого предназначен этот фрейм. В данном примере поле типа фрейма содержит шестнадцатеричное значение 0x0800, которое говорит о том, что данные, взятые из фрейма, должны быть перенаправлены в протокол Интернета (IP), перед чем отбрасываются заголовок и концевик фрейма.



Итог

- Каким образом Ethernet определяет протокол, к которому должен быть доставлен обрабатываемый фрейм?
- Каким образом определяется, должен ли быть фрейм обработан или откинут после получения его устройством?

1. Фреймы канального уровня содержат поле типа, которое ссылается на следующий протокол, которому должны быть отправлены данные, содержащиеся в фрейме. Обычными примерами протоколов пересылки являются IP (0x0800) и ARP (0x0806).
2. MAC-адрес назначения, содержащийся в заголовке фрейма, анализируется принимающим конечным устройством и сравнивается с MAC-адресом интерфейса, на котором был получен фрейм. Если MAC-адрес назначения и MAC-адрес интерфейса не совпадают, фрейм отбрасывается.



Thank you

www.huawei.com

IP-адресация

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

Протокол Интернета предназначен для предоставления средств межсетевой связи, которая не поддерживается протоколами более низкого уровня, таких как Ethernet. Применение логической (IP) адресации позволяет использовать протокол Интернета другими протоколами для пересылки данных между сетями в виде пакетов. Для эффективного проектирования сети должно быть обеспечено отличное знание IP-адресации, а также четкое знакомство с поведением протокола для понимания IP как маршрутизируемого протокола.

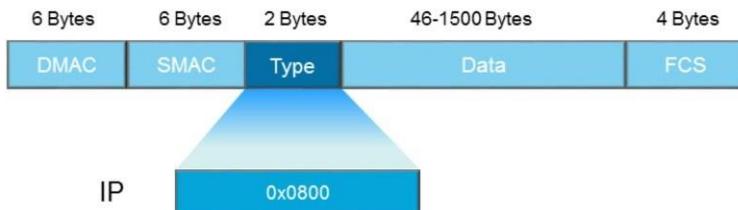


Цели

По завершении этого раздела проходящие обучение смогут:

- Описывать поля и характеристики, содержащиеся в IP.
- Различать публичные, приватные и специальные диапазоны IP-адресов.
- Успешно применять VLSM-адресацию.
- Объяснять назначение IP-шлюза.

Обработка следующего заголовка

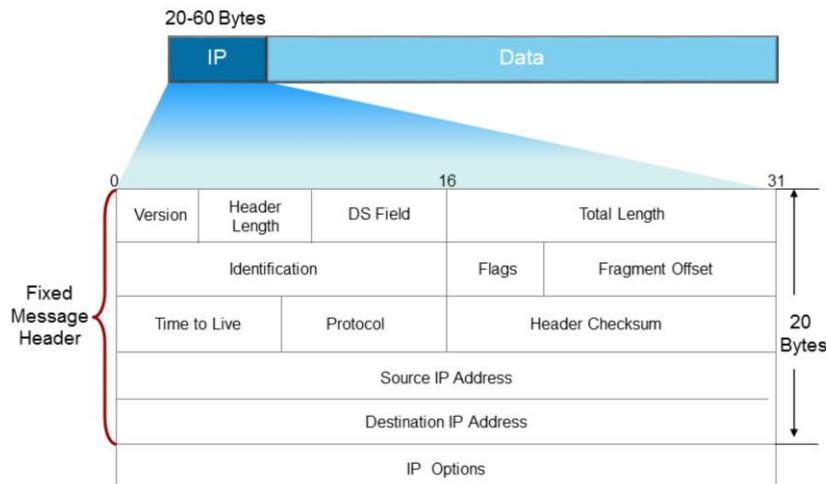


- Следующий набор инструкций для обработки находится в поле типа заголовка фрейма

Перед отбрасыванием заголовка и концевика фрейма необходимо, чтобы был обработан следующий набор инструкций для их определения из заголовка фрейма. Как показано, это осуществляется путем определения значения поля типа, которое в этом случае обозначает фрейм, предназначенный для IP-протокола, заканчивая процесс обработки фрейма.

Ключевая функция фрейма - определить, достигнуто ли предполагаемое физическое назначение, что фрейм остался неповрежденным. Основное внимание в этом разделе будет уделено тому, как обрабатываются данные после отбрасывания заголовков фреймов и распространения оставшихся данных в протоколе Интернета.

Заголовок IP-пакета



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 5



IP-заголовок используется для поддержки двух ключевых операций, маршрутизации и фрагментации. Маршрутизация — это механизм, позволяющий перенаправлять трафик из одной сети в другие, поскольку канальный уровень представляет собой только одну сеть со своими границами. Фрагментацией называется разбивка данных на удобные для передачи по сети блоки.

IP-заголовок переносится как часть данных и представляет собой служебные данные размером не менее 20 байт, которые определяют то, как трафик может быть переслан между сетями, и где конечный пункт назначения находится в сети, отличной от сети, в которой данные были первоначально отправлены. Поле версии определяет версию IP, которая в данный момент используется, в данном случае версия 4 или IPv4. Поле DS первоначально называлось полем типа обслуживания, однако теперь оно функционирует как поле для поддержки различных сервисов, в основном используется в качестве механизма для применения качества обслуживания (quality of service - QoS) для оптимизации сетевого трафика, однако этот материал находится за рамками данного курса.

IP-адресация источника и получателя представляет собой логические адреса, назначенные хостам и используемые для соединения отправителя и назначенного получателя на сетевом уровне. IP-адресация позволяет проводить оценку, находится ли назначенный конечный пункт в пределах данной или другой сети, как средство помочь процессу маршрутизации между сетями, с целью достигнуть пункты назначения за пределами локальной сети.

IP-адресация

Network	Host
192.168.1	.1
11000000.10101000.00000001	.00000001

- IP-адрес определяет сеть и хоста сети.
- Стандартная система счисления для IP-адресации - двоичная

Каждый адрес IPv4 представляет собой 32-битное значение, которое часто отображается в десятичном формате с точками, но для подробного понимания базового поведения также представлено в двоичном формате. IP-адреса работают как идентификаторы для конечных систем, а также других устройств в сети, как средство обеспечения доступности таких устройств как локально, так из источников, которые расположены удаленно, за пределами границ текущей сети.

IP-адрес состоит из двух информационных полей, которые используются для четкого указания сети, к которой принадлежит IP-адрес, и идентификатора хоста в пределах сети, который, по большей части, уникален в данной сети.

IP-адресация

Network Address

192.168.1	.0
11000000.10101000.00000001	.00000000

Broadcast Address

192.168.1	.255
11000000.10101000.00000001	11111111

- Верхние и нижние значения адреса хоста зарезервированы

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 7



Каждый сетевой диапазон содержит два важных адреса, которые исключаются из назначаемого сетевого диапазона хостам или другим устройствам. Первым из этих исключенных адресов является сетевой адрес, который представляет всю заданную сеть, а не конкретный хост в сети. Сетевой адрес можно идентифицировать, обратившись к полю хоста сетевого адреса, в котором все двоичные значения в этом диапазоне установлены на 0, также следует отметить, что полностью нулевое двоичное значение не всегда может представлять нулевое значение в десятичном формате с точками.

Второй исключенный адрес — это широковещательный адрес, который используется сетевым уровнем для ссылки на любую передачу, которая должна будет быть отправлена всем получателям в данной сети. Широковещательный адрес определяется в поле хоста IP-адреса, где для всех двоичных значений в этом диапазоне установлено значение 1. Адреса узлов составляют диапазон, который существует между сетевым и широковещательным адресами.

Десятичное, двоичное и шестнадцатеричное представления

Format	Value Range	Base Value
Binary	0 — 1	2
Decimal	0 — 9	10
Hexadecimal	0 — F	16

- Двоичная и шестнадцатеричная системы чаще всего используются в IP-сетях

Использование двоичных, десятичных и шестнадцатеричных обозначений обычно применяется во всех IP-сетях для представления схем адресации, протоколов и параметров, поэтому знание фундаментальной конструкции этих базовых представлений важно для понимания поведения и применения численных значений в IP-сетях.

Каждая система счисления представлена разной базой, которая определяет количество цифр, используемых для обозначений. В случае двоичной системы используются только два значения: 0 и 1, которые в совокупности могут обеспечивать бесконечное число значений, часто представляемых как 2^x в степени x , где x обозначает количество двоичных значений. Шестнадцатеричная система счисления представляет собой нотацию с базой 16 со значениями от 0 до F, (0-9 и A-F), где A представляет следующее значение после 9, а F, таким образом, представляет собой значение, эквивалентное 15 в десятичной или 1111 в двоичной системе счисления.

Перевод двоичной и десятичной систем счисления

Bit Order	1	1	1	1	1	1	1	1
Binary Power	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Binary	128	64	32	16	8	4	2	1

Decimal	Binary	Hexadecimal
0	00000000	00
1	00000001	01
2	00000010	02
3	00000011	03
4	00000100	04
5	00000101	05
6	00000110	06
7	00000111	07
8	00001000	08

Decimal	Binary	Hexadecimal
9	00001001	09
10	00001010	0A
11	00001011	0B
12	00001100	0C
13	00001101	0D
14	00001110	0E
15	00001111	0F
...
255	11111111	FF

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 9



Байт содержит 8 бит и является обычным обозначением в IP-сетях, поэтому байт представляет собой битовую величину 256, имея значения от 0 до 255. Это явно можно увидеть при переводе десятичной нотации в двоичную, и использовании степени базы с каждым двоичным значением для достижения диапазона значений 256 бит. Перевод нумерации в двоичную можно увидеть в примере для ознакомления с нумерацией в двоичной системе. В этом примере также четко показано, как представлены значения широковещательных адресов в десятичной, двоичной и шестнадцатеричной системах счисления для обеспечения широковещательной передачи как в IP-адресации, так и в MAC-адресации на сетевом и канальном уровнях.

Перевод из двоичной системы счисления

	Network			Host
Binary	11000000	10101000	00000001	00000001
	$2^7 + 2^6$	$2^7 + 2^5 + 2^3$	2^0	2^0
Decimal	192	168	1	1

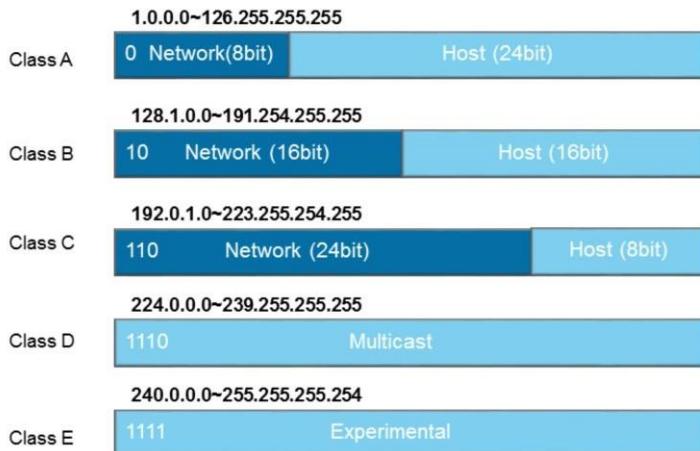
Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 10



Комбинация 32 битов в IP-адресе соответствует четырем октетам или байтам, каждый из которых может представлять диапазон значений 256, что дает теоретическое число 4'294'967'296 возможных IP-адресов, однако на самом деле только часть из общего количества адресов может быть присвоена хостам. Каждый бит в байте представляет степень базы, и поэтому каждый октет может представлять конкретный сетевой класс, причем каждый сетевой класс основывается либо на одном октете, либо на комбинации октетов. В этом примере три октета использовались для представления сети, а четвертый октет представлял диапазон хостов, поддерживаемых сетью.

Классы IP-адресов



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 11



Количество октетов, поддерживаемых сетевым адресом, определяется классами адресов, на которые разбивается область адресов IPv4. Классы А, В и С являются назначаемыми диапазонами адресов, каждый из которых поддерживает различное количество сетей и хостов, которые могут быть назначены для данной сети. Класс А, в данном случае, состоит из 126 возможных сетей, каждая из которых поддерживает 2^{24} или 16'777'216 адресов хоста, однако нужно иметь в виду, что сетевые и широковещательные адреса диапазона классов не могут быть назначены хостам.

На самом деле, одна сеть Ethernet никогда не сможет поддерживать такое большое количество хостов, поскольку Ethernet плохо масштабируется, отчасти из-за широковещательных передач, которые генерируют чрезмерный сетевой трафик в рамках одной локальной сети. Диапазоны адресов класса С позволяют создать гораздо более сбалансированную сеть, которая хорошо масштабируется в случае с Ethernet, обеспечивая чуть более 2 миллионов возможных сетей, а каждая сеть может поддерживать около 256 адресов, из которых 254 могут быть назначены хостам.

Класс D — это диапазон адресов, зарезервированных для многоадресатной передачи, чтобы хосты могли прослушивать определенный адрес в этом диапазоне, и если адрес назначения пакета является многоадресатным, который прослушивается хостом, то пакет обрабатывается таким же образом как пакет, IP-адресом хоста. Каждый класс легко различим в двоичном формате, если просмотреть значение бита в первом октете, в классе А, например, главный (первый) бит октета всегда будет 0, тогда как в классе В первые два бита старшего порядка всегда как 1 и 0, что позволяет легко различать классы в двоичном формате.

Типы IP-адресов

Private Address Ranges	
Class A	10.0.0.0~10.255.255.255
Class B	172.16.0.0~172.31.255.255
Class C	192.168.0.0~192.168.255.255

Special Addresses	
Diagnostic	127.0.0.0 ~ 127.255.255.255
Any Network	0.0.0.0
Network Broadcast	255.255.255.255

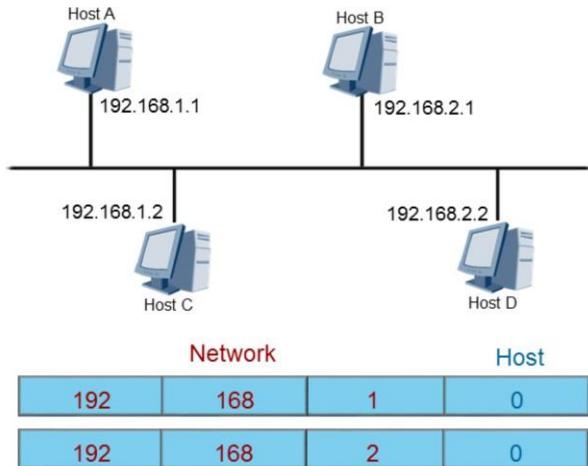
- IP-адреса сетей были поделены, и некоторые конкретные адреса и диапазоны получили специальные назначения в сети

В IPv4 определенные адреса и диапазоны адресов были зарезервированы для специальных целей. Чтобы отсрочить быстрое уменьшение количества доступных IP-адресов, в диапазонах адресов классов А, В и С существуют диапазоны частных адресов. Сегодня число фактических конечных систем и устройств, которые требуют IP-адресации, превышает 4'294'967'296 адресов, которые доступны в 32-битном диапазоне IPv4, поэтому решение этой нарастающей проблемы заключалось в том, чтобы выделить диапазоны частных адресов, которые могли бы быть назначены частным сетям, с целью сохранения адресов общедоступных сетей, которые обеспечивают обмен данными через общие сети, такие как Интернет.

Частные сети стали популярны в корпоративных сетях, однако хосты не могут взаимодействовать с общедоступной сетью, так как эти же диапазоны адресов могут быть использованы повторно во многих других корпоративных сетях. Трафик, предназначенный для общедоступной сети, таким образом, должен пройти процесс перевода адресов перед тем, как данные смогут достичь назначенного адресата.

Другими специальными адресами являются диагностический диапазон, определяемый как 127.0.0.0, а также первый и последний адреса в диапазоне адресов IPv4, где 0.0.0.0 представляет любую сеть, а его применение будет рассмотрено более подробно вместе с принципами маршрутизации. Адрес 255.255.255.255 является широковещательным адресом в IPv4 (0.0.0.0), однако диапазон любой широковещательной передачи в IP ограничен границами локальной сети, из которой она и исходит.

IP-связь



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

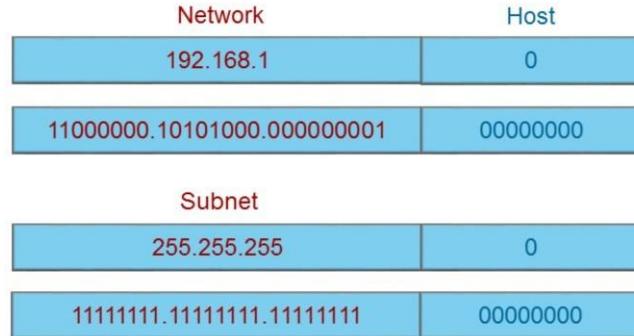
Page 13



Чтобы хост передал трафик адресату, хост должен знать сеть назначения. Хост, естественно, знает о сети, к которой он принадлежит, но обычно он не знает о других сетях, даже если эти сети являются частью одной и той же физической сети. Поэтому хосты не будут отправлять данные адресату, пока хост не узнает о его сети и, таким образом, интерфейс, через который может быть достигнут адресат.

Чтобы хост переслал трафик другому хосту, он должен сначала определить, является пункт назначения частью той же IP-сети. Это достигается путем сравнения конечной сети с исходной (IP-адрес хоста), из которой и отправляются данные. В случае, если сетевые диапазоны совпадают, пакет может быть перенаправлен на нижние уровни, на которых уже Ethernet займется обработкой фреймов. В случае же, когда сеть назначения отличается от исходной сети, хост должен иметь информацию о назначеннной конечной сети и интерфейсе, через который пакет/фрейм должен быть отправлен до того, как пакет будет обработан нижними уровнями. Без этой информации хост отбросит пакет прежде, чем он достигнет канального уровня.

Маска подсети



- Маски подсети позволяют различать, какие двоичные значения, представляют (под)сеть, а какие - хост

Идентификация уникального сегмента сети определяется применением значения маски, которое используется для различения количества бит, представляющих сегмент сети, причем остальные биты показывают количество хостов, поддерживаемых в данном сегменте сети. Сетевой администратор может разделить сетевой адрес на подсети, чтобы широковещательные пакеты могли передаваться только в пределах одной подсети. Мaska подсети состоит из строки непрерывных 1, за которой следует аналогичная непрерывная строка из 0. Единицы соответствуют полю ID сети, а нули соответствуют полю ID хоста.

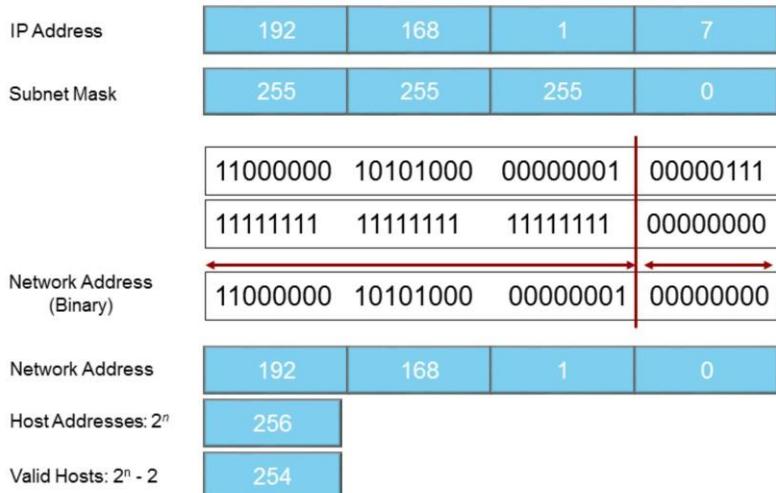
Маска подсети по умолчанию

Class A	255	0	0	0
Class B	255	255	0	0
Class C	255	255	255	0

- Определенные маски подсети применяются к диапазонам адресов по умолчанию для обозначения фиксированного диапазона, который используется для каждого сетевого класса

Для каждого класса сетевого адреса применяется соответствующая маска подсети для указания размера сегмента сети по умолчанию. Любая сеть, которая является частью диапазона адресов класса А, фиксируется с помощью маски подсети по умолчанию, содержащей 8 левых битов, которые соответствуют первому октету IP-адреса, причем оставшиеся три октета остаются доступными для назначения ID хоста. Аналогичным образом, сеть класса В имеет маску подсети по умолчанию 16 бит, что позволяет увеличить количество сетей в пределах класса В за счет количества хостов, которые могут быть назначены для стандартной сети. В сети класса С по умолчанию используется 24-битная маска, которая обеспечивает большое количество потенциальных сетей, но значительно ограничивает количество хостов, которые могут быть назначены в стандартной сети. Стандартные сети обеспечивают обыкновенную границу диапазонов адресов, однако диапазоны адресов классов А и В не обеспечивают практического масштаба для выделения адресов для сетей на основе Ethernet.

Планирование адресов



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 16



Применение маски подсети к данному IP-адресу позволяет идентифицировать сеть, к которой принадлежит хост. Мaska подсети также покажет широковещательный адрес для сети и количество хостов, которые поддерживаются в данном сетевом диапазоне. Такая информация обеспечивает основу для эффективного планирования сетевых адресов. В приведенном примере хост имеет адрес 192.168.1.7 с применением 24-битной маски подсети по умолчанию (класс С). Разделив части IP-адреса, которые представляют собой сегмент сети и хоста, можно определить сетевой адрес по умолчанию для данного сегмента.

Под этим понимается адрес, где все значения битов хоста установлены равными 0, в этом случае создается сетевой адрес по умолчанию 192.168.1.0. Если значения хоста представлены непрерывной строкой из 1, то это широковещательный адрес. Если последний октет содержит строку из 1, он представляется десятичным значением 255, и широковещательный адрес будет 192.168.1.255.

Возможные адреса хоста подсчитываются на основе формулы 2^n , где n представляет количество битов хоста, определяемое маской подсети. В данном примере n представляет равно 8 битам хоста, и 2^8 , таким образом, дает 255 хостов. Однако для определения числа используемых адресов хостов нужно из этого результата вычесть сетевые и широковещательные адреса, и тогда количество допустимых адресов хостов будет равно 254.

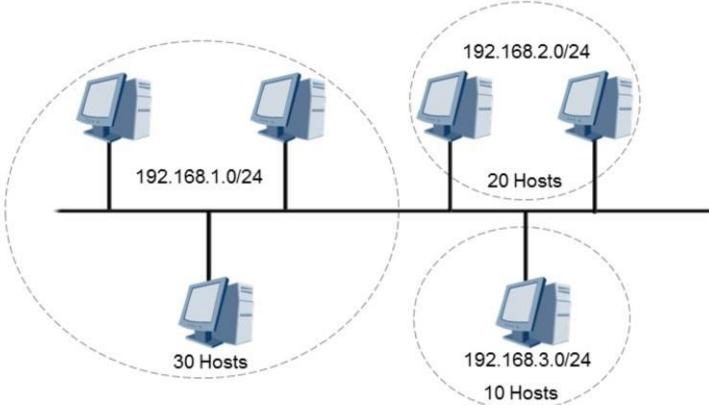
Задача

IP Address	172	16	1	7
Subnet Mask	255	255	0	0
Network Address	?	?	?	?
Host Addresses: 2^n	?			
Valid Hosts: $2^n - 2$?			

- Определите сеть для данного IP-адреса, и количество фактических и действительных адресов хостов в сети

В задании дан обычный диапазон адресов класса В, для которого необходимо определить сеть, к которой принадлежит указанный хост, а также широковещательный адрес и количество действительных хостов, поддерживаемых данной сетью. Применяя те же принципы, что и для диапазона адресов класса С, можно определить сетевой адрес хоста, а также их диапазон в данной сети.

Ограничения адресации



- Проектирование сети с использованием стандартной маски подсети приводит к бесполезной потере адресов

Одно из основных ограничений стандартной маски проявляется, когда на данном предприятии используются несколько диапазонов сетевых адресов для создания логических границ между хостами в одной физической корпоративной сети. При использовании базовой схемы адресации может быть использовано ограниченное количество хостов, связанных с данной сетью, в случае использования нескольких сетей для обеспечения логической сегментации сети. Тем не менее, большое количество адресного пространства остается неиспользованным, тем самым демонстрируя неэффективность использования стандартной маски подсети.

Вычисление VLSM

IP Address	192	168	1	7
Subnet Mask	255	255	255	128
	11000000	10101000	00000001	00000111
	11111111	11111111	11111111	10000000
	11000000	10101000	00000001	00000000
Network Address	192	168	1	0
Host Addresses: 2^n	128			
Valid Hosts: $2^n - 2$	126			

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

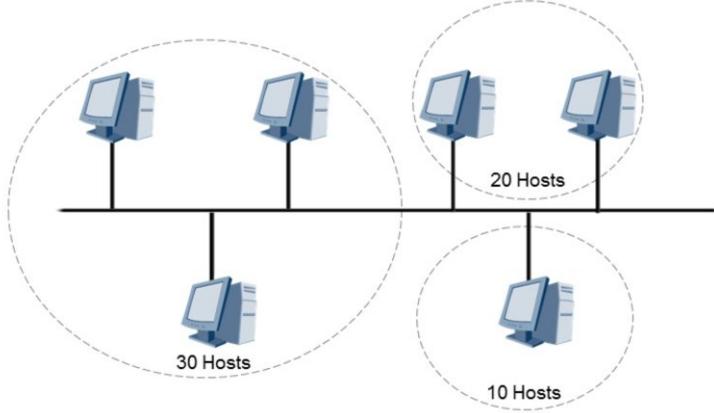
Page 19



В качестве средства устранения ограничений стандартных масок подсети вводится концепция масок подсети переменной длины, которые позволяют разбивать стандартную маску подсети на несколько подсетей, которые могут иметь фиксированную длину (например, маска подсети фиксированной длины или FLSM) или переменной длины, известной как VLSM. Применение таких масок подсети состоит в использовании стандартной классовой сети, и делении ее посредством манипулирования маской подсети. В приведенном примере были внесены простейшие изменения для сети класса C, которая по умолчанию управляется 24-битной маской. Изменение заключается в заимствовании бита из ID хоста и использовании его как части сетевого адреса. При смещении битов по сравнению со стандартной сетью, дополнительные биты представляют собой ID подсети.

В данном случае был взят один бит, и из этой подсети могут быть получены две разные подсети, поскольку одно битовое значение может представлять только два состояния - 1 или 0. Если бит установлен на 0, он представляет значение 0, если он установлен на 1, он представляет собой значение 128. При настройке битов хоста на 0 адрес подсети можно найти для каждой подсети, установив биты хоста на 1, широковещательные адреса для каждой подсети также можно найти. Количество поддерживаемых хостов в этом случае равно 2^7 за исключением подсетевых и широковещательных адресов для каждой подсети, в результате чего каждая подсеть будет поддерживать в общей сложности 126 действительных адресов хоста.

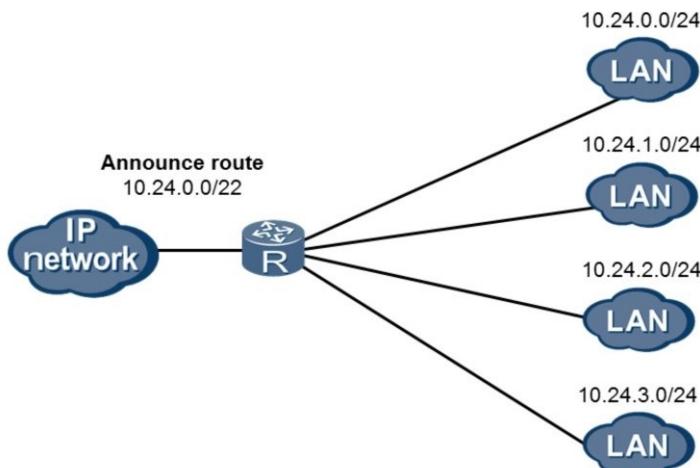
VLSM Сценарий случая



- Используя только сеть 192.168.1.0/24, реализуйте VLSM для заданного количества хостов в каждом сегменте сети.

В связи с проблемой ограничения адресов, из-за которых сети по умолчанию имели увеличенное количество сбоев адресов, концепция масок подсети переменной длины может применяться для уменьшения потерь адресов и обеспечения более эффективной схемы адресации для корпоративной сети. Определяется один диапазон адресов класса C класса по умолчанию, для которого требуются маски подсети с переменной длиной, чтобы разместить каждую из логических сетей в пределах одного диапазона адресов по умолчанию. Для эффективного назначения маски подсети требуется определить количество хост-бит, необходимое для размещения требуемого количества хостов, для которых остальные хост-биты могут быть применены как часть ID подсети, который представляет собой вариант ID сети из адреса сети по умолчанию.

Бесклассовая Междоменная Маршрутизация



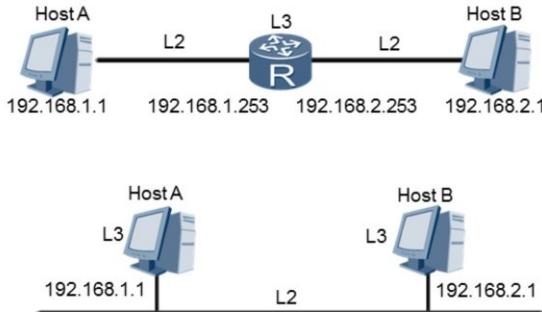
Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 21



Бесклассовая междоменная маршрутизация была первоначально введена как решение для проблем, возникающих в результате быстрого роста того, что теперь известно как Интернет. Основная проблема заключалась в неизбежном исчерпании адресного пространства класса В, которое обычно принималось организациями среднего размера в качестве наиболее подходящего диапазона адресов, где класс С был неприменимым, а класс А был слишком обширным, и управление 65534 адресами хостов может быть достигнуто посредством VLSM. Кроме того, продолжающийся рост означал, что шлюзовые устройства, такие как маршрутизаторы, начали увеличиваться в количестве, чтобы не отставать от растущего числа сетей, которым, как ожидается, будут необходимы такие устройства. Приведенное решение включает переход к бесклассовой системе адресации, в которой классические границы были заменены адресными префиксами. Эта нотация работает по принципу, что классовые диапазоны адресов, такие как класса C, могут быть поняты как имеющие 24-битный префикс, который представляет подсеть или основную границу сети, и для которых можно суммировать несколько сетевых префиксов в одну большую сеть адресных префиксов, который представляет одни и те же сети, но как один адресный префикс. Это помогло облегчить количество маршрутов, которые содержатся, в частности, в широкомасштабных устройствах маршрутизации, работающих в глобальном масштабе, и предоставило более эффективные средства управления адресами. Результат CIDR имеет далеко идущие последствия и, как понимается, эффективно замедляет общую скорость исчерпания адресного пространства IPv4.

IP шлюзы

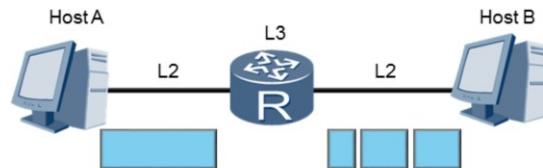


- Используя IP шлюзы передают пакеты между сетями
- Хосты могут действовать как шлюзы между сетями в LAN

Для пересылки пакетов требуется, чтобы пакет сначала определял путь пересылки к данной сети и интерфейс, через который должен быть переадресован пакет, перед тем как быть инкапсулированным как кадр и перенаправленным из физического интерфейса. В случае, когда конечная сеть отличается от исходной сети, пакет должен быть перенаправлен на шлюз, через который пакет может достичь своего назначенного адресата.

Во всех сетях шлюз - это устройство, которое способно обрабатывать пакеты и принимать решения о том, как следует маршрутизировать пакеты, чтобы им достичь своего назначенного адресата. Однако рассматриваемое устройство должно знать маршрут до предполагаемой целевой IP-сети до того, как произойдет маршрутизация пакетов. Если сети разделяются при помощи физического шлюза, IP-адрес интерфейса (в той же сети или подсетевой сети), через который этот шлюз может быть достигнут, считается адресом шлюза. В случае хостов, принадлежащих к разным сетям, которые не разделены физическим шлюзом, хоста должен выполнять роль шлюза, для которого хост должен сначала знать маршрут для сети, в которую входят пакеты для пересылки и должен указывать IP-адрес собственного интерфейса хоста в качестве IP-адреса шлюза, через который может быть достигнута целевая сеть назначения.

IP фрагментация



Version	Header Length	DS Field	Total Length	
Identification		Flags	Fragment Offset	
Time to Live		Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
IP Options				

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 23

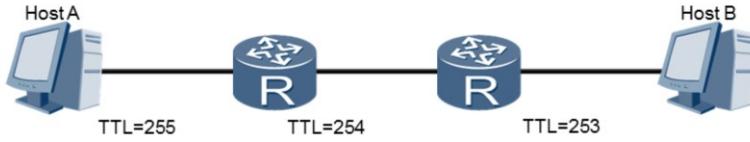


Данные пересылаемых пакетов существуют во многих форматах и состоят из разных размеров, часто размер передаваемых данных превышает размер, который поддерживается для передачи. Там, где это происходит, необходимо, чтобы блок данных был разбит на более мелкие блоки данных, прежде чем может произойти передача. Процесс разбивки этих данных на управляемые блоки известен как фрагментация.

Поля идентификации, флагов и полей смещения используются для управления повторной сборкой фрагментов данных после их получения в конечной точке назначения. Идентификация различает блоки данных потоков трафика, которые могут исходить от одного и того же хоста или разных хостов. Поле flags определяет, какой из фрагментов представляет собой последний фрагмент, в котором время начала таймера запускается до повторной сборки и уведомляется о том, что должна начинаться сборка пакета.

Наконец, смещение фрагмента помещает значение бита для каждого фрагмента как часть количества фрагментов, первый фрагмент установлен со значением 0, а последующие фрагменты определяют значение первого бита, следующего за предыдущим фрагментом, например, где исходный фрагмент содержит бит данных от 0 до 1259, последующему фрагменту будет присвоено значение смещения 1260.

Время жизни



Version	Header Length	DS Field	Total Length	
Identification		Flags	Fragment Offset	
Time to Live	Protocol	Header Checksum		
Source IP Address				
Destination IP Address				
IP Options				

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

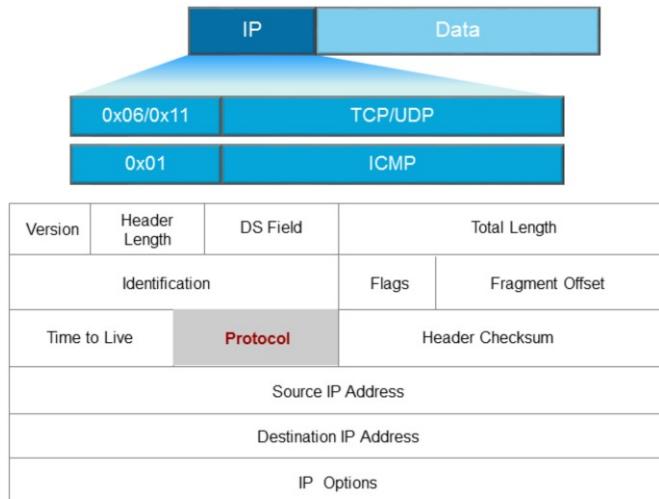
Page 24



Поскольку пакеты пересыпаются между сетями, пакеты могут попадать в петли, потому что маршруты к IP-сетям были неправильно определены в устройствах, ответственных за маршрутизацию трафика между несколькими сетями. Это может привести к тому, что пакеты будут потеряны в течение цикла пересылки пакетов, что не позволит пакету достичь своего назначенного адресата. В этом случае перегрузка в сети будет возникать по мере того, как все больше и больше пакетов, предназначенных для одного и того же пункта назначения, становятся предметом одной и той же участи, до тех пор, пока сеть не будет заполнена ошибочными пакетами.

Чтобы предотвратить такую перегрузку, возникающую в случае петель, поле времени для жизни (TTL) определяется как часть заголовка IP, которое уменьшается на значение 1 каждый раз, когда пакет обходит устройство уровня 3, чтобы достичь определенной сети. Начальное значение TTL может варьироваться в зависимости от исходного источника, однако, если значение TTL уменьшится до значения 0, пакет будет отброшен и сообщение об ошибке (ICMP) будет возвращено источнику на основе исходного IP-адреса, который можно найти в IP-заголовке блуждающего пакета.

Поле Protocol



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 25



После проверки того, что пакет достиг своего назначенного адресата, сетевой уровень должен определить следующий набор инструкций, которые должны быть обработаны. Это определяется путем анализа поля протокола заголовка IP. Как и в поле типа заголовка фрейма, шестнадцатеричное значение используется для указания следующего набора инструкций для обработки. Следует понимать, что поле протокола может ссылаться на протоколы на сетевом уровне, например, в случае протокола управляющих сообщений Интернета (ICMP), но также может ссылаться на протоколы верхнего уровня, таких как протокол управления передачей (06/0x06) или протокол пользовательских дейтаграмм (17/0x11), оба из которых существуют как часть транспортного уровня как в справочных моделях TCP/IP, так и в OSI.



Итог

- Для чего используется маска IP подсети?
- Для чего используется TTL поле в заголовке IP?
- Как используются шлюзы в IP сети?

1. Маска подсети IP представляет собой 32-битное значение, которое описывает логическое деление между битовыми значениями IP-адреса. IP-адрес как таковой разделен на две части, для которых значения битов представляют собой сеть или подсеть, а также хост в данной сети или подсетевой сети.
2. IP-пакеты, которые не могут достичь предполагаемой сети, подвержены бесконечной пересылке между сетями, пытаясь обнаружить их конечный пункт назначения. Функция Time To Live (TTL) используется для обеспечения того, чтобы время жизни применялось ко всем IP-пакетам, чтобы гарантировать, что в случае, если IP-пакет не сможет достичь своего назначения, он в конечном итоге будет прекращен. Значение TTL может варьироваться в зависимости от исходного источника.
3. Шлюзы представляют точки доступа между IP-сетями, к которым может быть перенаправлен трафик, или маршрутизироваться в том случае, если целевая сеть назначения зависит от сети, в которой был создан пакет.



Thank you

www.huawei.com

Протокол межсетевых управляющих сообщений
(ICMP)

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

ICMP - это протокол, который работает вместе с IP как форма обмена сообщениями, чтобы компенсировать ненадежность IP. Внедрение ICMP необходимо для ознакомления с поведением многочисленных операций и приложений, которые в значительной степени зависят от ICMP, чтобы поддерживать базовую передачу сообщений, так как на их основе часто выполняются процессы.

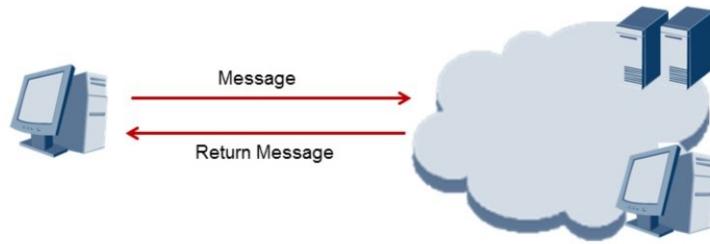


Цели

После завершения этой главы вы сможете:

- Описать процессы, в которых применяется ICMP
- Определять типы и значения используемые в ICMP
- Объяснить функцию ICMP в ping и traceroute приложениях

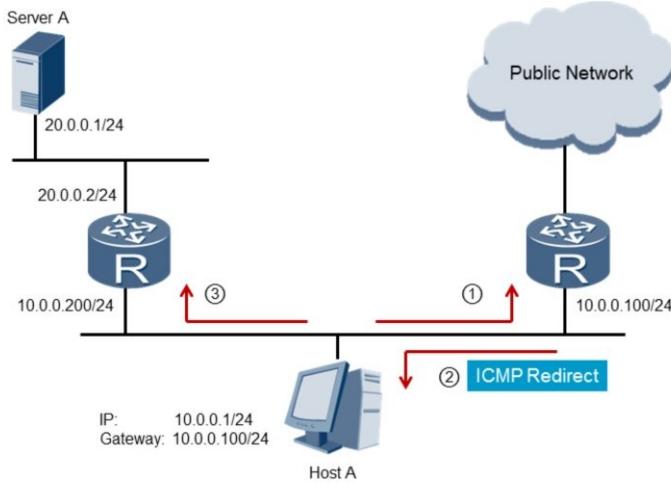
ICMP



- ICMP сообщения используются для поддержки множественных операций, включая маршрутизацию, диагностику ошибок

Протокол управляющих сообщений Интернета является неотъемлемой частью IP, предназначенный для облегчения передачи уведомлений между шлюзами и исходными узлами, где необходимы запросы на диагностическую информацию, поддержку маршрутизации и как средство сообщения об ошибках в обработке дейтаграмм. Назначение этих управляющих сообщений - обеспечить обратную связь о проблемах в среде связи и не гарантировать, что дейтаграмма будет доставлена, или что управляющее сообщение будет возвращено.

ICMP (Маршрутизация)



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 5



Сообщения ICMP Redirect представляют собой общий сценарий, в котором ICMP используется как средство облегчения функций маршрутизации. В этом примере пакет пересыпается шлюзу хостом А на основе адреса шлюза узла А. Шлюз идентифицирует, что полученный пакет отправляется на адрес следующего шлюза, который является частью одного и того же как хост, который инициировал пакет, выделяя неоптимальное поведение пересылки между хостом и шлюзами.

Чтобы разрешить это, сообщение переадресации отправляется хосту. Сообщение о переадресации советует хосту отправить свой трафик для предполагаемого адресата непосредственно на шлюз, с которым связана целевая сеть, поскольку это представляет собой более короткий путь к получателю. Однако шлюз отправляет данные исходного пакета в место назначения.

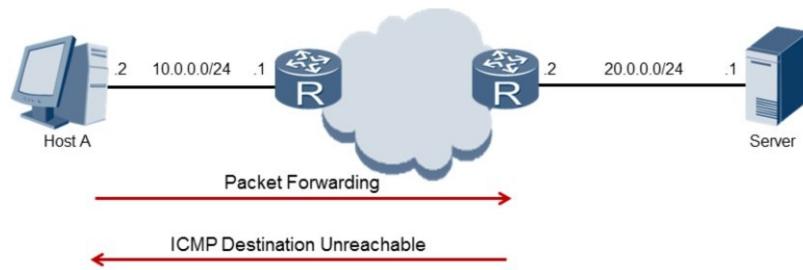
ICMP (Диагностика)



- Два раздельных сообщения используются для запроса и
- Их связывает Ping приложение

Эхо-сообщения ICMP представляют собой средство диагностики для определения, в первую очередь, связи между данным источником и получателем, но также предоставляют дополнительную информацию, такую как время прохождения в оба конца для передачи, диагностику для измерения задержки. Данные, полученные в эхо-сообщении, возвращаются как отдельное сообщение ответа эха.

ICMP (Ошибки)



- Уведомляет источник пакетов о проблемах с пересылкой пакетов.
- Используется исходный IP-адрес в заголовке IP для уведомления.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

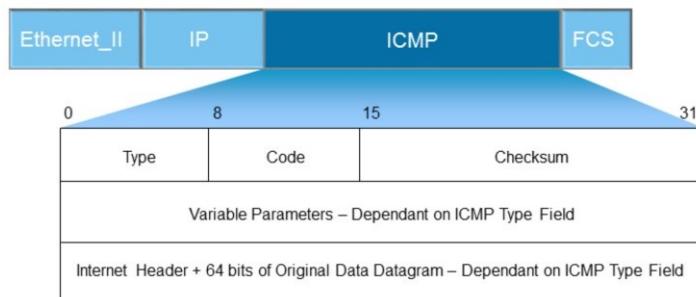
Page 7



ICMP предоставляет различные сообщения об ошибках, которые часто определяют проблемы доступности и генерируют конкретные отчеты об ошибках, которые позволяют более четко понимать с точки зрения хоста причину отказа передачи информации до цели.

Типичные примеры включают случаи, когда в сети могут возникать петли, и, как следствие, время истечения срока действия параметра в заголовке IP заканчивается, в результате чего генерируется сообщение об ошибке «ttl превышено в пути». Другие примеры включают недопустимый пункт назначения, который не известна принимающему шлюзу, или что предполагаемый узел в целевой сети не обнаружен. Во всех случаях ICMP-сообщение генерируется на основе исходного IP-адреса, найденного в заголовке IP, чтобы гарантировать, что сообщение уведомляет отправляющий узел.

ICMP Format



- ICMP параметры представлены в type/code формате

Дополнительные данные обычно передаются для определения недоставленных

Сообщения ICMP отправляются с использованием основного IP-заголовка, функции которого - неотъемлемая часть сообщения ICMP, например, с параметром TTL, который используется для предоставления поддержки для определения того, доступна ли цель. Формат сообщения ICMP зависит от двух полей для идентификации сообщений в виде формата type/code, где поле type содержит общее описание типа сообщения, а code более конкретные параметры для типа сообщения. Контрольная сумма предоставляет средство проверки целостности сообщения ICMP. Дополнительные 32 бита включены для предоставления переменных параметров, часто неиспользуемых и, таким образом, устанавливаются как 0 при отправке сообщения ICMP, однако в таких случаях, как перенаправление ICMP, это поле содержит IP-адрес шлюза, которому хост должен перенаправлять пакеты. Поле параметров в случае эхо-запросов будет содержать идентификатор и порядковый номер, используемый для помощи отправителю-источнику отправленных эхо-запросов с полученными ответами эха, особенно в случае, когда несколько запросов перенаправляются в заданный пункт назначения.

В качестве окончательного способа отслеживания данных для конкретного процесса сообщение ICMP может передаваться заголовок IP и часть данных, которые содержат информацию верхнего уровня, которая позволяет источнику идентифицировать процесс, для которого произошла ошибка, например, случаи, когда ICMP TTL истекает в пути.

ICMP Type/Code Поля

Type	Code	Description
0	0	Echo Reply
3	0	Network Unreachable
3	1	Host Unreachable
3	2	Protocol Unreachable
3	3	Port Unreachable
5	0	Redirect Datagram for the Network
8	0	Echo Request

- Значение Type обозначает формат сообщения
- Значение Code обеспечивает более точное описание сообщения

Существует большое количество значений типа ICMP для четкого определения различных приложений протокола управления ICMP. В некоторых случаях поле code не требуется, чтобы предоставить более конкретную запись в поле type, как показано с помощью эхо-запросов, которые имеют поле типа 8 и соответствующий ответ, который генерируется и отправляется в виде отдельного сообщения ICMP в адрес источника отправителя и определяется с использованием поля типа 0.

В качестве альтернативы, определенные типы полей определяют очень общий тип, для которого действие определяется через поле code, как в случае параметра типа 3. Поле типа 3 указывает, что данный пункт назначения недоступен, в то время как поле кода отражает конкретное отсутствие сети, хоста, протокола, порта (TCP/UDP), способности выполнять фрагментацию (код 4) или маршрута источника (например, код 5), в котором пакет, для которого путь пересылки по сети строго или частично определен, не достигает своего адресата.

ICMP Приложение - Пинг



```
<RTA>ping ?
-a      Select source IP address, the default is the IP address of
       the output interface
-c      Specify the number of echo requests to be sent, the
       default is 5
-n      Numeric output only. No attempt will be made to lookup
       host addresses for symbolic names
-t      Timeout in milliseconds to wait for each reply, the
       default is 2000ms
STRING<1-255> IP address or hostname of a remote system
.....
<RTA>ping 10.0.0.2
```

Применение ICMP можно понять с помощью таких инструментов, как Ping. Приложение Ping может использоваться как инструмент, чтобы определить, доступно ли место назначения, а также собирать другую связанную информацию. Параметры приложения Ping позволяют конечному пользователю определять поведение конечной системы при генерации сообщений ICMP с учетом размера дейтаграммы ICMP, количества сообщений ICMP, генерируемых хостом, а также продолжительности, в которой это ожидается, что ответ будет получен до истечения тайм-аута. Это важно, когда происходит большая задержка, так как тайм-аут может быть сообщен приложением Ping до того, как сообщение ICMP получит возможность вернуться к источнику.

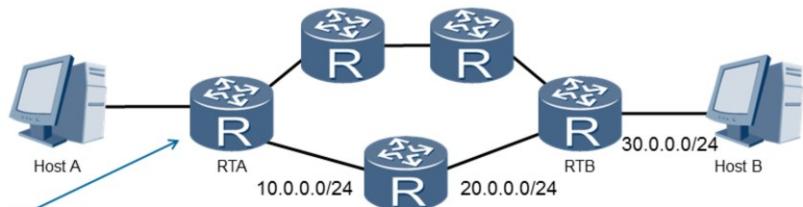
Ping Результаты

```
<RTA>ping 10.0.0.2
PING 10.0.0.2 : 56 data bytes, press CTRL_C to break
Reply from 10.0.0.2 : bytes=56 Sequence=1 ttl=255 time=340 ms
Reply from 10.0.0.2 : bytes=56 Sequence=2 ttl=255 time=10 ms
Reply from 10.0.0.2 : bytes=56 Sequence=3 ttl=255 time=30 ms
Reply from 10.0.0.2 : bytes=56 Sequence=4 ttl=255 time=30 ms
Reply from 10.0.0.2 : bytes=56 Sequence=5 ttl=255 time=30 ms

--- 10.0.0.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 10/88/340 ms
```

Общий вывод ответа ICMP на созданный Ping запрос ICMP указывает место назначения, которому была отправлена дейтаграмма, и размер генерируемой дейтаграммы. Кроме того, отображается порядковый номер поля последовательности, который переносится как часть ответа эха (тип 0) вместе со значением TTL, которое берется из заголовка IP, а также время округления, которое снова переносится как часть поля IP-параметров в заголовке IP.

ICMP Приложение - Трассировка



```
<RTA>tracert ?
-a      Set source IP address, the default is the IP
address of the output interface
-f      First time to live, the default is 1
-m      Max time to live, the default is 30
-name   Display the host name of the router on each hop
-p      Destination UDP port number, the default is 33434
STRING<1-255> IP address or hostname of a remote system
.....
<RTA>tracert 30.0.0.2
```

Другим распространенным приложением к ICMP является traceroute, который обеспечивает средство измерения пути пересылки и задержки на основе переходов между несколькими сетями посредством ассоциации со значением TTL в заголовке IP.

Для данного адресата достижимость до каждого скачка вдоль пути измеряется путем первоначального определения значения TTL в IP-заголовке 1, в результате чего значение TTL истекает до того, как принимающий шлюз сможет больше распространять ICMP сообщение, тем самым генерируя истекший в транзите TTL сообщение вместе с информацией о временной отметке, что позволяет оценивать маршрут маршрута, пройденного по сети, по дейтаграмме до места назначения, и измерять время прохождения в оба конца. Это обеспечивает эффективное средство определения точки потери или задержки пакетов, которые могут быть в сети, а также помогает в обнаружении петель маршрутизации.

Traceroute Результаты

```
<RTA>tracert 30.0.0.2  
traceroute to 30.0.0.2(30.0.0.2), max hops:30, packet length:40,  
press CTRL_C to break  
1 10.0.0.2 130 ms 50 ms 40 ms  
2 20.0.0.2 80 ms 60 ms 80 ms  
3 30.0.0.2 80 ms 60 ms 70 ms
```

TTL значение используется для определения лимита прыжков для каждого множества результатов.

Traceroute отображает результаты каждого прыжка

Реализация traceroute в маршрутизаторах серии Huawei ARG3 использует протокол транспортного уровня UDP для определения служебного порта в качестве адресата. Каждый скачок посыпает три пробных пакета, для которых значение TTL изначально устанавливается равным 1 и увеличивается после каждого трех пакетов. Кроме того, для первого пакета задан порт назначения UDP 33434 и увеличивается для каждого последующего отправленного пробного пакета. Сгенерированный результат прыжков позволяет определить путь, а также любую общую задержку, которая может возникнуть для его обнаружения.

Это достигается путем измерения времени между отправкой сообщения ICMP и получением соответствующего TTL при транзитной ICMP-ошибке. При получении пакета конечный пункт назначения не может обнаружить порт, указанный в пакете, и таким образом возвращает пакет ICMP Type 3, Code 3 (Port Unreachable), и после трех попыток тест traceroute заканчивается. Результат теста каждой пробы отображается источником в соответствии с путём, взятым в пункт назначения. Если при использовании команды трассировки возникает ошибка, может отображаться следующая информация:

- !H: Host недоступен.
- !N: Сеть недоступна.
- !: Порт недоступен.
- !P: Тип протокола неверен.
- !F: Пакет неправильно фрагментирован.
- !S: Исходный маршрут неверен.



Итог

- Какие два типа сообщений ICMP используются как часть успешного Ping?
- В случае, если значение TTL в IP-заголовке дейтаграммы достигает нуля, какое действие будет приниматься принимающим шлюзом?

1. Приложение Ping использует сообщение запроса эха типа 8, чтобы попытаться обнаружить пункт назначения. Отдельное сообщение эхоС ответа, определяемое полем типа 0, возвращается исходному источнику на основе исходного IP-адреса в поле заголовка IP.
2. В случае, если значение TTL IP-дейтаграммы достигает 0 до того, как дейтаграмма сможет достичь назначенного адресата, шлюзовое устройство, принимающее дейтаграмму, продолжит отбрасывать его и возвращает сообщение ICMP источнику, чтобы уведомить, что дейтаграмма в итоге не смогла добраться до намеченного пункта назначения. Конкретная причина будет определяться значением кода, чтобы отразить, например, был ли отказ вызван неспособностью обнаружить хост, порт на хосте или не поддерживалась служба для данного протокола и т. д.



Thank you

www.huawei.com

Протокол определения адреса (ARP)

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

Для того чтобы передача данных в место назначения сети была успешной, необходимо создать связь между протоколами сетевых и нижних уровнях. Средства, с помощью которых используется протокол преобразования адресов для предотвращения ненужного дополнительного широковещательного трафика в сети должны быть четко поняты.

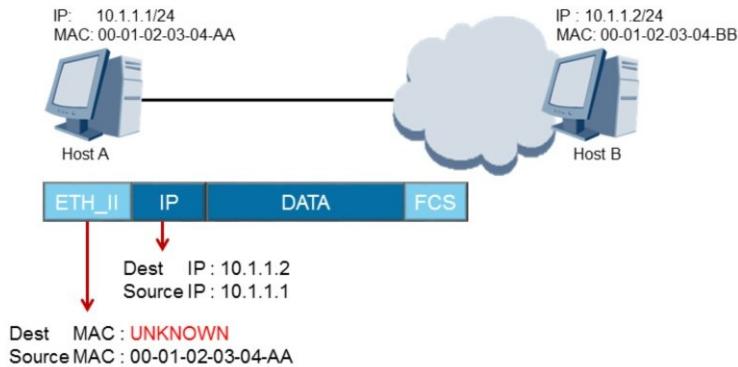


Цели

После завершения этой главы вы сможете:

- Объяснить, как разрешается MAC адрес, при помощи ARP
- Объяснить функцию таблицы ARP кэша

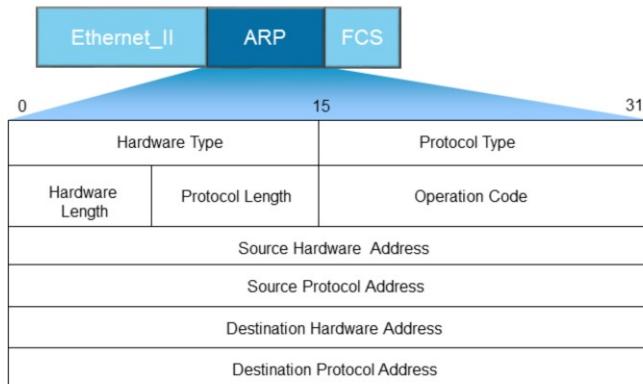
ARP



- Пересылка линии передачи данных основана на знании MAC-адреса пункта назначения канала передачи данных.

По мере инкапсуляции данных IP-протокол на сетевом уровне может указать IP-адрес назначения, которому в конечном итоге предназначены данные, а также интерфейс, через который данные должны быть переданы, однако до того, как передача может произойти, источник должен знать об адресе назначения Ethernet (MAC), которому должны передаваться данные. Протокол преобразования адресов (ARP) представляет собой важную часть пакета протоколов TCP/IP, который позволяет обнаруживать адреса пересылки MAC для обеспечения доступности IP-адресов. Ethernet-скажок должен быть обнаружен до завершения инкапсуляции данных.

ARP Формат



- Пакет ARP работает на границе линии передачи данных, как это можно понять из-за отсутствия IP-заголовка.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 5

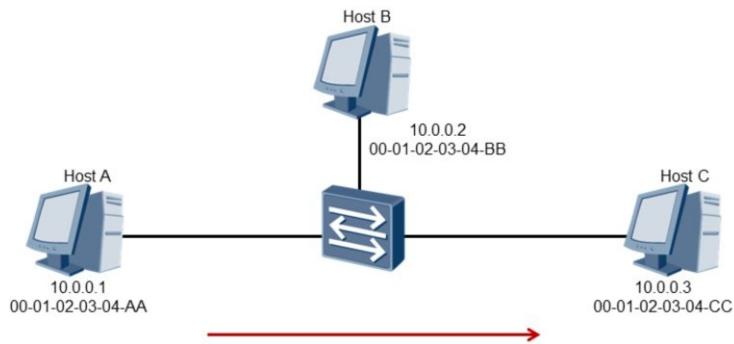


Пакет ARP генерируется как часть процесса обнаружения физического целевого адреса. Первоначальное обнаружение будет содержать частичную информацию, поскольку должен быть обнаружен адрес аппаратного назначения или MAC-адрес. Тип аппаратного обеспечения относится к Ethernet с типом протокола, относящимся к IP, определяя технологию, связанные с обнаружением ARP. Размер аппаратного обеспечения и протокола определяет длину адреса для MAC-адреса Ethernet и IP-адреса и определяется в байтах.

Код операции определяет одно из двух состояний, где обнаружение ARP установлено как REQUEST, для которого прием ARP из точки назначения будет определять, что должен быть сформирован ответ. Ответ будет генерировать REPLY, для которого больше не требуется принимающий хост для этого пакета, после чего пакет ARP будет отброшен. Исходный аппаратный адрес относится к MAC-адресу отправителя на физическом сегменте, к которому создается ARP. Адрес исходного протокола относится к IP-адресу отправителя.

Аппаратный адрес назначения указывает физический (Ethernet) адрес, по которому данные могут быть перенаправлены стандартами протокола Ethernet, однако эта информация отсутствует в запросе ARP, вместо этого заменяется значением 0. Адрес целевого протокола определяет предполагаемый IP-адрес предназначенный для достижения достижимости по Ethernet.

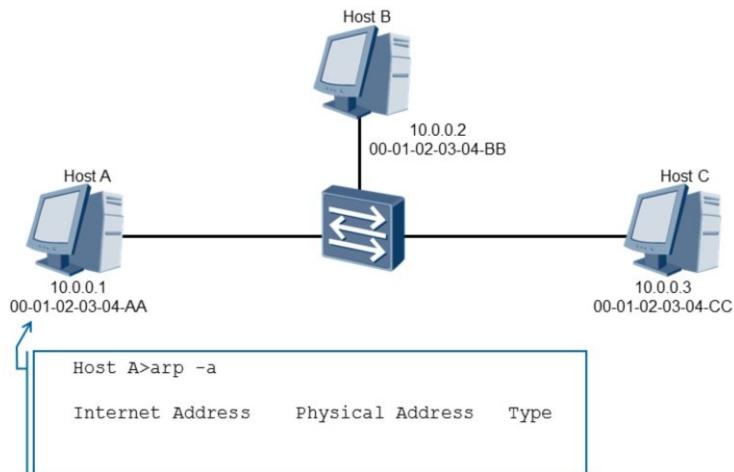
ARP Процесс



- Host A желает переслать данные в Host C, но сначала он должен понять, может ли он достичь места назначения на уровне канала

Сетевой уровень представляет собой логический путь между источником и получателем. Достигение намеченного IP-адресата зависит, во-первых, на то, чтобы установить физический путь к назначенному адресату, и для этого необходимо создать связь между назначенным целевым IP-адресом и физическим интерфейсом следующего перехода, которому может быть перенаправлен трафик. Для данного адресата хост определит IP-адрес, по которому данные должны быть переадресованы, однако до того, как инкапсуляция данных может начаться, хост должен определить, известен ли путь физической пересылки. Если путь пересылки известен, то инкапсуляция в пункт назначения может продолжаться, однако довольно часто пункт назначения неизвестно, и ARP должен быть реализован до того, как инкапсуляция данных может быть выполнена.

Поиск ARP Кэша



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 7

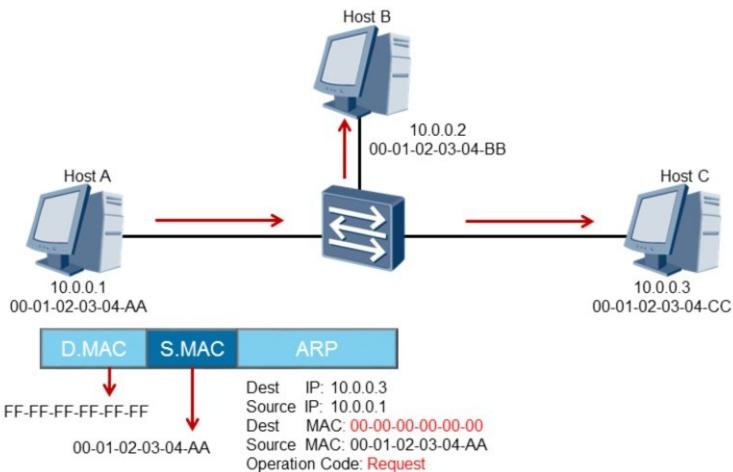


Кэш ARP - это таблица для объединения IP-адресов хоста и связанных с ними физических (MAC) адресов. Любой хост, который занимается связью с местным или удаленным пунктом назначения, сначала должен узнать о MAC-адресе назначения, посредством которого может быть установлено сообщение.

Выделенные адреса будут заполнять таблицу кэша ARP и оставаться активными в течение фиксированного периода времени, в течение которого предполагаемое место назначения может быть обнаружено без необходимости использования процессов обнаружения ARP. По истечении определенного периода времени таблица ARP-кеша удалит записи ARP для сохранения целостности таблицы кэша ARP, поскольку любое изменение физического расположения целевого хоста может привести к тому, что отправляющий узел непреднамеренно обращается к данным в пункт назначения, в котором конечный узел больше не определен.

Поиск ARP-кеша - это первая операция, которую будет выполнять конечная система, прежде чем определять, нужно ли генерировать ARP-запрос. Для пунктов назначения за пределами собственной сети хостов выполняется поиск ARP-кеша для обнаружения физического адреса назначения шлюза, через который может быть достигнута необходимая сеть.

Процесс ARP Запроса



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

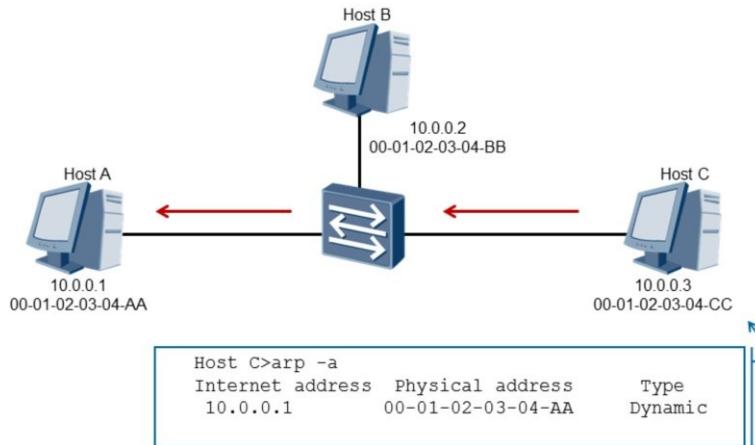
Page 8



Если запись кэша ARP не может быть определена, выполняется запрос Request ARP. Этот процесс включает в себя создание пакета запроса ARP и совокупности полей с адресами протокола источника и получателя, а также адрес исходного оборудования. Адрес устройства назначения неизвестен. Таким образом, адрес целевого аппаратного обеспечения заполняется значением, равным 0. Запрос ARP инкапсулируется в заголовок фрейма Ethernet как часть процесса пересылки. Исходный MAC-адрес заголовка кадра задается в качестве исходного адреса отправляющего узла.

Хост в настоящее время не знает о местонахождении адресата и поэтому должен отправлять запрос ARP в качестве широковещательной передачи всем адресатам в пределах одной и той же локальной сети. Это означает, что широковещательный адрес используется в качестве MAC-адреса назначения. Как только кадр заполняется, он перенаправляется на физический уровень, где он распространяется вдоль физического носителя, к которому подключен хост. Переданный пакет ARP будет заполнен по всей сети всем адресатам, включая любой шлюз, который может присутствовать, однако шлюз предотвратит пересылку этого широковещания в любую сеть за пределами текущей сети.

Процесс ARP Ответа



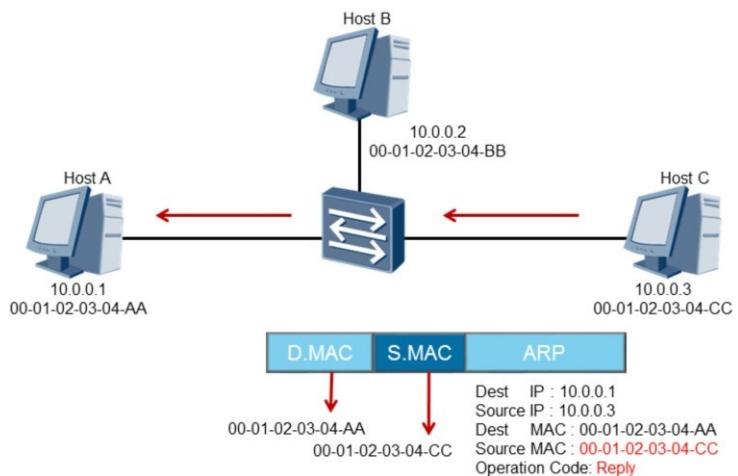
Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 9



Если предполагаемый сетевой узел существует, кадр будет поступать на физический интерфейс адресата, после чего будет выполняться обработка нижнего уровня. Передача ARP означает, что все адресаты на границе сети получат заполненный фрейм, но перестанут обрабатывать запрос ARP, поскольку адрес протокола назначения не соответствует IP-адресу этих адресатов. Если IP-адрес назначения совпадает с принимающим хостом, будет обработан пакет ARP. Принимающий узел сначала обработает заголовок фрейма, а затем обработает запрос ARP. Хост-получатель будет использовать информацию из поля исходного аппаратного адреса в заголовке ARP, чтобы заполнить свою собственную таблицу кэша ARP, тем самым позволяя генерировать одноадресный кадр для любой пересылки фреймов, который может потребоваться, источнику, из которого ARP запрос был получен.

Процесс ARP Ответа



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

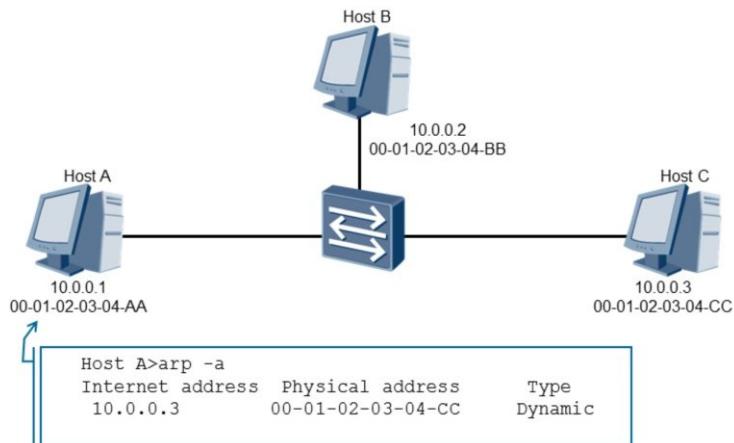
Page 10



Пункт назначения определит, что полученный ARP-пакет является ARP-запросом и продолжит генерировать ответ ARP, который будет возвращен источнику, на основе информации, найденной в заголовке ARP. Для ответа создается отдельный ARP-пакет, для которого будут заполнены поля адреса источника и адреса протокола назначения. Однако адрес целевого протокола в пакете запроса ARP теперь представляет адрес исходного протокола в ответном пакете ARP, и аналогичным образом адрес исходного протокола запроса ARP становится адресом целевого протокола в ответе ARP.

Поле адресного аппаратного адреса заполняется MAC-адресом источника, обнаруженным в результате приема запроса ARP. Для требуемого аппаратного адреса целевого ARP-запроса он включается в качестве исходного аппаратного адреса ответа ARP, а код операции настроен на ответ, чтобы сообщить адресату о назначении принятого пакета ARP, после чего конечный пункт способен отбрасывать пакет ARP без дальнейшей связи. Ответ ARP инкапсулируется в заголовок Ethernet с MAC-адресом назначения кадра Ethernet, содержащим запись MAC в таблице кэша ARP, что позволяет пересыпать кадр в виде кадра одноадресной передачи обратно на хост, который инициировал ARP запрос.

ARP Кэш



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

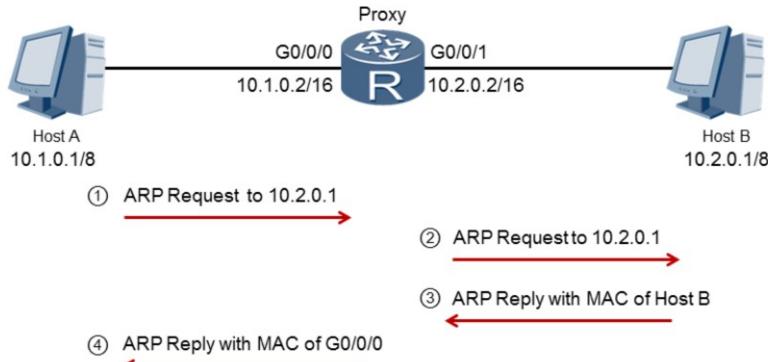
Page 11



После получения ответа ARP исходный узел будет проверять правильность назначенного адресата на основе заголовка фрейма, так же что заголовок пакета является ARP из поля типа и отбрасывать заголовки фреймов. Затем будет обработан ответ ARP с исходным аппаратным адресом ответа ARP, который будет использоваться для заполнения таблицы кэша ARP исходного узла (Host A).

После обработки ответа ARP пакет отбрасывается, и информация MAC-адреса пункта назначения используется для облегчения процесса инкапсуляции исходного приложения или протокола, изначально запрашивающего обнаружение адресата на уровне линии передачи данных.

ARP Прокси

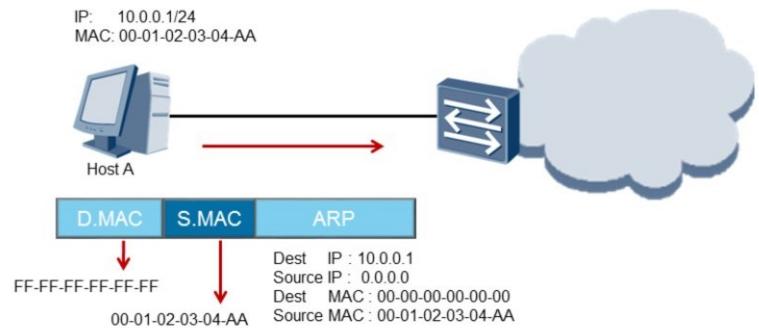


- Proxy ARP позволяет обнаруживать связь между сетями.
- Прокси отвечает собственным (G0/0/0) адресом от имени Host B.

Протокол ARP также применяется к другим случаям, например, когда должны быть реализованы прозрачные шлюзы подсети для облегчения связи между физическими сетями, где хосты считаются частью одной и той же подсети. Это называется Proxy ARP, поскольку шлюз работает как прокси-сервер для двух физических сетей. Когда ARP-запрос генерируется для адресата, который считается частью одной и той же подсети, запрос в конечном итоге будет получен шлюзом. Шлюз может определить, что предназначенный пункт назначения существует за пределами физической сети, на которой был сгенерирован запрос ARP. Поскольку запросы ARP не могут быть перенаправлены за пределы широковещательного домена, шлюз будет продолжать генерировать свой собственный запрос ARP для определения достижимости до предполагаемого адресата, используя свои собственные протокольные и аппаратные адреса в качестве исходных адресов для сгенерированного запроса ARP. Если предполагаемое место назначения существует, ответ ARP должен быть получен шлюзом, для которого используется аппаратный адрес источника назначения для заполнения таблицы кэша ARP шлюза.

Шлюз, после подтверждения доступности для предполагаемого адресата, генерирует ответ ARP исходному источнику (хост А), используя аппаратный адрес интерфейса, на который был отправлен ответ ARP. В результате шлюз будет действовать как агент между двумя физическими сетями для облегчения обмена каналами линии передачи данных, причем оба узла перенаправляют трафик, предназначенный для адресатов в разных физических сетях, к соответствующему физическому адресу шлюза «Прокси».

Самообращенные запросы ARP



- Дублирование IP адресов может быть применимо в единой IP сети.
- ARP может использоваться для обнаружения конфликтов IP адресов

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 13



В случае, когда новое оборудование вводится в сеть, необходимо, чтобы хост определял, является ли адрес протокола, которому он был назначен, уникальным в сети, чтобы предотвратить конфликты с повторяющимися адресами. Запрос ARP генерируется как средство определения того, является ли адрес протокола уникальным, установив адрес назначения в ARP-запросе равным собственному IP-адресу хоста. Запрос ARP заливается по всей сети всем адресатам канального уровня, устанавливая MAC-адрес назначения как широковещательный, чтобы гарантировать, что все конечные станции и шлюзы получат заполненный кадр. Все адресаты будут обрабатывать кадр, и если какой-либо пункт назначения обнаружит, что IP-адрес назначения в запросе ARP совпадает с адресом принимающей конечной станции или шлюза, ответ ARP будет сгенерирован и возвращен хосту, который сгенерировал запрос ARP.

С помощью этого метода исходный хост может идентифицировать дублирование IP-адреса в сети и помечать конфликт IP-адреса, чтобы запросить назначение уникального адреса. Это средство генерации запроса, основанного на собственном IP-адресе хостов, определяет основные принципы самообращенного ARP.



Итог

- Прежде чем генерировать запрос ARP, какие действия необходимо предпринять конечной станции?
- В каких случаях генерируются самообращенные сообщения ARP и распространяются локальной сети?

1. Хост должен сначала определить, знает ли он адрес перенаправления уровня канала в своем собственном кеше ARP (таблица MAC-адресов). Если обнаружена запись, конечная система способна создать фрейм для пересылки без помощи протокола разрешения адреса. Если запись не может быть найдена, процесс ARP будет инициироваться, и запрос ARP будет транслироваться в локальной сети.
2. Самообращенные сообщения ARP обычно генерируются в том месте, где IP-адрес настроен или изменен для устройства, подключенного к сети, и в любое время, когда устройство физически подключено к сети. В обоих случаях самообращенный процесс ARP должен гарантировать, что используемый IP-адрес остается уникальным.



Thank you

www.huawei.com

More Learning Resources: <http://Learning.huawei.com/en>

Транспортный уровень

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

Уровни передачи связаны со сквозным поведением протоколов уровня передачи, которые определяются после того, как данные достигнут места назначения. TCP и UDP представляют собой обычно поддерживаемые протоколы в сетях IP. Характеристики данных, такие как чувствительность к задержке и необходимость в надежности часто определяют протоколы, используемые в уровнях передачи. В этом разделе основное внимание уделяется знанию того, как характеристики поддерживаются посредством поведения каждого протокола.

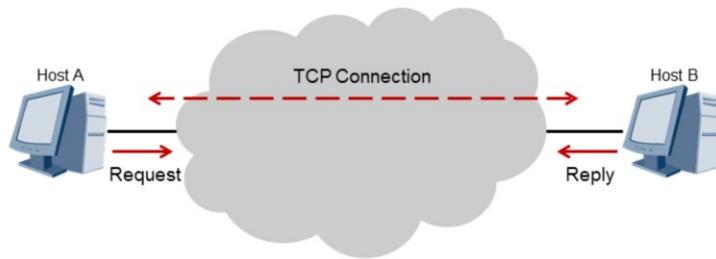


Цели

По завершении этого раздела слушатели смогут:

- Описать общие различия между TCP и UDP.
- Описать формы данных, к которым применяются TCP и UDP.
- Определить известные номера портов на основе TCP и UDP.

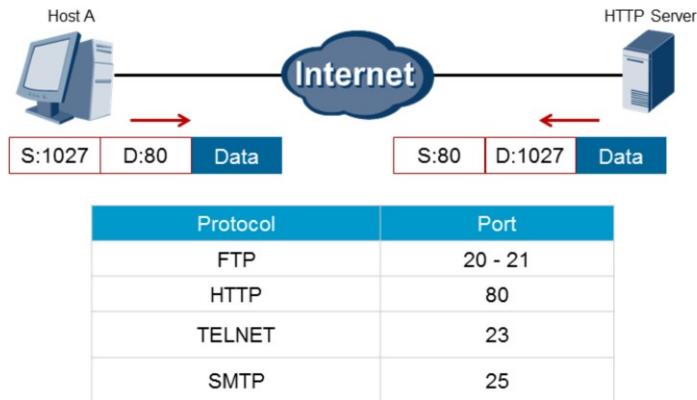
Протокол управления передачей



- Соединение устанавливается перед отправкой данных.

TCP - это протокол, основанный на подключении, сквозной протокол, который существует как часть уровня передачи стека протоколов TCP/IP, чтобы поддерживать приложения, которые охватывают многосетевые среды. Протокол управления передачей обеспечивает средство надежной межпроцессной связи между парами процессов на хост-компьютерах, которые подключены к различным, но взаимосвязанным сетям компьютерной связи. TCP использует протоколы более низкого уровня, чтобы обеспечить доступность между хостами, поддерживающими процесс, по которым устанавливается надежная служба соединения между парами процессов. Ориентированное на соединение поведение TCP включает предварительные обмены между источником и получателем, через которые соединение устанавливается до передачи сегментов уровней связи.

TCP порты



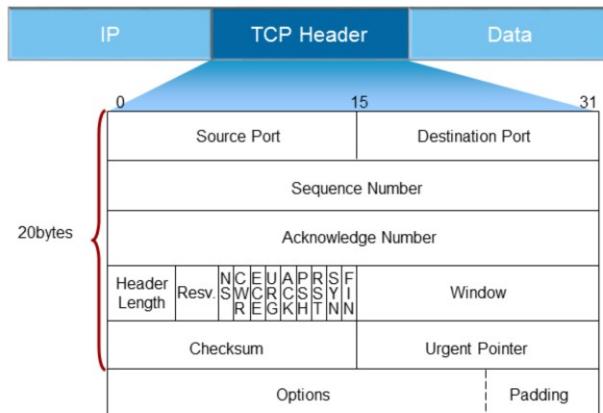
- Порты представляют собой отдельные службы, такие как перечисленные выше.

В качестве средства, позволяющего многим процессам внутри одного хоста использовать средства связи TCP одновременно, TCP предоставляет набор логических портов в каждом хосте. Значение порта вместе с адресом сетевого уровня называется сокетом, для которого пара сокетов предоставляет уникальный идентификатор для каждого соединения, в частности, когда сокет используется одновременно в нескольких соединениях. То есть процесс может потребовать различать несколько потоков обмена между собой и другим процессом (или процессами), для которого каждый процесс может иметь несколько портов, через которые он обменивается данными с портом или портами других процессов.

Некоторые процессы могут владеть портами, и эти процессы могут инициировать подключения к портам, которые у них есть. Эти порты понимаются как назначенные IANA системные порты или известные порты и существуют в диапазоне значений порта от 0 до 1023. Диапазон назначенных пользователем или зарегистрированных портов IANA также существует в диапазоне 1024 - 49151, с динамическими портами, также известными как частные или эфемерные порты в диапазоне от 49152 до 65535, которые не ограничены каким-либо конкретным приложением. Хосту обычно присваивается значение пользовательского порта, для которого сокет генерируется для данного приложения.

Общие примеры приложений на основе TCP, для которых были назначены известные номера портов, включают FTP, HTTP, TELNET и SMTP, которые часто будут работать вместе с другими известными почтовыми протоколами, такими как POP3 (порт 110) и IMAP4 (порт 143).

TCP Заголовок



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 6

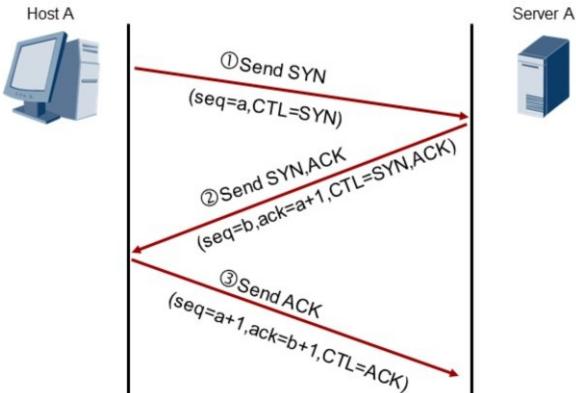


Заголовок TCP позволяет TCP-приложениям устанавливать потоки данных, ориентированные на соединение, которые предоставляют надежность и к которым применяется управление потоком. Номер исходного порта создается, когда хост намеревается установить соединение с приложением на основе TCP, для которого порт назначения будет относиться к хорошо известному/зарегистрированному порту, к которому относится известное/зарегистрированное приложение.

Биты кода представляют собой функции в TCP и включают в себя URG, совместно используемое поле срочных указателей для пользовательских уведомлений о срочных данных, подтверждение полученных октетов в связи с полем подтверждения (ACK), функцию push для пересылки данных (PSH), операции сброса соединения (RST), синхронизация порядковых номеров (SYN) и указание, что от отправителя больше не требуется получать данные (FIN). Дополнительные кодовые биты были введены в виде ECN-Echo (ECE) и флагов с уменьшенными окнами (CWR) в качестве средства поддержки уведомления о перегрузке для приложений с задержкой TCP.

Явное сообщение о несоответствии с пересылкой (ECN) (NS) было введено как последующее изменение для устранения потенциального злоупотребления ECN, когда устройства вдоль пути передачи могут удалять метки перегрузки ECN. Поле «Параметры» содержит параметры, которые могут быть включены как часть заголовка TCP, часто используемого во время первоначального установления соединения, как в случае максимального значения размера сегмента (MSS), которое может использоваться для определения размера сегмента, который приемник должен использовать. Размер заголовка TCP должен быть в сумме 32 бита, и там, где это не так, будет выполнено заполнение 0 значений.

TCP Создание соединения

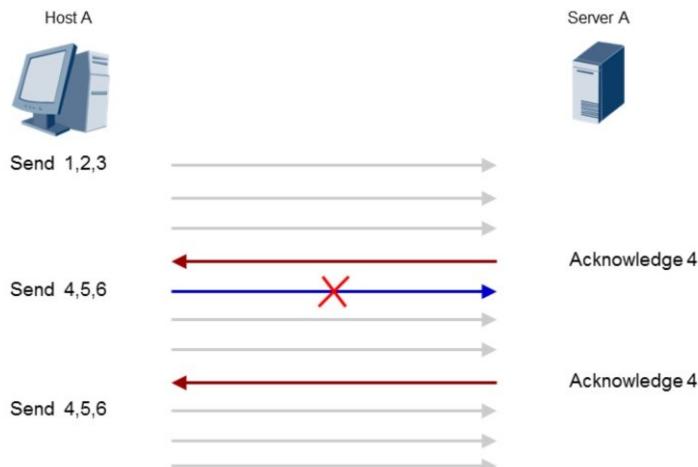


- TCP-соединение устанавливается после трехстороннего рукопожатия.

Когда двум процессам необходимо связаться, каждый TCP должен сначала установить соединение (инициализировать синхронизацию связи с каждой стороны). Когда связь завершена, соединение прекращается или закрывается, чтобы освободить ресурсы для других целей. Поскольку соединения должны устанавливаться между ненадежными хостами и ненадежным доменом Интернета, для устранения ошибочной инициализации соединений используется механизм рукопожатия с часовыми номерами последовательностей. Соединение происходит через ряд состояний во время создания. Состояние LISTEN представляет TCP, ожидающий запроса на соединение с любого удаленного TCP и порта. SYN-SENT возникает после отправки запроса на соединение и до получения соответствующего запроса. Состояние SYN-RECEIVED возникает во время ожидания подтверждения подтверждения запроса на соединение, после того как он получил и отправил запрос на соединение. Состояние ESTABLISHED происходит после рукопожатия, при котором создается открытое соединение, и полученные данные могут доставляться пользователю.

Механизм трехстороннего рукопожатия TCP начинается с того, что начальный порядковый номер генерируется инициирующим TCP как часть процесса синхронизации (SYN). Первоначальный сегмент TCP затем устанавливается с помощью бита кода SYN и передается в назначенный IP-адрес TCP для достижения состояния SYN-SENT. В рамках процесса подтверждения пиринговый TCP генерирует собственный порядковый номер, чтобы синхронизировать поток TCP в другом направлении. Этот пиринговый TCP будет передавать этот порядковый номер, а также номер подтверждения, который равен принятому порядковому номеру, увеличенному на единицу, вместе с установленными битами кода SYN и ACK в заголовке TCP для достижения состояния SYN-RECEIVED. Заключительный шаг рукопожатия подключения включает в себя исходный TCP, подтверждающий порядковый номер пирингового TCP, путем установки номера подтверждения, равного принятому порядковому номеру плюс один, вместе с битом ACK в заголовке TCP, позволяющим достичь состояния ESTABLISHED.

TCP Процесс передачи



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 8

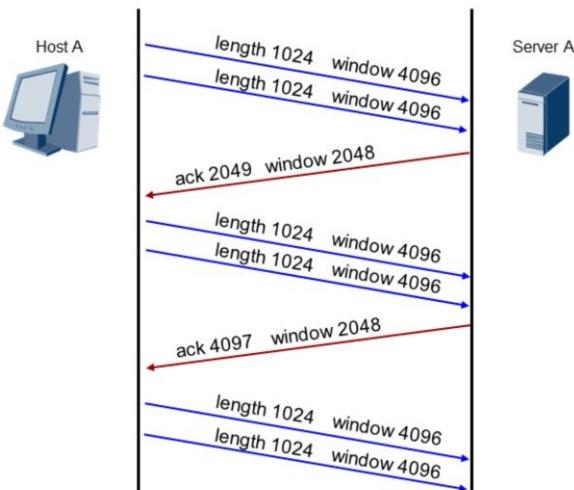


Поскольку передача TCP отправляется как поток данных, каждый октет может быть упорядочен, и поэтому каждый октет может быть подтвержден. Номер подтверждения используется для достижения этого, отвечая отправителю подтверждением приема данных, обеспечивая таким образом надежность передачи данных. Однако процесс подтверждения является кумулятивным, что означает, что строка октетов может быть подтверждена одним подтверждением, сообщая источнику порядковый номер, который сразу же следует за порядковым номером, который был успешно получен.

В примере число байтов (октетов) передается вместе до подтверждения TCP-подтверждения. Если октет не может быть передан адресату, последовательность передаваемых октетов будет подтверждена только до точки, в которой произошла потеря. Полученное подтверждение будет отражать октет, который не был получен, чтобы возобновить передачу с точки в потоке данных, в котором был потерян октет.

Возможность накапливать несколько октетов вместе до подтверждения позволяет TCP работать намного эффективнее, однако необходим баланс, чтобы гарантировать, что количество октетов, отправленных до подтверждения, не слишком велико, поскольку если октет не может быть принят, весь поток октетов от точки потери должен быть повторно передан.

TCP Контроль потока



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 9

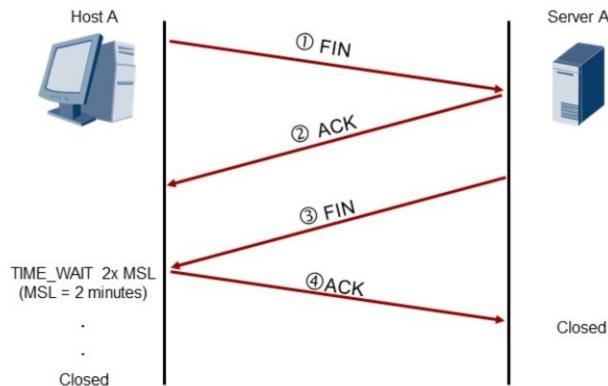


Поле окна TCP предоставляет средство управления потоком, которое определяет объем данных, отправленных отправителем. Это достигается путем возврата «окна» с каждым сегментом TCP, для которого установлено поле ACK, что указывает диапазон допустимых порядковых номеров за последний успешно полученный сегмент. В окне указывается допустимое количество октетов, которое отправитель может передать до получения разрешения.

В этом примере передача TCP от хоста А к серверу А содержит текущий размер окна для узла А. Размер окна для сервера А определяется как часть рукопожатия, которое на основе передачи можно принять за 2048. Как только данные эквивалентны размеру окна был получен, подтверждение будет возвращено относительно количества полученных байтов плюс один. После этого хост А продолжит передачу следующей партии данных.

Размер окна TCP, равный 0, фактически запрещает обработку сегментов, за исключением сегментов, где для входящих сегментов заданы биты кода ACK, RST и URG. Если существует размер окна 0, отправитель должен периодически проверять статус размера окна при приеме TCP, чтобы гарантировать, что любое изменение размера окна эффективно сообщается, период повторной передачи обычно составляет две минуты. Когда отправитель отправляет периодические сегменты, принимающий TCP должен все же подтвердить с объявлением номера последовательности текущего размера окна 0.

TCP прекращение соединения



- Host A обеспечит получение ACK сервером А перед закрытием.

В рамках процесса завершения TCP-соединения определен ряд состояний, через которые будет осуществляться переход TCP. Эти состояния включают FIN-WAIT-1, который представляет ожидающий запрос завершения соединения (FIN) от удаленного TCP или подтверждение запроса о завершении соединения, который был ранее отправлен. FIN-WAIT-2 представляет ожидающий запрос завершения соединения от удаленного TCP, после которого обычно переходит в состояние TIME-WAIT. Состояние CLOSE-WAIT указывает на ожидание локально определенного запроса завершения соединения, как правило, когда приложение сервера находится в процессе закрытия.

Состояние LAST-ACK представляет собой ожидание подтверждения запроса завершения соединения, ранее отправленного на удаленный TCP (который включает подтверждение его запроса завершения соединения). Наконец, появляется состояние TIME-WAIT и ожидает достаточно времени для прохождения, чтобы гарантировать, что удаленный TCP получил подтверждение его запроса завершения соединения. Этот период управляется таймером (MSL), который определяет период ожидания 2 минуты. После периода ожидания, равного двум MSL, TCP-соединение считается закрытым / завершенным.

Протокол дейтаграмм пользователя



- Данные на основе UDP отправляются без установления соединения.

UDP представляет собой альтернативу TCP и применяется там, где TCP, как установлено, действует как неэффективный механизм передачи, прежде всего в случае высокочувствительного трафика с высокой задержкой. В тех случаях, когда TCP считается сегментом, UDP распознается как форма PDU, для которых дейтаграмма может быть понята как автономная независимая сущность данных, несущих достаточную информацию для маршрутизации из источника в конечную систему, не полагаясь на более ранние обмены между этим источником и конечными системами назначения и сетью передачи, как определено в RFC 1594. Фактически это означает, что UDP-трафик не требует установления соединения до отправки данных.

Упрощенная структура и работа UDP делает его идеальным для приложений-программ для отправки сообщений другим программам с минимальным протокольным механизмом, например, в случае подтверждений и оконной обработки, как показано в сегментах TCP. Однако UDP не гарантирует доставку данных, а также защиту от дублирования данных.

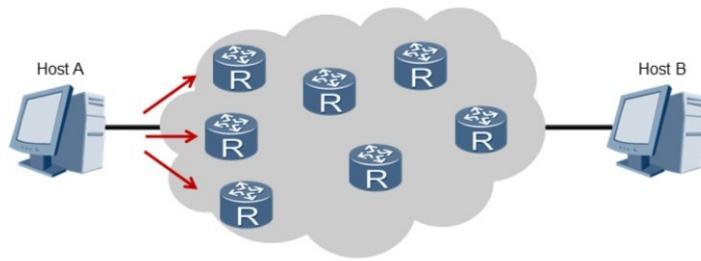
Формат дейтаграмм UDP



- UDP обеспечивает минимальные накладные расходы для каждой датаграммы.
- Доставка дейтаграмм не гарантируется с UDP.

Заголовок UDP обеспечивает минималистический подход к уровню передачи, реализуя только базовую конструкцию, которая помогает идентифицировать порт назначения, которому предназначен трафик на основе UDP, а также поле длины и значение контрольной суммы, которое обеспечивает целостность заголовка UDP. Кроме того, минимальные накладные расходы выступают в качестве идеального средства для предоставления большего количества данных для каждого пакета, что благоприятствует трафику в реальном времени, таком как голосовая и видеосвязь, где TCP обеспечивает 20-байтовые служебные данные и механизмы, которые влияют на задержки, например, в случае подтверждений , однако отсутствие таких полей означает, что доставка дейтаграмм не гарантируется.

UDP процесс пересылки

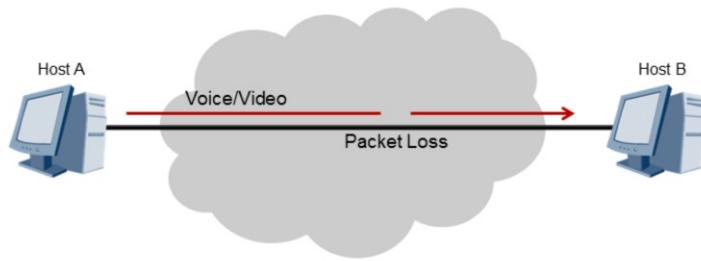


- UDP восприимчив к возможности дублирования дейтаграммы или нестандартной доставке дейтаграмм.

Поскольку передача дейтаграмм UDP не отправляется как поток данных, передача данных подвержена дублированию дейтаграмм. Кроме того, отсутствие порядковых номеров в UDP означает, что доставка передачи данных по различным путям, скорее всего, будет приниматься в пункте назначения в некорректном, не упорядоченном порядке.

Если данные потока передаются по UDP, например, в случае голосовых и видеоприложений, для повышения возможности UDP могут применяться дополнительные протокольные механизмы, как в случае транспортного протокола реального времени (RTP), который помогает поддерживать неспособность UDP, предоставляя механизм секвенирования с использованием временных меток для поддержания порядка таких потоков аудио / видео данных, эффективно поддерживая поведение, ориентированное на частичное соединение, по транспортному протоколу без установления соединения.

UDP процесс пересылки



- Нет подтверждений, поэтому потерянные пакеты не ретранслируются, однако это выгодно для задержки чувствительных данных.

Общее поведение переадресации UDP очень полезно для задержки чувствительного трафика, такого как голос и видео. Следует понимать, что в случае транспортного протокола, ориентированного на соединение, потерянные данные потребуют репликации после периода задержки, в течение которого ожидается подтверждение отправителем. Если подтверждение не получено, данные должны быть повторно переданы. Для чувствительных к задержкам потоков данных это приведет к непонятным аудио- и видеопередачам из-за задержки и дублирования в результате повторной передачи с точки, где генерируются подтверждения. В таких случаях минимальная потеря потока данных предпочтительнее, чем повторная передача, и как таковой UDP выбирается в качестве транспортного механизма для поддержки чувствительного к задержке трафика.



Итог

- Какова цель поля подтверждения в заголовке TCP?
- Какие биты кода TCP участвуют в трехстороннем рукопожатии TCP?

1. Поле подтверждения в заголовке TCP подтверждает получение сегмента, полученного процессом TCP в пункте назначения. Номер последовательности в заголовке TCP принятой IP-дейтаграммы принимается и увеличивается на 1. Это значение становится номером подтверждения в возвращенном заголовке TCP и используется для подтверждения получения всех данных перед пересылкой вместе с установленным битом кода ACK до 1, исходному отправителю.
2. Трехстороннее рукопожатие включает в себя SYN и ACK кодовые биты, чтобы установить и подтвердить соединение между двумя конечными системами, между которыми должна произойти передача дейтаграмм.



Thank you

www.huawei.com

Сценарий пересылки данных

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

Набор протоколов TCP/IP работает как набор правил для того, чтобы поддерживать сквозную пересылку данных вместе с протоколами нижнего уровня, такие как те, которые определены в стандартах IEEE 802. Знание жизненного цикла пересылки данных позволяет глубже понять поведение сети IP для эффективного анализа сети, эксплуатации и устранения неполадок в сети. Поэтому процесс инкапсуляции и декапсуляции представляет собой фундаментальную часть всех знаний TCP/IP.

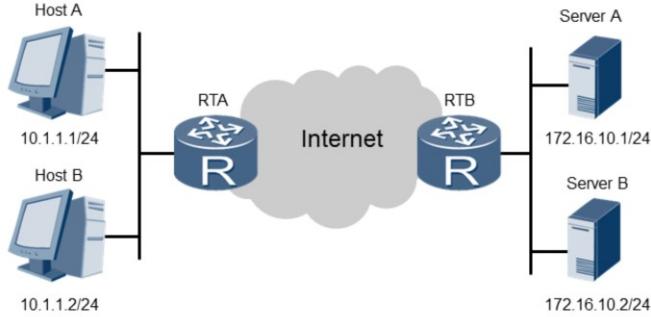


Цели

По завершении этого раздела слушатели смогут:

- Объяснить шаги процесса инкапсуляции и декапсуляции данных.
- Устранять основные проблемы пересылки данных.

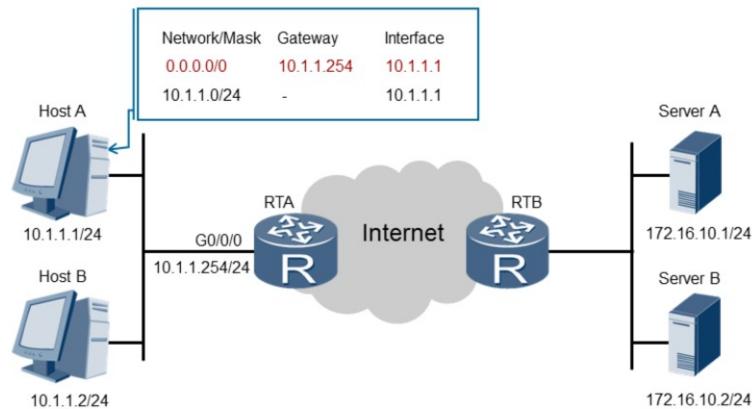
Сценарий пересылки



- Пересылка данных может быть локальной или удаленной, однако в общем процесс пересылки схожий.

Пересылка данных может быть определена как локальная или удаленная, для которых процесс пересылки опирается на приложение стека протоколов для достижения сквозной передачи. Конечные системы могут быть частью одной и той же сети или расположены в разных сетях, однако общий принцип пересылки для обеспечения передачи между хостами следует четкому набору протоколов, которые были введены как часть устройства. Взаимодействие данных протоколов должно быть усилено, а также установлена связь между протоколами TCP/IP верхнего уровня и стандартами протокола Ethernet на основе нижнего канала.

Поиск пути



Хост А должен знать путь к месту назначения.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

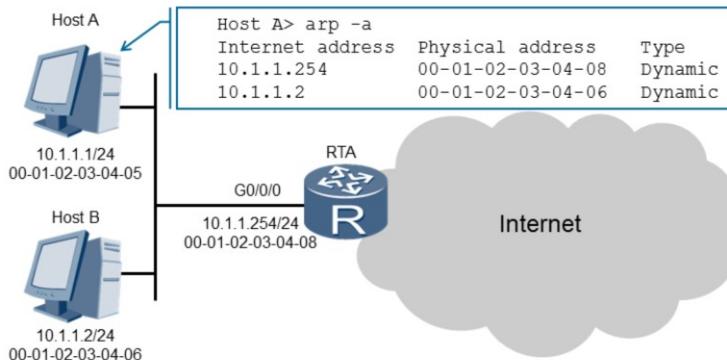
Page 5



Конечная система, которая намеревается перенаправить данные в данный пункт назначения, должна сначала определить, возможно ли достичь целевого адресата. Чтобы достичь этого, конечная система должна пройти процесс обнаружения пути. Следует понимать, что конечная система способна поддерживать работу на всех уровнях, поскольку ее основная функция - быть хостом для приложений. В связи с этим он также должен быть способен поддерживать операции нижнего уровня, такие как перенаправление (переключение) маршрутизации и канального уровня, чтобы иметь возможность пересыпать данные верхнего / прикладного уровня. Поэтому конечная система содержит таблицу, которая обеспечивает доступность сетевого уровня к сети, для которой предназначены данные верхнего уровня.

Конечные системы обычно будут знать о сети, в которой они находятся, но могут быть без пути пересылки в случаях, когда удаленное обнаружение сети не было достигнуто. В приведенном примере хост А имеет путь к выделенной сети через адрес «любой сети», который был кратко введен как часть раздела IP-адресации. В таблице пересылки указывается, что трафик должен быть перенаправлен на шлюз в качестве следующего перехода через интерфейс, связанный с логическим адресом 10.1.1.1.

Протокол преобразования адресов - ARP



- Таблица кэша ARP используется для обнаружения следующего канала передачи данных.
- Неизвестный следующий канал передачи данных будет генерировать ARP-запрос.

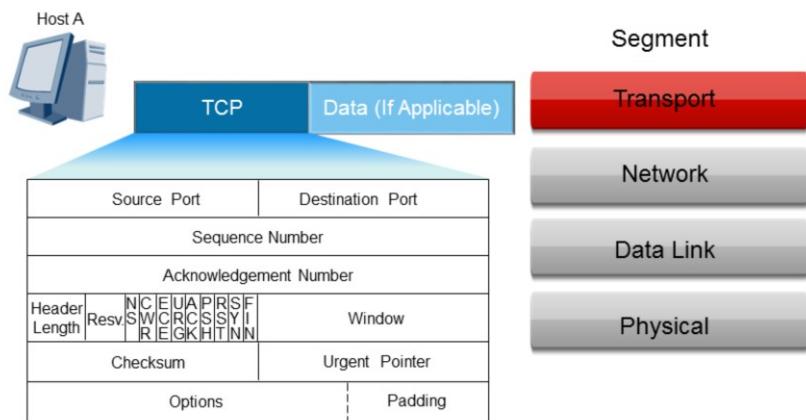
Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 6



После обнаружения возможного маршрута в направлении предполагаемой целевой сети необходимо также обнаружить физический следующий канал для упрощения переадресации кадров. Набор протоколов TCP / IP отвечает за определение этого, прежде чем пакетная инкапсуляция сможет продолжаться. Начальный этап включает в себя определение того, существует ли физический путь к следующему ходу, идентифицированному как часть процесса обнаружения пути. Для этого требуется, чтобы таблица ARP-кэша использовалась с целью выяснить, известна ли связь между предполагаемым следующим каналом и физическим путем. Из примера видно, что запись в адресе шлюза следующего перехода присутствует в таблице кэша ARP. Если запись не может быть найдена, необходимо инициировать протокол ARP для выполнения обнаружения и разрешения физического пути.

TCP инкапсуляция



- Инкапсуляция выполняется после подтверждения пути.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 7

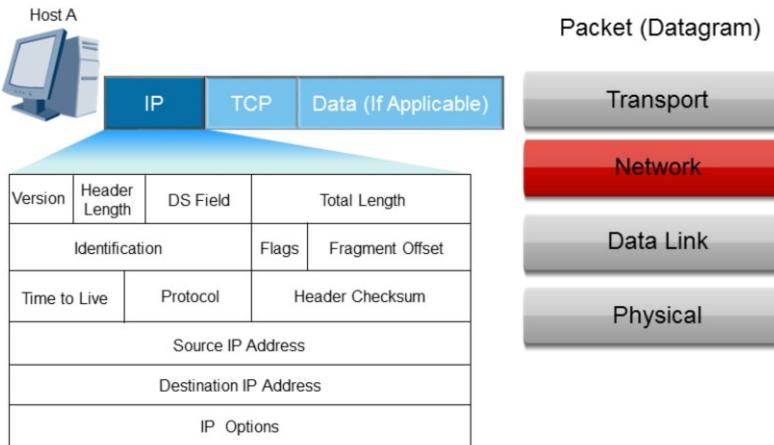


Когда логическое и физическое обнаружение пересылки маршрута завершено, возможно инкапсулирование данных для успешной передачи по сетям на основе IP / Ethernet. Процессы верхнего уровня с точки зрения шифрования и сжатия могут выполняться после того, как произойдет инкапсуляция транспортного уровня, идентифицируя исходный и конечный порты, через которые данные верхнего уровня должны быть перенаправлены.

В случае TCP будут заполнены поля последовательности и подтверждения, кодовые биты будут установлены, если необходимо, с ACK-битом, который обычно применяется. Поле окна будет заполнено текущим поддерживаемым размером окна, на который хост будет уведомлять о максимальном буфере данных, который может поддерживаться до подтверждения данных.

Значения, представляющие поля TCP, включаются как часть контрольной суммы, которая рассчитывается с использованием процесса вычисления комплемента, чтобы обеспечить целостность сегмента TCP после того, как заголовок TCP получен и обработан в конечном месте назначения. В случае базовых операций TCP-кода данные верхнего уровня не всегда могут переноситься в сегменте, как в случае синхронизации соединения, и подтверждения полученным данным.

IP инкапсуляция



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

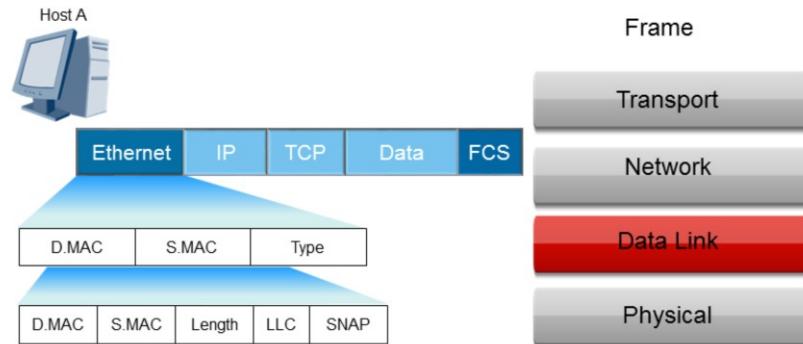
Page 8



После инкапсуляции уровня передачи обычно требуется предоставление инструкций, в которых подробно описывается, как должна осуществляться передача по одной или нескольким сетям. Это включает в себя перечисление источника IP, а также конечный пункт назначения, для которого предназначен пакет. IP-пакеты обычно ограничены размером 1500 байтов Ethernet, включая заголовки сетевого и транспортного уровней, а также любые данные верхнего уровня. Первоначальный размер пакета будет определяться Ethernet как максимальным модулем передачи или MTU, которому будут соответствовать пакеты, поэтому фрагментация не будет происходить в источнике.

В случае, когда MTU изменяется вдоль пути пересылки, только тогда будет выполняться фрагментация. Поле Time to Live будет заполнено заданным значением в зависимости от системы, в маршрутизаторах серии ARG3, это устанавливается с начальным значением 255. Поле протокола заполняется на основе протокола, заключенного в IP. В этом случае рассматриваемый протокол представляет собой TCP, для которого заголовок IP заполняет поле протокола значением 0x06 в качестве инструкции для следующей обработки заголовка. Исходная и целевая IP-адресация будет отражать исходный источник и конечный пункт назначения.

Обработка Ethernet



Тип кадра зависит от инкапсулированных протоколов.
IP - это протокол верхнего уровня, поэтому используется Ethernet II frame.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

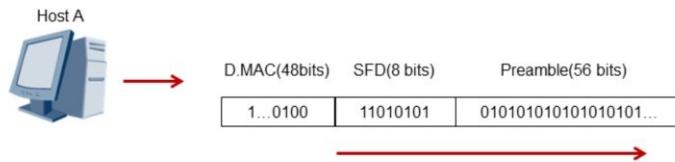
Page 9



Инкапсуляция уровня канала основана на стандартах Ethernet IEEE 802.3 для физической передачи данных верхнего уровня по сетям Ethernet. Инкапсуляция на нижних уровнях выполняется путем первоначального определения используемого типа кадра.

Если протокол верхнего уровня представлен значением типа больше 1536 (0x0600), как в случае с IP (0x0800), используется тип кадра Ethernet II. Поле типа заголовка кадра Ethernet II заполняется значением типа 0x0800, чтобы отразить, что следующий протокол, который будет обрабатываться после обработки кадра, будет IP. MAC-адрес назначения определяет следующую физическую пересылку, которую в этом случае представляет сетевой шлюз.

Передача фреймов



- Уровень канала передачи данных использует смысл несущей для обнаружения существующего трафика.
- Вводная часть и SFD, используются для синхронизации с пересылаемым кадром.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

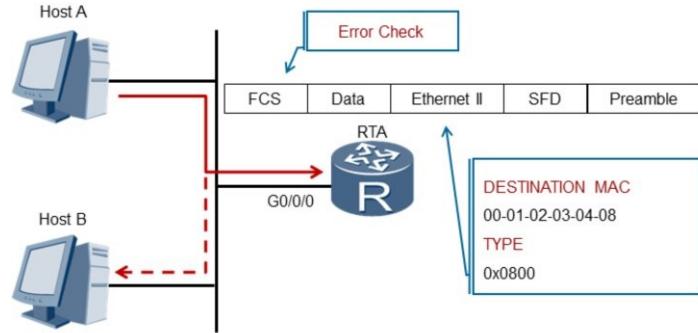
Page 10



В рамках операции канала связи необходимо обеспечить, чтобы среда передачи была очищена от сигналов в области общего коллизионного взаимодействия. Хост сначала будет прослушивать любой трафик в сети как часть CSMA / CD, и если линия останется ясной, будет подготовлена передача данных. Необходимо, чтобы получающий физический интерфейс был информирован о входящем кадре, чтобы избежать потери начальных значений битов, которые сделали бы исходные кадры незавершенными. Таким образом, фреймам предшествует 64-битное значение, указывающее на назначение целевого уровня канала для приближающегося прибытия кадра.

Исходные 56 бит представляют собой чередующийся шаблон 1, 0, который называется преамбулой, и за ним сразу следует октет, который понимается как начало разделителя кадров (SFD). Последние два бита SFD отклоняются от чередующегося шаблона до 1,1-битовой комбинации, которая уведомляет, что последующие биты представляют собой первые битовые значения MAC-адреса назначения и, следовательно, начало заголовка кадра.

Обработка фреймов



- Кадр будет приниматься всеми в том же коллизионном домене.
- Только шлюз RTA будет обрабатывать кадр.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 11

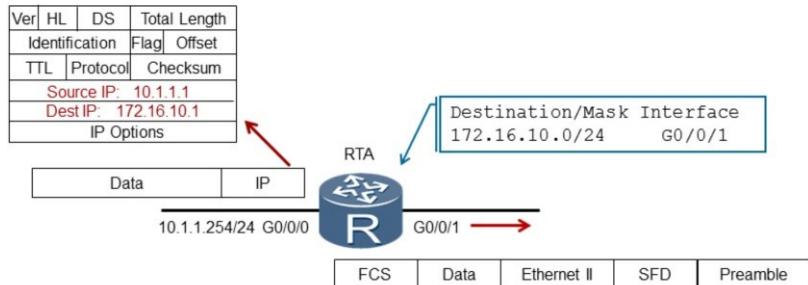


Поскольку кадр принимается уровнем передачи канала связи, он должен пройти через несколько проверок, чтобы определить его целостность, а также действительность. Если кадр передавался по общей сети Ethernet, другие конечные станции могут также получать экземпляр переданного кадра, однако, поскольку MAC-адрес назначения кадра отличается от MAC-адреса конечной станции, кадр будет отброшен.

Кадры, полученные в месте назначения, будут выполнять проверку ошибок, вычисляя значение одного комплемента на основе текущих полей кадра и сравнивая их со значением в поле FCS. Если значения не совпадают, кадр будет отброшен. Для получения промежуточных и конечных систем, которые принимают действительные кадры, необходимо определить, предназначен ли кадр для их физического интерфейса, путем сравнения MAC-адреса назначения с MAC-адресом интерфейса (или устройства в некоторых случаях).

Если есть совпадение, кадр обрабатывается и поле типа используется для определения следующего заголовка, подлежащего обработке. После определения следующего заголовка заголовок кадра и трейлер будут отброшены.

Обработка пакетов



- IP-адрес назначения проверяется с адресом шлюза.
- Новый заголовок кадра создается после процесса обнаружения.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 12

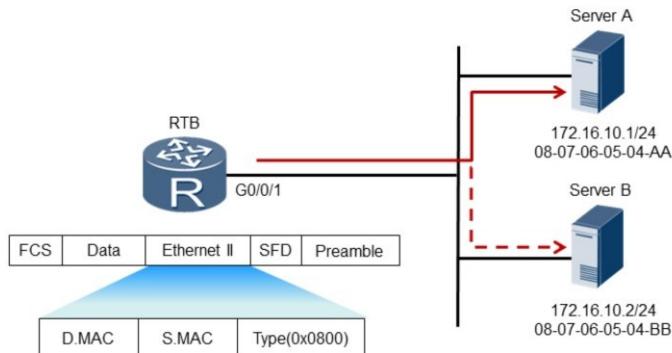


Пакет принимается сетевым уровнем и, в частности, IP, после чего обрабатывается IP-заголовок. Значение контрольной суммы существует на каждом уровне стека протоколов, чтобы поддерживать целостность на всех уровнях для всех протоколов. IP-адрес назначения используется для определения того, достиг ли пакет конечной цели. Однако шлюз определяет, что это не так, поскольку IP-адрес назначения и IP-адрес шлюза не совпадают.

Поэтому шлюз должен определить ход действий, который необходимо предпринять в отношении маршрутизации пакета к альтернативному интерфейсу, и перенаправить пакет в сеть, для которой он предназначен. Во-первых, шлюз должен гарантировать, что значение TTL не достигло 0, а размер пакета не превышает максимальное значение единицы передачи для шлюза. В случае, если пакет больше, чем значение MTU шлюза, обычно начинается фрагментация.

После назначения адресата пакета в таблице переадресации шлюза пакет будет инкапсулирован в новый заголовок кадра, состоящий из новых MAC-адресов источника и назначения для сегмента канала связи, по которому должен быть перенаправлен результирующий фрейм, перед снова передается на следующий физический скачок. Если следующий физический скачок неизвестен, ARP снова будет использоваться для разрешения MAC-адреса.

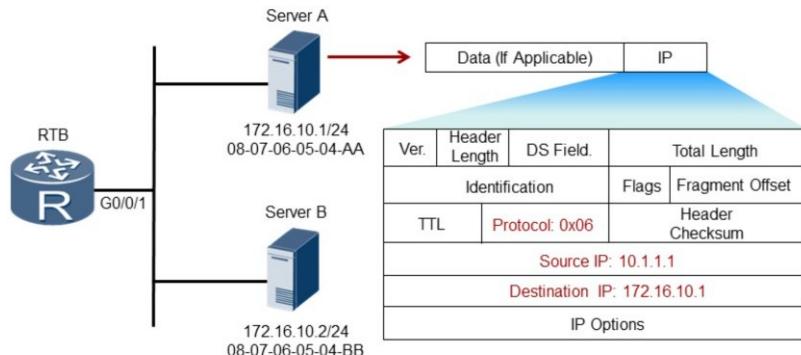
Декапсуляция фреймов



- Кадр перенаправляется с MAC-адресом назначения сервера А.
- Сервер А сравнивает MAC-адрес с MAC-адресом назначения кадра.

Кадры, полученные в конечном пункте назначения, будут первоначально определять, достиг ли кадр предполагаемого места. В этом примере показаны два сервера в общей сети Ethernet, в которых оба получаются копии кадра. Кадр, в конечном счете, отбрасывается сервером В, поскольку значение MAC-адреса назначения и MAC-адрес интерфейса сервера В не совпадают. Сервер А, однако, успешно получает кадр и узнает, что поля MAC одинаковы, целостность кадра на основе FCS также может быть понята как правильная. Кадр будет использовать поле типа, чтобы идентифицировать 0x0800 в качестве следующего заголовка, после чего заголовок кадра и трейлер будут отброшены и пакет будет принят по IP.

Декапсуляция пакетов



- Сервер А сравнивает собственный IP-адрес с адресом назначения IP-заголовка.
- IP-заголовок обрабатывается и отбрасывается, данные направляются в TCP.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 14

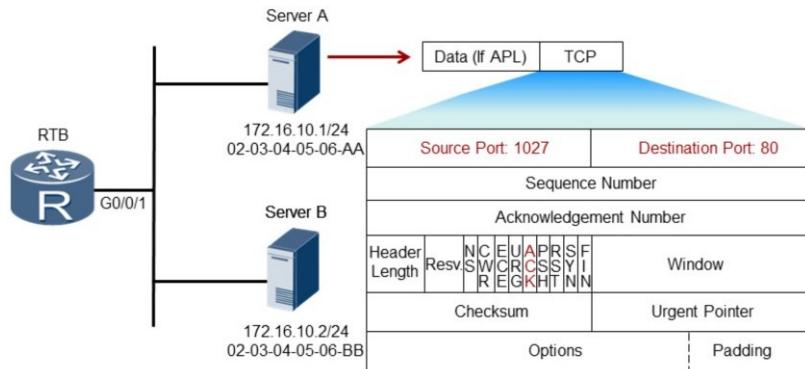


По достижении конечного адресата заголовок IP-пакета должен облегчать ряд процессов. Первый включает проверку целостности заголовка пакета через поле контрольной суммы, снова применяя сравнение значений сравнения, основанное на сумме полей заголовка IP. Если это правильно, заголовок IP будет использоваться для определения того, соответствует ли IP-адрес назначения IP-адресу текущей конечной станции, которая в этом случае является истиной.

Если во время передачи между источником и получателем произошла какая-либо фрагментация, пакет должен быть повторно собран в этот момент. Поле идентификации будет собирать фрагменты, принадлежащие одному источнику данных, вместе, смещение будет определять порядок, а поле flags укажет, когда должна начинаться сборка, так как все фрагменты должны быть получены сначала, а фрагмент с флагом 0 будет равен признанный в качестве последнего фрагмента, который должен быть получен.

Затем будет выполняться таймер, в течение которого сборка должна быть завершена, если повторная сборка не будет выполнена в течение этого периода времени, все фрагменты будут отброшены. Поле протокола будет использоваться для идентификации следующего заголовка для обработки, и заголовок пакета будет отброшен. Следует отметить, что следующий заголовок не всегда может быть заголовком транспортного уровня, ярким примером того, где это можно понять, является ICMP, который, как считается, также является протоколом сетевого уровня с значением поля протокола 0x01.

Декапсуляция сегментов



- TCP-заголовок создает соединение с сервисом на порту 80.
- Параметры в заголовке TCP используются для управления соединением.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 15



В случае, когда заголовок пакета отбрасывается, результирующий сегмент или дейтаграмма передается на транспортный уровень для обработки на основе приложения на приложение. Информация заголовка принимается в этом случае по протоколу TCP (0x06).

В этом примере можно понять, что TCP-соединение уже установлено, и сегмент представляет собой подтверждение для передачи HTTP-трафика с HTTP-сервера на подтверждающий хост. Хост представлен портом 1027 в качестве средства для различия нескольких HTTP-соединений, которые могут существовать между тем же исходным хостом и целевым сервером. При получении этого подтверждения HTTP-сервер будет продолжать пересыпать хосту в пределах границ размера окна хоста.



Итог

- Какая информация требуется, прежде чем данные могут быть инкапсулированы?
- Что происходит, когда кадр отправляется в пункт назначения, которому он не предназначен?
- Как данные в кадре в конечном итоге достигают приложения, для которого они предназначены?
- Когда несколько сеансов одного и того же приложения активны (например, несколько веб-браузеров), как возвращенные данные достигают правильной сессии?

1. До инкапсуляции и пересылки данных источник должен иметь информацию о назначении IP или эквивалентном адресе пересылки, таком как адрес по умолчанию, по которому могут быть отправлены данные. Кроме того, необходимо, чтобы адрес пересылки был связан с физическим следующим переходом, которому данные могут быть перенаправлены в локальной сети.
2. Любой кадр, который принимается шлюзом или конечной системой (хостом), к которой он не предназначен, впоследствии удаляется после проверки MAC-адреса назначения в заголовке кадра.
3. Доставка данных зависит от номера порта назначения в заголовках TCP и UDP для определения приложения, для которого предназначены данные. После анализа этого значения по протоколу TCP или UDP данные пересылаются.
4. Исходный порт заголовка TCP для HTTP-трафика различает различные активные сеансы приложений. Возврат HTTP-трафика с HTTP-сервера позволяет идентифицировать каждый отдельный сеанс веб-браузера на основе этого номера порта источника. Например, исходный порт двух отдельных запросов для HTTP-трафика, исходящих из источника IP 10.1.1.1 может исходить из исходных портов 1028 и 1035, однако порт назначения в обоих случаях остается в качестве порта 80, HTTP-сервера.



Thank you

www.huawei.com

Основы VRP

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

Поскольку все больше и больше конечных устройств выполнены в виде хост-устройств, сетевых принтеров и других подобных продуктов внедренных в локальную сеть, увеличение количества устройств приводит к ограничению интерфейсных портов, а также проблемы коллизий в любой общей топологии сети. Коммутаторы стали средством поддержки этого роста. VRP используется в продуктах Huawei в качестве средства настройки и управления такими устройствами, для которых должны быть разработаны знания и практические навыки.

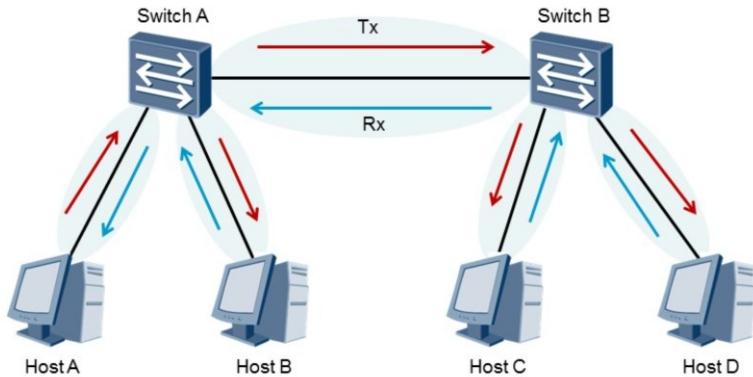


Цели

После завершения этой главы вы сможете:

- Объяснить роль коммутаторов в Ethernet сетях
- Объяснить разницу, между коллизиями и широковещательными доменами
- Объяснить главное применение VRP в Huawei продуктах

Применение коммутирующих устройств



- Коммутатор создает множество доменов коллизий

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 4

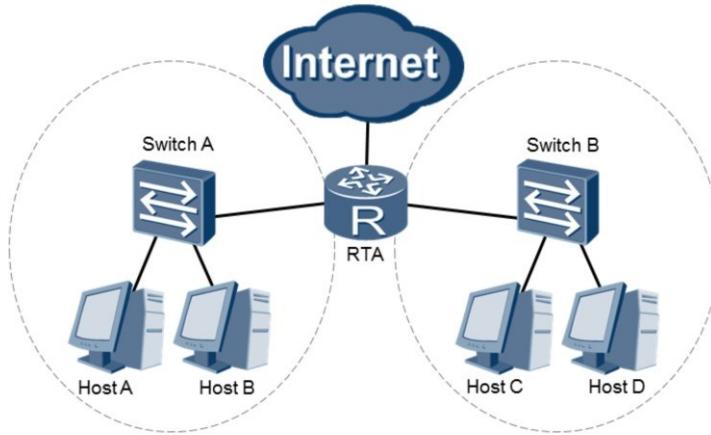


До сих пор сеть Ethernet понималась как обменивающихся общими медиаданными совокупность устройств, такими как 10Base2, через которые хосты могут взаимодействовать с соседними узлами или конечными системами. Было установлено, что сеть Ethernet является противоречивой сетью, а это означает, что хосты должны конкурировать за доступ к медиа, которое становится все более ограниченным, как все больше и больше устройств, подключенных по этой общей информации; что вызывает дополнительные ограничения в масштабируемости и возрастающий потенциал для коллизий.

В результате потребность в обнаружении столкновений в виде CSMA/CD всегда присутствует в таких общих сетях Ethernet. После внедрения коммутируемых носителей, таких как 100BaseT, передача и прием данных были изолированы внутри каналов (пары проводов), что позволило исключить возможность коллизий. Этот носитель как форма несетевого Ethernet обеспечивает только средство для двухточечной связи, однако оно используется вместе с другими устройствами, такими как HUB'ы, что позволяет совместно использовать сеть Ethernet, но и возможность коллизий.

Коммутатор был введен как часть эволюции моста и способен разрушить общий домен коллизии в несколько доменов коллизий. Домены коллизий работают как набор двухточечных соединений, для которых устранена угроза столкновения, и трафик канала связи изолирован, чтобы обеспечить более высокую скорость передачи, оптимизирующую поток трафика в сети Ethernet.

Применение устройств маршрутизации

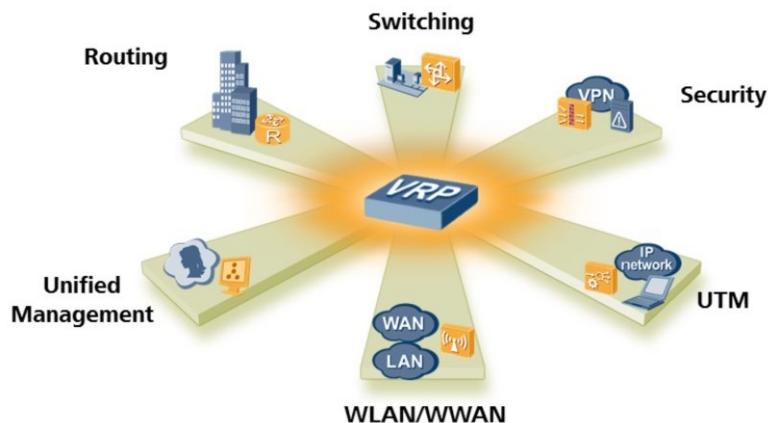


Шлюзовые устройства, такие как маршрутизаторы, создают широковещательные домены

Широковещательной домен может состоять из одного или нескольких доменов коллизии, и любая широковещательная передача содержится в пределах границы широковещательного домена. Край границы домена широковещательной передачи обычно определяется шлюзом, который действует как среда, через которую достигаются другие сети, и ограничивает пересылку любого широковещательного трафика за пределы интерфейса, на котором принимается широковещательная передача.

Маршрутизаторы являются синонимом термина «шлюз», для которого эти два часто используются взаимозаменяющими. Как правило, одной IP-сетью может быть образован широковещательный домен, который относится к сфере действия сегмента канального уровня. Маршрутизаторы, как правило, отвечают за маршрутизацию Интернет-дейтаграмм (IP-пакетов) на конкретный пункт назначения на основе знания адреса пересылки для сети назначения, найденного внутри таблицы пересылки, управляемой внутренним образом.

Введение в VRP



- VRP это платформа, на которой оперируют множество продуктов Huawei

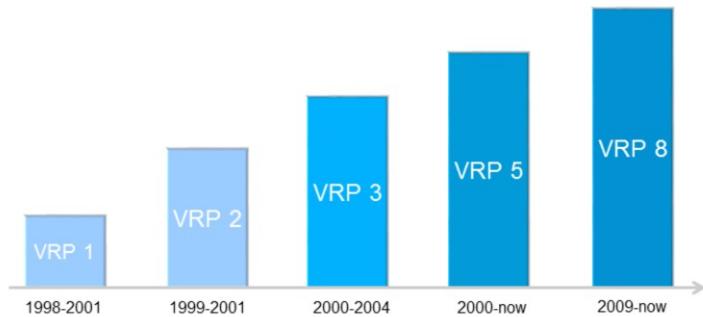
Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 6



Универсальная платформа маршрутизации (VRP) представляет собой основу многих продуктов Huawei, включая маршрутизаторы и коммутаторы. Его технологии прошли через многие этапы эволюции, чтобы обеспечить постоянное совершенствование управления данными и их переадресации. Архитектурные технологии привели к еще большей модульности, которая позволяет повысить общую производительность. Конфигурация, управление и мониторинг устройств, использующих VRP, основаны на стандартизированной и иерархической системе командной строки, для которой разработана документация для поддержки навигации и работы продуктов Huawei, управляемых с помощью программного обеспечения VRP.

VRP временная линия



- VRP версии 5 и 8 сейчас используются в продукции Huawei

Знание версий сетевой операционной системы VRP помогает гарантировать, что используемая версия является актуальной и поддерживает некоторые функции, которые могут потребоваться в корпоративной сети. Большинство устройств Huawei работают с VRP версии 5.x, где x может варьироваться в зависимости от продукта и выпуска VRP. Версия VRP 8 - это недавняя версия VRP, построенная с использованием усовершенствованной архитектуры для следующего поколения технологий и построенная вокруг необходимости повышения эффективности, но не присутствует во всех продуктах Huawei.

Установка соединения

AR2200



S5700



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 8

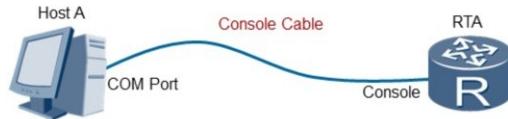


AR-маршрутизаторы (AR) включают в себя: AR150, AR200, AR1200, AR2200 и AR3200. Они являются продуктами следующего поколения Huawei и обеспечивают функции маршрутизации, коммутации, беспроводной связи, голоса и безопасности. Серия AR позиционирует себя между корпоративной сетью и общедоступной сетью, функционируя как входной и выходной шлюз для передачи данных между двумя сетями. Разворачивание различных сетевых сервисов по маршрутизаторам серии AR снижает затраты на эксплуатацию и обслуживание, а также затраты, связанные с созданием корпоративной сети. Маршрутизаторы серии AR различных спецификаций могут использоваться в качестве шлюзов на основе пользовательской емкости предприятия.

Коммутатор Ethernet Sx7 обеспечивает функции передачи данных и был разработан Huawei для удовлетворения требований к надежному доступу и высококачественной передаче нескольких услуг в корпоративной сети. Эта серия коммутаторов позиционируется для работы уровня доступа в корпоративной сети и обеспечивает большую коммутационную способность, высокую плотность портов и экономичные возможности пересылки пакетов.

Управление маршрутизаторами серии ARG3 и коммутатором серии Sx7 может быть достигнуто путем установления соединения с консольным интерфейсом, а в случае с AR2200 соединение также возможно установить через интерфейс Mini USB.

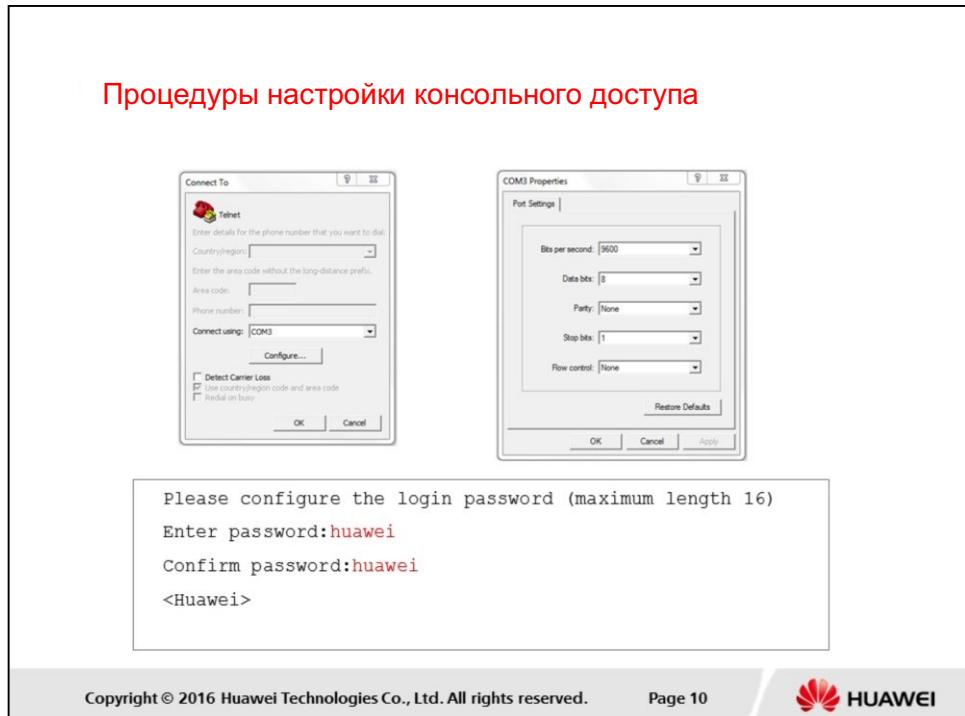
Доступ к устройству через консоль



- Физическое соединение устанавливается между серийным (COM) портом, и консольным интерфейсом маршрутизатора/коммутатора.

Консольный кабель используется для отладки или поддержки локально установленного устройства, такого как маршрутизатор или коммутатор, и будет взаимодействовать с консольным портом таких устройств. Консольный интерфейс коммутатора серии S5700 и маршрутизатора AR2200 - это соединение типа RJ-45, а интерфейс, к которому выполняется соединение хоста, представляет собой последовательный разъем RS-232. Часто такие последовательные разъемы больше не присутствуют на более новых устройствах, которые могут использоваться для установления соединения, например портативных компьютеров, и, следовательно, выполняется преобразование RS-232 в USB. Однако для большинства настольных устройств на COM-порт хост-устройства можно установить консольное соединение на основе RS-232.

Процедуры настройки консольного доступа



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

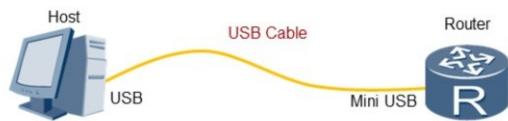
Page 10



Консоль настраивается через один из нескольких доступных программ эмуляции терминала. Пользователи Windows часто применяют приложение HyperTerminal, как показано в примере, для взаимодействия с операционной системой VRP. Следуя спецификации СОМ-порта, который должен использоваться для установления соединения, должны быть определены настройки порта.

В этом примере определяются параметры порта, которые должны быть применены по умолчанию. После нажатия кнопки OK будет установлен сеанс с VRP устройством. Если устройство работает с заводскими настройками по умолчанию, пользователю будет предложено ввести пароль, который будет назначен в качестве пароля по умолчанию для будущих попыток подключения.

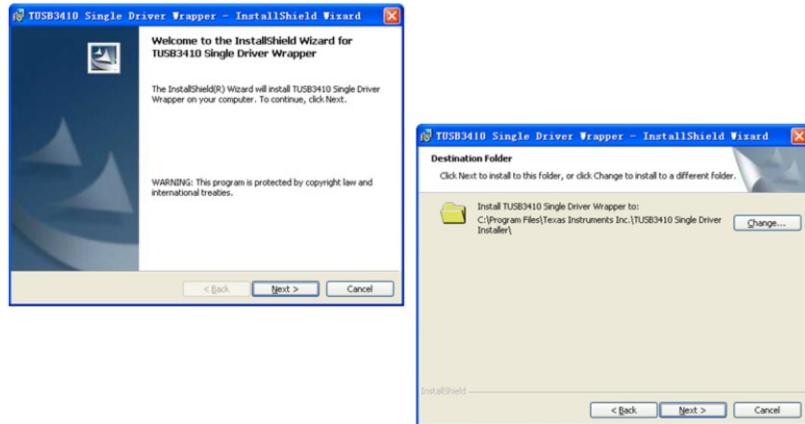
Доступ к маршрутизатору через Mini USB



- Устанавливается соединение между USB портом хоста и mini USB интерфейсом маршрутизатора.

Маршрутизатор Huawei AR2200 также поддерживает средства для подключения терминала через USB-соединение. Интерфейс мини-USB типа B существует на передней панели маршрутизатора серии AR2200, через который хости могут устанавливать соединение на основе USB в качестве альтернативы для RS-232.

Установка Mini USB драйвера



- Установка драйверов USB соединения является обязательным.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 12

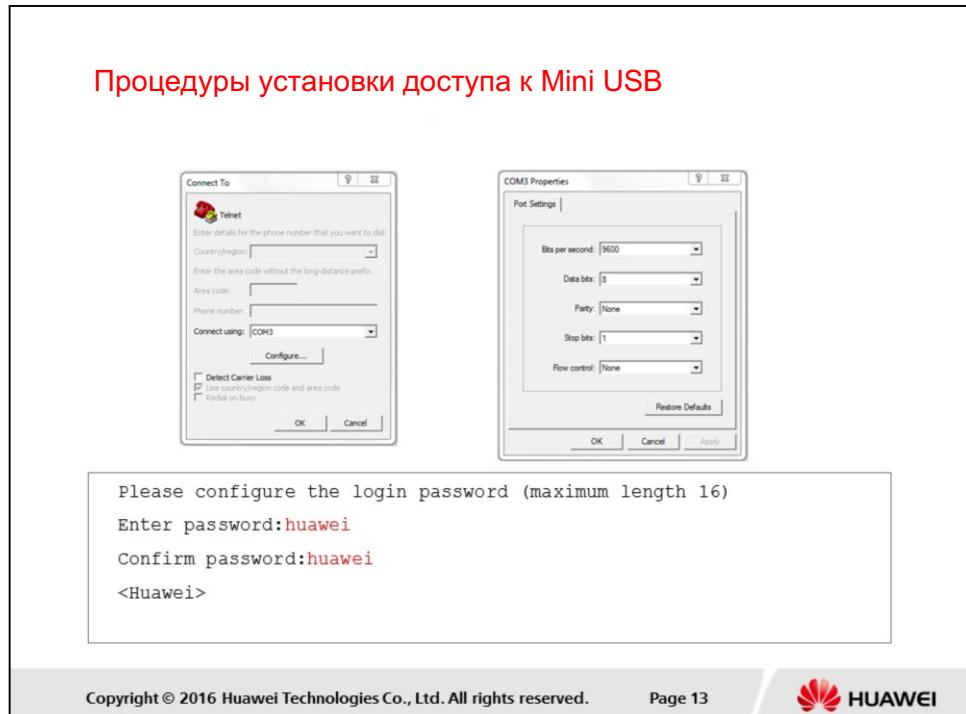


В процессе установки требуется сначала установить драйверы mini USB, чтобы обеспечить функциональность USB. Mini USB драйвер можно получить, посетив <http://support.huawei.com/enterprise> и по пути Support > Software > Enterprise Networking > Router > Access Router > AR > AR2200, выбрать соответствующую версию VRP и путь загрузки, и загрузить файл с названием AR & SRG_MiniUSB_driver.zip. Следует отметить, что драйвер mini USB поддерживает только операционные системы Windows XP, Windows Vista и Windows 7.

При обновлении программного обеспечения устройства или установке патча можно проверить значение хеша MD5, чтобы подтвердить достоверность программного обеспечения. Чтобы предотвратить изменение или замену программного обеспечения, рекомендуется выполнить эту операцию. Для установки требуется, чтобы пользователь сначала дважды щелкнул на установочный файл драйвера на ПК и нажмите «Далее». Во-вторых, выберите «Я принимаю условия лицензионного соглашения» и нажмите «Далее». Нажмите кнопку «Изменить», чтобы при необходимости изменить каталог установки драйверов, и нажмите «Далее». Нажмите Установить и распаковать драйвер. Когда система завершит распаковку драйвера, нажмите «Готово».

Затем пользователи должны найти папку DISK1 в указанном каталоге драйверов и дважды щелкнуть файл setup.exe. После открытия второго окна установки нажмите «Далее». Пользователи должны снова выбрать Я принимаю условия лицензионного соглашения и нажмите «Далее», чтобы установить драйвер. После завершения нажмите Finish, чтобы завершить установку драйвера. Щелкните правой кнопкой мыши Мой компьютер и выберите «Управление» > «Диспетчер устройств» > «Порты» (COM & LPT). Система должна отобразить устройство TUSB3410 с указанием установленного драйвера.

Процедуры установки доступа к Mini USB



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 13



Как и в случае с консольным соединением RS-232, соединение Mini USB требует установки программного обеспечения эмуляции терминала для взаимодействия с командной строкой VRP.

Используйте программное обеспечение эмуляции терминала для входа в устройство через мини-порт USB (в качестве примера используется Windows HyperTerminal). На главном ПК запустите приложение HyperTerminal, и создайте соединение, предоставив подходящее имя подключения терминала и нажмите «OK». Выберите соответствующий порт (COM) и затем установите параметры связи для порта ПК. Эти параметры должны соответствовать значениям по умолчанию, которые устанавливаются при нажатии кнопки Восстановить значения по умолчанию.

После нажатия клавиши «Ввод» отображается информация о консоли, запрашивающая пароль для входа. Введите соответствующий пароль и его подтверждения, система сохранит пароль.



Итог

- Если происходит широковещательная передача Ethernet, например, в случае ARP, в которой пункт назначения является локальным, каков будет ответ шлюза?
- Какие версии VRP поддерживаются продукцией Huawei

1. Любая трансляция, которая генерируется конечной системой в локальной сети, будет перенаправлена всем адресатам. После того, как кадр передается маршрутизатору или устройству, действующему в качестве шлюза для сети, будет проанализирован кадр, и если будет определено, что назначение предназначено для локально определенного хоста, отличного от шлюза, кадр будет удален. Это определяет границу любого широковещательного домена.
2. VRP версия 5 поддерживается большинством текущих продуктов Huawei, а высокопроизводительные продукты часто могут поддерживать VRP версии 8.



Thank you

www.huawei.com

Навигация по CLI

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

Применение устройств Huawei в корпоративной сети требует уровень знаний и возможностей в навигации по VRP интерфейсу командной строки и конфигурации системных настроек. Поэтому в этой главе вводится принципиальная архитектура командной строки, раздел с навигацией, вспомогательными функциями и общей системой параметров, которые необходимо понимать для успешного конфигурирования любого управляемого устройства VRP.



Цели

После завершения этой главы вы сможете:

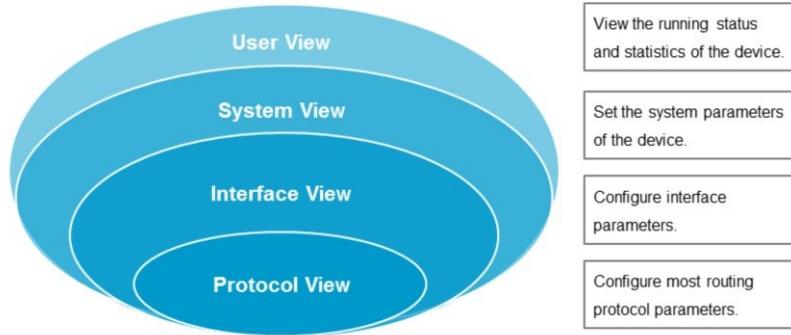
- Ориентироваться в VRP интерфейсе командной строки
- Конфигурировать базовые настройки VRP системы
- Выполнять базовую конфигурацию и управлению VRP интерфейса

Начальная настройка на устройстве

```
BIOS Creation Date : Jan 5 2013, 18:00:24
DDR DRAM init : OK
Start Memory Test ? ('t' or 'T' is test):skip
Copying Data : Done
Uncompressing : Done
-----
Press Ctrl+B to break auto startup ... 1
Now boot from flash:/AR2220E-V200R007C00SPC600.cc,
-----
<Huawei>
Warning: Auto-Config is working. Before configuring the device, stop
Auto-Config. If you perform configurations when Auto-Config is
running, the DHCP, routing, DNS, and VTY configurations will be lost.
Do you want to stop Auto-Config? [y/n]:Y
```

Процесс запуска/загрузки - это начальный этап работы для любого администратора или инженера, который использует продукты Huawei, работающие с VRP. Экран загрузки информирует о процедурах запуска системы, а также о версии VRP, которое в настоящее время реализовано на устройстве, вместе с местом хранения, откуда он загружен. После первоначальной процедуры запуска параметр автоматической настройки начальных системных параметров запрашивает ответ, для которого администратор может выбрать, следует ли следовать шагам конфигурации или вручную настроить основные системные параметры. Процесс автоматической настройки можно завершить, выбрав опцию "да" в заданном приглашении.

Виды командной строки CLI



```
<Huawei>system-view  
Enter system view, return user view with Ctrl+Z.  
[Huawei]interface GigabitEthernet 0/0/0  
[Huawei-GigabitEthernet0/0/0]
```

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 5



Иерархическая структура команд VRP определяет несколько видов команд, которые управляют командами, для которых пользователи могут выполнять операции. Интерфейс командной строки имеет несколько видов команд, из которых в этом примере представлены общие представления. Каждая команда зарегистрирована для запуска в одном или нескольких командных представлениях, и такие команды могут запускаться только после ввода соответствующего командного вида. Первоначальный командный вид VRP представляет собой User View, который работает для наблюдения за статусами параметров и общей статистической информацией. Для применения изменений в системных параметрах пользователи должны войти в System View. Также может быть найдено несколько уровней вспомогательных команд в виде представлений интерфейса и протокола, где могут выполняться задачи уровня подсистемы. Представления командной строки могут быть определены на основе скобок и информации, содержащейся в этих скобках. Присутствие <chevrons!> идентифицирует, что пользователь в настоящее время находится в User View, тогда как квадратные скобки показывают, что произошел переход к System View.

Функции CLI

Command	Function
CTRL+A	Помещает курсор в начало строки
CTRL+C	Останавлививает выполнение текущей функции
CTRL+Z	Возвращает к User View
CTRL+]	Останавливает входящие соединения и перенаправляет их

```
<Huawei>system-view  
Enter system view, return user view with Ctrl+Z.  
[Huawei]^z //Ctrl+Z  
<Huawei>
```

В этом примере показан набор общих сочетаний клавиш, которые широко используются для упрощения процесса навигации в интерфейсе командной строки VRP. Дополнительные команды:

CTRL + B перемещает курсор назад на один символ.

CTRL + D удаляет символ, в котором находится курсор.

CTRL + E перемещает курсор в конец текущей строки.

CTRL + F перемещает курсор вперед на один символ.

CTRL + H удаляет символ слева от курсора.

CTRL + N отображает следующую команду в буфере командной строки.

CTRL + P отображает предыдущую команду в буфере командной строки.

CTRL + W удаляет слово слева от курсора.

CTRL + X удаляет все символы слева от курсора.

CTRL + Y удаляет все символы справа от курсора.

ESC + B перемещает курсор на одно слово назад.

ESC + D удаляет слово справа от курсора.

ESC + F перемещает курсор вперед на одно слово.

Функции CLI

Command	Function
Backspace	Удаляет символ слева или справа, и помещает курсор слева
← or Ctrl+B	Перемещает курсор на знак влево
→ or Ctrl+F	Перемещает курсор на знак вправо
TAB	Завершает ввод уникальной команды

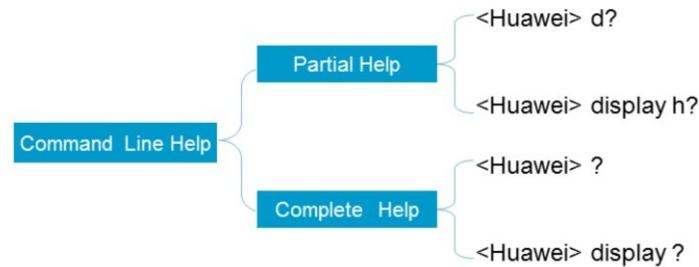
```
[Huawei]inter //TAB  
[Huawei]interface
```

- Клавиша **tab** автоматически заполнит введенную символьную строку.

Дополнительные функции клавиш могут использоваться для выполнения аналогичных операций, операция backspace имеет то же поведение, что и использование CTRL + H для удаления символа слева от курсора. Левые (←) и правые (→) клавиши курсора могут использоваться для выполнения той же операции, что и клавиши быстрого доступа CTRL + B и CTRL + F. Клавиша курсора вниз (↓) работает так же, как Ctrl + N, а клавиша курсора вверх (↑) действует как альтернатива операции CTRL + P.

Кроме того, функции командной строки поддерживают средство автоматического завершения, когда командное слово уникально. В этом примере демонстрируется, как интерфейс командного слова может быть автоматически завершен путем частичного завершения слова до такого состояния, в котором команда уникальна, за ней следует клавиша табуляции, которая обеспечит автоматическое завершение командного слова. Если командное слово не уникально, функция табуляции будет циклически переключаться с возможными параметрами завершения при каждом нажатии клавиши табуляции.

Вспомогательные функции CLI



[Huawei]d?	ddns	dhcp
	dhcpv6	diagnose
	display	dns
	domain	dot1x

Есть две формы помощи, которые можно найти в VRP, они представлены в виде частичной справки и полных справочных функций. При вводе символьной строки, непосредственно связанной с вопросительным знаком (?), VRP реализует функцию частичной справки для отображения всех команд, начинающихся с этой символьной строки, для этого показан пример на слайде. В случае функции полной справки знак вопроса (?) можно поместить в командной строке в любом представлении, чтобы отобразить все возможные имена команд, а также описания для всех команд, относящихся к этому представлению. Кроме того, полная функция справки поддерживает ввод команды, за которой следует знак вопроса (?), который разделяется пробелом. Затем отображаются все ключевые слова, связанные с этой командой, а также простые описания.

Базовая установки устройства CLI

Command	Function
sysname	Устанавливает имя устройства

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname RTA
[RTA]
```

- Системное имя должно быть связано с уникально идентифицируемым устройством в корпоративной сети.

В большинстве случаев, вероятно, будет существовать несколько устройств, и каждые из которых должны управляться. Таким образом, одной из первых важных задач ввода устройства в эксплуатацию является установка имен устройств для однозначного определения каждого устройства в сети. Параметр имени системы на маршрутизаторе серии AR2200 настроен как Huawei по умолчанию, для коммутатора серии S5720 по умолчанию используется системное имя HUAWEI. Внедрение имени системы вступает в силу сразу же после завершения настройки.

Настройка часов CLI

Command	Function
clock timezone	Установка часового пояса
clock datetime	Установка даты и времени
clock daylight-saving-time	Перевод на летнее время

```
<Huawei>clock timezone BJ add 08:00:00
<Huawei>clock datetime 10:20:29 2016-04-11
<Huawei>display clock
2016-04-11 10:20:48
Thursday
Time Zone (BJ) : UTC+08:00
```

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 10



Системные часы отражают системное время и могут быть настроены на соответствие правилам любого региона. Системные часы должны быть правильно настроены для обеспечения синхронизации с другими устройствами и рассчитываться по формуле: Coordinated Universal Time (UTC) + смещение часового пояса + переход на летнее время. Команда `datetime` используется для установки системных часов по формуле `HH:MM:SS YYYY-MM-DD`. Следует отметить, однако, что если часовой пояс не был настроен или установлен на 0, дата и время считаются UTC, поэтому рекомендуется сначала установить часовой пояс, прежде чем настраивать системное время и дату.

Настройка локального часового пояса достигается с помощью команды часового пояса и выполняется на основе `time-zone-name { add / minus }`, где значение `add` указывает, что `time-zone-name` = UTC плюс смещение по времени, а `minus` указывает, что время `time-zone-name` = UTC минус смещение по времени.

В некоторых регионах требуется переход на летнее время для поддержания синхронизации часов с любым изменением часового пояса в определенные периоды года. VRP может поддерживать функции летнего времени для фиксированных дат и дат, которые определяются на основе набора предопределенных правил. Например, переход на летнее время в United Kingdom происходит в последнее воскресенье марта и в последнее воскресенье октября, поэтому правила могут применяться для обеспечения того, чтобы изменения происходили на основе таких плавающих дат.

Сообщения заголовка CLI

Command	Function
header login	Устанавливает заголовок, который отображается, когда пользователь авторизовался на устройстве
header shell	Устанавливает заголовок, который отображается, когда пользователь вошел на устройство

```
[Huawei]header login information "welcome to huawei certification!"  
[Huawei]header shell information "Please don't reboot the device!"  
.....  
welcome to huawei certification!  
Login authentication  
Password:  
Please don't reboot the device!  
<Huawei>
```

Команда заголовка предоставляет средство для отображения уведомлений при подключении к устройству. Заголовок входа в систему указывает заголовок, который отображается, когда соединение терминала активировано, и пользователь аутентифицируется устройством. Заголовок оболочки указывает заголовок, который отображается, когда сеанс настроен, после входа пользователя в устройство. Информация заголовка может применяться либо как текстовая строка, либо извлекаться из указанного файла. Если используется текстовая строка, символ начала и конца должен быть определен как маркер для идентификации информационной строки. Стока представляет значение в диапазоне от 1 до 2000 символов, включая пробелы. Команда заголовка, основанная на информации, соответствует формату *header {login | shell}*, где *text* представляет информационную строку, включая начальные и конечные маркеры. В случае файлового заголовка, применяется файл заголовка формата *{login | shell}*, где *file-name* представляет каталог и файл, из которого может быть получена информационная строка.

Уровни команд CLI

User Level	Command Level	Name
0	0	Visit level
1	0 and 1	Monitoring level
2	0,1 and 2	Configuration level
3-15	0,1,2 and 3	Management level

```
<Huawei> system-view  
[Huawei]command-privilege level 3 view user save
```

- Уровни привилегий управляют доступом аккаунта к командам

Системные структуры обеспечивают доступ к функциям команд иерархически для защиты безопасности системы. Системный администратор устанавливает уровни доступа пользователей, которые предоставляют конкретным пользователям доступ к определенным уровням команд. Уровень команды пользователя - это значение от 0 до 3, а уровень доступа пользователя - от 0 до 15. Уровень 0 определяет уровень доступа к командам, которые запускают средства диагностики сети (например, пинг и traceroute), а также такие команды, как telnet-клиентские соединения и команды отображения.

Уровень мониторинга определяется на уровне пользователя 1, для которого могут применяться командные уровни 0 и 1, что позволяет использовать большинство команд отображения, за исключением команд отображения текущей и сохраненной конфигурации. Уровень пользователя 2 представляет собой уровень конфигурации, для которого могут быть определены уровни команд до 2, что обеспечивает доступ к командам, которые настраивают сетевые службы, предоставляемые непосредственно пользователям, включая команды маршрутизации и сетевого уровня. Конечным уровнем является уровень управления, который представляет собой уровень пользователя от 3 до 15 и командный уровень до 3, обеспечивая доступ к командам, которые контролируют основные системные операции и обеспечивают поддержку служб.

Эти команды включают файловую систему, FTP, TFTP, переключение конфигурационных файлов, управление питанием, управление резервным копированием, управление пользователями, настройку уровней, настройку внутренних параметров системы и команды отладки для диагностики неисправностей. Данный пример демонстрирует, как можно изменить командную привилегию, где в этом случае команда для сохранения требуется 3 уровень, из-за чего команда не может быть применена.

Пользовательские интерфейсы CLI

User Interface	Relative Number
Console	0
VTY	0-4

```
<Huawei>system-view  
[Huawei]user-interface vty 0 4  
[Huawei-ui-vty0-4]
```

- Число VTY может быть расширено до 0-14 для дополнительных Telnet/SSH пользовательских соединений.

Каждый пользовательский интерфейс содержит его представление или представление командной строки, предоставляемое системой. Вид командной строки используется для настройки и управления всеми физическими и логическими интерфейсами в асинхронном режиме. Пользователи, желающие подключиться к устройству, должны указать определенные параметры, чтобы пользовательский интерфейс стал доступным. Реализованы две общие формы пользовательского интерфейса: консольный интерфейс (CON) и интерфейс виртуального телетайпа (VTY).

Консольный порт представляет собой асинхронный последовательный порт, предоставляемый основной панелью управления устройства, и использует относительное число 0. VTY - это логическая терминальная линия, которая позволяет настроить соединение, когда устройство использует службы telnet для подключения к терминалу для локального или удаленного доступа к устройству. Максимум 15 пользователей могут использовать логический пользовательский интерфейс VTY для входа в устройство, расширив диапазон от 0 до 4, достигнув путем применения команды *user-interface maximum-vty 15*. Если установлено максимальное количество пользователей входа в систему 0, пользователям не разрешается регистрироваться на маршрутизаторе через telnet или SSH. Команда *display user-interface* может использоваться для отображения релевантной информации о пользовательском интерфейсе.

CLI Атрибуты терминала

Command	Function
idle-timeout	Устанавливает длительность пользовательского соединения
screen-length	Устанавливает количество линий отображаемых в терминале
history-command max-size	Устанавливает количество команд в буфере прошлых команд

```
# Set the size of the history command buffer to 20.  
<Huawei>system-view  
[Huawei]user-interface console 0  
[Huawei-ui-console0]history-command max-size 20  
# Set the timeout duration to 1 minute and 30 seconds.  
[Huawei-ui-console0]idle-timeout 1 30
```

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 14



Для консольных и VTY-терминальных интерфейсов некоторые атрибуты могут применяться расширения функций и повышения безопасности. Пользователь позволяет подключению оставаться бездействующим в течение определенного периода времени, представляет угрозу безопасности для системы. Система будет ожидать период ожидания до автоматического завершения соединения. Этот период ожидания простоя на пользовательском интерфейсе устанавливается по умолчанию по умолчанию 10 минут.

Если может потребоваться увеличить или уменьшить количество строк, отображаемых на экране терминала при использовании команды отображения, например, можно использовать команду *screen-length*. По умолчанию это значение равно 24, однако, может быть увеличено до 512 строк. *screen-length 0*, однако, не рекомендуется, так как вывод не будет отображаться.

Для каждой используемой команды запись сохраняется в буфере команд истории, который может быть получен путем навигации с помощью клавиш (\uparrow) или CTRL + P и (\downarrow) или клавиш Ctrl + N. Количество записанных команд в буфере команд истории может быть увеличено с помощью команды *history-command max-size*, чтобы определить до 256 сохраненных команд. Количество команд, сохраненных по умолчанию, равно 10.

CLI интерфейс Разрешений

Command	Function
user privilege	Устанавливает уровень пользователя
set authentication password	Устанавливает локальный пароль

```
# Set the user level on the VTY0 user interface to 2.  
<Huawei>system-view  
[Huawei]user-interface vty 0  
[Huawei-ui-vty0]user privilege level 2  
[Huawei-ui-vty0-4]set authentication password cipher  
Enter Password(<8-128>):huawei123
```

Доступ к интерфейсам пользовательских терминалов обеспечивает четкую точку входа для неавторизованных пользователей для доступа к устройству и реализации изменений конфигурации. Таким образом, возможность ограничения доступа и ограничения того, какие действия могут быть выполнены, необходима как средство обеспечения безопасности устройства. Конфигурация пользовательских привилегий и аутентификации - это два способа обеспечения безопасности терминала. Пользовательские привилегии позволяют определить пользовательский уровень, который ограничивает возможности пользователя для определенного диапазона команд. Уровень пользователя может быть любым значением в диапазоне от 0 до 15, где значения представляют собой уровень посещения (0), уровень мониторинга (1), уровень конфигурации (2) и уровень управления (3).

Аутентификация ограничивает возможности пользователя обращаться к терминальному интерфейсу, запрашивая аутентификацию пользователя с использованием пароля или комбинации имени пользователя и пароля, прежде чем доступ через пользовательский интерфейс будет предоставлен. В случае соединений VTY все пользователи должны пройти аутентификацию до того, как возможен доступ. Для всех пользовательских интерфейсов существует три возможных режима аутентификации, в виде AAA, аутентификации паролем и без аутентификации. AAA обеспечивает аутентификацию пользователя с высокой степенью безопасности, для которой необходимо ввести имя пользователя и пароль для входа. Для аутентификации паролем требуется только пароль для входа в систему, поэтому для всех пользователей может применяться один пароль. Не использование аутентификации устраняет любую аутентификацию, применяемую к пользовательскому интерфейсу.

Следует отметить, что интерфейс консоли по умолчанию использует режим без аутентификации. Обычно рекомендуется, чтобы для каждого пользователя, которому был предоставлен доступ к telnet, пользователь вводил имя и пароль, чтобы обеспечить различие между отдельными пользователями. Каждому пользователю также должны быть предоставлены уровни привилегий, основанные на каждой роли и ответственности пользователей.

CLI интерфейс Конфигурации



```
# Configure an IP address of 10.0.12.1/24 on interface G0/0/0  
and an IP address of 1.1.1.1/32 on loopback interface 0.  
<Huawei>system-view  
[Huawei]interface GigabitEthernet 0/0/0  
[Huawei-GigabitEthernet0/0/0]ip address 10.0.12.1 255.255.255.0  
[Huawei-GigabitEthernet0/0/0]interface loopback 0  
[Huawei-LoopBack0]ip address 1.1.1.1 32
```

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 16



Для запуска IP-сервисов на интерфейсе IP-адрес должен быть настроен для интерфейса. Как правило, для интерфейса требуется только первичный IP-адрес. В особых случаях для интерфейса может быть настроен дополнительный IP-адрес.

Например, когда интерфейс маршрутизатора, такого как AR2200, подключается к физической сети, а хосты в этой физической сети относятся к двум сегментам сети. Чтобы AR2200 мог взаимодействовать со всеми хостами в физической сети, настройте первичный IP-адрес и вторичный IP-адрес для интерфейса. Интерфейс имеет только один первичный IP-адрес. Если новый IP-адрес настроен на интерфейсе, который уже имеет первичный IP-адрес, новый IP-адрес переопределяет исходный IP-адрес. IP-адрес можно настроить для интерфейса, используя команду `ip address <ip-address> {mask / mask-length}`, где `mask` представляет маску подсети 32 бит, например. 255.255.255.0, а `mask-length` представляет собой альтернативное значение длины маски например 24, оба из которых могут быть взаимозаменяемы.

Интерфейс `loopback` представляет собой логический интерфейс, который применяется для представления адреса сети или IP-хоста и часто используется как форма интерфейса управления для поддержки ряда протоколов, посредством которых осуществляется связь с IP-адресом интерфейса `loopback`, в отличие от IP-адреса физического интерфейса, на котором принимаются данные.



Итог

- Сколько пользователей могут присоединяться к интерфейсу консоли в одновременно?
- Какое состояние устанавливает команда loopback interface 0

1. Консольный интерфейс способен поддерживать только одного пользователя в любой момент времени; это осуществлено представлением пользовательского интерфейса консоли 0.

2. Интерфейс loopback представляет собой логический интерфейс, который отсутствует в маршрутизаторе до его создания. После создания, интерфейс loopback считается включенным. Однако на устройствах ARG3 интерфейсы loopback могут быть отключены.



Thank you

www.huawei.com

Навигация и управление в файловой системе

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

Файловая система представляет собой базовую платформу, на которой работает VRP и где системные файлы хранятся в физическом хранилище устройства продукта. Возможность навигации и управления этой файловой системой необходима для обеспечения эффективного управления конфигурацией файлов, обновления программного обеспечения VRP и содержание физических устройств в хорошем состоянии.



Цели

После завершения этой главы вы сможете:

- Успешно перемещаться в файловой системе устройства
- Управлять файловой системой и папками
- Управлять маршрутизаторами Huawei и коммутационными устройствами хранения

Просмотр файловой системы

Function	Command
Изменить директорию	cd
Просмотреть текущую директорию	pwd
Просмотреть содержимое директории	dir
Просмотреть содержимое	more

```
<Quidway>dir
Directory of flash:/
  Idx Attr      Size(Byte) Date        Time      FileName
  0  drw-          - Apr 10 2016 09:30:35  src
  1  -rw-         28 Apr 10 2016 09:31:38  private-data.txt
  2  -rw-        120 Apr 10 2016 09:32:38  wzbk1.cfg
32,004 KB total (31,995 KB free)
```

Файловая система управляет файлами и каталогами на устройствах хранения. Он может создавать, удалять, изменять или переименовывать файл или каталог, отображать содержимое файла.

Файловая система имеет две функции: управление устройствами хранения и управление файлами, хранящимися на этих устройствах. Существует ряд каталогов, в которых файлы хранятся в логической иерархии. Эти файлы и каталоги могут управляться с помощью ряда функций, которые позволяют изменять или отображать каталоги, отображать файлы в таких каталогах или подкаталогах, а также создавать или удалять каталоги.

Общие примеры команд файловой системы для общей навигации включают команду *cd*, используемую для изменения текущего каталога, *pwd* для просмотра текущего каталога и *dir*, чтобы отобразить содержимое каталога, как показано в примере. Доступ к файловой системе осуществляется из User View.

Управление файловой системой

Function	Command
Создать директорию	mkdir
Удалить директорию	rmdir

```
<Quidway>mkdir test
Info: Create directory flash:/test.....Done.
<Quidway>dir
Directory of flash:/
  Idx Attr      Size(Byte) Date        Time      FileName
  0  drw-       -   Apr 10 2016 09:30:35  src
  1  -rw-       28  Apr 10 2016 09:31:38  private-data.txt
  2  -rw-       120 Apr 10 2016 09:32:38  wzbk1.cfg
  3  drw-       -   Apr 10 2016 09:53:11  test
32,004 KB total (31,995 KB free)
```

Внесение изменений в существующие каталоги файловой системы обычно связано с необходимостью создания и удаления существующих каталогов в файловой системе. Две общие команды, которые используются в этом случае, команда *mkdir directory* используется для создания папки в указанном каталоге на определенном устройстве хранения, где *directory* ссылается на имя, указанное в каталоге, и для которого имя каталога может содержать строку от 1 до 64 символов. Чтобы удалить папку в файловой системе, используется команда каталога *rmdir directory*, а *directory* снова ссылается на имя каталога. Следует отметить, что каталог можно удалить только в том случае, если в нем нет файлов.

Управление файловой системой

Function	Command
Копировать файл	copy
Переместить файл	move
Переименовать файл	rename

```
<Quidway>rename test huawei
Rename flash:/test to flash:/huawei ?[Y/N]:y
Info: Rename file flash:/test to flash:/huawei .....Done.
<Quidway>dir
Directory of flash:/
Idx Attr Size(Byte) Date Time FileName
0 drw- - Apr 10 2016 09:30:35 src
1 -rw- 28 Apr 10 2016 09:31:38 private-data.txt
2 -rw- 120 Apr 10 2016 09:32:38 wzbk1.cfg
3 drw- - Apr 10 2016 09:53:11 huawei

32,004 KB total (31,995 KB free)
```

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 6



Внесение изменений в файлы в файловой системе включает в себя копирование, перемещение, переименование, сжатие, удаление, деинсталляцию, удаление файлов в корзине, запуск файлов в пакетном режиме и настройку режимов подсказки. Создание дубликата существующего файла может быть выполнено с помощью команды *copy source-filename destination-filename*, где, если *destination-filename* совпадает с именем существующего файла (*source-filename*), система отобразит сообщение, указывающее, что существующий файл будет заменен. Имя целевого файла не может совпадать с именем загрузочного файла, иначе система отобразит сообщение о том, что операция недействительна и файл является загрузочным. Команда *move source-filename destination-filename* может использоваться для перемещения файлов в другой каталог. После успешного выполнения команды *move* исходный файл вырезается и перемещается в определенный файл назначения. Однако следует отметить, что команда перемещения может перемещать только файлы на одном и том же устройстве хранения.

Управление файловой системой

Function	Command
Удалить [безвозвратно] файл	delete /unreserved
Восстановить файл	undelete
Безвозвратно очистить корзину	reset recycle-bin

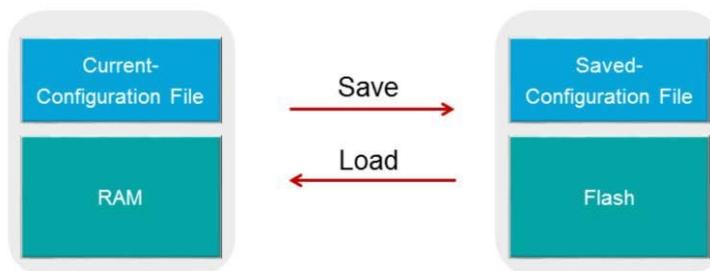
```
<Quidway>delete /unreserved flash:/wzbk1.cfg
<Quidway>dir
Directory of flash:/
  Idx Attr      Size(Byte) Date        Time      FileName
  0  drw-       -          Apr 10 2016 09:30:35  src
  1  -rw-       28         Apr 10 2016 09:31:38  private-data.txt
  2  drw-       -          Apr 10 2016 09:53:11  huawei

32,004 KB total (30,995 KB free)
```

Для удаления файлов в файловой системе функция удаления может быть применена с помощью команды `delete [/unreserved] [/force] {filename | device-name}`. Как правило, удаленные файлы направляются в корзину, из которой файлы могут быть восстановлены с помощью `undelete {filename | device-name}`, однако при использовании команды `/unreserved` файл будет удален безвозвратно. Обычно система выводит сообщение с просьбой подтвердить удаление файла, однако, если параметр `/force` включен, запрос не будет выдаваться. Параметр `filename` относится к файлу, который должен быть удален, а параметр `device-name` определяет место хранения файла.

Если файл перенаправлен в корзину, он не удаляется навсегда и может быть легко восстановлен. Чтобы гарантировать, что такие файлы в корзине будут удалены постоянно, можно применить команду `reset recycle-bin [filename]`, где параметр `filename` позволит удалить конкретный файл.

Система управления файлами



- Текущая конфигурация загружена из сохраненной конфигурации в Flash-памяти системы при ее загрузке.

При включении, устройство извлекает файлы конфигурации из пути сохранения для инициализации по умолчанию, которые затем сохраняются в RAM устройстве. Если файлы конфигурации отсутствуют в пути сохранения, маршрутизатор использует параметры инициализации по умолчанию.

Текущий файл конфигурации указывает на конфигурации, действующие на устройстве, когда он запущен. Когда конфигурации сохранены, текущие конфигурации хранятся в файлах сохраненных конфигураций в месте хранения устройства. Если устройство загрузило файл текущей конфигурации, основанной на определении инициализации параметров, файл сохраненной конфигурации не будут существовать в хранилище пути по умолчанию, но будут генерироваться после сохранения текущей конфигурации.

Просмотр файлов конфигурации

Command	Function
display current-configuration	Просмотр текущей конфигурации
display saved-configuration	Просмотр сохраненной конфигурации

```
<Huawei>display current-configuration
#
sysname Huawei
....
#
return
<Huawei>display saved-configuration
#
sysname Huawei
....
#
return
```

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 9



Используя команду *display current-configuration*, параметры устройства, которые вступают в силу, могут быть запрошены. Если по умолчанию значения для определенных параметров будут использоваться, эти параметры не выводятся на экран. Команда текущих конфигураций включает номера параметров, которые позволяют фильтровать список команд во время использования функции отображения. *Display current-configuration | begin {regular-expression}* это пример как текущие конфигурации могут быть использованы для отображения активных параметров, которые начинаются с определенного ключевого слова или выражения. Альтернатива этой команды *display current-configuration | include {regular-expression}* позволяет параметрам включать конкретные ключевые слова или выражения в пределах файлов текущих конфигураций.

display saved-configuration [last | time] показывает вывод сохраненных файлов конфигурации используемых при запуске для генерации текущих конфигураций. Где параметр *last* используется для отображения файлов конфигурации, используемые в текущем запуске. Файлы конфигурации отображаются только тогда, когда он настроен для текущего запуска. Параметр *time* отобразит время, когда конфигурация была последний раз сохранена.

Сохранение файлов конфигурации

Command	Function
Save	Сохранение текущей конфигурации

```
<Huawei>save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]y
It will take several minutes to save configuration file, please
wait.....
Configuration file had been saved successfully
Note: The configuration file will take effect after being activated
```

Используя команду `save [configuration-file]` будет сохранена текущая информация конфигураций на пути хранения по умолчанию. Параметр `configuration-file` позволяет текущей информации конфигурации сохраняться в специальный файл. Запуск команды `save` с параметром `configuration-file` не влияет на текущий запуск файлов конфигурации системы. Когда параметр `configuration-file` совпадает с файлом конфигурации, хранящимся на пути хранения по умолчанию в системе, функция этой команды совпадает с командой `save`.

В примере демонстрируется использование команды `save` текущих конфигураций, которые по умолчанию буду сохранены в файле `vrgcfg.zip` по умолчанию в хранилище устройства.

Просмотр параметров запуска

Command	Function
Display startup	Просмотр текущих параметров конфигурации

```
<Huawei>display startup
MainBoard:
    Configured startup system software:          flash:/ar2220.cc
    Startup system software:                     flash:/ar2220.cc
    Next startup system software:                NULL
    Startup saved-configuration file:           flash:/vrpcfg.zip
    Next startup saved-configuration file:       flash:/vrpcfg.zip
    Startup paf file:                          NULL
    Next startup paf file:                     NULL
    Startup license file:                      NULL
    Next startup license file:                 NULL
    Startup patch package:                     NULL
    Next startup patch package:                NULL
```

Используемый в настоящее время файл сохранения конфигурации может быть обнаружен с помощью команды *display startup*. К тому же команда *display startup* может быть использована для запроса имени текущего файла системного программного обеспечения, имени следующего файла системного программного обеспечения, имени предыдущего файла системного программного обеспечения, имени четырех используемых (если используется) файлов системного программного обеспечения, и имени следующих четырех файлов системного программного обеспечения. Четыре файла системного программного обеспечения являются вышеупомянутыми файлами конфигурации, голосовыми файлами, файл путей, файл лицензии.

Изменение параметров запуска

Command	Function
startup saved-configuration	Указать сохраненный файл конфигурации для загрузки при запуске


```
<Huawei>startup saved-configuration flash:/huawei.zip
Info: Succeeded in setting the configuration for booting system.
<Huawei>display startup
MainBoard:
    Configured startup system software:          flash:/ar2220.cc
    Startup system software:                      flash:/ar2220.cc
    Next startup system software:                 NULL
    Startup saved-configuration file:            flash:/vrpcfg.zip
    Next startup saved-configuration file:        flash:/huawei.zip
    Startup paf file:                           NULL
    Next startup paf file:                      NULL
    Startup license file:                       NULL
    Next startup license file:                  NULL
    Startup patch package:                      NULL
    Next startup patch package:                 NULL
```

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 12



После обнаружения файла «*startup save-configuration*», может потребоваться определить новый файл конфигурации, который будет загружен при следующем запуске. Если конкретный файл конфигурации не указан, по умолчанию файл конфигурации будет загружен при следующем запуске.

Имя файла конфигурации должно быть расширения .cfg или .zip, и файл должен быть помещен в корень каталога из сохраняемого устройства. Когда маршрутизатор включен, файл конфигурации читается из Flash-памяти по умолчанию для инициализации. Дата в файле конфигурации - это первоначальная конфигурация. Если нет сохраненных файлов конфигурации в Flash-памяти, маршрутизатор использует по умолчанию первоначальные параметры.

Через использования запуска «*saved-configuration [configuration-file]*», где параметр «*configuration-file*» это файл конфигурации используемый к запуску, возможен при следующей инициализации запуска системы в файле конфигурации по умолчанию.

Сравнение файлов конфигурации

Command	Function
compare configuration	Сравнение файлов конфигурации

```
<Huawei>compare configuration
===== Current configuration line 36 =====
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
interface NULL0
===== Configuration file line 37 =====
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
interface NULL0
```

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 13



При использовании команды `compare configuration [configuration-file] [current-line-number save-line-number]`, система выполняет построчно сравнение из сохраненной конфигурации с текущей конфигурацией начиная с первой линии. Если параметры `current-line-number` и `save-line-number` указаны, система игнорирует конфигурацию `non-relevant` до сравнения линий и продолжения нахождения различий между файлами конфигураций.

Затем система будет продолжать выводить разные конфигурации между файлами сохраненной конфигурацией и текущими конфигурациями. Сравнение выходной информации ограничена в 150 символов по умолчанию. Если для сравнения требуется меньше 150 символов, то отображаются все варианты до конца двух файлов.

Очистка файла конфигурации

Command	Function
reset saved-configuration	Удалить сохраненный файл конфигурации

```
<Huawei>reset saved-configuration
Warning: This will delete the configuration in the flash memory.
The device configurations will be erased to reconfigure. Are you
sure? [Y/N]:y
Info: Clear the configuration in the device successfully.
```

Команда *reset saved-configuration* используется для удаления файла конфигурации запуска устройства с запоминающего устройства ЗУ. При выполнении системы сравнивает файлы конфигурации использованные в текущем запуске и в следующем запуске при удалении файла конфигурации с маршрутизатора.

Если оба файла конфигурации одинаковые, они удаляются одновременно после выполнения этого команды. По умолчанию, файл конфигурации используется, когда маршрутизатор запускается в следующий раз. Если оба файла конфигурации различны, файл конфигурации, используемый в текущем запуске, удаляется после выполнения этой команды.

Если файл конфигурации не настроен для текущего запуска устройства, система выводит сообщение о том, что файла конфигурации не существует после выполнения этой команды. После использования команды *saved-configuration*, вам будет предложено подтвердить действие, для которого ожидается подтверждение пользователя, как показано на примере.

Типы запоминающих устройств

- SDRAM
- Flash
- NVRAM
- SD Card
- USB

```
<Huawei>display version
.....
SDRAM Memory Size      : 1024      M bytes
Flash Memory Size       : 512       M bytes
NVRAM Memory Size      : 512       K bytes
.....
```

Запоминающие устройства ЗУ зависят от продукта и включают flash-память, SD-карты или USB-накопители. Например, маршрутизатор AR2200E имеет встроенную flash-память и встроенную SD-карту (в слоте usb1). Маршрутизатор предоставляет два зарезервированных USB слота (usb0, Usb1) и слот SD-карты (sd0). Для модели S5700 она включает в себя встроенную flash-память с емкостью, которая зависит от модели, с 64 Мб в моделях S5700-LI, S5700S-LI и S5710-EL, и 32 Мб для других. Подробная информация о запоминающих устройствах ЗУ Huawei может подробно описана с помощью команды *display version*, как показано на рисунке.

Очистка запоминающего устройства

```
<Huawei>format flash:  
All data(include configuration and system startup file) on flash:  
will be lost, proceed with format? (y/n) [n]:  
  
<Huawei>format sd1:  
All data(include configuration and system startup file) on sd1: will  
be lost, proceed with format? (y/n) [n]:
```

- Следует соблюдать осторожность при использовании команд *format*, поскольку данные будут потеряны.

Форматирование запоминающего устройства, вероятно, приведет к потере всех файлов на устройстве хранения, и файлы не смогут быть восстановлены, поэтому при выполнении любой команды *format* следует проявлять особую осторожность, ее следует избегать, если это абсолютно необходимо. Команда *format [storage-device]* используется вместе с параметром *storage-device* для определения места хранения, которое требуется отформатировать.

Исправление запоминающего устройства

```
<Huawei>fixdisk flash:  
Fixdisk flash: will take long time if needed  
%Fixdisk flash: completed.  
<Huawei>fixdisk sd1:  
sd1:/ - disk check in progress.....sd1:/ - Volume is OK  
total # of clusters: 481,869  
# of free clusters: 455,777  
# of bad clusters:  
total free space: 1,780 Mb  
..... max contiguous free space: 1,789,952,000 bytes  
# of files: 22  
.....  
%Fixdisk sd1: completed.
```

Когда последние устройства показывают, что система потерпела неудачу, команда *fixdisk* может использоваться для попытки исправления неработоспособного файла системы в запоминающем устройстве, однако она не дает никаких гарантий относительно успешного восстановления файловой системы. Если в системе не возникли проблемы, то не рекомендуется запускать эту команду, поскольку команда используется для устранения проблем. Следует отметить, что команда не устраняет проблемы на уровне устройства.



Итог

- Что означает *d* в атрибуте *dmx* файловой системы?
- Как файл конфигурации, хранящийся в файловой системе устройства, будет задействован для использования?

1. Атрибут файловой системы *d* означает, что запись является каталогом в файловой системе. Следует отметить, что этот каталог можно удалить только после удаления всех файлов, содержащихся в каталоге. Остальные значения *mx* ссылаются на то, можно ли читать, записывать, и/или выполнять их.
2. Конфигурация может быть сохранена под отдельным именем по умолчанию *vrgcfg.zip* и сохранена на запоминающем устройстве маршрутизатора или переключателя. Если этот файл необходимо использовать в качестве активного файла конфигурации в системе, следует использовать команду *startup saved-configuration <configuration-file-name>*, где *configuration-file-name* – имя файла и расширения файла.



Thank you

www.huawei.com

Управление образами операционной системы VRP

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

Эффективное администрирование и управление сетью в корпоративной сети зависит от всех устройств, поддерживающих резервные файлы в случае сбоев системы или других событий, которые могут привести к потере важных системных файлов и данных. Удаленные серверы, использующие службу протокола передачи файлов (FTP), часто используются для обеспечения хранения файлов в целях резервного копирования и поиска по мере необходимости. В этом разделе представлены средства установки связи с приложениями таких служб.

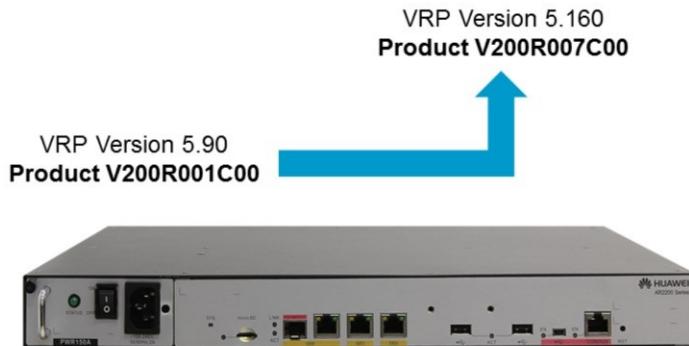


Цели

По завершению этой главы вы сможете:

- Объяснить важность поддержания современных версий VRP.
- Установка отношений клиента с FTP-сервером.
- Успешное обновление изображения системы VRP.

Обновление образа VRP



- Иногда может потребоваться обновление до новой версии для поддержания новых функций и обновление универсальной платформы маршрутизатора.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 4



Платформа VRP постоянной обновляется, чтобы поддерживать соответствующие изменения в технологии и поддерживать новые достижения аппаратного обеспечения. Изображения VRP обычно определяется версией VRP номером устройства. Продукты Huawei ARG3 и Sx7 серии в целом согласуются с VRP версии 5, с которой связаны различные устройства.

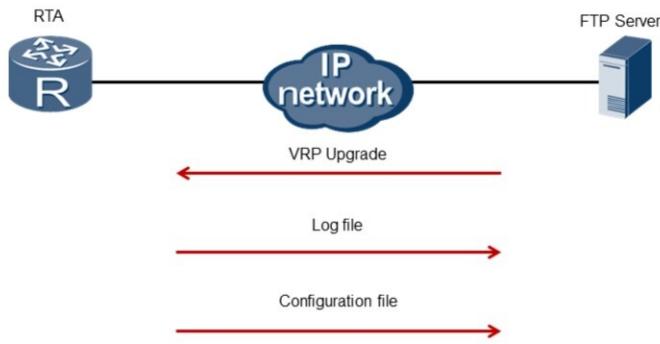
По мере увеличения версии устройств, так же увеличиваются функции, поддерживаемые версией. Формат версии устройства включает код продукта Vxxx, Rxxx обозначающие выпуск основной версии и Cxx неосновной (вторичной) версии. Если пакет обновления используется для исправления версии продукта VRP, значение SPC также может быть включено в номер версии продукта VRP. Типичные примеры обновления версии VRP для AR2200E включают:

Version 5.90 (AR2200 V200R001C00)

Version 5.110 (AR2200 V200R002C00)

Version 5.160 (AR2200 V200R007C00)

Передача файлов



- Передача файлов может использоваться для получения файлов образа VRP, а также резервных журналов и файлов конфигурации.

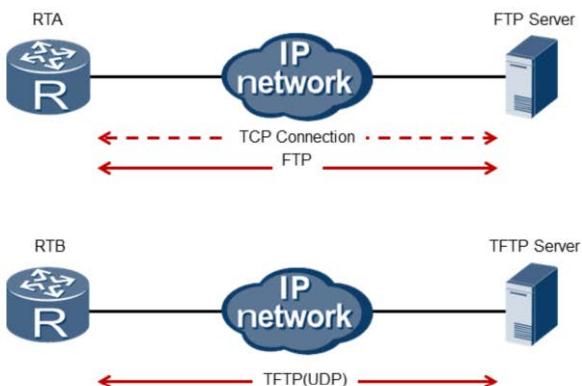
Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 5



Передача файлов относится к средствам, с помощью которых файлы отправляются или извлекаются с удаленного сервера или места хранения. В рамках IP-сети это приложение может быть реализовано для самых разных целей функционирования. В рамках эффективной практики, обычно дублируются важные файлы и резервируются в удаленном хранилище, чтобы предотвратить любые потери, которые могут повлиять на работу критической системы. Сюда входят такие файлы, как изображение устройств VRP, которые (если существующее изображение потерпит потерю посредством использования команды *format* или других форм ошибок) могут быть извлечены удаленно и использованы для восстановления системных операций. Аналогичные принципы применимы к важным файлам конфигурации и сохранению записей о деятельности на устройствах, хранящихся в файлах журналов, которые могут храниться в течение длительного времени на удаленном сервере.

Методы передачи файлов

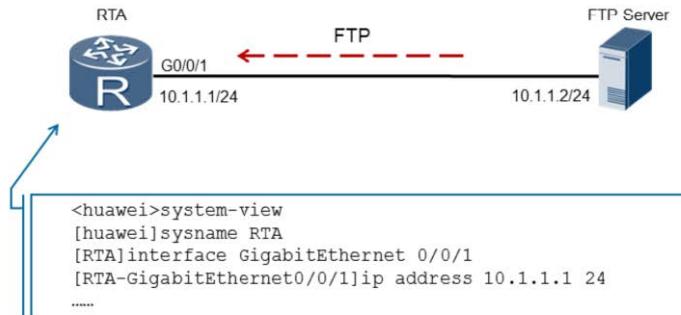


- Общие формы передачи файлов включают FTP и TFTP, соответственно, различаются в используемых протоколах третьего уровня.

FTP - стандартный протокол приложений, основанный на наборе протоколов TCP/IP и используемый для передачи файлов между локальными клиентами и удаленными серверами. FTP использует два подключения ТРС для копирования файла из одной системы в другую. ТРС-соединения обычно устанавливаются в режиме клиент-сервер, один для управления (номер порта сервера 21), а другой для передачи данных (номер порта сервера 20). FTP как протокол передачи файлов используется для управления соединениями путем выдачи команд от клиента (RTA) на сервер и передачи ответов от сервера клиенту, что минимизирует задержку передачи. Что касается передачи данных, FTP передает данные между клиентом и сервером, максимизируя пропускную способность.

Протокол Trivial File Protocol (TFTP) - это простой протокол передачи файлов, по которому маршрутизатор может работать в качестве TFTP-клиента для доступа к файлам на TFTP-сервере. В отличие от FTP, TFTP не имеет сложного интерфейса интерактивного доступа и проверки подлинности. Реализация TFTP основана на протоколе User Datagram Protocol (UDP). Клиент инициирует передачу UDP. Для загрузки файлов клиент отправляет пакет запроса на чтение на TFTP-сервер, принимает пакеты с сервера и возвращает подтверждение на сервер. Чтобы загрузить файлы, клиент отправляет пакет на сервер и получает подтверждение от сервера.

Процесс обновления VRP



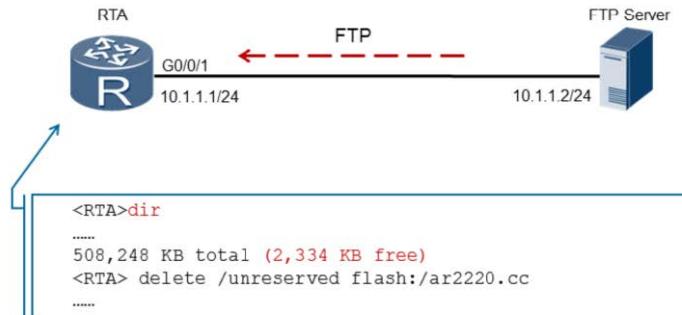
Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 7



В этом примере показано, как устанавливается связь между FTP-сервером и клиентом для получения изображения VRP, которое может использоваться как часть процесса обновления системы. Перед любой передачей данных необходимо установить базовое соединение, по которому файлы могут быть переданы. Это начинается с предоставления подходящей IP-адресации для клиента и сервера. Если устройства подключены напрямую, могут применяться интерфейсы, принадлежащие к одной и той же сети. Если устройства принадлежат сетям, расположенным на большой географической территории, устройства должны устанавливать соответствующую IP-адресацию в пределах своих заданных сетей и иметь возможность обнаруживать соответствующий сетевой путь по IP, через который можно установить соединение между клиентом и сервером.

Доступное место для хранения



- Если емкость хранилища недостаточна для передачи образов, старые образы и файлы могут быть удалены.

Пользователь должен определить достаточно ли пространства для хранения файла, который должен быть извлечен для обновления системы. Команды файловой системы могут использоваться для определения текущего состояния файлов системы, включая файлы, которые в настоящее время присутствуют в папке хранения файлов устройства, а также объем доступного пространства. В случае FTP-сервера если места хранения недостаточно для передачи файлов, некоторые файлы могут быть удалены или загружены, если они все еще могут понадобиться для будущего использования.

В примере демонстрируется использование команды `delete` файловой системы для существующего файла изображения. Следует отметить, что системное удаленное изображения не повлияет на текущую работу устройства, пока устройство остается в рабочем состоянии, поэтому устройство не следует отключать или перезапускать потому, как новый файл изображения VRP будет восстановлен в пределах места хранения устройства и настроен для использования при следующем запуске системы.

Получение файлов с FTP-сервера



```
<RTA>ftp 10.1.1.2
Trying 10.1.1.2 ...
Press CTRL+K to abort
Connected to 10.1.1.2.
220 FTP service ready.
User(10.1.1.2:(none)) :huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[ftp]get vrp.cc
```

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

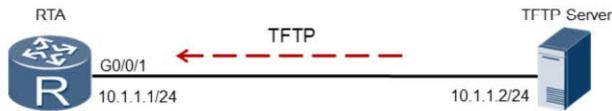
Page 9



Для извлечения файлов с FTP-сервера необходимо сначала установить соединение до того, как произойдет передача файла. В клиентском устройстве услуга FTP инициируется с использованием адреса FTP <ip address>, где IP-адрес относится к адресу FTP-сервера, к которому клиент хочет подключиться. FTP-соединения будут установлены с использованием TCP, потребуются аутентификация в виде имени и пароля, которые определены FTP-сервером. Как только аутентификация будет успешно пройдена, клиент установит доступ к FTP-серверу и сможет использовать различные команды для просмотра существующих файлов, хранящихся в локальном текущем каталоге сервера.

До передачи файла пользователю может потребоваться установка файла, для которого существуют два формата: ASCII и Binary. Режим ASCII используется для текста, в котором данные преобразуются из символьного представления отправителя в «8-разрядный ASCII» перед передачей, а затем в представление символов для получателя. Двоичный режим, с другой стороны, требует, чтобы отправитель отправил каждый файла побитово. Этот режим часто используется для передачи файлов изображений и программных файлов и должен применяться при отправке или извлечении любого файла изображения VRP. В этом примере команда `get vrp.cc` была выпущена для получения нового изображения VRP, расположенного на удаленном сервере.

Получение файлов с TFTP-сервера.

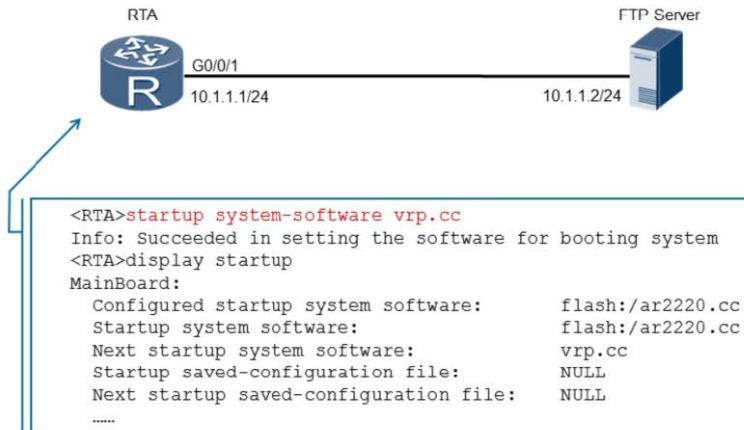


```
<RTA>tftp 10.1.1.2 get AR2220E-V200R007C00SPC600.cc
```

- Одна команда, включая IP-адрес назначения, используется для извлечения файлов с TFTP-сервера.

В случае, если клиент хочет получить изображение VRP с TFTP-сервера, сначала не нужно устанавливать соединение с сервером. Вместо этого клиент должен определить путь к серверу в командной строке, а также операцию, которая должна быть выполнена. Следует также отметить, что модели AR2200E & S5720 служат только как TFTP-клиент и передают файлы только в двоичном формате. Как видно из примера, команда «get» применяется для извлечения файла изображения VRP с TFTP-сервера после определения адреса назначения TFTP-сервера.

Процесс управления загрузкой VRP



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

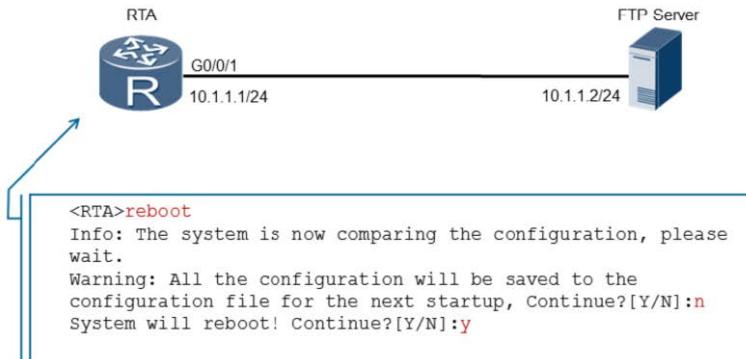
Page 11



Передача файла изображения VRP клиенту после его успешного достижения требует, чтобы изображение было включено в качестве программного обеспечения для запуска при следующем запуске системы. Чтобы изменить версию системного программного обеспечения, необходимо запустить команду *startup system-software* и включить файл системного программного обеспечения, который будет использоваться при следующем запуске. Файл системного программного обеспечения должен использовать .cc в качестве расширения имени файла, а файл системного программного обеспечения, используемый при следующем запуске, не может быть использован в текущем запуске.

Кроме того, каталог хранилища файла системного программного обеспечения должен быть корневым каталогом, иначе файл не будет работать. Команда *display startup* должна использоваться для проверки успешного выполнения изменения запуска программного обеспечения. Выход для запуска программного обеспечения системы должен показывать существующее изображение VRP, в то время как следующий запуск программного обеспечения системы должна отображать переданное изображение VRP, которое теперь присутствует в корневой директории устройства.

Применение изменений



- Система должна быть перезапущена до того, как новый образ вступит в действие.

Подтверждение запуска программного обеспечения системы позволяет безопасно запускать системное программное обеспечение во время следующей загрузки системы. Чтобы применить изменения и позволить новому системному программному обеспечению вступить в силу, устройство необходимо перезапустить. Команда *reboot* может быть использована для перезапуска системы. Во время процесса перезагрузки будет отображено приглашение с запросом подтверждения о том, будет ли сохранен файл конфигурации для следующего запуска системы.

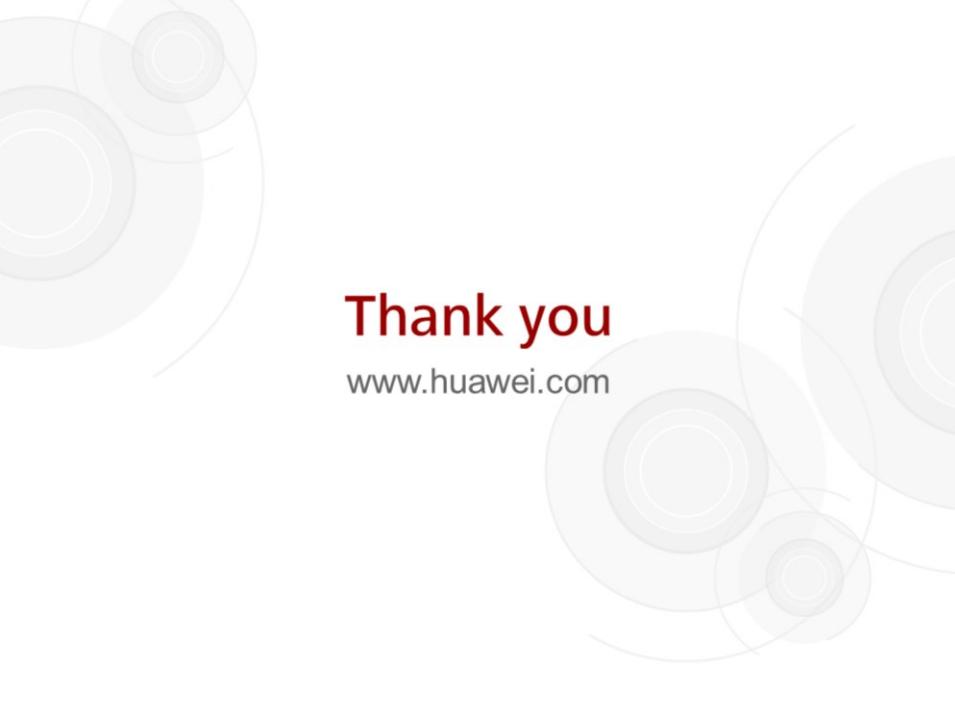
В некоторых случаях файл сохраненной конфигурации может быть удален пользователем, чтобы можно было использовать новую конфигурацию, если это произошло, ожидается, что пользователь ответит «*но*» на «*Продолжить*». Если пользователь выбирает «*yes*», в этой точке текущая конфигурация будет перезаписана в файл сохраненной конфигурации и снова применена во время следующего запуска. Если пользователь не знает об изменениях, для которых запрос сохранения содержит предупреждение, рекомендуется выбрать «*но*» или «*п*» и выполнить сравнение сохраненной и текущей конфигурации, чтобы проверить изменения. Для запроса перезагрузки ответ «*yes*» или «*у*» требуется для завершения процесса перезагрузки.



Итог

- Что должно быть настроено на клиенте, чтобы установить соединение с FTP-сервером?
- Как пользователь может подтвердить, что изменения в программном обеспечении запуска вступили в силу после перезагрузки?

1. Клиентское устройство должно иметь возможность доступа к FTP-серверу по IP-адресу, требуя, чтобы IP-адрес был настроен на интерфейсе, через который может быть достигнут FTP-сервер. Это позволит проверять путь к серверу FTRP на сетевом уровне, если он существует.
2. Пользователь может запустить запуск отображения команды конфигурации, чтобы проверить, что текущее системное программное обеспечение запуска (VRP) активно, идентифицированное расширением .cc.



Thank you

www.huawei.com

Создание единой
коммутируемой сети

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

Внедрение коммутационного устройства как части сети предприятия демонстрирует, как сети могут расширяться за пределы соединений «точка-в-точку» и совместно использовать сетей, в которых могут возникать конфликты. Поведение коммутатора предприятия при входе в локальную сеть подробно описано вместе с пониманием управления фреймами одноадресного и широковещательного типов, чтобы продемонстрировать, как коммутаторы позволяют сетям преодолевать препятствия производительности общих сетей.

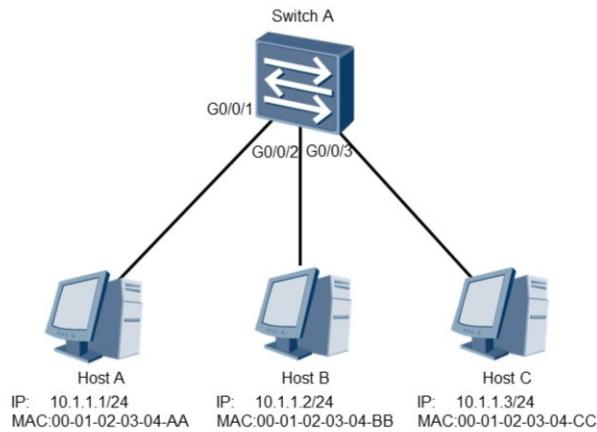


Цели

После завершения этой главы вы сможете:

- Объяснить процесс принятия решений переключателем уровня ссылки.
- Настроить параметры для согласования на коммутаторе уровня ссылки.

Построение единой коммутируемой сети



- Переключатели работают в пределах уровня канала передачи данных.

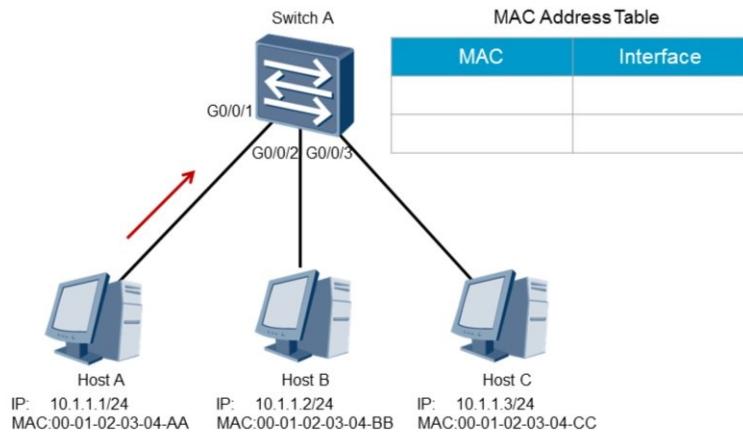
Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 4



По мере расширения сети предприятия необходимо создать несколько пользователей в составе сети с множественным доступом. Эволюция сетевых технологий показала переход от общих локальных сетей к сетям, которые поддерживают множественные области конфликтов и поддерживают использование форм носителя 100BaseT, которые изолируют передачу и прием данных по отдельным парам проводов, тем самым устранивая конфликты, происходящие и обеспечивающие более высокую скорость передачи в дуплексном режиме. Создание коммутатора позволяет повысить плотность портов, чтобы обеспечить подключение большего количества конечных системных устройств в пределах одной локальной сети. Каждая конечная система или хост в локальной сети должна быть подключена как часть одной и той же IP-сети для облегчения связи на сетевом уровне. Однако IP-адрес относится только к хост-системам, поскольку коммутационные устройства работают в пределах уровня канала связи и поэтому опираются на MAC-адресацию для пересылки фреймов.

Начальное состояние переключателя



- Каждый коммутатор использует MAC таблицу для принятия решения о пересылке.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

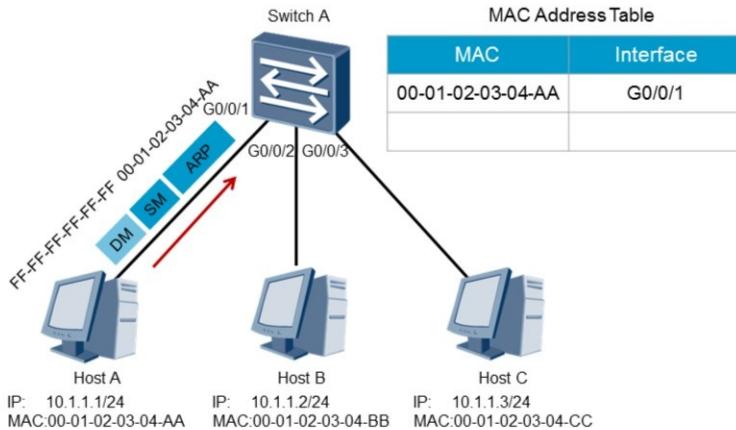
Page 5



В качестве устройства уровня канала каждый коммутатор использует таблицу на основе MAC, которая обеспечивает связь между MAC-адресом назначения и интерфейсом порта, через который должен быть переадресован фрейм. Это обычно называют таблицей MAC-адресов.

Начало инициализации коммутатора начинается с того, что коммутатор не знает конечных систем и как следует передавать фреймы, полученные от конечных систем. Необходимо, чтобы записи сборки коммутатора в таблице MAC-адресов определяли путь, который должен получить каждый принятый фрейм, чтобы достичь определенного адресата, чтобы ограничить широковещательный трафик в локальной сети. Эти записи маршрута заполняются в MAC-адресе таблицу в результате полученных от конечных систем фреймов. В этом примере узел А переадресовал фрейм коммутатору А, который в настоящее время не имеет записей в своей таблице MAC-адресов.

Изучение MAC-адресов



- Записываются исходные MAC-адреса принятых кадров.

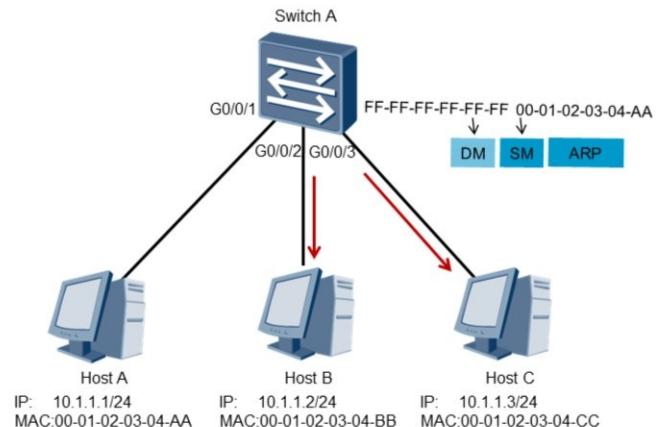
Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 6



Фрейм, который пересыпается из хоста А, содержит запись широковещательного MAC-адреса в поле адреса заголовка фрейма. Поле исходного адреса содержит MAC-адрес пирингового устройства, в данном случае хост А. Этот исходный MAC-адрес используется коммутатором для заполнения таблицы MAC-адресов путем связывания записи MAC в поле адреса источника с коммутатором интерфейсом порта, на который был получен фрейм. В этом примере показано, как MAC-адрес связан с интерфейсом порта, чтобы позволить любому возвращающемуся трафику для этого адресата MAC перенаправляться напрямую через соответствующий интерфейс.

Пересылка первых данных.



- Кадры, предназначенные для неизвестных целей канала связи, теряются.

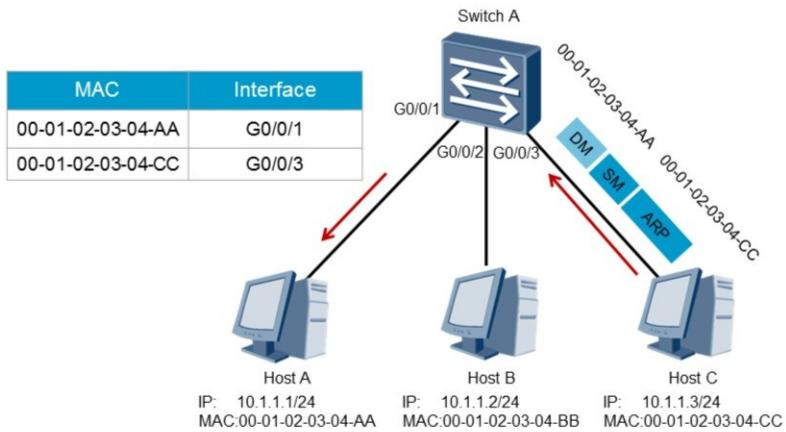
Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 7



Общее поведение запроса ARP предполагает, что фрейм загружается во все предназначенные адресаты в основном из-за широковещательной передачи MAC (FF-FF-FF-FF FF-FF), которая представляет текущий пункт назначения. Поэтому коммутатор отвечает за пересылку этого фрейма из каждого интерфейса порта, за исключением интерфейса порта, на котором был получен фрейм, в попытке найти назначенный IP-адрес, указанный в заголовке ARP, для которого может быть сгенерирован ответ ARP. Как показано в примере, отдельные фреймы заливаются из коммутатора через интерфейсы портов G0/0/2 и G0/0/3 в сторону хоста В и хоста С соответственно.

Ответ адресата информации



- Кадры передаются адресатам на основе MAC таблицы.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 8

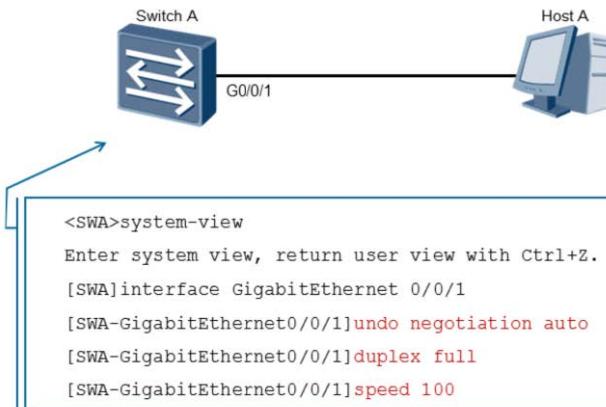


В результате заголовок запроса ARP принимающий узел может определить, что заголовок ARP предназначен для IP-адресата 10.1.1.3, а также локальный адрес источника (MAC), из которого был создан фрейм, и использовать эту информацию для генерации одноадресного ответа.

Информация, относящаяся к хосту А, связана с IP-адресом 10.1.1.3 и сохраняется в таблице MAC-адресов узла С. При этом генерация широковещательного трафика сводится к минимуму, тем самым уменьшая количество прерываний до местных адресатов, а также уменьшает количество фреймов, распространяющих локальную сеть.

После того, как фрейм принимается от хоста С с помощью коммутатора А, коммутатор заполняет таблицу MAC-адресов исходным MAC-адресом принятого фрейма и связывает его с интерфейсом порта, на котором находится фрейм, который был получен. Затем коммутатор использует таблицу MAC-адресов для выполнения поиска, чтобы обнаружить интерфейс пересылки на основе MAC-адреса назначения фрейма. В этом случае MAC-адрес фрейма относится к узлу А, для которого теперь существует запись через интерфейс G0/0/1, позволяя пересылать фрейм известному адресату.

Основные конфигурации



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 9

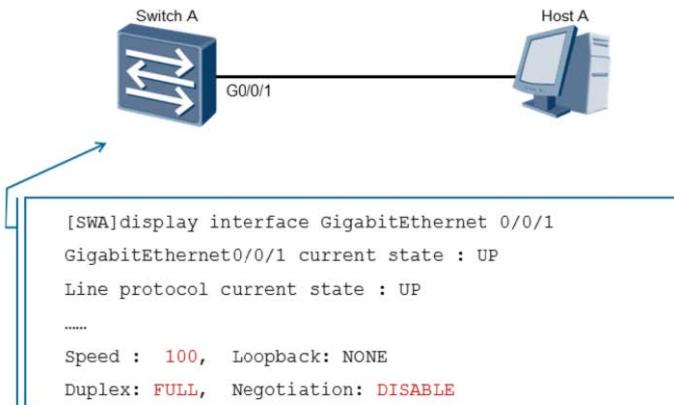


Ранние Ethernet-системы работали на основе полудуплексного режима 10 Мбит/с и применяли такие механизмы, как CSMA/CD, чтобы обеспечить стабильность системы. Переход на среду с витой парой вызвал появление полнодуплексного Ethernet, что значительно улучшило производительность Ethernet и позволило согласовать две формы дуплекса. Технология автоматического согласования позволяет более новым системам Ethernet быть совместимыми с более ранними системами Ethernet.

В режиме автосогласования интерфейсы на обоих концах линии связывают свои рабочие параметры, включая дуплексный режим, скорость и управление потоком. Если согласование завершается успешно, оба интерфейса работают с одинаковыми рабочими параметрами. Однако, в некоторых случаях, необходимо вручную определить параметры переговоров, например, когда интерфейсы Gigabit Ethernet, работающие в режиме автосогласования, подключаются через сетевой кабель 100 Мбит/с. В таких случаях переговоры между интерфейсами не удастся.

Из-за разных моделей продуктов коммутаторы HUAWEI могут не поддерживать дуплексный режим смены портов, см. Руководство по продукту.

Проверка основных конфигураций



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 10



В случае изменения параметров конфигурации для согласования с использованием автосогласования определенные параметры должны быть проверены с помощью команды *display interface <interface>*, чтобы убедиться, что параметры позволяют успешно согласовать интерфейс канала связи. Это подтверждается текущим состоянием протокола линии, отображаемым как UP. Отображаемая информация показывает текущие настройки параметров для интерфейса.



Итог

- Если коммутатор записывает исходный MAC-адрес хост-устройства в интерфейс порта, а физическое соединение хоста затем переключается на другой интерфейс порта на коммутаторе, какое действие будет принимать коммутатор?

Когда хост или другая конечная система подключена к интерфейсу порта коммутатора, создается добровольный ARP, который предназначен для обеспечения уникальности IP-адресов в сегменте сети. Однако сообщение ARP также предоставляет коммутатору информацию о MAC-адресе хоста, который затем включается в таблицу MAC-адресов и связан с интерфейсом порта, на котором подключен хост.

Если физическое соединение хоста, подключенного к интерфейсу порта коммутатора удалено, коммутатор обнаружит, что физическая ссылка не работает и удалит запись MAC из таблицы MAC-адресов. После того, как среда подключена к другому интерфейсу порта, порт обнаружит, что физическая ссылка активна, и добровольный ARP будет генерироваться хостом, позволяя коммутатору обнаруживать и заполнять таблицу MAC-адресов MAC-адресом подключенного хоста.

Протокол остовного дерева (STP)

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

По мере того как сеть предприятия расширяется, мультикоммутируемые сети вводятся для обеспечения связи уровня коммуникаций между растущим числом конечных систем. По мере формирования новых взаимосвязей между множественными коммутаторами предприятия, появляются новые возможности для построения устойчивых сетей, однако увеличивается вероятность ошибки коммутации в результате петель становится все более вероятной. Следовательно, STP следует понимать с точки зрения поведения в предотвращении петли коммутации и того, как им можно управлять, чтобы он подошел проекту и производительности сети.

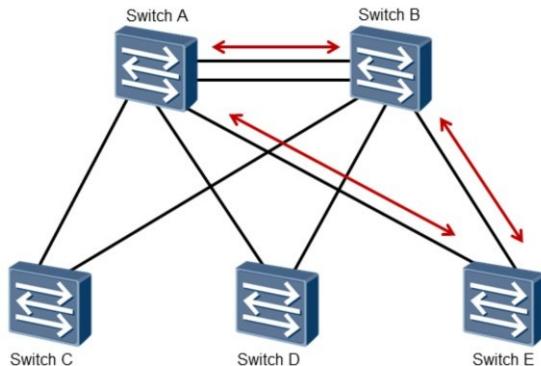


Цели

По завершении этого раздела вы сможете:

- Описывать проблемы, возникающие при использовании мульти-коммутируемых сетей.
- Объяснять процесс предотвращения зацикливания STP.
- Настраивать параметры для управления проектом сети STP.

Избыточность

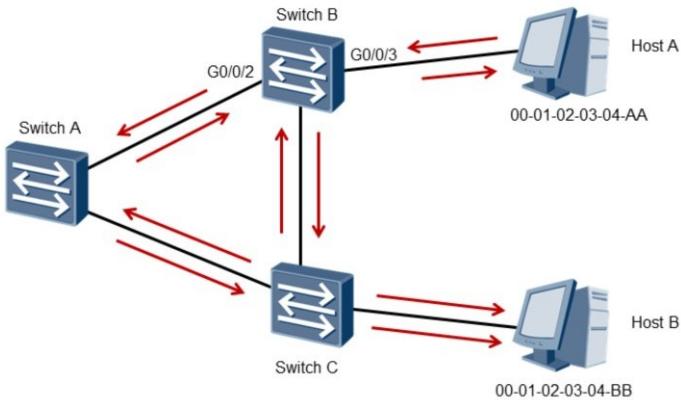


Резервирование в коммутационной сети сводит к минимуму ошибки соединения, но создает потенциально переключающие петли.

Рост предприятия приводит к вводу нескольких коммутаторов для поддержки взаимосвязи конечных систем и сервисов, необходимых для ежедневных операций. Однако взаимосвязь нескольких коммутаторов создает дополнительные проблемы, которые необходимо решить. Коммутаторы могут быть установлены как двухточечные линии связи, через которые конечные системы могут направлять кадры в адресаты, расположенные через другие коммутаторы в широковещательном домене. Однако отказ от любой двухточечной связи приводит к немедленной изоляции нисходящего коммутатора и всех конечных систем, к которым подключена связь. Чтобы решить эту проблему, избыточность настоятельно рекомендуется в любой коммутационной сети.

Таким образом, избыточные связи обычно используются в коммутационной сети Ethernet для обеспечения резервного копирования ссылок и повышения надежности сети. Однако использование избыточных ссылок может создавать петли, которые приводят к резкому ухудшению качества связи, а также к серьезным перебоям в обслуживании связи.

Широковещательные штормы

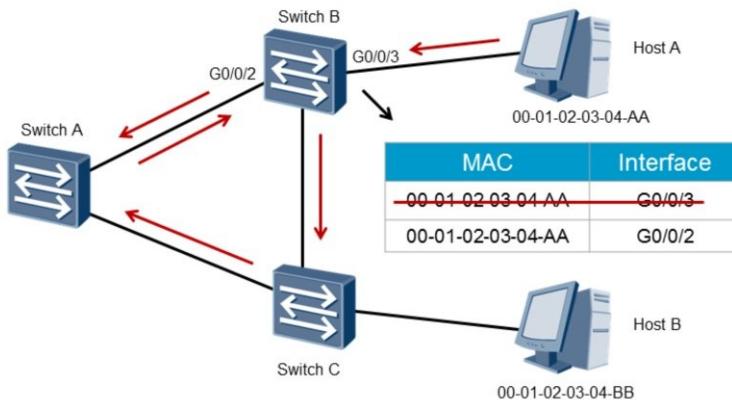


Коммутационные петли позволяют осуществлять широковещательные штормы и дублирование кадров, которые должны быть получены конечными станциями.

Один из первых эффектов избыточных переключающих петель приходит в виде широковещательных штормов. Это происходит, когда конечная система пытается обнаружить место назначения, для которого не известно ни сам путь, ни переключатели по пути переключения. Таким образом, широковещательная передача генерируется конечной системой, которая заполняется принимающим коммутатором.

Эффект заполнения означает, что кадр пересыпается через все интерфейсы, исключая интерфейс, на который был получен кадр. В этом примере хост А генерирует кадр, который принимается коммутатором В, который впоследствии пересыпается из всех других интерфейсов. Экземпляр кадра принимается подключенными коммутаторами А и С, которые, в свою очередь, заполняют кадр из всех других интерфейсов. Продолжающийся эффект заполнения приводит к тому, что экземпляры заполнений Switch A и Switch C с одного переключателя на другой, которые, в свою очередь, заполняются обратно в Switch B, и, следовательно, петля продолжается. Кроме того, эффект повторного заполнения приводит к тому, что несколько экземпляров кадра принимаются конечными станциями, что фактически приводит к прерываниям и экстремальному снижению производительности коммутатора.

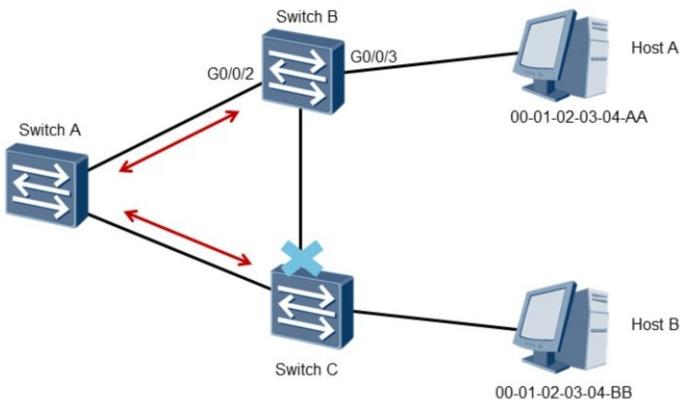
Нестабильность MAC-адресов



Получение ранее пересылаемых кадров генерирует ложный MAC-адрес записей и нестабильность в таблице MAC-адресов.

Коммутаторы должны содержать записи о пути, по которому доступно место назначения. Это идентифицируется путем объединения исходного MAC-адреса кадра с интерфейсом, на который был получен кадр. Только один экземпляр MAC-адреса может быть сохранен в таблице MAC-адресов коммутатора, и когда принимается второй экземпляр MAC-адреса, более поздняя информация имеет приоритет. В этом примере коммутатор B обновляет таблицу MAC-адресов MAC-адресом хоста A и связывает этот источник с интерфейсом G0/0/3, интерфейсом порта, на котором был получен кадр. Поскольку кадры неконтролируемо заполняются в коммутационную сеть, кадр снова принимается с тем же исходным MAC-адресом, что и хост A, однако на этот раз кадр принимается на интерфейсе G0/0/2. Поэтому коммутатор B должен предположить, что хост, который был первоначально доступен через интерфейс G0/0/3, теперь доступен через G0/0/2 и соответственно обновит таблицу MAC-адресов. Результат этого процесса приводит к неустойчивости MAC и продолжает происходить бесконечно между интерфейсами портов коммутатора, соединяющимися с коммутатором A и коммутатором C, поскольку кадры заполняются в обоих направлениях как часть эффекта широковещательной шторма.

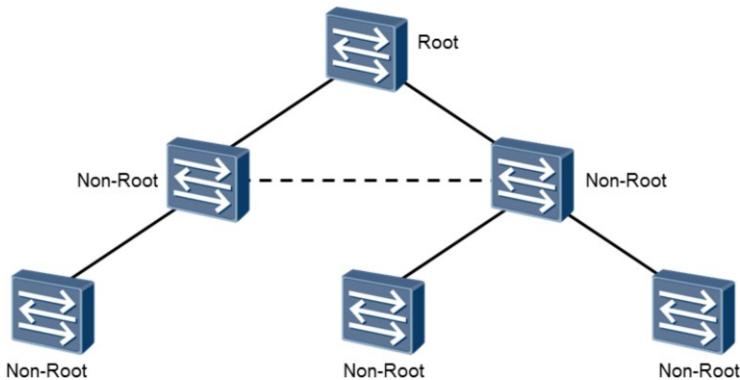
Проблемы избыточности



Петли устраняются путем ограничения потока трафика по избыточному пути.

Задача для коммутационной сети заключается в возможности поддерживать избыточность коммутации, чтобы избежать изоляции конечных систем в случае отказа коммутационной системы или отказа канала, а также возможность избежать повреждающих эффектов коммутационных петель в топологии коммутации, которая реализует избыточность. Полученное решение в течение многих лет заключалось в том, чтобы реализовать STP, чтобы предотвратить эффекты переключающих петель. Связующее дерево работает по принципу, что избыточные ссылки логически отключены, чтобы обеспечить топологию без петель, в то же время имея возможность динамически активировать вторичные ссылки в случае возникновения сбоя по первому пути переключения, тем самым выполняя требование избыточности сети в топологии без петель. Коммутационные устройства, работающие с STP, обнаруживают петли в сети, обмениваясь информацией друг с другом и блокируя определенные интерфейсы для обрезания петель. STP продолжает оставаться важным протоколом для LAN более 20 лет.

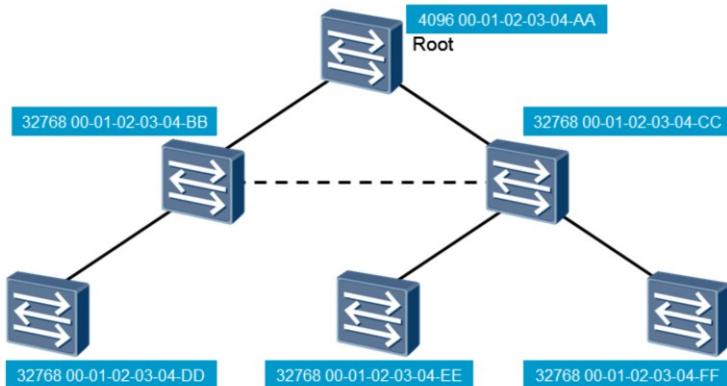
Связующий корневой мост



В результате STP создается инвертированная древовидная архитектура. Корневой мост представляет собой основание связующего дерева.

Удаление любой возможности появления петель - основная цель связующего дерева, для которого формируется архитектура с инвертированным деревом. В основе этого логического дерева лежит корневой мост / переключатель. Корневой мост представляет собой логический центр, но не обязательно физический центр сети, поддерживающей STP. Назначенный корневой мост способен динамически меняться с топологией сети, как в случае, когда существующий корневой мост не может продолжать работать как корневой мост. Некорневыми мостами считаются находящиеся ниже по потоку от корневого моста, а соединение с некорневыми мостами идет от корневого моста к некорневым. Только один корневой мост может существовать в конвергентной сети, поддерживающей STP, в любой момент времени.

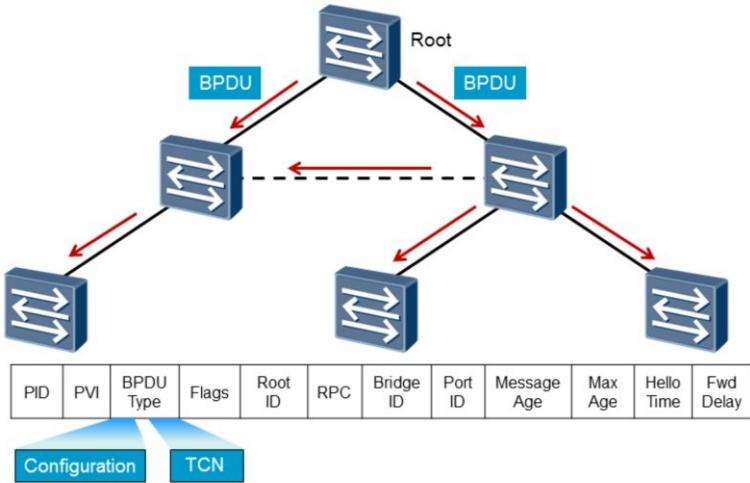
Bridge ID



Идентификаторы моста используются для выбора корневого моста. Приоритет моста можно изменять для принудительного выбора корня.

Обнаружение корневого моста для сети STP является основной задачей, выполняемой для формирования связующего дерева. Протокол STP работает на основе выборов, через которые определяется роль всех коммутаторов. Идентификатор моста определяется как средство, с помощью которого обнаруживается корневой мост. Он состоит из двух частей, первый из которых является приоритетом 16-битного моста, а второй - 48-битным MAC-адресом. Устройство, которое, как говорят, содержит наивысший приоритет (наименьший идентификатор моста), выбирается как корневой мост для сети. При сопоставлении идентификаторов моста первоначально учитывается приоритет моста, и если это значение приоритета неспособно однозначно идентифицировать корневой мост, дополнительно используется MAC-адрес. Идентификатором моста можно управлять путем изменения приоритета моста в качестве средства включения данного переключателя в качестве корневого моста, часто поддерживающего оптимизированный проект сети.

Bridge Protocol Data Unit



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 10

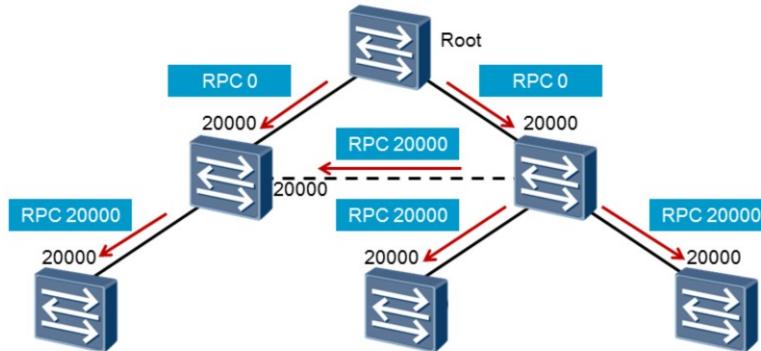


Топология оственного дерева основывается на передаче конкретной информацией для определения роли и статуса каждого коммутатора в сети. Модуль данных мостового протокола (BPDU) облегчает обмен данными в сети оственного дерева. В STP используются две формы BPDU. Конфигурация BPDU изначально создается корнем и распространяется по нисходящему потоку, чтобы гарантировать, что все некорневые мости остаются в курсе состояния топологии оственного дерева и, что еще важнее, корневого моста. BPDU TCN является второй формой BPDU, которая распространяет информацию в направлении вверх по направлению к корню и должна быть представлена более подробно как часть процесса изменения топологии.

BPDU напрямую не пересылаются коммутаторами, вместо этого информация, которая передается в BPDU, часто используется для генерации собственных BPDU коммутаторов для передачи. Конфигурация BPDU содержит ряд параметров, которые используются мостом для определения в первую очередь наличия корневого моста и обеспечения того, чтобы корневой мост оставался мостом с наивысшим приоритетом. Кажется, что каждый сегмент ЛВС имеет назначенный коммутатор, который отвечает за распространение BPDU вниз по течению до не назначенных коммутаторов.

Поле Bridge ID используется для определения текущего назначенного коммутатора, из которого ожидается получение BPDU. BPDU генерируется и перенаправляется корневым мостом на основе таймера Hello, который по умолчанию установлен на 2 секунды. Поскольку BPDU принимаются коммутаторами нисходящего потока, новый BPDU генерируется с локально определенными параметрами и перенаправляется всем не назначенным коммутаторам для сегмента LAN.

Стоимость пути



Стоимость корневого пути переносится в BPDU и используется для определения кратчайший путь к корню.

Другой особенностью BPDU является распространение двух параметров, относящихся к стоимости пути. Стоимость корневого пути (RPC) используется для измерения стоимости пути к корневому мосту для определения кратчайшего пути связующего дерева и тем самым генерации свободной петли. Когда мост является корневым мостом, стоимость корневого пути равна 0.

Стоимость пути (PC) - это значение, связанное с корневым портом, который является портом в нисходящем коммутаторе, который подключается к сегменту LAN, на котором находится назначенный коммутатор или корневой мост. Это значение используется для генерации стоимости корневого пути для коммутатора путем добавления стоимости пути к значению RPC, которое получено от назначенного коммутатора в сегменте локальной сети, для определения нового значения стоимости корневого пути. Это новое значение стоимости корневого пути переносится в BPDU назначенного коммутатора и используется для представления стоимости пути для корня.

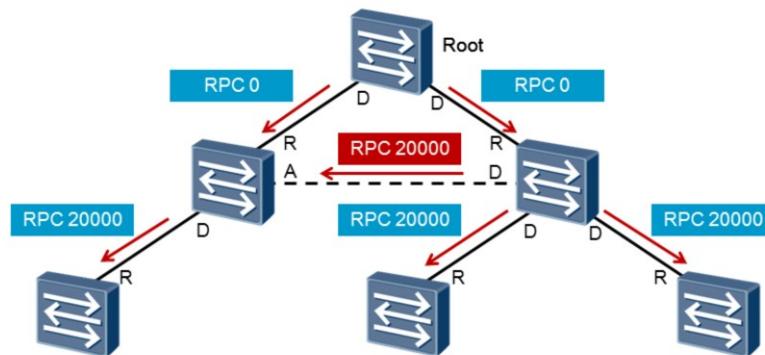
Стандарты стоимости пути

Port Speed	802.1D	802.1t	Path Cost Legacy
10 Mbps	99	1999999	1999
100 Mbps	18	199999	199
1 Gbps	4	20000	20
10 Gbps	2	2000	2

STP поддерживает различные стандарты стоимости пути. 802.1t является стандартом по умолчанию, используемым коммутаторами Huawei.

Коммутаторы серии Huawei Sx7 поддерживают ряд альтернативных стандартов стоимости пути, которые могут быть реализованы на основе требований предприятия, например, где может существовать сеть коммутации с несколькими поставщиками. Коммутаторы серии Huawei Sx7 по умолчанию используют стандарт затрат по стандарту 802.1t, обеспечивая более высокую метрическую точность для расчета стоимости пути.

Роли портов связующего дерева



Связующее дерево поддерживает назначенные, корневые и альтернативные порты.

Стоимость корневого пути позволяет определить роли портов.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 13



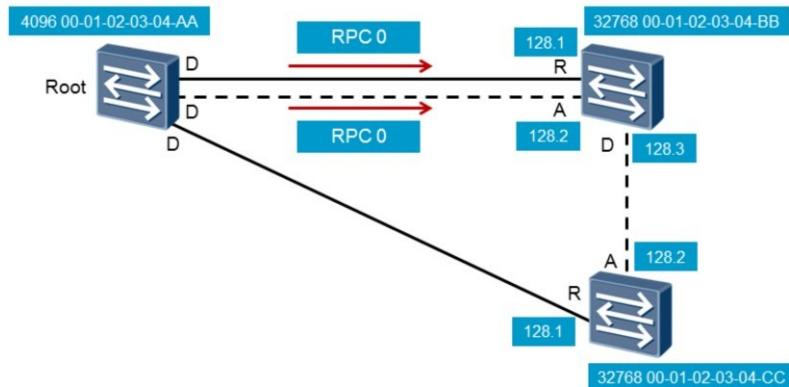
Конвергентная сеть оставных деревьев определяет, что каждому интерфейсу должна быть назначена определенная роль порта. Роли портов используются для определения поведения интерфейсов портов, которые участвуют в активной топологии оставного дерева. Для STP определены три роли порта - назначенный, корневой и альтернативный.

Назначенный порт связан с корневым мостом или назначенным мостом сегмента локальной сети и определяет нисходящий путь, через который переадресовываются BPDU конфигурации. Корневой мост отвечает за формирование конфигурации BPDU для всех нисходящих коммутаторов, и поэтому интерфейсы портов корневого моста всегда принимают назначенную роль порта.

Корневой порт определяет порт, который предлагает путь с наименьшей стоимостью для корня, исходя из стоимости корневого пути. В примере демонстрируется случай, когда два пути остаются в корне, однако в качестве корневого порта назначается только порт, который предлагает самую низкую стоимость корневого пути. Если два или более порта предлагают равные затраты на корневой путь, решение о том, какой интерфейс порта будет корневым, определяется путем сравнения идентификатора моста в конфигурации BPDU, которая принимается на каждом порту.

Любой порт, которому не назначен назначенная или корневая роль порта, считается альтернативным портом и может принимать BPDU от назначенного коммутатора для сегмента LAN для контроля состояния резервной ссылки, но не будет обрабатывать полученные BPDU. Стандарт IEEE 802.1D-1990 для STP первоначально определял эту роль порта как резервное копирование, однако в него были внесены поправки, чтобы стать альтернативной ролью порта в пересмотре стандартов IEEE 802.1D-1998.

ID порта

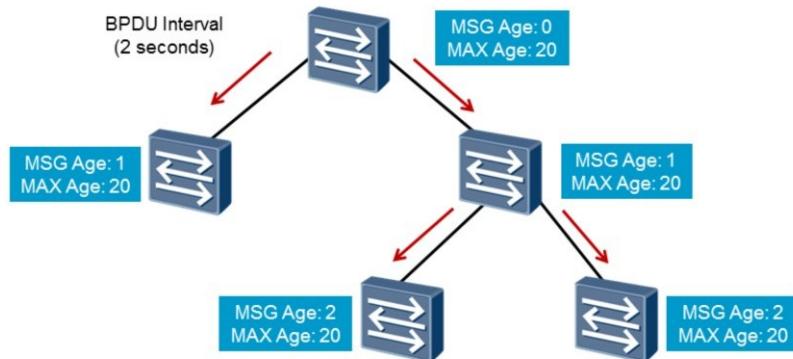


Если стоимости корневых путей равны, то идентификатор порта используется для определения активного и альтернативного пути к корню.

Идентификатор порта представляет собой окончательное средство для определения ролей портов наряду с механизмом мостового идентификатора и корневого пути. В сценариях, где два или более портов предлагают равные стоимости корневого пути обратно к корню и для которых, как считается, имеет место идентификатор моста, который в первую очередь связан с тем, что восходящий коммутатор является одним и тем же переключателем для обоих путей, для определения ролей портов необходимо использовать идентификатор порта.

Идентификатор порта привязан к каждому порту и содержит приоритет порта и номер порта, который ассоциируется с интерфейсом порта. Приоритет порта - это значение в диапазоне от 0 до 240, назначаемое с шагом 16 и представляемое значением по умолчанию 128. Если оба порта имеют одинаковое значение приоритета порта, уникальный номер порта используется для определения ролей портов. Самый высокий идентификатор порта (самый низкий номер порта) представляет порт, назначенный в качестве корневого порта, при этом оставшийся порт по умолчанию выполняет роль альтернативного порта.

Таймеры



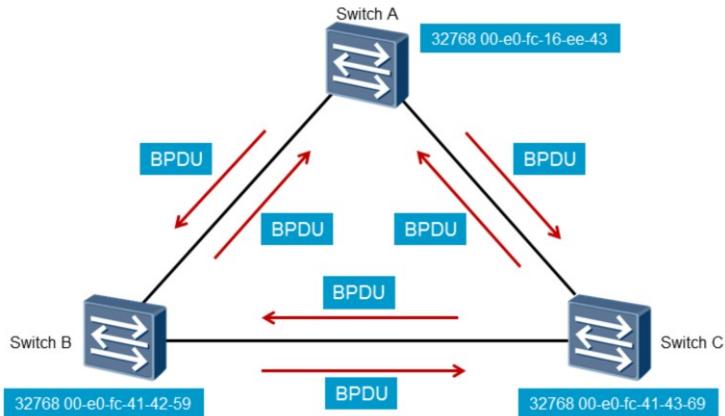
MAX Age представляет собой таймер старения BPDU. BPDU отбрасываются, когда Message Age превышает MAX Age.

Корневой мост отвечает за формирование BPDU конфигурации на основе интервала BPDU, который определяется таймером Hello. Таймер Hello по умолчанию представляет собой период в 2 секунды. Конвергентная сеть связующего дерева должна гарантировать, что в случае сбоя в сети, коммутаторам которого в сети с поддержкой STP, становится известно об ошибке. MAX Age таймер связан с каждым BDPU и представляет собой продолжительность жизни BPDU с точки зрения корневого моста и в конечном счете контролирует период действия BPDU, прежде чем он считается устаревшим. Таймер MAX Age по умолчанию представляет собой период в 20 секунд.

После того, как конфигурация BPDU получается от корневого моста, считается, что нисходящий коммутатору необходима приблизительно 1 секунда, чтобы генерировать новый BPDU и распространять сгенерированный BPDU ниже по потоку. Чтобы компенсировать это время, для каждого BPDU применяется значение возраста (MSG Age) для представления смещения между MAX Age и задержкой распространения, а для каждого переключателя это значение возрастает на 1.

Поскольку BPDU распространяются с корневого моста на нисходящие коммутаторы, обновляется таймер MAX Age. Таймер MAX Age подсчитывается и истекает, когда значение MAX Age превышает значение возраста сообщения, чтобы гарантировать, что время жизни BPDU ограничено возрастом MAX Age, как определено корневым мостом. В случае, если BPDU не принимается до истечения времени ожидания MAX Age, коммутатор будет рассматривать информацию BPDU, находящуюся в настоящее время как устаревшую, и предполагается, что произошел сбой сети STP.

Процесс выбора корня

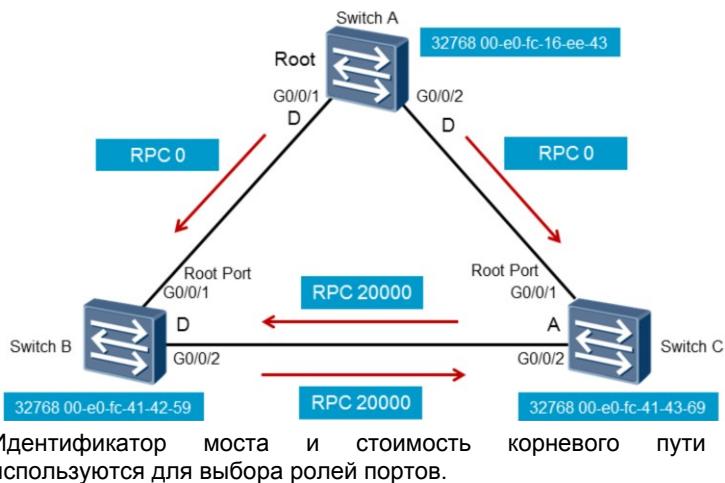


Все коммутаторы STP анонсируют BPDU для узлов с root статусом.

Процесс конвергенции связующего дерева - это автоматизированная процедура, которая начинается в момент запуска коммутатора. Все коммутаторы при запуске принимают на себя роль корневого моста в коммутационной сети. Поведение корневого моста по умолчанию заключается в назначении назначенной роли порта всем интерфейсам портов, чтобы включить пересылку BPDU через все подключенные интерфейсы портов. Поскольку BPDU принимаются пиринговыми коммутаторами, идентификатор моста будет сравнивать, чтобы определить, существует ли лучший кандидат на роль корневого моста. В случае, если полученный BPDU содержит идентификатор нижнего моста по отношению к корневому идентификатору, принимающий коммутатор будет продолжать анонсировать свою собственную BPDU конфигурацию для соседнего коммутатора.

Там, где BPDU вышеуказанный, коммутатор признает наличие лучшего кандидата для роли корневого моста, переставая распространять BPDU в направлении, из которого был получен старший BPDU. Коммутатор также изменит поле корневого идентификатора своего BPDU, чтобы объявить идентификатор моста корневого моста в качестве текущего нового корневого моста.

Процесс создания роли порта



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

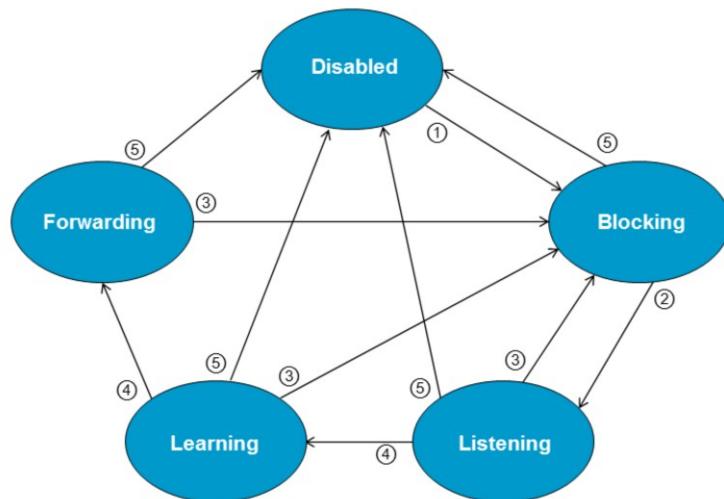
Page 17



Выбранный корневой мост, как только он будет установлен, будет генерировать конфигурацию BPDU для всех других некорневых коммутаторов. BPDU будет передавать стоимость корневого пути, которая будет информировать нисходящие коммутаторы о стоимости до корня, чтобы можно было определить самый короткий путь. Стоимость корневого пути, переносимая в BPDU, которая генерируется корневым мостом, всегда имеет значение 0. Затем принимающие нисходящие коммутаторы добавляют эту стоимость к стоимости пути интерфейсов портов, на которых был получен BPDU, и из которых коммутатор способен идентифицировать корневой порт.

В случае, когда равные затраты на корневой путь существуют на двух или более сегментах локальной сети для одного и того же восходящего коммутатора, идентификатор порта используется для обнаружения ролей портов. Если существует одинаковая стоимость корневого пути между двумя коммутаторами, как в данном примере, идентификатор моста используется для определения того, какой коммутатор представляет назначенный коммутатор для сегмента LAN. Если порт коммутатора не является ни корневым портом, ни назначенным портом, роль порта назначается как альтернативная.

Переход состояния порта



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 18



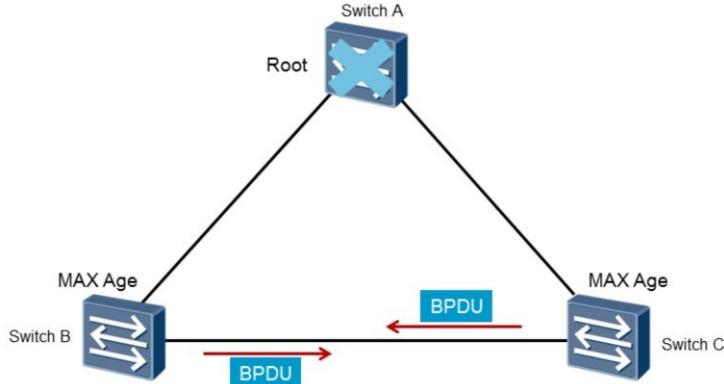
В рамках создания корневого моста и создания роли порта каждый коммутатор будет проходить через несколько переходов состояния порта. Любой отключенный административный порт будет считаться находящимся в отключенном состоянии. Включение порта в отключенном состоянии отобразит переход состояния в состояние блокировки ①.

Любой порт, который считается заблокированным, не может перенаправлять какой-либо пользовательский трафик, но способен принимать фреймы BPDU. Любой BPDU, полученный на интерфейсе порта в состоянии блокировки, не будет использоваться для заполнения таблицы MAC-адресов коммутатора, но вместо этого необходимо определить, необходим ли переход к состоянию прослушивания. Состояние прослушивания позволяет сообщать информацию BPDU после согласования роли порта в STP ②, но поддерживает ограничение на заполнение таблицы MAC-адресов информацией о соседе.

Переход в состояние блокировки из состояния прослушивания или других состояний может происходить в случае изменения порта на роль альтернативного порта. Переход между прослушиванием к обучению и обучению к следующим состояниям ④ в значительной степени зависит от таймера прямой задержки, который существует для обеспечения того, чтобы любое распространение информации BDPU всем коммутаторам в топологии оставшегося дерева достигалось до состояния перехода.

Состояние обучения поддерживает ограничение пересылки пользовательского трафика, чтобы гарантировать, что предотвращение любых петель переключения, однако, позволяет содержание таблицы MAC-адресов по всей топологии оставшегося дерева обеспечить стабильную коммутирующую сеть. После периода прямой задержки достигается состояние пересылки. Отключенное состояние применимо в любое время в течение переходного периода состояния посредством ручного вмешательства (т. е. Команды выключения) ⑤.

Корневая ошибка



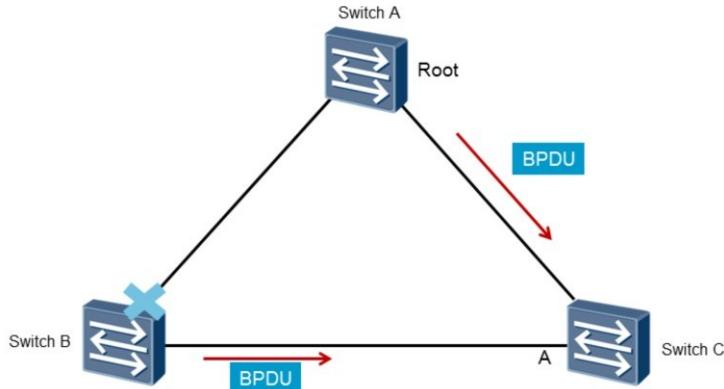
Некорневые мосты ждут MAX Age до того, как начнется потеря пакетов от корня.

Затем начинается процесс конвергенции, начиная с выбора корня.

События, которые вызывают изменение в установленной топологии связующего дерева, могут встречаться по-разному, для них протокол связующего дерева должен реагировать на быстрое восстановление устойчивой и свободной от петель топологии. Неисправность корневого моста является основным примером того, где требуется повторная конвергенция. Некорневые коммутаторы полагаются на прерывистый импульс BPDU от корневого моста для поддержки своих отдельных ролей в качестве некорневых коммутаторов в топологии STP. В случае отказа корневого моста переключатели нисходящего потока не смогут получить BPDU от корневого моста и, таким образом, также перестанут нисходящие распространять любой BPDU.

Таймер MAX Age обычно сбрасывается до установленного значения (по умолчанию 20 секунд) после нисходящего получения каждого BPDU. Однако с потерей любого BPDU, таймер MAX Age начинает отсчитывать время жизни для текущей информации BPDU каждого некорневого коммутатора на основе формулы ($\text{MAX Age} - \text{MSG Age}$). В тот момент, когда значение возраста MSG больше значения таймера MAX Age, информация BPDU, полученная от корня, становится недействительной, а некорневые коммутаторы начинают принимать на себя роль корневого моста. Конфигурация BPDU снова отправляется из всех активных интерфейсов в попытке обнаружить новый корневой мост. Сбой корневого моста вызывает длительность восстановления примерно 50 секунд из-за Max Age + 2x период конвергенции с обратной задержкой.

Сбой непрямой ссылки



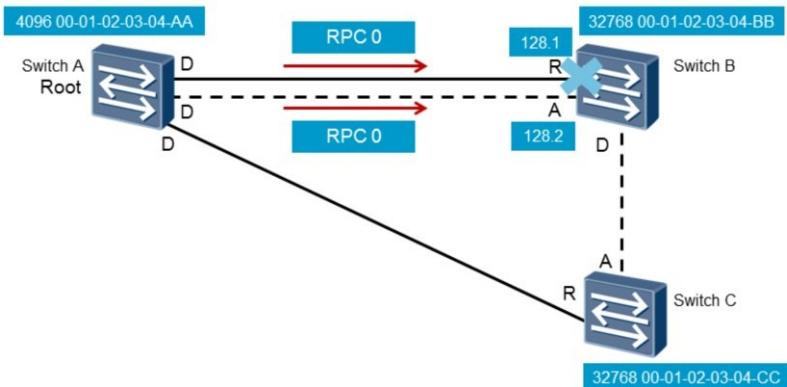
Коммутатор В начинает выборы корня, но BPDU игнорирует Коммутатор С. Пакеты BPDU распространяются до коммутатора В после истечения срока MAX Age.

В случае неисправности непрямой связи коммутатор теряет соединение с корневым мостом из-за отказа порта или носителя или, возможно, от ручного отключения интерфейса, действующего в качестве корневого порта. Сам коммутатор сразу же узнает об ошибке, и поскольку он получает только BPDU от корня в одном направлении, он будет немедленно начнет терять пакеты от корневого моста и утвердит свое положение в качестве нового корневого моста.

В этом примере коммутатор В начинает пересыпать BPDU для коммутатора С, чтобы изменить положение переключателя В как новый корневой мост, однако коммутатор С продолжает получать BPDU от исходного корневого моста и, следовательно, игнорирует любой BPDU из коммутатора В. Альтернативный порт начнет увеличивать свое состояние с помощью таймера MAX Age, поскольку интерфейс больше не получает BPDU, содержащий пакеты ID корневого моста.

По истечении таймера MAX Age коммутатор С изменит роль порта альтернативного порта на порт назначенного порта и перейдет к BPDU от корня к коммутатору В, что приведет к тому, что коммутатор уступит его утверждению в качестве корневого моста и изменит интерфейс порта к роли корневого порта. Это представляет собой частичный отказ топологии, однако из-за необходимости ждать периода, эквивалентного MAX Age + 2x прямой задержки, полное восстановление топологии STP требует приблизительно 50 секунд.

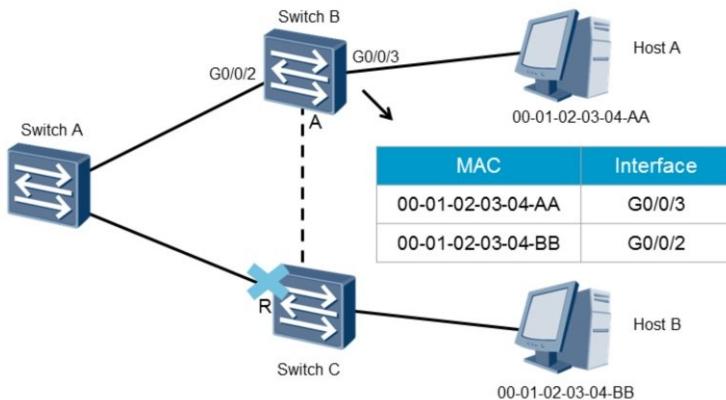
Сбой прямой ссылки



Переключатель В обнаруживает неисправность и переключает альтернативный порт на корневой порт.
STP конвергируется после двойной задержки (по умолчанию 30 секунд).

Окончательный сценарий, связанный с восстановлением конвергенции связующего дерева, происходит там, где несколько сегментов LAN подключены между двумя коммутационными устройствами, для которых в одна - активная ссылка, а другая - альтернативный путь к корню. Если произойдет событие, которое приводит к тому, что коммутатор, который принимает BPDU, обнаруживает потерю соединения на своем корневом порту, например, в случае возникновения сбоя корневого порта или сбоя связи, при котором ныходящий коммутатор немедленно понимает, что коммутатор может мгновенно перейти на альтернативный порт. Это начнет переход через состояния прослушивания, обучения и пересылки и достигнет восстановления в течение двойного перерыва. В случае какого-либо сбоя, когда ссылка, которая обеспечивает лучший путь, снова активируется, топология оставшегося дерева должна снова повторно конвергироваться, чтобы применить оптимальную топологию связующего дерева.

Топология изменения нестабильности MAC



Изменения топологии STP могут привести к аннулированию записей таблицы MAC.

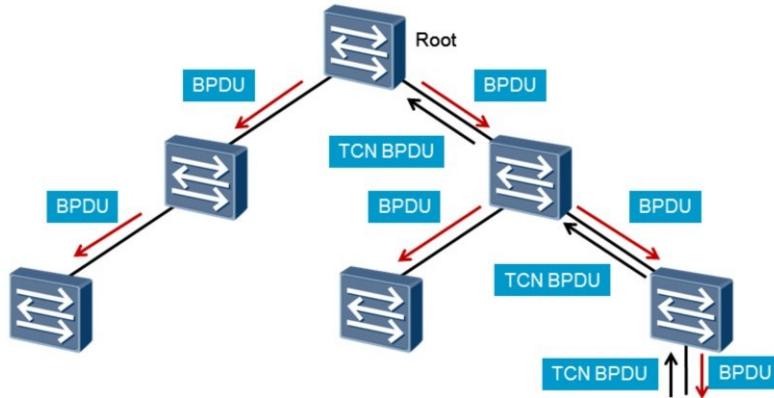
Записи таблицы MAC по умолчанию устаревают только через 300 секунд.

В конвергентной сети оставных сетей коммутаторы поддерживают базы данных фильтров или таблицы MAC-адресов для управления распространением кадров через топологию связующего дерева. Записи, которые обеспечивают связь между назначением MAC и интерфейсом порта пересылки, сохраняются по умолчанию на конечный период в 300 секунд (5 минут). Однако изменение топологии связующего дерева означает, что любые существующие записи таблицы MAC-адресов могут стать недействительными из-за изменения пути переключения и, следовательно, должны быть обновлены.

В этом примере демонстрируется существующая топология связующего дерева, для которой коммутатор В имеет записи, которые позволяют достичь хоста А через интерфейс Gigabit Ethernet 0/0/3 и хост В через интерфейс Gigabit Ethernet 0/0/2. Сбой моделируется на коммутаторе С, для которого текущий корневой порт стал неактивным. Эта ошибка приводит к перерасчету топологии оставного дерева для начала и, следовательно, активации избыточной связи между коммутатором С и коммутатором В.

Однако после повторной конвергенции обнаружено, что кадры от хоста А до хоста В не достигают цели. Поскольку записи таблицы MAC-адресов еще не истекают в соответствии с правилом 300 секунд, кадры, достигающие переключателя В, предназначенные для хоста В, продолжают пересыпаться через интерфейс порта Gigabit Ethernet 0/0/2 и эффективно становятся черными, когда кадры перенаправляются к неактивному интерфейсу порта коммутатора С.

Процесс изменения топологии



Уведомление об изменении топологии информирует корень об изменении топологии.

Root сбрасывает MAC-записи с использованием BPDU с установленным битом TC.

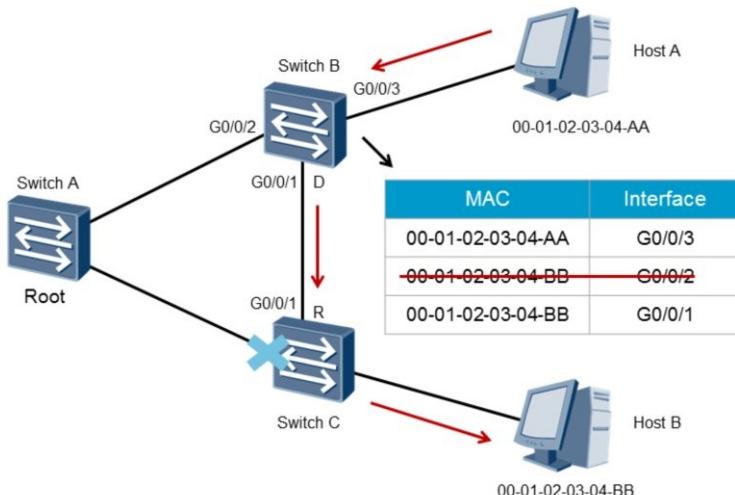
Должен быть введен дополнительный механизм для обработки периода времени ожидания интервала MAC-адресов, который приводит к недействительным вводам пути, которые поддерживаются после сближения связующего дерева. Внедренный процесс называется процессом уведомления об изменении топологии (TCN) и представляет новую форму BPDU для операции STP.

Этот новый BPDU называется BPDU TCN и отличается от исходного BPDU конфигурации STP посредством установки значения типа BPDU на 128 (0x80). Функция BPDU TCN заключается в информировании корневого моста восходящего потока о любом изменении текущей топологии, тем самым позволяя корню отправлять уведомление в BPDU конфигурации всем переключателям нисходящего потока, чтобы уменьшить период ожидания для записей таблицы MAC-адресов для эквивалента таймера прямой задержки или 15 секунд по умолчанию.

Поле флагов конфигурации BPDU содержит два поля для изменения топологии (TC) и подтверждения изменения топологии (TCA). После приема BPDU TCN корневой мост генерирует BPDU с установленными битами TC и TCA, чтобы соответственно уведомлять об изменении топологии и информировать нисходящие коммутаторы о том, что корневой мост получил BPDU TCN, и, следовательно, передача TCN BPDU должна прекратиться.

Бит TCA должен оставаться активным в течение периода, равного таймеру Hello (2 секунды), после чего конфигурация BPDU, генерируемая корневым мостом, будет поддерживать только бит TC на протяжении (MAX Age + forward delay) или 35 секунд на по умолчанию.

Обновление MAC при изменении топологии



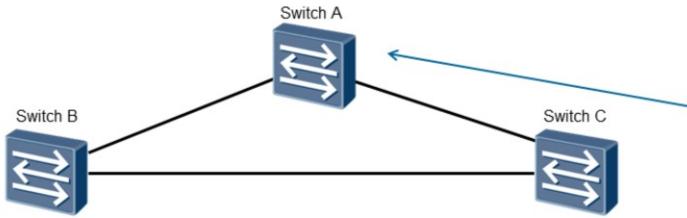
Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 24



Эффект BPDU TCN в процессе изменения топологии гарантирует, что корневой мост уведомляется о любом сбое в топологии связующего дерева, для которого корневой мост способен генерировать необходимые флаги, чтобы очистить текущие записи таблицы MAC-адресов в каждом из коммутаторов. В этом примере демонстрируются результаты процесса изменения топологии и влияние на таблицу MAC-адресов. Записи, относящиеся к коммутатору B, были сброшены, и были обнаружены новые обновленные записи, для которых определено, что хост B теперь доступен через интерфейс порта Gigabit Ethernet 0/0/1.

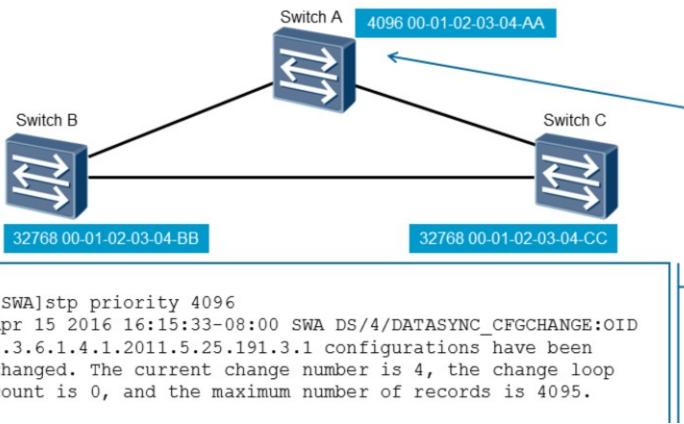
Режимы STP



```
[SWA]stp mode ?
mstp  Multiple Spanning Tree Protocol (MSTP) mode
rstp  Rapid Spanning Tree Protocol (RSTP) mode
stp   Spanning Tree Protocol (STP) mode
[SWA]stp mode stp
```

Коммутаторы серии Huawei Sx7, к которым принадлежит модель серии S5700, способны поддерживать три формы STP. Используя команду режима stp, пользователь может определить режим STP, который должен применяться к отдельному коммутатору. Режим STP по умолчанию для коммутаторов серии Sx7 - это MSTP, и поэтому его необходимо перенастроить до использования STP.

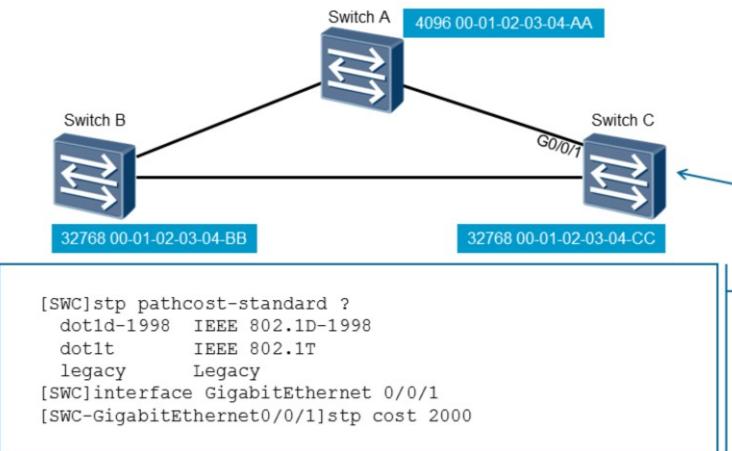
Назначение корня



Корень может быть установлен вручную или путем определения коммутатора как основного.

В рамках хорошей практики проектирования коммутаторов рекомендуется вручную определить корневой мост. Позиционирование корневого моста обеспечивает оптимальный путь потока трафика внутри корпоративной сети путем настройки значения приоритета моста для STP. Команда `stp priority [priority]` может использоваться для определения значения приоритета, где приоритет относится к целочисленному значению от 0 до 61440, назначается с шагом 4096. Это позволяет в общей сложности 16 приращений со значением по умолчанию 32768. Также можно назначить корневой мост для связующего дерева через основную команду `stp root primary`.

Назначение стоимости пути



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 27

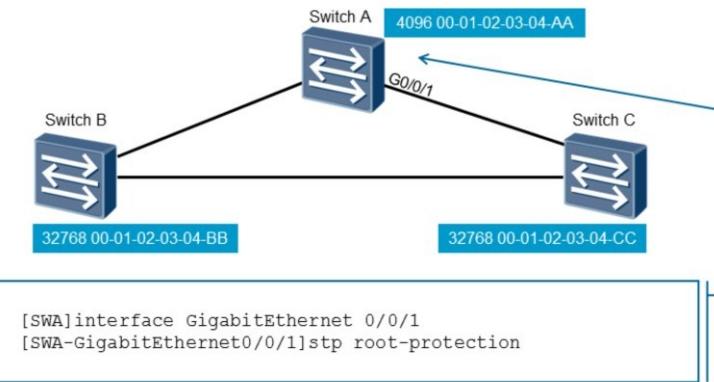


Понятно, что коммутаторы серии Huawei Sx7 поддерживают три стандартные формы стоимости пути, чтобы обеспечить совместимость там, где это необходимо, однако по умолчанию поддерживает стандарт стоимости пути 802.1t. Стандарт стоимости пути может быть скорректирован для данного коммутатора с использованием *stpc pathcost-standard {dot1d-1998 | dot1t | legacy}*, где dot1d-1998, dot1t и legacy отсылает к стандартам стоимости пути, описанным ранее в этом разделе.

Кроме того, стоимость пути для каждого интерфейса также может быть назначена вручную с помощью средств детальной манипуляции с стоимостью пути stpc. Этот метод манипулирования стоимостью пути следует использовать с большой осторожностью, однако, поскольку стандарты стоимости пути предназначены для реализации оптимальной топологии связующего дерева для данной коммутирующей сети, а манипулирование стоимостью stpc может привести к формированию предоптимального связующего дерева топологии.

Используется команда *stpc cost [cost]*, для которой значение стоимости должно соответствовать диапазону, определенному стандартом стоимости пути. Если используется стандарт Huawei, стоимость маршрута колеблется от 1 до 200000. Если используется стандарт IEEE 802.1D, стоимость маршрута колеблется от 1 до 65535. Если используется стандарт IEEE 802.1t, стоимость пути колеблется от 1 до 200000000.

Защита корня



Защита корня предотвращает изменения топологии в результате перехода корневого моста, вызванный получением BPDU с более высоким приоритетом.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 28



Если корневой коммутатор в сети неправильно настроен или атакован, он может получить BPDU с более высоким приоритетом, и, таким образом, корневой коммутатор становится не-корневым коммутатором, что вызывает изменение топологии сети. В результате трафик может быть переключен с высокоскоростных каналов на низкоскоростные линии связи, что приводит к перегрузке сети.

Чтобы решить эту проблему, коммутатор предоставляет функцию защиты корня. Функция защиты корня защищает роль корневого коммутатора, сохраняя роль назначенного порта. Когда порт получает BPDU с более высоким приоритетом, порт останавливает пересылку пакетов и переходит в состояние прослушивания, но он по-прежнему сохраняет назначенную роль порта. Если порт не получает BPDU с более высоким приоритетом в течение определенного периода времени, статус порта восстанавливается из состояния прослушивания.

Сконфигурированная корневая защита действительна только тогда, когда порт является назначенным портом, а порт сохраняет роль. Если порт сконфигурирован как граничный порт или если на порту включена команда, известная как защита от петель, в порт не может быть включена защита корня.

Подтверждение конфигурации

```
[SWA]display stp
-----[CIST Global Info] [Mode STP]-----
CIST Bridge      :4096 .00-01-02-03-04-BB
Bridge Times     :Hello 2s MaxAge 20s Fwdly 15s MaxHop 20
CIST Root/ERPC   :4096 .00-01-02-03-04-BB / 0
CIST RegRoot/IRPC :4096 .00-01-02-03-04-BB / 0
CIST RootPortId  :0.0
BPDU-Protection   :Disabled
TC or TCN received :37
TC count per hello :0
STP Converge Mode :Normal
Share region-configuration :Enabled
Time since last TC  :0 days 0h:1m:29s
.....
```

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 29



Используя команду *stp display*, можно определить текущую конфигурацию STP. Существует множество таймеров для управления конвергенцией связующего дерева, включая таймер hello, max age таймер и forward задержку, для которых отображаемые значения представляют собой настройки таймера по умолчанию, и их рекомендуется поддерживать.

Текущий идентификатор моста может быть идентифицирован для данного коммутатора через конфигурацию Bridge CIST, состоящий из идентификатора моста и MAC-адреса коммутатора. Статистика предоставляет информацию о том, произвел ли коммутатор изменения топологии, через полученное значение TC или TCN вместе с последним входом во время, начиная с момента последней записи TC.

Подтверждение конфигурации

```
[SWA]display stp
-----
-----[Port1(GigabitEthernet0/0/1)] [FORWARDING]-----
Port Protocol      :Enabled
Port Role          :Designated Port
Port Priority      :128
Port Cost(Dot1T)   :Config=2000 / Active=2000
Designated Bridge/Port :4096.00-01-02-03-04-BB / 128.1
Port Edged         :Config=default / Active=disabled
Point-to-point     :Config=auto / Active=true
Transit Limit      :147 packets/hello-time
Protection Type    :Root
-----
```

Для отдельных интерфейсов на коммутаторе можно отобразить эту информацию с помощью команды *display stp*, чтобы отобразить все интерфейсы или использовать команду *display stp interface <interface>* для определения конкретного интерфейса. Состояние интерфейса соответствует состояниям портов MSTP и поэтому будет отображаться как Discarding, Learning or Forwarding. Также отображаются другие допустимые данные, такие как роль порта и стоимость порта, а также все применяемые механизмы защиты.



Итог

- В случае, если корневой мост (коммутатор) временно не работает в STP сети, следующий рабочий коммутатор станет корневым мостом. Что произойдет, как только не рабочий корневой мост снова станет активным?
- В чем разница между стоимостью пути и стоимостью корневого пути?

1. После отказа корневого моста для сети оставшегося дерева, следующий лучший кандидат будет избран в качестве корневого моста. В случае, если исходный корневой мост снова станет активным в сети, процесс выборов на место корневого моста будет происходить еще раз. Это эффективно приводит к простоям в коммутационной сети по мере того, как происходит конвергенция.
2. Стоимость корневого пути - это стоимость, связанная с возвратом пути к корневому мосту, тогда как стоимость пути это только часть стоимости корневого пути.



Thank you

www.huawei.com

Быстрый протокол разворачивающегося
дерева (RSTP)

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

Оригинальный STP (протокол распределенного связующего дерева) стандарт был определен в 1998 году для которых был обнаружен ряд ограничений, особенно в течение времени, необходимого конвергенции (объединение нескольких услуг в одной). В свете этого, был представлен RSTP (Rapid Spanning Tree Protocol – быстрый протокол разворачивающегося дерева). Основные характеристики RSTP соответствуют STP, а различия рассмотрены в этой главе.

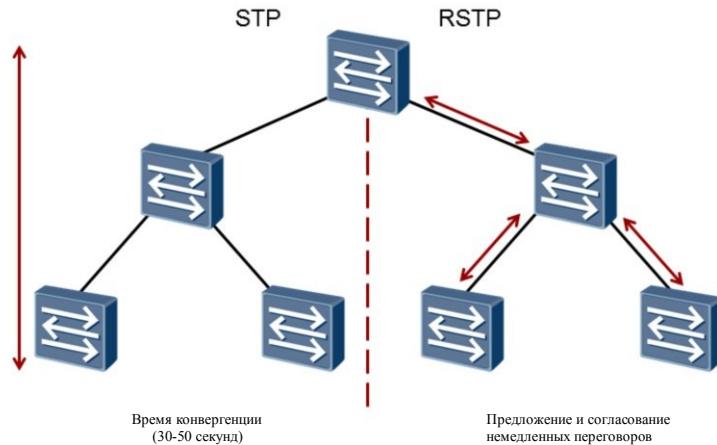


Цели

После завершения этой главы вы сможете:

- Описать характеристики, связанные с RSTP
- Конфигурировать RSTP параметры

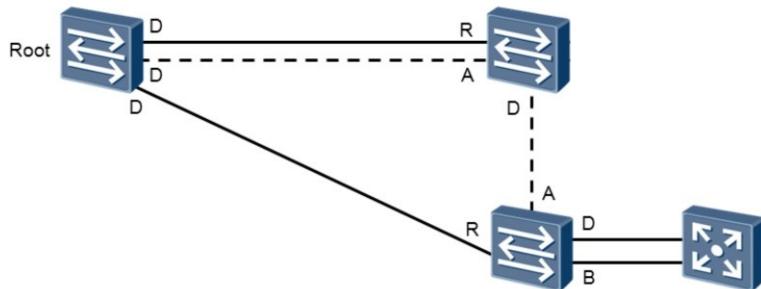
Недостатки STP



STP обеспечивает сеть без петли, но имеет медленную скорость конвергенции топологии сети, что приводит к ухудшению обслуживания. Если сетевая топология часто меняется, соединения в сети, поддерживающей STP, часто срываются, что приводит к регулярному прерыванию обслуживания.

RSTP использует процесс предложения и согласования, который позволяет немедленно согласовывать ссылки, эффективно удаляя время, затрачиваемое на конвергенцию, до истечения срока действия, прежде чем может произойти конвергенция связующего дерева. Процесс предложения и соглашения имеет тенденцию следовать каскадному эффекту от точки корневого моста через коммутационную сеть, так как каждый нисходящий коммутатор начинает изучать истинный корневой мост и путь, через который может быть достигнут корневой мост.

RSTP роли портов



Roles	Description
Backup	Резервное копирование на нижестоящие узлы, где избыточные ссылки существуют на том же LAN сегменте, что и указанный порт
Alternate	Альтернативный путь к корневому мосту, который отличается от пути, обеспеченным корневым портом коммутатора.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

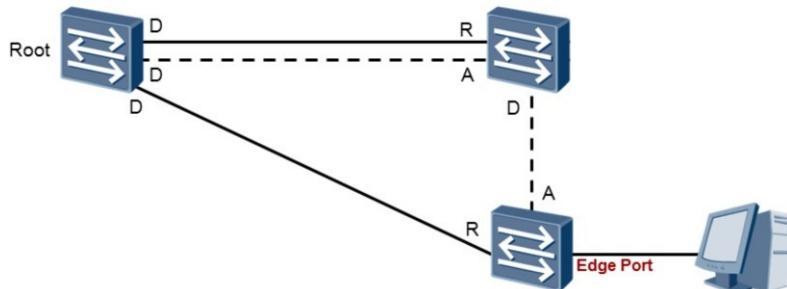
Page 5



Коммутаторы, работающие в режиме RSTP, реализуют две отдельные роли портов для резервирования. Альтернативный порт представляет собой дополнительный путь к корневому мосту в случае отказа текущего пути к корневому мосту. Роль резервного порта представляет собой резервную копию пути для сегмента LAN в направлении, ведущем от корневого моста. Понятно, что backup порт представляет собой способ обеспечения избыточности назначеннной роли порта аналогичным способом, что и альтернативный порт обеспечивает способ резервирования корневого порта.

Роль резервного порта может существовать там, где коммутатор имеет два или более подключений к совместно используемому медиаустройству, или где используется одна связь точка-точка для создания физического соединения с обратной связью между портами на таком же коммутаторе. Однако в обоих случаях принцип резервного порта, существующий, когда два или более портов на одном коммутаторе подключаются к одному сегменту LAN, по-прежнему применяется.

RSTP Границные порты



- Системы, которые не принимают участие в RSTP соединении к граничным портам
- Границные порты не принимают BPDU и могут немедленно передавать данные

В RSTP назначенный порт на границе сети называется граничным портом. Граничный порт напрямую подключается к терминалу и не подключается к каким-либо другим коммутационным устройствам. Граничный порт не получает конфигурацию BPDU, поэтому он не участвует в расчете RSTP.

Он может напрямую переключиться из состояния «Отключено» в состояние «Пересылка» без каких-либо задержек, точно так же, как порт, не совместимый с STP. Если пограничный порт получает ложную конфигурацию BPDU от злоумышленников, он лишен атрибутов пограничного порта и становится общим STP-портом. Расчет STP выполняется снова, что приводит к разрыву сети.

RSTP Состояния портов

STP	RSTP	Port Role
Disabled	Discarding	Disabled
Blocking	Discarding	Alternate or Backup
Listening	Discarding	Root or Designated
Learning	Learning	Root or Designated
Forwarding	Forwarding	Root or Designated

RSTP вводит изменения в состояния портов, которые упрощаются от пяти до трех типов. Эти типы портов основаны на том, отправляет ли порт пользовательский трафик и узнает MAC-адреса. Если порт не перенаправляет пользовательский трафик и не узнает MAC-адреса, порт находится в состоянии «Сбрасывание» (Discarding). Порт считается находящимся в состоянии «Обучения» (Learning), когда порт не передает пользовательский трафик, но узнает MAC-адреса. Наконец, когда порт перенаправляет пользовательский трафик и узнает MAC-адреса, порт, как говорят, находится в состоянии «Пересылки» (Forwarding).

a

RST BPDU

PID	PVI	BPDU Type	Flags	Root ID	RPC	Bridge ID	Port ID	Message Age	Max Age	Hello Time	Fwd Delay
-----	-----	-----------	-------	---------	-----	-----------	---------	-------------	---------	------------	-----------

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
TCA	Agreement	Forwarding	Learning	Port Role	Proposal	TC	

PortRole = 00	Unknown
01	Alternate/Backup Port
10	Root Port
11	Designated Port

- Неиспользованные поля STP BPDU активны в RSTP.
- Новые возможности вводятся как часть RSPT.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

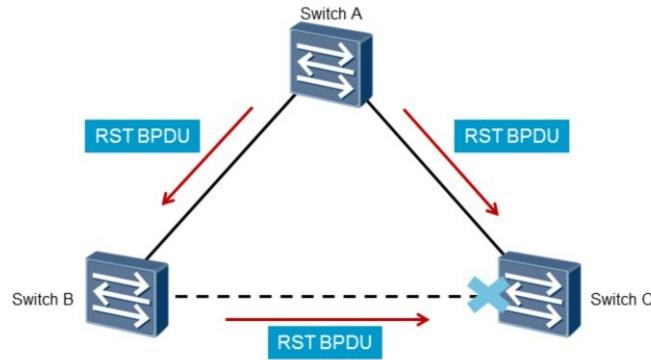
Page 8



Формат BPDU, используемый в STP, также применяется к RSTP с отклонениями в некоторых из общих параметров. Чтобы отличать BPDU конфигурации STP от BPDU Rapid Spanning Tree, известным как RST BPDU, определяется тип BPDU. STP определяет тип BPDU конфигурации 0 (0x00) и Topology Change Notification BPDU (TCN BPDU) 128 (0x80), BPDU RST идентифицируются значением типа BPDU = 2 (0x02). В поле флагов RST BPDU для полей BPDU назначаются дополнительные обозначения параметров.

В поле флагов в STP реализовало только использование Topology Change (TC) и Acknowledgement (TCA) как часть процесса Topology Change, в то время как другие поля были зарезервированы. RST BPDU принял эти поля для поддержки новых параметров. К ним относятся флаги, указывающие процесс предложения и соглашения, используемый RSTP для быстрой конвергенции, определения роли порта и состояния порта.

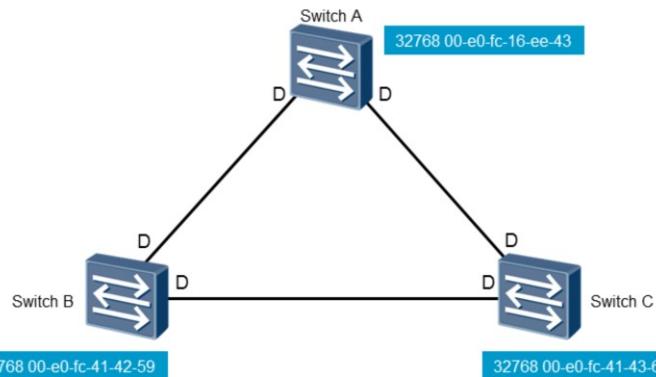
RST BPDU



- Спроектированные коммутаторы генерируют собственный BPDU в Hello time, независимо от того, получен ли RST BPDU

В STP после того, как топология станет стабильной, корневой мост отправляет конфигурацию BPDU с интервалом, заданным Hello time. Мост без полномочий root не отправляет конфигурацию BPDU до тех пор, пока не получит конфигурацию BPDU, отправленную с восходящего устройства. Это делает расчет STP сложным и трудоемким. В RSTP после того, как топология становится стабильной, корневой модуль отправляет конфигурацию BPDU по Hello intervals, независимо от того, получила ли она конфигурацию BPDU, отправленную с корневого моста; такие операции выполняются на каждом устройстве независимо.

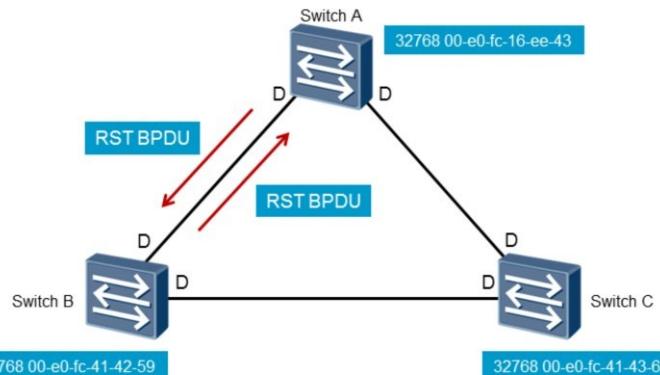
RSTP Конвергенция



- Все RSTP коммутаторы начинают свою работы как корневые и отправляют RST BPDU
- Порты установлены в назначеннюю роль и статус Discarding

Конвергенция RSTP следует некоторым основным принципам STP при определении того, что все коммутаторы при инициализации утверждают роль корневого моста и, таким образом, назначают каждому порту интерфейс с назначенной ролью порта. Однако состояние порта настроено на состояние Discarding до тех пор, пока мириングовые коммутаторы не смогут подтвердить состояние ссылки.

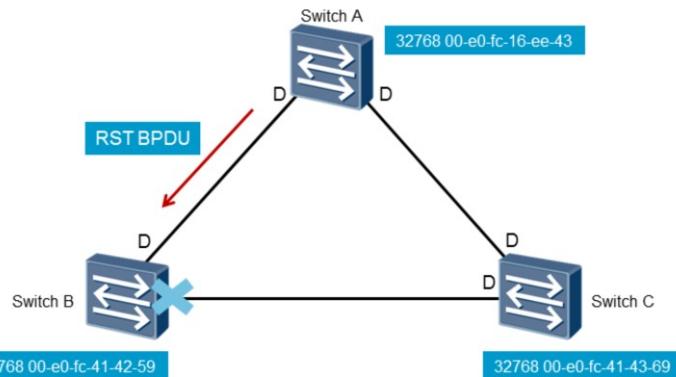
RST BPDU Предложения



- Предложения отправляются в RST BPDU во время выбора корневого порта
- Коммутатор будет игнорировать предложения, если имеет лучший bridge ID.

Каждый коммутатор, являющийся корневым мостом, будет согласовывать состояния портов для данного сегмента локальной сети, генерируя BPDU RST с предложенным набором бит, установленным в поле flags. Когда порт получает BPDU RST от вышеописанного моста, порт сравнивает полученный RST BPDU со своим RST BPDU. Если его собственный RST BPDU превосходит полученный, порт сбрасывает полученный RST BPDU и сразу же реагирует на пиринговое устройство собственным RST BPDU, которое включает в себя набор предложенных бит.

RSTP Процесс синхронизации

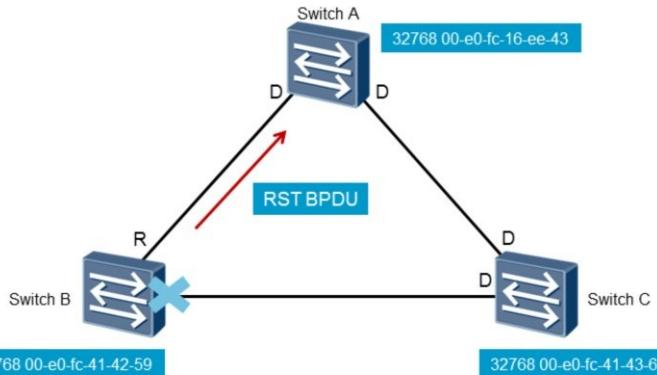


- После получения превосходящего BPDU, коммутатор В прекратит отправку RST BPDU содержащиеся предложения, и начнет синхронизировать

Поскольку таймеры не играют роли в большинстве процессов конвергенции топологии RSTP, найденных с помощью STP, важно, чтобы возможность для переключения циклов во время согласования роли порта была ограничена. Это управляется реализацией процесса синхронизации, который определяет, что после получения превосходящего BPDU, содержащего предложенные биты, принимающий коммутатор должен установить все последующие назначенные порты на Discarding, как часть процесса синхронизации.

Если нисходящий порт является альтернативным портом или граничным портом, статус роли порта остается неизменным. В этом примере демонстрируется временный переход назначенного порта в сегменте локальной сети вниз по отношению к состоянию отбрасывания и, следовательно, блокирование любой пересылки фреймов во время предшествующего предложения и процесса согласования.

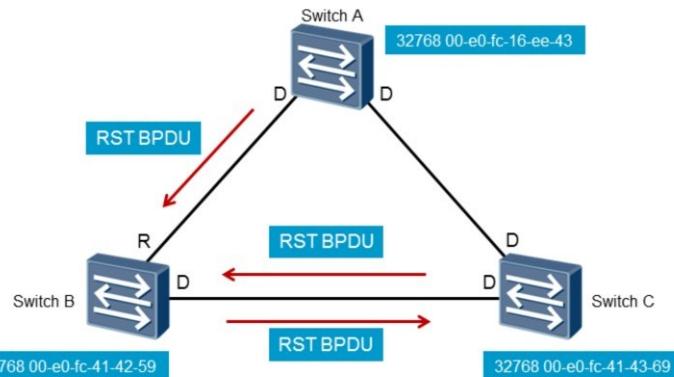
RST BPDU Соглашение



- После того, как все нижепоточные неграничные назначенные порты будут заблокированы, коммутатор В будет отправлять соглашение с RST BPDU.

Подтвержденный переход нисходящего назначенного порта в состояние Discarding позволяет отправлять BPDU RST в ответ на предложение, отправленное коммутатором восходящего потока. На этом этапе роль порта интерфейса была определена как корневой порт, поэтому флаг согласования и корневая роль порта установлены в поле флагов RST BPDU, которое возвращается в ответ на предложение.

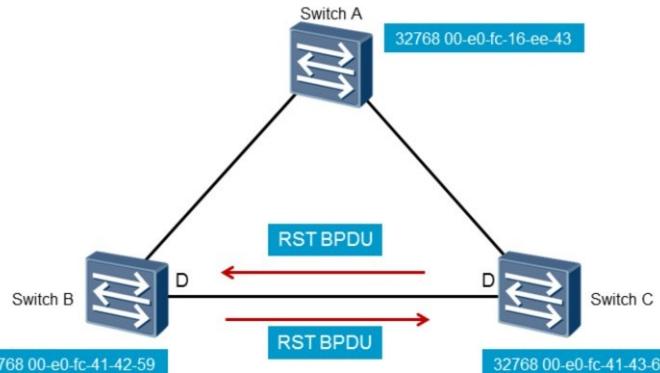
RSTP Конвергентная ссылка



- Нижепоточный порт снова разблокирован, и начался новый круг синхронизации между коммутаторами В и С.

На заключительном этапе процесса предложения и соглашения RST BPDU, содержащий бит соглашения, принимается переключателем восходящего потока, позволяя назначенному порту немедленно перейти из состояния Discarding в состояние Forwarding. После этого сегмент (ы) по нисходящей LAN начнет согласовывать портовые порты интерфейсов, используя тот же процесс предложения и соглашения.

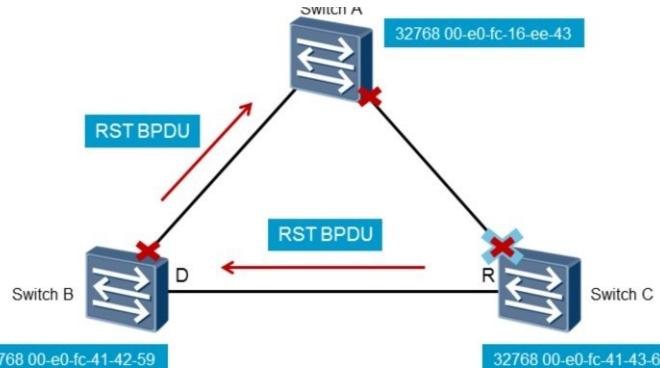
Ошибка соединения/корня



- Потеря восходящего RST BPDU сигнала из-за ошибок соединения/устройства
- Произойдет конвергенция, основанная на предложении и соглашении

В STP устройству приходится ждать период Max Age до определения ошибки согласования. В RSTP, если порт не получает конфигурационные BPDU, отправленные из восходящего устройства в течение трех последовательных интервалов Hello, связь между локальным устройством и его одноранговым узлом завершается с ошибкой, в результате чего процесс предложения и соглашения должен быть инициализирован, чтобы обозначить роли порта для сегмента LAN.

Процесс изменения топологии



- Во время отправки соглашения, адреса удаляются для всех портов, за исключением порта, на который был получен RST BPDU

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 16

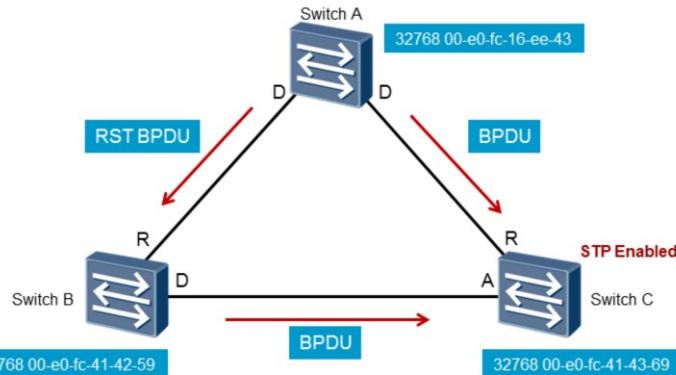


Изменения топологии влияют на RSTP аналогично тому, как влияет STP, однако между ними существуют некоторые незначительные различия. В этом примере на коммутаторе С произошел сбой связи. Коммутатор А и коммутатор С немедленно обнаружат сбой связи и очистят записи адресов для портов, подключенных к этой ссылке. RST BPDU начнет согласование с состоянием порта в рамках процесса предложения и соглашения, после чего будет происходить уведомление об изменении топологии вместе с пересылкой RST BPDU, содержащей соглашение.

Этот RST BPDU будет иметь как бит соглашения, так и бит TC, установленный в 1, для информирования коммутаторов восходящего потока о необходимости сбросить свои MAC-адреса на всех интерфейсах портов, кроме интерфейса порта, на котором был получен RST BPDU, содержащий установленный бит TC.

Бит TC будет установлен в периодически отправленном RST BPDU и перенаправлен вверх по потоку в течение периода, эквивалентного Hello Time + 1 секунде, в течение которого все соответствующие интерфейсы будут сброшены и должны будут повторно заполнять записи MAC на основе новой топологии RSTP. Красный (темный) «х» в примере подчеркивает, какие интерфейсы будут сброшены в результате изменения топологии.

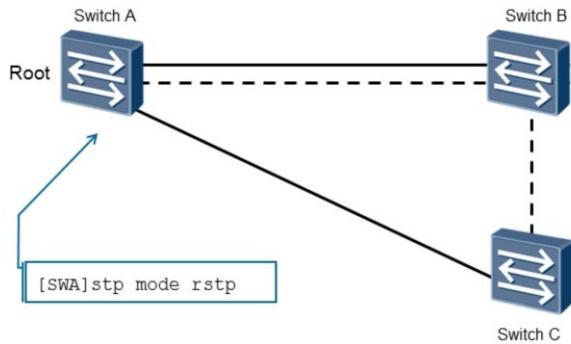
STP Взаимодействие



- Порты RSTP коммутатора будут возвращаться к STP, когда соединится с LAN сегментом, содержащим STP включенное устройство.

Реализация STP в топологии коммутации на основе RSTP возможна, однако не рекомендуется, поскольку любое ограничение, относящееся к STP, становится очевидным в пределах диапазона связи коммутатора STP. Порт, участвующий в процессах согласования для определения своей роли в STP, должен ждать до 50 секунд, прежде чем конвергенция может быть завершена, так как преимущества RSTP теряются.

Настройка режима



- *Stp mode rstp* – команда, разрешающая всем портам коммутатора генерировать RST BPDU.

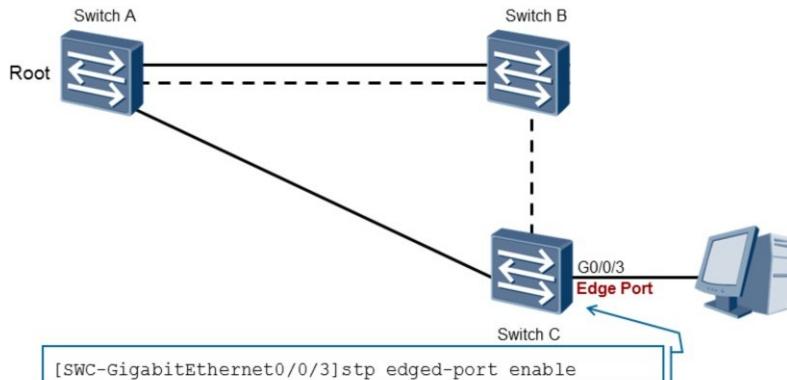
Конфигурация режима связующего дерева коммутаторов Sx7 требует, чтобы команда режима *stp* использовалась для установки режима в RSTP. При этом коммутатор серии Sx7 будет генерировать RST BPDU по отношению к RSTP, в отличие от других реализаций spanning tree. Эта команда настроена из системного представления и должна применяться ко всем коммутаторам, участвующим в топологии быстрого связующего дерева.

Проверка конфигурации

```
[SWA]display stp
-----[CIST Global Info] [Mode RSTP]-----
CIST Bridge      :32768.00-e0-fc-16-ee-43
Bridge Times     :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC   :32768.00-e0-fc-16-ee-43 / 0
CIST RegRoot/IRPC :32768.00-e0-fc-16-ee-43 / 0
CIST RootPortId  :0.0
BPDU-Protection   :Disabled
TC or TCN received :37
TC count per hello :0
STP Converge Mode :Normal
Share region-configuration :Enabled
Time since last TC  :0 days 0h:14m:43s
```

Команда `stp display` предоставляют относительную информацию о конфигурации RSTP, так как многие из параметров соответствуют основной архитектуре STP. Информация о режиме определит, работает ли переключатель в настоящий момент с использованием RSTP.

Установка граничного порта



- Разрешает использование граничного порта для передачи без задержки
- Интерфейсы на S5700 без граничных портов по умолчанию

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

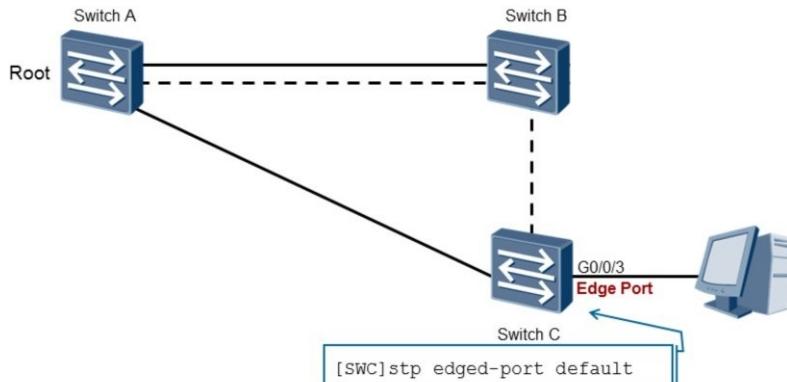
Page 20



Граничный интерфейс определяет порт, который не участвует в топологии связующего дерева. Эти интерфейсы используются конечными системами для подключения к коммутационной сети с целью пересылки кадров. Поскольку для таких конечных систем не требуется согласовывать состояние интерфейса порта, предпочтительно, чтобы порт был перенесен непосредственно в состояние пересылки, чтобы позволить пересылать фреймы через этот интерфейс.

Команда `enable stp edged-port enable` используется для переключения порта, чтобы он стал граничным портом, так как все порты по умолчанию не являются граничными. Чтобы отключить граничный порт, используется команда отключения `stp edged-port`. Эти команды применяются только к одному интерфейсу порта на данном коммутаторе. Важно отметить, что поведение граничного порта связано с RSTP, как определено в документации по стандартам IEEE 802.1D-2004, однако из-за специфического приложения VRP базового конечного автомата RSTP на STP (что также приводит к состояниям портов RSTP представленных в STP), также можно применить настройки граничного порта RSTP к STP в продуктах серии Huawei Sx7.

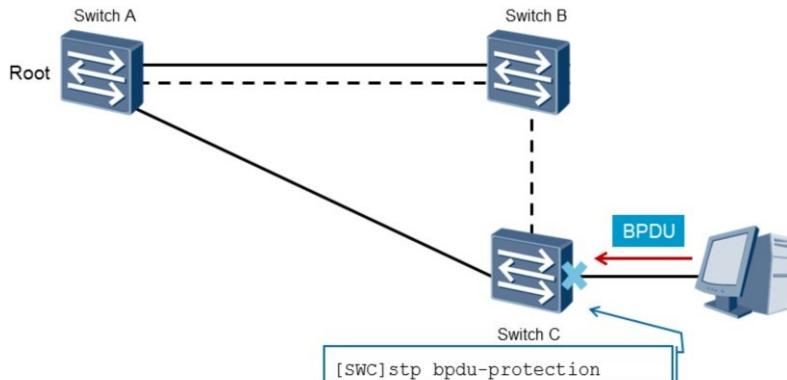
Установка граничного порта



- Все порты на коммутаторе будут сконфигурированы как граничные порты.
- Следует соблюдать осторожность с этой командой чтобы избежать STP зацикливаний.

В случае, когда несколько портов на коммутаторе должны быть настроены как граничные порты, применяется стандартная команда `stp edged-port default`, которая устанавливает все интерфейсы портов на коммутаторе граничными портами. Важно запустить команду отключения `stp edged-port disable` на портах, которые должны участвовать в вычислении STP между устройствами, чтобы избежать возможных циклов, которые могут быть вызваны в результате расчетов топологии STP.

BPDU Защита



- Защита BPDU предотвращает вредоносную инъекцию BPDU в RSTP

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

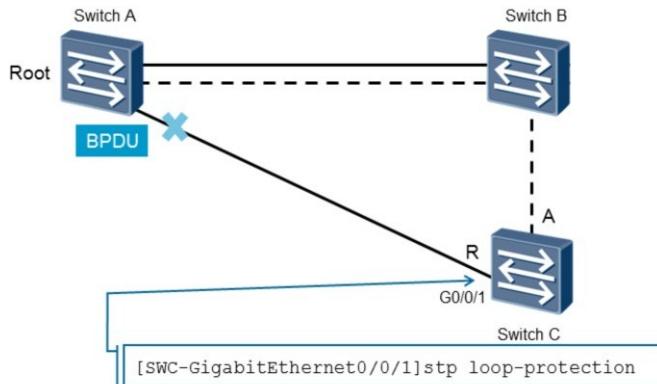
Page 22



Порт, который напрямую подключен к пользовательскому терминалу, например ПК или файловому серверу, понимается как настраиваемый граничный порт для обеспечения быстрого перехода статусов порта. Как правило, ни один BPDU не отправляется на пограничные порты, однако, если коммутатор атакован псевдо BPDU, коммутатор устанавливает граничные порты в качестве портов не граничных. После того, как эти граничные порты получают BPDU, топология связующего дерева пересчитывается, и в результате происходит зависание сети.

Для защиты от псевдо-BPDU-атак, RSTP обеспечивает защиту BPDU. После того, как включена защита BPDU, коммутатор отключает граничный порт, который получает BPDU и информирует любую активную станцию управления сетью (NMS). Резервные порты, которые выключаются коммутатором, могут запускаться вручную только администратором сети. Команда `stp bpdu-protection` должна использоваться для включения защиты BPDU и настроена глобально в системном представлении.

Защита от петель



- Если BPDU не может быть принят нисходящим коммутатором, корневой порт блокируется, чтобы предотвратить появление петель коммютирования.

Коммутатор поддерживает состояние корневого порта и заблокированных портов, постоянно получая BPDU от восходящего коммутатора. Если корневой коммутатор не может получить BPDU от восходящего коммутатора из-за перегрузки канала или сбоя односторонней линии, коммутатор повторно выбирает корневой порт. Предыдущий корневой порт затем становится назначенным портом, и заблокированные порты изменяются в состояние пересылки. В результате в сети могут возникать петли.

Коммутатор обеспечивает защиту контура для предотвращения сетевых циклов. После того, как функция защиты цикла включена, корневой порт блокируется, если он не может принимать BPDU от восходящего коммутатора. Блокированный порт остается в заблокированном состоянии и не передает пакеты. Это предотвращает появление петель в сети. Если интерфейс сконфигурирован как граничный интерфейс или на интерфейсе включена защита от root, защита контура не может быть включена на интерфейсе. Для включения этой функции в интерфейсе-представлении должна применяться команда *stp loop-protection*.

Проверка конфигурации

```
[SWC]display stp interface GigabitEthernet 0/0/1
----[CIST][Port1(GigabitEthernet0/0/1)][FORWARDING]----
  Port Protocol      :Enabled
  Port Role          :Root Port
  Port Priority      :128
  Port Cost(Dot1T )  :Config=auto / Active=20000
  Designated Bridge/Port :32768.00-e0-fc-16-ee-43 / 128.1
  Port Edged         :Config=default / Active=disabled
  Point-to-point     :Config=auto / Active=true
  Transit Limit      :147 packets/Hello-time
  Protection Type    :Loop
  Port STP Mode      :RSTP
  Port Protocol Type :Config=auto / Active=dot1s
  BPDU Encapsulation :Config=stp / Active=stp
  ....
```

Проверка конфигурации RSTP для данного интерфейса достигается с помощью команды *display stp interface <interface>*. Соответствующая информация идентифицирует состояние порта интерфейса как Discarding, Learning or Forwarding. Определяется соответствующая информация для интерфейса порта, включая приоритет порта, стоимость порта, состояние порта в качестве граничного порта или поддерживающее двухточечное соединение и т. д.



Итог

- Какова цель синхронизации, которая возникает во время процессов RSTP предложения и согласования?

1. Синхронизация является этапом процесса конвергенции, который включает в себя блокирование назначенных портов, в то время как RST BPDU передает сообщения предложения и согласования для конвергенции сегмента коммутатора. Этот процесс предназначен для обеспечения согласованности всех интерфейсов с их ролями портов, для гарантии того, что петли коммутации не будут выполняться после того, как назначенный порт для любого нисходящего коммутатора будет разблокирован.



Thank you

www.huawei.com

Базовые знания IP-маршрутизации

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

Пересылка кадров и коммутация ввели уровень канала передачи данных операций и, в частности, роль стандарта IEEE 802 в качестве поддерживающий основной механизм связи, в котором, как правило, функционируют комплекты протоколов на верхнем уровне. С внедрением маршрутизации устанавливаются процессы, которые определяют протоколы верхнего уровня и межсетевую связь. Домен корпоративной сети обычно состоит из нескольких сетей, для управления которыми необходимо использовать оптимальные маршруты для пересылки IP-пакетов (или дейтаграмм) предназначенных для сетевых целей. В этом разделе представлены основы, на которых основана такая IP-маршрутизация.

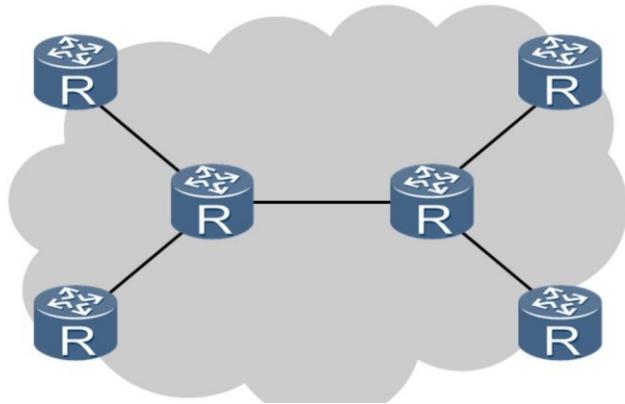


Цели

По завершении этого раздела вы узнаете:

- Принципы, которые управляют решениями IP-адресации.
- Основные требования к пересылке пакетов.

Автономные системы

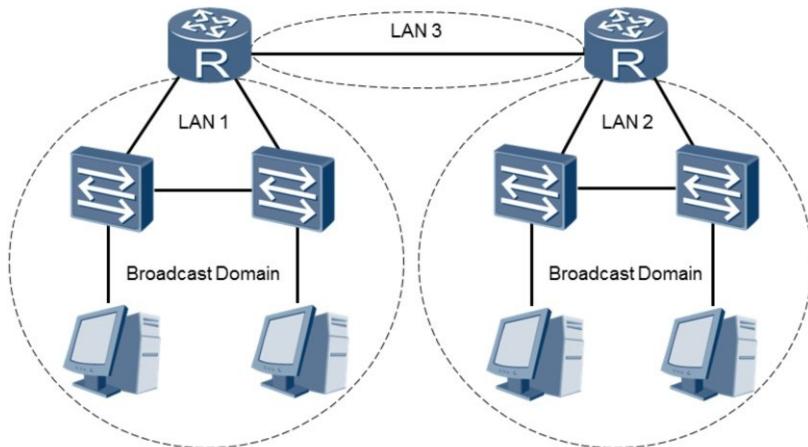


- IP-сеть или сети, контролируемые одним или несколькими операторами с четкой политикой, которая определяет, как принимаются решения о маршрутизации.

Корпоративная сеть обычно понимается как экземпляр автономной системы. Как определено в RFC 1030, автономная система или AS, как она также широко известна, представляет собой связанную группу из одного или нескольких префиксов IP, выполняемых одним или несколькими сетевыми операторами, который имеет политику маршрутизации SINGLE и CLEARLY DEFINED.

Концепция автономных систем изначально считалась существованием одного протокола маршрутизации, однако по мере развития сетей можно поддерживать несколько протоколов маршрутизации, которые взаимодействуют путем ввода маршрутов из одного протокола в другой. Политикой маршрутизации можно считать набор правил, определяющих, как управление трафиком осуществляется в автономной системе, к которой должен придерживаться один или несколько операторов.

Локальная сеть и Широковещательные домены



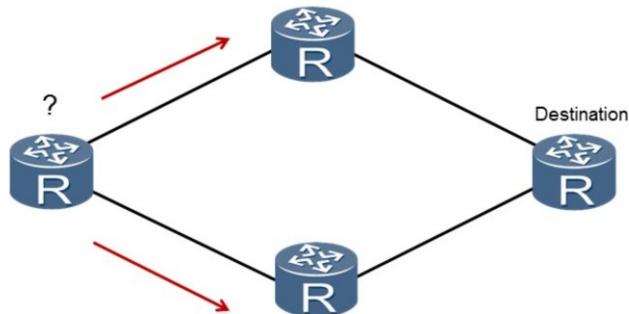
Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 5



Принципы, связанные с маршрутизацией, касались главным образом переадресации трафика в рамках локальной сети и шлюза, который до сих пор определял границу широковещательного домена. Маршрутизаторы являются основной формой устройства сетевого уровня, используемого для определения шлюза каждой локальной сети и включения сегментации IP-сети. Маршрутизаторы обычно функционируют как средство для маршрутизации пакетов из одной локальной сети в другую, опираясь на IP-адресацию для определения сети IP, для которой предназначены пакеты.

Решения о маршрутизации



- Роутеры отвечают за процесс принятия решений, который определяет путь, по которому пересыпаются пакеты

Маршрутизатор отвечает за определение пути адресации, через который пакеты должны быть отправлены по маршруту к данному месту назначения. Каждый маршрутизатор несет ответственность за принятие решений относительно того, как данные передаются. Если маршрутизатор имеет несколько путей к определенному пункту назначения, принимаются решения о маршрутах, основанные на расчетах, чтобы определить лучший следующий прыжок для предполагаемого адресата. Решения, касающиеся маршрута, которые должны быть приняты, могут варьироваться в зависимости от используемого протокола маршрутизации, в конечном итоге полагаясь на показатели каждого протокола, чтобы принимать решения в отношении различных факторов, таких как пропускная способность и количество переходов.

Таблица IP маршрутизации

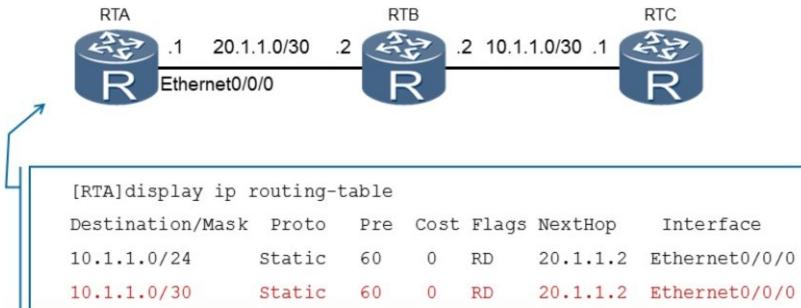
```
[Huawei]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
Destinations : 2      Routes : 2
Destination/Mask Proto Pre Cost Flags NextHop     Interface
127.0.0.0/8      Direct 0    0      D   127.0.0.1  InLoopBack0
127.0.0.1/32     Direct 0    0      D   127.0.0.1  InLoopBack0
```

- В таблице IP маршрутизации представлены сети, который доступны через роутер. Пакеты, который не имеют маршрута, в последствии сбрасываются.

Маршрутизаторы пересыпают пакеты на основе таблиц маршрутизации и базы данных пересылки (FIB) и поддерживают, по меньшей мере, одну таблицу маршрутизации и одну FIB. Маршрутизаторы выбирают маршруты из таблиц маршрутизации для пересылаемых пакетов на основе FIB. Маршрутизатор использует локальную таблицу маршрутизации для хранения маршрутов протокола и предпочтительных маршрутов. Затем маршрутизатор отправляет предпочтительные маршруты в FIB для пересылки пакетов. Маршрутизатор выбирает маршруты в соответствии с приоритетами протоколов и расходами, хранящимися в таблице маршрутизации. Таблица маршрутизации содержит ключевые данные для каждого IP-пакета.

Место назначения и маска используются в комбинации для идентификации IP-адреса назначения или сегмента сети назначения, где находится хост-получатель или маршрутизатор. Поле протокола (Proto) указывает протокол, по которому изучаются маршруты. Предпочтение (Pre) указывает значение предпочтения, которое связано с протоколом, и используется для определения того, какой протокол применяется к таблице маршрутизации, где два протокола предлагают аналогичные маршруты. Маршрутизатор выбирает маршрут с наивысшим приоритетом (наименьшее значение) в качестве оптимального маршрута. Значение стоимости представляет собой метрику, которая используется, чтобы различать, когда несколько маршрутов к одному и тому же месту назначения имеют одинаковое предпочтение, маршрут с наименьшей стоимостью выбирается как оптимальный маршрут. Значение следующего скачка указывает IP-адрес следующего устройства сетевого уровня или шлюза, через который проходит IP-пакет. Наконец, параметр интерфейса указывает исходящий интерфейс, через который пересыпается IP-пакет.

Решения о маршрутизации – наибольшее совпадение



- Маршруты для одной и той же сети буду сравниваться и выбираться на основе самого длинного совпадения.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 8

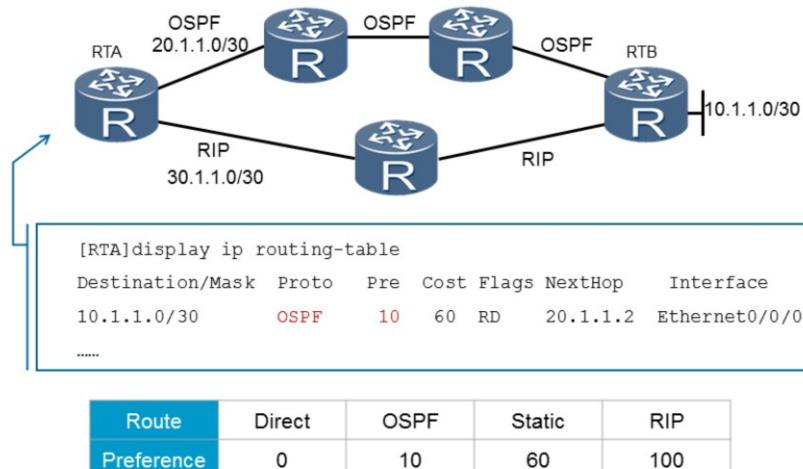


Чтобы позволить пакетам достигнуть своего назначенного адресата, маршрутизаторы должны принимать конкретные решения относительно маршрутов, которые были изучены, и какой из этих маршрутов применяется. Маршрутизатор, скорее всего, узнает о пути к данному сетевому назначению через информацию о маршрутизации, которая декларируется у соседних маршрутизаторов, в качестве альтернативы возможно, чтобы статически применяемые маршруты были вручную реализованы с помощью вмешательства администратора.

Каждая запись в таблице FIB содержит физический или логический интерфейс, через который отправляется пакет для перехода к следующему маршрутизатору. Запись также указывает, может ли пакет быть отправлен непосредственно на целевой хост в сети с прямым подключением. Маршрутизатор выполняет операцию «AND» по адресу назначения в пакете и маске сети каждой записи в таблице FIB. Затем маршрутизатор сравнивает результат операции «AND» с записями в таблице FIB, чтобы найти совпадение.

Маршрутизатор выбирает оптимальный маршрут для пересылки пакетов в соответствии с лучшим или «самым длинным» совпадением. В этом примере две записи в сети 10.1.1.0 существуют со следующим переходом 20.1.1.2. Перенаправление в пункт назначения 10.1.1.1 приведет к применению самого длинного принципа соответствия, для которого сетевой адрес 10.1.1.0/30 обеспечивает самое длинное совпадение.

Решения о маршрутизации – Предпочтение



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 9

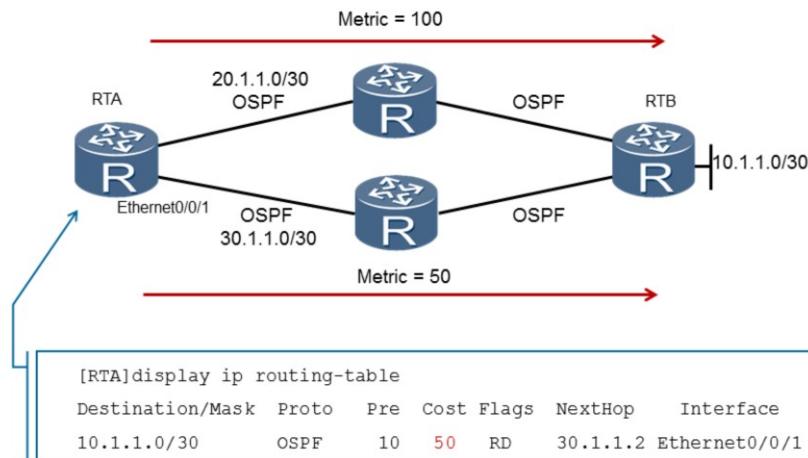


Таблица маршрутизации может содержать маршруты, исходящие из нескольких протоколов, в заданный пункт назначения. Не все протоколы маршрутизации считаются равными и если наибольшее совпадение для нескольких маршрутов разных протоколов маршрутизации для одного и того же адресата одинаково, то необходимо принять решение относительно того, какой протокол маршрутизации (включая статические маршруты) будет иметь приоритет.

Только один протокол маршрутизации в любой момент определяет оптимальный маршрут к месту назначения. Чтобы выбрать оптимальный маршрут, каждый протокол маршрутизации (включая статический маршрут) настроен с предпочтением (чем меньше значение, тем выше предпочтение). Когда существуют несколько источников информации маршрутизации, маршрут с наивысшим приоритетом выбирается как оптимальный маршрут и добавляется в таблицу локальной маршрутизации.

В этом примере определены два протокола, которые обеспечивают средство обнаружения сети 10.1.1.0 через два разных пути. Путь, определенный протоколом RIP, кажется, обеспечивает более прямой маршрут к назенненному получателю, однако из-за значения предпочтения маршрут, определенный протоколом OSPF, является предпочтительным и, следовательно, установлен в таблице маршрутизации в качестве предпочтительного маршрута. Сводка значений предпочтений по умолчанию для некоторых общих механизмов маршрутизации предоставляется для понимания порядка предпочтений по умолчанию.

Решения о маршрутизации – Метрика



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

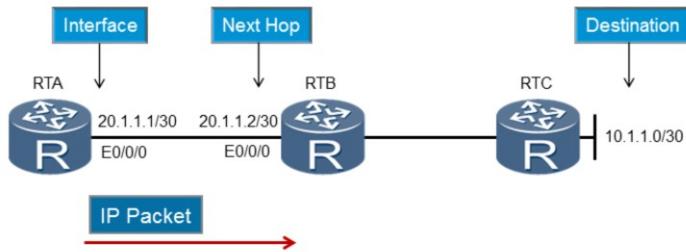
Page 10



Если маршрут нельзя отличить либо самым длинным значением соответствия, либо предпочтением, то в качестве меры при определении маршрута принимается метрика затрат, которая должна быть установлена в таблице маршрутизации. Стоимость представляет собой длину пути к целевой сети.

Каждый сегмент предоставляет значение показателя стоимости по пути, который объединяется для определения стоимости маршрута. Другим распространенным фактором является пропускная способность сети, на которой иногда основан механизм затрат. Связь с более высокой скоростью (пропускной способностью) представляет собой более низкую себестоимость, позволяя сделать предпочтение одного пути над другим, в то время как ссылки равной скорости получают сбалансированную стоимость для эффективной балансировки нагрузки. Нижняя метрика всегда имеет приоритет и, следовательно, показатель 50, как показано в примере, определяет оптимальный маршрут к данному месту назначения, для которого запись может быть найдена в таблице маршрутизации.

Требования к пересылке таблицы маршрутизации



- Для пересылки пакетов требуется, чтобы пункт назначения содержал интерфейс пересылки и следующий шаг.

Возможность маршрутизатора перенаправлять IP-пакет в данный пункт назначения требует, чтобы была известна определенная информация пересылки. Любой маршрутизатор, желающий перенаправить IP-пакет, должен сначала знать о допустимом адресе адресата, которому должен быть переадресован пакет. Это означает, что запись должна существовать в таблице маршрутизации, с которой маршрутизатор может консультироваться. Эта запись также должна идентифицировать интерфейс, через который должны быть переданы IP-пакеты, и следующий переход по пути, на который ожидается получение пакета, до того, как будет принято решение для следующего решения о пересылке.



Итог

- В каком порядке принимаются решения о маршрутизации?
- Для чего используют предпочтения?

1. Решения о маршрутизации принимаются изначально на основе самого длинного совпадающего значения, независимо от значения предпочтений, назначенного для маршрутов в одну и ту же сеть. Если самое длинное совпадающее значение для двух маршрутов в одном и том же пункте назначения равно, то сравниваются предпочтения, когда предпочтение также равны, используется метрика. В тех случаях, когда метрическое значение также одинаково, протоколы обычно применяют форму балансировки нагрузки данных по каналам с равной стоимостью.

2. Предпочтение обычно используется для обозначения надежности маршрута по маршрутам, которые могут считаться менее надежными. Однако поставщики оборудования маршрутизации могут назначать разные значения предпочтений для протоколов, которые поддерживаются в каждом продукте каждого поставщика. Значения предпочтений некоторых общих протоколов маршрутизации, поддерживаемых устройствами маршрутизации Huawei, можно найти в этом разделе.



Thank you

www.huawei.com

Маршруты статических IP

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

Реализация маршрутов в таблице IP-маршрутизации маршрутизатора может быть определена вручную с использованием статических маршрутов или с помощью динамических протоколов маршрутизации. Ручная настройка маршрутов позволяет контролировать таблицу маршрутизации, однако может привести к сбою маршрута, если переход на следующий шаг маршрутизатором не выполняется. Однако конфигурация статических маршрутов часто используется в дополнении к протоколам динамической маршрутизации для предоставления альтернативных маршрутов в случае, если динамически обнаруженные маршруты не выполняют переход на следующий шаг. Знание различных применений статических маршрутов и конфигурации необходима для эффективного администрирования сети.

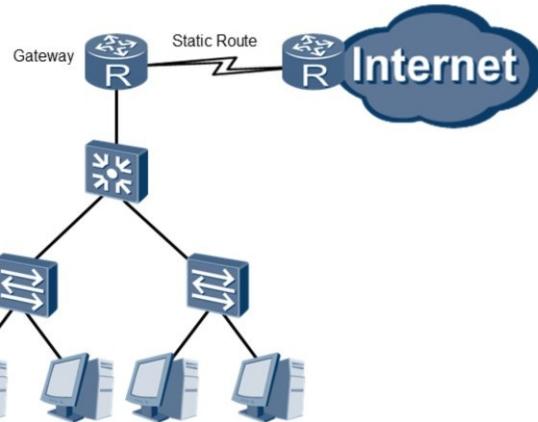


Цели

После изучения этой главы вы сможете:

- Понимать различные приложения для статических маршрутов
- Успешно конфигурировать статические маршруты в таблице IP-маршрутизации

Приложение для статического маршрута



- Статические маршруты определяют возможности выбора пути к другим сетям

Статический маршрут - это специальный маршрут, который вручную настраивается сетевым администратором. Недостатком статических маршрутов является то, что они не могут автоматически адаптироваться к изменению сети, поэтому для изменения сети требуется ручная реконфигурация. Статические маршруты подходят для сетей со сравнительно простыми структурами. Не рекомендуется настраивать и поддерживать статические маршруты для сети со сложной структурой. Однако статические маршруты уменьшают влияние пропускной способности и потребления ресурсов ЦП, возникающих при реализации других протоколов.

Поведение статического маршрута



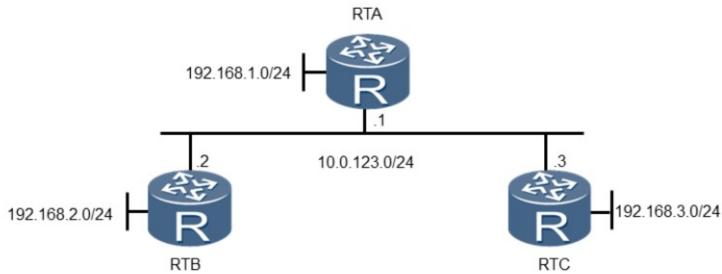
- Пересылка пакетов на основе последовательного интерфейса требует, чтобы исходящий интерфейс был определен

Статические маршруты могут применяться к сетям, использующим как последовательные, так и Ethernet-носители, однако в каждой ситуации условия применения статического маршрута изменяются, а именно должен быть определен исходящий интерфейс или IP-адрес следующего перехода.

Серийный носитель представляет собой форму интерфейса «точка-точка» (P2P), для которой должен быть настроен исходящий интерфейс. Для интерфейса P2P адрес следующего перехода указывается после указания исходящего интерфейса. То есть адрес удаленного интерфейса (интерфейса на одноранговом устройстве), подключенного к этому интерфейсу, является адресом следующего перехода.

Например, протокол, используемый для инкапсуляции через последовательный носитель, представляет собой протокол «точка-точка» (PPP). Удаленный IP-адрес получается после согласования PPP, поэтому необходимо указать только исходящий интерфейс. В этом примере также определяется форма соединения «точка-точка» Ethernet, однако Ethernet представляет собой технологию вещания в среде, и поэтому принципы технологии «точка-точка» не применяются.

Поведение статического маршрута



- Пересылка пакетов в широковещательных сетях, такой как Интернет требует, чтобы исходящий интерфейс был определен

В случае широковещательных интерфейсов, таких как Ethernet, необходимо определить следующий переход. Если в качестве исходящего интерфейса указан Ethernet-интерфейс, может появиться несколько следующих переходов, и система не сможет решить, какой из них должен использоваться. При определении следующего перехода маршрутизатор может идентифицировать локальное соединение, по которому должен быть принят пакет.

В этом примере пакеты, предназначенные для адресата 192.168.2.0/24, должны быть отправлены на следующий переход у 10.0.123.2 для обеспечения доставки. В качестве альтернативы для достижения пункта назначения 192.168.3.0 требуется, чтобы следующий переход 10.0.123.3 был определен.

Конфигурация статического маршрута

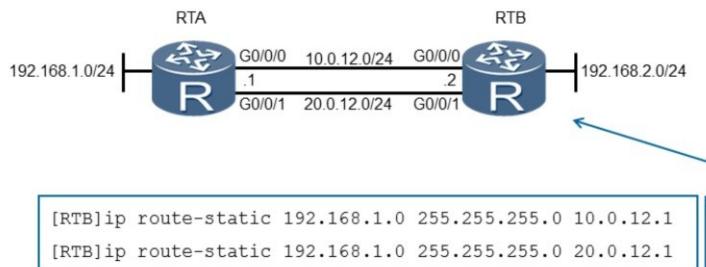


```
[RTB]ip route-static 192.168.1.0 255.255.255.0 10.0.12.1  
[RTB]ip route-static 192.168.1.0 255.255.255.0 Serial 1/0/0  
[RTB]ip route-static 192.168.1.0 24 Serial 1/0/0
```

- Статический маршрут может быть сконфигурирован на основе одного из трех вариантов

Конфигурация статического маршрута достигается с помощью *ip route-static ip-address {mask | mask-length} interface-type interface-number [nexthop-address]*, где *ip*-адрес относится к сети или адресу назначения хоста. Поле маски может быть определено как значение маски или на основе номера префикса. В случае широковещательной среды, такой как Ethernet, используется адрес следующего перехода. Если используется последовательный носитель, то интерфейсный тип и номер интерфейса назначаются (например, *serial 1/0/0*) команде для определения исходящего интерфейса.

Распределение загрузки статического маршрута



- Статические маршруты используют распределенную загрузки к месту назначения, если стоимость маршрутов эквивалентна

Там, где существуют одинаковые пути затрат между сетями источника и назначения, можно реализовать балансировку нагрузки, чтобы трафик мог переноситься по обеим ссылкам. Чтобы достичь этого, используют статические маршруты. Оба маршрута должны иметь одинаковые параметры максимального совпадения, предпочтения и метрического значения. Требуется конфигурация нескольких статических маршрутов, по одному для каждого следующего перехода или исходящего интерфейса в случае последовательного носителя.

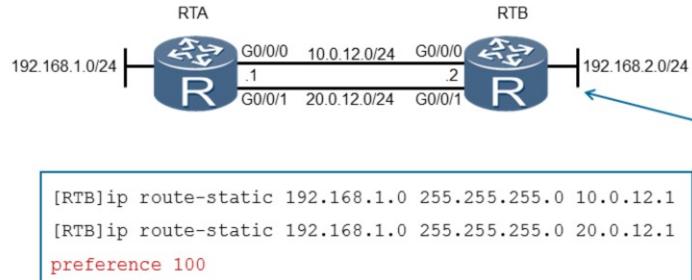
В этом примере показано, как реализованы две *ip route-static* команды, каждая из которых определяет один и тот же адрес назначения IP-адреса и маску, а также альтернативные местоположения следующего перехода. Это гарантирует, что наибольшее совпадение (/24) равно, так же равны значения предпочтения, поскольку оба маршрута являются статическими маршрутами, которые имеют предпочтение по умолчанию 60. Стоимость обоих путей также равна допустимому распределения нагрузки.

Проверка распределения загрузки статического маршрута

```
[RTB]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public Destinations : 13      Routes : 14
Destination/Mask Proto Pre Cost Flags NextHop Interface
...
192.168.1.0/24      Static 60  0    RD 10.0.12.1 GigabitEthernet 0/0/0
                    Static 60  0    RD 20.0.12.1 GigabitEthernet 0/0/1
```

После настройки статических маршрутов таблица маршрутизации может быть запрошена для проверки результатов, при помощи команды *display ip routing-table*. Статический маршрут отображается в таблице маршрутизации, а результаты показывают две записи для одного и того же адресата с соответствующими значениями предпочтения и метрики. Различные адреса следующего перехода и изменения в исходящем интерфейсе идентифицируют два пути, которые были приняты, и подтверждает, что балансировка нагрузки достигнута.

Плавающие статические маршруты



- Плавающие статические маршруты обеспечивают альтернативные маршруты в случае, если первичный статический маршрут неисправен

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 10



Применение статических маршрутов позволяет использовать несколько способов управления маршрутами для достижения требований маршрутизации. Возможно, чтобы предпочтение статического маршрута было изменено с целью преимущества предпочтения одного статического маршрута над другим или использования его с другими протоколами для обеспечения того, чтобы статический маршрут был либо предпочтительным, либо предпочтение отдавалось альтернативному протоколу маршрутизации.

Значение предпочтения по умолчанию для статического маршрута равно 60, поэтому, отрегулировав это значение предпочтения, данный статический маршрут может обрабатываться с неравным предпочтением по любому другому маршруту, включая другие статические маршруты. В приведенном примере два статических маршрута существуют в двух физических сегментах LAN, тогда как обычно оба статических маршрута считаются равными. Второму маршруту присваивается меньшее предпочтение (более высокое значение), вызывающее его удаление из таблицы маршрутизации. Принцип плавающего статического маршрута означает, что маршрут с меньшей степенью предпочтения будет применен к таблице маршрутизации, если основной маршрут не будет работать.

Проверка Плавающих статических маршрутов

```
[RTB]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public Destinations : 13      Routes : 14
Destination/Mask Proto Pre Cost Flags NextHop      Interface
.....
192.168.1.0/24  Static  60    0  RD  10.0.12.1 GigabitEthernet0/0/0
```

- До сбоя основного маршрута только первичный статический маршрут будет присутствовать в таблице маршрутизации.

При использовании команды *show ip routing-table* можно ожидать, что результаты изменения соответствуют значению предпочтения, которое приводит к плавающему статическому маршруту. Обычно в таблице маршрутизации отображаются два маршрута с равной стоимостью, определяющих один и тот же пункт назначения, но имеющие альтернативные значения следующего перехода и исходящие интерфейсы. В этом случае, однако, можно увидеть только один экземпляр, содержащий значение предпочтения статического маршрута по умолчанию 60. Поскольку второй статический маршрут теперь имеет значение предпочтения 100, он не сразу включается в таблицу маршрутизации, так как он больше не рассматривается оптимальный маршрут.

Проверка Плавающих статических маршрутов

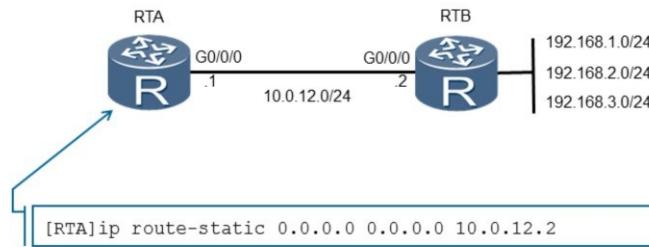
```
[RTB]interface GigabitEthernet 0/0/0
[RTB-GigabitEthernet 0/0/0]shutdown
[RTB]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public Destinations : 13      Routes : 14
Destination/Mask Proto Pre Cost Flags NextHop Interface
.....
192.168.1.0/24 Static 100 0 RD 20.0.12.1 GigabitEthernet 0/0/1
```

- При сбое первичного маршрута, плавающий статичный маршрут добавляется в таблицу маршрутизации

В случае отказа первичного статического маршрута в результате отказа физической линии или отключения интерфейса, статический маршрут больше не сможет предоставить маршрут назначенному адресату и поэтому будет удален из таблицы маршрутизации. Плавающий статический маршрут, вероятно, станет следующим лучшим вариантом для достижения целевого назначения и будет добавлен в таблицу маршрутизации, что позволит передавать пакеты по второму альтернативному пути к назначенному месту назначения, обеспечивая непрерывность в свете любого сбоя.

Когда физическое соединение для исходного маршрута будет восстановлено, исходный статический маршрут снова будет использоваться вместо текущего плавающего статического маршрута, для которого маршрут будет восстановлен в таблице маршрутизации, в результате чего плавающий статический маршрут еще раз будет ожидать.

Статические маршруты по умолчанию



- Маршруты по умолчанию обеспечивают возможность последнего пути в случае, если в таблице маршрутизации не найдено ни одного другого самого длинного совпадения

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 13



Статический маршрут по умолчанию представляет собой специальную форму статического маршрута, которая применяется к сетям, в которых целевой адрес неизвестен, чтобы обеспечить доступ к пути пересылки. Это обеспечивает эффективное средство маршрутизации трафика для неизвестного адресата маршрутизатору или шлюзу, который может знать путь пересылки в корпоративной сети.

Маршрут по умолчанию основывается на «любом сетевом» адресе 0.0.0.0 для соответствия любой сети, которой совпадение не может быть найдено в таблице маршрутизации, и предоставляет путь пересылки по умолчанию, по которому должны быть маршрутизированы пакеты для всех неизвестных сетевых адресатов. В этом примере статический маршрут по умолчанию был реализован в RTA, идентифицируя, что должны быть получены пакеты для неизвестной сети, такие пакеты должны быть отправлены в пункт назначения 10.0.12.2.

Что касается принятия решений в таблице маршрутизации, то в качестве статического маршрута маршрут по умолчанию сохраняет предпочтение 60 по умолчанию, однако действует как последнее средство с точки зрения самого длинного правила соответствия в процессе сопоставления маршрутов.

Проверка статического маршрута по умолчанию

```
[RTA]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public Destinations : 13      Routes : 14
Destination/Mask Proto Pre Cost Flags NextHop Interface
...
0.0.0.0/0      Static  60    0   RD  10.0.12.2 GigabitEthernet0/0/0
```

Конфигурация статического маршрута после его настройки появится в таблице маршрутизации маршрутизатора. Команда *display ip routing-table* используется для просмотра этой информации. В результате все маршруты в примере, не связанные с какими-либо другими маршрутами в таблице маршрутизации, будут перенаправлены в пункт назначения следующего перехода 10.0.12.2 через интерфейс Gigabit Ethernet 0/0/0.



Итог

- Что нужно изменить, чтобы статический маршрут стал плавающим статическим маршрутом?
- Какой сетевой адрес должен быть определен для того, чтобы статический маршрут был определен в таблице маршрутизации?

1. Плавающий статический маршрут может быть реализован путем корректировки значения предпочтения статического маршрута, где два статических маршрута поддерживают балансировку нагрузки.
2. Статический маршрут по умолчанию может быть реализован в таблице маршрутизации, указав адрес «любой сети» 0.0.0.0 в качестве адреса назначения вместе с адресом следующего перехода интерфейса, к которому пакеты, захваченные этим статическим маршрутом по умолчанию, переадресовываются.



Thank you

www.huawei.com

Дистанционно-векторная маршрутизация с
протоколом маршрутной информации
(Routing information protocol – RIP)

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

Протоколы дистанционно-векторной маршрутизации - это форма протокола динамической маршрутизации, которые работают по принципу алгоритма Беллмана-Форда для определения маршрута, по которому должны передаваться пакеты для достижения других сетевых точек назначения. Протокол маршрутной информации (RIP) часто применяется в небольших сетях и, следовательно, остается актуальным и популярным протоколом даже несмотря на то, что сам протокол существует гораздо дольше, чем другие динамические протоколы маршрутизации, используемые сегодня. Характеристики протоколов дистанционно-векторной маршрутизации представлены в этом разделе вместе с протоколом маршрутной информации RIP.

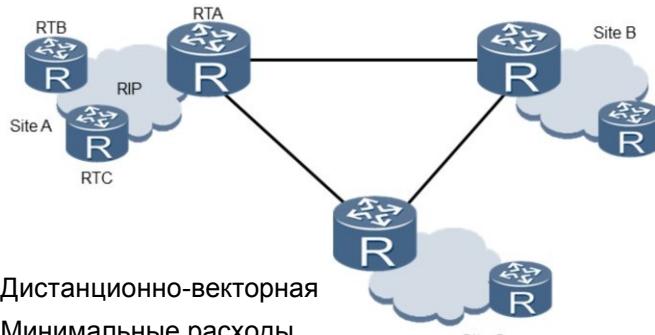


Цели

После изучения этой главы вы сможете:

- Описать поведение протокола маршрутной информации
- Успешно конфигурировать RIP маршрутизацию и связанные с ней атрибуты

Протокол маршрутной информации

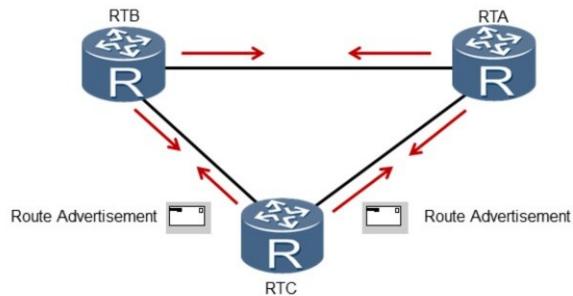


- Дистанционно-векторная
- Минимальные расходы
- Подходит для небольших сетей
- Простая реализация

Протокол маршрутной информации или RIP, как он широко известен, представляет собой одну из более простых форм протокола маршрутизации, которые применяются к корпоративным сетям. RIP работает как протокол внутреннего шлюза (IGP), основанный на принципах алгоритма Белмана-Форда, который работает на основе вектора расстояния, определяя путь, который должен принимать трафик относительно оптимального расстояния, которое измеряется с использованием фиксированного метрического значения.

Протокол RIP содержит минимальное количество параметров и требует ограниченной пропускной способности, конфигурации и времени управления, что делает его идеальным для небольших сетей. Однако RIP не был разработан с возможностью обработки подсетей, поддержки взаимодействия с другими протоколами маршрутизации и не предоставляет никаких средств аутентификации, поскольку его создание предшествовало периоду, в котором эти принципы были введены.

Принцип поведения

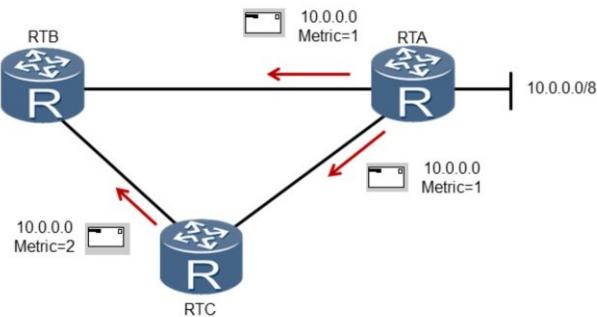


Анонс маршрута отправляется периодически

Информация анонса используется для обнаружения лучших маршрутов

Маршрутизаторы, которые поддерживают RIP, участвуют в анонсе информации о маршрутизации на соседние маршрутизаторы. Создаются анонсы маршрутов, которые содержат информацию о сетях, которые известны передающему маршрутизатору, и расстояние до этих сетей. Маршрутизаторы, поддерживающие RIP, анонсируют друг друга, при этом несут самую лучшую информацию маршрутизации в своих анонсах маршрута.

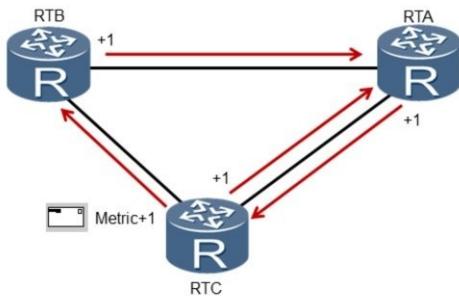
Метрика



- Метрика используется для измерения дистанции к данной сети
- Расчет основан на прыжках, представляющих метрику равную 1

Каждый анонс содержит несколько маршрутов, каждый из которых связан с данным показателем. Метрика используется для определения расстояния между маршрутизатором и пунктом назначения, с которым связан анонс маршрута. В RIP метрика связана с механизмом подсчета переходов, где каждый прыжок между маршрутизаторами представляет собой фиксированный подсчет переходов, обычно один. Эта метрика не учитывает никаких других факторов, таких как пропускная способность для каждой ссылки или любая задержка, которая может быть наложена на ссылку. В этом примере маршрутизатор RTB узнает о сети через два разных интерфейса, каждый из которых предоставляет метку перехода, через которую можно обнаружить лучший маршрут до пункта назначения.

Маршрутизации петлей и лимиты прыжков



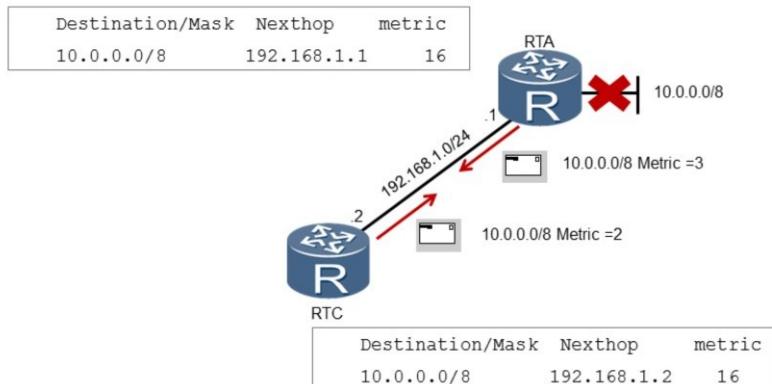
- Метрика увеличивается на 1 до пересылки объявления
- Для предотвращения бесконечных пересылок устанавливается лимит прыжков = 15

Поскольку каждый маршрутизатор обрабатывает объявление маршрута, значение метрики увеличивается перед пересылкой объявления на соседний маршрутизатор. Где маршруты становятся недоступными, однако, есть потенциал для входления в число прыжков становится бесконечной.

Для решения проблемы с бесконечными метриками маршрута было определено значение, которое представляло бы бесконечность, что позволило ограничить количество возможных прыжков до предела в 15 прыжков. Эта метрика считается подходящей для размеров сетей, для которых подходит протокол маршрутизации RIP, а также за пределами того масштаба, который, как ожидается, ожидается в любой сети этого типа.

Количество переходов 16 будет предполагать, что маршрут недоступен, и необходимо изменить эту сеть. Маршрутизация может происходить через маршрутизатор, отправляющий пакеты самому себе, между пикировыми маршрутизаторами или в результате потока трафика между несколькими маршрутизаторами.

Формирование петли

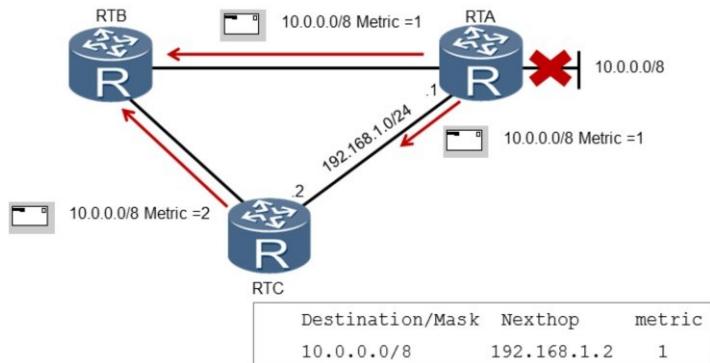


- Когда сеть рушится, следующий лучший маршрут может создать петлю
- Метрика = 16 представляет собой недостижимый маршрут

В этом примере показано, как может сформироваться цикл, если RIP является протоколом маршрутизации. Сеть (10.0.0.0/8) была изучена путем отправки анонсов маршрута из RTA в RTC, для которых RTC будет обновлять свою таблицу маршрутизации сетью и метрикой 1, чтобы добраться до пункта назначения.

В случае отказа подключения маршрутизатора RTA и сети, к которой он напрямую подключен, маршрутизатор сразу обнаруживает потерю маршрута и считает маршрут недоступным. Поскольку RTC обладает знаниями в сети, анонс пересыпается с информацией о сети 10.0.0.0/8. После получения этого RTA узнает о новой записи маршрута для 10.0.0.0/8 с метрикой 2. Поскольку RTC изначально узнал маршрут из RTA, любые изменения необходимо будет обновить и в RTC, при этом анонс маршрута будет отправляться в RTC с метрикой 3. Это будет повторяться в течение бесконечного периода времени. Метрика, равная 16, позволяет закрывать колпачок на бесконечность, тем самым позволяя любому маршруту, достигающему количества переходов 16, считаться недостижимым.

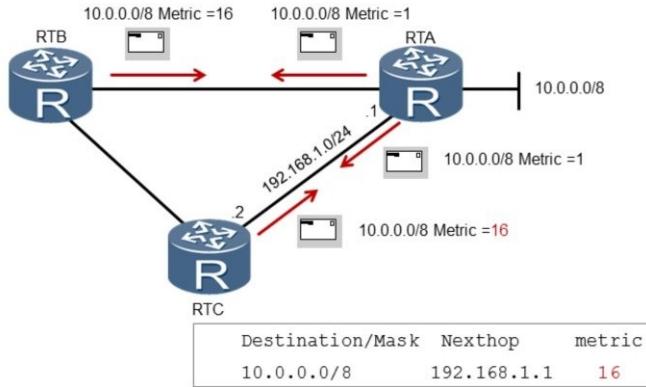
Метод предотвращения петель «Расщепление горизонта»



- Маршрут не может быть анонсирован на интерфейсе, через который он был изучен

Для решения проблем цикла маршрутизации, как часть протокола маршрутизации RIP, были реализованы механизмы, которые возникают, когда маршруты становятся недоступными. Один из этих механизмов известен как "Расщепление горизонта" и работает по принципу, что маршрут, который изучается на интерфейсе, нельзя анонсировать обратно по тому же интерфейсу. Это означает, что сеть 10.0.0.0/8, анонсируемая маршрутизатору RTC, не может быть объявлена обратно в RTA по тому же интерфейсу, однако будет анонсироваться соседям, подключенным через все другие интерфейсы.

Метод предотвращения петель Poisoned Reverse

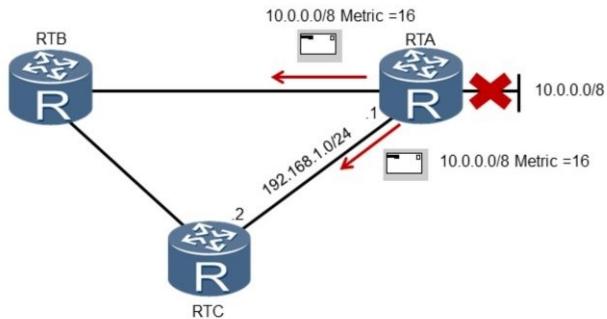


- Poisoned Reverse улучшает время конвергенции, однако генерирует дополнительные издержки из-за дополнительной информации о маршруте.

Внедрение механизма "poison reverse" позволяет ускорить время, в течение которого ошибочные маршруты могут быть увеличены почти мгновенно, в результате возврата маршрутов на исходный маршрутизатор с метрикой 16, чтобы эффективно исключить любое рассмотрение для лучшего маршрута, где маршрут становится недействительным.

В этом примере RTA анонсирует метрику 1 для сети для RTC, тогда как RTC объявляет одну и ту же сеть обратно в RTA, чтобы гарантировать, что если сеть 10.0.0.0/8 не удастся, RTA не обнаружит лучшего пути к этой сети через любой другой маршрутизатор. Это связано с увеличением размера сообщения маршрутизации RIP, поскольку маршруты, содержащие полученную сетевую информацию, также должны нести сетевое обновление, считая маршрут недоступным, обратно на соседний маршрутизатор, с которого возник анонс. В маршрутизаторах серии Huawei AR2200 "расщепленный горизонт" и "poisoned reverse" нельзя применять одновременно, если оба настроены, будет включен только "poisoned reverse".

Метод предотвращения петель «Инициированные обновления» (Triggered Updates)

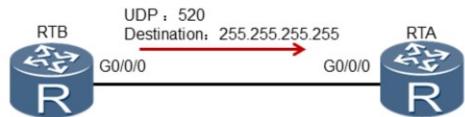


- Обновления отправляются автоматически каждый 30 секунд
- Инициированные обновления разрешают отправлять сообщения мгновенно.

Поведение RIP по умолчанию включает в себя обновления таблицы маршрутизации, периодически отправляемой соседним маршрутизаторам в качестве анонсам маршрута, которая по умолчанию устанавливается примерно каждые 30 секунд. Однако, когда ссылки не работают, это также требует, чтобы срок действия этого периода истекал, прежде чем сообщать соседним маршрутизаторам о неисправности.

Запущенные обновления происходят, когда изменяется локальная информация о маршрутизации, и локальный маршрутизатор немедленно уведомляет своих соседей об изменениях в информации о маршрутизации путем отправки инициированного пакета обновления. Инициированные обновления сокращают время конвергенции сети. Когда изменяется локальная информация о маршрутизации, локальный маршрутизатор немедленно уведомляет соседние маршрутизаторы об изменениях в информации о маршрутизации, а не ждет периодического обновления.

Обмен сообщениями в RIP (Протокол маршрутной информации)



Command	Version	Must be Zero
Address Family Identifier		Must be Zero
	IP Address	
	Must be Zero	
	Must be Zero	
	Metric	

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 12

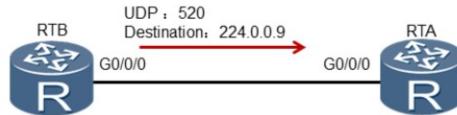


RIP - это протокол на основе UDP. Каждый маршрутизатор, который использует RIP, использует процесс маршрутизации, который включает в себя все коммуникации, направленные на другой маршрутизатор, отправляемые на порт 520, включая все сообщения обновления маршрутизации. RIP обычно передает сообщения обновления маршрутизации в виде широковещательных сообщений, предназначенных для широковещательного адреса 255.255.255.255, ссылаясь на все сети. Однако каждый маршрутизатор будет генерировать свою собственную трансляцию обновлений маршрутизации после каждого периода обновления.

Поля команды и версии используются один раз для каждого пакета, причем поле команды указывает, является ли пакет запросом или ответным сообщением, для которого все сообщения обновления считаются ответными сообщениями. Версия относится к версии RIP, которая в этом случае является версией 1. Остальные поля используются для поддержки сетевых анонсов, для которых может быть объявлено до 25 записей маршрута в одном сообщении об обновлении RIP.

Идентификатор семейства адресов отображает тип протокола, который поддерживается RIP, которым, в этом примере, является IP. Остальные поля используются для переноса IP-адреса сети и метрики перехода, которые содержат значение от 1 до 15 (включительно) и определяют текущий показатель до пункта назначения; или значение 16 (бесконечность), что указывает на то, что цель недоступна.

Расширения в RIP (Протокол маршрутной информации)



Command	Version	Unused
Address Family Identifier		Route Tag
	IP Address	
	Subnet Mask	
	Next Hop	
	Metric	

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 13

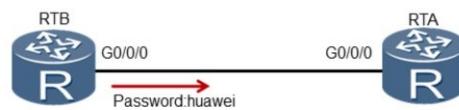


Внедрение новой версии RIP, известной как RIP v. 2, не изменила RIP как таковой, а скорее предоставляет расширения для текущего протокола RIP, чтобы можно было решить некоторые задачи. Формат RIPдейтограмм применяет те же принципы исходного протокола RIP с теми же параметрами команды. Поле версии подчеркивает, что расширенные поля являются частью версии 2.

Идентификатор семейства адресов продолжает ссылаться на поддерживаемый протокол, а также может использоваться для поддержки информации аутентификации. Тег маршрута - еще одна функция, которая вводится для устранения ограничений, которые существуют с поддержкой взаимодействия между автономными системами в RIP, детали которых, выходят за рамки этого курса. Дополнительные расширения параметров были сделаны частью записи маршрута, включая поле Маска подсети, которое содержит маску подсети, которая применяется к IP-адресу, для определения сетевой или подсетевой части адреса.

В поле Next Hop теперь можно указать IP-адрес следующего перехода, которому должны быть отправлены пакеты, предназначенные для адреса назначения, указанного в записи маршрута. Чтобы уменьшить ненужную загрузку хостов, которые не получают пакеты RIP версии 2, для облегчения периодических широковещательных рассылок используется многоадресный IP-адрес.

Расширения в RIP (Протокол маршрутной информации) - Авторизация



Command	Version	Unused
0xFFFF	Authentication Type	
Authentication		

- RIP v/.2 поддерживает аутентификацию между узлами
- Поддерживает простой текст и шифрование

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 14

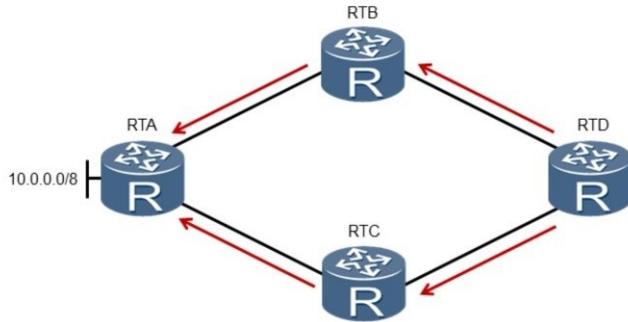


Аутентификация представляет собой средство, с помощью которого можно фильтровать вредоносные пакеты, гарантируя, что все полученные пакеты могут быть проверены как исходящие из существующего партнера с использованием значения ключа. Это ключевое значение первоначально представляет собой строку пароля открытого текста, которая может быть сконфигурирована для каждого интерфейса, и распознано аутентификацией RIP v.2. Аутентификация, настроенная между одноранговыми узлами, должна совпадать до того, как сообщения RIP могут быть успешно обработаны. Для проверки подлинности, если маршрутизатор не настроен для аутентификации сообщений RIP версии 2, будут приняты сообщения RIP версии 1 и неавторизованные сообщения RIP версии 2; аутентифицированные сообщения RIP версии 2 должны быть отброшены.

Если маршрутизатор настроен для аутентификации сообщений RIP версии 2, то принимаются сообщения RIP версии 1 и сообщения RIP версии 2, которые проходят проверку подлинности; не прошедшие проверку подлинности и аутентификацию сообщения RIP версии 2 должны быть отброшены.

RIP версия 2 первоначально поддерживала только простую аутентификацию открытого текста, которая обеспечивала минимальную безопасность, поскольку строка аутентификации может быть легко захвачена. С повышенной потребностью в безопасности для RIP была введена криптографическая аутентификация, первоначально с поддержкой MD5 (RFC 2082) и дальнейшим усовершенствованием посредством поддержки аутентификации HMAC-SHA-1, введенной как RFC 4822. Хотя Huawei Маршрутизаторы серии AR2200 способны поддерживать все известные типы аутентификации, приведенный пример демонстрирует оригинальную аутентификацию для простоты.

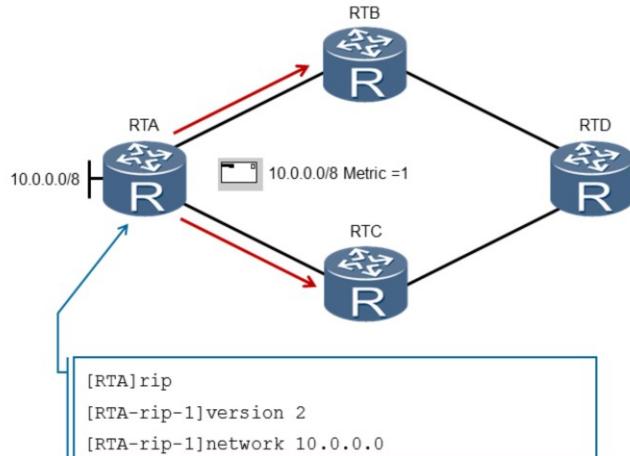
RIP распределение загрузки



- Распределение загрузки может быть использоваться в RIP для устранения избыточных ссылок.
- AR2200 поддерживает 8 маршрутов, равных по ценности.

Если сеть имеет несколько избыточных ссылок, можно настроить максимальное количество маршрутов с равной стоимостью для реализации балансировки нагрузки. Таким образом, сетевые ресурсы полностью используются, а ситуации, когда некоторые ссылки перегружены, а другие - в режиме ожидания, можно избежать, и можно предотвратить длительные задержки в передаче пакетов. По умолчанию и максимальное количество маршрутов равной стоимости, поддерживаемых RIP, равно 8 в любой момент времени.

RIP сетевые анонсы



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

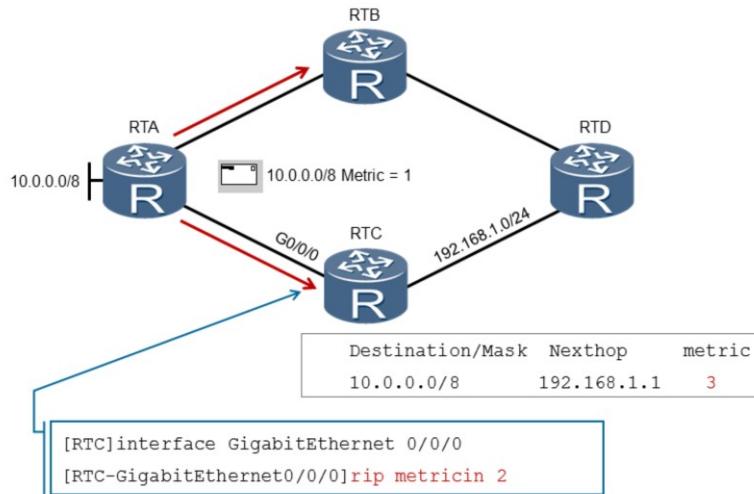
Page 16



Для всех маршрутизаторов, поддерживающих процесс маршрутизации RIP, требуется сначала включить процесс на каждом маршрутизаторе. Для включения этой команды используется команда `rip [process-id]`, при этом `process-id` идентифицирует конкретный process ID, с которым связан маршрутизатор. Если process ID не настроен, процесс по умолчанию будет иметь process ID 1. Если существует вариация в идентификаторе процесса, локальный маршрутизатор будет создавать отдельные записи таблицы маршрутизации RIP для каждого определенного процесса.

Команда RIP v.2 обеспечивает дополнительную возможность для подсетей, аутентификации, взаимодействия между автономными системами и т. д. Команда `network <network-address>` указывает сетевой адрес, для которого включен RIP, и должен быть адрес natural сегмента сети.

Команда RIP metricin



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

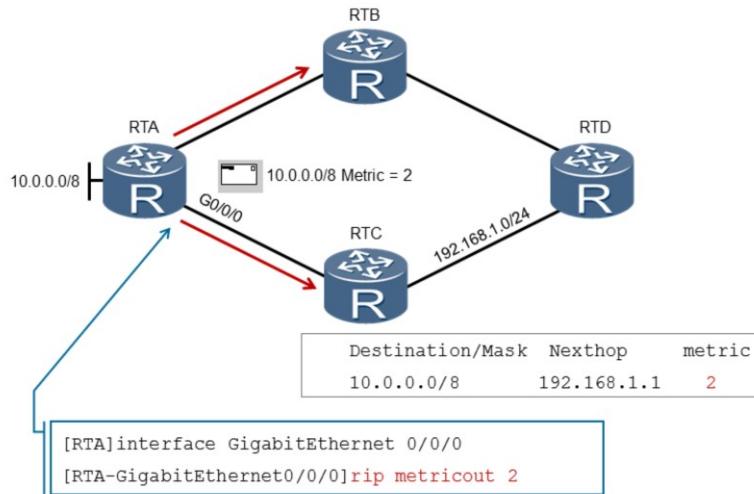
Page 17



RIP также способен поддерживать манипуляции с метриками RIP для управления потоком трафика в домене маршрутизации RIP. Один из способов достижения этой цели - настроить метрику, связанную с вводом маршрута, когда он получен маршрутизатором. Когда интерфейс получает маршрут, RIP добавляет дополнительную метрику интерфейса к маршруту и затем устанавливает маршрут в таблицу маршрутизации, тем самым увеличивая метрику интерфейса, которая также увеличивает метрику маршрута RIP, полученную интерфейсом.

Команда `rip metricin <metric value>` позволяет манипулировать метрикой, где `metric value` относится к метрике, которая должна применяться. Следует также отметить, что для команды `rip metricin` значение метрики добавляется к метрическому значению, которое в настоящее время связано с маршрутом. В этом примере запись маршрута для сети 10.0.0.0/8 содержит метрику 1 и обрабатывается по прибытии на интерфейс RTC, в результате чего метрическое значение 3 связано с маршрутом.

Команда RIP metricout



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

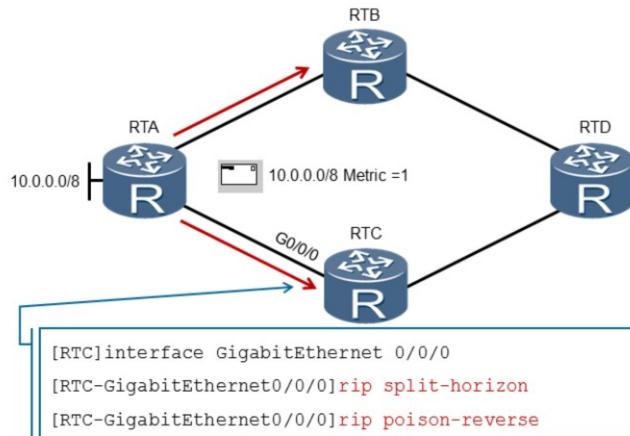
Page 18



Команда *rip metricout* позволяет манипулировать метрикой для маршрута, когда анонсируется маршрут RIP. Увеличение метрики интерфейса также увеличивает метрику маршрута RIP, отправленного по интерфейсу, но не влияет на метрику маршрута в таблице маршрутизации маршрутизатора, к которому применяется команда *rip metricout*.

В своей самой базовой форме команда *rip metricout* определяет значение, которое должно быть принято пересылаемой записью маршрута, но также способно поддерживать механизмы фильтрации, чтобы выборочно определять, к каким маршрутам должен применяться метрика. Общее поведение RIP заключается в том, чтобы увеличить метрику на единицу перед пересылкой записи маршрута в следующий прыжок. Если команда *rip metricout* настроена, применяется только *metric value*, указанное в команде.

Расщепление горизонта & Poisoned reverse



- Если активны оба, только *rip poison-reverse* будет иметь эффект

Конфигурация как "расщепленного горизонта", так и *poisoned reverse* выполняется для каждого интерфейса, при этом по умолчанию команда *rip split-horizon* включена (за исключением сетей NBMA), чтобы избежать многих проблем петель маршрутизации, которые были обозначены в этой главе. Реализация как "расщепленного горизонта", так и *poisoned reverse* не допускается на маршрутизаторе серии AR2200, поэтому, когда *poisoned reverse* сконфигурирован на интерфейсе с помощью команды *rip poison-reverse*, расщепление горизонта будет отключено.

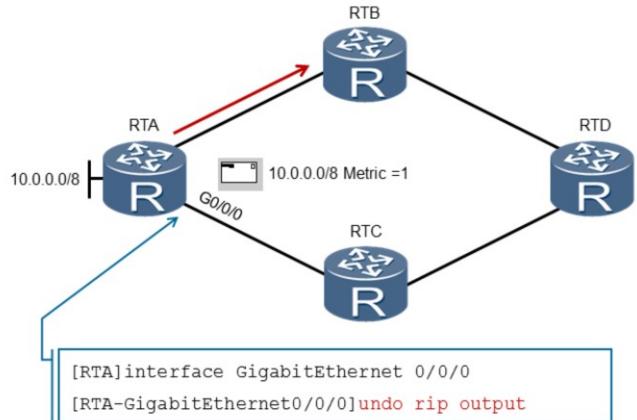
Проверка конфигурации

```
[RTC] display rip 1 interface GigabitEthernet0/0/0 verbose
GigabitEthernet0/0/0(192.168.1.2)
  State        : UP          MTU     : 500
  Metricin    : 2
  Metricout   : 1
  Input       : Enabled      Output : Enabled
  Protocol    : RIPv2 Multicast
  Send version: RIPv2 Multicast Packets
  Receive version : RIPv2 Multicast and Broadcast Packets
  Poison-reverse      : Enabled
  Split-Horizon       : Enabled
  Authentication type : None
  Replay Protection   : Disabled
```

- Оба отображаются как активные, но только Poison-reverse будет иметь эффект

Конфигурация протокола маршрутной информации для каждого интерфейса может быть проверена с помощью команды *display rip <process_id> interface <interface> verbose*. Связанные параметры RIP можно найти на отображаемом выходе, включая версию RIP, применяемую вместе с другими параметрами, такими как применение poison-reverse и расщепление горизонта. Если команда отображения ссылается на то, что оба режима poison-reverse и расщепления горизонта оба включены, будет действовать только команда poison-reverse.

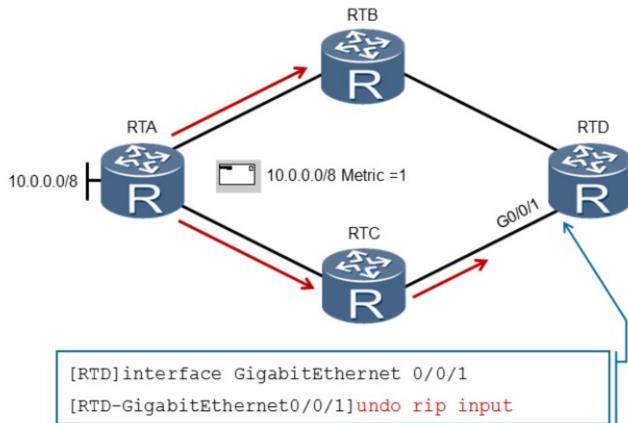
RIP вывод



- Исходящие анонсы RIP ограничены интерфейсом G0/0/0.

Команда *rip output* применяется к интерфейсу маршрутизатора, участвующего в маршрутизации RIP, и позволяет RIP пересыпать сообщения обновления из интерфейса. Если для интерфейса применяется команда отмены *undo rip output*, сообщение об обновлении RIP перестает быть перенаправленным из данного интерфейса. Его применение действительно в тех случаях, когда корпоративная сеть не хочет делиться своими внутренними маршрутами через интерфейс, который подключается к внешней сети, чтобы защитить сеть, часто применяя маршрут по умолчанию к этому интерфейсу, вместо любых маршрутов, которые хотят достичь внешних сетей.

RIP ввод



- Входящие анонсы RIP ограничены интерфейсом G0/0/1.

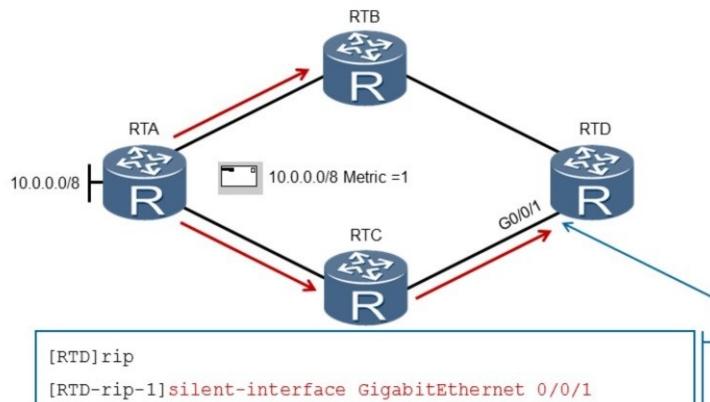
Команда *undo rip input* позволяет интерфейсу отклонить все сообщения об обновлении RIP и запретить добавление информации RIP в таблицу маршрутизации для данного интерфейса. Это может быть применено в ситуациях, когда поток трафика может потребоваться контролировать только с помощью определенных интерфейсов или полностью предотвратить прием RIP маршрутизатором. Таким образом, любые сообщения об обновлении RIP, отправленные на интерфейс, будут немедленно отброшены. Команда *rip input* может использоваться для повторного включения интерфейса для возобновления получения обновлений RIP.

Проверка конфигурации

```
[RTD] display rip 1 interface GigabitEthernet0/0/1 verbose
GigabitEthernet0/0/1(192.168.1.2)
  State        : UP          MTU     : 500
  Metricin    : 1
  Metricout   : 1
  Input       : Disabled    Output : Enabled
  Protocol    : RIPv2 Multicast
  Send version: RIPv2 Multicast Packets
  Receive version : RIPv2 Multicast and Broadcast Packets
  Poison-reverse      : Enabled
  Split-Horizon       : Enabled
  Authentication type : None
  Replay Protection   : Disabled
```

Команда `display rip <process_id> interface <interface> verbose` также может использоваться для подтверждения реализации ограничений для интерфейса. Если интерфейс сконфигурирован с `undo rip input`, возможность приема маршрутов RIP будет считаться отключенной, как выделено в параметре `Input`.

Silent интерфейс



- Интерфейс не принимает участие в RIP, но получает RIP маршруты
- Имеет превосходство над rip input и rip output командами.

Silent интерфейс позволяет получать обновления маршрута RIP и использоваться для обновления таблицы маршрутизации маршрутизатора, но не позволит интерфейсу участвовать в RIP. Для сравнения, команда с Silent интерфейсом имеет более высокий приоритет, чем команды вывода rip input и rip output. Когда применяется команда all-all-interface, команда принимает наивысший приоритет, а это означает, что ни один интерфейс не может быть активирован. Для интерфейса необходимо применять команду «silent-interface», чтобы обеспечить комбинацию активных и silent интерфейсов.

Общее применение silent интерфейса - для сетей широковещательного множественного доступа. Маршрутизаторы могут потребоваться для получения сообщений об обновлении RIP, но не будут транслировать/вещать свои собственные обновления, требуя вместо этого, чтобы отношения с пиринговым маршрутизатором выполнялись с помощью команды peer <ip address>.

Проверка конфигурации

```
[RTD] display rip
Public VPN-instance
    RIP process : 1
        RIP version      : 2
        Preference       : 100
        Checkzero        : Enabled
        Default-cost     : 0
        Summary          : Enabled
        Host-route       : Enabled
        Maximum number of balanced paths : 8
        Update time      : 30 sec           Age time : 180 sec
        Garbage-collect time : 120 sec
        Graceful restart  : Disabled
        BFD               : Disabled
        Silent-interfaces : GigabitEthernet0/0/1
```

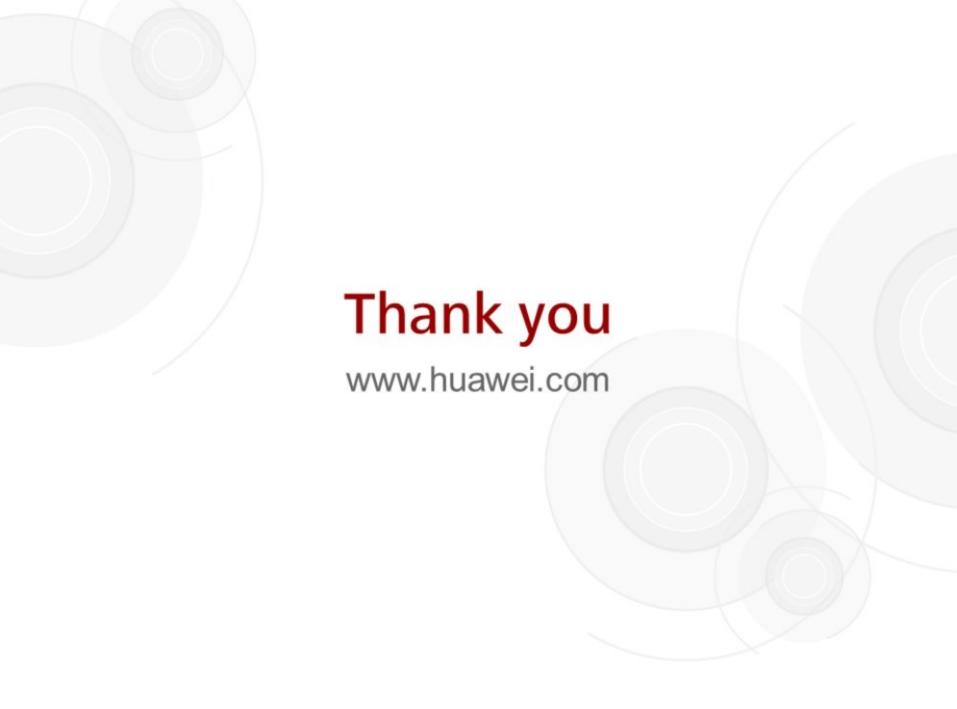
Команда *display rip* обеспечивает более полный выход на основе маршрутизатора, для которого глобальные параметры могут быть проверены вместе с определенными параметрами на основе интерфейса. С помощью этой команды можно наблюдать реализацию команды *silent-interface* на данном интерфейсе.



Итоги:

- В какой момент метрика увеличивается для анонсируемых маршрутов?
- Какая конфигурация необходима для анонса маршрутов RIP?

1. Метрика увеличивается до пересылки анонса маршрута из исходящего интерфейса.
2. Анонс маршрутов RIP достигается посредством конфигурации сетевой команды. Для каждой сети, которая должна анонсироваться маршрутизатором, необходимо настроить сетевую команду.



Thank you

www.huawei.com

Маршрутизация по состоянию канала с помощью OSPF - открытого протокола поиска первого кратчайшего пути (Open Shortest Path First)

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

OSPF - это протокол внутреннего шлюза (IGP), предназначенный для IP-сетей и основанный на принципах маршрутизации связи. Поведение состояния канала предоставляет множество альтернативных преимуществ для средних и даже больших корпоративных сетей. Его применение как IGP вводится вместе с информацией, относящейся к пониманию конвергенции OSPF и для поддержки OSPF в корпоративных сетях.

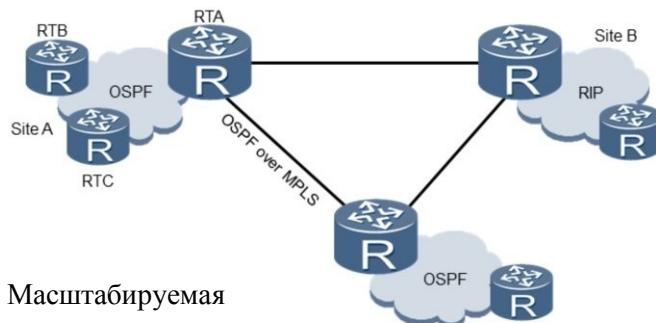


Цели

После изучения этой главы вы сможете:

- Объяснить OSPF процесс конвергенции
- Описать различные типы сетей, поддерживаемые OSPF
- Успешно настраивать единую область OSPF сетей

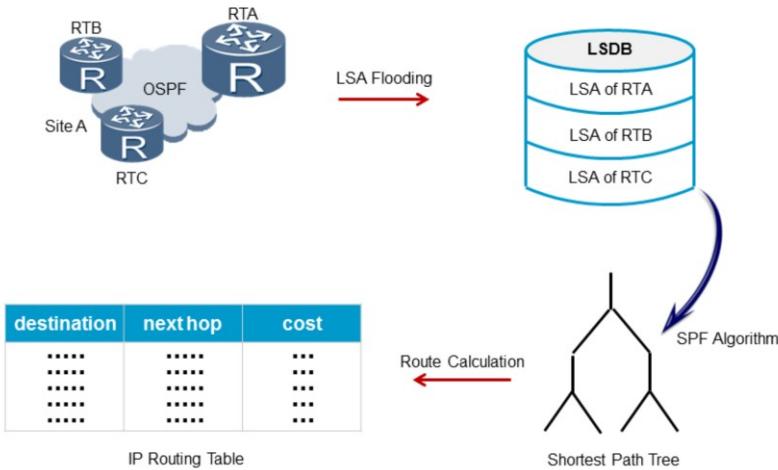
Открытый протокол поиска первого кратчайшего пути (OSPF)



- Масштабируемая
- Быстрая конвергенция
- Минимальный поток маршрутизации
- Точные метрики маршрута

Открытый протокол поиска первого кратчайшего пути (Open Shortest Path First) или OSPF рассматривается как протокол состояния канала, который способен быстро обнаруживать топологические изменения в автономной системе и устанавливать короткие маршруты за короткий промежуток времени с минимальными дополнительными издержками связи для согласования изменений топологии между пиринговыми маршрутизаторами. OSPF также занимается проблемами масштабируемости, возникающими, когда связь между растущим числом маршрутизаторов становится настолько экстремальной, что она начинает приводить к нестабильности в автономной системе. Это управляется с помощью областей, которые ограничивают объем взаимодействия маршрутизатора с изолированной группой в автономной системе, позволяющей поддерживать OSPF малыми, средними и даже большими сетями. Протокол также может работать над другими протоколами, такими как MPLS или протокол переключения меток, чтобы обеспечить масштабируемость сети даже в географически разбросанных местах. Что касается оптимального обнаружения пути, OSPF обеспечивает богатые показатели маршрута, которые обеспечивают большую точность, чем метрики маршрута, применяемые к протоколам, таким как RIP, для обеспечения оптимизации маршрутов на основе не только расстояния, но и скорости связи.

OSPF поведение конвергенции



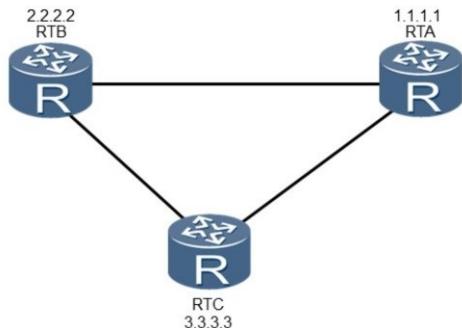
Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 5



Для конвергенции OSPF требуется, чтобы каждый маршрутизатор, активно работающий по протоколу OSPF, знал о состоянии всех интерфейсов и примыканий (связей между маршрутизаторами, к которым они подключены), чтобы установить лучший путь к каждой сети. Первоначально это формируется путем заполнения Link State Advertising (LSA), которые являются единицами данных, содержащими информацию об известных сетях и состояниях ссылок для каждого интерфейса в домене маршрутизации. Каждый маршрутизатор будет использовать полученную LSA для создания базы данных состояния канала (LSDB), которая обеспечивает основу для создания кратчайшего дерева путей для каждой сети, из которых маршруты включаются в таблицу IP-маршрутизации.

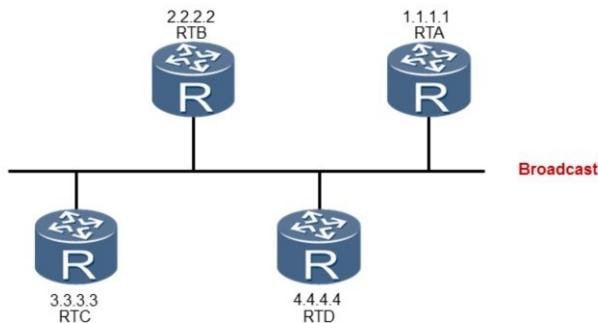
ID маршрутизатора



Router ID это 32 битное значение, используемое для идентификации каждого маршрутизатора, использующего OSPF протокол

Идентификатор маршрутизатора (Router ID) - это 32-битное значение, назначенное каждому маршрутизатору, работающему по протоколу OSPF. Это значение однозначно идентифицирует маршрутизатор в автономной системе. Идентификатор маршрутизатора можно назначить вручную или его можно взять с настроенного адреса. Если логический (loopback) интерфейс настроен и существует несколько логических интерфейсов, идентификатор маршрутизатора будет основан на IP-адресе самого сконфигурированного логического интерфейса. Если логические интерфейсы не настроены, маршрутизатор будет использовать самый наивысший IP-адрес, настроенный на физическом интерфейсе. Любой маршрутизатор, работающий с OSPF, может быть перезапущен с использованием функции graceful перезапуска, чтобы обновить идентификатор маршрутизатора. Рекомендуется идентификатор маршрутизатора настраивать вручную, чтобы избежать непредвиденных изменений в идентификаторе маршрутизатора в случае изменения адреса интерфейса.

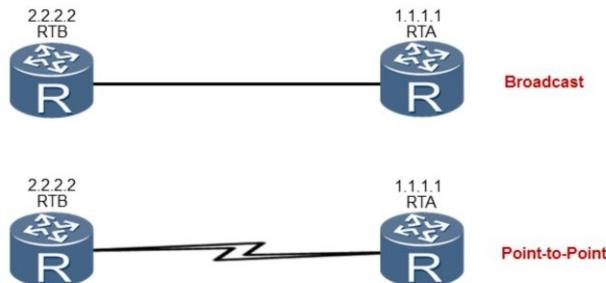
OSPF поддерживаемые типы сетей



- Ethernet сети наследуют широковещательный тип сети по умолчанию

OSPF поддерживает различные типы сетей и в каждом случае будет применять другое поведение в отношении того, как формируются отношения соседа и как облегчается связь. Ethernet представляет собой форму широковещательной сети, которая включает в себя несколько маршрутизаторов, подключенных к одному и тому же сегменту сети. Одна из основных проблем связана с тем, как происходит связь между соседними маршрутизаторами, чтобы минимизировать служебные данные маршрутизации OSPF. Если установлена сеть Ethernet, тип широковещательной сети будет применяться автоматически в OSPF.

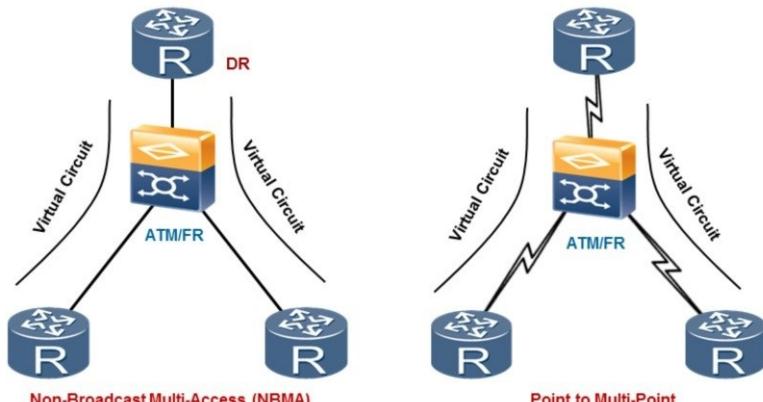
OSPF поддерживаемые типы сетей



- Серийные технологии, такие как PPP и HDLC по умолчанию используют двухточечный тип сети

Если два маршрутизатора установлены в топологии точка-точка, применяемый тип сети будет варьироваться в зависимости от применяемой технологии уровня среды и уровня канала связи. Как уже упоминалось, использование Ethernet-среды приведет к тому, что тип широковещательной сети для OSPF будет назначен автоматически. Если физический носитель является последовательным, тип сети рассматривается как двухточечный. Общие формы протоколов, которые работают на последовательных носителях на уровне канала связи, включают протокол двухточечного соединения (PPP) и высокоуровневый протокол управления каналом (HDLC).

OSPF поддерживаемые типы сетей

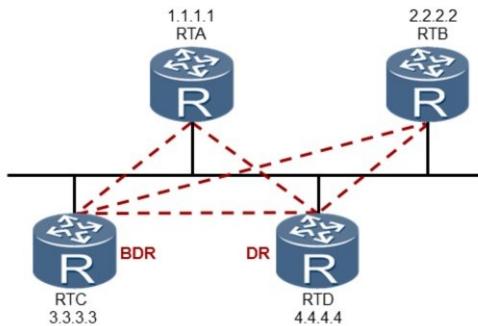


- ATM & Frame Relay по умолчанию используют нешироковещательный мульти-доступ

OSPF может работать в сетях с множественным доступом, которые не поддерживают широковещательные передачи. К таким сетям относятся Frame Relay и ATM, которые обычно работают с использованием топологий типа хаба и говорящего типа, которые полагаются на использование виртуальных цепей для обеспечения связи. OSPF может указывать два типа сетей, которые могут применяться к каналам, связанным с такими средами. Тип сети без широковещательного многоадресного доступа (NBMA) эмулирует широковещательную сеть и поэтому требует, чтобы каждый пиринговый интерфейс был частью одного и того же сегмента сети. В отличие от широковещательной сети, NBMA пересыпает пакеты OSPF как одноадресную передачу, тем самым требуя создания нескольких экземпляров одного и того же пакета для каждого адресата.

Point-to-Multipoint также может применяться в качестве типа сети для каждого интерфейса, и в этом случае применяется поведение типа «точка-точка». Это означает, что каждый пиринг должен быть связан с различными сегментами сети. Назначенные маршрутизаторы связаны с широковещательными сетями и поэтому реализуются сетями NBMA. Самое главное - это позиционирование DR, которое должно быть назначено на узле архитектуры чтобы гарантировать, что все узлы могут связываться с DR.

Назначенный маршрутизатор & Резервный назначенный маршрутизатор

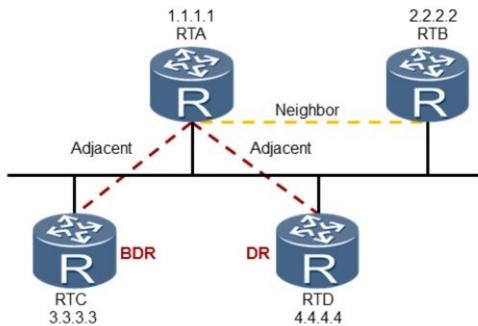


- Назначенные маршрутизаторы ограничивают количество примыканий, необходимых в сетях вещания (Ethernet)

Чтобы адресовать и оптимизировать связь OSPF по широковещательным сетям, OSPF реализует назначенный маршрутизатор (DR - Designated Router), который выступает в качестве центральной точки связи для всех других маршрутизаторов, связанных с широковещательной сетью, по меньшей мере, по одному интерфейсу. В теоретической широковещательной сети, которая не применяет DR, можно понять, что коммуникация следует формуле $n(n-1)/2$, где n представляет количество интерфейсов маршрутизатора, участвующих в OSPF. В приведенном примере это относится к 6 смежностям между всеми маршрутизаторами. Когда применяется DR, все маршрутизаторы устанавливают связь с DR, который отвечает за выполнение функции центральной точки связи для всех соседних маршрутизаторов в широковещательной сети.

Резервный назначенный маршрутизатор (BDR) - это маршрутизатор, который выбирается для перехода с DR, если он терпит неудачу. Таким образом, необходимо, чтобы BDR установил базу данных состояния связи, как и DR, чтобы обеспечить синхронизацию. Это означает, что все соседние маршрутизаторы также должны связываться с BDR в широковещательной сети. С применением DR и BDR число ассоциаций уменьшается с 6 до 5, поскольку RTA и RTB должны взаимодействовать только с DR и BDR. Это может показаться недостаточным, однако, когда это применяется к сети, содержащей, например, 10 маршрутизаторов, то есть $(10 * 9) / 2$, полученная в результате эффективность связи становится очевидной.

Статус «Сосед»

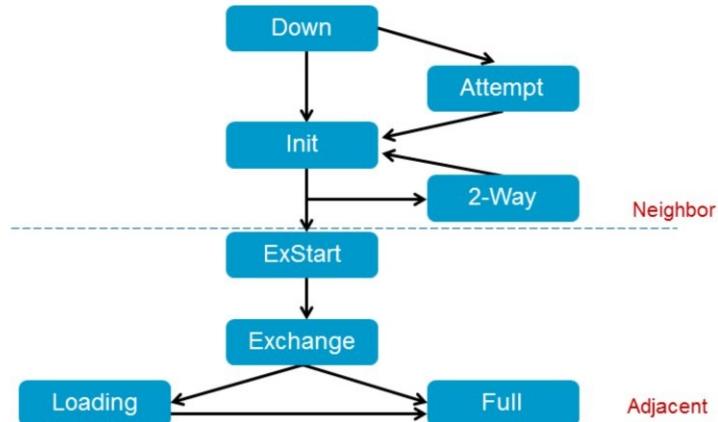


- Определяет форму отношений между соседями
- Возможны два соседних состояния: сосед и смежность

OSPF создает смежности между соседними маршрутизаторами для обмена информацией маршрутизации. Не каждые два соседних маршрутизатора станут смежными, особенно если один из двух маршрутизаторов, устанавливающих смежность не является DR или BDR. Эти маршрутизаторы известны как DROther и только признают присутствие DROther, но не устанавливают полную связь; это состояние известно как соседнее состояние. Однако DROther routers образуют полную смежность с маршрутизаторами DR и BDR, чтобы обеспечить синхронизацию базы данных состояния канала DR и BDR-маршрутизаторов с каждым из маршрутизаторов DROther. Эта синхронизация достигается путем установления соседнего состояния с каждым DROther.

Смежность привязана к сети, которая имеет два маршрутизатора. Если два маршрутизатора имеют несколько общих сетей, они могут иметь несколько смежных связей между ними.

Создание статуса канала



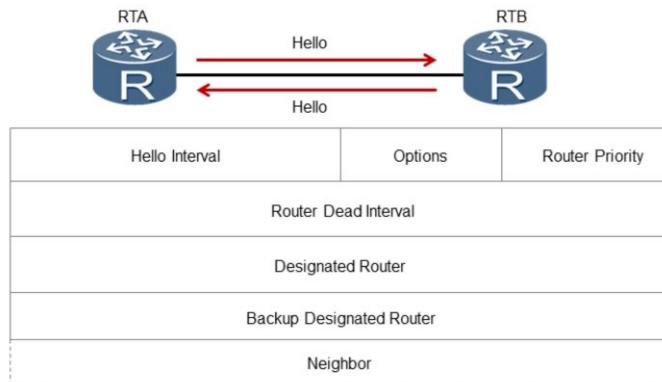
- Изменение состояния позволяет получить отношение соседства

Каждый маршрутизатор, участвующий в OSPF, будет переходить через несколько состояний связи для достижения либо состояния соседства, либо смежного состояния. Все маршрутизаторы начинают в исходящем состоянии после инициализации и проходят процесс обнаружения соседей, что предполагает, во-первых, присутствие маршрутизаторов, известных в сети OSPF, через пакет Hello. При выполнении этого действия маршрутизатор переходит в состояние init.

Как только маршрутизатор получит ответ в виде пакета Hello, содержащего идентификатор маршрутизатора, получающего ответ, будет достигнуто двухстороннее состояние и сформировано соседнее отношение. В случае сетей NBMA состояние attempt достигается, когда связь с соседом становится неактивной, и предпринимается попытка восстановить связь посредством периодической отправки пакетов Hello. Маршрутизаторы, не достигшие смежных отношений, останутся в соседнем состоянии с двухсторонним состоянием связи.

Маршрутизаторы, такие как DR и BDR, будут строить смежное соседнее состояние со всеми соседними маршрутизаторами и, следовательно, должны обмениваться информацией о состоянии канала, чтобы установить полную базу данных состояния канала. Для этого требуется, чтобы пиринговые маршрутизаторы, которые устанавливают смежность, сначала установили связь для обмена информацией о состоянии канала (ExStart), прежде чем переходить к сводной информации о сетях, о которых они знают. Соседи могут определять маршруты, на которые они либо не знают, либо не имеют актуальной информации, и поэтому запрашивают дополнительные данные для этих маршрутов как часть состояния загрузки. Полнотью синхронизированная взаимосвязь между соседями определяется состоянием full, при котором оба пиринговых маршрутизатора могут считаться смежными.

Обнаружение соседей

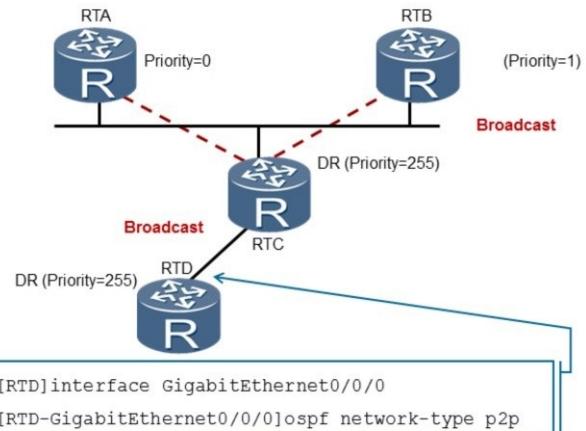


- Протокол Hello отвечает за обнаружение соседей и обслуживание двусторонней связи между соседями.

Обнаружение соседей достигается за счет использования пакетов Hello, которые генерированы с интервалом на основе Hello timer, который по умолчанию составляет каждые 10 секунд для широковещательных и двухточечных сетевых типов; тогда как для сетей NBMA и типа «Point-to-Multipoint» hello интервал составляет 30 секунд. Пакет hello содержит этот период интервала вместе с полем приоритета маршрутизатора, который позволяет соседям определять соседа с самым высоким идентификатором маршрутизатора для идентификации DR и BDR в сетях вещания и NBMA.

Период, определяющий, как долго пакет приветствия до того, как соседа будет считаться потерянным, также должен быть определен, и это переносится как мертвый интервал маршрутизатора в пакет hello. Этот мертвый интервал устанавливается по умолчанию в четыре раза по интервалу hello, таким образом, он составляет 40 секунд для сетей вещания и «точка-точка» и 120 секунд для сетей NBMA и Point-to-Multipoint. Кроме того, идентификатор маршрутизатора как DR, так и BDR переносится, если это применимо, на основе сети, для которой генерируется hello пакет.

Выбор назначенного маршрутизатора



- Назначенный маршрутизатор выбирается на основе значения приоритета.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

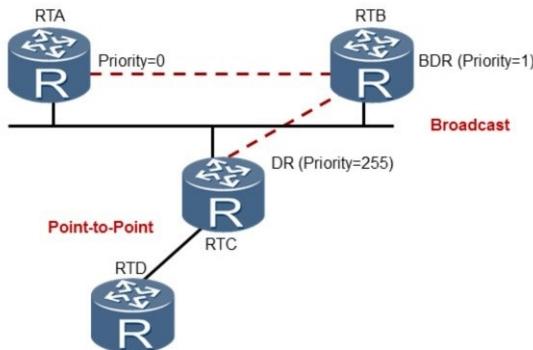
Page 14



После обнаружения соседа, выбор DR может происходить в зависимости от сетевого типа сетевого сегмента. Сети вещания и NMBA будут проводить выборы DR. Выборы DR основаны на приоритете, который назначается для каждого интерфейса, который участвует в процессе выборов в DR. Это значение приоритета устанавливается как 1 по умолчанию, а более высокий приоритет представляет собой лучшего кандидата DR.

Если установлен приоритет 0, интерфейс маршрутизатора больше не будет участвовать в выборах, чтобы стать DR или BDR. Возможно, что, когда двухточечные соединения (с использованием Ethernet в качестве физического носителя) настроены на поддержку типа широковещательной сети, будут возникать ненужные выборы DR, которые генерируют чрезмерный трафик протокола. Несмотря на это рекомендуется, чтобы тип сети был настроен как тип сети точка-точка.

Резервный выбор назначенного маршрутизатора

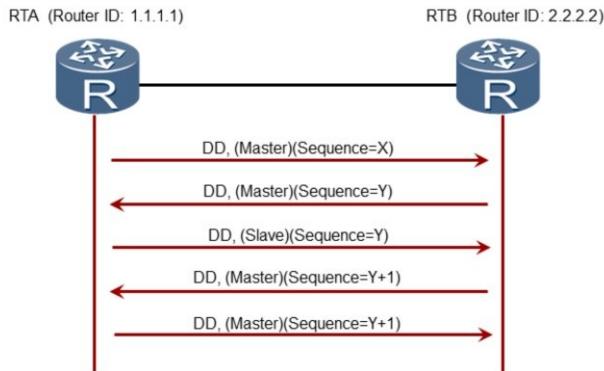


- Резервный назначенный маршрутизатор (BDR) создает смежности со всеми другими маршрутизаторами и становится DR, если существующий DR не работает.

Чтобы повысить эффективность перехода на новый назначенный маршрутизатор, для каждой сети вещания и NBMA назначается резервный назначенный маршрутизатор. Резервный маршрутизатор также находится рядом со всеми маршрутизаторами в сети и становится назначенным маршрутизатором, когда предыдущий назначенный маршрутизатор выходит из строя. Если бы не было резервных обозначенных маршрутизаторов, новые соединения должны были быть сформированы между новым назначенным маршрутизатором и всеми другими маршрутизаторами, подключенными к сети.

Часть процесса формирования смежности включает в себя синхронизацию баз данных состояния канала, что может занять довольно много времени. В течение этого времени сеть не будет доступна для передачи данных. Резервный назначенный маршрутизатор устраняет необходимость в создании этих примыканий, поскольку они уже существуют. Это означает, что период сбоев в транзитных перевозках продолжается только до тех пор, пока это требуется для наводнения новых LSA (которые объявляют новый назначенный маршрутизатор). Резервный назначенный маршрутизатор также выбирается пакетом Hello. В каждом пакете Hello есть поле, в котором указывается резервный назначенный маршрутизатор для сети.

Синхронизация базы данных



- Соседние маршрутизаторы формируют master/slave отношения
- Пакеты описания БД содержат информацию об LSA

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

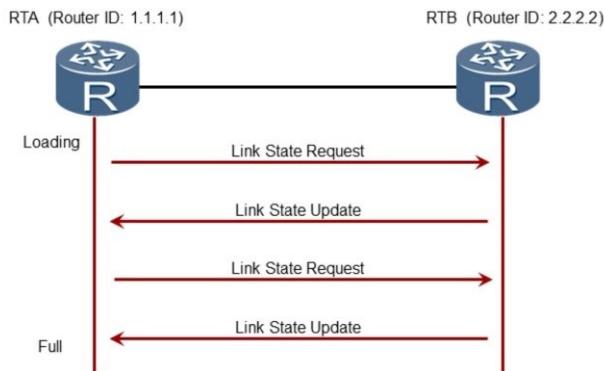
Page 16



В алгоритме маршрутизации состояния канала очень важно, чтобы все базы данных маршрутизаторов оставались синхронизированными. OSPF упрощает это, требуя, чтобы только соседние маршрутизаторы оставались синхронизированными. Процесс синхронизации начинается, как только маршрутизаторы пытаются выявить смежность. Каждый маршрутизатор описывает свою базу данных, отправляя последовательность пакетов описания базы данных своему соседу. Каждый пакет описания базы данных описывает набор LSA, принадлежащих базе данных маршрутизатора.

Когда сосед видит LSA, который является более поздним, чем его собственная копия базы данных, он отмечает, что этот новый LSA должен быть запрошен. Эта отправка и получение пакетов описания базы данных называется «процессом обмена базами данных». Во время этого процесса два маршрутизатора образуют отношение «ведущий / ведомый». Каждый пакет описания базы данных имеет порядковый номер. Пакеты с описание базы данных, отправленные ведущим, подтверждаются ведомым посредством эхо-номера порядкового номера.

Установление полной смежности



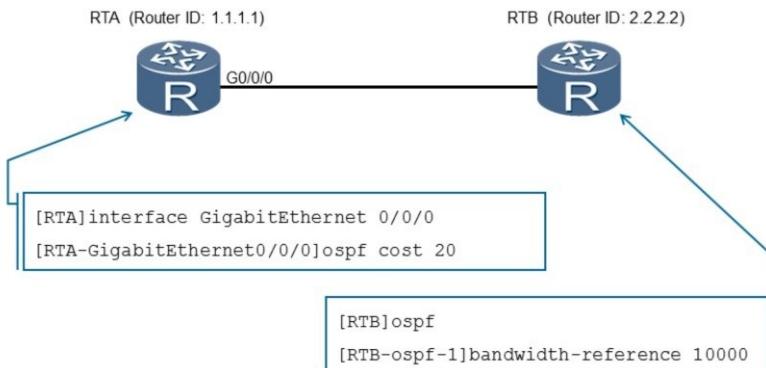
- Отсутствующие или более новые экземпляры LSA запрашиваются с помощью LSR.
- Весь запрошенный LSA отправляется как обновление.

Во время и после процесса обмена базами данных каждый маршрутизатор имеет список тех LSA, для которых у соседа есть более современные экземпляры. Пакет запроса состояния канала используется для запроса более актуальных частей базы данных соседа.

Пакеты обновления состояния канала реализуют наполнение LSA. Каждый пакет обновления состояния канала передает коллекцию LSA на один шаг дальше от их источника. Несколько LSA могут быть включены в один пакет. В широковещательных сетях пакеты обновления состояния канала являются многоадресными. IP-адрес назначения, указанный для пакета обновления состояния канала, зависит от состояния интерфейса. Если состояние интерфейса DR или Backup, следует использовать адрес AllSPFRouters (224.0.0.5). В противном случае следует использовать адрес AllIDRouters (224.0.0.6). В нешироковещательных сетях отдельные пакеты обновления состояния канала должны быть отправлены, как одноадресные, каждому соседнему соседу (т. е. В состоянии Exchange или выше). IP-адреса назначения для этих пакетов - это IP-адреса соседей.

Когда процесс описания базы данных завершен и все запросы состояния канала выполнены, базы данных считаются синхронизированными, а маршрутизаторы отмечены полностью смежными. В это время смежность полностью функциональна и анонсируется в двух маршрутизаторах LSA.

OSPF метрика



- Стоимость метрики основана на формуле 108/пропускная способность.
- Команда *bandwidth reference* повышает точность метрики.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 18

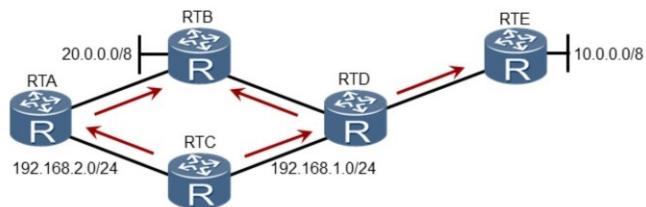


OSPF вычисляет стоимость интерфейса на основе пропускной способности интерфейса. Формула расчета: стоимость интерфейса = контрольное значение полосы пропускания/пропускной способности. Контрольное значение пропускной способности настраивается по умолчанию 100 Мбит/с. С формулой 100000000/пропускная способность это дает показатель стоимости 1562 для последовательного порта 64 кбит/с, 48 для интерфейса E1 (2.048 Мбит/с) и стоимость 1 для Ethernet (100 Мбит/с) или выше.

Чтобы иметь возможность отличать высокоскоростные интерфейсы, необходимо, чтобы метрика затрат была скорректирована в соответствии с поддерживаемыми в настоящий момент скоростями. Полоса пропускания ссылок команды позволяет изменение метрики путем изменения опорного значения ширины полосы в формуле затрат. Чем выше значение, тем точнее метрика. Там, где передача 10Gb в настоящее время поддерживается, рекомендуется, чтобы ширина полосы пропускания - контрольное значение была увеличена до «10000» или 1010/пропускная способность для обеспечения метрики 1, 10 и 100 для 10Gb, 1Gb и пропускной способности 100 Мбит соответственно.

В качестве альтернативы, стоимость может быть вручную настроена с помощью команды *ospf cost*, чтобы определить стоимость для данного интерфейса. Себестоимость составляет от 1 до 65535 со значением по умолчанию = 1.

Дерево кратчайших путей

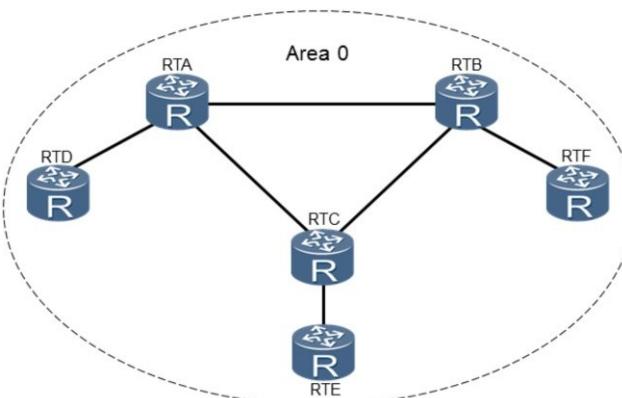


[RTC]display ip routing-table						
Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.0.0.0/8	OSPF	10	20	D	192.168.1.4	G0/0/0
20.0.0.0/8	OSPF	10	20	D	192.168.1.4	G0/0/0
	OSPF	10	20	D	192.168.2.1	G0/0/1

- Каждый маршрутизатор считает кратчайший путь ко всем другим сетям.

Предполагается, что маршрутизатор, достигший полного состояния, получил все анонсы (LSA) и синхронизировал базу данных состояния канала (LSDB) с смежными соседями. Информация о состоянии канала, собранная в базе данных состояний канала, затем используется для вычисления кратчайшего пути к каждой сети. Каждый маршрутизатор полагается только на информацию в LSDB, чтобы самостоятельно рассчитать кратчайший путь к каждому пункту назначения, а не полагаться на выбранную информацию маршрута от одноранговых узлов, который считается лучшим маршрутом к месту назначения. Однако вычисление кратчайшего пути дерева означает, что каждый маршрутизатор должен использовать дополнительные ресурсы для достижения этой операции.

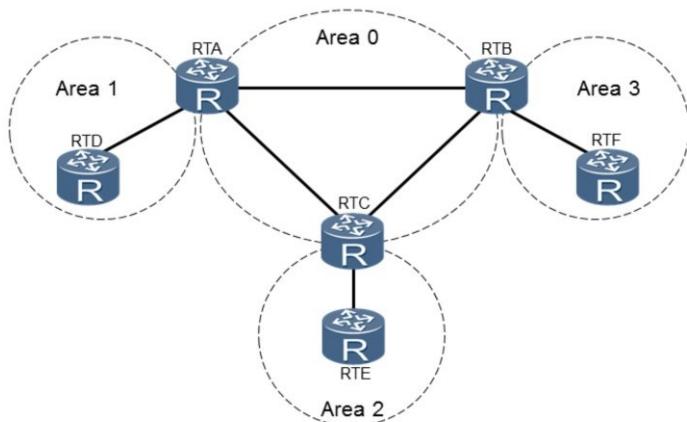
OSPF Области – Единая область



- Односвязное состояние БД для домена администратора
- Области может быть присвоен любой номер, но лучше 0

Меньшие сети могут включать в себя выбранное количество маршрутизаторов, которые работают как часть домена OSPF. Эти маршрутизаторы считаются частью области, которая представлена идентичной базой состояний связей для всех маршрутизаторов внутри домена. В качестве единой области OSPF может быть назначен любой номер области, однако для будущей реализации проекта рекомендуется, чтобы эта область была назначена как область 0.

OSPF Области – Много областей

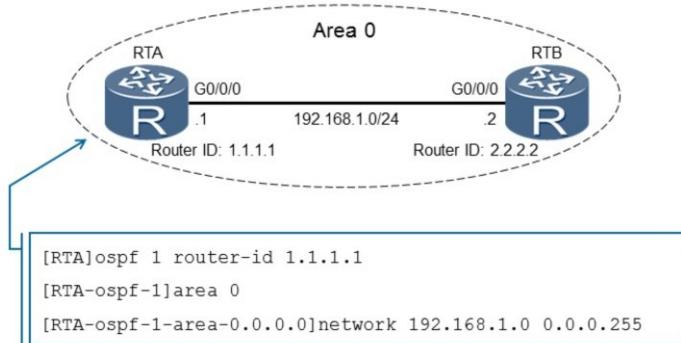


- Области строят раздельные LSDB, уменьшая трудности при изменении

Необходимость пересыпать анонсы состояний канала и последующий расчет кратчайшего пути на основе базы данных состояния связи становится все более сложной, поскольку все больше и больше маршрутизаторов становятся частью домена OSPF. Таким образом, OSPF способен поддерживать иерархическую структуру, чтобы ограничить размер базы данных состояния канала и количество вычислений, которое должно выполняться при определении кратчайшего пути к данной сети.

Реализация нескольких областей позволяет домену OSPF разделять процесс расчета на основе базы данных состояния канала, которая является не только идентичной для каждой области, но предоставляет информацию для охвата всех получателей в домене OSPF. Некоторые маршрутизаторы, известные как пограничные маршрутизаторы (ABR), работают между областями и содержат несколько баз данных состояний канала для каждой области, к которой подключен ABR. Область 0 должна быть сконфигурирована там, где существует OSPF с несколькими областями и для которой обычно требуется трафик, отправляемый между областями, чтобы обеспечить отсутствие циклов маршрутизации для прохождения области 0.

OSPF Сетевые анонсы



- Сетевые команды определяют сеть как анонсированную
- На основе областей анонсы пересыпаются по маршрутам

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 22



Создание OSPF в домене AS требует, чтобы каждый маршрутизатор, который должен участвовать в OSPF, сначала включал процесс OSPF. Это достигается с помощью команды `ospf [process id]`, где идентификатор процесса может быть назначен и обозначает собой процесс, с которым связан маршрутизатор. Если маршрутизаторам присвоены разные идентификационные номера процессов, будут созданы отдельные базы данных состояний ссылок на основе каждого индивидуального идентификатора процесса. Если идентификатор процесса не назначен, будет использоваться идентификатор процесса по умолчанию 1. Идентификатор маршрутизатора также может быть назначен с помощью команды `ospf [process ID] [router-id <router-id>]`, где `<router-id>` относится к идентификатору, который должен быть назначен маршрутизатору, учитывая, что более высокое значение идентификатора представляет собой DR в сетях вещания и NBMA.

Информация в скобках отражает процесс ospf и уровень, на котором могут быть настроены параметры ospf, включая область, к которой привязана каждая ссылка (или интерфейс). Сети, которые должны анонсироваться в данной области, определяются с помощью сетевой команды. Мaska представлена в виде маски подстановочного знака, для которой значение 0 представляет биты, которые являются фиксированными (например, сетевой идентификатор), и где значения бит в маске представляют значение 1, адрес может представлять любое значение.

Проверка конфигурации

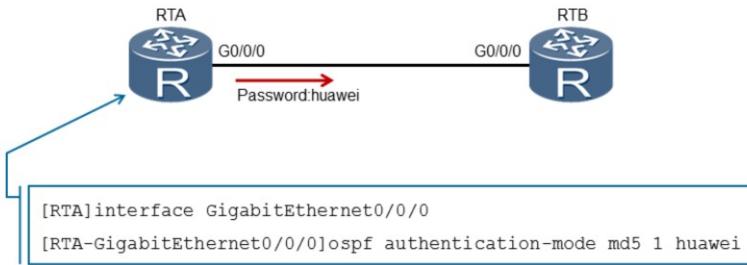
```
[RTA]display ospf peer

OSPF Process 1 with Router ID 1.1.1.1
    Neighbors

    Area 0.0.0.0 interface 192.168.1.1(GigabitEthernet0/0/0)'s neighbors
    Router ID: 2.2.2.2          Address: 192.168.1.2
        State: Full Mode:Nbr is Master Priority: 1
        DR: 192.168.1.2 BDR: 192.168.1.1 MTU: 0
        Dead timer due in 40 sec
        Retrans timer interval: 5
        Neighbor is up for 00:00:31
        Authentication Sequence: [ 0 ]
```

Конфигурация связи соседей между одноранговыми узлами OSPF проверяется с помощью команды *ospf peer*. Атрибуты, связанные с одноранговым соединением, перечислены, чтобы дать четкое объяснение конфигурации. Важные атрибуты включают область, в которой установлена ассоциация одноранговых узлов, состояние одноранговой организации, ассоциация master / slave для согласования смежности и достижения full состояния, а также назначения DR и BDR, которые подчеркивают, что связь ассоциируется с типом сети вещания.

OSPF Аутентификация



- OSPF поддерживает два вида аутентификации: простой пароль или зашифрованная аутентификация

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 24



OSPF способен поддерживать аутентификацию, чтобы гарантировать, что маршруты защищены от вредоносных действий, которые могут возникнуть в результате манипулирования или повреждения существующей топологии OSPF и маршрутов. OSPF позволяет использовать простую аутентификацию, а также криптографическую аутентификацию, которая обеспечивает повышенную защиту от возможных атак.

Аутентификация назначается для каждого интерфейса с помощью команды для простой аутентификации `ospf authentication-mode {simple [[plain] <plain-text> |] cipher <cipher-text>} | null}`, где `plain` применяет пароль с четким текстом, `cipher` пароль шифрованного текста, чтобы скрыть исходное содержимое, и `null`, чтобы указать нулевую аутентификацию.

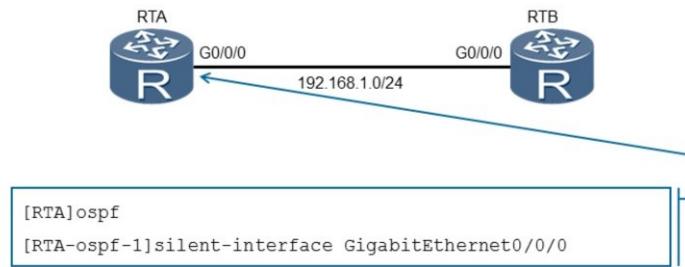
Криптографическая аутентификация применяется с использованием режима аутентификации `ospf {md5 | hmac-md5} [key-id {plain <plain-text> | [cipher] <cipher-text>}]`. MD5 представляет криптографический алгоритм для обеспечения аутентификации к каналу, с его конфигурацией, продемонстрированной в данном примере. Ключ идентифицирует уникальный key ID шифрованной аутентификации интерфейса. Идентификатор ключа должен соответствовать идентификатору партнера.

Проверка конфигурации

```
<RTA>terminal debugging
<RTA>debugging ospf packet
Aug 19 2013 08:10:06.850.2+00:00 RTA RM/6/RMDEBUG: Source Address:
192.168.1.1
Aug 19 2013 08:10:06.850.3+00:00 RTA RM/6/RMDEBUG: Destination
Address: 224.0.0.5
.....
Aug 19 2013 08:10:06.850.6+00:00 RTA RM/6/RMDEBUG: Area: 0.0.0.0,
Chksum: 0
Aug 19 2013 08:10:06.850.7+00:00 RTA RM/6/RMDEBUG: AuType: 02
Aug 19 2013 08:10:06.850.8+00:00 RTA RM/6/RMDEBUG: Key(ascii): * *
* * * * *
```

Если применяется аутентификация, можно реализовать отладку на терминале для просмотра процесса аутентификации. Поскольку отладка может включать в себя множество событий, команда *debugging ospf packet* должна использоваться для указания того, что отладка должна выполняться только для определенных пакетов OSPF. В результате процесс проверки подлинности можно просмотреть, чтобы подтвердить, что конфигурация аутентификации была успешно реализована.

OSPF скрытый интерфейс



- Команда *silent-interface* предотвращает формирование соседских отношений

Часто необходимо контролировать поток информации маршрутизации и ограничивать диапазон, для которого могут распространяться такие протоколы маршрутизации. Это особенно касается соединения с внешними сетями, от которых необходимо защищать знание внутренних маршрутов. Для достижения этой цели команда *silent-interface* может применяться как средство для ограничения всей связи OSPF через интерфейс, на котором выполняется эта команда.

После того как интерфейс OSPF установлен в состояние *silent*, интерфейс все равно может рекламировать свои прямые маршруты. Hello пакеты на интерфейсе, однако, будут заблокированы и никакие отношения соседей не будут установлены на интерфейсе. Команда *silent-interface [interface-type interface-number]* может использоваться для определения определенного интерфейса, который должен ограничивать работу OSPF, или, как альтернатива, команда может использоваться для обеспечения того, чтобы все интерфейсы под определенным процессом были ограничены от участия в OSPF.

Проверка конфигурации

```
[RTA]display ospf 1 interface GigabitEthernet0/0/0

OSPF Process 1 with Router ID 1.1.1.1
    Interfaces

    Interface: 192.168.1.1 (GigabitEthernet0/0/0)
        Cost: 1      State: DR      Type: Broadcast      MTU: 1500
        Priority: 1
        Designated Router: 192.168.1.1
        Backup Designated Router: 0.0.0.0
        Timers: Hello 10 , Dead 40 , Poll 120 , Retransmit 5 , Transmit
        Delay 1
    Silent interface, No hellos
```

Внедрение *silent* интерфейса на основе интерфейса означает, что должен соблюдаться конкретный интерфейс для проверки успешного применения команды бесшумного интерфейса. Через команду *ospf <process_id> interface <interface> display*, где *interface* представляет собой интерфейс, к которому применяется команда *silent-interface*, можно проверить реализацию *silent* интерфейса.



Итоги:

- Какая цель у dead интервала в OSPF?
- В широковещательной сети, используются назначенный маршрутизатор (DR - Designated Router) и резервный назначенный маршрутизатор (BDR - Backup Designated Router) для прослушивания информации о состоянии состояния ссылки?

1. Dead интервал - это значение таймера, которое используется для определения того, прекращено ли распространение пакетов OSPF Hello. Это значение эквивалентно четырем интервалам Hello или 40 секундам по умолчанию в широковещательных сетях. В случае, если мертвый интервал отсчитывается до нуля, отношения соседства OSPF будут прекращены.
2. DR и BDR используют многоадресный адрес 224.0.0.6 для прослушивания обновлений состояния связи, когда тип сети OSPF определяется как широковещательный.



Thank you

www.huawei.com

Принципы DHCP протокола

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

Корпоративная может часто состоять из значительного числа хостов, каждый из которых требует сетевых параметров в виде IP-адресации и дополнительную информацию о конфигурации сети. Распределение вручную часто утомительный и неточный процесс, который может привести к тупикам, связанных с дублированием адреса или неспособностью достичь необходимых услуг для бесперебойной работы сети. DHCP - это протокол уровня приложения, который предназначен для автоматизации процесса предоставления информации о конфигурации для клиентов в сети TCP/IP. Таким образом, DHCP помогает обеспечить правильную адресацию, и уменьшает нагрузку на администрирование для всех корпоративных сетей. Этот раздел представляет применение DHCP в корпоративной сети.

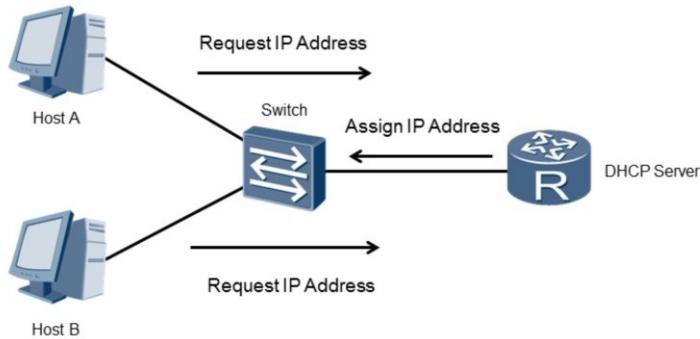


Цели

После изучения этой главы вы сможете:

- Описать функцию DHCP в корпоративной сети.
- Объяснить процесс аренды DHCP
- Сконфигурировать DHCP пулы для аренды адресов.

Применение DHCP в корпоративной сети



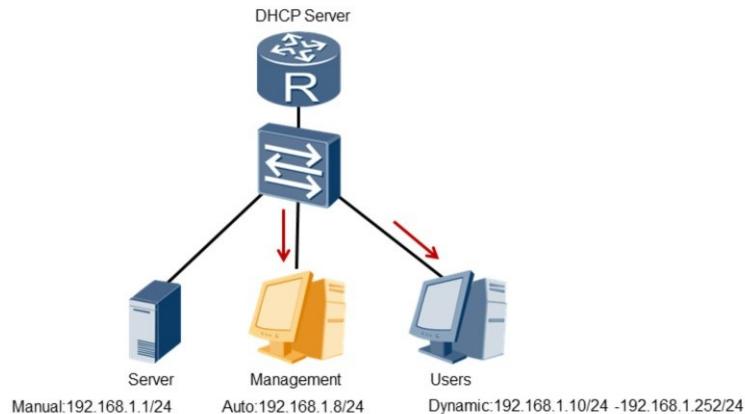
Сети, состоящие из большого числа пользователей, требуют наличия центральной системы управления распределением IP-адресов.

Корпоративные сети часто состоят из нескольких конечных систем, которым требуется назначение IP-адреса для подключения к сегменту сети, к которому присоединена конечная система. Для небольших сетей минимальное количество конечных систем, подключенных к сети, позволяет просто управлять адресацией для всех конечных систем.

Однако для средних и крупных сетей становится все труднее вручную настраивать IP-адреса с повышенной вероятностью дублирования адресации, а также ошибочной конфигурации из-за человеческой ошибки, и поэтому необходимость внедрения централизованного решения управления по всей сети становится все более заметным. Протокол Динамического Конфигурирования Хостов (DHCP - Dynamic Host Configuration Protocol) реализуется как решение для управления, позволяющее динамическое распределение адресов для существующих фиксированных и временных конечных систем, обращающихся к сетевому домену.

Также возможно, что в сети может быть больше хостов, чем доступных IP-адресов. Некоторым хостам не может быть назначен фиксированный IP-адрес и необходимо динамически получать IP-адреса с помощью DHCP-сервера. Только несколько хостов в сети требуют фиксированных IP-адресов.

Механизмы распределения адресов



- DHCP поддерживает три механизма распределения IP адресов

DHCP поддерживает три механизма распределения IP-адресов. Метод автоматического распределения включает DHCP, назначающий постоянный IP-адрес клиенту. Динамическое распределение использует DHCP для назначения IP-адреса клиенту в течение ограниченного периода времени или, по крайней мере, до тех пор, пока клиент явно не удалит IP-адрес.

Третий механизм называется ручным распределением, для которого IP-адрес клиента назначается сетевым администратором, а DHCP используется только для обработки назначения вручную определенного адреса клиенту. Динамическое распределение - это единственный из трех механизмов, который позволяет автоматически повторно использовать адрес, который больше не нужен клиенту, которому он был назначен. Таким образом, динамическое распределение особенно полезно для назначения адреса клиенту, который будет подключен к сети только временно, или для совместного использования ограниченного пула IP-адресов среди группы клиентов, которым не нужны постоянные IP-адреса.

Динамическое распределение также может быть хорошим выбором для назначения IP-адреса новому клиенту, постоянно подключенному к сети, где IP-адресов недостаточно, а адреса могли бы восстанавливаться при удалении старых клиентов. Ручное распределение позволяет использовать DHCP для устранения подверженного ошибкам процесса ручной настройки хостов с IP-адресами в средах, где может быть более желательным тщательное управление назначением IP-адресов.

DHCP сообщения

Message Types	Function
DHCP DISCOVER	Трансляция клиента используется для поиска доступных DHCP-серверов.
DHCP OFFER	Сервер отвечает на DHCPDISCOVER предложением конфигурации параметров.
DHCP REQUEST	Клиентское сообщение серверам: (а) запрошенные параметры с одного сервера и отклонение предложений от всех остальных, (б) подтверждение правильности ранее назначенного адреса после, например, перезагрузки системы, (с) расширение аренды по определенному сетевому адресу.
DHCP ACK	Подтверждение от сервера, отправленное клиенту с конфигурацией параметров, включая фиксированный сетевой адрес.
DHCP NAK	Сервер указывает клиенту, что сетевой адрес не может быть назначен.
DHCP RELEASE	Клиент отказывается от сетевого адреса на сервере и отменяет оставшуюся аренду.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 6



DHCP сервер и DHCP клиент взаимодействуют друг с другом, обмениваясь разными типами сообщений. Первоначальная связь зависит от передачи сообщения DHCP Discover. Оно передается клиентом DHCP, чтобы найти DHCP-сервер, когда клиент пытается подключиться к сети в первый раз. Сообщение DHCP Offer затем отправляется DHCP-сервером для ответа на сообщение DHCP Discover и содержит информацию о конфигурации.

Сообщение DHCP Request отправляется после инициализации DHCP-клиента, в котором он передает сообщение DHCP Request, чтобы ответить на сообщение DHCP Offer, отправленное DHCP сервером. Сообщение DHCP Request также отправляется после перезапуска клиента DHCP, и в это время он передает сообщение для подтверждения конфигурации, например назначенного IP-адреса. Сообщение DHCP Request также отправляется после того, как клиент DHCP получает IP-адрес, чтобы продлить аренду IP-адреса.

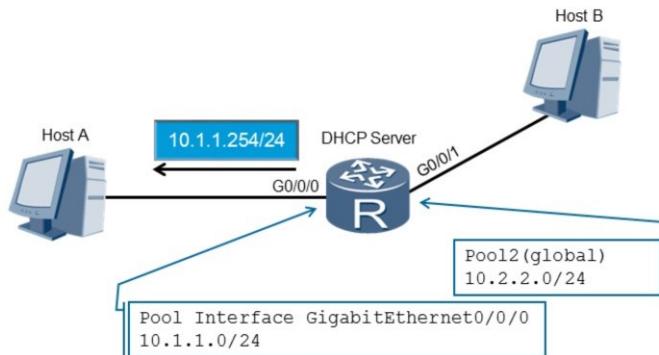
DHCP ACK сообщение отправляется сервером DHCP для подтверждения сообщения DHCP Request от клиента DHCP. После получения сообщения ACK DHCP клиент DHCP получает параметры конфигурации, включая IP-адрес. Однако не все случаи приведут к назначению IP-адреса клиенту. Сообщение DHCP NAK отправляется DHCP-сервером, чтобы отклонить сообщение DHCP Request от клиента DHCP, когда истекает IP-адрес, предназначенный клиенту DHCP, или в случае, если клиент DHCP переместится в другую сеть.

Сообщение DHCP Decline отправляется клиентом DHCP, чтобы уведомить DHCP сервер, что назначенный IP-адрес конфликтует с другим IP-адресом. Затем клиент DHCP будет применяться к DHCP серверу для другого IP-адреса.

Сообщение DHCP Release отправляется клиентом DHCP для выпуска его IP-адреса. После получения сообщения DHCP Release, DHCP сервер назначает этот IP-адрес другому клиенту DHCP.

Финальным типом сообщения является сообщение DHCP Inform, и оно отправляется клиентом DHCP для получения другой информации о конфигурации сети, такой как адрес шлюза и адрес DNS-сервера после того, как клиент DHCP получил IP-адрес.

Пул адресов



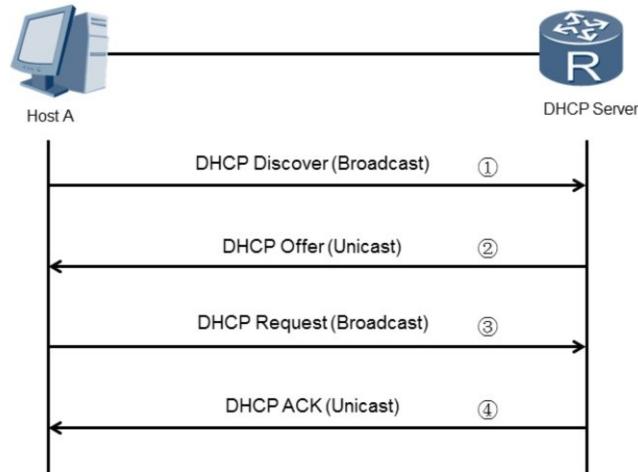
- Пул адресов может быть либо глобальным, либо интерфейсным

Устройства серии AR2200 и S5700 могут работать как DHCP сервер, для назначения IP-адресов пользователям сети. Пулы адресов используются для определения адресов, которые должны быть назначены конечным системам. Существует две общие формы пулов адресов, которые могут использоваться для распределения адресов, глобального пула адресов и пула адресов интерфейса.

Использование пула адресов интерфейса позволяет только конечным системам подключаться к одному и тому же сегменту сети, как и интерфейс, который будет выделен IP-адресами из этого пула. Объединенный глобальный адресный пул, который был сконфигурирован, позволяет всем конечным системам, связанным с сервером, получать IP-адреса из этого пула адресов с помощью глобальной команды `dhcp select interface` для определения глобального пула адресов. В случае пула адресных интерфейсов команда интерфейса выбора `dhcp` идентифицирует интерфейс и сегмент сети, с которыми связан пул адресов интерфейса.

Пул адресов интерфейса имеет приоритет над глобальным пулом адресов. Если пул адресов настроен на интерфейс, клиенты, подключенные к интерфейсу, получают IP-адреса из пула адресов интерфейса, даже если настроен пул глобальных адресов. На коммутаторе S5700 можно настраивать только логические интерфейсы VLANIF с пулами интерфейсных адресов.

DHCP получение адреса



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 8



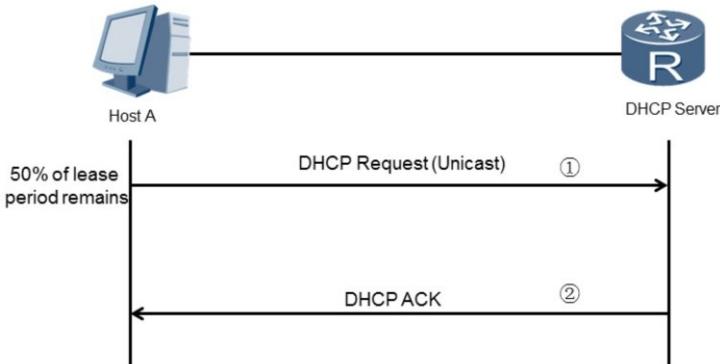
Получение IP-адреса и другой конфигурационной информации требует, чтобы клиент вступил в контакт с DHCP-сервером и получил через запрос информацию адресации, чтобы стать частью IP-домена. Этот процесс начинается с процесса обнаружения IP, в котором клиент DHCP выполняет поиск DHCP-сервера. Клиент DHCP передает сообщение DHCP Discover, а DHCP-сервер отвечает на него.

Открытие одного или нескольких серверов DHCP приводит к тому, что каждый DHCP-сервер, предлагается IP-адрес клиенту DHCP. После получения сообщения DHCP Discover каждый DHCP-сервер выбирает неназначенный IP-адрес из пула IP-адресов и отправляет клиенту предложение о предоставлении DHCP-предложения с назначенным IP-адресом и другой информацией о конфигурации.

Если несколько DHCP-серверов отправляют клиенту сообщения о предоставлении DHCP-предложения, сначала клиент принимает сообщение DHCP Offer. Затем клиент передает сообщение DHCP Request с выбранным IP-адресом. После получения сообщения DHCP Request, сервер DHCP, который предлагает IP-адрес, отправляет DHCP-ACK сообщение DHCP-клиенту. Сообщение ACK DHCP содержит предлагаемый IP-адрес и другую информацию о конфигурации.

Получив сообщение ACK DHCP, клиент DHCP транслирует безвозвратные ARP-пакеты, чтобы определить, использует ли какой-либо хост IP-адрес, выделенный DHCP-сервером. Если ответ не получен в течение указанного времени, то клиент DHCP использует этот IP-адрес. Если хост использует этот IP-адрес, клиент DHCP отправляет пакет DHCP Decline на сервер DHCP, сообщая, что IP-адрес не может использоваться, после чего DHCP-клиент применяет другой IP-адрес.

DHCP Продление аренды



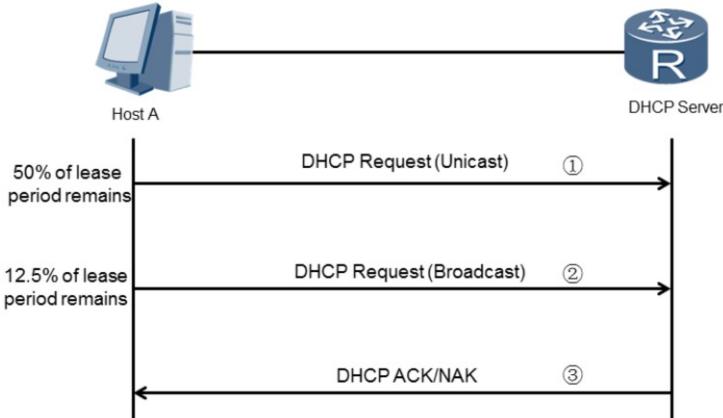
- DHCP начинает процесс продления аренды IP, когда осталось <50% времени аренды

После получения IP-адреса клиент DHCP переходит в связанное привязки. Три таймера устанавливаются клиентом DHCP для управления обновлением аренды, переконфигурации аренды и сроком аренды. При назначении IP-адреса клиенту, сервер DHCP задает значения для таймеров.

Если DHCP-сервер не устанавливает значения для таймеров, клиент DHCP использует значения по умолчанию. Значения по умолчанию определяют, что, когда остается 50% периода аренды, должен начаться процесс продления срока действия, для которого ожидается, что клиент DHCP возобновит аренду своего IP-адреса. Клиент DHCP автоматически отправляет сообщение DHCP Request на сервер DHCP, который назначил IP-адрес клиенту DHCP.

Если IP-адрес действителен, DHCP-сервер отвечает сообщением ACK DHCP, чтобы предоставить клиенту DHCP новый договор аренды, а затем клиент повторно переходит в состояние привязки. Если клиент DHCP получает сообщение NAK DHCP с сервера DHCP, он переходит в состояние инициализации.

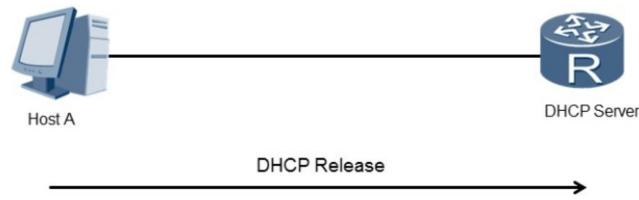
DHCP Повторная сборка



Пересборка начинается, если процесс аренды не был продлен вовремя

После того как DHCP-клиент отправит сообщение DHCP Request для продления аренды, клиент DHCP останется в состоянии обновления и будет ждать ответа. Если клиент DHCP не получает ответ DHCP Reply с сервера DHCP после истечения таймера перезаписи сервера DHCP, который по умолчанию возникает, когда остается 12,5% периода аренды, клиент DHCP предполагает, что исходный DHCP-сервер недоступен и начинает транслировать сообщение DHCP Request, для которого любой DHCP-сервер в сети может отвечать сообщением ACK DHCP или NAK. Если полученное сообщение является сообщением ACK DHCP, клиент DHCP возвращается в состояние привязки и сбрасывает таймер продления срока аренды и таймер привязки сервера. Если все принятые сообщения являются сообщениями DHCP NAK, клиент DHCP возвращается в состояние инициализации. В это время клиент DHCP должен немедленно прекратить использование этого IP-адреса и запросить новый IP-адрес.

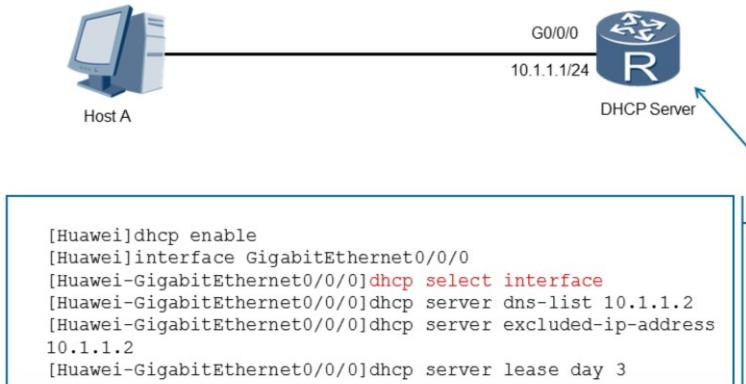
Освобождение IP адреса



- DHCP освободить IP адрес, если клиент не обновит IP адрес, до истечения срока аренды.

Таймер аренды - это финальный таймер в процессе истечения срока действия, и если клиент DHCP не получит ответ до истечения срока действия лимита аренды, клиент DHCP должен немедленно прекратить использование текущего IP-адреса и вернуться в состояние инициализации. Затем клиент DHCP отправляет сообщение DHCP DISCOVER для подачи заявки на новый IP-адрес, тем самым перезапуская DHCP цикл.

DHCP интерфейс конфигурации пула



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 12



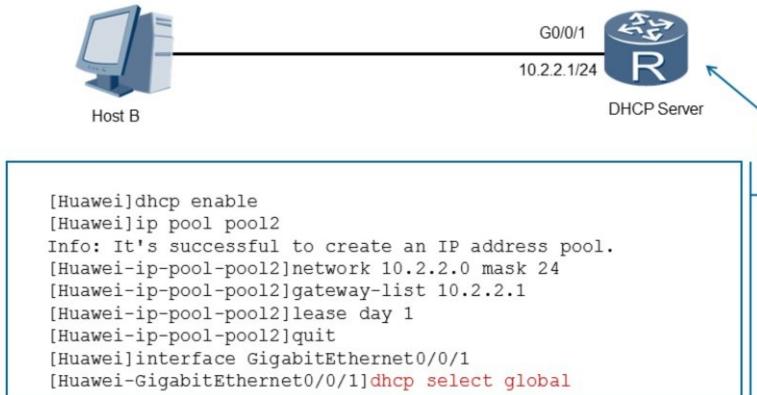
Существуют две формы конфигурации пула, которые поддерживаются в DHCP: определение глобального пула или пула интерфейса. Команда *dhcp select interface* используется для связывания интерфейса с пулом адресов интерфейса, чтобы предоставить информацию о конфигурации подключенным хостам. В этом примере демонстрируется, как интерфейс Gigabit Ethernet 0/0/0 был назначен как часть пула адресных интерфейсов.

DHCP Проверка конфигурации

```
[Huawei]display ip pool interface GigabitEthernet0/0/0
  Pool-name      : GigabitEthernet0/0/0
  Pool-No       : 0
  Lease         : 3 Days 0 Hours 0 Minutes
  Domain-name   : huawei.com
  DNS-Server0   : 10.1.1.2
  NBNS-Server0  : -
  Netbios-type  : -
  Position      : Interface      Status      : Unlocked
  Gateway-0     : 10.1.1.1
  Mask          : 255.255.255.0
  VPN instance  : --
  -----
  Start        End      Total Used  Idle(Expired) Conflict Disable
  -----
  10.1.1.1    10.1.1.254 253    1      251(0)      0      1
```

Каждый DHCP-сервер будет определять один или несколько пулов, которые могут быть связаны глобально или с данным интерфейсом. Для определения атрибутов пула, связанных с интерфейсом, используется команда *display ip pool interface <interface>*. Пул DHCP будет содержать информацию, включая период аренды для каждого арендуемого IP-адреса, а также поддерживаемый диапазон пулов. В случае, если поддерживаются другие атрибуты для распространения DHCP для клиентов, таких как шлюз IP, маска подсети и DNS-сервер, они также будут отображаться.

DHCP Конфигурация глобального пула



- Создание пула адресов и связанных параметров реализовано на DHCP сервере.

В этом примере показана конфигурация DHCP для глобального пула адресов, который назначается для сети 10.2.2.0. Команда `enable dhcp` является обязательным условием для настройки функций, связанных с DHCP, и вступает в силу только после запуска команды `dhcp enable`. DHCP-сервер требует, чтобы команда `ip pool` была настроена в системном представлении, чтобы создать пул IP-адресов и задать параметры пула IP-адресов, включая адрес шлюза, период аренды IP-адреса и т. д. Затем настроенный DHCP-сервер может назначать IP-адреса в пул IP-адресов для клиентов.

DHCP-сервер и его клиент могут находиться в разных сегментах сети. Чтобы клиент мог взаимодействовать с DHCP-сервером, команда `gateway-list` используется для указания адреса исходящего шлюза для глобального пула адресов DHCP-сервера. Затем DHCP-сервер может назначить клиенту как IP-адрес, так и указанный адрес выходного шлюза. Адрес сконфигурирован в десятичной системе с точками, для которой можно настроить максимум восемь адресов шлюза, разделенных пробелами.

DHCP Проверка конфигурации

```
[Huawei]display ip pool
-----
Pool-name      : pool2
Pool-No       : 0
Position       : Local          Status        : Unlocked
Gateway-0     : 10.2.2.1
Mask          : 255.255.255.0
VPN instance   : --
IP address Statistic
Total         :253
Used          :1           Idle        :252
Expired       :0           Conflict    :0           Disable  :0
```

Информацию о пуле можно также узнать с помощью команды *display ip pool*. Эта команда предоставит обзор общих параметров конфигурации, поддерживаемых настроенным пулом, включая маску шлюза и подсети для пула, а также общую статистику, которая позволяет администратору отслеживать текущее использование пула, определять количество выделенных адресов, наряду с другой статистикой использования.



Итоги:

- Какие IP адреса должны быть исключены из пула адресов?
- Каково значение периода аренды IP адреса по умолчанию?

1. IP-адреса, используемые для распределения сервером, также как любые локальные DNS-серверы, чтобы избежать конфликтов адресов.
2. Период аренды по умолчанию для назначенных DHCP IP-адресов равен одному дню.



Thank you

www.huawei.com

Принципы FTP протокола

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

Раннее развитие стандартов внесло основы протокола передачи данных, с целью содействия обмену файлами между удаленными местами, на которые не повлияли изменения в файловых хранилищах между хостами. В результате FTP приняли как часть пакета протоколов TCP / IP. Служба FTP остается неотъемлемой частью сетей в качестве приложения для обеспечения надежной и эффективной передачи данных, обычно реализуемая для эффективного резервного копирования и извлечение файлов и журналов, тем самым улучшая общее управление корпоративной сетью. Поэтому в этом разделе вводится средства для инженеров и администраторов для реализации FTP-сервисов в продуктах Huawei.

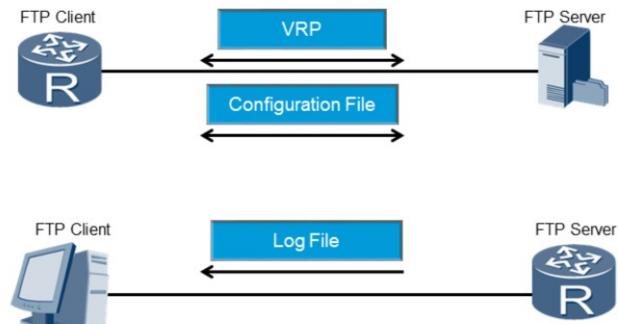


Цели

После изучения этой главы вы сможете:

- Объяснить процесс передачи файлов в FTP.
- Конфигурировать FTP сервис на поддерживаемых Huawei устройствах

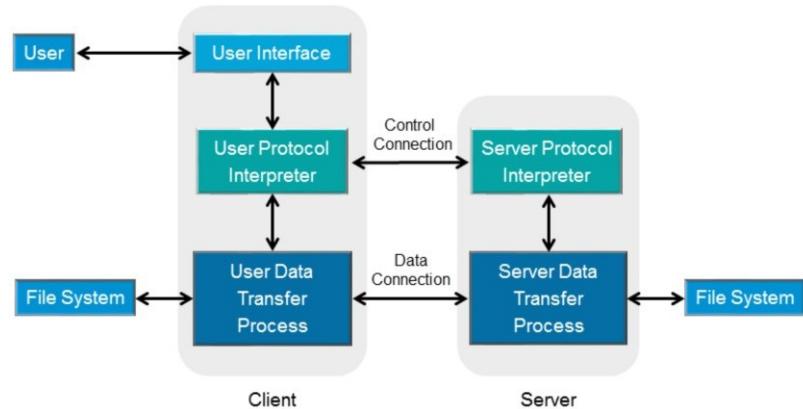
Применение FTP в корпоративных сетях



- FTP предоставляет эффективные средства для резервного копирования и восстановления важных файлов

Реализация FTP-сервера в корпоративной сети позволяет эффективно выполнять резервное копирование и восстановление важных системных и пользовательских файлов, которые могут использоваться для поддержания ежедневной работы корпоративной сети. Типичные примеры использования FTP-сервера включают резервное копирование и восстановление файлов изображений VRP и файлов конфигурации. Это также может включать в себя восстановление файлов журнала с FTP-сервера для отслеживания произошедшей активности FTP.

FTP процесс передачи файлов

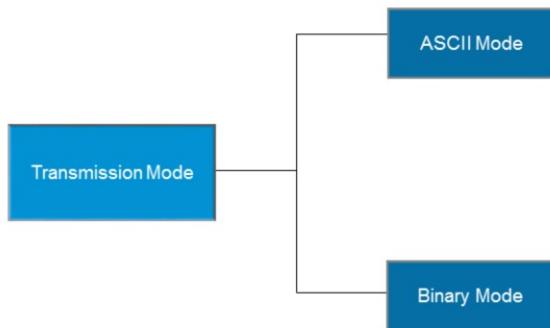


- FTP работает на двух TCP соединениях для передачи файлов

Передача файлов FTP зависит от двух TCP-соединений. Первым из них является управляющее соединение, которое устанавливается между FTP-клиентом и FTP-сервером. Сервер разрешает общий порт 21, а затем ожидает запроса соединения от клиента. Затем клиент отправляет запрос на настройку соединения с сервером. Контрольное соединение всегда ожидает связи между клиентом и сервером, передает связанные команды от клиента на сервер, а также ответы от сервера на клиента.

Сервер использует порт TCP 20 для data соединения. Как правило, сервер может активно открывать или закрывать подключение к данным. Однако для файлов, отправленных с клиента на сервер в виде потоков, только клиент может закрыть data соединение. FTP передает каждый файл в потоках, используя индикатор конца файла (EOF - End Of File), чтобы идентифицировать конец файла. Поэтому для каждого файла или списка каталогов необходимо передать новое соединение. Когда файл передается между клиентом и сервером, он указывает, что настроено соединение с данными.

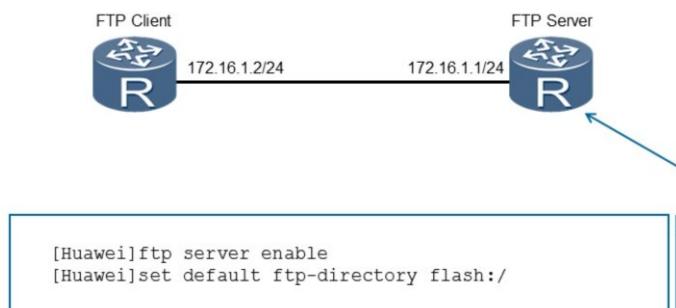
FTP базовые концепты



- Режимы передачи данных определяют формат данных до их обмена между отправителем и получателем

Существует два режима передачи FTP, которые поддерживаются Huawei, это режим ASCII и двоичный режим. Режим ASCII используется для текста, в котором данные преобразуются из символьного представления отправителя в «8-разрядный код ASCII» перед передачей. Проще говоря, символы ASCII используются для разделения символов возврата из линейных каналов. В двоичном режиме отправитель отправляет каждый байт файла за байтом. Этот режим часто используется для передачи файлов изображений и файлов программ, для которых символы могут передаваться без преобразования формата.

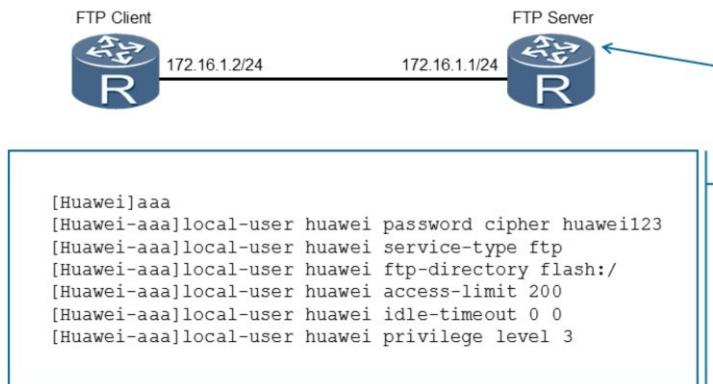
FTP Обслуживание



- Служба FTP должна быть включена и FTP-каталог по умолчанию работал в режиме обработки файлов

Реализация службы FTP достигается как на маршрутизаторе серии AR2200, так и на коммутаторе серии S5700, для которого услуга может быть активирована с помощью команды *enable ftp server*. После включения функции FTP-сервера пользователи могут управлять файлами в режиме FTP. Команда *set default ftp-directory* устанавливает рабочий каталог по умолчанию для пользователей FTP. Если не установлен рабочий каталог по умолчанию FTP, пользователь не сможет войти в маршрутизатор, и ему будет сообщено, что у пользователя нет полномочий на доступ к любому рабочему каталогу.

FTP Создание пользовательских сервисов



Учетные записи пользователей реализованы для идентификации пользователей и имеют индивидуальные разрешения для каждого пользователя отдельно.

Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 8

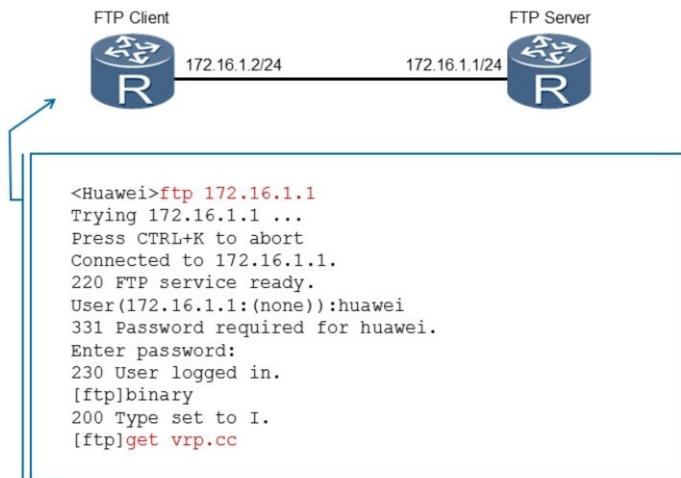


Доступ к службе FTP может быть достигнут путем назначения индивидуального входа пользователя для управления доступом. AAA используется для настройки локальной аутентификации и авторизации. После ввода AAA локальный пользователь может быть создан путем определения учетной записи пользователя и пароля. Учетная запись способна связываться с различными службами, которые задаются с помощью команды *service-type*, чтобы разрешить тип службы ftp для поддержки AAA.

Если каталог ftp пользователя должен отличаться от каталога по умолчанию, команда *ftp-directory* может использоваться для указания каталога для пользователя. Если количество активных подключений, доступных с локальной записью пользователя, должно быть ограничено, можно применить команду ограничения доступа *access-limit*. Значение варьироваться от 1 до 800 или неограниченно, если ограничение доступа не применяется.

Конфигурация тайм-аута простоя помогает предотвратить несанкционированный доступ в случае, если пользовательское окно сеанса остается бездействующим в течение определенного периода времени. Команда *idle timeout* определяется в минутах и секундах, при этом тайм-аут ожидания 0 0 означает, что период таймаута не применяется. Наконец, уровень привилегий определяет разрешенный уровень пользователя с точки зрения команд, которые могут применяться при установлении сеанса ftp. Это можно установить для любого уровня от 0 до 15, причем большее значение указывает на более высокий уровень пользователя.

FTP Конфигурация пользователя



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 9



После настройки службы FTP на FTP-сервере пользователи могут установить соединение между клиентом и сервером. С помощью команды *ftp* на клиенте будет установлен сеанс, через который аутентификация AAA будет использоваться для проверки пользователя. При правильной аутентификации клиент сможет настраивать, а также отправлять/извлекать файлы на FTP-сервер и с него.



Итоги:

- Какие порты необходимы для работы службы FTP?
- Считается, что пользователь не имеет права доступа к любой рабочей директории. Какие шаги необходимы для решения этой проблемы?

1. Чтобы соединение управления и соединения data службы FTP было установлено успешно, должны быть включены TCP-порты 20 и 21.
2. Если у пользователя нет полномочий на доступ к любому рабочему каталогу, необходимо определить каталог FTP по умолчанию. Это делается с помощью команды `set default ftp-directory <directory location>`, где имя каталога может быть, например, системной директорией.



Thank you

www.huawei.com

Принципы Telnet протокола

HUAWEI TECHNOLOGIES CO., LTD.





Предисловие

По мере расширения корпоративной сети поддерживаемые устройства могут существовать несмотря на огромные географические расстояния между ними и все они требует администрирования. Кроме того, администрирование сети часто происходит из централизованного управления, из которого все устройства контролируются. Чтобы облегчить администрирование был разработан telnet-протокол, один из самых ранних изобретенных протоколов, применяемый для управления устройствами. Принципы, касающиеся протокола и его внедрение представлены в этом разделе.

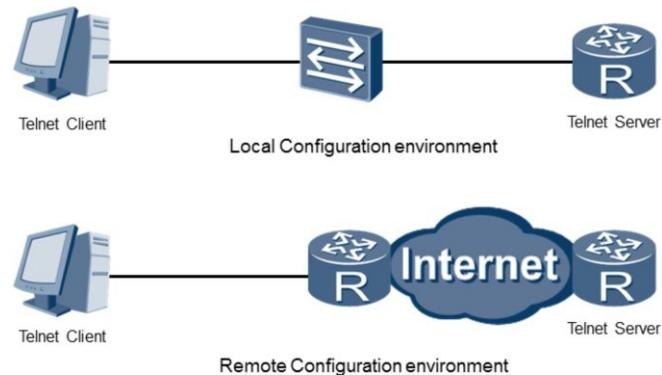


Цели

После изучения этой главы вы сможете:

- Объяснить применение и принципы telnet
- Установить telnet сервис на поддерживаемых Huawei устройствах

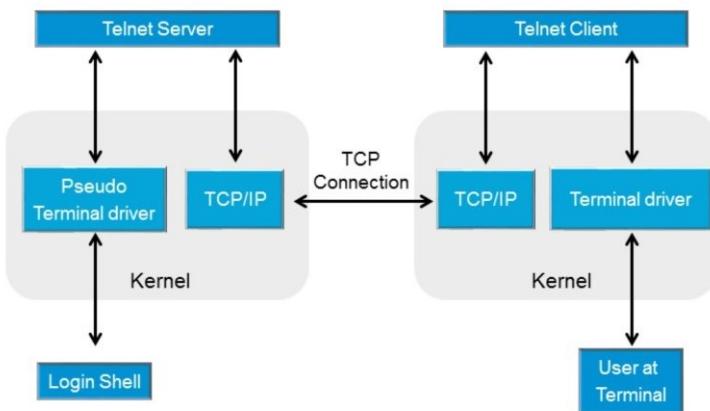
Telnet Применение



Telnet представляет собой эмуляцию терминала на основе дву направленного текстового терминала программы для использования через локальные и удаленные сети.

Протокол телекоммуникационной сети (Telnet) позволяет терминалу удаленно регистрироваться на любом устройстве, которое может работать как сервер telnet, и обеспечивает интерактивный рабочий интерфейс, посредством которого пользователь может выполнять операции таким же образом, как это достигается локально посредством консольного соединения. Удаленные хосты не должны подключаться напрямую к аппаратным терминалам, что позволяет вместо этого использовать преимущества возможностей IP для удаленного управления устройствами практически из любого места в мире.

Telnet Модель Клиент/Сервер



- Архитектура Telnet демонстрирует, как пользовательские нажатия клавиш интерпретируются терминальными драйверами перед доставкой через TCP.

Telnet работает по принципу модели клиент/сервер, для которого установлено telnet TCP-соединение между портом пользователя и портом telnet сервера, который по умолчанию назначается как порт 23. Сервер контролирует этот хорошо известный порт для таких соединений. TCP-соединение является полнодуплексным и идентифицируется портами источника и назначения. Сервер может участвовать во многих одновременных соединениях с его хорошо известными портом и пользовательскими портами, которые назначаются из не известного диапазона портов.

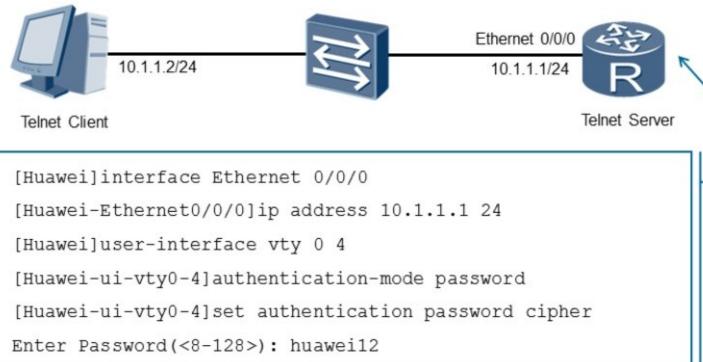
Драйверы терминала telnet интерпретируют нажатия клавиш пользователей и переводят их на универсальный набор символов, основанный на сетевом виртуальном терминале (NVT), который работает как форма виртуальный посредник между системами, после чего передача через соединение TCP/IP на сервер выполняется. Сервер декодирует символы NVT и передает декодированные символы в псевдотерминалный драйвер, который нужен, чтобы позволить операционной системе принимать декодированные символы.

Режим аутентификации

Authentication Mode	Description
None	Вход без аутентификации
AAA	AAA аутентификация
Password	Аутентификация с паролем пользователя интерфейса терминала

Доступ к службе telnet обычно включает аутентификацию пользователя для получения доступа. Существует три основных режима, которые определены для аутентификации telnet.

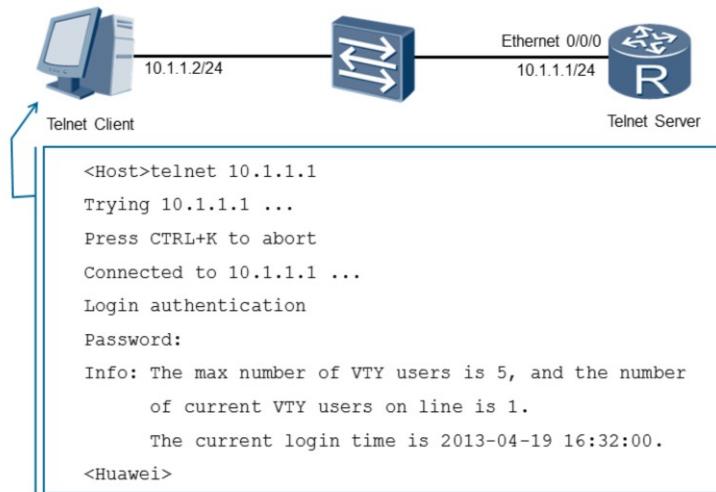
Telnet Конфигурация



- Telnet требует аутентификации для виртуального текстового интерфейса перед установкой соединения.

Устройство, работающее в качестве сервера telnet, обычно использует общую схему аутентификации пароля, которая используется для всех пользователей, подключающихся к пользовательскому интерфейсу vty. Как только IP-соединение устанавливается через подходящую схему адресации, команда *authentication-mode password* используется для диапазона vty вместе с паролем, который будет использоваться.

Telnet Конфигурация



Copyright © 2016 Huawei Technologies Co., Ltd. All rights reserved.

Page 8



После настройки удаленного устройства, которое должно работать как сервер telnet, клиент может установить telnet-соединение через команду `telnet` и получить приглашение для аутентификации. Пароль аутентификации должен соответствовать паролю, реализованному на сервере telnet, как часть предварительной настройки аутентификации пароля. Затем пользователь сможет установить удаленное соединение через telnet с удаленным устройством, работающим в качестве сервера telnet, и эмулировать командный интерфейс на локальном telnet-клиенте.



Итог

- Если служба telnet включена, но пользователь не может установить соединение telnet, в чем может быть причина?

1. Если пользователь не может установить telnet-соединение, пользователь должен убедиться, что устройство, поддерживающее службу telnet, доступно. Если устройство доступно, необходимо проверить пароль. Если пароль правильный, необходимо проверить количество пользователей, которые в настоящее время обращаются к устройству через telnet. Если необходимо расширить число пользователей, получающих доступ к устройству через telnet, следует использовать команду user-interface maximum-vty <0-15>, где 0-15 обозначает количество поддерживаемых пользователей.



Thank you

www.huawei.com