Основные сведения о среде передачи

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

Организация корпоративной сети требует знания и понимания общих принципов построения сетей. Сюда относится и само понятие «сеть» и знание общих стандартов технологий и физических компонентов, которые используются для построения корпоративных сетей. Понимание того, как передаются данные по сети и как это физически реализуется в действующей сети имеет первостепенное значение для эффективной реализации связи.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

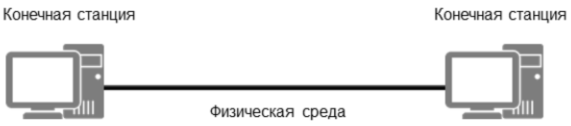
Цели

По окончании этого модуля слушатели смогут:

- Объяснить, что представляет собой сеть.
- Определить основные компоненты сети.
- Описать основные механизмы организации связи в сети.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Простые сети Ethernet с топологией точка-точка



- Сети состоят как минимум из двух компьютеров и среды передачи данных.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Под сетью можно понимать способность двух или более объектов обмениваться данными через определенную среду. Этот принцип установления связи применяется для организации любой сети. Обычно объекты в сети, которые отвечают за передачу и прием связи, называются конечными станциями, а средство, с помощью которого обеспечивается связь, называются средой передачи (или носителем). В корпоративной сети среда передачи может принимать различные формы от физического кабеля до радиоволн.

Коаксиальный кабель

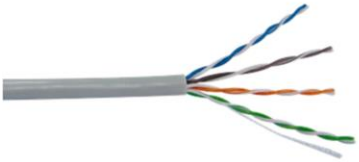
Стандарт	Кабели	Максимальное расстояние передачи
10Base2	Тонкий коаксиальный	185 м
10Base5	Толстый коаксиальный	500 м

- Медные коаксиальные кабели, как правило, используются для объединения пользователей в общую сеть.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Коаксиальный кабель представляет собой самое распространенное средство передачи данных, использование которого может быть ограничено в рамках корпоративной сети. В качестве носителя, используются, как правило, коаксиальные кабели двух стандартов: 10Base2 и 10Base5, известные как Thinnet или ThinWire, и Thicknet или Thickwire соответственно.
- Стандарты поддерживают пропускную способность 10 Мбит/с, передача осуществляется в виде сигналов базовой полосы на расстояния 185 и 500 метров соответственно. В современных корпоративных сетях пропускная способность сильно ограничена. Разъем (коннектор) Bayonet Neill-Concelman (BNC) служит для подключения тонких коаксиальных кабелей 10Base2, а разъем типа N применяется для более толстого кабеля 10Base5.

Кабель Ethernet



Стандарт	Физическая среда	Расстояние
10Base-T	Две пары кабелей - витая пара категории 3/4/5	100 м
100Base-TX	Две пары кабелей - витая пара категории 5	100 м
1000Base-T	Четыре пары кабелей - витая пара категории 5e	100 м

- Основной физический носитель, используемый в корпоративных сетях.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Кабельная система Ethernet стала стандартом для многих корпоративных сетей, которая обеспечивает среду передачи, отличающуюся значительно более высокой пропускной способностью. Такая среда передачи представляет собой четыре медные провода в оболочке, которые защищены или не защищены от внешних электрических помех. Пропускная способность определяется главным образом категорией кабеля, а именно, категория 5 (CAT5) с поддержкой пропускной способности Fast Ethernet до 100 Мбит/с и категория 5 (CAT5e) и выше с более высокой пропускной способностью Gigabit Ethernet.
- Передача по Ethernet в качестве физической среды подвержена затуханию, в результате чего дальность передачи ограничивается 100 метрами. Разъем RJ-45 используется для обеспечения возможности подключения с помощью проводных пар и особым порядком расположения контактов в разъеме RJ-45, для обеспечения правильной передачи и приема конечными станциями в данной среде передачи.

Волоконно-оптический кабель

Стандарт	Физическая среда	Расстояние
10Base-F	Волоконно-оптический кабель с двумя жилами	2000 м
100Base-FX	Многомодовый волоконно-оптический кабель с двумя жилами	2000 м
1000Base-LX	Одномодовый волоконно-оптический или многомодовый волоконно-оптический кабель	316 – 5000 м
1000Base-SX	Многомодовый волоконно-оптический кабель	275 – 550 м

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Оптические носители для передачи сигналов используют свет в отличие от передачи электрических сигналов, свойственных для Ethernet и коаксиальных кабелей. Волоконно-оптическая среда поддерживает целый ряд стандартов передачи 10 Мбит/с, 100 Мбит/с, 1 Гбит/с и 10 Гбит/с (10GBASE). Одномодовое или многомодовое оптоволокно определяет использование оптического носителя для распространения света. Одномодовое волокно способно распространять только одну основную моду оптического излучения, и обычно используется для высокоскоростной передачи на большие расстояния.
- Многомодовое — это волокно, в котором распространяется больше одной моды оптического излучения, восприимчиво к затуханию в результате рассеивания света вдоль оптического носителя, и поэтому не поддерживают передачу на большие расстояния. Такое волокно часто применяется в локальных вычислительных сетях с гораздо меньшим диапазоном передачи. Существует большое количество стандартов оптических коннекторов, при этом наиболее распространенными являются коннекторы ST, LC и SC или фиксаторы.

Последовательный кабель

Стандарт	Скорость
RS-232	Стандартная – до 20000 бит/с, может достигать 1 Мбит/с
RS-422	100 Кбит/с ~ 10 Мит/с

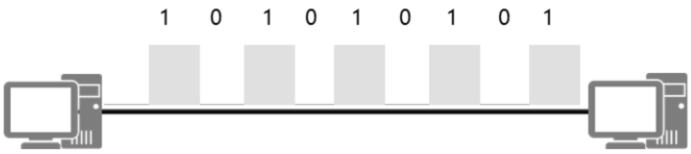
- Последовательный кабель представляет собой традиционную форму передачи данных.
- Развитие стандарта получило в формате USB.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Последовательный интерфейс представляет собой стандарт, первоначально разработанный более 50 лет назад для обеспечения надежной передачи между устройствами. За это время стандарт претерпел много изменений. Последовательное соединение предназначено для передачи данных, при которой биты передаются друг за другом последовательно. Применяемый стандарт (рекомендуемый стандарт) RS-232 ограничен как расстоянием, так и скоростью. Исходные стандарты RS-232 определяют, что поддерживаемые скорости связи не должны превышать 20 Кбит/с, исходя из длины кабеля 50 футов (15 метров), однако скорость передачи для последовательного порта не бывает ниже 115 Кбит/с. Общее поведение последовательных средств передачи означает, что по мере увеличения длины кабеля поддерживаемая скорость передачи битов уменьшается, например, при использовании кабеля длиной около 150 метров, или длиной в 10 раз превышающей первоначальные стандарты, скорость передачи битов будет сокращена вдвое.
- Другие стандарты последовательных интерфейсов могут обеспечивать гораздо большую дальность передачи, как например, в случае со стандартами RS-422 и RS-485, которые охватывают расстояния до 4900 футов (1200 метров), и часто используют разъемы V.35, которые устарели в конце 1980-х годов, но все еще часто встречаются и используются при поддержке таких технологий, как Frame Relay и ATM. RS-232 не определяет стандарты разъемов, однако двумя общими формами разъемов, поддерживающими стандарт RS-232, являются разъемы DB-9 и DB-25. Для замены большей части используемых последовательных интерфейсов RS-232 были разработаны новые стандарты, включая FireWire и универсальной последовательной шины (USB), последний из которых широко используется в новых продуктах и устройствах.

Кодирование данных сигналов



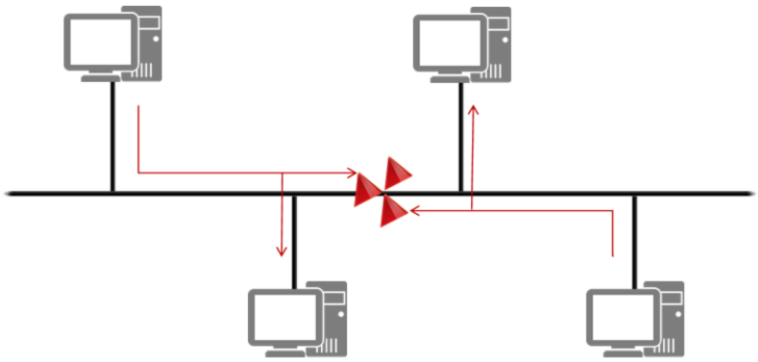
0000	0001	0010	0011	0100
0	1	2	3	4

- Шаблоны сигналов для интерпретации сообщений.
- Кодирование для синхронизации передачи.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Для обеспечения связи по физическим линиям между передающей и приемной станциями должны передаваться сигналы. Такой сигнал будет изменяться в зависимости от используемой среды передачи, как в случае оптической и беспроводной передачи. Основной целью сигнала является обеспечение синхронизации между отправителем и приемником по физическому носителю, а также поддержка передачи сигнала данных в форме, которая может быть интерпретирована как отправителем, так и приемником.
- Форма сигнала обычно распознается как свойство линейного кодирования, где напряжение переводится в двоичное представление значений 0 и 1, которые могут быть преобразованы принимающей станцией. Существуют различные стандарты линейного кодирования, причем стандарты 10Base Ethernet поддерживают стандарт линейного кодирования, известный как Манчестерское кодирование. Fast Ethernet с частотным диапазоном 100 МГц инициирует более высокие частоты, которые могут поддерживаться при использовании Манчестерского кодирования.
- Поэтому используется альтернативная форма линейного кодирования, известная как NZRI, которая сама по себе содержит изменения, зависящие от физического носителя, и поддерживая MLT-3 для 100Base-TX и 100Base-FX наряду с расширенным линейным кодированием, известным как кодирование 4B/5B для решения потенциальных проблем синхронизации. 100Base-T4, например, использует другую форму, известную как расширенное кодирование 8B/6T. Gigabit Ethernet поддерживает линейное кодирование 8B/10B, за исключением 1000Base-T, которое опирается на сложное блочное кодирование, называемое 4D-PAM5.

Коллизионные домены



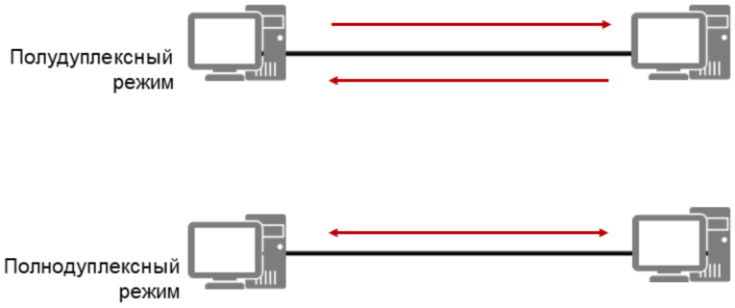
- В общей сети могут возникать коллизии (столкновения) сигналов.
- Для выявления коллизий используется механизм обнаружения коллизий.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Ethernet — это сеть с множественным доступом, в которой для передачи данных две или более конечных станций используют общую среду. Совместно используемая сеть, однако, подвержена коллизиям (столкновениям), когда данные передаются конечными станциями одновременно по общему носителю. Сегмент, в котором происходят такие столкновения называется коллизионным доменом.
- Конечные станции в пределах такого коллизионного домена используют конфликт при передачи данных в предполагаемое место назначения. Такое поведение требует, чтобы каждая конечная станция отслеживала входящие данные в данном сегменте, прежде чем предпринять попытку передачи. Данный процесс называется CSMA/CD (Carrier Sense Multiple Access with Collision Detection — множественный доступ с прослушиванием несущей и обнаружением коллизий). Однако даже после принятия таких мер предосторожности вероятность возникновения коллизий в результате одновременной передачи двумя конечными станциями остается высокой.

Дуплексные режимы



- Дуплексные режимы поддерживают одновременную и неодновременную двунаправленную связь.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Для определения поведения, связанного с передачей данных по физическому носителю, выделяют режимы передачи — полудуплекс и полный дуплекс.
- Полудуплекс — это связь двух или более устройств по общему физическому носителю, в котором существует коллизионный домен. При использовании данного режима, для обнаружения коллизий требуется CSMA/CD. Станция прослушивает прием трафика на собственном интерфейсе, и при стихании в течение определенного периода, начинает передавать данные. Если происходит коллизия, передача прекращается. Далее запускается алгоритм задержки (backoff algorithm), чтобы предотвратить дальнейшие передачи, пока не истечет случайное значение таймера, после чего выполняется повторная передача.
- Дуплексная связь предусматривает одновременную двустороннюю передачу информации по проводной паре, что гарантирует отсутствие возможности для возникновения коллизий, и поэтому применение механизма CSMA/CD не требуется.

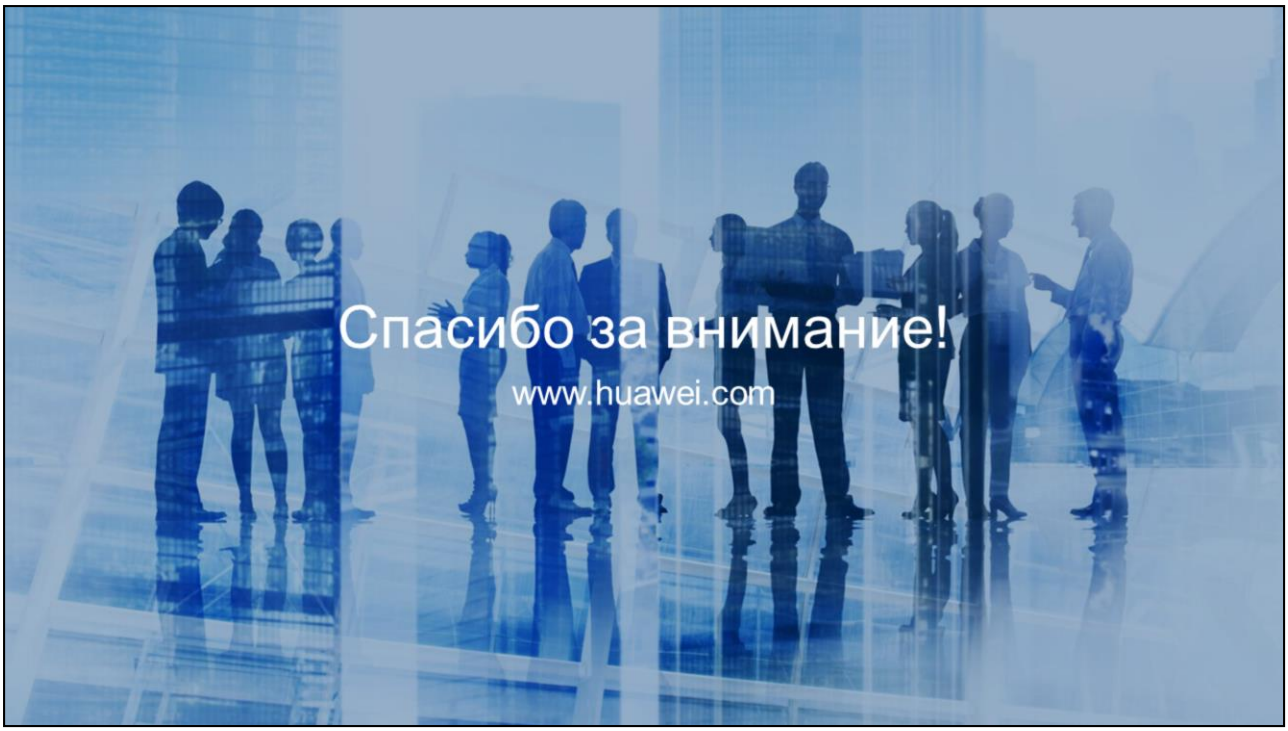
Заключение

- Какие кабели можно использовать для поддержки передачи Gigabit Ethernet в корпоративной сети?
- Что такое коллизионный домен?
- Для чего предназначен CSMA/CD?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Gigabit Ethernet поддерживается кабелями CAT 5e и выше, а также любой формой оптоволоконного кабеля 1000Base или выше.
- Коллизионный домен - это сетевой сегмент, в котором для двунаправленной связи используется один физический носитель. При одновременной передаче данных между хостами в одной общей сетевой среде могут возникать коллизии сигналов, до того как эти сигналы достигают места назначения. Как правило, это приводит к получению получателем неправильных сигналов, большего или меньшего, приемлемого для передачи размера (64 байта - 1500 байтов), также известных как runts и giants.
- CSMA/CD представляет собой механизм обнаружения и сведения к минимуму возможности коллизий, которые могут произойти в общей сети. CSMA требует, чтобы передающий хост сначала, до передачи, прослушивал сигналы, передаваемые в общей среде. Передача продолжается, если в данный момент передача не обнаружена. В противном случае, когда сигналы передаются одновременно и происходит коллизия, применяются процессы обнаружения коллизий, чтобы остановить передачу на заданный период времени, удалить события коллизий и избежать дальнейших коллизий между передающими хостами.


Спасибо за внимание!
www.huawei.com

Кадрирование Ethernet

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

Передача в любой физической среде требует правил, определяющих режим работы системы связи. Управление режимом передачи по Ethernet-сетям контролируется с помощью стандартов IEEE 802, определенных для канала передачи данных Ethernet. Фундаментальные знания этих стандартов необходимы для полного понимания принципа организации связи на канальном уровне в сетях Ethernet.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Цели

По завершении этого раздела обучающиеся научатся:

- Объяснять, как применять эталонные модели в сетях.
- Описывать, как формируются кадры.
- Объяснять принцип работы функции MAC-адресации на канальном уровне.
- Описывать принцип обработки и передачи кадров Ethernet.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Управление сетевой связью

- Сети управляются главным образом протоколами верхнего и нижнего уровней.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

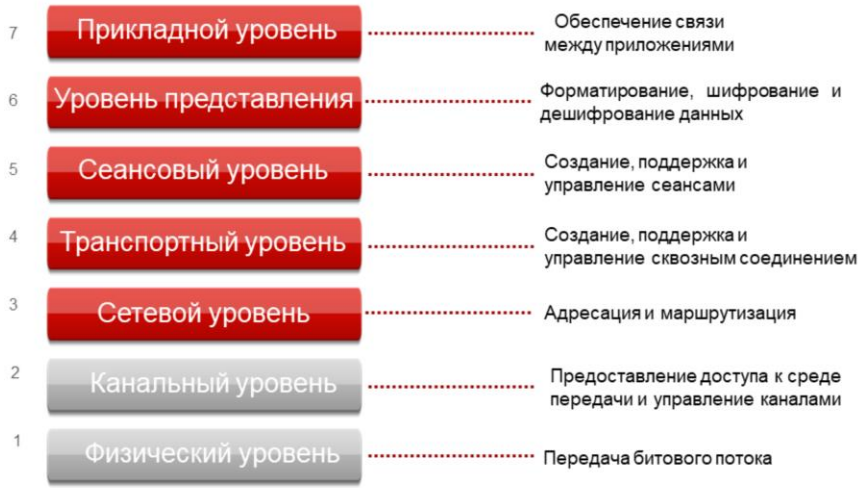
- Передача по сетям основана на применении определенных правил, регулирующих методы передачи и обработки данных, понятные как посылающему, так и принимающему узлам. В результате в течение определенного времени были разработаны многочисленные стандарты, часть из которых получили широкое распространение. Однако существует четкое различие между стандартами, регулирующими физический поток данных, и стандартами, которые отвечают за логическую переадресацию и доставку трафика.
- IEEE 802 — это набор универсальных стандартов для управления физической передачей данных по физической сети, включающий стандарт Ethernet 802.3 для физической передачи по локальной вычислительной сети.
- Существуют альтернативные стандарты передачи по глобальным вычислительным сетям, работающих в среде передаче на основе последовательной связи, включая Ethernet, PPP и HDLC. TCP/IP был широко принят в качестве набора протоколов, определяющих стандарты верхнего уровня, которые регулируют правила (протоколы) и методы, связанные с управлением логической передачей и доставкой между конечными станциями.

Многоуровневые модели: TCP/IP

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Эталонная модель TCP/IP, описывающая базовые принципы работы набора протоколов – логическую передачу и доставку трафика между конечными станциями - представляет сеть с помощью четырех уровней, причем физическая передача включена в уровень сетевого интерфейса, поскольку описание работы нижнего уровня не является задачей модели.
- Основной акцент по-прежнему сделан на сетевом уровне (или уровне Интернета), который описывает принцип логической передачи трафика между сетями, и транспортном уровне (иногда именуемого уровнем передачи между хостами), который управляет сквозной доставкой трафика, обеспечивая надежность транспортировки между станциями источника и назначения. На прикладном уровне представлен интерфейс, работающий с различными протоколами, которые позволяют применять сервисы в прикладных процессах конечных пользователей.

Многоуровневые модели: OSI



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Хотя эталонная модель TCP/IP рассматривается как стандартная модель, основанная на наборе протоколов TCP/IP, ее главный принцип не позволяет четко разграничивать и отличать функциональности при обращении к более нижнему уровню физической передачи.
- В свете этого, в качестве модели для ссылки на стандарты IEEE 802 часто используется модель взаимосвязи открытых систем (эталонная модель OSI) благодаря четкому определению и представлению принципов взаимосвязи на нижних уровнях, которые очень близки к стандартам эталонной модели LAN/MAN, определенных как часть задокументированных стандартов IEEE 802-1990 для локальных и городских вычислительных сетей. Кроме того, модель, которая в целом связана с набором протоколов ISO, обеспечивает расширенный анализ обработки верхнего уровня.

Инкапсуляция

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Поскольку для передачи по сети из конечной системы определяются данные верхнего уровня, перед передачей к таким данным необходимо применить ряд процессов и команд. Этот процесс добавления и предварительного ожидания команд, применяемых к данным, называется инкапсуляцией, и для него необходимо определить каждый уровень эталонной модели.
- По мере применения команд к данным, увеличивается их общий размер. Дополнительные команды, представляющие собой дополнительную служебную информацию по отношению к существующей полезной нагрузке, применяются на уровне, на котором были применены основные команды. Что касается остальных уровней, то инкапсулированные команды не отличаются от исходных данных. Прежде чем команды будут переданы в виде кодированного сигнала по физической среде, выполняется окончательное добавление команд в соответствии со стандартами протоколов нижнего уровня (например, стандартом IEEE 802.3 Ethernet).

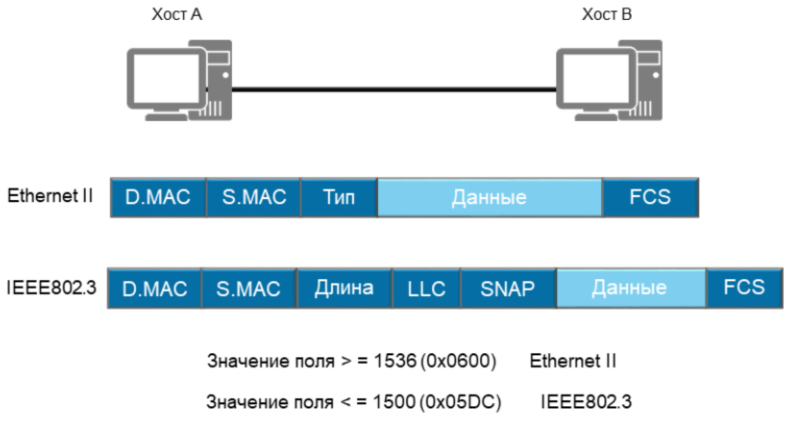
Связь между двумя конечными станциями

- Кадры канального уровня используются для управления передачей по среде передачи.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- В соответствии со стандартом IEEE 802.3 Ethernet, данные инкапсулируются в команды в виде заголовка и хвостовой части до их передачи по физической среде, в которой поддерживается Ethernet. Каждому этапу инкапсуляции соответствует блок данных протокола или PDU, который на уровне канала данных известен как кадр.
- Кадры Ethernet содержат команды, регулирующие порядок передачи данных по физической среде между двумя или более точками. Кадры Ethernet приходят в двух общих форматах, выбор которых зависит от протоколов, которые определяются до кадрирования.

Форматы кадров



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Эти два формата кадра признаны стандартными кадрами для сетей на базе Ethernet. Стандарт кадра DIX версии 2 был первоначально разработан в начале 1980-х годов, и сегодня он используется в качестве типа кадра Ethernet II. Ethernet II был в конечном итоге принят и введен в стандарты IEEE 802, входящие в раздел 3.2.6 документации по стандартам IEEE 802.3x-1997. Стандарт IEEE 802.3 Ethernet был первоначально разработан в 1983 году с ключевыми различиями в формате кадра, включая изменение поля типа, используемого для идентификации протокола, по которому должны передаваться данные сразу после обработки команд, содержащихся в кадре. В формате IEEE 802.3 Ethernet это поле длины, для которого используется расширенный набор команд 802.2 LLC для идентификации протокола передачи.
- Ethernet II и IEEE 802.3 ассоциируются с протоколами верхнего уровня и отличаются между собой диапазоном значений поля «Тип». Протоколы, поддерживающие значение менее 1500 (или 05DC в шестнадцатеричной системе), используют тип кадра IEEE 802.3 Ethernet на канальном уровне. Протоколы, представленные значением поля «Тип», который превышает или равен 1536 (или 0600 в шестнадцатеричной системе), используют стандарт Ethernet II и представляют собой большую часть всех кадров в сетях Ethernet.
- Остальные поля кадра – это поля MAC-адреса источника и назначения, которые идентифицируют отправителя и предполагаемого получателя(ей), а также поле последовательности проверки кадров, которое используется для подтверждения целостности кадра во время передачи.

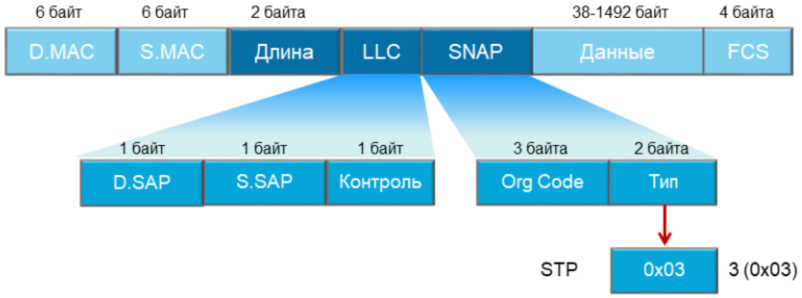
Кадр Ethernet II

- Тип кадра Ethernet II используется протоколами, значение поля «Тип» которых более 1536 (0x600).

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Кадр Ethernet II содержит поле «Тип», значение которого представляется в шестнадцатеричном формате и определяет протокол верхнего уровня. Одним из примеров этого является Интернет-протокол (IP), который представлен шестнадцатеричным значением 0x0800. Поскольку это значение больше 0x0600, значит, во время инкапсуляции должен применяться тип кадра Ethernet II. Другим общим протоколом, в котором используется тип кадра Ethernet II на канальном уровне, является ARP, и он представлен шестнадцатеричным значением 0x0806.

Кадр IEEE802.3

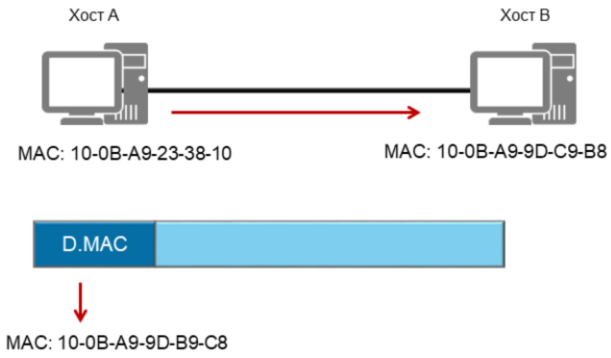


- Тип кадра IEEE 802.3 используется протоколами, значение поля «Тип» которых менее 1500 (0x05DC).

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Поле «Тип» кадра IEEE 802.3 включен в заголовок расширения SNAP и в целом не так часто применяется в протоколах в современных сетях, частично из-за дополнительных команд, которые приводят к избыточной служебной информации, включаемой в кадр. В некоторых устаревших протоколах, которые все еще применяются в поддержку сетей Ethernet, вероятно, будет применяться тип кадра IEEE 802.3. Один из наглядных примеров — протокол STP (Spanning Tree Protocol), который представлен значением 0x03 в поле «Тип» заголовка SNAP.

Передача кадров

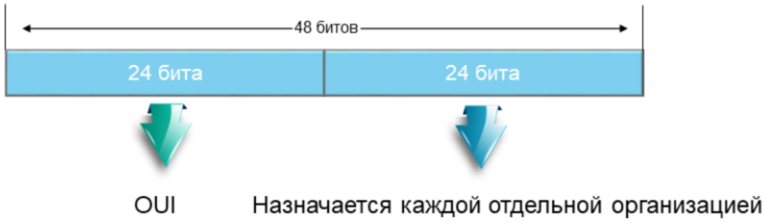


- Связь на канальном уровне организуется посредством назначения MAC-адресов.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Сети Ethernet обеспечивают связь между двумя конечными станциями локальной вычислительной сети посредством MAC-адреса, который позволяет отличать конечные системы в сетях множественного доступа. MAC-адрес — это физический адрес, содержащийся на сетевой интерфейсной плате, к которой подключается физическая среда. Этот же MAC-адрес извлекается и используется в качестве MAC-адреса назначения перед передачей кадра на физический уровень с целью его продвижения по подключенной физической среде.

MAC-адрес Ethernet

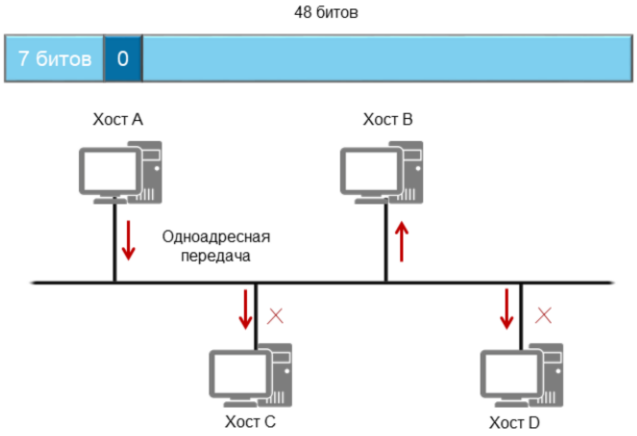


- MAC-адрес включает в себя уникальный идентификатор и установленное поставщиком значение адреса.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.
HUAWEI

- Каждый MAC-адрес является 48-разрядным значением, обычно представляемым в шестнадцатеричном формате и состоящим из двух частей. Глобальная уникальность каждого MAC-адреса достигается за счет уникального идентификатора, который зависит от конкретного поставщика. Происхождение продукта можно отследить по первым 24 битам MAC-адреса. Остальные 24 бита MAC-адреса — это значение, которое назначается каждому продукту единственным образом (например, сетевая интерфейсная плата или аналогичный продукт, поддерживающий интерфейсы порта, для которых требуется MAC-адрес).

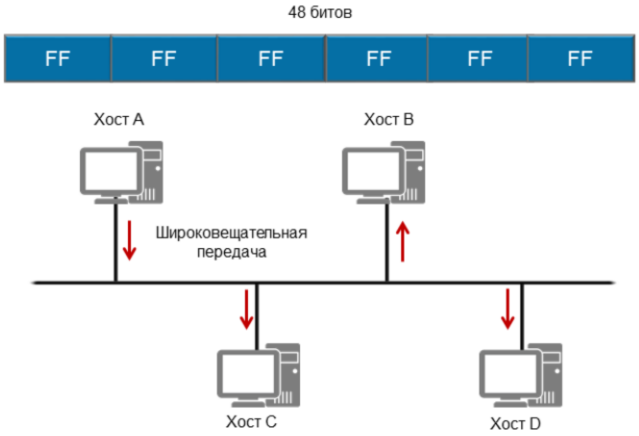
Одноадресная передача кадров



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Передача кадров в локальной сети достигается с помощью одного из трех методов передачи, первый из которых является одноадресным и выполняется от одного источника в один пункт назначения. Каждый хост-интерфейс представлен уникальным MAC-адресом, содержащим уникальный идентификатор, для которого 8-й бит наиболее значимого октета (или первого байта) в поле MAC-адреса идентифицирует тип адреса. Этот 8-й бит всегда устанавливается в значение 0, где MAC-адрес является MAC-адресом хоста, и означает, что любой кадр, содержащий это значение в поле MAC-адреса назначения, предназначен только для одного получателя.
- В случае с общим доменом коллизии, все подключенные хосты получают кадр одноадресной рассылки, но такой кадр обычно игнорируется всеми хостами, у которых значение в поле MAC-адреса назначения кадра не соответствует такому же значению на принимающем хосте на данном интерфейсе. Таким образом, назначенный хост сможет только принимать и обрабатывать полученные данные. Кадры одноадресной рассылки передаются только от одного физического интерфейса в назначенный пункт, даже в тех случаях, когда существуют несколько интерфейсов.

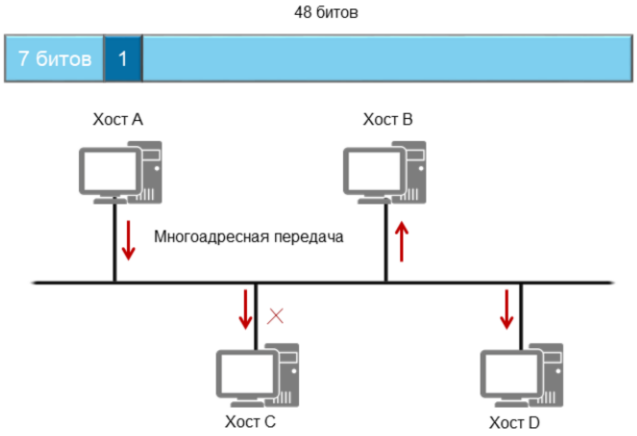
Широковещательная передача кадров



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Широковещательная передача представляет собой метод передачи, который позволяет рассылать кадры из одного источника, информация о котором получена всеми пунктами назначения в локальной сети. Для того, чтобы трафик транслировался на все хосты в локальной сети, в поле MAC-адреса назначения кадра устанавливается значение в шестнадцатеричном формате в виде FF: FF: FF: FF: FF: FF, и данное значение указывает, что все получатели кадра по указанному адресу должны принять этот кадр, обработать заголовок кадра и хвостовую часть.
- Широковещание используется протоколами для выполнения ряда важных сетевых процессов, включая обнаружение и поддержку работы сети, однако в результате такой рассылки генерируется избыточный трафик, который часто вызывает прерывания в конечных системах, а характер загрузки полосы пропускания, как правило, снижает общую производительность сети.

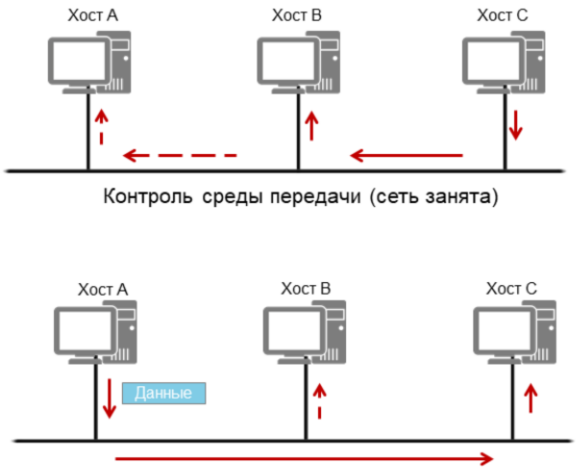
Многоадресная передача кадров



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Более эффективной альтернативой широковещанию стала многоадресная передача, которая заменила широковещание во многих новых технологиях. Многоадресную передачу можно рассматривать как форму селективного широковещания, позволяющей выбрать хосты, которые будут анализировать конкретный MAC-адрес многоадресной рассылки в дополнение к MAC-адресу одноадресной рассылки , связанному с хостом, и обрабатывать любые кадры, содержащие MAC-адрес многоадресной рассылки в поле MAC-адреса назначения кадра.
- Поскольку не существует относительного различия между форматами MAC-адресов многоадресной и одноадресной рассылки, адрес многоадресной рассылки отличается значением 8-го бита первого октета. Если значение равно 1, значит это многоадресная рассылка, а значение 0 соответствует одноадресной рассылке.
- В локальной вычислительной сети реальная возможность многоадресной рассылки на канальном уровне ограничена, так как метод передачи все еще напоминает широковещание, для которого характерны прерывания по всей сети. Единственная заметная разница от широковещания заключается в выборочной обработке с помощью приемных конечных станций. По мере развития технологий, которые могут поддерживать несколько локальных вычислительных сетей, становится более очевидной реальная возможность технологии многоадресной рассылки как эффективного средства передачи.

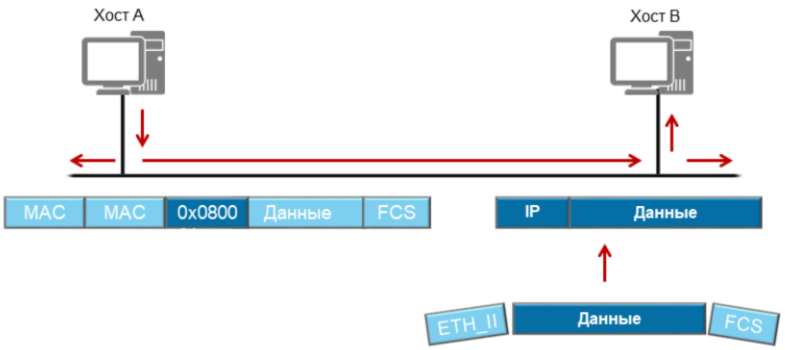
Контроль среды передачи



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- В ходе подготовки трафика к передаче по физической сети необходимо, чтобы хосты в общих доменах коллизий умели определять, занимает ли тот или иной поток трафика в настоящий момент среду передачи. 10Base2 представляет собой общую среду передачи, в которой для устранения коллизий должен применяться метод CSMA/CD. При обнаружении каналом передачи кадра, хост задерживает передачу своих собственных кадров до тех пор, пока линия не освободится, после чего хост начнет пересылать кадры от физического интерфейса к пункту назначения.
- Если два хоста подключены к среде, поддерживающей полнодуплексную передачу, например 10BaseT, то считается, что передаваемые кадры не пострадают от коллизий, так как передача и получение кадров происходит по отдельным линиям и поэтому нет необходимости применения метода CSMA/CD.

Обработка кадров



- Команды на получение, обработку и отбрасывание кадров по каналу.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.
HUAWEI

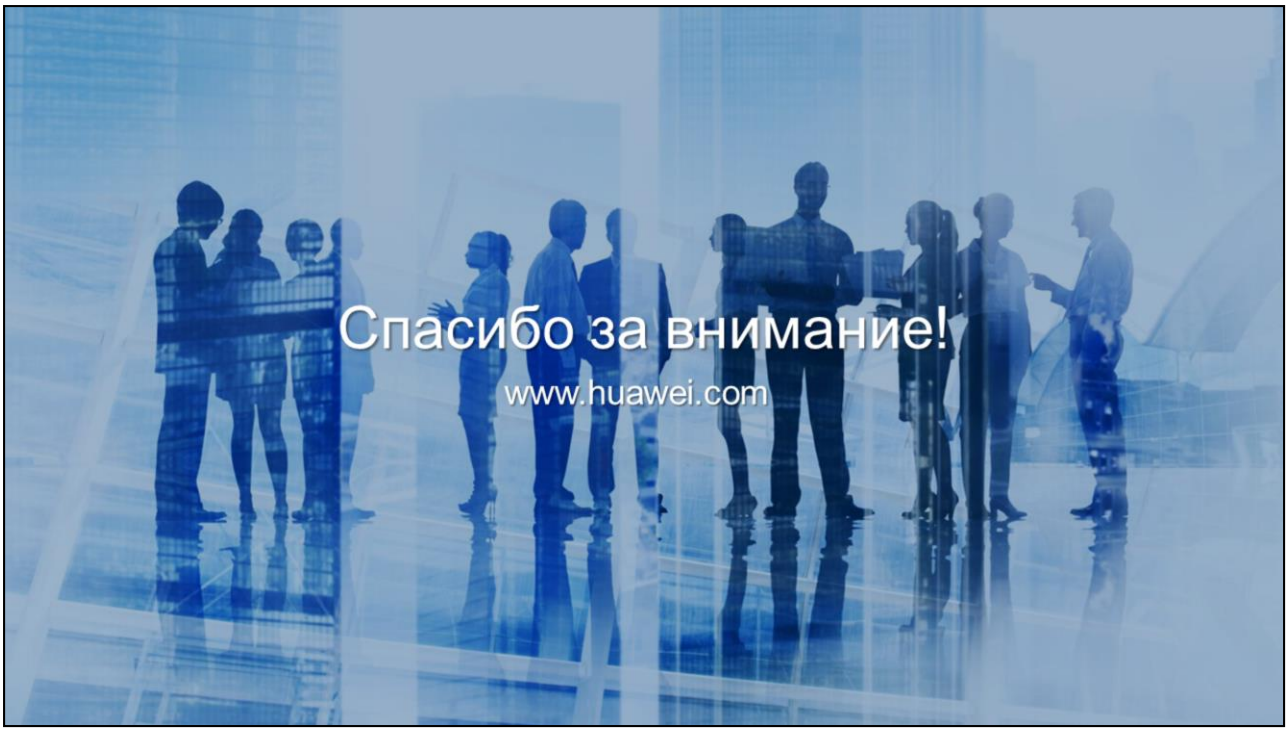
- Кадр, переданный физическим интерфейсом хоста, сразу передается по среде передачи в пункт назначения. В случае общей сети, этот кадр могут получить несколько хостов, которые оценивают, кому предназначен кадр, анализируя MAC-адрес назначения в заголовке кадра. Если MAC-адрес назначения и MAC-адрес хоста не совпадают, или MAC-адрес назначения не является MAC-адресом широковещательной или многоадресной рассылки, который прослушает хост, кадр будет проигнорирован и отброшен.
- В пункте назначения кадр будет принят и обработан после подтверждения, что его получатель - физический интерфейс хоста. Хост должен также подтвердить целостность кадра, сохраненную во время передачи, путем сравнения значение поля последовательности проверки кадров (FCS) и со значением, установленным принимающим хостом. Если значения не совпадают, кадр будет считаться поврежденным и впоследствии будет отброшен.
- Далее хост определяет следующий этап обработки действительных кадров, анализируя поле типа заголовка кадра и определя протокол кадра. В этом примере поле типа кадра содержит шестнадцатеричное значение 0x0800, которое означает, что данные кадра должны быть переданы модулю Интернет-протокола, и перед этим заголовок и хвостовая часть кадра отбрасываются.

Заключение

- Каким образом технология Ethernet определяет протокол, по которому должен передаваться обработанный кадр?
- Как принимается решение, какая операция – обработка или отбрасывание – будет выполнена с кадром, полученным конечным устройством?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Кадры, передаваемые на канальном уровне, содержат поле «Тип», его значение ссылается на следующий протокол, к модулю которого должны быть переданы данные, содержащиеся в кадре. Примеры протоколов передачи — IP (0x0800) и ARP (0x0806).
- MAC-адрес назначения, содержащийся в заголовке кадра, анализируется получающей конечной станцией и сравнивается с MAC-адресом интерфейса, который получил данный кадр. Если MAC-адрес назначения и MAC-адрес интерфейса не совпадают, кадр отбрасывается.


Спасибо за внимание!
www.huawei.com

Адресация в протоколе IP

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

Интернет-протокол (IP) предназначен для обеспечения межсетевого обмена, не поддерживаемого протоколами нижнего уровня, такими как Ethernet. Реализация логической (IP) адресации позволяет использовать Интернет-протокол другими протоколами для передачи данных в виде пакетов между сетями. Для эффективного проектирования сети необходимы глубокие знания в области IP-адресации, а также полное понимание принципов работы протокола для получения четкого представления о том, как IP-протокол реализуется в качестве протокола маршрутизации.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Цели

По завершении этого раздела обучающиеся научатся :

- Описывать поля и параметры, содержащиеся в IP-пакете.
- Различать между собой государственные, частные и специальные диапазоны IP-адресов.
- Успешно реализовать VLSM-адресацию.
- Объяснять функцию IP-шлюза.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

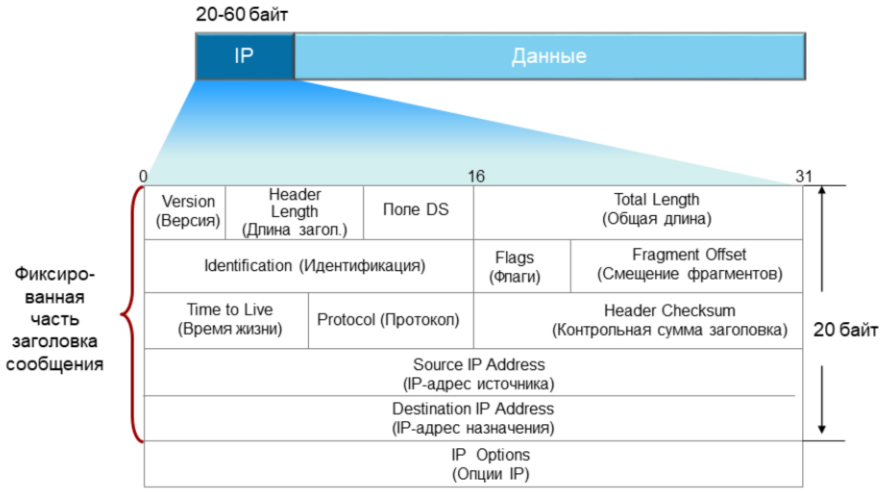
Последующие команды, содержащиеся в заголовке

- Последующий набор команд на выполнение содержится в поле «тип» заголовка кадра.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

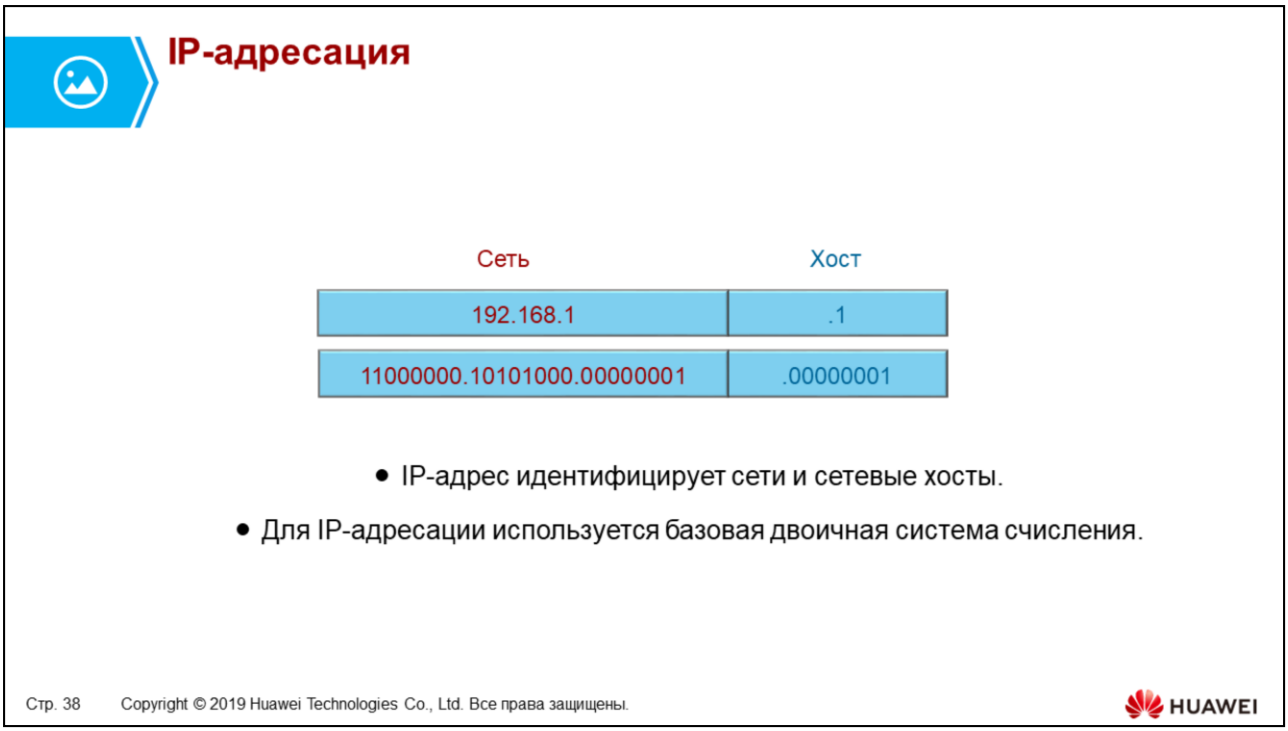
- Перед отбрасыванием заголовка кадра и хвостовой части необходимо определить последующий набор команд на выполнение. Набор команд определяется по значению поля типа в заголовке кадра. В текущем примере это значение указывает на отправку кадра в модуль протокола IP после завершения его обработки.
- Ключевой функцией кадра является определение того, был ли достигнут запланированный физический пункт назначения, а также сохранена ли целостность кадра. Основное внимание в данном разделе уделено вопросу обработки данных после отбрасывания заголовков кадра и передачи оставшихся данных в модуль IP-протокол.

Заголовок пакета IP-протокола



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Заголовок IP-пакета используется для поддержки двух ключевых операций — маршрутизации и фрагментации. Маршрутизация — это механизм, который позволяет переадресовать трафик из данной сети в другие сети, так как канальный уровень представляет собой единую сеть, в которой существуют границы. Фрагментация — это разбиение данных на управляемые блоки, которые могут передаваться по сети.
- Заголовок IP-пакета передается в составе данных и представляет собой служебную информацию размером не менее 20 байт, которая указывает на то, как трафик может пересылаться между сетями, при этом запланированный получатель находится в сети, отличной от сети, из которой данные были первоначально переданы. В поле «Версия» содержится версия IP-протокола, которая в настоящее время поддерживается, в данном случае это версия 4 или IPv4. Поле DS первоначально называлось типом сервисного поля, однако теперь поле поддерживает значения дифференцированных услуг и используется для применения механизма качества обслуживания (QoS) с целью оптимизации сетевого трафика. Данное поле не входит в объем текущего курса.
- IP-адреса источника и назначения — это логические адреса, назначаемые хостам и указывающие на отправителя и запланированного получателя на сетевом уровне. По IP-адресам можно оценить, в какой сети находится запланированный получатель — в той же или в другой. Эти параметры помогают маршрутизировать пакеты между сетями с целью достижения адресатов, находящихся за пределами локальной вычислительной сети.



- Каждый адрес IPv4 представляет собой 32-разрядное значение, которое часто представляется в десятичном формате с точкой, но для детального понимания принципа представляется также в двоичном формате (Base 2). IP-адреса выступают в качестве идентификаторов, используемых конечными системами, а также других устройств в сети, в качестве средства обеспечения доступности таких устройств как локально, так и из удаленных источников, расположенных за пределами текущей сети.
- IP-адрес состоит из двух полей, информация которых используется для четкого определения сети, к которой принадлежит IP-адрес, а также идентификатора хоста, входящего в сетевой диапазон. Как правило, IP-адрес уникален в данной сети.

- Каждый сетевой диапазон содержит два важных адреса, которые исключаются из сетевого диапазона, назначаемого хостам или другим устройствам. Первым из таких исключаемых адресов является сетевой адрес, представляющий данную сеть, в отличие от конкретного хоста в сети. Сетевой адрес можно определить по значению поля хоста сетевого адреса, где в пределах этого диапазона устанавливаются все двоичные значения 0. При этом следует отметить, что все двоичные нули не всегда представляют значение 0 в десятичном формате с точкой.
- Второй исключаемый адрес — это широковещательный адрес, используемый сетевым уровнем для обозначения любой передачи, которая, как ожидается, будет отправлена во все пункты назначения в данной сети. Широковещательный адрес представлен в поле хоста IP-адреса, где в этом диапазоне устанавливаются все двоичные значения 1. Адреса хостов формируют диапазон между сетевыми и широковещательными адресами.

Десятичная, двоичная и шестнадцатеричная системы счисления

Формат	Диапазон значений	Основание
Двоичный	0 — 1	2
Десятичный	0 — 9	10
Шестнадцатеричный	0 — F	16

- Наибольшее распространение в IP-сетях получили двоичная и шестнадцатеричная системы счисления.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Двоичный, десятичный и шестнадцатеричный форматы обычно применяются во всех IP-сетях для представления схем адресации, протоколов и параметров, и поэтому знание базовых структур данных форматов имеет важное значение для понимания и применения принципов адресации в IP-сетях.
- Каждая система счисления отличается количеством цифр или цифр и букв, используемых в структуре адреса. В случае с двоичным форматом, используются только два значения, 0 и 1. Число, увеличиваемое путем изменения комбинации этих значений, часто представляется как 2 в степени x, где x — это количество двоичных значений. В шестнадцатеричной системе счисления основание равно 16, значения находятся в диапазоне от 0 до F, (0-9 и A-F), где A представляет следующее значение после 9 и F означает значение, эквивалентное 15 в десятичном, или 1111 в двоичном.

Преобразование из десятичной в двоичную систему счисления

Двоичный символ	1	1	1	1	1	1	1	1
Степень	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Число	128	64	32	16	8	4	2	1

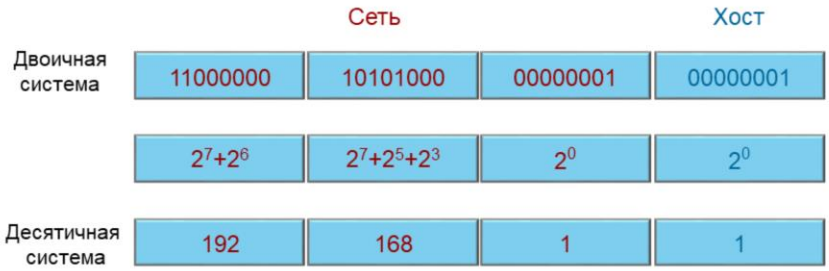
Десятичная система	Двоичная система	Шестнадцате-ричная система
0	00000000	00
1	00000001	01
2	00000010	02
3	00000011	03
4	00000100	04
5	00000101	05
6	00000110	06
7	00000111	07
8	00001000	08

Десятичная система	Двоичная система	Шестнадцате-ричная система
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 © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Байт содержит 8 битов и выступает в качестве общей единицы информации в IP-сетях. Может принимать любое значение от 0 до 255. Данная единица информации образуется путем преобразования из десятичной в двоичную систему счисления и применения степени к каждому двоичному значению для достижения 256-битного диапазона значений. Преобразование из десятичной в двоичную систему показано в примере, который также наглядно демонстрирует, как представляются значения широковещательных адресов в десятичной, двоичной и шестнадцатеричной системах счисления и как осуществляется широковещательная передача с IP- и MAC-адресами на сетевом и канальном уровнях.

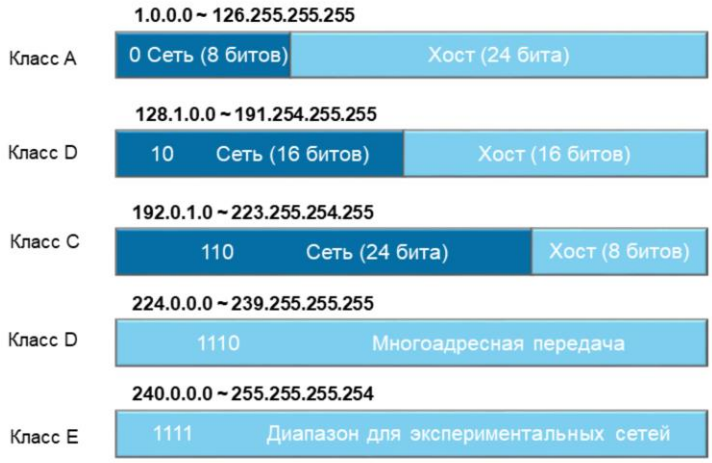
Преобразование из двоичной в десятичную систему счисления



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Комбинация из 32 бит в IP-адресе коррелирует с четырьмя октетами или байтами, каждый из которых может представлять значение из диапазона 256. Таким образом, теоретическое количество возможных IP-адресов равно 4’294’967’296, однако в действительности только часть из общего числа адресов может быть выделена хостам. Каждый бит в байте представляет собой степень и каждый октет может представлять определенный сетевой класс, при этом каждый класс сети базируется либо на одном октете, либо на комбинации октетов. В данном примере для представления сети использованы три октета, а четвертый октет представляет диапазон адресов, которые сеть может выделить хостам.

Классы IP-адресов



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Количество октетов, поддерживаемых сетевым адресом, определяется классом адресов, на которые подразделяется область адресов IPv4. Классы A, B и C относятся к диапазонам выделяемых адресов, каждый из которых поддерживает различные сети и ряд хостов, которые могут быть назначены данной сети. Класс A, например, включает 126 потенциальных сетей, каждая из которых поддерживает 2^{24} (или 16’777’216) потенциальных адресов хостов с учетом того, что сетевые и широковещательные адреса из диапазона определенного класса нельзя выделить хостам.
- Одна сеть Ethernet не может поддерживать такое большое количество хостов, поскольку Ethernet плохо поддается масштабированию, отчасти из-за широковещаний, которые генерируют избыточный сетевой трафик в пределах одной локальной сети. Диапазоны адресов класса C позволяют сформировать гораздо более сбалансированную сеть, которая хорошо масштабируется в отношении Ethernet, обеспечивая более 2 миллионов потенциальных сетей, каждая из которых способна поддерживать 256 адресов, и 254 адреса можно выделять хостам.
- Класс D — это диапазон, зарезервированный для многоадресной рассылки. В этом диапазоне хосты могут прослушивать конкретный адрес, и если адрес назначения пакета содержит адрес многоадресного рассылки, который хост прослушивает, пакет обрабатывается таким же образом, как и пакет, предназначенный для хостов, которым выделен IP-адрес. Каждый класс легко определить в двоичной системе счисления по битовому значению в первом октете, где адрес класса A, например, всегда начинается с 0 для старшего разряда, в то время как в классе B первые два старших разряда всегда имеют значения 1 и 0, что позволяет легко отличать классы в двоичной системе счисления.

Типы IP-адресов

Диапазоны частных адресов	
Класс A	10.0.0.0~10.255.255.255
Класс B	172.16.0.0~172.31.255.255
Класс C	192.168.0.0~192.168.255.255

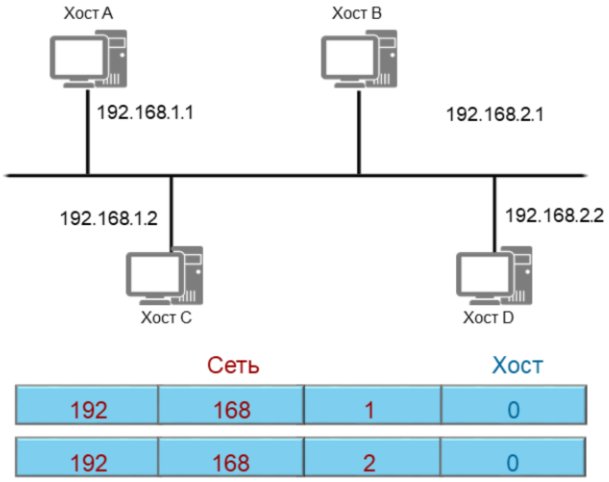
Специальные адреса	
Диагностика	127.0.0.0 ~ 127.255.255.255
Любая сеть	0.0.0.0
Сетевое широковещание	255.255.255.255

- Диапазон адресов IP-сети был разделен, и некоторые адреса и диапазоны предназначены для особых целей.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- В сети IPv4 для особых целей зарезервированы конкретные адреса и адресные диапазоны. Диапазоны частных адресов существуют в классах A, B и C, это позволяет избежать быстрого использования доступных IP-адресов. Количество фактических конечных систем и устройств, требующих IP-адресации, в мире превышает 4’294’967’296 в диапазоне 32-разрядных адресов IPv4, и поэтому решение этой проблемы заключается в выделении диапазонов, которые могут быть назначены частным сетям, с целью сохранения адресов, с помощью которых организуется связь по инфраструктуре сети общего пользования, например Интернет.
- Частные сети сейчас распространены в корпоративных сетях, но хосты не могут взаимодействовать с сетью общего пользования, это означает, что диапазоны адресов можно повторно использовать во многих разнородных корпоративных сетях. Однако адреса трафика, связанного с сетями общего пользования, должны быть преобразованы до того, как данные смогут достичь запланированного места назначения.
- Другие специальные адреса — это адреса диагностического диапазона, обозначаемого как 127.0.0.0, а также первый и последний адреса в диапазоне IPv4, где 0.0.0.0 представляет любую сеть и его применение должно быть более детально представлено вместе с принципами маршрутизации. Адрес 255.255.255.255 представляет собой широковещательный адрес в сети IPv4 (0.0.0.0), однако масштаб любого широковещания в IP-протоколе ограничен границами локальной вычислительной сети, из которой генерируется такая широковещательная передача.

Связь по IP



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Для того, чтобы хост пересылал трафик в пункт назначения, необходимо, чтобы у него была информация о сети назначения. Как правило хосту известно о сети, к которой он принадлежит, но не известно о других сетях, даже если эти сети можно считать частью одной и той же физической сети. Таким образом, такой хост не пересылает данные, предназначенные для заданного пункта назначения, до тех пор, пока не узнает о сети и об интерфейсе, через который можно достичь адресата.
- Для того, чтобы хост переслал трафик другому хосту, он должен сначала определить, входит ли адресат в ту же IP-сеть. Это достигается путем сравнения сети назначения с исходящей сетью (IP-адрес хоста), с которой отправляются данные. При совпадении диапазонов сети, пакет пересылается на обработку на нижние уровни, где имеет место кадрирование Ethernet. В случае, если запланированная сеть назначения отличается от исходящей сети, хост, как ожидается, получит информацию о запланированной сети и интерфейсе, через который должен пересылаться пакет/кадр, до того, как пакет будет обработан нижними уровнями. Без этой информации хост отбросит пакет до того, как он достигнет канального уровня.

Маска подсети

Сеть	Хост
192.168.1	0
11000000.10101000.000000001	00000000

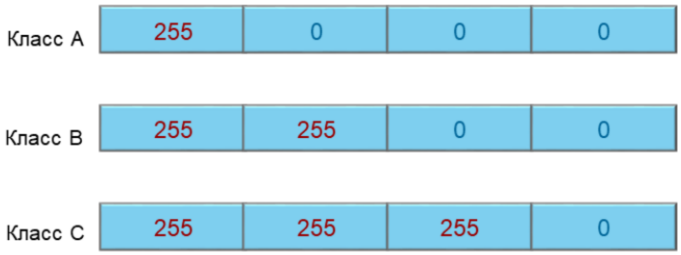
Подсеть	
255.255.255	0
11111111.11111111.11111111	00000000

- В маске подсети часть двоичных значений представляет адрес определенной (под)сети, а другая часть — адрес определенного хоста.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Идентификация уникального сегмента сети зависит от реализации значения маски, в которой часть числа битов указывают на данный сегмент сети, а остальные биты означают количество хостов, поддерживаемых в данном сегменте сети. Сетевой администратор может разделить сетевой адрес на подсети, с тем чтобы широковещательные пакеты передавались в пределах одной подсети. Маска подсети состоит из строки непрерывно идущих значений 1, за которой следует аналогичная непрерывная строка значений 0. Единицы соответствуют полю «ID сети», в то время нули соответствуют полю «ID хоста».

Маска подсети по умолчанию

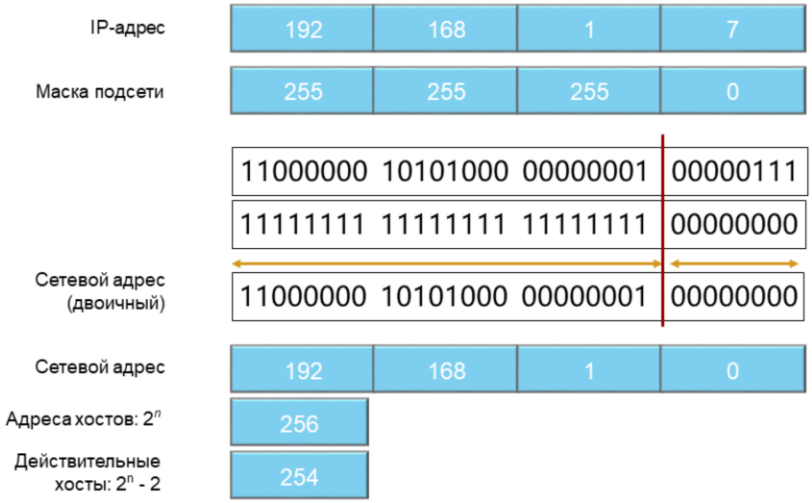


- Некоторые маски подсети применяются в адресных диапазонах по умолчанию и обозначают фиксированный диапазон, который используется в каждом классе сети.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Для каждого класса сетевого адреса используется соответствующая маска подсети, указывающая размер сетевого сегмента по умолчанию. Для любой сети с адресами класса A устанавливается 8-разрядная маска подсети по умолчанию, где первый октет адреса обозначает адрес сети, а последние три октета — адрес хоста.
- Аналогичным образом, в сетях класса B используется 16-разрядная маска подсети по умолчанию, что увеличивает число сетей в данном диапазоне за счет количества хостов, которые могут быть назначены в сети по умолчанию. Сеть класса C по умолчанию имеет 24-разрядную маску, которая обеспечивает большое количество потенциальных сетей, но значительно ограничивает количество хостов, которые могут быть назначены в сети по умолчанию. Сеть по умолчанию — это общая граница между диапазонами адресов, однако в случае классов A и B, не обеспечивает масштаба, достаточного для практического выделения адресов в сетях Ethernet.

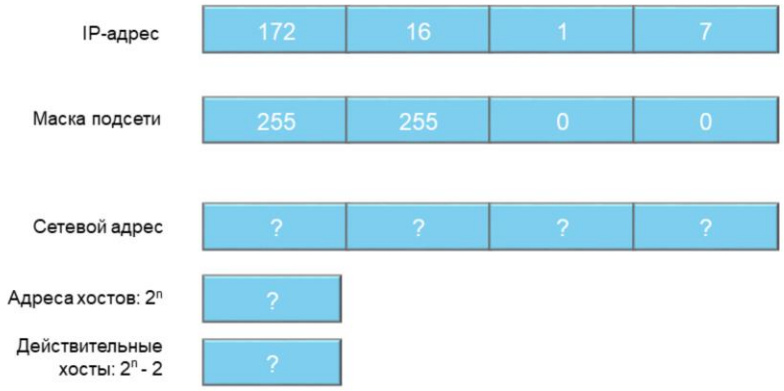
Планирование адресов



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Применение маски подсети к данному IP-адресу позволяет идентифицировать сеть, к которой принадлежит хост. Маска подсети также идентифицирует адрес широковещательной передачи, а также количество хостов, которые могут поддерживаться в данном диапазоне. Такая информация служит основой для эффективного планирования сетевых адресов. В данном примере хост определен адресом 192.168.1.7, который принадлежит сети с примененной 24-разрядной маской подсети по умолчанию (класс C). При определении частей IP-адреса, которые представляют собой сегменты сети и хоста, для каждого сегмента определяется сетевой адрес по умолчанию.
- Это адрес, в котором все значения битов хоста установлены в 0, в этом случае генерируется сетевой адрес по умолчанию 192.168.1.0. Если значения хоста представлены непрерывной строкой из единиц, можно определить адрес широковещательной передачи. Если последний октет содержит строку из единиц, он представляет собой десятичное значение 255, для которого можно получить адрес широковещательной передачи 192.168.1.255.
- Возможные адреса хостов рассчитываются по формуле 2^n, где n — это количество битов хоста, определенных маской подсети. В данном случае n равно 8 битам хоста, таким образом, 2^8 дает результат 256. Однако в отношении используемых адресов хоста, необходимо из этого результата вычесть сетевые и широковещательные адреса, чтобы получить число действительных адресов хоста 254.

Пример



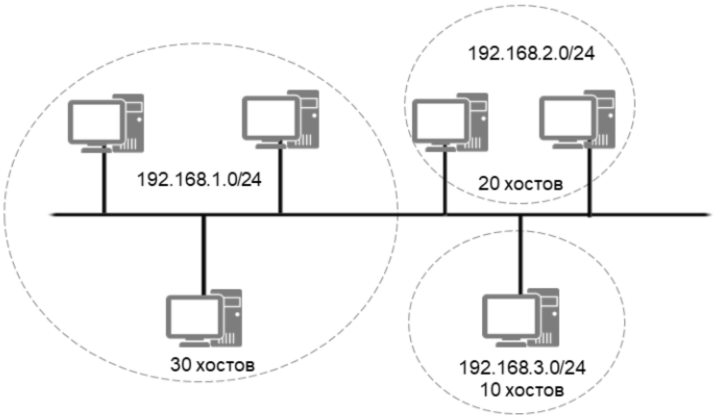
- Определите сеть представленного IP-адреса и количество фактических и действительных адресов хостов в сети.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- В данном примере представлен обычный диапазон адресов класса B. Для него необходимо определить сеть, к которой принадлежит указанный хост, а также адрес широковещательной передачи и количество действительных хостов, поддерживаемых данной сетью. Сетевой адрес хоста, а также число хостов в данной сети определяется по тому же принципу, что и для диапазона адресов класса C.

Ограничения адресов



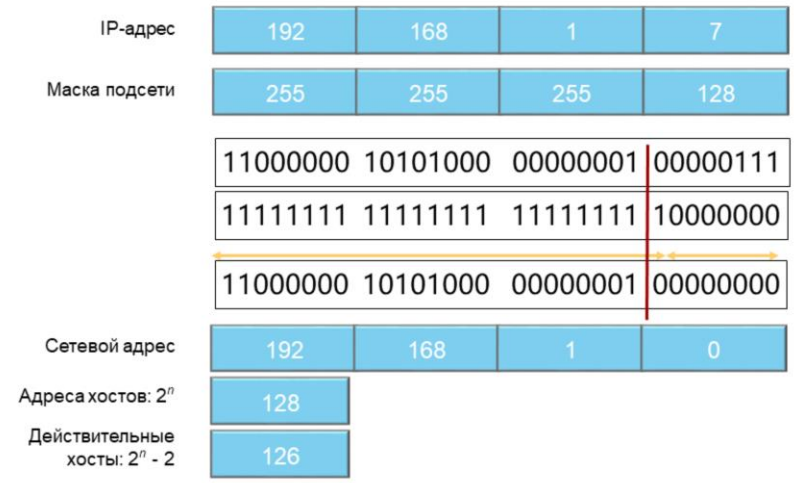
- Проектирование сети с использованием маски подсети по умолчанию приводит к нерациональному использованию адресов.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Одно из основных ограничений маски подсети по умолчанию возникает при использовании нескольких диапазонов сетевых адресов для предприятия, приведенного в примере, чтобы генерировать логические границы между хостами внутри физической и корпоративной сетей, Для применения базовой схемы адресации может потребоваться ограниченное число хостов, связанных с данной сетью. Для обеспечения логической сегментации данной сети применяются несколько сетей. Однако при этом большое количество адресного пространства остается неиспользуемым, что свидетельствует о неэффективности применения маски подсети по умолчанию.

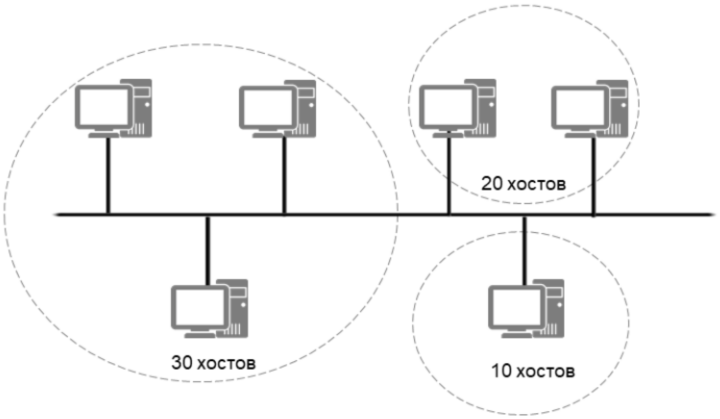
Реализация с использованием VLSM



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- В качестве меры устранения ограничений маски подсети по умолчанию вводится концепция масок подсети переменной длины, позволяющая разбивать маску подсети по умолчанию на несколько подсетей, которые могут быть фиксированной длины (также называемые маски подсети фиксированной длины или FLSM) или переменной длины (VLSM). Реализация таких масок подсети заключается в использовании сети с классом по умолчанию и делении сети с помощью маски подсети.
- В данном примере применено простое изменение сети класса C, в которой по умолчанию используется 24-разрядная маска. Изменение заключается в бите, заимствованном из ID хоста, который был применен как часть сетевого адреса. Если биты отличаются от сети по умолчанию, то дополнительные биты представляют собой ID подсети.
- В этом примере один бит представляет подсеть, из которой можно получить две подсети, поскольку одно битовое значение может принимать только два состояния — либо 1, либо 0. Если бит установлен в значение 0, число равно 0, если бит установлен в значение 1, число равно 128. Установкой битов хоста в нули определяется адрес для каждой подсети, установкой битов хоста в единицы определяется адрес широковещательной передачи для каждой подсети. Количество поддерживаемых хостов в данном примере равно 2^7 минус адрес подсети и адрес широковещательной передачи для каждой подсети, в результате чего каждая подсеть поддерживает в общей сложности 126 действительных адресов хоста.

Пример использования VLSM

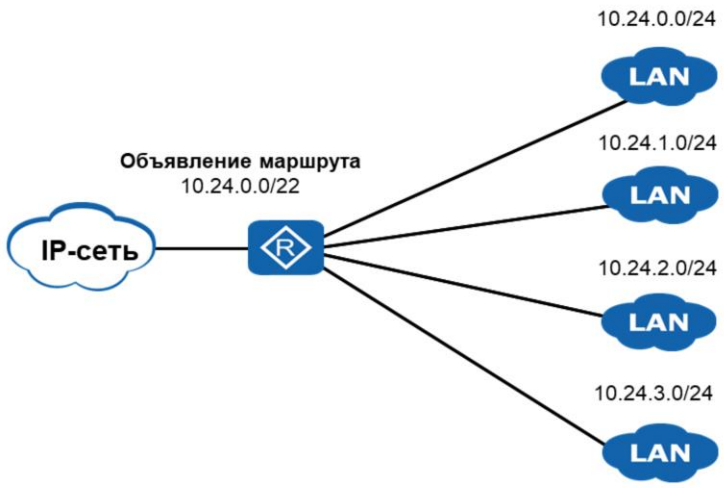


- Используя только сеть 192.168.1.0/24, рассчитайте VLSM для указанного количества хостов в каждом сегменте сети.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- В связи с проблемой ограничений адресов, которые привели к нерациональному использованию адресов сети по умолчанию, применяется концепция масок подсети переменной длины, которая уменьшает расход адресов и обеспечивает более эффективную схему адресации в корпоративной сети.
- Определен единый диапазон адресов класса C по умолчанию, для которого требуются маски подсети переменной длины с целью размещения каждой логической сети в пределах одного диапазона адресов по умолчанию. Для эффективного назначения маски подсети требуется определить количество битов хоста, необходимых для размещения требуемого количества хостов, а остальные биты хоста могут быть использованы для ID подсети, что означает изменение ID сети, входящего в диапазон адресов по умолчанию.

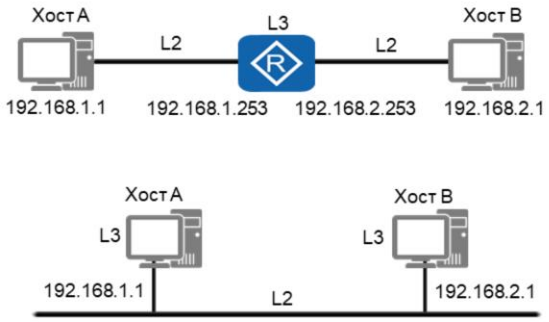
Бесклассовая междоменная маршрутизация



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Бесклассовая междоменная маршрутизация (CIDR) была первоначально внедрена в качестве меры решения проблем, возникающих в результате быстрого развития Интернета. Основные проблемы были связаны с неизбежным исчерпанием адресного пространства класса B, которое обычно выбиралось организациями среднего размера как наиболее подходящий диапазон адресов, поскольку класс C ограничен, а класс A слишком обширен, и управление адресами 65534 хоста достигалось через маску переменной длины VLSM. Кроме того, растущее число сетей привело к росту числа таких шлюзовых устройств, как маршрутизаторы, которые обслуживали такие сети. Переход на бесклассовую систему адресации означал замену классовых границ адресными префиксами.
- Принцип заключался в том, что в диапазоне адресов, например класса C, 24-разрядный префикс представляет подсеть или основную границу сети, при этом несколько сетевых префиксов суммируются в один более крупный префикс одного адреса, представляющий те же сети. Это помогло сократить число маршрутов устройств маршрутизации, функциорующих в глобальном масштабе, и повысило эффективность управления адресами. CIDR – перспективно направление, фактически замедляющее общую скорость исчерпания адресного пространства IPv4.

Шлюзы IP

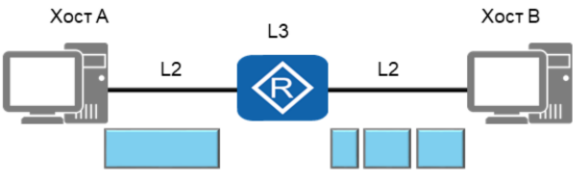


- Шлюзы используют IP-протокол для передачи пакетов между сетями.
- В локальной вычислительной сети роль шлюзов могут выполнять хосты.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- При пересылке пакет, прежде чем он будет инкапсулированием в кадр и передан физическим интерфейсом, сначала должен определить путь пересылки в данную сеть, а также интерфейс, через который он будет передан. Если запланированная сеть отличается от исходящей сети, пакет передается на шлюз, через который он может дойти до запланированного места назначения.
- Во всех сетях шлюз представляет собой устройство, способное управлять пакетами и принимать решения о том, как маршрутизировать пакеты, с тем чтобы достичь желаемого места назначения. Однако данное устройство должно получить информацию о маршруте к запланированной IP-сети назначения до маршрутизации пакетов. Если сети разделены физическим шлюзом, IP-адрес интерфейса (в одной сети или подсети), через который может быть достигнут этот шлюз, считается адресом шлюза.
- Если хосты принадлежат разным сетям, которые не разделены физическим шлюзом, функции шлюза должен выполнять хост, который сначала должен получить информацию о маршруте к сети, в которую должны быть переадресованы пакеты, и затем указать IP-адрес своего интерфейса как IP-адрес шлюза, через который можно достичь запланированной сети назначения.

Фрагментация IP

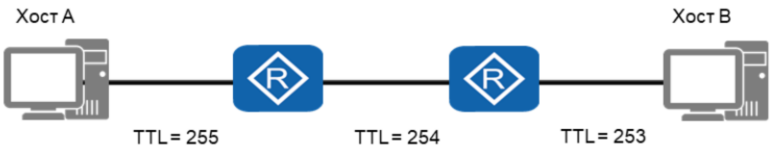


Версия	Длина заголовка	Поле DS	Общая длина
Идентификация		**Флаги**	**Смещение фрагментов**
Время жизни	Протокол	Контрольная сумма заголовка	
IP-адрес источника			
IP-адрес назначения			
Опции IP			

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Данные пересылаемых пакетов представляются в различных форматах и размерах, и часто размер передаваемых данных превышает размер, поддерживаемый средой передачи. Если это происходит, блок данных разбивается на меньшие блоки данных до их передачи. Процесс разбивки данных на управляемые блоки известен как фрагментация.
- Поля «идентификация», «флаги» и «смещение фрагментов» используются для управления сборкой фрагментов после их получения в конечном планируемом пункте назначения. Поле «идентификация» позволяет различать блоки данных потоков трафика, которые могут инициироваться одним и тем же хостом или различными хостами. Поле «флаги» определяет, какой из нескольких фрагментов представляет собой последний фрагмент, на котором запускается таймер до повторной сборки, и уведомляет о том, что должна начаться повторная сборка пакета.
- Наконец, поле «смещение фрагментов» содержит битовое значение каждого фрагмента, означающее часть числа фрагментов. Первый фрагмент задается значением 0 и последующие фрагменты определяют значение первого бита, следующего за предыдущим фрагментом, например, если исходный фрагмент содержит биты от 0 до 1259, следующему фрагменту будет присвоено значение смещения 1260.

Время жизни (Time To Live)

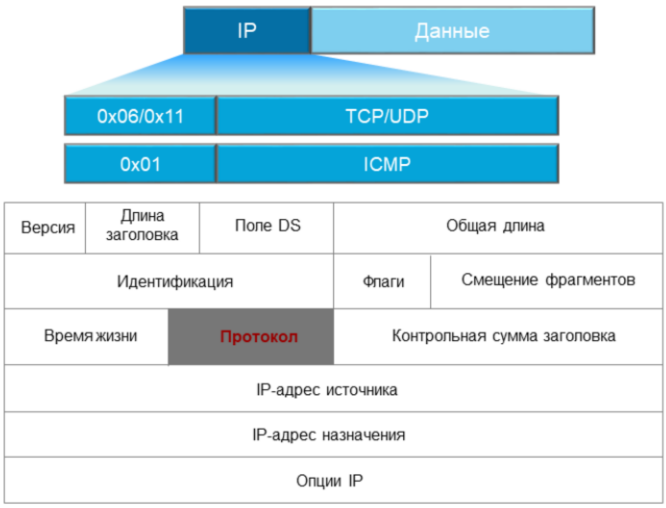


Версия	Длина заголовка	Поле DS	Общая длина	
Идентификация			Флаги	Смещение фрагментов
Время жизни	Протокол	Контрольная сумма заголовка		
IP-адрес источника				
IP-адрес назначения				
Опции IP				

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Поскольку пакеты передаются между сетями, то в случае некорректного определения маршрутов к IP-сетям в устройствах, выполняющих маршрутизацию трафика, они могут попадать в петли. Это может привести к потере пакетов в течение цикла передачи, и они, в итоге, не достигнут целевого назначения. Если это происходит, то по мере потери все большего и большего числа пакетов, направленных в один и тот же пункт назначения, в сети будет возникать перегрузка, обусловленная большим числом ошибочных пакетов.
- Чтобы предотвратить такую перегрузку при формировании петель, поле «время жизни» (TTL) определяется как часть заголовка IP, в котором устанавливается значение 1 каждый раз, когда пакет походит через устройство уровня 3 для достижения данной сети. Начальное значение TTL зависит от первоначального источника, однако, если TTL имеет значение 0, пакет будет отбрасываться, а на IP-адрес источника, который можно найти в заголовке IP отброшенного пакета, будет приходить сообщение об ошибке (ICMP).

Поле «Протокол»



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Во время проверки, достиг ли пакет целевого назначения, сетевой уровень должен определить следующий набор команд на выполнение. Для этого анализируется поле «протокол» в заголовке IP. Как и в поле «тип» заголовка кадра, следующий набор команд задается шестнадцатеричным значением.
- Следует понимать, что поле «протокол» может содержать значение протокола сетевого уровня, например Internet Control Message Protocol (ICMP), но также и значение протокола верхнего уровня, например Transmission Control Protocol (06/0x06) или Datagram User Datagram Protocol (17/0x11). Последние два являются протоколами транспортного уровня эталонных моделей TCP/IP и OSI.

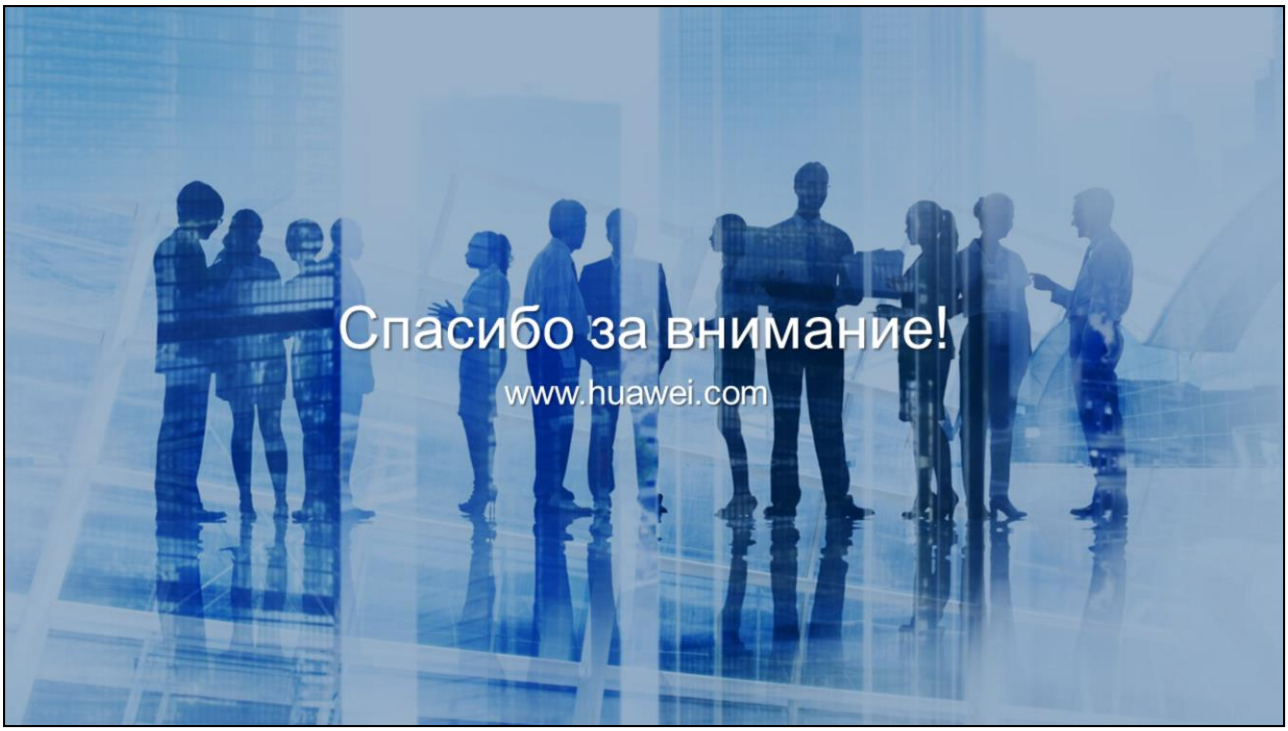
Заключение

- Для чего используется маска подсети IP?
- Какова цель поля «время жизни» (TTL) в заголовке IP?
- Как используются шлюзы в IP-сети?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Маска подсети IP представляет собой 32-разрядное значение, которое описывает логическое разделение между битовыми значениями IP-адреса. IP-адрес делится на две части, в которых битовые значения представляют либо адрес сети, либо адрес подсети, а также адрес хоста в данной сети или подсети.
- Функция Time To Live (TTL) применяется к IP-пакетам, которые не могут достичь запланированной сети, и означает предельный период времени или переходов, за который набор данных может существовать до своего исчезновения. Наличие этого параметра не позволяет пакету бесконечно ходить по сети. Значение TTL зависит от первоначального источника.
- Шлюзы представляют собой точки доступа между IP-сетями, к которым можно перенаправлять трафик в случае, если запланированная сеть назначения отличается от сети, из которой исходит пакет.


Спасибо за внимание!
www.huawei.com

Протокол обмена управляющими сообщениями (ICMP)

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

ICMP — это протокол, который наряду с IP-протоколом выполняет обмен сообщениями и при этом компенсирует недостаточную надежность IP. Изучение принципов реализации ICMP поможет разобраться в дальнейшем с многочисленными операциями и приложениями, работающими по протоколу ICMP, а также базовыми сообщениями, на основе которых часто выполняются процессы.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

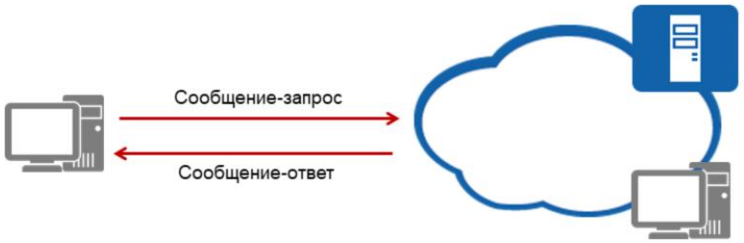
Цели

По завершении этого раздела обучающиеся научатся :

- Описывать определенные процессы, которые работают с протоколом ICMP.
- Определять значения полей «Тип» и «Код», используемых в ICMP.
- Объяснять функцию ICMP в работе утилит ping и traceroute.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

ICMP

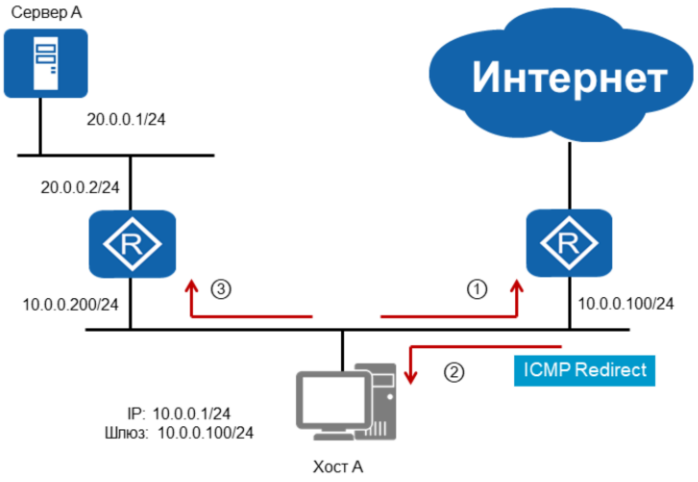


- Сообщения ICMP используются для передачи информации маршрутизации, диагностики и ошибок.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Протокол обмена управляющими сообщениями (Internet Control Message Protocol), являющийся неотъемлемой частью протокола IP, осуществляет передачу уведомлений между шлюзами и хостами источника, если требуются запросить диагностическую информацию или обеспечить поддержку маршрутизации, а также для передачи сообщений об ошибках при обработке датаграмм. Цель этих управляющих сообщений заключается в достижении обратной связи о проблемах в среде передачи, и такие сообщения не гарантируют, что датаграмма будет доставлена, или что будет возвращено контрольное сообщение.

ICMP (маршрутизация)



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Сообщения ICMP Redirect — это самый стандартный пример, в котором ICMP используется в качестве средства поддержки функций маршрутизации. На приведенной схеме пакет пересылается шлюзу хостом A на основе адреса шлюза хоста A. Шлюз определяет, что полученный пакет предназначен для пересылки по адресу следующего шлюза, который является частью той же сети, что и хост, инициирующий пакет, отдельно выделив неоптимальный путь передачи между хостом и шлюзами.
- Для решения этой задачи на хост отправляется сообщение о перенаправлении (ICMP Redirect), в котором содержится рекомендация хосту отправлять трафик, предназначенный для планируемого пункта назначения, непосредственно на шлюз, с которым связана сеть назначения, так как такой маршрут является наиболее коротким путем к месту назначения. Однако шлюз принимает решение о передаче данных исходного пакета в запланированный пункт назначения.

ICMP (диагностика)

- Для запроса и ответа используются два отдельных сообщения.
- Данные сообщения обычно связаны с работой утилиты Ping.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Эхо-сообщение ICMP служит средством диагностики, которое определяет наличие связи между данным источником и пунктом назначения, а также предоставляет дополнительную информацию, например время прохождения маршрута в обоих направлениях, с целью диагностической передачи, в процессе которой будет измерена задержка. Данные, полученные в эхо-запросе, возвращаются в виде отдельного эхо-ответа.

ICMP (ошибки)

- Сообщение уведомляет источник отправки пакетов о проблемах с передачей пакетов.
- Используется IP-адрес источника в заголовке IP-кадра уведомления.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- ICMP обеспечивает обмен различными сообщениями об ошибках, в которых часто содержатся проблемы достижимости узлов, и формируют конкретные отчеты об ошибках, позволяющие получить более четкое представление для хоста о том, почему передача в планируемый пункт назначения не выполнена.
- Среди типичных примеров — возникновение петли в сети, которая привела к истечению срока жизни (параметр time to live, содержащийся в заголовке IP), в результате чего сгенерировалось сообщение об ошибке «ttl exceeded in transit». Другой пример — недостижимый планируемый пункт назначения, что может быть связано с более конкретной проблемой планируемой сети, не известной получающим шлюзом, или с тем, что планируемый хост в сети назначения не обнаружен. Во всех таких событиях генерируется сообщение ICMP с информацией о пункте назначения в соответствии с IP-адресом источника, найденном в заголовке IP-кадра, для гарантии, что сообщение будет передано отправляющему хосту.

Формат ICMP

- Параметры ICMP представлены полями «тип» и «код».
- Для идентификации недоставленного пакета часто передаются дополнительные данные.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Сообщения ICMP отправляются с использованием основного заголовка IP, который является неотъемлемой частью сообщения ICMP, как например в случае с параметром TTL, который используется для определения достижимости пункта назначения. В основе формата сообщения ICMP лежат два поля идентификации сообщений — «тип» и «код», где поле «тип» содержит общее описание типа сообщения, а поле «код» содержит более конкретный параметр типа сообщения.
- Контрольная сумма — это средство проверки целостности сообщения ICMP. 32 бита включены для обозначения переменных параметров, часто неиспользуемых и поэтому устанавливаемых в значение 0 при отправке сообщения ICMP, однако если это сообщение о перенаправлении (ICMP redirect), данное поле содержит IP-адрес шлюза, на который хост должен перенаправлять пакеты. Поле параметра при передаче эхо-запросов содержит идентификатор и порядковый номер, которые источник использует для ассоциирования отправленных эхо-запросов с полученными эхо-ответами, особенно в случае, если в определённый пункт назначения передаются несколько запросов.
- В качестве последнего средства трассировки данных в отношении конкретного процесса, в сообщении ICMP могут передаваться заголовок IP-кадра и блок, содержащий информацию верхнего уровня. Такая информация позволяет источнику идентифицировать процесс, в котором произошла ошибка, например при истечении времени жизни (ICMP TTL) в транзитной передаче.

Поля ICMP «Тип» и «Код»

Тип	Код	Описание
0	0	Эхо-ответ
3	0	Сеть недостижима
3	1	Хост недостижим
3	2	Протокол недостижим
3	3	Порт недостижим
5	0	Датаграмма перенаправления в сети
8	0	Эхо-запрос

- В поле «Тип» указывается формат сообщения.
- В поле «Код» содержится более конкретное описание сообщения.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Существует большое количество значений типа ICMP, которые четко определяют функцию протокола ICMP. В некоторых случаях для конкретизации записи в поле «тип» поле «код» не требуется. Например, это характерно для эхо-запроса, у которого в поле «тип» стоит значение 8, и соответствующего эхо-ответа, который генерируется и отправляется как отдельное ICMP-сообщение по исходному адресу отправителя и определяется значением 0 в поле «тип».
- Напротив, в некоторых случаях значение поля «тип» содержит общую информацию, которую необходимо конкретизировать с помощью поля «код», например значение 3. Такое значение указывает, что данное место назначения недостижимо, в то время как поле «код» определяет конкретно, что отсутствует — сеть, хост, протокол, порт (TCP/UDP), способность выполнять фрагментацию (код 4) — или указывает исходный маршрут (код 5), в котором пакет, для которого точно или частично определен путь передачи через сеть, не достигает места назначения.

Применение ICMP-сообщений: утилита ping


```
                        <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
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Понять принципы применения ICMP можно с помощью таких инструментов, как утилита Ping, которая определяет достижимость пункта назначения, а также собирает необходимую информацию. Параметры утилиты позволяют конечному пользователю указывать характер поведения конечной системы при генерировании сообщений ICMP с учетом размера датаграммы ICMP, количества сообщений ICMP, генерируемых хостом, а также продолжительности ожидания ответа до истечения таймаута. Это важно, когда происходит большая задержка, поскольку утилита Ping может сообщить о таймауте до того, как сообщение ICMP получит возможность вернуться к источнику.

Результаты выполнения команды ping

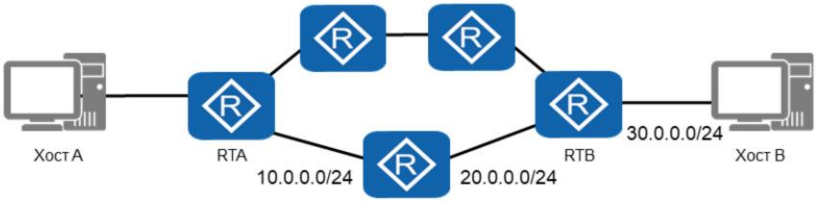
```
<RTA>ping 10.0.0.2
  PING 10.0.0.2 : 56  data bytes, press CTRL_C to break
Reply from 10.0.0.2 : bytes=56 Sequence=1 ttl=255 time=340 ms
Reply from 10.0.0.2 : bytes=56 Sequence=2 ttl=255 time=10 ms
Reply from 10.0.0.2 : bytes=56 Sequence=3 ttl=255 time=30 ms
Reply from 10.0.0.2 : bytes=56 Sequence=4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


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- В общем выводе ICMP-ответа на ICMP-запрос Ping содержится подробная информация о месте назначения, к которому была послана датаграмма, и о размерах создаваемой датаграммы. Кроме того, выводится порядковый номер поля «последовательность», переданное как часть эхо-ответа (значение «тип» равно 0), значение TTL, взятое из заголовка IP, а также время прохождения маршрута в обоих направлениях, которое также передается в поле «Опции IP» в заголовке IP-кадра.

Применение ICMP-сообщений: утилита Traceroute




```
<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
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Еще одним стандартным инструментом ICMP является утилита traceroute, которая измеряет путь передачи и задержки на основе последовательности транзитных узлов между сетями и сравнивает его со значением TTL в заголовке IP.
- Достижимость каждого транзитного узла вдоль маршрута до определенного пункта назначения определяется путем установки значения TTL в заголовке IP в значение 1, что приведет к истечению времен жизни TTL до того, как приемный шлюз сможет продолжить передачу ICMP-сообщения. В результате информация об истекшем TTL будет передана в транзитном сообщении вместе с информацией о метке времени, что позволит провести оценку пути по сети посредством датаграммы, направленной в пункт назначения, и измерения времени прохождения маршрута в обоих направлениях. Это обеспечивает эффективность определения точки потери любого пакета или задержки, которые могут возникнуть в сети, а также помогает при обнаружении петель маршрутизации.

Результаты выполнения команды traceroute

```
<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
```

- В выводе команды traceroute отображаются результаты передачи через последовательность транзитных узлов.
- Значение TTL используется для определения предельного времени выполнения перехода на следующий узел для каждого набора результатов.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

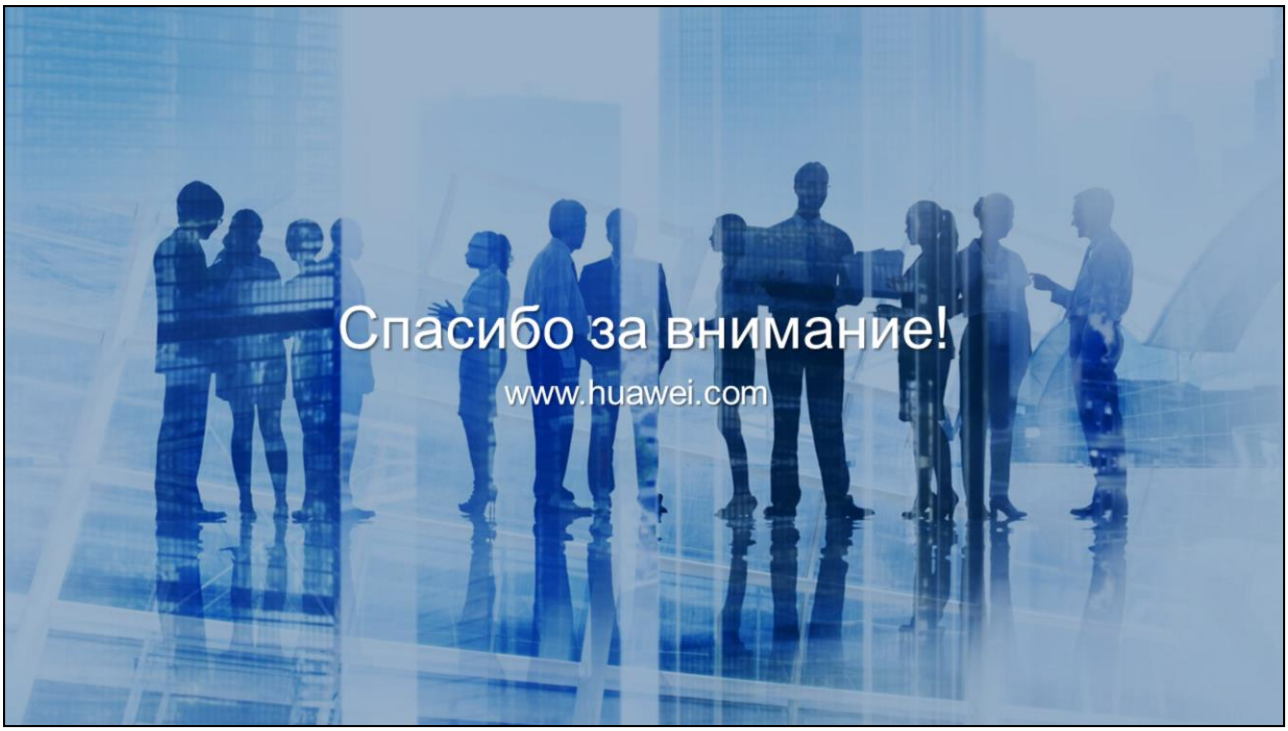
- Для реализации функции traceroute в маршрутизаторах Huawei серии ARG3 используется протокол транспортного уровня UDP, который определяет сервисный порт в качестве пункта назначения. Каждый узел посылает три тестовых пакета, для которых значение TTL сначала устанавливается в значение 1 и увеличивается после каждых трех пакетов. Кроме того, для первого пакета порт назначения UDP устанавливается в значение 33434, которое увеличивается с каждым последовательным тестовым пакетом. Генерируется результат последовательности транзитных узлов, позволяющий определить путь, а также обнаружить любую возникшую общую задержку.
- Это достигается путем измерения продолжительности между моментом отправки сообщения ICMP и получением ошибки ICMP транзитной передачи, вызванной истечением времени TTL. При получении пакета конечный пункт назначения не может обнаружить порт, указанный в пакете, и, таким образом, возвращает пакет ICMP с параметрами Type 3, Code 3 (Port Unreachable). После трех попыток тест трассировки заканчивается. Результат проверки каждого тестового пакета отображается на узле-источнике в соответствии с маршрутом от источника до пункта назначения. Если при использовании команды trace route возникает ошибка, может отображаться следующая информация:
- !H: The host is unreachable. (Хост недостижим)
- !N: The network is unreachable. (Сеть недостижима)
- !: The port is unreachable. (Порт недостижим)
- !P: The protocol type is incorrect. (Неверный тип протокола)
- !F: The packet is incorrectly fragmented. (Пакет некорректно фрагментирован)
- !S: The source route is incorrect. (Неверный исходный маршрут)

Заключение

- Какие два типа сообщений ICMP используются для успешного выполнения утилиты Ping?
- Какие действия будут предприняты принимающим шлюзом, если значение TTL в заголовке IP датаграммы достигнет нуля?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Утилита Ping пытается обнаружить пункт назначения с помощью эхо-запроса типа 8. Исходному источнику возвращается эхо-ответ, поле «тип» которого содержит значение 0, на основе IP-адреса источника в поле заголовка IP.
- Если значение TTL IP-датаграммы достигнет 0 до того, как датаграмма достигнет запланированного пункта назначения, шлюзовое устройство, получающее датаграмму, отбросит ее и возвратит сообщение ICMP источнику, уведомив его, что данная датаграмма не смогла достичь запланированного пункта назначения. Конкретная причина будет определяться значением поля «код», например это может быть ошибка обнаружения хоста или порта на хосте, а также отсутствие поддержки данного сервиса данным протоколом и т.д.


Спасибо за внимание!
www.huawei.com

Протокол определения адреса (ARP)

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

Для передачи данных в конечный пункт сети необходима взаимосвязь между сетевым уровнем и протоколами нижнего уровня. Необходимо четко понимать принцип создания такой взаимосвязи с помощью протокола определения адреса (Address Resolution Protocol; ARP) и предотвращения генерирования ненужного дополнительного широковещательного трафика в сети.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Цели

По завершении этого раздела обучающиеся научатся:

- Объяснять, как определяется MAC-адрес с помощью ARP.
- Объяснять функцию таблицы кэша ARP.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

ARP

- **Передача на канальном уровне основана на знании MAC-адреса получателя на данном уровне.**

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- После инкапсуляции данных IP-протокол на сетевом уровне указывает целевой IP-адрес, которому, в конечном итоге, предназначены эти данные, а также интерфейс, через который передаются данные, однако перед передачей источнику необходимо сообщить о целевом (MAC-) адресе Ethernet, на который должны передаваться данные. Протокол определения адреса (ARP), входящий в стек протоколов TCP/IP, выполняет обнаружение MAC-адреса пересылки, обеспечивая достижимость IP-узла. Следующий узел Ethernet должен быть обнаружен до завершения инкапсуляции данных.

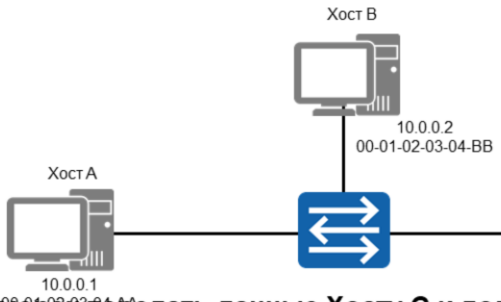
Формат ARP

- Пакет ARP работает на канальном уровне, этим объясняется отсутствие заголовка IP.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Пакет ARP генерируется в процессе обнаружения физических целевых адресов. Первоначально в сообщении обнаружения будет содержаться частичная информация, поскольку необходимо выяснить адрес оборудования назначения или MAC-адрес. Поле «Тип оборудования» содержит значение Ethernet, а поле «Тип протокола» — IP, что указывает на технологии определения адреса, выполняемого протоколом ARP. В полях «Длина оборудования» и «Длина протокола» содержатся длина физического адреса и длина логического адреса соответственно, значение указывается в байтах.
- В поле «Код операции» указывается одно из двух состояний — ARP discovery устанавливается в значение REQUEST, и это означает, что при получении пунктом назначения ARP transmission должен быть сгенерирован ответ – REPLY, в отношении которого хосту, принимающему этот пакет, не требуется выполнять дальнейшие операции и после которого пакет ARP будет отброшен. Физический адрес источника — это MAC-адрес отправителя на физическом сегменте, которому генерируется сообщение ARP. Логический адрес источника — это IP-адрес отправителя.
- Адрес оборудования назначения — это физический адрес (Ethernet), на который пересылаются данные по протоколу Ethernet, однако эта информация отсутствует в запросе ARP, вместо нее указывается значение 0. Адрес протокола назначения определяет планируемый IP-адрес получателя, достижимый по каналам Ethernet.

Процесс работы протокола ARP

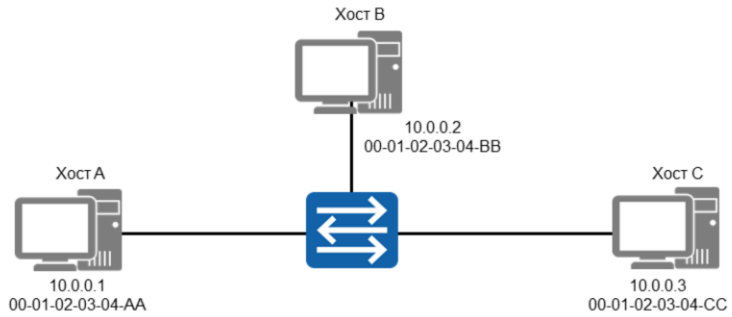


- **Хост A намерен передать данные Хосту C и должен определить достижимость пункта назначения на канальном уровне.**

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Сетевой уровень представляет собой логический путь между источником и пунктом назначения. Достижение целевого IP-адреса назначения зависит, во-первых, от возможности установления физического пути к пункту назначения, и для этого необходимо создать взаимосвязь между планируемым IP-адресом получателя и физическим интерфейсом следующего транзитного узла, на который может быть переадресован трафик.
- Для пункта назначения хост определяет IP-адрес, на который необходимо переслать данные, однако перед началом инкапсуляции данных хост должен определить, известен ли физический путь передачи. Если такой путь передачи известен, выполняется инкапсуляция, однако часто пункт назначения не известен, поэтому до выполнения инкапсуляции данных необходим процесс определения адреса с помощью ARP.

Поиск в кэше ARP



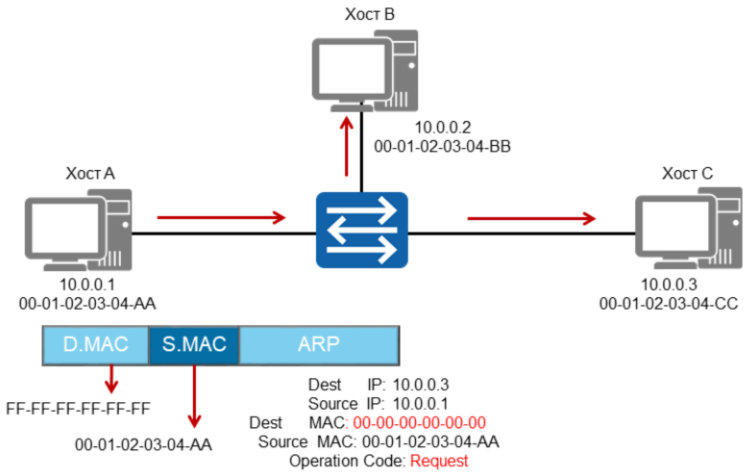

```
Host A>arp -a

Internet Address    Physical Address   Type
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Кэш ARP представляет собой таблицу, в которой IP-адреса хостов ассоциированы с физическими (MAC) адресами. Любой хост, связывающийся с локальным или удаленным пунктами назначения, сначала должен узнать MAC-адрес получателя, через который будет установлена связь.
- Изученные адреса заполнят таблицу кэша ARP и останутся активными в течение фиксированного периода времени, отведенного для обнаружения запланированного пункта назначения без необходимости добавления процессов обнаружения ARP. После окончания фиксированного периода таблица кэша ARP удалит записи ARP для сохранения целостности таблицы кэша ARP, так как любое изменение в физическом местоположении хоста назначения может привести к тому, что отправляющий хост непреднамеренно направит данные в пункт назначения, где узел назначения больше не расположен.
- Поиск кэша ARP — это первая операция, выполняемая конечной системой, прежде чем определить, необходима ли генерация запроса ARP. Для пунктов назначения, находящихся за пределами собственных сетей хостов, выполняется поиск кэша ARP, во время которого определяется физический адрес назначения шлюза, через который можно достичь запланированной сети назначения.

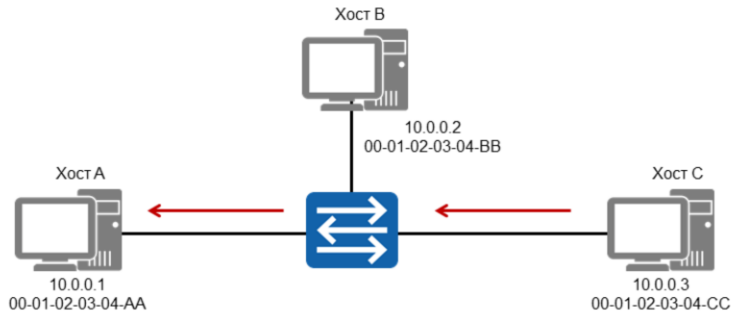
Процесс запроса ARP



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Если запись кэша ARP невозможно определить, выполняется процесс запроса ARP. Данный процесс включает генерирование пакета запроса ARP, а также заполнение полей пакета значениями адресов отправителя и получателя, а также значением физического адреса отправителя. Физический адрес получателя неизвестен, поэтому в поле указывается значение, равное 0. Запрос ARP инкапсулируется в заголовок и хвостовую часть кадра Ethernet в процессе передачи. Исходный MAC-адрес заголовка кадра устанавливается в качестве исходного адреса хоста-отправителя.
- Хост в настоящее время не знает о местоположении пункта назначения и поэтому должен отправить запрос ARP широковещательной передачей всем пунктам назначения в пределах одной локальной сети. Это означает, что в качестве MAC-адреса назначения используется широковещательный адрес. Кадр с заполненными полями направляется на физический уровень, где он передается по физической среде, к которой подключен хост. Широковещательный пакет ARP будет передаваться по всей сети во все пункты назначения, включая любой шлюз, однако такой шлюз не допустит пересылку такого пакета в любую сеть за пределами текущей сети.

Процесс ответа ARP

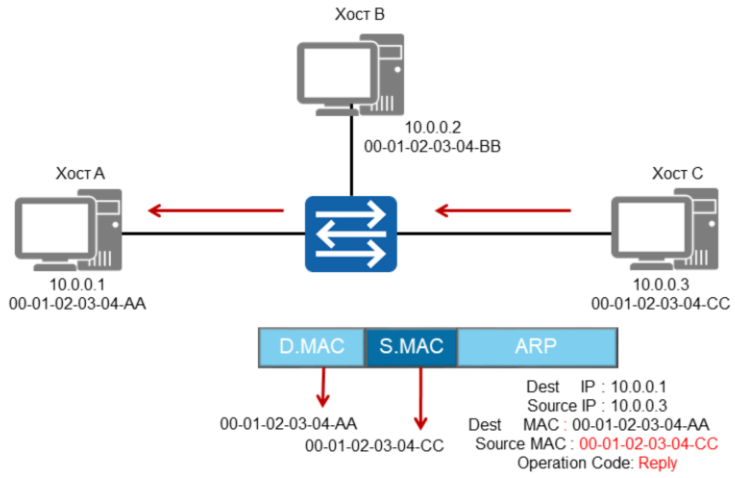



```
                    Host C>arp -a
  Internet address  Physical address      Type
  10.0.0.1          00-01-02-03-04-AA     Dynamic
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Если запланированный пункт назначения сети существует, кадр поступит на его физический интерфейс, где он будет обработан протоколами нижнего уровня. Широковещание ARP означает, что все пункты назначения в пределах сети получат рассылаемый кадр, но обработка запроса ARP будет остановлена, так как логический адрес пункта назначения не совпадает с IP-адресом этих пунктов назначения.
- Если IP-адрес назначения соответствует принимающему хосту, пакет ARP будет обработан. Принимающий хост сначала обрабатывает заголовок кадра, а затем запрос ARP. Хост назначения вносит в свою таблицу кэша ARP информацию, содержащуюся в поле физического адреса источника в заголовке ARP, таким образом, при любой потребности в передаче кадров будет сгенерирован кадр одноадресной передачи на источник, с которого был получен запрос ARP.

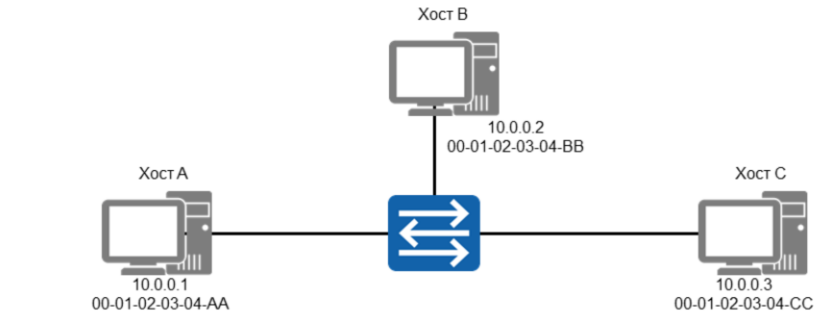
Процесс ответа ARP



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Пункт назначения определит, что полученный пакет ARP является запросом ARP, и сгенерирует ответ ARP, который будет возвращен источнику на основе информации, содержащейся в заголовке ARP. Для ответа генерируется отдельный пакет ARP, для которого заполняются поля логических адресов отправителя и получателя. Однако, логический адрес получателя, содержащийся в ARP-запросе, будет теперь логическим адресом отправителя в ARP-ответе, и наоборот логический адрес отправителя, содержащийся в ARP-запросе, будет теперь логическим адресом получателя в ARP-ответе.
- В поле физического адреса получателя указывается MAC-адрес источника, определенный при получении запроса ARP. А требуемый физический адрес получателя запроса ARP включается как физический адрес отправителя ответа ARP, и в поле кода операции устанавливается значение ответа, которое информирует получателя о цели полученного пакета ARP, после чего пункт назначения может отбросить пакет ARP без каких-либо дополнительных сообщений. Ответ ARP инкапсулируется в заголовок и хвостовую часть кадра Ethernet, при этом в качестве MAC-адреса назначения кадра Ethernet будет использована запись из таблицы кэша ARP, что позволит переслать кадр как кадр одноадресной передачи на хост, инициирующий запрос ARP.

Кэш ARP

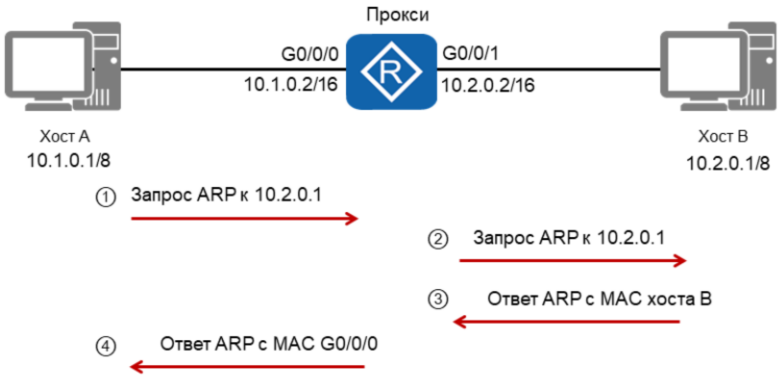



```
Host A>arp -a
Internet address  Physical address      Type
10.0.0.3          00-01-02-03-04-CC     Dynamic
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Получив ответ ARP, исходный хост подтвердит, что запланированный пункт назначения корректен, по заголовку кадра, а по значению поля «тип» определит, что заголовком пакета является ARP, после чего отбросит заголовки кадра. Затем ответ ARP будет обработан, при этом физический адрес отправителя ответа ARP будет внесен в таблицу кэша ARP исходного хоста (Хост A).
- После обработки ответа ARP пакет будет отброшен, и MAC-адрес получателя будет использован в процессе инкапсуляции исходного приложения или протокола, который первоначально запрашивал обнаружение пункта назначения на канальном уровне.

Прокси-ARP

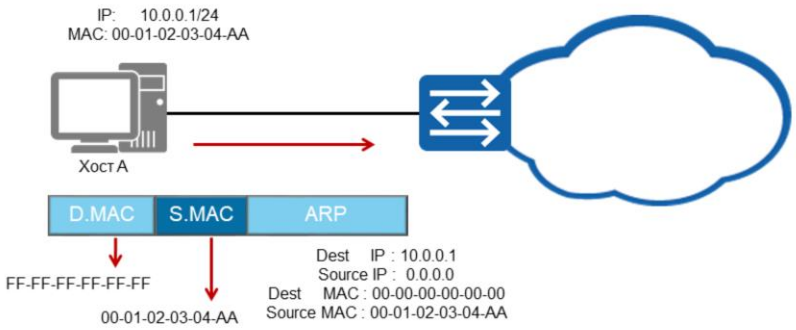


- Прокси-ARP обеспечивает обнаружение каналов передачи данных между сетями.
  - Прокси отвечает от имени хоста B, указав свой адрес (G0/0/0).

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Протокол ARP также применяется, например для реализации шлюзов прозрачных подсетей, которые необходимо для передачи по физическим сетям, где хосты считаются частью одной и той же подсети. Это называется Proxy ARP, так как шлюз работает в качестве прокси для двух физических сетей. Запрос ARP, сгенерированный для пункта назначения, который входит в состав той же подсети, в конечном итоге будет получен шлюзом. Шлюз может определить, что запланированный пункт назначения находится за пределами физической сети, на которой был сгенерирован запрос ARP.
- Поскольку запросы ARP нельзя перенаправить за пределы широковещательного домена, шлюз продолжит генерировать свой запрос ARP для определения достижимости запланированного пункта назначения, используя свои логический и физический адреса в качестве адресов отправителя для генерируемого запроса ARP. Если запланированный пункт назначения существует, ответ ARP будет получен шлюзом, в таблицу кэша ARP которого будет внесен физический адрес отправителя.
- Шлюз при подтверждении достижимости запланированного пункта назначения генерирует ответ ARP на исходный источник (Хост A), используя физический адрес интерфейса, с которого был передан ответ ARP. Для передачи на канальном уровне шлюз будет функционировать в качестве агента между двумя физическими сетями, при этом оба хоста будут пересылать трафик, предназначенный пунктам назначения, расположенных в различных физических сетях, на соответствующий физический адрес шлюза "Proxy".

Gratuitous ARP



- В одной IP-сети возможна ситуация выделения одного и того же IP-адреса.
- Для обнаружения конфликтов IP-адресов используется ARP.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

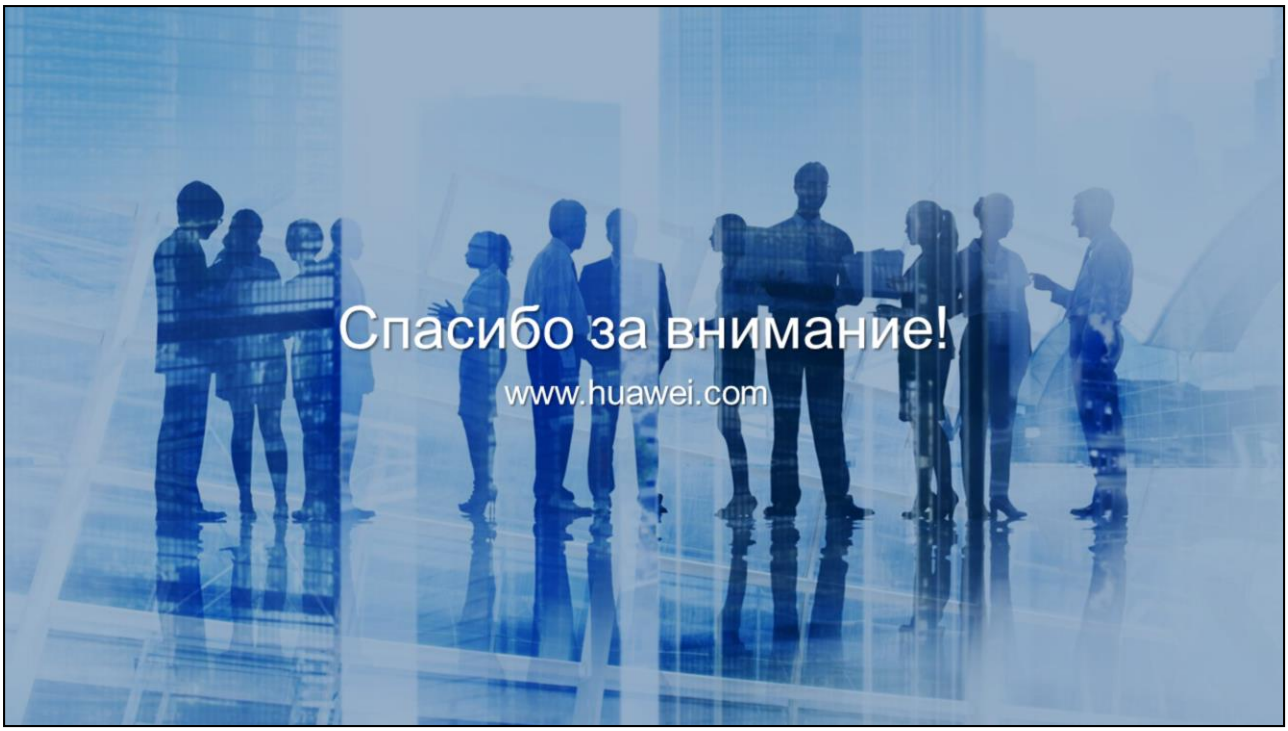
- В случае ввода в сеть нового оборудования, необходимо, чтобы хост мог определить, является ли выделенный ему логический адрес уникальным в сети — это предотвратит конфликты, связанные с дублированием адресов. Для этого генерируется запрос ARP, где в качестве адреса получателя запроса ARP выступает IP-адрес самого хоста.
- Запрос ARP рассылается по всей сети по всем пунктам назначения на канальном уровне. Для этого MAC-адрес получателя устанавливается как широковещательный, таким образом, все конечные станции и шлюзы получат рассылаемый кадр. Все пункты назначения будут обрабатывать данный кадр, и если один из них обнаружит, что IP-адрес получателя в запросе ARP совпадает с адресом принимающей конечной станции или шлюза, будет сгенерирован ответ ARP и возвращен на хост, который сгенерировал запрос ARP.
- С помощью этого метода исходный хост может распознать дубликат IP-адреса в сети и пометить этот конфликт флагом с целью запроса на выделение уникального адреса. Данный метод генерации запроса на основе IP-адреса хоста лежит в основе механизма самообращенных запросов - gratuitous ARP.

Заключение

- Какие действия должны быть предприняты конечной станцией перед генерированием запроса ARP?
- Когда генерируются и рассылаются сообщения gratuitous ARP в локальной сети?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Хост должен сначала определить, известен ли уже адрес пересылки на канальном уровне, проверив свой кэш ARP (таблица MAC-адресов). Если запись будет обнаружена, конечная система создаст кадр для передачи без использования протокола ARP. Если запись найти не удастся, будет инициирован процесс ARP, и запрос ARP будет разослан в локальной сети широковещательной передачей.
- Сообщения Gratuitous ARP обычно генерируются на узле, где для устройства, подключенного к сети, имеет место новая настройка или изменение IP-адреса, а также в любое время, когда любое устройство физически подключается к сети. В обоих случаях процесс gratuitous ARP должен гарантировать, что используемый IP-адрес является уникальным.


Спасибо за внимание!
www.huawei.com

Протоколы транспортного уровня

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

Транспортный уровень связан с работой протоколов сквозной передачи. Тип используемого протокола определяется, как только данные достигают запланированного пункта назначения. TCP и UDP — пример протоколов транспортного уровня, поддерживаемые IP-сетями. Выбор протоколов, используемых на транспортном уровне, часто зависит от таких характеристик, как чувствительность к задержке и потребность в высокой надежности. В данном разделе основное внимание уделено характеристикам, которые демонстрирует работа каждого протокола.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

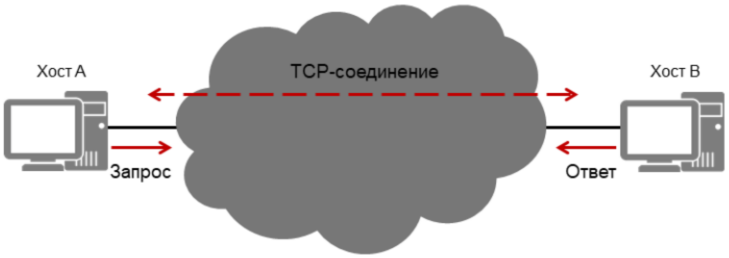
Цели

По завершении этого раздела обучающиеся научатся:

- Описывать общие различия между протоколами TCP и UDP.
- Описывать виды нагрузок, для передачи которых применяются протоколы TCP и UDP.
- Различать известные номера портов TCP и UDP.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Протокол управления передачей (TCP)



- Перед началом передачи данных устанавливается соединение.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Transmission Control Protocol (TCP) является протоколом сквозной передачи с предварительной установкой соединения. Протокол, входящий в стек TCP/IP и выполняющий функции транспортного уровня, призван поддерживать приложения, работающие в многосетевых средах. Протокол управления передачей обеспечивает надежную связь между парами процессов в хост-компьютерах, подключенных к отдельным, но взаимосвязанным компьютерным сетям связи. Опираясь на протоколы нижнего уровня, TCP обеспечивает достижимость хостов, посредством которых устанавливается надежное соединение между данными процессами. Принцип работы TCP основан на предварительном информационном обмене между источником и пунктом назначения, на основе которого устанавливается соединение перед началом передачи сегментов транспортного уровня.

Порты TCP

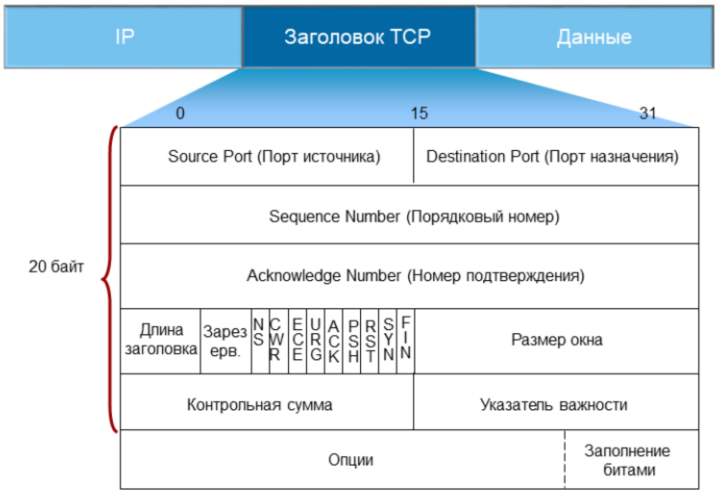
Протокол	Порт
FTP	20 - 21
HTTP	80
TELNET	23
SMTP	25

- Определенные порты выделяются определенным сервисам.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Протокол TCP, позволяющий множеству процессов на одном хосте одновременно использовать средства передачи TCP, предоставляет набор логических портов на каждом хосте. Значение порта вместе с адресом сетевого уровня называется сокетом. Два сокета в паре формируют уникальный идентификатор каждого соединения, в частности, если сокет используется одновременно в нескольких соединениях. Иными словами, любому процессу может потребоваться отличить определенные свои потоки связи от потоков другого процесса (или процессов), при этом каждый процесс может взаимодействовать с портом или портами других процессов через свои определенные порты.
- Определенные процессы, имеющие свои порты, могут инициировать соединения на таких портах. Эти порты, определенные Агентством по выделению имен и уникальных параметров протоколов (IANA), также называемые хорошо известными портами, имеют диапазон значений 0-1023. Выделенные или зарегистрированные порты IANA также могут иметь диапазон значений 1024-49151. Динамические порты, также называемые частными или эфемерными портами, имеют значения в диапазоне 49152-65535, и такие порты не предназначены для какого-либо конкретного применения. Хостам обычно выделяется порт пользователя, для которого сгенерирован сокет в данном приложении.
- Примеры стандартных работающих на базе TCP-протокола приложений, которым были выделены хорошо известные номера портов — FTP, HTTP, TELNET и SMTP, которые, в свою очередь, часто работают вместе с другими известными транспортными протоколами, такими как POP3 (порт 110) и IMAP4 (порт 143).

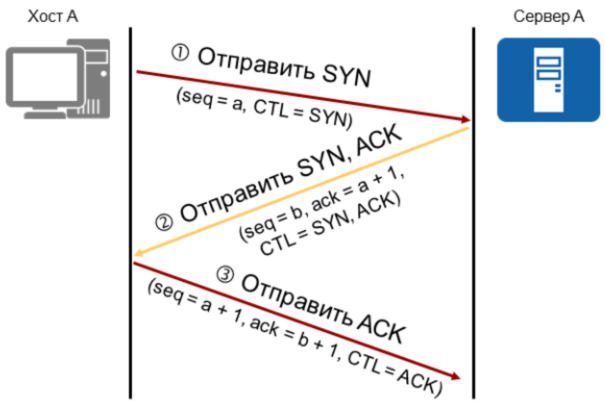
Заголовок TCP



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- С помощью заголовка TCP приложения, работающие на базе TCP, надежно передают потоки данных с предварительным установлением соединения. К таким потокам применяется процедура управления. Номер порта источника генерируется при попытке хоста установить соединение с TCP-приложением. Для данного приложения портом назначения будет являться известный или зарегистрированный порт, с которым ассоциировано известное или зарегистрированное приложение.
- Управляющие биты (флаги) выполняют следующие функции: бит URG означает, что поле «Указатель важности» задействовано; бит ACK означает, что поле «Номер подтверждения» задействовано; бит PSH инструктирует получателя протолкнуть данные, накопившиеся в приемном буфере, в приложение пользователя; бит RST — оборвать соединения, сбросить буфер, бит SYN — синхронизация номеров последовательности; установка флага FIN указывает на завершение соединения. Дополнительные управляющие биты: CWR (Congestion Window Reduced) — поле «Окно перегрузки уменьшено» — флаг установлен отправителем, чтобы указать, что получен пакет с установленным флагом ECE; ECE (ECN-Echo) — Поле «Эхо ECN» — указывает, что данный узел способен на ECN (явное уведомление перегрузки) и для указания отправителю о перегрузках в сети.
- ECN-nonce позволяет получателю уведомить отправителя, что подтверждаемый сегмент отправителя был принят без маркеров перегрузки. Случайные однобитовые значения (nonce) помещаются в 2-битовый код ECT. Однобитовая сумма этих значений возвращается в виде флага в заголовке TCP, называемого битом NS. Поле «Опции» содержит параметры, которые могут быть включены в состав заголовка TCP и часто используются во время первоначального установления соединения, как в случае с максимальным размером сегмента (MSS), используемым для определения размера сегмента, который должен использовать приемник. Размер заголовка TCP должен быть равен 32 битам, в противном случае добавляются дополнительные 0.

Установление соединения TCP

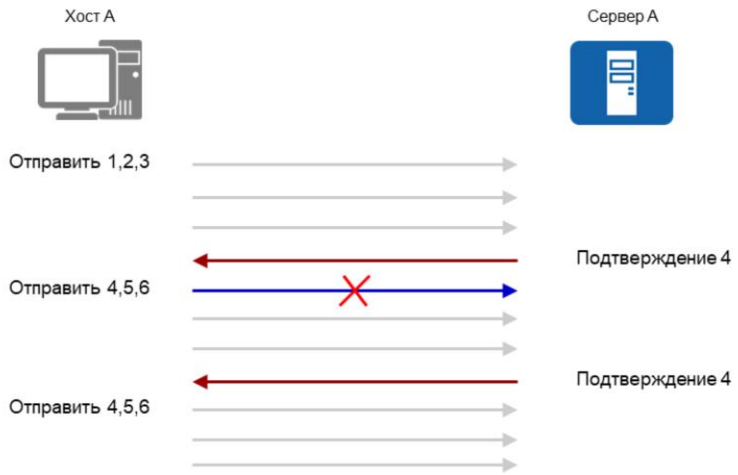


- Соединение TCP устанавливается после прохождения процедуры трехстороннего рукопожатия.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.
HUAWEI

- При возникновении необходимости обмена данными между двумя процессами каждый TCP должен сначала установить соединение (инициализировать синхронизацию передачи с каждой стороны). Когда передача будет завершена, соединение будет разъединено или закрыто, чтобы освободить ресурсы для других сеансов. Поскольку соединения устанавливаются между ненадежными хостами и через ненадежный интернет-домен, во избежание ошибочной инициализации соединений используется механизм рукопожатия с синхронизированными номерами последовательности.
- Создаваемое соединение проходит через серию состояний. Состояние LISTEN означает, что сервер ожидает запросов установления соединения от клиента. SYN-SENT - клиент отправил запрос серверу на установление соединения и ожидает ответа. SYN-RECEIVED - сервер получил запрос на соединение, отправил ответный запрос и ожидает подтверждения. ESTABLISHED - соединение установлено, идёт передача данных.
- Механизм рукопожатия TCP-интерфейса начинается с номера начальной последовательности, генерируемого инициирующим TCP в рамках процесса синхронизации (SYN). Затем исходный сегмент TCP с установленным флагом SYN передается запланированному TCP-узлу назначения для достижения состояния SYN-SENT. В рамках процесса подтверждения, TCP-узел на другом конце генерирует свой номер начальной последовательности, чтобы синхронизировать поток TCP в другом направлении. Этот TCP передает этот номер последовательности, а также номер подтверждения, который равен полученному номеру последовательности, увеличенному на один, вместе с установленными флагами SYN и ACK в заголовке TCP для достижения состояния SYN-RECEIVED.
- Последний шаг рукопожатия заключается в подтверждении исходным TCP-узлом номера последовательности TCP-узла на противоположном конце путем установки номера подтверждения, равным полученному номеру последовательности плюс один, вместе с флагом ACK в заголовке TCP, что позволяет достичь состояния ESTABLISHED.

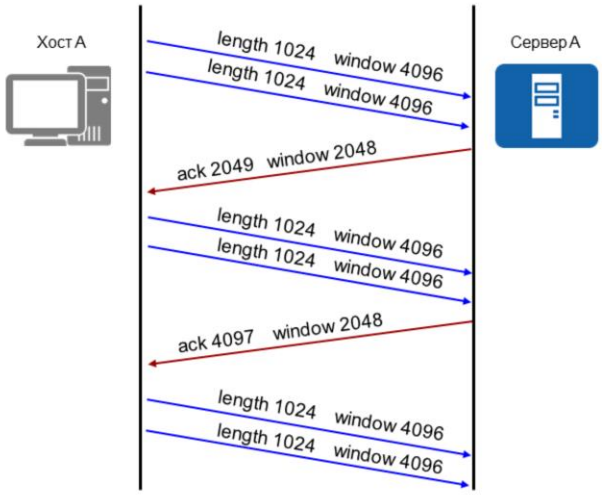
Процесс передачи TCP



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Поскольку передача TCP осуществляется как передача потока данных, каждый октет может быть включен в последовательность, а значит, может быть подтвержден. Для этого используется номер подтверждения, который посылается отправителю как подтверждение получения данных, чем достигается надежность передачи. Однако процесс подтверждения носит накопительный характер, что означает, что последовательность октетов может быть подтверждена одним сообщением-подтверждением, в котором источнику будет сообщен порядковый номер, который следует сразу же за успешно полученным порядковым номером.
- В примере несколько байтов (октетов) передаются вместе до получения подтверждения TCP. Если какой-либо октет потеряется и не достигнет пункта назначения, последовательность передаваемых октетов будет подтверждена только в точке, в которой произошла потеря. Такое подтверждение будет содержать неполученный октет, указывая на инициацию его повторной передачи из той точки потока данных, в которой он был потерян.
- Способность накоплять несколько октетов вместе до подтверждения повышает эффективность работы TCP, однако должен быть соблюден определенный баланс, то есть количество октетов, отправленных до получения подтверждения, не должно быть слишком большим, ибо если октет не будет получен, необходимо будет повторно передать весь поток октетов из точки потери.

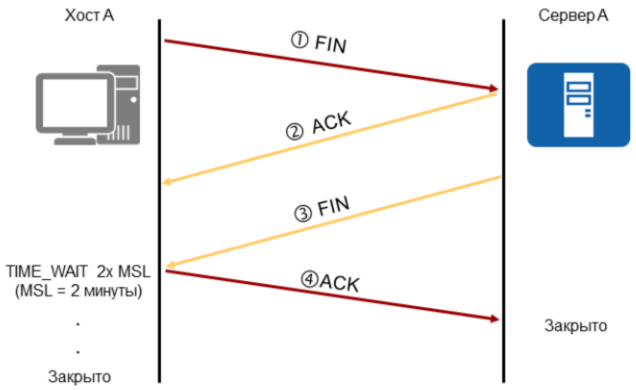
Управление потоком TCP



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Поле размера окна TCP (window) отвечает за управление потоком, регулируя количество данных, посылаемых отправителем. Это достигается путем возвращения значения "window" с каждым сегментом TCP, для которого установлено поле ACK, с указанием диапазона допустимых порядковых номеров, не входящих в последний успешно принятый сегмент. Окно указывает на разрешенное количество октетов, которые отправитель может передать перед получением дальнейшего разрешения.
- В приведенном примере сегмент TCP, переданный от хоста A к серверу A, содержит текущий размер окна для хоста A. Определение размера окна для сервера A входит в процесс рукопожатия и в зависимости от передачи может принимать значение 2048. После получения данных, эквивалентных размеру окна, будет возвращено подтверждение относительно количества полученных байтов плюс один. После этого хост A продолжит передачу следующего набора данных.
- Размер окна TCP, равный 0, означает, что сегменты обрабатываться не будут, за исключением входящих сегментов с установленными флагами ACK, RST и URG. Если существует окно с размером 0, отправитель должен периодически проверять размер окна получающего TCP-узла с целью своевременного оповещения об изменении размера окна. Период ретрансляции, как правило, составляет две минуты. Когда отправитель отправит периодические сегменты, TCP-получатель должен отправить в ответ подтверждение с порядковым номером текущего окна с размером 0.

Завершение соединения TCP



- Хост A отвечает за получение подтверждения ACK сервером A перед закрытием соединения.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- В процессе завершения TCP-соединения определяется ряд состояний, через которые TCP должен пройти. Эти состояния включают в себя FIN-WAIT-1, которое представляет собой ожидание запроса на завершение соединения (FIN) от удаленного TCP, или подтверждение запроса на прекращение соединения, который был ранее отправлен. FIN-WAIT-2 представляет собой ожидание запроса на завершение соединения от удаленного TCP, после которого обычно происходит переход в состояние TIME-WAIT. Состояние CLOSE-WAIT указывает на ожидание локально определенного запроса на завершение соединения, как правило, когда приложение сервера находится в процессе закрытия.
- Состояние LAST-ACK представляет собой ожидание подтверждения запроса на завершение соединения, ранее отправленного на удаленный TCP (который включает в себя подтверждение его запроса на завершение соединения). Наконец, возникает состояние TIME-WAIT, которое ожидает достаточного времени для подтверждения того, что удаленный TCP получил подтверждение своего запроса на завершение соединения. Этот период управляется таймером MSL (Max Segment Lifetime), который определяет период ожидания в 2 минуты. После периода ожидания, равного двухкратному MSL, TCP-соединение считается закрытым/прерванным.

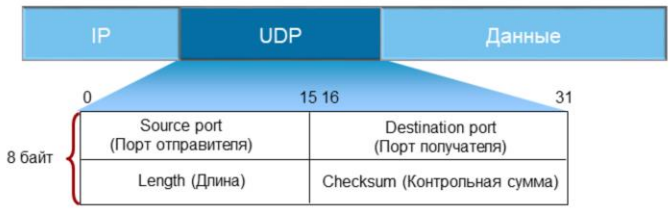
Протокол пользовательских датаграмм

- Данные UDP отправляются без установления соединения.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- User Datagram Protocol или UDP представляет собой альтернативу TCP и применяется в тех случаях, когда TCP считается неэффективным транспортным механизмом, главным образом при передаче трафика, чувствительного к высокой задержке. Если TCP считается сегментом, то UDP – это датаграмма блока данных протокола (PDU), под которой понимается самостоятельный, независимый объект, передающий информацию, которой достаточно для осуществления маршрутизации из источника в конечную систему назначения без необходимости установления предварительного соединения между этим источником и конечными системами назначения и транспортной сетью, как это определено в RFC 1594. По сути это означает, что UDP-трафик не требует установления соединения перед отправкой данных.
- Простая структура пакета UDP и простой процесс работы делает этот протокол идеальным для приложений, которым требуется отправлять сообщения в другие программы с использованием минимального ориентированного на обработку сообщений механизма, например в случае подтверждения и установления размера окон, как в случае с сегментами TCP. Вместе с тем UDP не гарантирует доставку данных, а также защиту от дублирования датаграмм.

Формат датаграмм UDP

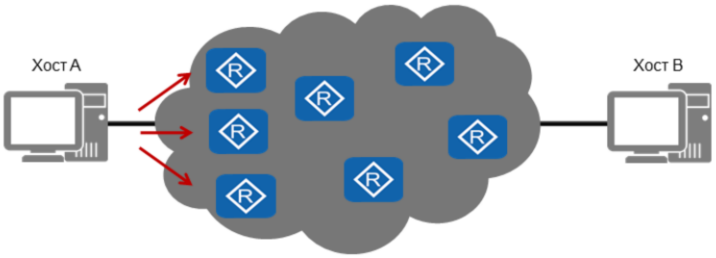


- UDP задействует минимальный объем служебной информации для каждой датаграммы.
- Доставка датаграмм не гарантируется протоколом UDP.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Структура заголовка UDP крайне проста. Содержит поле, определяющее порт назначения, которому предназначен UDP-трафик, а также поле длины и значение контрольной суммы, обеспечивающие целостность заголовка UDP. Кроме того, минимальный объем служебной информации гарантирует передачу большего количества полезных данных на пакет, оставляя ресурсы для трафика в реальном времени, например голосовых и видеоуслуг, где служебная информация TCP занимает всего 20 байтов, и используются механизмы, влияющие на задержку, как в случае с подтверждением, однако отсутствие таких полей означает, что доставка датаграмм не гарантируется.

Процесс передачи UDP

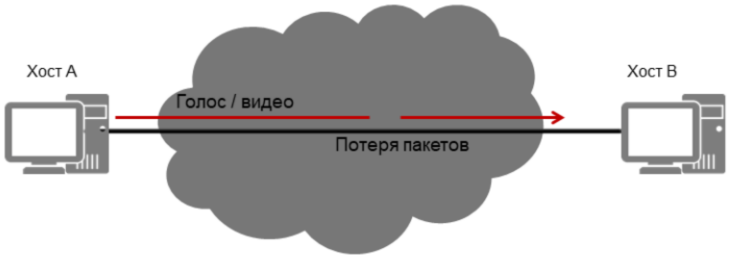


- UDP допускает дублирование датаграмм или неупорядоченную доставку датаграмм.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Поскольку UDP-датаграмма не передается как поток данных, передача подвержена дублированию датаграмм. Кроме того, отсутствие порядковых номеров в UDP означает, что передаваемые по различным маршрутам данные, скорее всего, будут получены в пункте назначения в неверном порядке следования.
- В тех случаях, когда по UDP передается поток данных, например голосовые и видеоуслуги, возможно применение дополнительных механизмов, расширяющих возможности UDP, например транспортного протокола реального времени (RTP), который устраняет недостаток UDP, обеспечивая последовательность получения данных (аудио и видео) с помощью временных меток, частично реализуя механизм с установлением соединения по протоколу без установления соединения.

Процесс передачи UDP



- Из-за отсутствия подтверждений потерянные пакеты не передаются повторно, однако это эффективно при передаче данных, чувствительных к задержке.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Общий принцип передачи UDP эффективен для трафика, чувствительного к задержке, например голоса и видео. Следует понимать, что при работе транспортного протокола с установлением соединения потерянные данные требуют повторной передачи после определенного периода задержки, в течение которого отправитель ожидает подтверждение. Если подтверждение не будет получено, данные передаются повторно.
- Для потоков данных, чувствительных к задержкам, это приведет к недоступности (голоса и видео) из-за задержки и дублирования в результате повторной передачи с точки, в которой генерируются подтверждения. В таких случаях минимальная потеря потока данных предпочтительнее по сравнению с повторной передачей, и поэтому в качестве транспортного механизма в поддержку трафика, чувствительного к задержке, выбирается UDP.

Заключение

- Какова цель поля подтверждения в заголовке TCP?
- Какие управляющие биты TCP используются в процессе трехстороннего рукопожатия TCP?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Поле подтверждения в заголовке TCP содержит подтверждение получения сегмента процессом TCP в пункте назначения. Порядковый номер в заголовке TCP получаемого IP-сегмента увеличивается на 1. Это значение становится номером подтверждения в возвращаемом заголовке TCP и используется для подтверждения получения всех данных, прежде чем они будут переданы с флагом ACK, установленным в значение 1, первоначальному отправителю.
- Трехстороннее рукопожатие включает в себя управляющие биты SYN и ACK, которые служат для установления и подтверждения соединения между двумя конечными системами, между которыми происходит передача сегментов.

Заключение

- Какова цель поля подтверждения в заголовке TCP?
- Какие управляющие биты TCP используются в процессе трехстороннего рукопожатия TCP?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Поле подтверждения в заголовке TCP содержит подтверждение получения сегмента процессом TCP в пункте назначения. Порядковый номер в заголовке TCP получаемого IP-сегмента увеличивается на 1. Это значение становится номером подтверждения в возвращаемом заголовке TCP и используется для подтверждения получения всех данных, прежде чем они будут переданы с флагом ACK, установленным в значение 1, первоначальному отправителю.
- Трехстороннее рукопожатие включает в себя управляющие биты SYN и ACK, которые служат для установления и подтверждения соединения между двумя конечными системами, между которыми происходит передача сегментов.

Сценарий передачи данных

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

Стек протоколов TCP/IP функционирует как набор правил сквозной передачи данных наряду с протоколами нижнего уровня, определенных стандартами IEEE 802. Знание жизненного цикла передачи данных позволяет глубже понять характер работы IP-сети, чтобы эффективно анализировать ее рабочее состояние и устранять неисправности. Таким образом, процесс инкапсуляции и декапсуляции представляет собой фундаментальную часть всей информации о работе стека TCP/IP.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

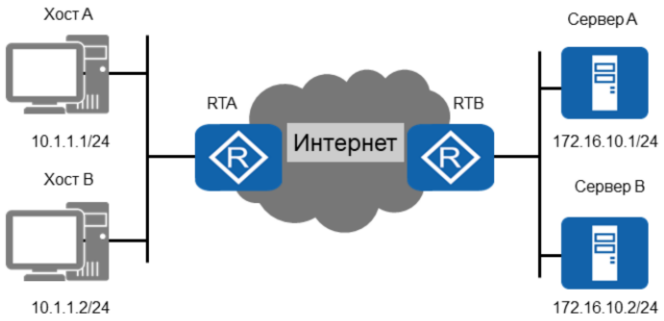
Цели

По завершении этого раздела обучающиеся научатся:

- Объяснять этапы процесса инкапсуляции и декапсуляции данных.
- Диагностировать и устранять основные проблемы передачи данных.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

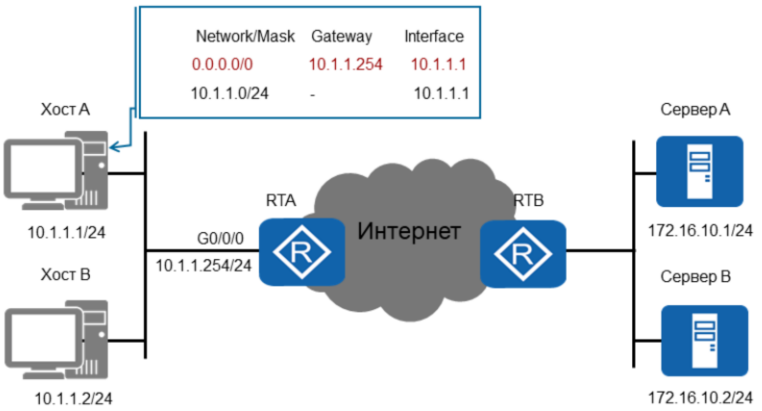


- Передача данных может быть локальной или удаленной, однако процесс передачи будет общим.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Различают локальную и удаленную передачу данных. В обоих случаях в процессе, который позволяет достичь сквозной передачи, применяется стек протоколов. Конечные системы могут быть частью одной сети или расположены в различных сетях, однако общий принцип передачи данных между хостами опирается на работу стека протоколов. Необходимо понимать принцип совместной работы этих протоколов, а также взаимосвязь между протоколами TCP/IP верхнего уровня и стандартами протокола Ethernet нижнего уровня.

Обнаружение пути

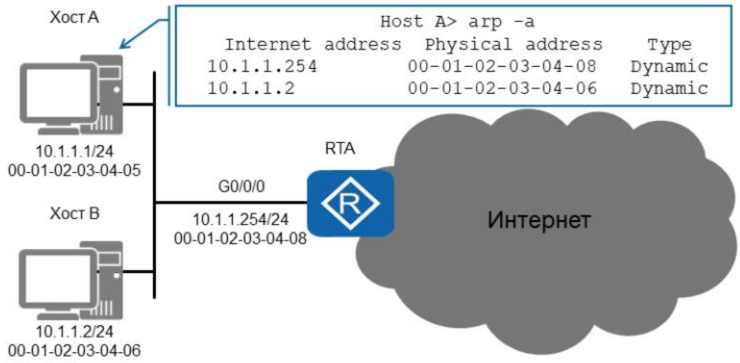


- Хост A должен иметь информацию о пути к месту назначения.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Конечная система, которая намерена направить данные в определенное место назначения, должна сначала установить, возможно ли достичь запланированного места назначения. Для этого конечная система должна пройти процесс обнаружения пути. Конечная система должна поддерживать работу на всех уровнях, поскольку ее основная функция заключается в выполнении роли хоста для приложений. Поэтому такая система также должна поддерживать операции нижнего уровня, такие как маршрутизация и пересылка на канальном уровне (коммутация), что позволит осуществлять передачу данных верхнего/прикладного уровней. Поэтому конечная система содержит таблицу, отражающую достижимость сетевого уровня для той сети, которой предназначены данные верхнего уровня.
- Конечные системы, как правило, имеют информацию о сети, в которой они находятся, но маршрута пересылки может и не быть, например в случае, если удаленная сеть не обнаружена. В данном примере хост A имеет путь к сети назначения, проходящий через «любую сеть», адрес которой входит состав IP-адреса. Таблица передачи определяет, что трафик должен быть переадресован на шлюз, выполняющий роль следующего транзитного узла, через интерфейс, ассоциированный с логическим адресом 10.1.1.1.

ARP

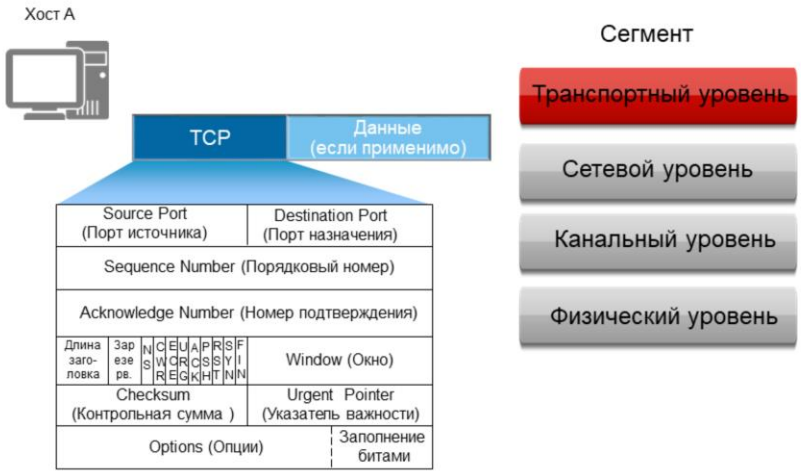


- Таблица кэша ARP используется для обнаружения следующего транзитного узла в канале данных.
- Неизвестный транзитный узел генерирует запрос ARP.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- После обнаружения рационального маршрута к запланированной сети назначения должен быть обнаружен физический транзитный узел, на который будет передан кадр. За это отвечает стек протоколов TCP/IP, и данная операция выполняется до начала инкапсуляции пакетов. На первом шаге определяется существование физического пути к данному транзитному узлу, и этот шаг является частью процесса обнаружения пути.
- Для этого необходимо по записям таблицы кэша ARP определить наличие связи между запланированным транзитным узлом и физическим путем. В приведенном примере в таблице кэша ARP запись адреса шлюза транзитного узла присутствует. Если запись не будет найдена, необходимо инициировать протокол определения адреса (ARP), который должен обнаружить и определить физический путь.

Инкапсуляция TCP

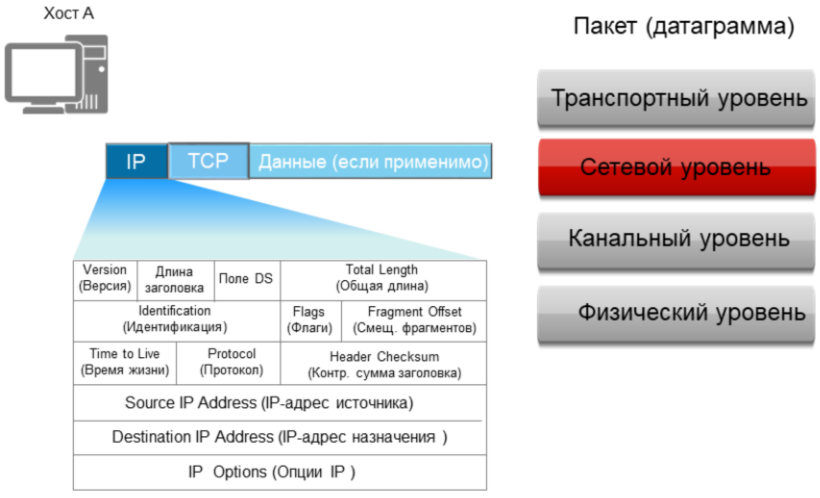


- Инкапсуляция выполняется после подтверждения пути.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- При завершении обнаружения как логического, так и физического путей, данные инкапсулируются для последующей передачи по сетям IP/Ethernet. Инкапсуляция на транспортном уровне, во время которой определяются порты источника и назначения, через которые должны передаваться данные верхнего уровня, выполняется после процессов верхнего уровня с точки зрения шифрования и сжатия.
- В случае с TCP, заполняются поля, отведенные под значения порядкового номера и номера подтверждения, управляющие биты (флаги) устанавливаются по необходимости с флагом ACK. Поле окна заполняется поддерживаемым в данный момент размером окна, при этом, хост сообщает максимальный размер данных, который может поддерживаться, до подтверждения данных.
- Значения полей TCP включаются в состав поля контрольной суммы, значение которого вычисляется с помощью процесса расчета добавочных значений для обеспечения целостности TCP-сегмента после получения и обработки заголовка TCP в конечной точке назначения. В отношении основных управляющих операций TCP, данные верхнего уровня не всегда можно передать в сегменте, например при синхронизации и подтверждении полученных данных.

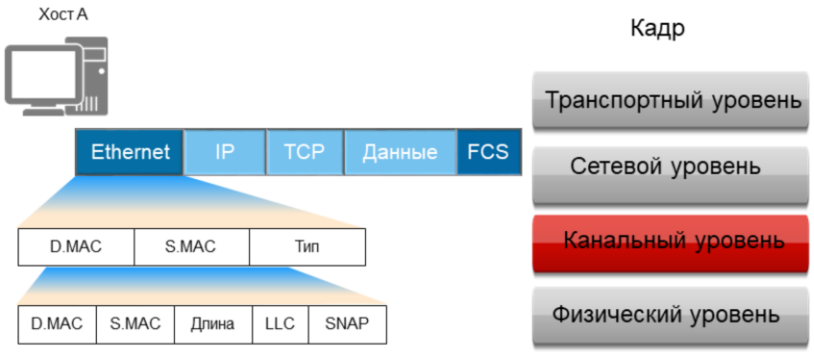
Инкапсуляция IP



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- После инкапсуляции транспортного уровня требуются команды, детализирующие, как должна осуществляться передача по одной или нескольким сетям с указанием источника IP, а также конечного пункта назначения, которому предназначен данный пакет. IP-пакеты ограничены возможностями Ethernet, их размер не превышает 1500 байт, включая заголовки сетевого и транспортного уровней, а также любые данные верхнего уровня. Исходный размер пакета будет определяться каналом Ethernet как максимальный блок передачи (MTU), которому будут соответствовать пакеты, поэтому фрагментация на узле-источнике не будет осуществляться.
- Фрагментация выполняется только в случае изменения MTU в процессе следования по пути передачи. Поле «время жизни» будет заполнено установленным значением в зависимости от системы. В маршрутизаторах серии ARG3 установлено начальное значение 255. Поле «протокол» заполняется значением типа протокола, инкапсулированного до IP. В этом случае протоколом является TCP, для которого заголовок IP внесет в поле «протокол» значение 0x06, означающее команду для следующей обработки заголовка. Поля «IP-адрес источника» и «IP-адрес пункта назначения» будут содержать адреса отправителя и получателя.

Кадрирование Ethernet

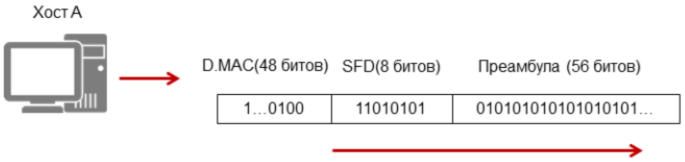


- Тип кадра зависит от инкапсулированных протоколов.
- IP — это протокол верхнего уровня, поэтому используется кадр Ethernet II.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Инкапсуляция канального уровня, основанная на стандартах IEEE 802.3 Ethernet, предназначена для физической передачи данных верхнего уровня по сетям Ethernet. Инкапсуляция на нижних уровнях выполняется с предварительным определением используемого типа кадра.
- Если значение типа протокола верхнего уровня превышает 1536 (0x0600), как это имеет место в случае с IP (0x0800), используется тип кадра Ethernet II. Поле «тип» заголовка кадра Ethernet II заполняется значением 0x0800, которое указывает на следующий протокол, который будет обрабатываться после обработки кадра - IP. MAC-адрес назначения определяет следующий физический транзитный узел, который в данном случае представляет собой сетевой шлюз.

Передача кадров

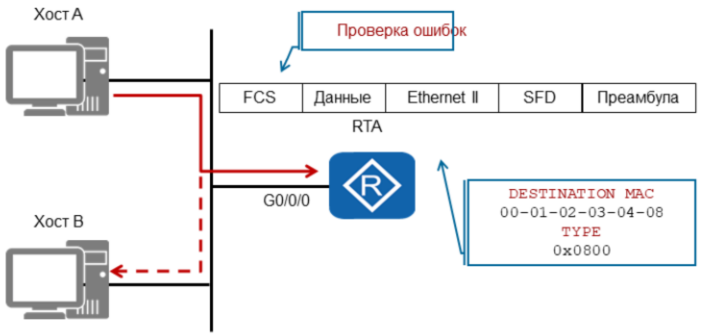


- Для обнаружения существующего трафика на канальном уровне используется метод опроса передающего канала.
- Преамбула и SFD используются для синхронизации с передаваемым кадром.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- В состав процедуры канального уровня входит операция проверки среды передачи, которая должна быть свободна от сигналов, передаваемых в общем домене коллизий. Хост сначала прослушивает любой трафик в сети (CSMA/CD) и, если линия свободна, готовится к передаче данных. Принимающий физический интерфейс должен быть информирован о входящем кадре. Это позволит избежать потери исходных битовых значений, в результате которых начальные кадры могут быть неполными. Таким образом, кадрам предшествует 64-разрядное значение, сообщающее пункту назначения канального уровня о предстоящем поступлении кадра.
- Начальные 56 битов представляют собой шаблон, в котором чередуются 1, 0, называемый преамбулой, и за ним сразу же следует октет, служащий началом кадра (Start of Frame Delimiter; SFD). Последние два бита SFD изменяются от принятого шаблона (их комбинация 1,1). Это означает, что следующие биты являются первыми битами MAC-адреса назначения и, следовательно, началом кадра .

Обработка кадров

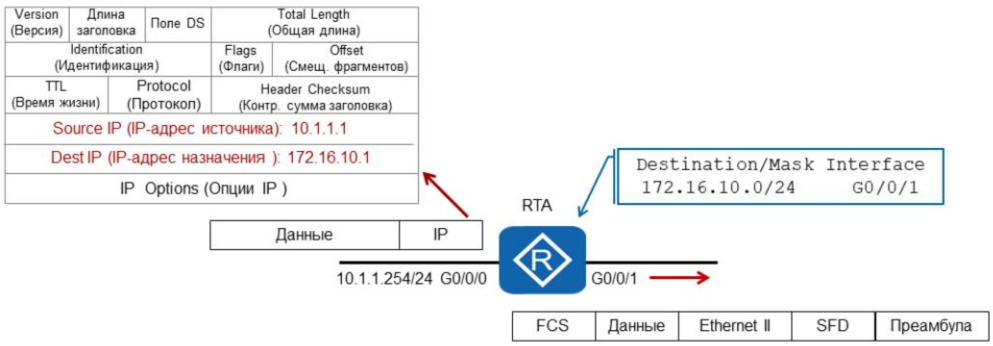


- Кадр будет получен всеми узлами, находящимися в одном домене коллизий.
  - Обработку кадра будет выполнять только шлюз (RTA).

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Кадр, полученный пунктом назначения канального уровня, должен пройти ряд проверок на предмет целостности и действительности. Если кадр передается по общей сети Ethernet, другие конечные станции также могут получить экземпляр передаваемого кадра, однако, поскольку MAC-адрес назначения отличается от MAC-адреса конечной станции, кадр будет отброшен.
- Кадры, полученные запланированным пунктом назначения, будут проходить проверку ошибок, во время которой будут вычислены добавочные значения на основе текущих полей кадра и затем сравнены со значением в поле Frame Check Sequence (FCS). Если значения не совпадут, кадр будет отброшен. Промежуточная и конечная системы, получившие действительный кадр, должны определить, предназначен ли данный кадр для их физического интерфейса, сравнив MAC-адрес назначения с MAC-адресом интерфейса (или устройства в некоторых случаях).
- Если адреса совпадут, кадр будет обработан, и для определения следующего заголовка, подлежащего обработке, будет использовано поле «тип». После определения следующего заголовка данные заголовок и хвостовая часть кадра отбрасываются.

Обработка пакетов

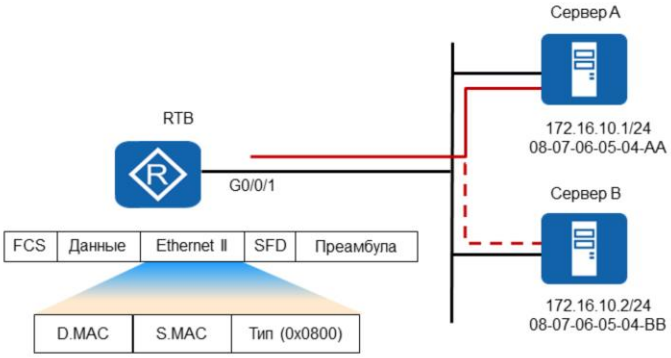


- IP-адрес назначения сравнивается с адресом шлюза.
- После процесса обнаружения создается новый заголовок кадра.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Пакет принимается сетевым уровнем, и в частности IP, на котором обрабатывается заголовок IP. Значение контрольной суммы присутствует на каждом уровне стека протоколов, обеспечивая целостность на всех уровнях для всех протоколов. IP-адрес назначения используется для определения, достиг ли пакет конечного получателя. Однако шлюз определяет, что это не так, так как IP-адрес назначения и IP-адрес шлюза не совпадают.
- Поэтому шлюз должен определить план действий с точки зрения перенаправления пакета на альтернативный интерфейс и переслать пакет в сеть, которой он предназначен. Во-первых, шлюз должен убедиться, что значение TTL не достигло 0 и что размер пакета не превышает максимального значения блока передачи для шлюза. В случае, если пакет больше, чем значение MTU шлюза, запускается процесс фрагментации.
- Поскольку адрес пункта назначения пакета включен в таблицу переадресации шлюза, пакет будет инкапсулирован в новый заголовок кадра, состоящий из новых MAC-адресов источника и назначения для сегмента канального уровня, через который будет передан результирующий кадр, прежде чем он снова будет передан следующему физическому узлу. Если следующий физический узел не известен, снова будет инициирован ARP для определения MAC-адреса.

Декапсуляция кадра

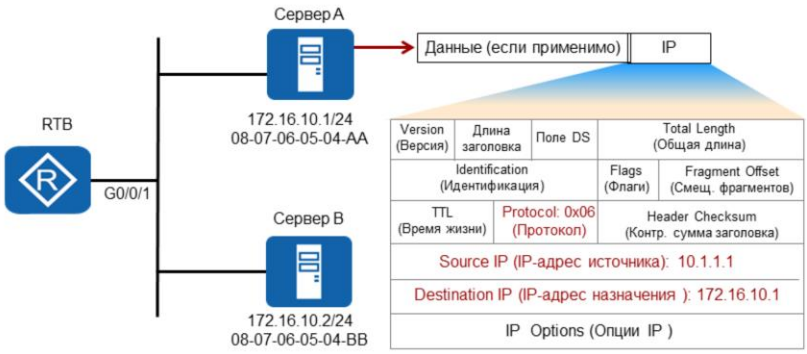


- Кадр передается с MAC-адресом пункта назначения сервера A.
- Сервер A сравнивает MAC-адрес интерфейса с MAC-адресом пункта назначения кадра.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Кадры, полученные в конечном пункте назначения, первоначально определят, прибыл ли кадр в предполагаемое место. На примере показаны два сервера в общей сети Ethernet, оба получившие копию кадра.
- Кадр в конечном счете отбрасывается сервером B, так как MAC-адрес пункта назначения и MAC-адрес интерфейса сервера B не совпадают. Однако сервер A успешно получает кадр и узнает, что значения полей MAC-адресов одинаковы, целостность кадра в соответствии с полем FCS сохранена. В поле «тип» кадра будет указано значение 0x0800 следующего заголовка, после чего заголовок и хвостовая часть кадра отбрасываются и пакет принимается IP.

Декапсуляция пакетов

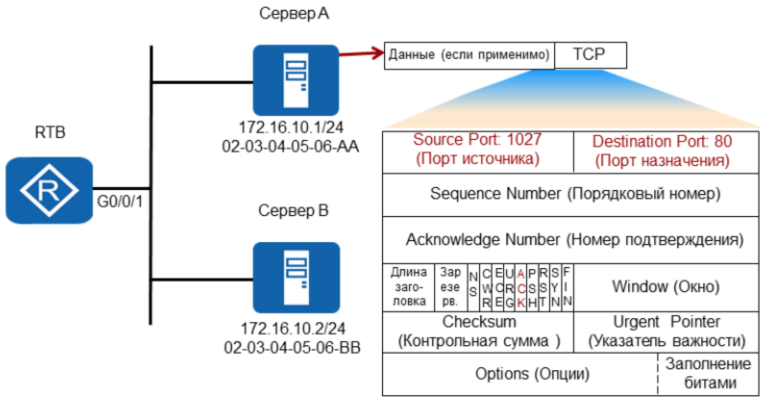


- Сервер A сравнивает собственный IP-адрес с адресом назначения, содержащимся в заголовке IP.
- Заголовок IP обрабатывается и отбрасывается, данные направляются в TCP.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- При достижении конечного пункта назначения заголовок IP-пакета будет использован в ряде процессов. Первый процесс заключается в проверке целостности заголовка пакета с помощью значения поля контрольной суммы, применения сравнения с добавочным значением на основе суммы полей заголовка IP. Если все правильно, заголовок IP-пакета будет использован для определения того, соответствует ли IP-адрес пункта назначения IP-адресу текущей конечной станции, что в данном случае верно.
- Если во время передачи между источником и пунктом назначения имела место фрагментация, пакет на данном этапе должен пройти повторную сборку. Поле «идентификация» будет содержать фрагменты, принадлежащие одному источнику данных. По смещению фрагментов можно будет определить порядок. Поле «флаги» будет содержать информацию, когда должна начаться повторная сборка, поскольку все фрагменты должны быть получены, а фрагмент с флагом 0 будет считаться последним полученным фрагментом.
- Затем запускается таймер, в течение которого необходимо выполнить повторную сборку, и если повторная сборка завершится в течение этого периода времени, все фрагменты будут отброшены. Поле «протокол» будет использовано для идентификации следующего заголовка, подлежащего обработке, и заголовок пакета будет отброшен. Следует отметить, что следующий заголовок не всегда может быть заголовком транспортного уровня, например в случае с ICMP, который рассматривается как протокол сетевого уровня со значением поля «протокол», равным 0x01.

Декапсуляция сегмента



- Заголовок TCP создает соединение с портом назначения 80.
- Параметры в заголовке TCP используются для управления соединением.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

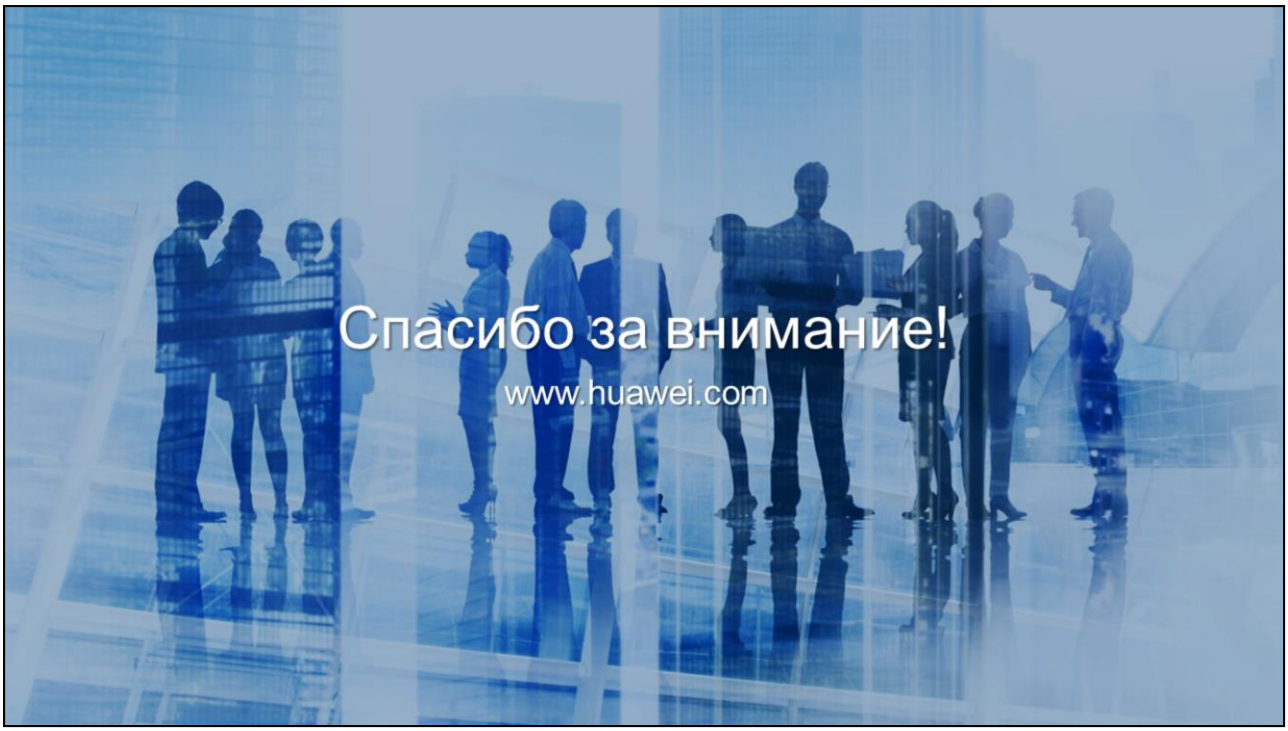
- В случае отбрасывания заголовка пакета результирующий сегмент или датаграмма передается на транспортный уровень для обработки по принципу «приложение-приложение». Информация заголовка поступает в данном случае по TCP (0x06).
- В приведенном примере соединение TCP уже установлено, и сегмент представляет собой подтверждение передачи HTTP-трафика с HTTP-сервера на принимающий хост. Хост представлен портом 1027, который служит для отличия HTTP-соединений, которые могут существовать между одним и тем же хостом и сервером назначения. При получении этого подтверждения, HTTP-сервер продолжит пересылку в пределах размера окна хоста.

Заключение

- Какая информация требуется до инкапсуляции данных?
- Что происходит, когда кадр пересылается в пункт назначения, которому он не предназначен?
- Как данные в кадре в конечном итоге доходят до приложения, для которого они предназначены?
- Как возвращаемые данные достигают правильного сеанса в случае, если активны несколько сеансов одного и того же приложения (например, несколько веб-браузеров)?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- До инкапсуляции и передачи данных источник должен получить информацию об IP-адресе пункта назначения или эквивалентном адресе передачи, например адресе по умолчанию, на который можно переадресовать данные. Кроме того, необходимо, чтобы адрес переадресации был ассоциирован с физическим транзитным узлом, на который данные могут быть переданы в локальной сети.
- Любой кадр, получаемый шлюзом или конечной системой (хостом), которой он не предназначен, отбрасывается после проверки MAC-адреса назначения в заголовке кадра.
- При доставке данных учитывается номер порта назначения в заголовках TCP и UDP, который определяет приложение, которому предназначены данные. После анализа этого значения протоколами TCP или UDP данные пересылаются.
- Порт источника в заголовке TCP, предназначенный для передачи HTTP-трафика, отличается в разных активных сеансах приложений. На основе этого номера HTTP-трафик, возвращаемый с HTTP-сервера, идентифицирует каждый отдельный сеанс браузера. Например, портами источника двух отдельных запросов на HTTP-трафик, поступающих из источника с IP-адресом 10.1.1.1, могут быть порты с номерами 1028 и 1035, однако порт назначения в обоих случаях остается портом 80, HTTP-сервером.


Спасибо за внимание!
www.huawei.com

Введение в VRP

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

Увеличение плотности устройств в связи с ростом числа конечных станций, применяемых в локальной вычислительной сети в виде хост-устройств, сетевых принтеров и других аналогичных продуктов, приводит к ограничению с точки зрения портов интерфейсов, а также к проблемам коллизий, возникающих в рамках любой общей сети. Для поддержки такой плотности развиваются технологии коммутации. В продуктах Huawei в качестве инструмента конфигурирования и эксплуатации таких управляемых устройств используется технология VRP, описываемая в данном курсе.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

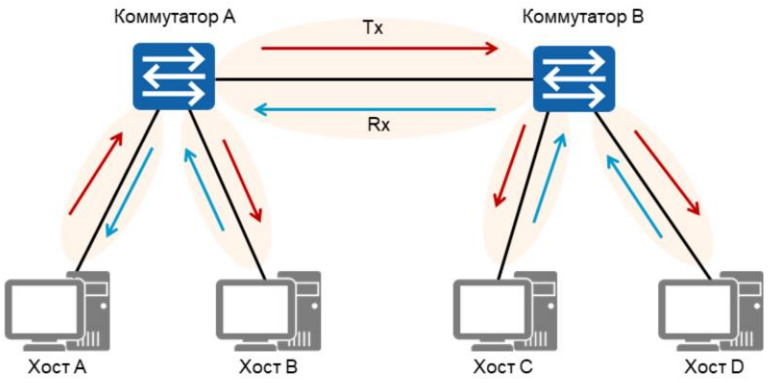
Цели

По завершении этого раздела обучающиеся смогут:

- Объяснить роль, которую коммутаторы играют в сетях Ethernet.
- Описать разницу между коллизионным и широковещательным доменами.
- Объяснить общий принцип работы VRP в продуктах Huawei.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Применение устройств коммутации

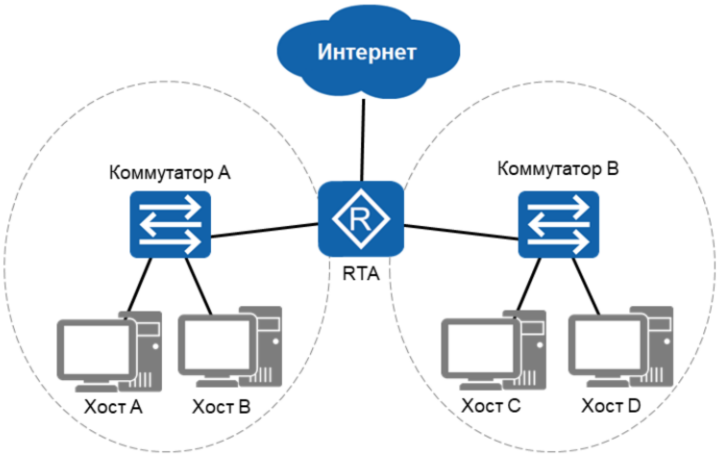


- Коммутаторы генерируют несколько доменов коллизий.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Сеть Ethernet до сих пор рассматривалась как набор устройств, связывающихся по общему каналу передачи, например 10Base2, и через эти устройства хосты взаимодействовали с соседними хостами или конечными системами. Сеть Ethernet признана коллизионной сетью, то есть хосты вынуждены конкурировать за доступ к каналу передачи, возможности которого, по мере подключения к нему все большего числа устройств, становятся ограниченными. Это приводит к дополнительным ограничениям масштабируемости и росту потенциальной возможности коллизий.
- В результате появилась необходимость применения в сетях Ethernet с разделяемой средой методики обнаружения коллизий CSMA/CD. С началом применения таких коммутируемых сетей, как 100BaseT, процессы передачи и приема данных стали изолированными в пределах каналов (пар проводов), что устранило вероятность коллизий. Но такой вариант Ethernet с неразделяемой средой обеспечивает только двухточечное соединение. Применение разделяемой сети Ethernet снова становится возможным даже при наличии вероятности возникновения коллизий – это достигается использованием такой сети вместе с другими устройствами, например, концентраторами.
- Внедряемые коммутаторы, ставшие результатом эволюции моста, разбивают общий домен коллизий на несколько доменов. Домены коллизий работают как набор каналов «точка-точка», в отношении которых угрозы коллизий уже больше не существует, а трафик канального уровня изолируется. Это позволяет повысить скорость передачи, оптимизируя поток трафика в сети Ethernet.

Применение устройств маршрутизации



- Шлюзовые устройства, такие как маршрутизаторы, генерируют широковещательные домены.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Широковещательный домен может состоять из одного или нескольких доменов коллизий, и любая широковещательная передача осуществляется в пределах границы широковещательного домена. Пределы границ широковещательного домена обычно определяются шлюзом, выступающим в роли средства передачи, через которое осуществляется связь с другими сетями, и ограничивают передачу любого широковещательного трафика дальше интерфейса, принимающего такой трафик.
- Термины «маршрутизатор» и «шлюз» часто взаимозаменяемы. IP-сеть формирует широковещательный домен в масштабе сегмента канального уровня. Маршрутизаторы, как правило, отвечают за маршрутизацию интернет-датаграмм (IP-пакетов) в указанный пункт назначения по адресу передачи сети назначения, найденному во внутренне управляемой таблице переадресации.

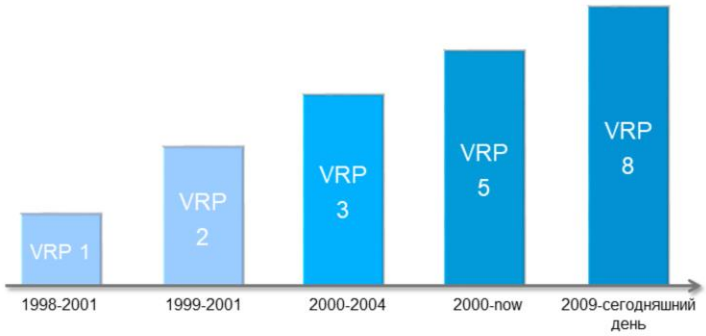
Введение в VRP

- VRP — это платформа, на которой работают многие продукты Huawei.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.
HUAWEI

- Платформа маршрутизации Versatile Routing Platform (VRP) лежит в основе многих продуктов Huawei, включая маршрутизаторы и коммутаторы. Ее конструкция много раз модернизировалась, чтобы добиться непрерывной передачи данных и их управления. Улучшен модульный принцип архитектуры, за счет чего повышена общая производительность. Конфигурация, управление и мониторинг устройств с использованием VRP основаны на стандартной иерархической структуре режима интерфейса командной строки. Знания этой структуры необходимо тем, кто занимается эксплуатацией устройств Huawei, управляемых с помощью программного обеспечения VRP.

Эволюция VRP

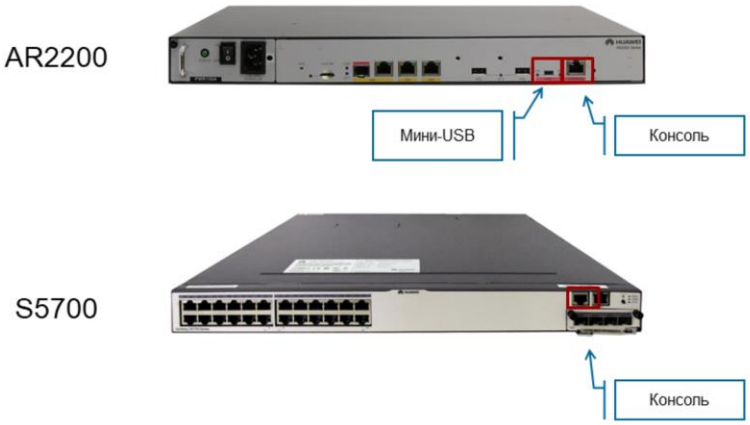


- В настоящее время в продуктах Huawei используется VRP версий 5 и 8.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Знания версий сетевой операционной системы VRP (NOS) поможет в отслеживании обновлений и определенных функций, которые могут потребоваться в корпоративной сети. Большинство устройств Huawei в настоящее время работают на VRP версии 5.x, где x зависит от продукта и версии платформы. VRP версии 8 - это последняя версия платформы, отличающаяся очень точной архитектурой, которая поддерживает технологии следующего поколения и построена в связи с необходимостью повышения эффективности. Однако эта версия используется не во всех продуктах Huawei.

Установление связи



 Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- В серию AR корпоративных маршрутизаторов входят AR150, AR200, AR1200, AR2200 и AR3200. Устройства представляют собой продукты Huawei следующего поколения и обеспечивают функции маршрутизации, коммутации, беспроводной связи, голосовой связи и информационной безопасности. Данные устройства, располагаемые между корпоративной и публичной сетями, функционируют в качестве входного и выходного шлюзов для передачи данных между этими сетями. Развертывание различных сетевых сервисов с помощью маршрутизаторов серии AR снижает затраты на эксплуатацию и техобслуживание (O&M), а также затраты, связанные с созданием корпоративной сети. Предусмотрены различные модели маршрутизаторов, которые в зависимости от числа пользователей предприятия можно использовать в качестве шлюзов.
- Ethernet-коммутатор серии Sx7, выполняющий функции передачи данных, разработан компанией Huawei для удовлетворения требований к надежному доступу и высококачественной передаче множества услуг в корпоративной сети. Эта серия коммутаторов позиционируется для работы на уровне доступа или уровне агрегации в корпоративной сети и обеспечивает большую емкость коммутации, высокую плотность портов и экономичность передачи пакетов.
- Управление маршрутизаторами серии ARG3 и коммутаторами серии Sx7 осуществляется путем установления соединения с консольным интерфейсом, а в случае с моделью AR2200 соединение можно установить также через интерфейс мини-USB.

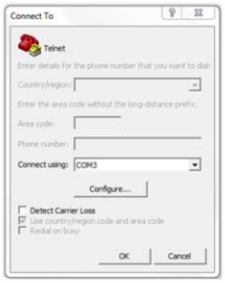
Доступ к устройству через консоль

- Между последовательным портом (COM) и консольным интерфейсом маршрутизатора/коммутатора установлено физическое соединение.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Консольный кабель, используемый для отладки или обслуживания локально установленного устройства, например, маршрутизатора или коммутатора, подключается к консольному порту таких устройств. Консольный интерфейс коммутатора серии S5700 и маршрутизатора AR2200 — RJ-45, а интерфейс хоста представляет собой разъем последовательного порта RS-232. Часто таких разъемов нет на современных устройствах, которые могут быть использованы для установления соединения, например, ноутбуках, и поэтому требуется преобразование между RS-232 и USB. Однако для большинства настольных устройств можно организовать консольное соединение RS-232 с портом COM на устройстве хоста.

Процедуры настройки доступа консоли




```
Please configure the login password (maximum length 16)
                Enter password:huawei
               Confirm password:huawei
                      <Huawei>
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Консоль создается через одну из нескольких доступных программ эмуляции терминала. Пользователи Windows часто применяют приложение HyperTerminal, как показано в примере для интерфейса с операционной системой VRP. В соответствии со спецификациями порта COM, который должен использоваться для установления соединения, необходимо выполнить настройки порта.
- В примере показаны настройки порта, которые необходимо применить. В случае любого изменения настроек будут автоматически заменены параметры в окне, открываемом нажатием кнопки Restore Defaults. После нажатия кнопки OK будет установлен сеанс с VRP устройства. Если устройство работает с заводскими настройками по умолчанию, пользователю будет предложено ввести пароль, который будет назначен в качестве пароля входа по умолчанию при дальнейшем подключении.

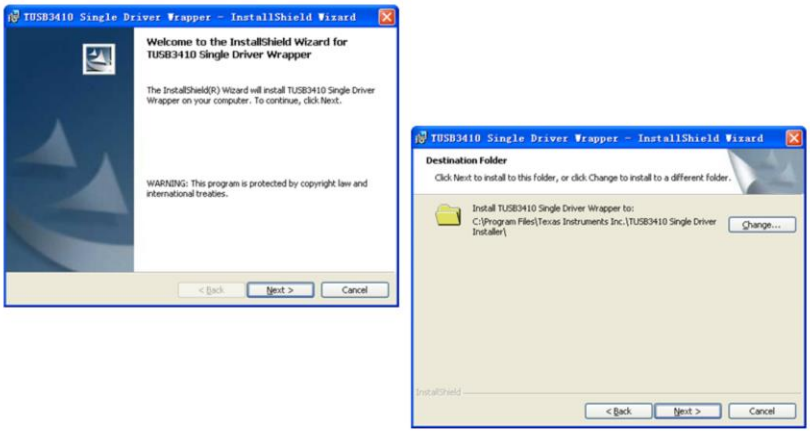
Доступ через мини-USB

- Соединение осуществляется между портом USB хоста и мини-интерфейсом USB маршрутизатора.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Маршрутизатор Huawei AR2200 дополнительно поддерживает средства подключения терминала через USB-соединение. Интерфейс мини-USB, тип B, расположен на передней панели маршрутизатора серии AR2200. Через него хосты могут установить соединение на базе USB (альтернатива последовательной связи RS-232).

Установка драйвера USB

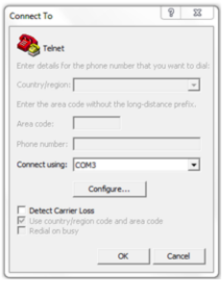


- Для подключения USB может потребоваться установка драйверов.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Небольшие отличия в процессе установки – для мини-USB необходимо сначала установить соответствующие драйверы. Их можно загрузить со страницы: http://support.huawei.com/enterprise. По пути Support > Software > Enterprise Networking > Router > Access Router > AR > AR2200 выберите соответствующую опцию версии VRP и путь к патчу, загрузите файл AR&SRG _ MiniUSB _ driver.zip. Следует отметить, что драйвер мини-USB поддерживает только операционные системы Windows XP, Windows Vista и Windows 7.
- Чтобы подтвердить действительность версии при обновлении программного обеспечения устройства или установке патча, необходимо проверить значение хэш-памяти MD5. Эта операция предотвратит изменение или замены программного обеспечения, поэтому рекомендуется ее выполнять.
- Для установки дважды щелкните кнопкой мыши по установочному файлу драйвера на ПК и нажмите Next. Поставьте галочку на «I accept the terms in the license agreement» и нажмите Next. Нажмите кнопку Change, чтобы изменить директорию драйвера, если требуется, и нажмите Next. Нажмите Install и распакуйте драйвер. Когда система завершит распаковку драйвера, нажмите кнопку Finish.
- Затем необходимо найти папку DISK1 в указанном каталоге драйверов и дважды щелкнуть по значку файла setup.exe. После открытия второго окна установки нажмите Next. Снова поставьте галочку напротив «I accept the terms in the license agreement» и нажмите Next для установки драйвера. После завершения установки нажмите кнопку Finish, чтобы завершить установку драйвера. Щелкните My Computer и выберите Manage > Device Manager > Ports(COM&LPT)). Система должна отобразить TUSB3410 Device с указанием установленного драйвера.

Процедуры настройки доступа к мини-USB




```
Please configure the login password (maximum length 16)
                    Enter password:huawei
                    Confirm password:huawei
                          <Huawei>
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

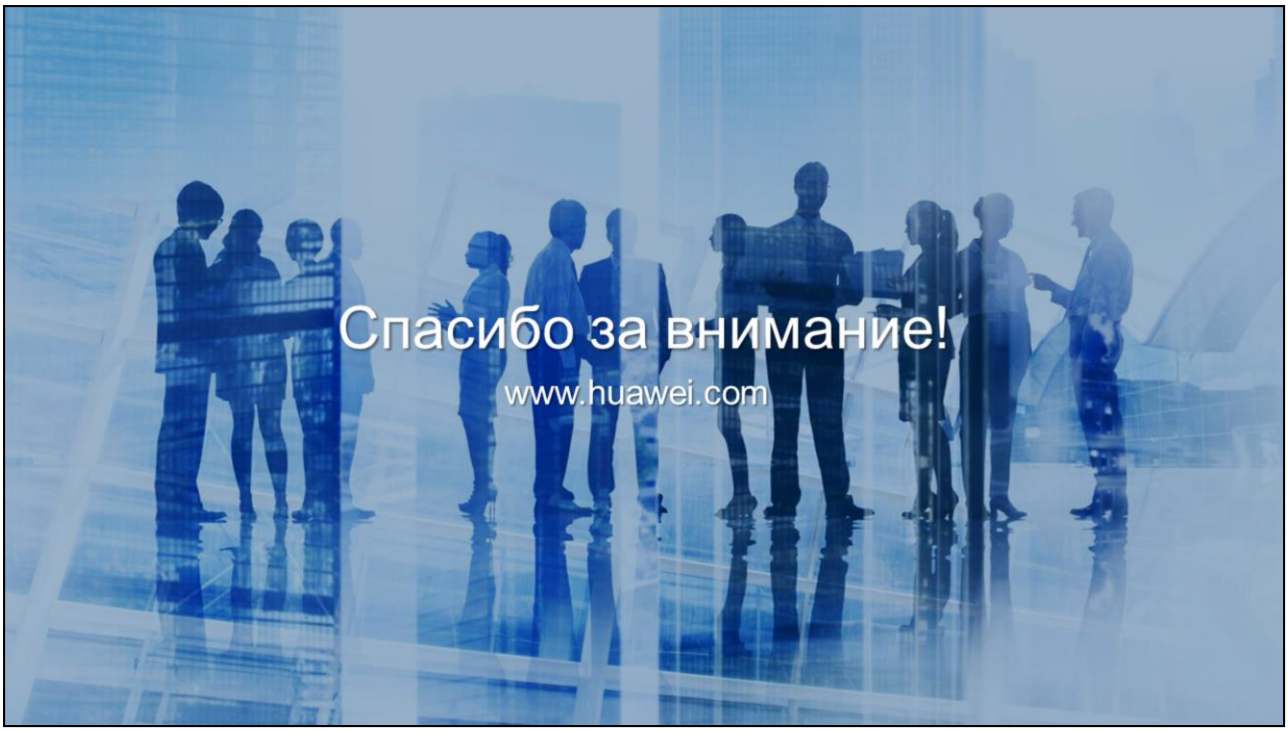
- Как и в случае с консольным соединением RS-232, последовательное соединение мини-USB требует связи с программным обеспечением эмуляции терминала для взаимодействия через командную строку VRP.
- Войдите на устройство через мини-порт USB, используя программное обеспечение эмуляции терминала (в примере используется Windows HyperTerminal). На хост-ПК запустите приложение HyperTerminal (пути к данному приложению отличаются в разных версиях Windows), создайте соединение, указав имя, и нажмите OK. Выберите порт соответствующего соединения (COM) и установите параметры связи для последовательного порта ПК. Эти параметры должны соответствовать значениям по умолчанию, установленным в окне, которое появляется нажатием кнопки Restore Defaults.
- После нажатия Enter отобразится информация о консоли с запросом пароля для входа в систему. Введите соответствующий пароль и пароль подтверждения, и система сохранит пароль.

Заключение

- Каким будет ответ шлюза при широковещательной передаче Ethernet, как в случае с ARP с локальным узлом назначения?
- Какие версии VRP в настоящее время поддерживаются продуктами Huawei?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Любой широковещательный трафик, генерируемый конечной системой в локальной сети, будет передаваться всем узлам назначения. Кадр, переданный маршрутизатору или устройству, выполняющему роль шлюза сети, будет проанализирован, и если будет обнаружено, что пункт назначения для локально определенного хоста не шлюз, а другой узел, кадр будет отброшен. Таким образом, определяется граница любого широковещательного домена.
- VRP версии 5 поддерживается большим числом текущих устройств Huawei, а устройства профессионального класса часто поддерживают VRP версии 8.


Спасибо за внимание!
www.huawei.com

Использование интерфейса командной строки (CLI)

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

Реализация устройств Huawei в корпоративной сети требует знаний и навыков работы с интерфейсом командной строки операционной системы VRP, умения конфигурировать параметры системы. Таким образом, в данном разделе предлагается изучить принципиальную архитектуру интерфейса командной строки наряду с функциями навигации и помощи, а также общими настройками системы, которые необходимо понимать для успешного конфигурирования любого устройства, управляемого с помощью VRP.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Цели

По завершении этого раздела обучающиеся смогут:

- Выполнять операции через интерфейс командной строки VRP.
- Конфигурировать основные параметры операционной системы VRP.
- Выполнять базовые настройки интерфейса VRP и управляющие операции.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

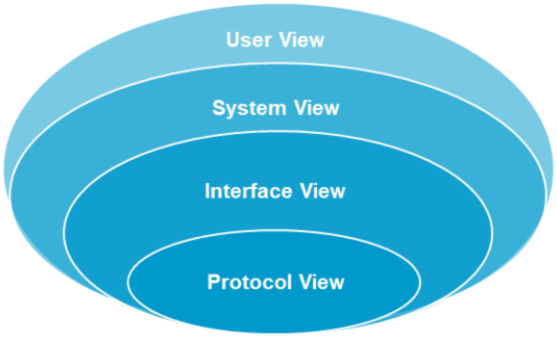
Запуск устройства

```
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
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Процесс запуска/загрузки представляет собой начальную фазу работы любого администратора или инженера, имеющего доступ к продуктам на базе Huawei, работающим под управлением VRP. Экран загрузки информирует о процедурах запуска системы, версии образа VRP, реализованной на устройстве, а также способе загрузки. После начальной процедуры запуска система предлагает сделать выбор режима конфигурирования исходных настроек системы — автоматический или ручной. Автоматический процесс настройки запускается при нажатии yes в окне запроса.

Представления интерфейса командной строки



Просмотр рабочего состояния и статистических данных устройства.

Установка системных параметров устройства.

Установка параметров интерфейса.

Установка большинства параметров протокола маршрутизации.

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


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Иерархическая структура режима командной строки VRP определяет ряд представлений команд, используя которые пользователи могут выполнять операции. В интерфейсе командной строки предусмотрено несколько командных представлений (в примере представлены общие представления). Каждую команду можно выполнить в одном или нескольких представлениях, то есть для выполнения любой команды необходимо войти в соответствующее представление. Исходным командным представлением VRP является User View. В нем отслеживаются статусы параметров и общая статистическая информация. Для применения изменений к системным параметрам пользователи должны войти в представление System View. Также предусмотрены несколько подуровней команд, где можно выполнять задачи уровня подсистемы, например Protocol View и Interface View.
- Названия представлений интерфейса командной строки вносятся в круглые скобки. Наличие символов указывает на то, что пользователь в настоящее время находится в представлении User View, в то время как квадратные скобки указывают на переход к System View.

Функции CLI

Команда	Функция
CTRL+A	Перемещение курсора в начало текущей строки.
CTRL+C	Остановка выполнения текущих функций.
CTRL+Z	Возвращение к пользовательскому представлению (user view).
CTRL+]	Прерывание входящих соединений или перенаправление соединений.

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


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- В примере показаны комбинации клавиш для быстрого вызова команд, которые широко используются для ускорения операций, выполняемых в интерфейсе командной строки VRP. Дополнительные команды:
  - CTRL + B перемещает курсор на один символ назад.
  - CTRL + D удаляет символ, на котором находится курсор.
  - CTRL + E перемещает курсор на конец текущей строки.
  - CTRL + F перемещает курсор на один символ вперед.
  - CTRL + H удаляет символ слева от курсора.
  - CTRL + N отображает следующую команду в буфере истории команд.
  - CTRL + P отображает предыдущую команду в буфере истории команд.
  - 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 на одно слово вперед.

Функции CLI

Команда	Функция
Backspace	Удаляет символ слева от курсора и перемещает курсор влево.
← или Ctrl+B	Перемещает курсор влево на расстояние одного символа.
→ или Ctrl+F	Перемещает курсор вправо на расстояние одного символа.
TAB	Выполняет команду по любому не полностью введенному ключевому слову.

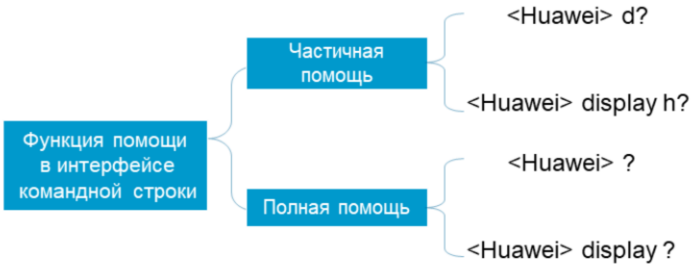
```
[Huawei]inter //TAB
[Huawei]interface
```

- Клавиша tab автоматически завершает выполнение команды по введенной строке символов.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Для выполнения одних и тех же операций можно использовать комбинацию клавиш или функциональные клавиши, например, клавиша backspace выполняет ту же операцию, что и комбинация CTRL + H – удаляет символ слева от курсора. Клавиши левой и правой стрелок (←) и (→) выполняют те же операции, что и комбинации CTRL + B и CTRL + F. Клавиша стрелка вниз (↓) выполняет ту же операцию, что и комбинация Ctrl + N, а клавише стрелка вверх (↑) соответствует комбинация CTRL + P.
- Кроме того, функции командной строки поддерживают средство автоматического завершения выполнения команды, если командное слово уникально. В примере показано автоматическое завершение выполнения команды при частичном вводе слова interface и нажатии клавиши tab. Если командное слово не является уникальным, при каждом нажатии клавиши tab будут предлагаться возможные варианты.

Функция помощи в CLI




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


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- В VRP две формы помощи — частичная и полная. Если за введенной строкой символов сразу следует знак вопроса (?), VRP реализует функцию частичной помощи, отображая все команды, начинающиеся с этой строки символов. Эта функция показана в текущем примере. В случае полной помощи, знак вопроса (?) может быть помещен в командную строку любого представления. Ответ будет содержать все возможные имена команд вместе с описаниями команд, относящихся к этому представлению. Кроме того, функция полной помощи поддерживает ввод команд, отделенных от знака вопроса (?) пробелом. Ответ будет содержать все ключевые слова, связанные с этой командой, а также простые описания.

Базовые настройки устройства через CLI

Команда	Функция
sysname	Конфигурирование имени устройства.

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

- Для уникальной идентификации каждого устройства в корпоративной сети необходимо присвоить имя системы.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- В большинстве отраслевых сетей, скорее всего, будут работать не одно, а несколько управляемых устройств. Таким образом, одной из первых важных задач ввода устройства в эксплуатацию является присвоение ему имени для уникальной идентификации в сети. На маршрутизаторе серии AR2200 по умолчанию задано имя Huawei, а на коммутаторах серии S5720 — HUAWEI. Имя системы вступает в силу сразу после завершения конфигурирования.

Настройки часов через CLI

Команда	Функция
clock timezone	Установка часового пояса.
clock datetime	Установка текущего времени и даты.
clock daylight-saving-time	Установка летнего времени.

```
<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 © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Системные часы отражают время системы и настраиваются в соответствии с правилами любого региона. Необходимо правильно установить системное время, чтобы обеспечить синхронизацию с другими устройствами. Формула расчета времени: Coordinated Universal Time (UTC) + Time zone offset + Daylight saving time offset. Команда clock datetime используется для установки системного времени по формуле ЧЧ:ММ:СС ГГГГ-ММ-ДД. Однако следует отметить, что если часовой пояс не был настроен или установлен в значение 0, то дата и время считаются по UTC, поэтому рекомендуется установить часовой пояс, прежде чем конфигурировать время и дату системы.
- Установка локального часового пояса выполняется с помощью команды clock timezone и реализуется на основе формулы time-zone-name { add | minus } offset, где значение add указывает на то, что время time-zone-name равно времени UTC плюс смещение часового пояса, а minus означает, что время time-zone-name равно времени UTC минус смещение часового пояса.
- Некоторые регионы требуют реализацию зимнего времени для обеспечения синхронизации времени с любыми изменениями часового пояса в течение определённых сезонов года. VRP также поддерживает функции энергосбережения как для фиксированных дат, так и для дат, которые определяются на основе набора предопределенных правил. Например, в Соединенном Королевстве переход с зимнего на летнее время происходит в последнее воскресенье марта и обратный переход - в последнее воскресенье октября, поэтому правила должны учитывать такие условия.

Настройка сообщений в CLI

Команда	Функция
header login	Настройка сообщения, отображаемого на терминале во время прохождения пользователем процедуры аутентификации на устройстве.
header shell	Настройка сообщения, отображаемого на терминале после входа пользователя 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>
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Команда header позволяет настроить уведомления, показываемые во время подключения к устройству. login header служит для настройки информации, отображаемой при подключении к терминалу и прохождении пользователем процедуры аутентификации. shell header служит для настройки информации, отображаемой при установке сеанса после входа пользователя на устройство. Текст можно ввести вручную или использовать текст из указанного файла. При вводе текста в текстовой строке необходимо определить начальный и конечный символы, которые будут служить маркером для идентификации сообщения (в приведенном примере таким символом является "). Строка может содержать от 1 до 2000 символов, включая пробелы. Данная команда имеет формат header { login | shell } information text, где information представляет собой текст сообщения, включая начальные и конечные символы.
- В случае использования текста из файла применяется формат header { login | shell } file file-name, где file-name представляет каталог и файл, из которого может быть получен текст сообщения.

Уровни команд CLI

Уровень пользователя	Уровень команды	Название
0	0	Visit
1	0 и 1	Monitoring
2	0, 1 и 2	Configuration
3-15	0, 1, 2 и 3	Management

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

- Права пользователей на выполнение команд регулируются уровнями привилегий.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

- Доступ к функциям команд иерархически структурирован, тем самым достигается безопасность системы. Администратор устанавливает уровни доступа пользователей, в соответствии с которыми определенные пользователи получают права на выполнение определенных команд. Уровень команд может принимать значение от 0 до 3, а уровень доступа пользователя - от 0 до 15. Уровень 0 – это уровень посещения Visit, предоставляющий доступ к командам на использование сетевых диагностических инструментов (например, ping и traceroute), а также к командам на клиентские соединения telnet и командам отображения select.
- Уровень мониторинга Monitoring определяется на уровне пользователя 1, для которого могут применяться уровни команд 0 и 1, что позволяет использовать большинство команд отображения, за исключением команд отображения текущей и сохраненной конфигурации. Уровень пользователя 2 представляет уровень конфигурирования Configuration, для которого могут быть определены уровни команд до 2, что позволяет получить доступ к командам на конфигурирование сетевых услуг, предоставляемых непосредственно пользователям, включая команды маршрутизации и сетевого уровня. Конечным уровнем является уровень управления Management, который представляет собой уровень пользователя от 3 до 15 и уровень команд до 3 и дает доступ к командам, которые контролируют основные операции системы и обеспечивают поддержку услуг.
- Эти команды охватывают файловую систему, FTP, TFTP, конфигурационные файлы, контроль источника питания, управление резервной платой, управление пользователями, настройки уровней, настройки внутренних параметров системы и команды отладки для диагностики неисправностей. Приведенный пример показывает, как можно изменить уровень команд – для выполнения команды save в представлении user view требуется получить уровень 3 до того, как команда будет использована.

Интерфейсы пользователя CLI

Интерфейс пользователя	Относительное число
Консоль	0
VTY	0-4

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

- Для увеличения числа пользовательских подключений Telnet/SSH диапазон VTY можно расширить до 0-14.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Каждый пользовательский интерфейс представлен в системе в виде интерфейса пользователя или в виде командной строки. Режим командной строки используется для конфигурирования и управления всеми физическими и логическими интерфейсами в асинхронном режиме. Пользователи, желающие подключиться к устройству, должны будут указать определенные параметры, которые сделают пользовательский интерфейс доступным. Две формы пользовательского интерфейса реализованы в виде интерфейса консоль (CON) и интерфейса VTY.
- Порт консоли представляет собой асинхронный последовательный порт, предоставляемый главной платой управления устройства, и использует относительное число 0. VTY - это логический канал терминала, который позволяет установить соединение, когда устройство подключается к терминалу через службу telnet для локального или удаленного доступа. Максимум 15 пользователей могут использовать логический пользовательский интерфейс VTY для входа на устройство, расширяя диапазон от 0 до 4. Это достигается с помощью команды user-interface maximum-vty 15. Если установлено максимальное число пользователей входа в систему 0, то пользователям не разрешается входить в маршрутизатор через telnet или SSH. Команда display user-interface может использоваться для отображения соответствующей информации о пользовательском интерфейсе.

Свойства терминала CLI

Команда	Функция
idle-timeout	Установка длительности таймаута пользовательского соединения.
screen-length	Установка количества линий, отображаемых на каждом экране терминала после выполнения команды.
idle-timeout	Задание размера буфера истории 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 © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- В целях расширения функций и повышения безопасности для интерфейсов терминала VTY и консоли задаются определённые свойства. Пользователь, оставляющий соединение простаивать в течение определенного периода времени, создает риск для безопасности системы. Система автоматически завершит соединение по истечении определенного времени. Этот период ожидания простоя на пользовательском интерфейсе по умолчанию установлен в 10 минут.
- При необходимости увеличения или уменьшения количества линий, отображаемых на экране терминала при использовании команды display, применяется команда screen-length. По умолчанию установлено значение 24, однако оно может быть увеличено максимум до 512 линий. Использовать значение 0 в команде screen-length, однако, не рекомендуется, так как командный вывод не будет отображаться.
- Для каждой используемой команды запись хранится в буфере истории команд, который можно получить с помощью клавиш (↑) или CTRL+P и (↓) или Ctrl+N . Количество записанных команд в буфере командной строки может быть увеличено с помощью команды history-command max-size до 256. Количество команд, хранящихся по умолчанию, составляет 10.

Настройка привилегий в CLI

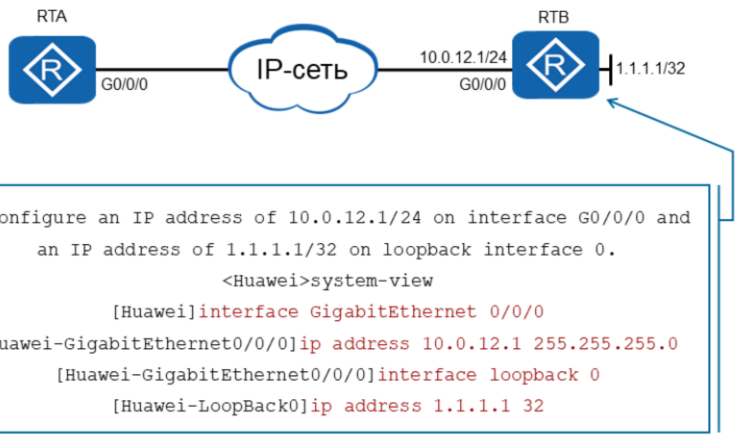
Команда	Функция
user privilege	Конфигурирование уровня пользователя.
set authentication password	Конфигурирование локального пароля для прохождения аутентификации.

```
# 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
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Через интерфейсы пользовательских терминалов возможен доступ к устройству со стороны несанкционированных пользователей, которые могут нечаянно или умышленно изменить настройки. Таким образом, в качестве средства обеспечения безопасности устройства необходимо ограничить доступ и масштаб выполняемых операций. Настройка пользовательских привилегий и аутентификация - это два способа повышения безопасности терминала. Привилегия пользователя позволяет определить уровень, который ограничивает команды, выполняемые данным пользователем. Уровень пользователя может быть любым значением в диапазоне от 0 до 15, которые означают уровень посещения (0), уровень мониторинга (1), уровень конфигурирования (2) и уровень управления (3).
- Аутентификация путем запроса пароля или комбинации имени пользователя ограничивает доступ пользователя к интерфейсу терминала. Что касается подключений VTY, все пользователи должны пройти аутентификацию перед получением доступа. Для всех пользовательских интерфейсов существуют три возможных режима аутентификации: AAA, аутентификация по паролю и режим без аутентификации. AAA обеспечивает аутентификацию пользователя с высокой степенью безопасности, для которой необходимо ввести имя пользователя и пароль для входа в систему. Для аутентификации по паролю требуется только пароль для входа в систему, поэтому один пароль может применяться ко всем пользователям. Использование режима без аутентификации отменяет любую аутентификацию, применимую к пользовательскому интерфейсу. Следует отметить, что по умолчанию интерфейс консоли использует режим без аутентификации.
- Рекомендуется, чтобы каждый пользователь, которому предоставляется доступ к telnet, имел имя и пароль, по которым его можно будет отличать от других пользователей. Каждому пользователю также должны предоставляться привилегии, основанные на его роли и степени ответственности.

Конфигурирование в CLI



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.
HUAWEI

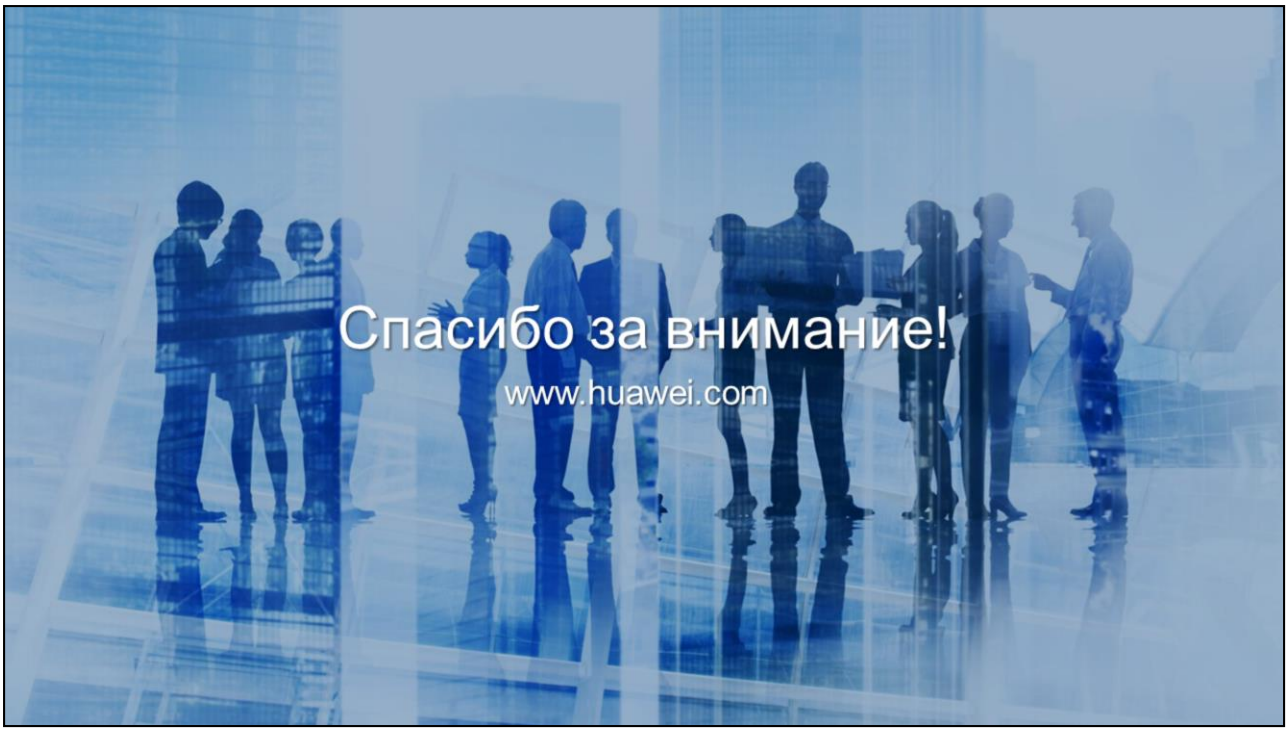
- Для запуска IP-служб на интерфейсе необходимо сконфигурировать для него IP-адрес. Как правило, необходим только первичный IP-адрес. В особых случаях может быть сконфигурирован вторичный IP-адрес. Например, когда интерфейс маршрутизатора, например AR2200 соединяется с физической сетью, и хосты этой физической сети принадлежат к двум сегментам сети.
- Чтобы устройство AR2200 могло взаимодействовать со всеми хостами в физической сети, сконфигурируйте основной IP-адрес и вторичный IP-адрес для интерфейса. Интерфейс имеет только один первичный IP-адрес. Если на интерфейсе, который уже имеет первичный IP-адрес, будет сконфигурирован новый первичный IP-адрес, его значение перезапишет исходный адрес. IP-адрес для интерфейса конфигурируется с помощью команды <ip-address > { mask | mask-length }, где mask – это 32-разрядная маска подсети, например, 255.255.255.0, а mask-length - альтернативное значение mask-length, например, 24. Эти параметры взаимозаменяемы.
- Интерфейс loopback представляет собой логический интерфейс, используемый для представления адреса сети или IP-хоста, и часто используется в качестве интерфейса управления в поддержку ряда протоколов, через которые осуществляется связь с IP-адресом интерфейса loopback, в отличие от IP-адреса физического интерфейса, на который поступают данные.

Заключение

- Сколько пользователей могут подключиться через интерфейс консоли в один момент времени?
- Каково состояние интерфейса loopback 0 при использовании команды *loopback interface 0*?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Интерфейс консоли обеспечивает доступ только одного пользователя в один момент времени; за это отвечает представление user interface консоли 0.
- Интерфейс loopback представляет собой логический интерфейс, который отсутствует в маршрутизаторе, и его необходимо создать. Созданный интерфейс loopback считается включенным. Однако на устройствах ARG3 интерфейсы loopback могут быть отключены.


Спасибо за внимание!
www.huawei.com

Работа с файловой системой и управление

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

Файловая система представляет собой базовую платформу, на которой работает операционная система VRP, и где системные файлы хранятся на физических устройствах хранения. Навыки работы с файловой системой необходимы для эффективного управления конфигурационными файлами, проведения обновлений программного обеспечения VRP и надлежащей поддержки физических устройств.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Цели

По окончании этого модуля слушатели смогут:

- Успешно работать с файловой системой устройства
- Выполнять операции с файлами и папками файловой системы.
- Управлять устройствами хранения маршрутизаторов и коммутаторов Huawei.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Просмотр файловой системы

Функция	Команда
Изменение каталога	cd
Просмотр текущего каталога	pwd
Просмотр содержимого каталога	dir
Просмотр содержимого файла	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)
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Файловая система управляет файлами и каталогами на устройствах хранения. В системе можно создавать, удалять, изменять или переименовывать файлы или каталоги или отображать содержимое файла.
- Файловая система имеет две функции: управление устройствами хранения и управление файлами, хранящимися на этих устройствах. Определен 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 поддиректориях, а также создавать или удалять каталоги.
- Примеры общих команд файловой системы: cd – команда, используемая для изменения текущего каталога, pwd - для просмотра текущего каталога и dir - для отображения содержимого каталога, как показано в примере. Доступ к файловой системе осуществляется через представление User View.

Управление файловой системой

Функция	Команда
Создание каталога	mkdir
Удаление каталога	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)
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Под внесением изменений в существующие каталоги файловой системы обычно понимается создание и удаление существующих каталогов в файловой системе. Для этого используются две команды. Команда mkdir directory используется для создания папки в указанном каталоге на заданном устройстве хранения, где directory – это имя, присвоенное каталогу, строка, содержащая от 1 до 64 символов. Для удаления папки в файловой системе используется команда rmdir directory, где directory – это также имя каталога. Следует отметить, что любой каталог может быть удален только в том случае, если в нем нет файлов.

Управление файловой системой

Функция	Команда
Копирование файла	copy
Перемещение файла	move
Переименование файла	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 © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Внесение изменений в файлы в файловой системе включает следующие операции: копирование, перемещение, переименование, сжатие, удаление, отмену удаления, удаление файлов из корзины, запуск файлов в пакетном режиме и конфигурирование режимов подсказок. Создание дубликата существующего файла можно выполнить с помощью команды copy source-filename destination-filename, при этом если destination-filename совпадает с именем существующего файла (source-filename), система выдаст сообщение, указывающее на то, что существующий файл будет заменен. Имя нового файла не может быть таким же, как и имя исходного файла, иначе система выдаст сообщение о том, что операция недействительна и что файл является исходным файлом.
- Команда move source-filename destination-filename перемещает файлы в другой каталог. После успешного выполнения команды move исходный файл вырезается и перемещается в указанный файл. Однако следует отметить, что команда move может перемещать файлы только в пределах одного устройства хранения.

Управление файловой системой

Функция	Команда
Обычное или безвозвратное удаление файла	delete /unreserved
Восстановление файла	undelete
Безвозвратная очистка корзины	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)
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Для удаления файлов из файловой системы применяется команда delete [/ unreserved] [/ force] {filename | device-name}. Как правило, удаленные файлы отправляются в корзину, откуда их можно восстановить с помощью команды undelete {filename | device-name}, но при использовании команды /unreserved файл будет удален безвозвратно. Система, как правило, выдает сообщение с запросом на подтверждение удаления файла, однако если включен параметр /force, сообщение не поступит. Параметр filename – это имя файла, который должен быть удален, а параметр device-name определяет место хранения.
- Если файл помещается в корзину, он не удаляется навсегда и его можно легко восстановить. Для безвозвратного удаления файлов из корзины применяется команда reset recycle-bin [filename], где параметр filename – это имя удаляемого файла.

Система управления конфигурационными файлами

- Текущая конфигурация загружается из конфигурационного файла, сохраненного во флеш-памяти, при запуске системы.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Во время включения питания устройство в целях инициализации извлекает конфигурационные файлы из места их хранения, заданного по умолчанию, путь к которому затем хранится в ОЗУ устройства. Если конфигурационные файлы не существуют в месте хранения по умолчанию, маршрутизатор использует параметры инициализации по умолчанию.
- Файл current-configuration содержит конфигурации, действующие на работающем устройстве. При сохранении текущая конфигурация помещается в файл saved-configuration на устройстве хранения. Если устройство загрузило файл current-configuration на основе параметров инициализации по умолчанию, файла saved-configuration не будет в месте хранения, заданном по умолчанию, но он будет сгенерирован после сохранения текущей конфигурации.

Просмотр конфигурационных файлов

Команда	Функция
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 © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- С помощью команды display current-configuration можно запросить параметры устройства, которые вступают в силу. Если для определенных параметров используются значения по умолчанию, эти параметры не отображаются. Команда current-configuration включает в себя ряд параметров, которые позволяют фильтровать список команд во время использования функции отображения. display current-configuration | begin {regular-expression} – это пример того, как можно использовать текущую конфигурацию для отображения активных параметров, начинающихся с конкретного ключевого слова или выражения. Альтернативой этой команде является команда display current-configuration | include {regular-expression}, которая позволяет задавать параметры, включающие конкретное ключевое слово или выражение из файла current-configuration.
- Команда display saved-configuration [last | time] выводит файл сохраненной конфигурации, используемого для создания файла с текущей конфигурации при запуске. Параметр last (если используется) отображает конфигурационный файл, используемый в текущем запуске. Файл конфигурации отображается только в том случае, если он сконфигурирован для текущего запуска. Параметр time будет отображать время последнего сохранения конфигурации.

Сохранение файла конфигурации

Команда	Функция
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
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Команда save [configuration-file] сохраняет текущую конфигурационную информацию в место хранения, заданное по умолчанию. Параметр configuration-file позволяет сохранить текущую конфигурационную информацию в указанном файле. Выполнение команды save с параметром configuration-file не влияет на текущий файл конфигурации запуска системы. Если параметр configuration-file совпадает с конфигурационным файлом, хранящимся в месте хранения системы, заданном по умолчанию, функция этой команды совпадает с функцией команды save.
- Пример показывает использование команды save для сохранения текущей конфигурации, которая по умолчанию будет храниться в файле vrpcfg.zip в месте хранения устройства по умолчанию.

Просмотр параметров запуска

Команда	Функция
Display startup	Просмотр текущих параметров запуска

```
<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
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Используемый в текущий момент файл конфигурации можно найти с помощью команды display startup. Кроме того, команда display startup может использоваться для запроса имени текущего файла системного программного обеспечения, имени следующего файла системного программного обеспечения, имени резервного файла программного обеспечения, имен четырех используемых в настоящее время (в случае использования) файлов системного программного обеспечения и имен четырех следующих файлов системного программного обеспечения. Четыре вышеупомянутых файла системного программного обеспечения: конфигурационный файл, голосовой файл, файл патча и файл лицензии.

Изменение параметров запуска

Команда	Функция
startup saved-configuration	Указание файла сохраненной 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 © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- После обнаружения файла startup saved-configuration необходимо определить новый файл конфигурации, который будет загружен при следующем запуске. Если конкретный файл конфигурации не будет указан, при следующем запуске будет загружен файл конфигурации, заданный по умолчанию.
- Расширение файла конфигурации должно быть .cfg или .zip, и файл должен храниться в корневом каталоге устройства хранения. Маршрутизатор после включения проходит инициализацию, считывая данный файл из флеш-памяти по умолчанию. Данные в этом файле являются исходной конфигурацией. Если нет сохраненного файла конфигурации во флеш-памяти, маршрутизатор использует для инициализации параметры по умолчанию.
- Используя команду startup saved-configuration [configuration-file] в тех случаях, где параметр configuration-file представляет собой конфигурационный файл, используемый при запуске, можно задать новый файл конфигурации для инициализации при следующем запуске системы.

Сравнение конфигурационных файлов

Команда	Функция
compare configuration	Сравнение конфигурационных файлов

```
<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 © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- При использовании команды compare configuration [configuration-file] [current-line-number save-line-number] система выполняет построчное сравнение сохраненной конфигурации с текущей конфигурацией, начиная с первой строки. Если заданы параметры current-line-number save-line-number, система пропускает нерелевантную информацию и продолжает искать различия между конфигурационными файлами.
- После этого система выводит различия между файлами сохраненной и текущей конфигурации. По умолчанию выводимая информация о сделанном сравнении ограничивается 150 символами. Если для сравнения требуется менее 150 символов, будут выведены все варианты до конца двух файлов.

Удаление файла конфигурации

Команда	Функция
reset saved-configuration	Удаление файла сохраненной 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.
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Команда reset saved-configuration используется для удаления файла конфигурации запуска устройства с устройства хранения. При выполнении операции система сравнивает конфигурационные файлы, используемые в текущем запуске и следующем запуске.
- Если два файла конфигурации одинаковы, они удаляются одновременно этой командой. Файл конфигурации, заданный по умолчанию, будет использован при запуске маршрутизатора в следующий раз. Если два файла конфигурации отличаются друг от друга, удаляется файл конфигурации, используемый в текущем запуске.
- Если конфигурационный файл не будет сконфигурирован для текущего запуска устройства, система после выполнения этой команды выдаст сообщение о том, что файл конфигурации не существует. После использования команды reset saved-configuration будет выдан запрос на подтверждение действия (см. пример).

Типы устройств хранения данных

- SDRAM
- Флеш-память
- NVRAM
- SD-карта
- USB-накопитель

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


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Тип применяемого устройства хранения зависит от типа продукта. Это может быть флеш-память, SD-карты или USB-накопители. Например, маршрутизатор AR2200E имеет встроенную флеш-память и SD-карту (в слоте sd1). Маршрутизатор предоставляет два зарезервированных слота USB (usb0 и usb1) и слот SD-карты (sd0). Коммутатор S5700 имеет встроенную флеш-память с емкостью, которая зависит от модели (память 64 МБ поддерживается в моделях S5700C-HI, S5700-LI, S5700S-LI и S5710-EI, а 32 МБ для всех остальных). Подробную информацию об устройствах хранения, используемых в продуктах Huawei, можно получить с помощью команды display version, как показано на рисунке.

Очистка памяти устройств хранения

```
<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]:
```

- Будьте осторожны, используя команды форматирования, поскольку в результате ее выполнения данные будут потеряны.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Форматирование устройства хранения, скорее всего, приведет к потере всех хранящихся на нем файлов, и их нельзя будет восстановить, поэтому при выполнении любой команды форматирования необходимо проявлять дополнительную осторожность, и рекомендуется ее избегать, если нет в этом необходимости. Команда format [storage-device] используется вместе с параметром storage-device, который определяет место расположения устройства хранения, которое требуется отформатировать.

Восстановление данных устройства хранения

```
<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.
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

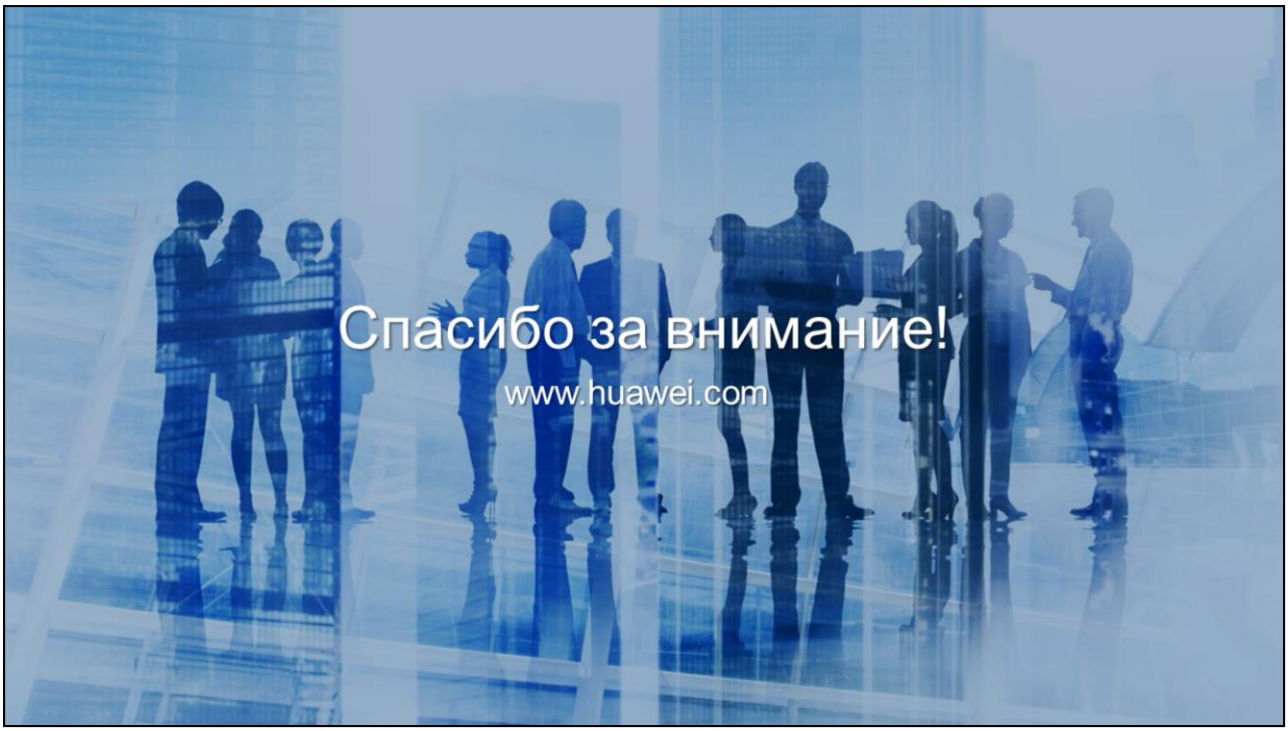
- Если терминальное устройство выводит информацию о сбое в файловой системе, для устранения проблемы применяется команда fixdisk, однако она не является залогом успешного восстановления работы файловой системы. Поскольку команда используется для устранения проблем, не рекомендуется ее запускать при отсутствии проблем в системе. Следует также отметить, что эта команда не устраняет проблемы на уровне устройства.

Заключение

- Что означает *d* в атрибуте *drwx* файловой системы?
- Как обеспечить использование устройством конфигурационного файла, хранящегося в файловой системе устройства?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Атрибут файловой системы d представляет собой каталог в файловой системе. Следует отметить, что этот каталог можно удалить только после удаления хранящихся в нем файлов. Остальные значения rwx связаны со свойствами чтения, записи и/или исполнения каталога (или файла).
- Конфигурацию можно сохранить под отдельным именем, взятым из архива vrpcfg.zip, заданного по умолчанию, и сохранить на устройстве хранения маршрутизатора или коммутатора. Если этот файл требуется использовать в качестве активного файла конфигурации в системе, применяется команда startup saved-configuration < configuration-file-name >, где configuration-file-name — это имя файла и его расширение.


Спасибо за внимание!
www.huawei.com

Управление образом операционной системы VRP

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

Эффективное управление корпоративной сетью зависит от всех устройств, поддерживающих резервные файлы в случае сбоев системы или других событий, которые могут привести к потере важных файлов и данных. Для резервного копирования и поиска файлов в случае необходимости часто используются удаленные серверы с поддержкой услуги FTP. В данном разделе представлено описание средств для установления связи с такими приложениями.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

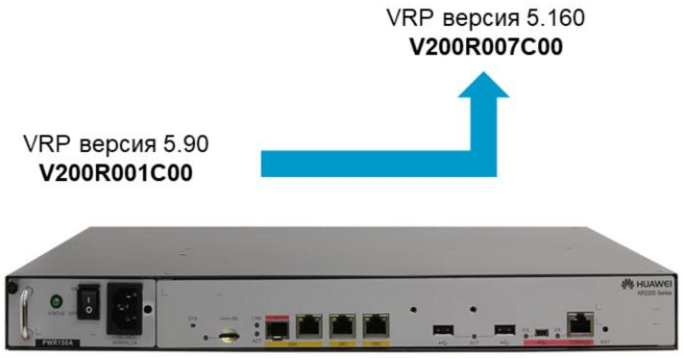
Цели

По окончании этого модуля слушатели смогут:

- Объяснить, для чего нужно поддерживать обновление VRP до актуальной версии.
- Устанавливать связь клиента с FTP-сервером.
- Обновлять образ системы VRP.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Обновление образа VRP



- Для обеспечения работы новых функций универсальной платформы маршрутизации (VRP) может потребоваться обновление системы.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Для того чтобы соответствовать постоянно изменяющимся технологиям и поддерживать усовершенствования оборудования, платформа VRP постоянно модернизируется. Образ VRP обычно определяется версией VRP и номером версии продукта. Продукты серии ARG3 и серии Sx7 Huawei, как правило, соответствуют версии VRP 5, с которой связаны различные версии продукта.

Увеличение номера версии продукта говорит о большем разнообразии функций, поддерживаемых версией. Формат версии продукта включает код продукта Vxxx, Rxxx означает старшую версию, а Cxx – младшую версию. Если для исправления версии продукта VRP используется пакет обновлений, то значение SPC может быть также включено в номер версии продукта VRP. Типичными примерами обновления версии VRP для AR2200E являются:

- Версия 5.90 (AR2200 V200R001C00)
- Версия 5.110 (AR2200 V200R002C00)
- Версия 5.160 (AR2200 V200R007C00)

Передача файлов

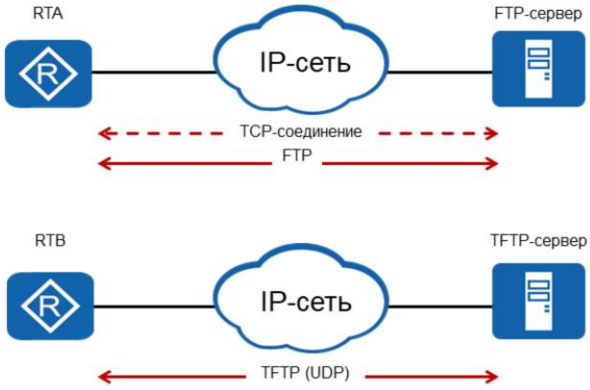
- Передача файлов используется для извлечения файлов образов VRP, а также журналов резервного копирования и конфигурационных файлов.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Передача файлов – это средство, с помощью которого файлы передаются или извлекаются с удаленного сервера или хранилища. В IP-сети это приложение может использоваться для самых разнообразных целей. Для повышения эффективности важные файлы часто дублируются и резервируются в удаленном хранилище, чтобы предотвратить потери, которые могут повлиять на критически важные системные операции. К важным файлам относятся, например, образы VRP продуктов, которые (в случае потери существующего образа в результате применения команды форматирования или других ошибок) могут быть извлечены удаленно и использованы для восстановления системных операций.

Аналогичные принципы применяются к важным файлам конфигурации и ведению записей о действиях в системных журналах, которые могут храниться в течение длительного времени на удаленном сервере.

Способы передачи файлов



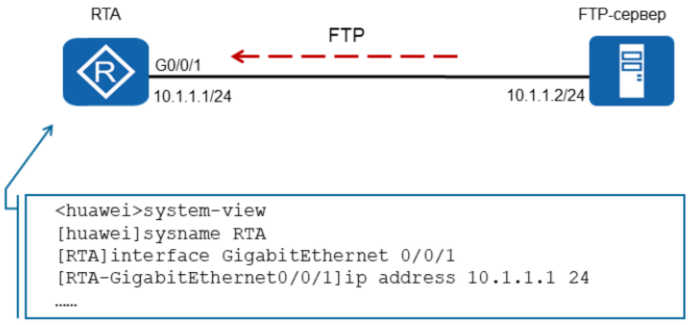
- Распространенные формы передачи файлов – это FTP и TFTP, которые зависят от используемого протокола транспортного уровня.

 Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

FTP – это стандартный протокол приложений, основанный на стеке протоколов TCP/IP и используемый для передачи файлов между локальными клиентами и удаленными серверами. FTP использует два TCP-соединения для копирования файла из одной системы в другую. TCP-соединения обычно устанавливаются в режиме клиент-сервер, один для управления (номер порта сервера - 21), а другой — для передачи данных (номер порта сервера - 20). FTP в качестве протокола передачи файлов используется для управления соединениями с помощью передачи команд от клиента (RTA) к серверу и передачи ответных сообщений с сервера клиенту, что позволяет сократить задержку передачи. С точки зрения передачи данных FTP передает данные между клиентом и сервером, максимизируя пропускную способность.

Trivial File Transfer Protocol (TFTP) – это простой протокол передачи файлов, по которому маршрутизатор может функционировать в качестве клиента TFTP для доступа к файлам на сервере TFTP. В отличие от FTP, TFTP не имеет сложного интерактивного интерфейса доступа и контроля аутентификации. Реализация TFTP основана на протоколе User Datagram Protocol (UDP). Клиент инициирует передачу TFTP. Для загрузки файлов клиент отправляет пакет запроса чтения на сервер TFTP, получает пакеты с сервера и передает подтверждение на сервер. Для выгрузки файлов клиент отправляет пакет запроса записи на сервер TFTP, отправляет пакеты на сервер и получает подтверждение от сервера.

Процесс обновления VRP



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Данный пример показывает способ установления соединения между сервером FTP и клиентом для извлечения образа VRP, который может быть использован в процессе обновления системы. Перед передачей данных необходимо установить соединение, по которому можно передавать файлы. Сначала клиенту и серверу выделяются соответствующие IP-адреса. При прямом подключении устройств применяются интерфейсы, принадлежащие одной и той же сети. В случаях, когда устройства принадлежат к сетям, расположенным в большой географической зоне, устройства должны установить соответствующую IP-адресацию в пределах своих сетей и определить соответствующий сетевой путь через IP, по которому можно установить связь между клиентом и сервером.

Доступное место в памяти


```
<RTA>dir
.....
508,248 KB total (2,334 KB free)
<RTA> delete /unreserved flash:/ar2220.cc
.....
```

- Если не удается выполнить передачу образов вследствие того, что в памяти недостаточно места, место в памяти можно освободить, удалив старые изображения и файлы.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Для любого обновления системы необходимо определить, имеется ли достаточное пространство для хранения файла, который необходимо получить. Команды файловой системы могут использоваться для определения текущего состояния файловой системы, включая файлы, которые в настоящее время находятся в хранилище файлов, а также объем имеющейся на данный момент памяти. Если объем памяти недостаточен для передачи файлов, то некоторые файлы могут быть удалены или выгружены на FTP-сервер в случае, если они могут понадобиться в будущем.

Данный пример демонстрирует использование команды delete для удаления существующего файла образа. Следует отметить, что удаление образа системы не повлияет на текущую работу устройства до тех пор, пока устройство остается в рабочем состоянии, поэтому не следует выключать или перезапускать устройство до восстановления нового файла образа VRP в хранилище устройства, и следует установить его для использования при следующем запуске системы.

Извлечение файлов с сервера FTP


```
<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 © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Для извлечения файлов с сервера FTP требуется установить соединение, прежде чем будет выполнена передача файлов. В клиентском устройстве услуга ftp инициируется с помощью ftp < ip address >, где IP-адрес – это адрес сервера FTP, к которому подключается клиент. Соединения FTP устанавливаются с использованием TCP и требуют аутентификации в виде имени пользователя и пароля, которые определяет сервер FTP. После успешного выполнения аутентификации клиент подключается к FTP-серверу и может использовать различные команды для просмотра существующих файлов, хранящихся в локальном текущем каталоге сервера.

- Перед передачей файла пользователь может задать тип файла, ASCII или Binary. Режим ASCII используется для текста, в котором данные преобразуются из символьного представления отправителя в «8-битный ASCII» перед передачей, а затем в символьное представление получателя. Двоичный (Binary) режим требует, чтобы отправитель отправлял каждый файл байт за байтом. Этот режим часто используется для передачи файлов образов и программных файлов, и его следует применять при отправке или получении любого файла образа VRP. В этом примере команда get vrp.cc используется для получения нового образа VRP, расположенного на удаленном компьютере.

Извлечение файлов с сервера TFTP

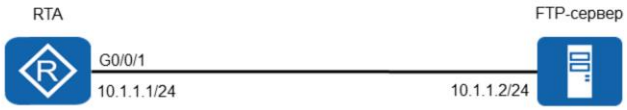

```
<RTA>tftp 10.1.1.2 get AR2220E-V200R007C00SPC600.cc
```

- Для извлечения файлов с сервера TFTP используется одна команда, включающая IP-адрес назначения.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Если клиент желает получить образ VRP с TFTP-сервера , соединение с сервером не требуется. Вместо этого клиент должен определить путь к серверу в командной строке вместе с выполняемой операцией. Следует также отметить, что модели AR2200E&S5720 выполняют только функции клиента TFTP и передают файлы только в двоичном формате. Как видно из примера, команда get применяется для извлечения файла образа VRP с сервера TFTP после определения адреса назначения сервера TFTP.

Процесс управления загрузкой VRP



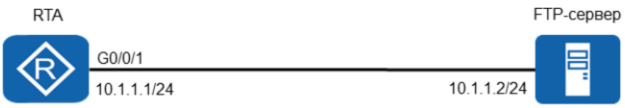

```
<RTA>startup system-software vrp.cc
Info: Succeeded in setting the software for booting system
<RTA>display startup
MainBoard:
 Configured startup system software:       flash:/ar2220.cc
 Startup system software:                  flash:/ar2220.cc
     Next startup system software:             vrp.cc
      Startup saved-configuration file:         NULL
      Next startup saved-configuration file:    NULL
.....
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Передача файла образа VRP клиенту после его успешного выполнения требует, чтобы образ был активирован при следующем запуске. Чтобы изменить версию ПО используется команда startup system-software, включая файл системного ПО, который будет использоваться при следующем запуске. Файл системного ПО должен использовать .cc в качестве расширения имени файла, а файл ПО, используемый при следующем запуске, не может использоваться при текущем запуске.

Кроме того, каталог хранения системного ПО должен быть корневым каталогом, иначе файл не будет запущен. Команда display startup должна использоваться для проверки успешного выполнения изменения ПО системы. Выходные данные для программного обеспечения системы запуска должны отображать существующий образ VRP, в то время как программное обеспечение следующего запуска должно отображать переданный образ VRP, который теперь присутствует в корневом каталоге устройства.

Применение изменений




```
<RTA>reboot
Info: The system is now comparing the configuration, please
wait.
Warning: All the configuration will be saved to the
configuration file for the next startup, Continue?[Y/N]:n
System will reboot! Continue?[Y/N]:y
```

- Перезапуск системы выполняется до того, как новый образ вступит в силу.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Подтверждение ПО системы запуска позволяет безопасно инициировать системное ПО во время следующей загрузки системы. Чтобы применить изменения и разрешить выполнение нового системного ПО необходимо перезапустить устройство. Для перезапуска системы используется команда reboot. Во время перезагрузки на экран будет выведено сообщение-запрос подтверждения сохранения файла конфигурации для следующего запуска системы.

В некоторых случаях сохраненный конфигурационный файл может быть стерт пользователем для того, чтобы выполнить новую конфигурацию. Если это произошло, то пользователь должен выбрать ответ «no» на вопрос «Continue?» Если пользователь на данном этапе выбирает «yes», то текущая конфигурация будет перезаписана в сохраненный конфигурационный файл и повторно применена во время следующего запуска. Если пользователь не знает об изменениях, для которых выводится подсказка-предупреждение, пользователю рекомендуется выбрать "no" или "n" и сравнить сохраненную и текущую конфигурации для проверки изменений. Для завершения процесса перезагрузки требуется ответ "yes" или "y".

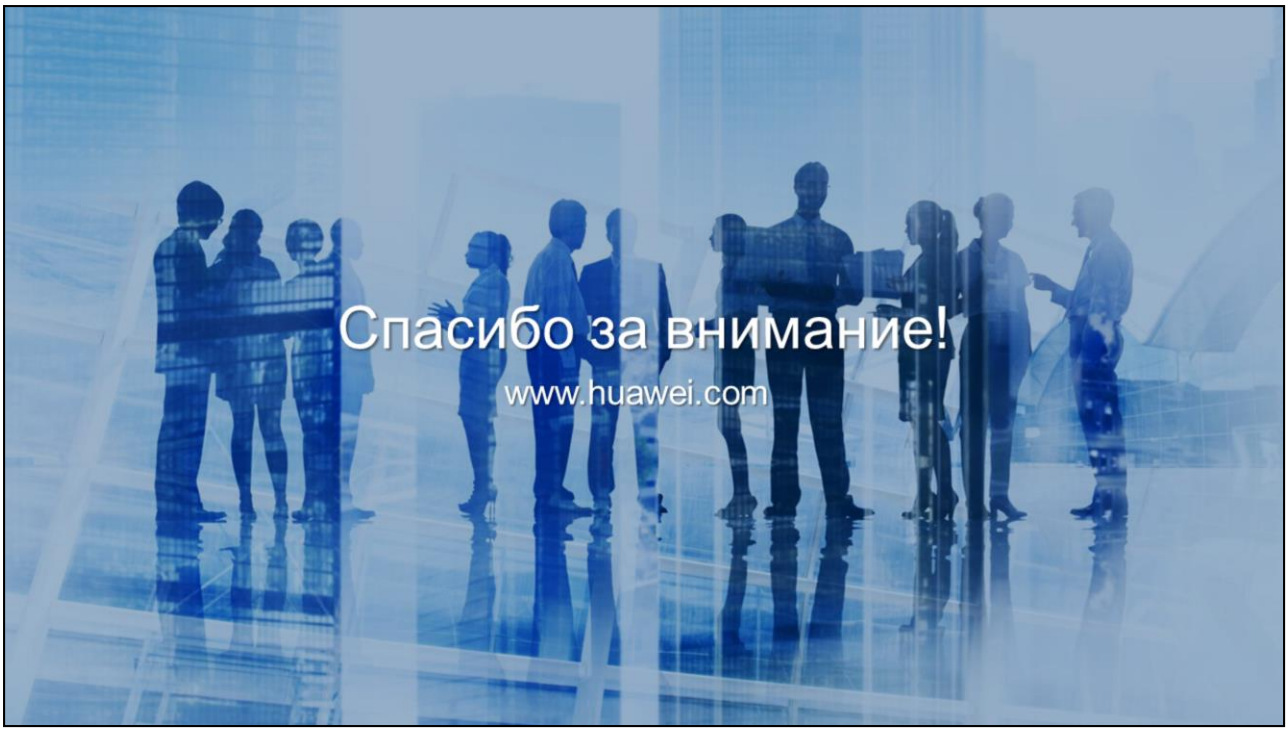
Заключение

- Что нужно сконфигурировать на клиенте для установления соединения с сервером FTP?
- Как пользователь может подтвердить, что изменения в программном обеспечении запуска вступили в силу после перезагрузки устройства?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Клиентское устройство должно подключаться к FTP-серверу по IP, что требует настройки IP-адреса на интерфейсе, по которому можно получить доступ к FTP-серверу. Это позволит проверить путь к серверу FTP на сетевом уровне, если он существует.

Пользователь может запустить команду display startup для подтверждения того, что текущее программное обеспечение системы запуска (VRP) активно и идентифицируется по расширению .cc.


Спасибо за внимание!
www.huawei.com

Развертывание сети с одним коммутатором

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

Представление коммутирующего устройства как части корпоративной сети позволяет продемонстрировать возможности расширения сетей за пределы соединений «точка-точка» и сетей общего доступа, в которых могут возникать конфликты при одновременной передаче данных. Принцип работы корпоративного коммутатора при его использовании в локальной сети подробно описывается при разъяснении процедуры обработки кадров одноадресного и широковещательного типа. Изучив данную процедуру, можно понять, каким образом коммутаторы позволяют обеспечить производительность сетей общего доступа.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

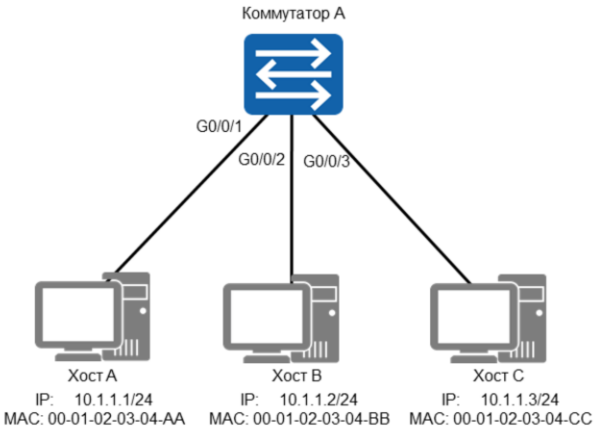
Цели

По окончании этого модуля слушатели смогут:

- Объяснить процесс принятия решения коммутатором уровня канала.
- Сконфигурировать параметры для согласования на коммутаторе уровня канала.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Организация сети с одним коммутатором

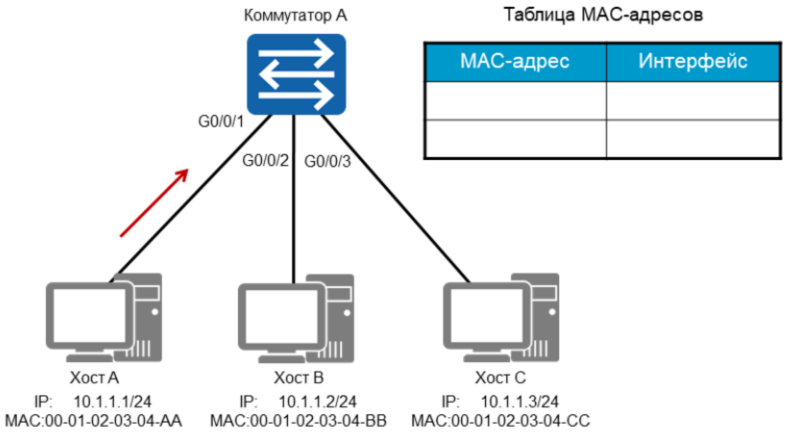


Коммутатор работает на уровне канала передачи данных.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

По мере расширения корпоративной сети необходимо создать несколько учетных записей пользователей для разграничения прав доступа. Эволюция сетевых технологий обеспечила переход от локальных сетей общего доступа к сетям, которые поддерживают несколько доменов коллизий и поддерживают использование сред 100BaseT. Это позволило изолировать передачу и прием данных по отдельным проводным парам, таким образом устраняя возможность коллизий и обеспечивая более высокие полнодуплексные скорости передачи. Развертывание коммутатора дает возможность увеличить плотность портов, чтобы обеспечить возможность подключения большего числа устройств конечной системы в пределах одной локальной сети. Каждая конечная система или хост в локальной сети должны быть подключены как часть одной и той же IP-сети, чтобы облегчить связь на сетевом уровне. Однако IP-адрес имеет отношение только к хост-системам, поскольку коммутационные устройства работают в рамках уровня канала и, следовательно, полагаются на MAC-адресацию при пересылке кадров.

Начальное состояние коммутатора

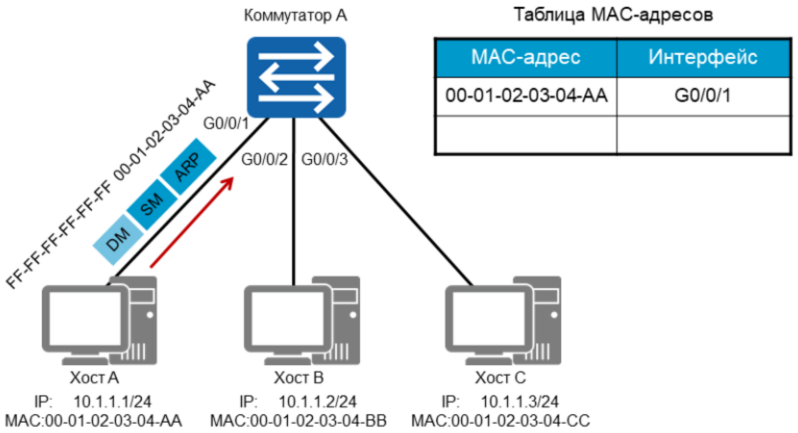


- Коммутатор использует таблицу MAC-адресов для принятия решений при передаче.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

В качестве устройства канального уровня каждый коммутатор опирается на таблицу MAC-адресов, которая обеспечивает связь между MAC-адресом назначения и интерфейсом порта, через который должен пересылаться кадр. Изначально коммутатор не знает конечных систем и того, как кадры, полученные от конечных систем, должны пересылаться. Необходимо, чтобы коммутатор создавал записи в таблице MAC-адресов, определяющие путь, который должен пройти каждый полученный кадр, чтобы достичь заданного пункта назначения. Это позволит ограничить широковещательный трафик в локальной сети. При получении кадров от конечных систем пути записываются в таблице MAC-адресов. В этом примере хост A отправил кадр коммутатору A, который в настоящее время не имеет записей в своей таблице MAC-адресов.

Запоминание MAC-адресов

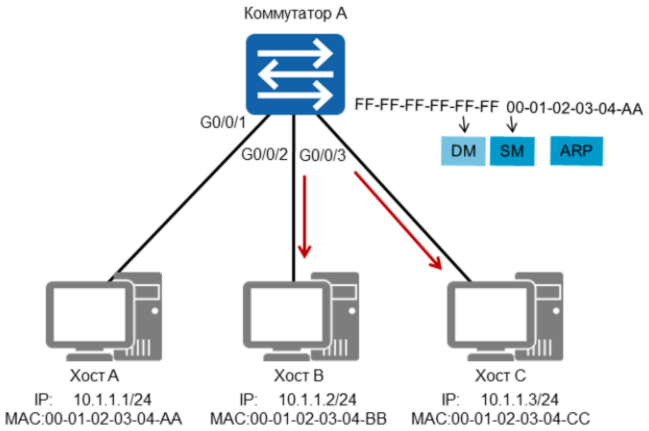


- MAC-адреса источников полученных кадров записываются в таблицу.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Кадр, который пересылается с хоста A, содержит запись MAC-адреса широковещательной рассылки в поле адреса назначения заголовка кадра. Поле адреса источника содержит MAC-адрес однорангового устройства, в данном случае хоста A. Этот MAC-адрес источника используется коммутатором для заполнения таблицы MAC-адресов путем сопоставления записи MAC-адреса в поле исходного адреса с интерфейсом порта коммутатора, через который был получен кадр. Пример показывает, как MAC-адрес ассоциируется с интерфейсом порта, чтобы любой возвращаемый трафик на данный MAC-адрес был переадресован непосредственно через соответствующий интерфейс.

Передача первоначальных данных

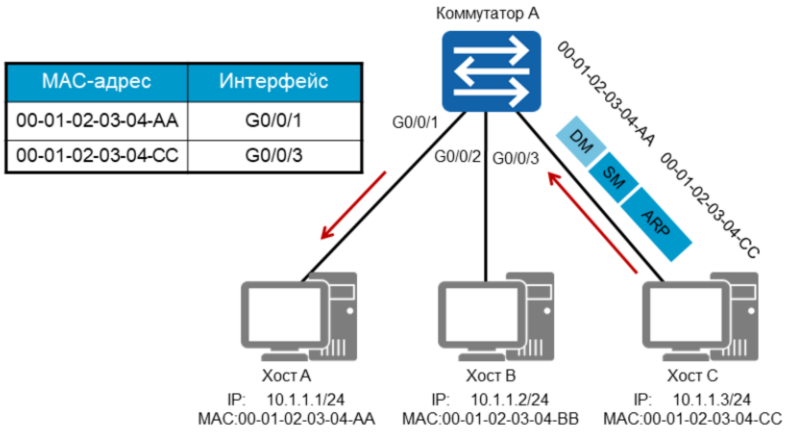


- Пересылка кадров, пункты назначения канального уровня которых неизвестны, осуществляется лавинным образом.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Общий принцип запроса ARP заключается в том, что кадр лавинным образом передается во все первоначально планируемые пункты назначения, главным образом благодаря широковещательной передаче MAC-адресов (FF-FF-FF-FF-FF-FF), которая представляет текущий пункт назначения. Таким образом, коммутатор отвечает за пересылку этого кадра из каждого интерфейса порта, за исключением интерфейса порта, на котором был получен кадр, в попытке найти предполагаемый пункт назначения IP, указанный в заголовке ARP, для которого может быть сгенерирован ответ ARP. Как показано в примере, отдельные кадры передаются от коммутатора через интерфейсы порта G0/0/2 и G0/0/3 к хостам B и C соответственно.

Ответ получателя



- Пересылка кадров по адресам назначения осуществляется на основе таблицы MAC-адресов.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

По заголовку из запроса ARP хост-получатель может определить, что заголовок ARP предназначен для пункта назначения с IP-адресом 10.1.1.3, наряду с локальным адресом источника (MAC), от которого был получен кадр, и использовать эту информацию для генерирования одноадресного ответа. Информация, касающаяся хоста A, ассоциируется с IP-адресом 10.1.1.3 и сохраняется в таблице MAC-адресов хоста C. При этом генерирование широковещательного трафика сводится к минимуму, тем самым уменьшая количество прерываний для локальных пунктов назначения, а также сокращая количество кадров, распространяющихся в локальной сети.

После получения кадра от хоста C коммутатор A внесет в таблицу MAC-адресов MAC-адрес источника полученного кадра и ассоциирует его с интерфейсом порта, на котором был получен кадр. Затем коммутатор выполнит поиск по таблице MAC-адресов, чтобы обнаружить интерфейс пересылки на основе MAC-адреса пункта назначения кадра. В этом случае MAC-адрес кадра относится к хосту A, для которого теперь существует запись через интерфейс G0/0/1, что позволит переслать кадр в нужное место назначения.

Базовая конфигурация


```
<SWA>system-view
Enter system view, return user view with Ctrl+Z.
[SWA]interface GigabitEthernet 0/0/1
[SWA-GigabitEthernet0/0/1]undo negotiation auto
[SWA-GigabitEthernet0/0/1]duplex full
[SWA-GigabitEthernet0/0/1]speed 100
```

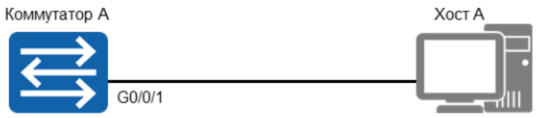

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Ранние системы Ethernet работали на основе полудуплексного режима 10 Мбит/с, и для обеспечения стабильности в них использовались такие механизмы, как CSMA/CD. Переход на витые пары в качестве передающей среды привел к появлению полнодуплексного режима Ethernet, что значительно улучшило производительность и позволило согласовать режимы дуплекса. Технология автоматического согласования обеспечивает совместимость новых систем Ethernet и систем Ethernet предыдущего поколения.

В режиме автосогласования обеспечивается соответствие рабочих параметров интерфейсов на обоих концах канала, включая дуплексный режим, скорость и управление потоком. Если согласование прошло успешно, оба интерфейса работают с одинаковыми рабочими параметрами. Однако в некоторых случаях необходимо вручную настраивать параметры согласования, например, если интерфейсы Gigabit Ethernet, работающие в режиме автосогласования, подключены через сетевой кабель 100 Мбит/с. В таких случаях реализовать согласование между интерфейсами не удастся.

Некоторые модели коммутаторов HUAWEI могут не поддерживать смену дуплексного режима порта, см. Руководство по продукту.

Проверка базовой конфигурации




```
[SWA]display interface GigabitEthernet 0/0/1
GigabitEthernet0/0/1 current state : UP
Line protocol current state : UP
……
Speed :  100,  Loopback: NONE
Duplex: FULL,  Negotiation: DISABLE
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

В автоматическом режиме согласования значения конфигурационных параметров могут измениться, поэтому необходимо проверить определенные параметры с помощью команды display interface <interface>, чтобы убедиться в том, что данные параметры обеспечивают успешное согласование интерфейса канального уровня. В результатах выполнения команды параметр Line protocol current state (текущее состояние протокола линии) должен иметь значение UP. Выведенная информация отражает текущие настройки параметров интерфейса.

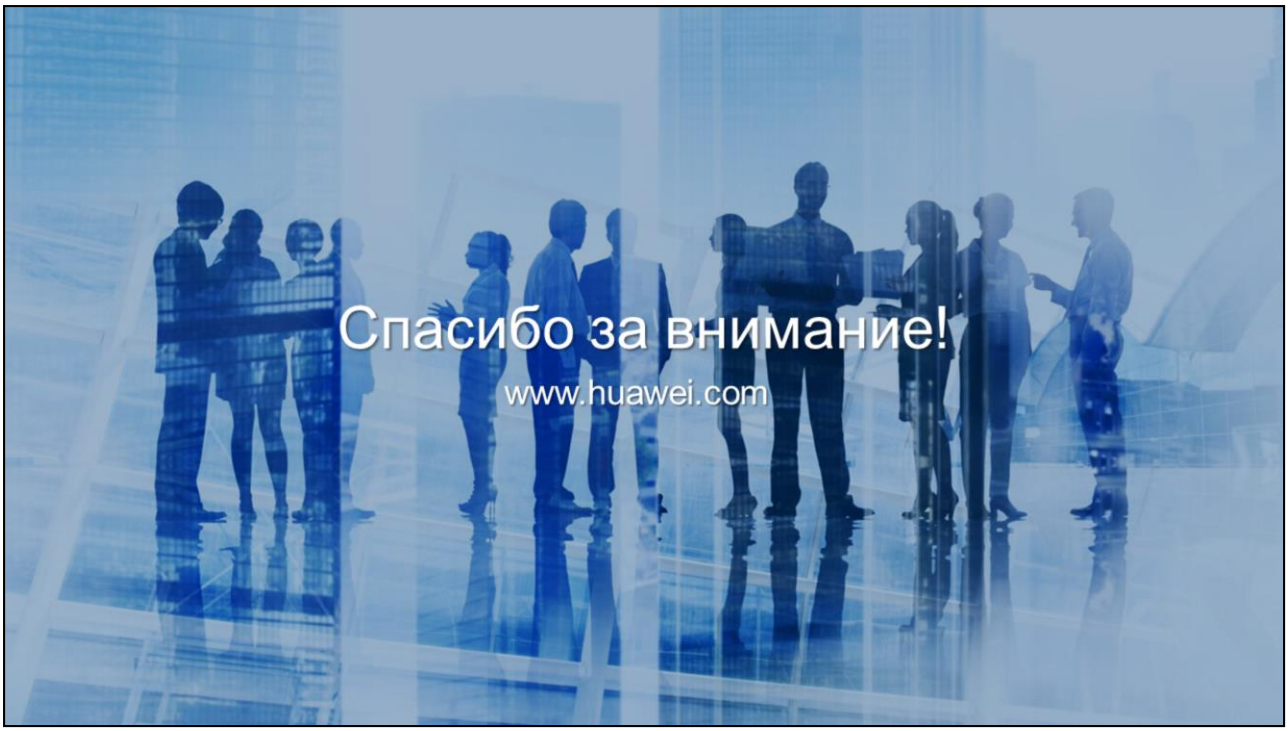
Заключение

- Какое действие выполнит коммутатор, если после записи исходного MAC-адреса хоста на интерфейсе порта физическое соединение хоста изменится на другой интерфейс порта коммутатора?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

При подключении хоста или другой оконечной системы к интерфейсу порта коммутатора генерируется самообращенный ARP, который предназначен для проверки уникальности IP-адреса в сетевом сегменте. Кроме того, самообращенный ARP предоставляет коммутатору информацию о MAC-адресе хоста, который затем включается в таблицу MAC-адресов и ассоциируется с интерфейсом порта, к которому подключен хост.

Если физическое соединение хоста, подключенного к интерфейсу порта коммутатора, будет удалено, коммутатор обнаружит, что физический канал не работает, и удалит MAC-адрес из таблицы MAC-адресов. При подключении носителя данных к другому интерфейсу порт обнаружит активность физического канала, и хост сгенерирует самообращенный ARP, что позволит коммутатору определить и записать в таблицу MAC-адрес подключенного хоста.


Спасибо за внимание!
www.huawei.com

Протокол связующего дерева (STP)

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

По мере расширения корпоративной сети появляются сети с несколькими коммутаторами (многокомпонентные сети), которые обеспечивают связь на канальном уровне между растущим числом оконечных систем. По мере формирования новых соединений между несколькими корпоративными коммутаторами появляются новые возможности для создания надежных сетей, однако вероятность сбоя переключения в результате возникновения петель становится все более высокой. Поэтому необходимо понимать, как работает протокол связующего дерева (STP) при предотвращении образования коммутационных петель и как его можно использовать для соответствия проектированию и производительности корпоративной сети.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

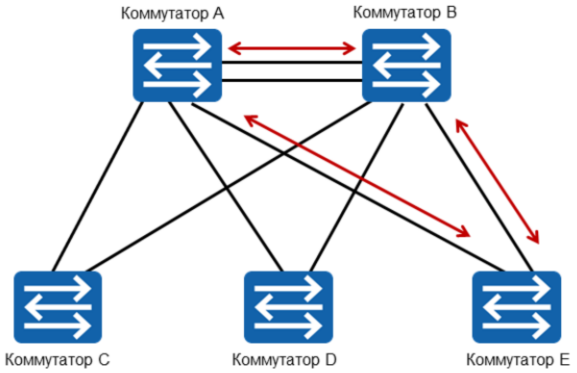
Цели

По окончании этого модуля слушатели смогут:

- Описать проблемы, возникающие при использовании сети с несколькими коммутаторами.
- Объяснить процесс предотвращения образования петель.
- Сконфигурировать параметры управления сетью STP.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Резервирование 2 уровня



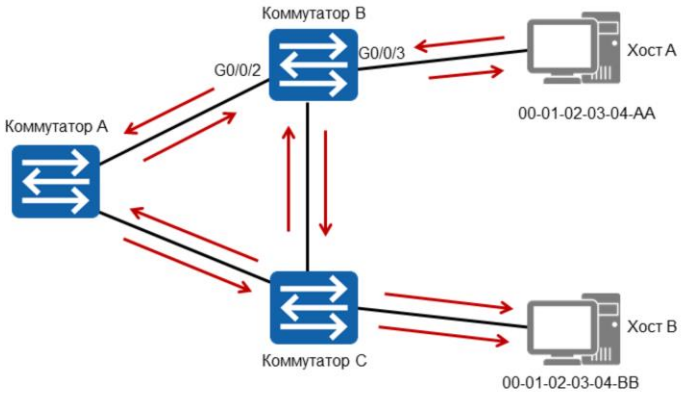
- Резервирование в коммутационной сети сводит к минимуму сбои соединения, но генерирует потенциальные коммутационные петли.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

В результате роста и расширения предприятий возникла потребность в использовании нескольких коммутаторов для обеспечения взаимодействия оконечных систем и служб, необходимых для повседневной работы. Однако соединение нескольких коммутаторов создает дополнительные проблемы. Между коммутаторами можно установить отдельные двухточечные каналы связи, по которым оконечные системы могут пересылать кадры на узлы назначения, обнаруженные другими коммутаторами в широковещательном домене. Однако отказ любого такого канала приводит к немедленной изоляции нижестоящего коммутатора и всех оконечных систем, к которым подключен канал. Для решения данной проблемы рекомендуется обеспечить резервирование каналов в коммутационной сети.

Резервные каналы используются в сети коммутации Ethernet для резервирования каналов и повышения надежности сети. Однако использование резервных каналов может привести к возникновению петель, что, в свою очередь, приводит к резкому ухудшению качества связи и возникновению серьезных перебоев в работе сети.

Широковещательные штормы



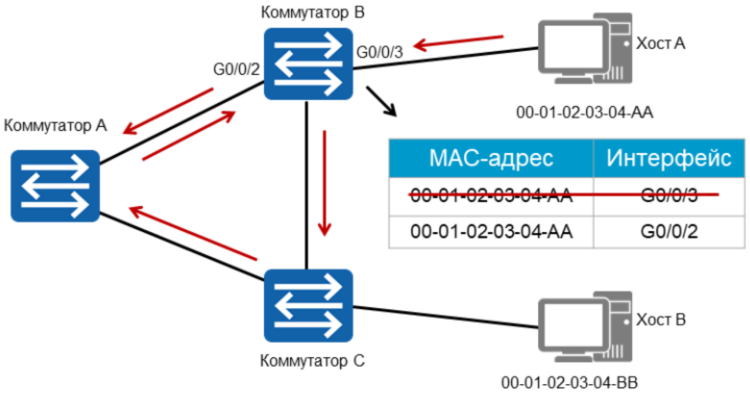
- Коммутационные петли приводят к возникновению широковещательных штормов и получению оконечными станциями дублированных кадров.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Одним из начальных эффектов избыточных коммутационных петель является передача широковещательных штормов. Это происходит, когда оконечная система пытается обнаружить пункт назначения, о котором не знают ни сама система, ни коммутаторы на пути переключения. Следовательно, широковещательная передача генерируется оконечной системой, которая подвергается лавинной рассылке от принимающего коммутатора.

Эффект лавинной рассылки означает, что кадр передается через все интерфейсы, за исключением интерфейса, по которому кадр был получен. В этом примере хост A генерирует кадр, который принимает коммутатор B, который впоследствии пересылается по всем другим интерфейсам. Подключенные коммутаторы A и C принимают экземпляр кадра, и лавинно рассылают кадр по всем другим интерфейсам. Эффект непрерывной лавинной рассылки приводит к тому, что коммутаторы A и C лавинно рассылают экземпляры кадра от одного коммутатора к другому, которые затем возвращаются на коммутатор B, и, таким образом, цикл продолжается. Повторяющийся эффект лавинной рассылки приводит к тому, что оконечные станции принимают множество экземпляров кадра, что вызывает прерывания и резкое снижение производительности коммутатора.

Нестабильность MAC-адресов



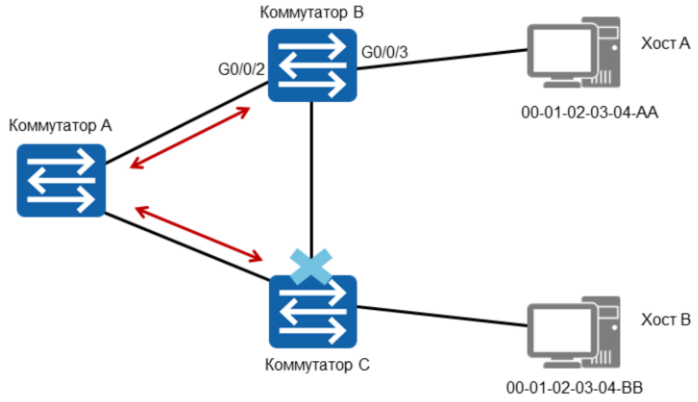
- Получение ранее переадресованных кадров генерирует ложные MAC-записи и нестабильность в таблице MAC-адресов.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Коммутаторы должны вести записи пути, по которым пункт назначения является доступным. Это можно идентифицировать с помощью ассоциации MAC-адреса источника, указанного в кадре, с интерфейсом, по которому был получен кадр. Только один экземпляр MAC-адреса может быть сохранен в таблице MAC-адресов коммутатора, и в случае приема второго экземпляра MAC-адреса приоритетной будет считаться более свежая информация.

В этом примере коммутатор B обновляет таблицу MAC-адресов информацией о MAC-адресе хоста A и связывает этот источник с интерфейсом G0/0/3, — интерфейсом порта, по которому был получен кадр. Поскольку в коммутируемой сети происходит неуправляемая лавинная рассылка кадров, выполняется повторный прием кадра с тем же MAC-адресом источника, что и у хоста A, однако на этот раз прием кадра осуществляется по интерфейсу G0/0/2. Поэтому коммутатор B должен сделать вывод, что хост, который был первоначально доступен по интерфейсу G0/0/3, теперь доступен по G0/0/2, и будет соответственно обновлять таблицу MAC-адресов. Результат этого процесса приводит к нестабильности MAC-адресов и продолжает происходить бесконечное число раз между интерфейсами портов коммутатора, соединяющими коммутатор A и коммутатор C, поскольку происходит лавинная рассылка кадров в обоих направлениях как часть эффекта широковещательного шторма.

Решение проблем резервирования 2 уровня



- Петли устраняются за счет ограничения потока трафика по резервным путям.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Задача коммутационной сети заключается в способности поддерживать резервирование с переключением, чтобы избежать изоляции оконечных систем в случае сбоя системы коммутации или канала, и в способности не допускать разрушительного воздействия коммутационных петель в топологии коммутации, которая реализует избыточность. В результате многолетних разработок было реализовано решение протокола связующего дерева (STP), позволяющее предотвратить влияние коммутационных петель. Связующее дерево работает по принципу, согласно которому резервные (избыточные) каналы должны быть логически отключены, чтобы гарантировать топологию без петель, а вторичные каналы должны включаться динамически в случае отказа первичного тракта коммутации, тем самым удовлетворяя требование резервирования сети в рамках топологии, свободной от петель. Коммутаторы, на которых работает STP, в процессе обмена информацией друг с другом обнаруживают петли в сети и блокируют определенные интерфейсы для отключения петель. STP продолжает оставаться важным протоколом для локальных сетей уже более 20 лет.

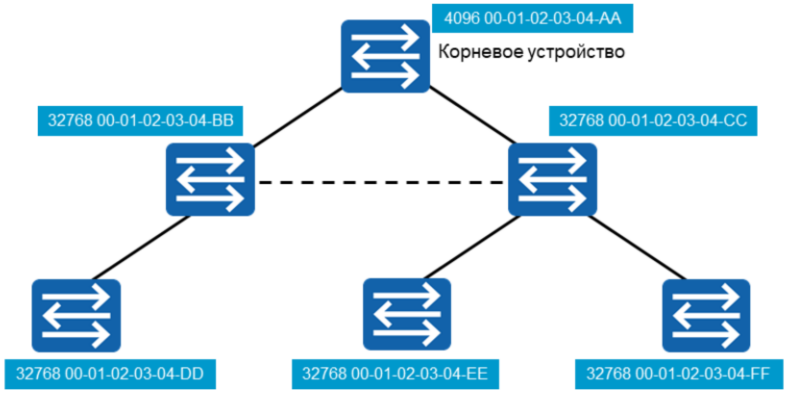
Корневой мост связующего дерева

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

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Удаление любой потенциальной возможности возникновения петель служит основной целью связующего дерева, для которого сформирована инвертированная древовидная архитектура. В основе этого логического дерева лежит корневой мост/коммутатор. Корневой мост представляет собой логический центр, но не обязательно физический центр сети с поддержкой STP. Выделенный корневой мост способен динамически изменяться в зависимости от топологии сети, как в случае, когда существующий корневой мост не может продолжать работать в качестве корневого моста. Некорневые мосты считаются нижестоящими по отношению к корневому мосту, и связь с некорневыми мостами осуществляется в направлении от корневого ко всем некорневым мостам. В любой фиксированный момент времени в конвергентной сети с поддержкой STP может существовать только один корневой мост.

Идентификатор моста



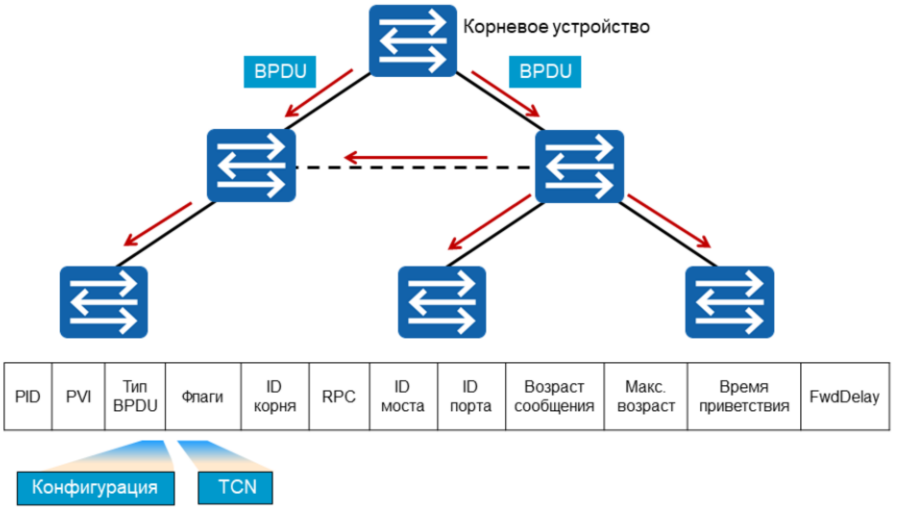
- Для выбора корневого моста используются идентификаторы моста.
- Приоритет моста можно изменять для принудительного выбора корня.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Обнаружение корневого моста для сети STP является основной задачей, выполняемой для формирования связующего дерева. Протокол STP работает на основе выборов, посредством которых определяется роль всех коммутаторов. Идентификатор моста является средством обнаружения корневого моста. Он состоит из двух частей: первая – это 16-битный приоритет моста, а вторая – 48-битный MAC-адрес.

Устройство, которое содержит самый высокий приоритет (наименьший идентификатор моста), выбирается в качестве корневого моста для сети. При сравнении идентификаторов мостов первоначально учитывается приоритет моста, а там, где значение приоритета не может однозначно идентифицировать корневой мост, в качестве прерывателя связи используется MAC-адрес. Идентификатором моста можно управлять путем изменения приоритета как средства для выбора данного коммутатора в качестве корневого моста, часто в поддержку оптимизированной сети.

Блок данных протокола моста



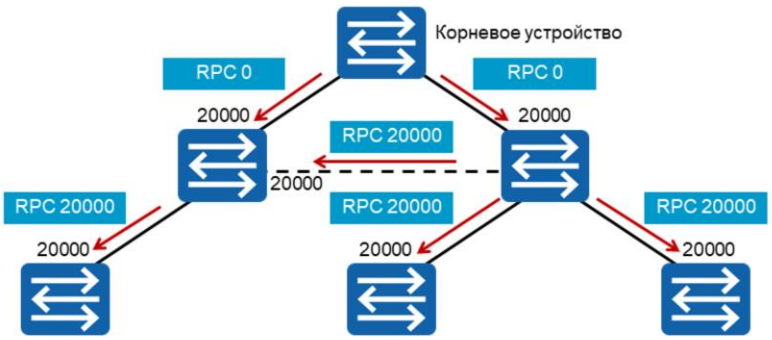
 Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Топология связующего дерева основана на передаче конкретной информации для определения роли и статуса каждого коммутатора в сети. Блок данных протокола моста (BPDU) упрощает связь в сети связующего дерева. В STP используются два типа кадров BPDU. Конфигурационный (Configuration) BPDU изначально создается корневым узлом и распространяется в нисходящем направлении, чтобы гарантировать, что все некорневые мосты осведомлены о состоянии топологии связующего дерева и, что важно, корневого моста. BPDU TCN является вторым типом BPDU, который распространяет информацию об изменении топологии в восходящем направлении к корневому узлу.

Блоки данных протокола моста непосредственно не передаются коммутаторами, вместо этого информация, которая передается в BPDU, часто используется для генерирования собственного BPDU коммутатора. Конфигурационный BPDU передает ряд параметров, которые используются мостом, чтобы сначала определить наличие корневого моста и гарантировать, что этот корневой мост имеет наивысший приоритет. Считается, что каждый сегмент LAN имеет назначенный коммутатор, который отвечает за распространение BPDU в нисходящем направлении на неназначенные коммутаторы.

Поле идентификатора моста используется для определения текущего назначенного коммутатора, от которого ожидается получение BPDU. BPDU генерируется и пересылается корневым мостом на основе таймера Hello, который по умолчанию равен 2 секундам. Поскольку BPDU принимаются нижестоящими коммутаторами, новый BPDU генерируется с параметрами, определенными локально, и отправляется всем неназначенным коммутаторам сегмента LAN.

Стоимость пути



- Стоимость корневого пути переносится в BPDU и используется для определения кратчайшего пути к корневому каталогу.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Еще одна особенность BPDU – распространение двух параметров, связанных со стоимостью пути. Стоимость корневого пути (RPC) используется для измерения стоимости пути к корневому мосту с целью определения кратчайшего пути связующего дерева и, таким образом, создания топологии без петель. Когда мост является корневым мостом, стоимость корневого пути равна 0.

Стоимость пути (PC) – это значение, связанное с корневым портом, являющимся портом нижестоящего коммутатора, который подключается к сегменту LAN, в котором находится назначенный коммутатор или корневой мост. Значение используется для генерирования стоимости корневого пути для коммутатора путем добавления стоимости пути к значению RPC, полученному от назначенного коммутатора в сегменте LAN, для того чтобы определить новое значение стоимости корневого пути. Это новое значение стоимости корневого пути передается в BPDU назначенного коммутатора и используется для предоставления стоимости пути корневому узлу.

Стандарты стоимости пути

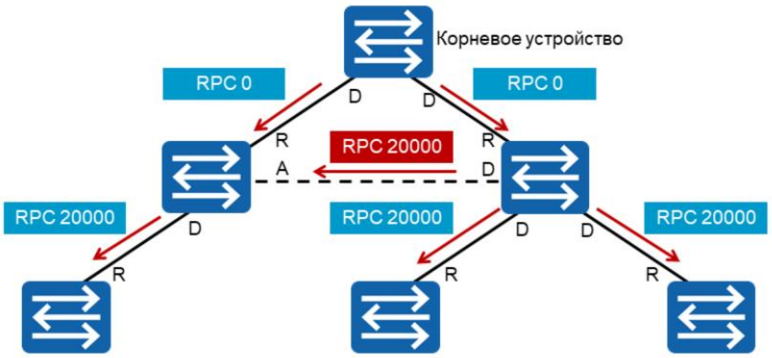
Скорость порта	802.1D	802.1t	Значение стоимости пути
10 Мбит/с	99	1999999	1999
100 Мбит/с	18	199999	199
1 Гбит/с	4	20000	20
10 Гбит/с	2	2000	2

- STP поддерживает различные стандарты стоимости пути.
- 802.1t – стандарт по умолчанию, используемый в коммутаторах Huawei.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Коммутаторы серии Sx7 Huawei поддерживают ряд альтернативных стандартов стоимости пути, которые могут быть реализованы на основе требований предприятия, например, в тех случаях, когда используется мультивендорная сеть. Коммутаторы серии Sx7 Huawei используют стандартную стоимость пути 802.1t по умолчанию, обеспечивая более высокую метрическую точность для расчета стоимости пути.

Роли порта связующего дерева



- Связующее дерево поддерживает следующие роли порта: назначенный, корневой и альтернативный.
- Стоимость корневого пути позволяет определить роли порта.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

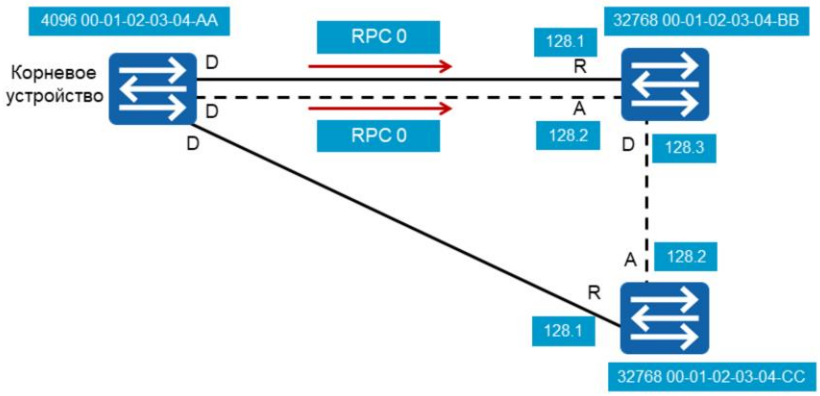
Сеть связующего дерева определяет роли порта. Роли портов используются для определения поведения интерфейсов, задействованных в активной топологии связующего дерева. Для протокола связующего дерева определены три роли порта: назначенный, корневой и альтернативный.

Назначенный порт связан с корневым мостом или назначенным мостом сегмента LAN и определяет нисходящий путь, по которому пересылаются Конфигурационные BPDU. Корневой мост отвечает за генерирование конфигурационных BPDU для всех нижестоящих коммутаторов, и поэтому интерфейсы портов корневого моста всегда принимают роль назначенного порта.

Корневой порт идентифицирует порт, который предлагает путь к корневому каталогу с наименьшей стоимостью. Данный пример демонстрирует ситуацию, когда к корневому устройству имеется два возможных обратных пути, однако в качестве корневого порта назначается только тот порт, который предлагает самую низкую стоимость корневого пути. Если два или более портов предлагают одинаковую стоимость корневого пути, решение о том, какой интерфейс порта будет выбран в качестве корневого, определяется путем сравнения идентификатора моста в конфигурационном BPDU, который получает каждый порт.

Любой порт, которому не присвоена роль назначенного или корневого порта, считается альтернативным портом и может принимать BPDU от назначенного коммутатора для сегмента LAN с целью мониторинга состояния резервного канала, но обрабатывать полученный BPDU не будет. Первоначально данная роль была определена в стандарте IEEE 802.1D-1990 для STP как роль резервного порта, однако в процессе пересмотра стандартов IEEE 802.1D-1998 она была изменена на роль альтернативного порта.

Идентификатор порта



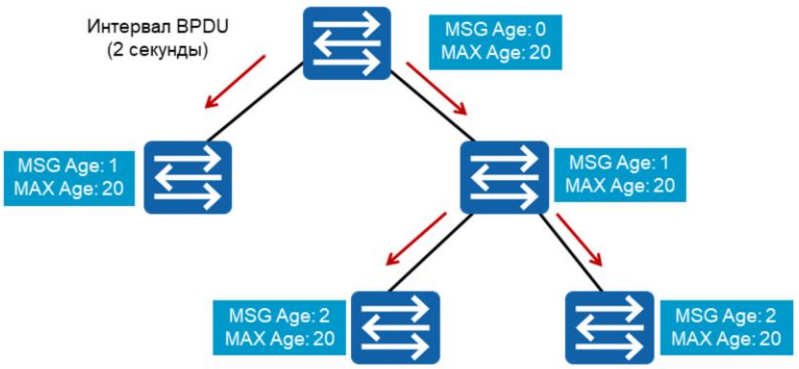
- Если стоимости корневого пути равны, идентификатор порта используется для определения активного и альтернативного путей к корню.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Идентификатор порта представляет собой окончательное средство для определения ролей порта наряду с идентификатором моста и механизмом стоимости корневого пути. В сценариях, где два или более порта предлагают одинаковую стоимость корневого пути обратно к корневому узлу, и в которых вышестоящий коммутатор и мост имеют одинаковые идентификаторы, главным образом из-за того, что вышестоящий коммутатор также является коммутатором для обоих путей, для определения ролей порта должен применяться ID порта.

Идентификатор порта привязан к каждому порту и содержит приоритет и номер порта, который связан с интерфейсом порта. Приоритет порта – это значение в диапазоне от 0 до 240, присваиваемое с шагом 16 и представленное значением 128 по умолчанию. Если оба интерфейса портов имеют одинаковое значение приоритета порта, то для определения роли порта используется уникальный номер порта. Самый высокий идентификатор порта (самый низкий номер порта) представляет порт, назначенный в качестве корневого порта, а для оставшегося порта по умолчанию используется роль альтернативного порта.

Таймеры



- MAX Age (макс. возраст) представляет собой таймер старения BPDU.
- BPDU отбрасывается, когда Message Age превышает MAX Age.

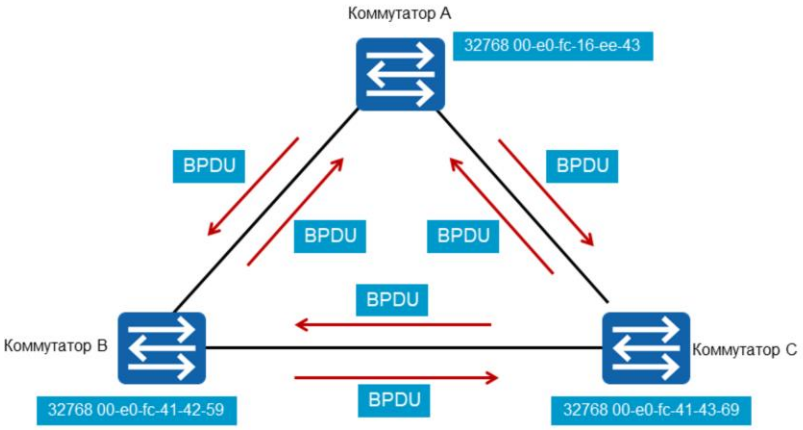
Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Корневой мост отвечает за генерирование конфигурационных BPDU на основе интервала BPDU, который определяется таймером Hello. Таймер Hello по умолчанию имеет значение 2 секунды. Конвергентная сеть связующего дерева должна гарантировать, что в случае сбоя сети коммутаторы в сети с поддержкой STP будут осведомлены о сбое. Таймер Max Age связан с каждым BDPU и описывает жизненный цикл BPDU с точки зрения корневого моста и в конечном итоге контролирует срок действия BDPU, прежде чем он будет считаться устаревшим. Таймер MAX Age по умолчанию имеет значение 20 секунд.

После получения конфигурационного BPDU от корневого моста, считается, что нижестоящему коммутатору требуется приблизительно 1 секунда для генерирования нового BPDU и передачи сгенерированного BPDU в нисходящем направлении. Чтобы компенсировать это время, значение MSG Age применяется к каждому BPDU, чтобы показать смещение между MAX Age и задержкой распространения, и для каждого коммутатора это значение увеличивается на 1.

Когда BPDU распространяется от корневого моста к нижестоящим коммутаторам, таймер MAX Age обновляется. Таймер MAX Age начинает обратный отсчет и истекает, когда значение MAX Age превышает значение возраста сообщения, чтобы гарантировать, что время жизни BPDU ограничено значением MAX Age, определенным корневым мостом. В случае, если BPDU не получен до истечения таймера MAX Age, коммутатор будет рассматривать информацию BPDU как устаревшую на данный момент и сделает вывод, что в сети STP произошел сбой.

Процесс выбора корневого устройства



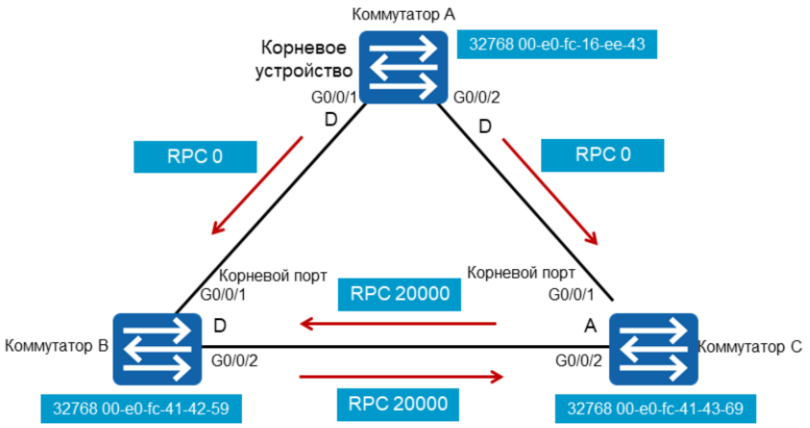
- Все коммутаторы STP анонсируют BDPU на одноранговые узлы, в которых они сами указаны как корневые устройства.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Процесс схождения (конвергенции) связующего дерева – это автоматизированная процедура, которая запускается в момент запуска коммутатора. Все коммутаторы при запуске принимают на себя роль корневого моста в сети коммутации. Поведение корневого моста по умолчанию заключается в присвоении роли назначенного порта всем интерфейсам портов, чтобы включить пересылку BPDU через все подключенные интерфейсы портов. Поскольку BPDU принимают одноранговые коммутаторы, то появляется необходимость сравнить идентификаторы моста, чтобы определить наилучшего кандидата на роль корневого моста. В случае, если полученный BPDU содержит идентификатор моста нижестоящего по отношению к корневому устройству, принимающий коммутатор продолжит анонсировать собственный конфигурационный BPDU на соседний коммутатор.

Если BDPU содержит идентификатор вышестоящего устройства, то коммутатор признает наличие лучшего кандидата на роль корневого моста, и прекращает распространять BPDU в направлении, по которому был получен BPDU с ID вышестоящего устройства. Коммутатор также изменит поле root ID в своем BPDU, чтобы анонсировать идентификатор моста кандидата на корневой мост в качестве текущего нового корневого моста.

Процесс создания роли порта



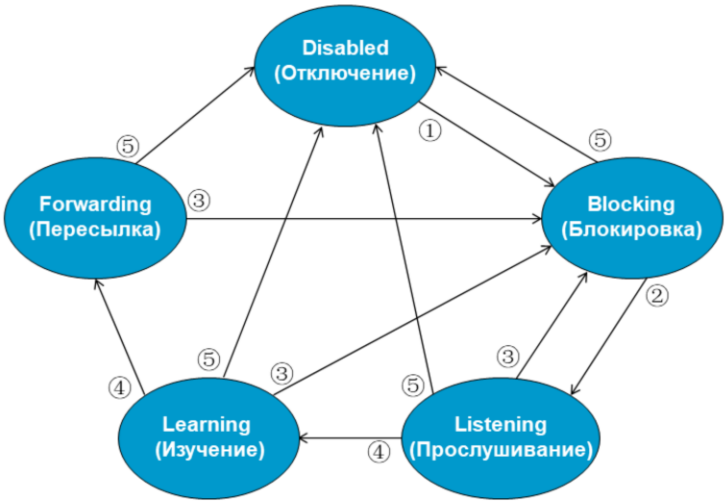
- Для выбора ролей порта используются ID моста и стоимость корневого пути.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Выбранный корневой мост генерирует конфигурационный BPDU для других некорневых коммутаторов. BPDU содержит стоимость корневого пути, которая будет сообщена нисходящим коммутаторам для определения кратчайшего пути. Стоимость корневого пути, переносимая в BPDU, который генерируется корневым мостом, всегда имеет значение 0. Затем получающие нижестоящие коммутаторы добавят эту стоимость к стоимости пути интерфейсов портов, на которых был получен BPDU, и с которых коммутатор может идентифицировать корневой порт.

В случае, если в двух или более сегментах локальной сети существует один и тот же восходящий коммутатор, для определения ролей порта используется одинаковая стоимость корневого пути. Если между двумя коммутаторами существует равная стоимость корневого пути, как в данном примере, идентификатор моста используется для определения того, какой коммутатор представляет собой назначенный коммутатор для сегмента LAN. Если порт коммутатора не является ни корневым портом, ни назначенным портом, порту назначается роль альтернативного порта.

Смена состояний порта



 Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

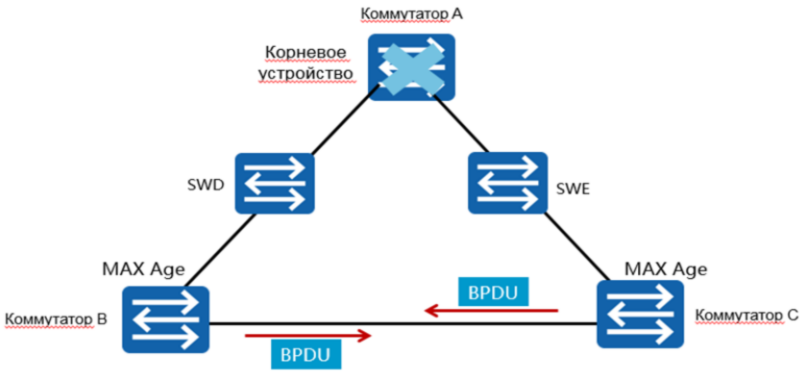
В качестве элемента корневого моста и при определении роли порта каждый коммутатор проходит через несколько состояний. Любой порт, который отключен администратором, будет считаться отключенным. Включение порта в отключенном состоянии приведет к переходу в состояние блокировки ①.

Порт в состоянии блокировки не может пересылать пользовательский трафик, но может принимать кадры BPDU. Любой BPDU, полученный по интерфейсу порта в состоянии блокировки, не будет использоваться для заполнения таблицы MAC-адресов коммутатора, но будет использоваться, чтобы определить необходимость перехода в состояние прослушивания. Состояние прослушивания позволяет передавать информацию BPDU после согласования роли порта в STP ②, но имеет ограничение на заполнение таблицы MAC-адресов информацией о соседних устройствах.

Переход в состояние блокировки из состояния прослушивания или других состояний может произойти в том случае, если роль порта изменится на роль альтернативного порта. Переход из состояния прослушивания к состоянию изучения и от состояния изучения к состоянию пересылки в значительной степени зависит от таймера forward delay, который должен гарантировать, что любое распространение информации BDPU на все коммутаторы в топологии связующего дерева возможно до того, как произойдет переход между состояниями.

Состояние изучения поддерживает ограничение пересылки пользовательского трафика, чтобы гарантировать предотвращение образования любых коммутационных петель, но допускает заполнение таблицы MAC-адресов по всей топологии связующего дерева для обеспечения стабильной работы сети коммутации. После периода forward delay происходит переход в состояние пересылки. Состояние отключения применимо в любое время в течение периода перехода между состояниями с помощью ручного вмешательства (т. е. команды shutdown) ⑤.

Сбой корневого устройства



- Перед тем, как признать потерю корневого устройства, некорневые мосты ждут сообщение MAX Age.
- Затем запускается повторная сходимость (конвергенция), которая начинается с выбора корневого устройства.

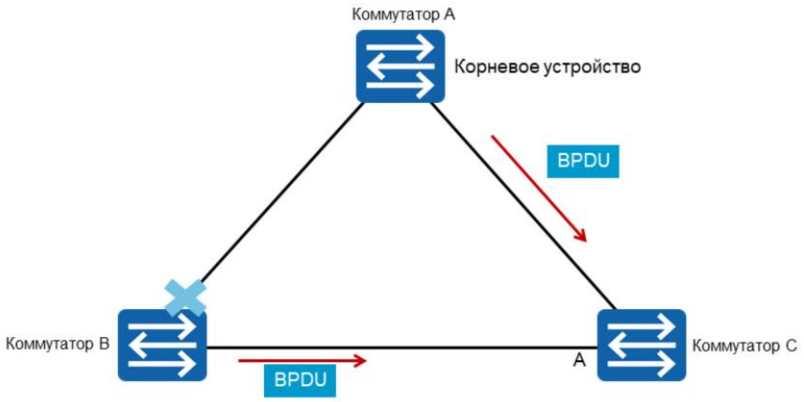
Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

HUAWEI

События, которые вызывают изменение установленной топологии связующего дерева, могут происходить различными способами, на которые протокол связующего дерева должен реагировать, чтобы быстро восстановить стабильную и свободную от петель топологию. Сбой корневого моста — это основной пример того случая, где необходима повторная сходимость (конвергенция). Некорневые коммутаторы используют прерывистый импульс BPDU от корневого моста, чтобы поддерживать свои индивидуальные роли в качестве некорневых коммутаторов в топологии STP. В случае отказа корневого моста нижестоящие коммутаторы не смогут получить BPDU от корневого моста и, следовательно, также прекратят распространение BPDU в нисходящем направлении. Таймер MAX Age обычно сбрасывается до установленного значения (по умолчанию 20 секунд) после получения каждого BPDU в нисходящем направлении.

В случае потери BPDU таймер MAX Age начинает отсчитывать время жизни текущей информации BPDU каждого некорневого коммутатора на основе формулы (MAX Age – MSG Age). В тот момент, когда значение MSG Age больше значения таймера MAX Age, информация BPDU, полученная от корневого устройства, становится недействительной, и некорневые коммутаторы начинают выполнять роль корневого моста. Конфигурационные BPDU снова перенаправляются из всех активных интерфейсов в попытке обнаружить новый корневой мост. Сбой корневого моста приводит к продолжительности восстановления приблизительно 50 секунд из-за периода сходимости (конвергенции) Max Age + 2x Forward Delay.

Сбой непрямого канала



- Коммутатор B запускает выбор корневого устройства, но коммутатор C игнорирует BPDU.
- Корневой BDPU передается на коммутатор B после истечения периода MAX Age.

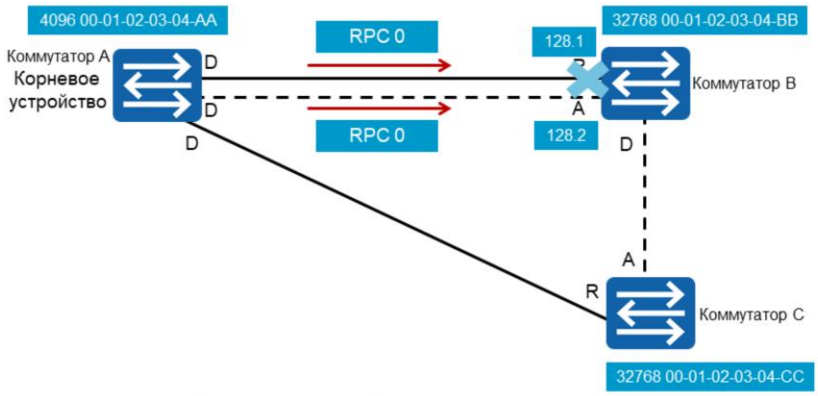
Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

В случае сбоя непрямого канала коммутатор теряет соединение с корневым мостом из-за сбоя порта или носителя или из-за ручного отключения интерфейса, выполняющего роль корневого порта. Коммутатор узнает о сбое, и, поскольку он получает BPDU только от корневого узла в одном направлении, он сразу же теряет корневой мост и занимает положение нового корневого моста.

В этом примере коммутатор B начинает пересылать BPDU на коммутатор C, чтобы уведомить о положении коммутатора B как нового корневого моста, однако коммутатор C продолжает получать BPDU от исходного корневого моста и поэтому игнорирует любой BPDU от коммутатора B. Начинается старение состояния альтернативного порта по таймеру MAX Age, так как интерфейс больше не получает BPDU, содержащий корневой идентификатор корневого моста.

По истечении таймера MAX Age коммутатор C изменяет роль альтернативного порта на роль назначенного порта и переходит к пересылке BPDU от корневого устройства к коммутатору B. В результате коммутатор признает себя как корневое устройство и переводит интерфейс порта в роль корневого порта. Это является частичным сбоем, но из-за необходимости ожидания периода, эквивалентного MAX Age + 2x forward delay, для полного восстановления топологии STP требуется приблизительно 50 секунд.

Сбой прямого канала



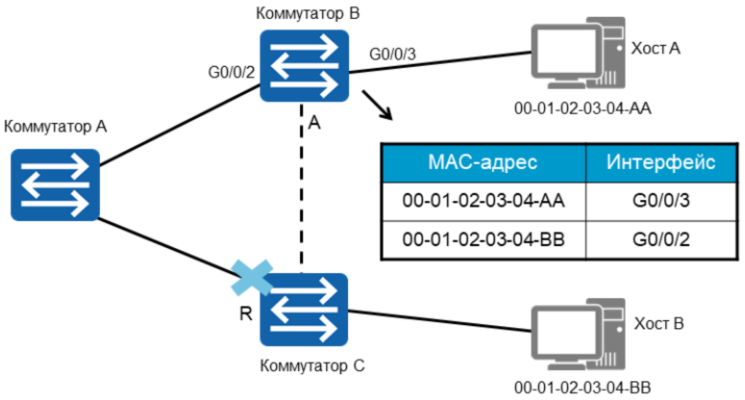
- Коммутатор B обнаруживает сбой и переключает альтернативный порт на корневой порт.
- STP преобразуется после 2-кратной задержки (по умолчанию 30 секунд).

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Окончательный сценарий, включающий восстановление конвергенции связующего дерева, происходит, когда несколько сегментов LAN подключены между двумя коммутаторами, один из которых в данный момент является активным каналом, а другой обеспечивает альтернативный путь к корневому устройству. В случае возникновения события, которое приводит к тому, что коммутатор, который получает BPDU, обнаруживает потерю соединения на своем корневом порту, например, в случае сбоя корневого порта или сбоя канала, о чем незамедлительно узнает нижестоящий коммутатор, коммутатор может мгновенно перейти на альтернативный порт.

Переход выполняется через состояния прослушивания, изучения и пересылки и обеспечивает восстановление в течение периода 2x forward delay. В случае любого сбоя, когда активируется канал, обеспечивающий наилучший путь, топология связующего дерева должна быть преобразована для применения оптимальной топологии связующего дерева.

Нестабильность MAC-адресов при изменении топологии



- Изменения в топологии STP могут аннулировать записи таблиц MAC-адресов.
- Срок действия записей таблицы MAC-адресов по умолчанию истекает только через 300 секунд.

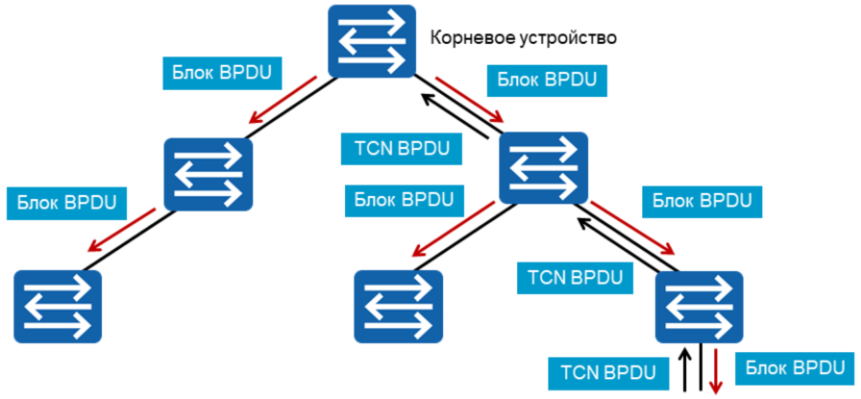
Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

В конвергентной сети связующего дерева коммутаторы поддерживают базы данных фильтров или таблицы MAC-адресов для управления распространением кадров по топологии связующего дерева. Записи, которые обеспечивают связь между MAC-адресатом и интерфейсом порта пересылки, сохраняются в течение ограниченного периода времени – 300 секунд (5 минут) по умолчанию. Изменение топологии связующего дерева означает, что любые существующие записи таблицы MAC-адресов, вероятно, станут недействительными из-за изменения тракта коммутации и, следовательно, должны быть обновлены.

В этом примере показана существующая топология связующего дерева, для которой коммутатор B имеет записи, позволяющие получить доступ к хосту A через интерфейс Gigabit Ethernet 0/0/3 и хосту B через интерфейс Gigabit Ethernet 0/0/2. На коммутаторе C смоделирован сбой, при котором текущий корневой порт становится неактивным. Этот сбой вызывает перерасчет топологии связующего дерева и активирует избыточную линию связи между коммутатором C и коммутатором B.

Однако, после повторной конвергенции обнаруживается, что кадры между хостами A и B не достигают пункта назначения. Поскольку записи таблицы MAC-адресов еще не истекли по правилу 300 секунд, кадры, достигающие коммутатора B, предназначенные для хоста B, продолжают передаваться через интерфейс порта Gigabit Ethernet 0/0/2 и фактически становятся «черными дырами», поскольку кадры пересылаются на неактивный интерфейс порта коммутатора C.

Процесс изменения топологии



- Уведомление об изменении топологии информирует корневой мост об изменении топологии.
- Корневое устройство сбрасывает MAC-записи с BPDU с набором битов TC.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

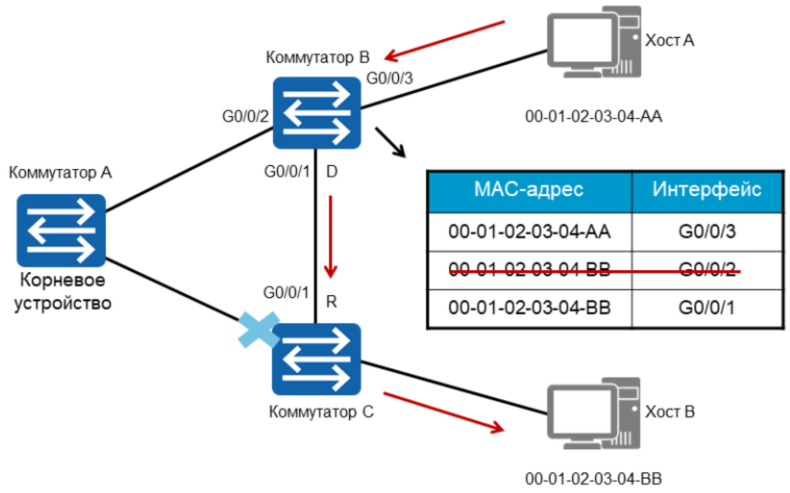
Для решения проблемы таймаута для записей таблицы MAC-адресов, который приводит к сохранению записей о недействительных маршрутах после конвергенции связующего дерева, необходим дополнительный механизм. Реализованный процесс называется процессом уведомления об изменении топологии (TCN) и представляет новую форму BPDU для работы протокола связующего дерева.

Этот новый BPDU называется BPDU TCN и отличается от конфигурационного BPDU настройками значения 128 (0x80) для типа BPDU. Функция BPDU TCN состоит в том, чтобы сообщать корневому мосту восходящего потока о любых изменениях в текущей топологии, тем самым позволяя корневому устройству отправлять уведомление в конфигурационном BPDU всем нижестоящим коммутаторам, чтобы сократить период таймаута для записей таблицы MAC-адресов до эквивалентного значения таймера forward delay или до 15 секунд по умолчанию.

Поле flags в конфигурационном BPDU содержит два поля Topology Change (TC) – Изменение топологии и Topology Change Acknowledgement (TCA) - Подтверждение изменения топологии. После получения BPDU TCN корневой мост генерирует BPDU с наборами битов TC и TCA, чтобы соответственно и уведомить об изменении топологии и проинформировать нижестоящие коммутаторы о том, что корневой мост принял BPDU TCN и, следовательно, передача TCN BPDU должна быть прекращена.

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

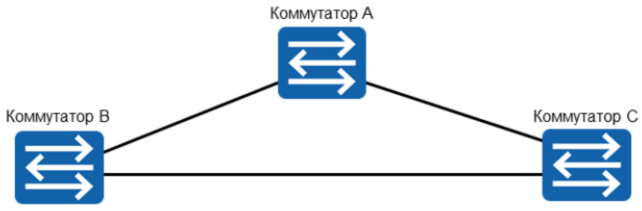
Обновление таблицы MAC-адресов при изменении топологии



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Влияние BPDU TCN на процесс изменения топологии гарантирует, что корневой мост будет уведомлен о любом сбое в топологии связующего дерева, для которого корневой мост может генерировать необходимые флаги для сброса записей текущей таблицы MAC-адресов на каждом коммутаторе. Данный пример демонстрирует результаты изменения топологии и влияния на таблицу MAC-адресов. Записи, относящиеся к коммутатору B, были сброшены, далее обнаружены обновленные записи, определяющие, что хост B теперь доступен через интерфейс порта Gigabit Ethernet 0/0/1.

Режимы STP

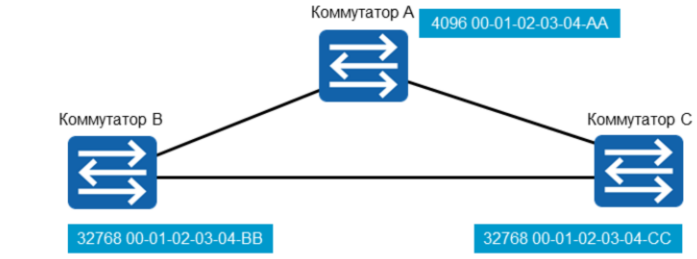



```
[SWA]stp mode ?
mstp  Multiple Spanning Tree Protocol (MSTP) mode
rstp  Rapid Spanning Tree Protocol (RSTP) mode
stp   Spanning Tree Protocol (STP) mode
[SWA]stp mode stp
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Коммутаторы серии Sx7 Huawei, к которым принадлежит модель S5700, способны поддерживать три формы протокола связующего дерева. С помощью команды stp mode пользователь может определить режим STP для отдельного коммутатора. По умолчанию режимом STP для коммутаторов серии Sx7 является MSTP, и поэтому перед использованием STP необходимо перенастроить режим.

Назначение корневого устройства



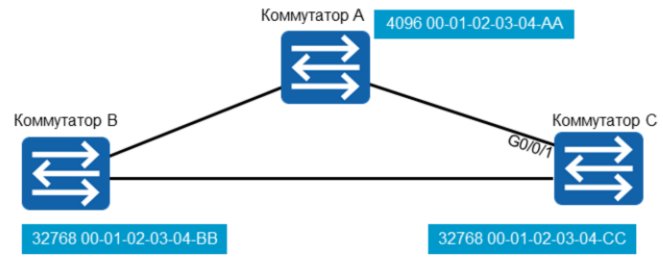

```
[SWA]stp priority 4096
Apr 15 2016 16:15:33-08:00 SWA DS/4/DATASYNC_CFGCHANGE:OID
1.3.6.1.4.1.2011.5.25.191.3.1 configurations have been
changed. The current change number is 4, the change loop
count is 0, and the maximum number of records is 4095.
```

- Корневое устройство можно установить вручную или установить коммутатор в качестве первичного.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

В рамках эффективной практики проектирования коммутаторов рекомендуется вручную определить корневой мост. Позиционирование корневого моста гарантирует, что оптимальный поток трафика в пределах корпоративной сети может быть достигнут путем конфигурирования значения приоритета моста для протокола связующего дерева. Команда stp priority [priority] используется для определения значения приоритета, где приоритет относится к целому значению от 0 до 61440, присваиваемому с шагом 4096. Это предоставляет в общей сложности 16 шагов со значением по умолчанию 32768. Также можно назначить корневой мост для связующего дерева с помощью команды stp root.

Назначение стоимости пути




```
[SWC]stp pathcost-standard ?
 dot1d-1998  IEEE 802.1D-1998
   dot1t       IEEE 802.1T
   legacy      Legacy
[SWC]interface GigabitEthernet 0/0/1
 [SWC-GigabitEthernet0/0/1]stp cost 2000
```

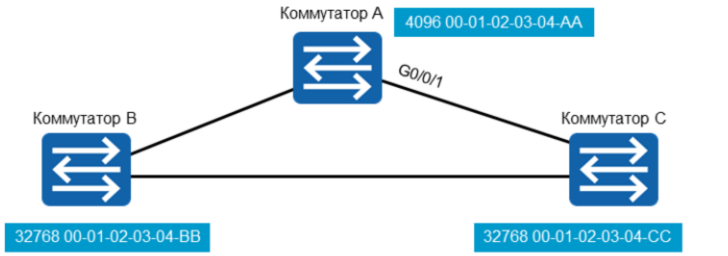

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Коммутаторы серии Huawei Sx7 поддерживают три формы стандарта стоимости пути, чтобы обеспечить совместимость там, где это необходимо, однако по умолчанию поддерживается стандарт стоимости пути 802.1t. Стандарт стоимости пути может быть скорректирован для данного коммутатора с помощью команды stp pathcost-standard {dot1d-1998 | dot1t | legacy}, где dot1d-1998, dot1t и legacy относятся к стандартам стоимости пути, описанным ранее в этом разделе.

Кроме того, стоимость пути для каждого интерфейса может быть назначена вручную для поддержки средств детализированного управления стоимостью пути stp. Этот метод управления стоимостью пути следует использовать с большой осторожностью, поскольку стандарты стоимости пути разработаны для реализации оптимальной топологии связующего дерева для данной сети коммутации, а управление стоимостью STP может привести к формированию нерациональной топологии связующего дерева.

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

Защита корневого устройства




```
[SWA]interface GigabitEthernet 0/0/1
[SWA-GigabitEthernet0/0/1]stp root-protection
```

- Защита корневого устройства предотвращает изменения в топологии в результате смены состояния корневого моста, вызванного получением BPDU более высокого приоритета.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Если корневой коммутатор в сети неправильно настроен или атакован, он может получать BPDU с более высоким приоритетом, и поэтому корневой коммутатор становится некорневым коммутатором, что приводит к изменению топологии сети. В результате трафик может быть переключен с высокоскоростных каналов на низкоскоростные, что приводит к перегрузке сети.

Для решения этой проблемы коммутатор предоставляет функцию root protection. Функция root protection (защита корня) защищает роль корневого коммутатора, сохраняя роль назначенного порта. Когда порт получает BPDU с более высоким приоритетом, порт останавливает переадресацию пакетов и переходит в состояние прослушивания, но сохраняет назначенную роль порта. Если порт не получает какой-либо BPDU с более высоким приоритетом в определенный период времени, статус порта восстанавливается из состояния прослушивания.

Сконфигурированная защита корня действительна только в том случае, если порт является назначенным портом и поддерживает эту роль. Если порт сконфигурирован как граничный порт или если на порте включена команда, известная как защита от петель (loop protection), функция root protection не может быть включена на порте.

Проверка 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 © 2019 Huawei Technologies Co., Ltd. Все права защищены.

С помощью команды display stp можно определить текущую конфигурацию STP. Существует несколько таймеров для управления конвергенцией связующего дерева, включая таймер Hello, max age timer и forward delay, для которых отображаемые значения представляют собой настройки таймера по умолчанию, и их рекомендуется поддерживать.

Для данного коммутатора текущий идентификатор моста может быть идентифицирован с помощью конфигурации моста CIST, которая включает идентификатор моста и MAC-адреса коммутатора. Статистические данные предоставляют информацию о том, как коммутатор отреагировал на изменения топологии, прежде всего через полученное значение TC или TCN вместе с последним вхождением, как это видно из значения времени последней записи TC.

Проверка 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
.....
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Для отдельных интерфейсов на коммутаторе эту информацию можно вывести на экран с помощью команды display stp для просмотра списка всех интерфейсов. Команда display stp interface <interface> позволяет определить конкретный интерфейс. Состояние интерфейса соответствует статусу порта MSTP и поэтому будет отображаться как Discarding, Learning или Forwarding. На экран выводится и другая действительная информация, например, роль порта, стоимость порта и любые применяемые механизмы защиты.

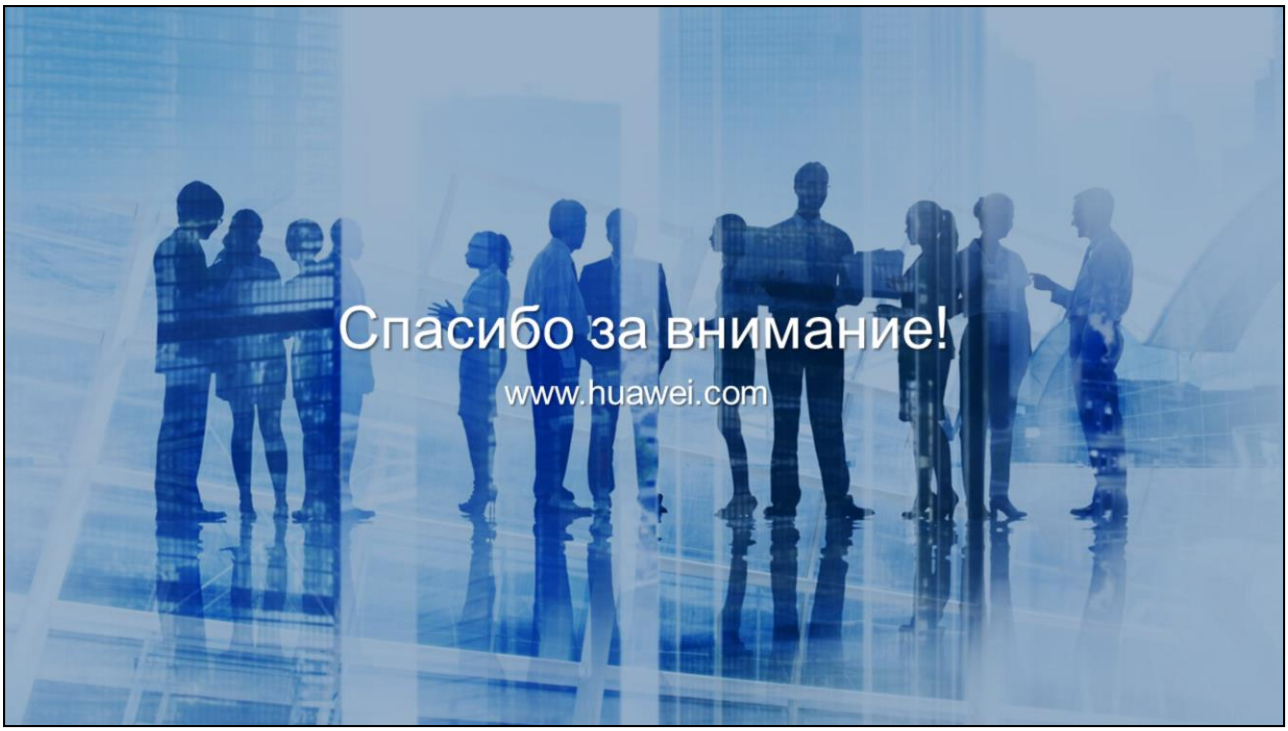
Заключение

- В случае, если корневой мост (коммутатор) временно выходит из строя в сети STP, следующий работоспособный коммутатор станет корневым мостом. Что произойдет, когда неисправный корневой мост снова станет активным в сети?
- В чем разница между стоимостью пути и стоимостью корневого пути?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

В случае отказа корневого моста в сети STP в качестве корневого моста выбирается следующий лучший кандидат. В случае, если исходный корневой мост снова становится активным, процесс выбора корневого моста повторяется. Это приводит к простоям в сети коммутации, когда выполняется конвергенция.

Стоимость корневого пути – это стоимость, связанная с путем к корневому мосту, тогда как стоимость пути – это значение стоимости, определенное для интерфейса на коммутаторе, которое добавляется к стоимости корневого пути, чтобы определить стоимость корневого пути для нижестоящего коммутатора.


Спасибо за внимание!
www.huawei.com

Протокол быстрого связующего дерева (RSTP)

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

Стандарт на протокол связующего дерева, разработанный в 1998 году, имеет ряд ограничений и недостатков, например, медленное время сходимости (конвергенции). Для преодоления отдельных ограничений протокола STP был разработан протокол быстрого связующего дерева – Rapid Spanning Tree (RSTP). Основные понятия и терминология протоколов STP и RSTP одинаковы. В данном документе рассматриваются основные существенные отличия.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

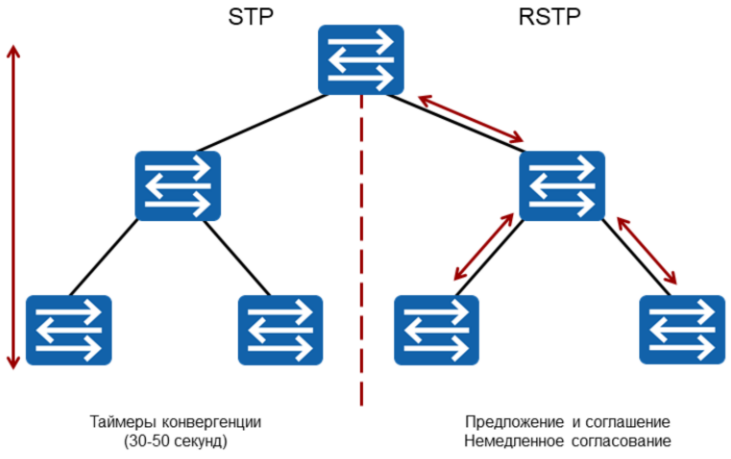
Цели

По окончании этого модуля слушатели смогут:

- Описать основные характеристики RSTP.
- Настроить параметры RSTP.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Недостатки STP

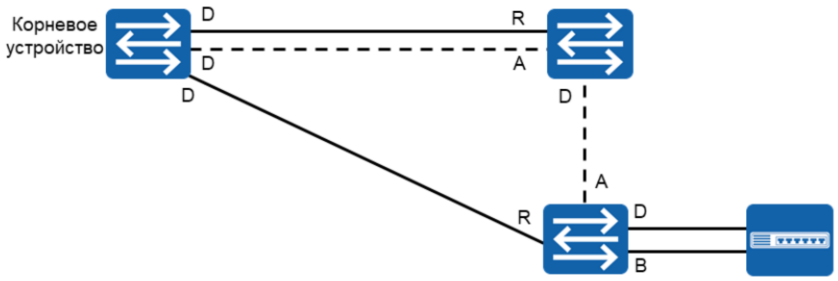


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

STP обеспечивает бесперебойную работу сети, свободной от петель, но имеет низкую скорость сходимости (конвергенции) топологии сети, что приводит к ухудшению качества услуг. Если топология сети часто меняется, соединения в сети с поддержкой STP часто разрываются, зачастую вызывая прерывание обслуживания.

RSTP использует процесс предложения и соглашения, который позволяет немедленно согласовать каналы, и исключить время, затрачиваемое на таймеры до того, как произойдет конвергенция связующего дерева. Процесс предложения и соглашения выполняется каскадно, от точки корневого моста через сеть коммутации, по мере того, как каждый нижестоящий коммутатор начинает определять правильный корневой мост и путь к этому корневому мосту.

Роли порта RSTP



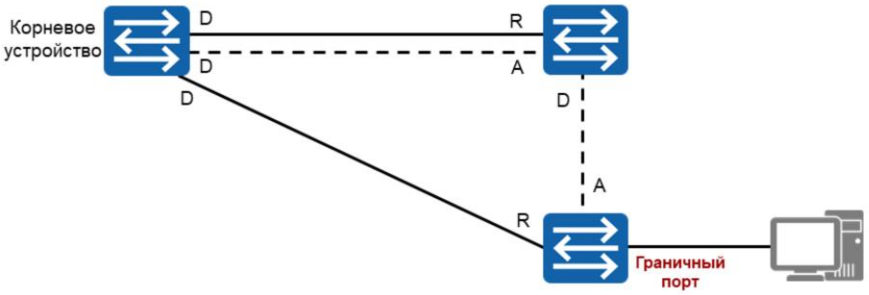
Роли	Описание
Резервный	Резервный путь к узлам в нисходящем направлении, где резервные каналы существуют в том же сегменте LAN, что и назначенный порт.
Альтернативный	Альтернативный путь к корневому мосту, отличающийся от пути, предоставляемого корневым портом коммутатора.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Коммутаторы, работающие в режиме RSTP, выполняют две отдельные роли. Альтернативный порт предлагает альтернативный путь в направлении корневого моста и может заменить корневой порт в случае выхода его из строя. Резервный порт предназначен для резервирования пути, предоставляемого назначенным портом в направлении сегментов сети, и не может гарантировать альтернативное подключение к корневому порту.

Резервные порты существуют только в конфигурациях, где есть два или более соединения данного моста с данной сетью (сегментом сети), с общим устройством, например, концентратором, или когда используется одно двухточечное соединение для создания физического закольцованного соединения между портами на одном коммутаторе. Однако в обоих случаях действует принцип резервного порта, при котором два или более порта на одном коммутаторе подключаются к одному сегменту локальной сети.

Граничные порты RSTP



- Системы, не участвующие в RSTP, подключаются к граничным портам.
- Граничные порты не получают BDPU и могут мгновенно пересылать данные.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

В RSTP назначенный порт на границе сети называется граничным портом. Граничный порт напрямую соединяется с терминалом и не подключается к другим устройствам коммутации. Граничный порт не получает конфигурацию BPDU, поэтому не участвует в вычислении RSTP.

Он может напрямую переключаться из состояния «Отключение» в состояние «Пересылка», по аналогии с портами, не поддерживающими STP. Если граничный порт получает фиктивную конфигурацию BPDU от злоумышленников, он лишается атрибутов граничного порта и становится общим STP-портом. Расчет STP выполняется снова, что может вызвать нестабильность сети.

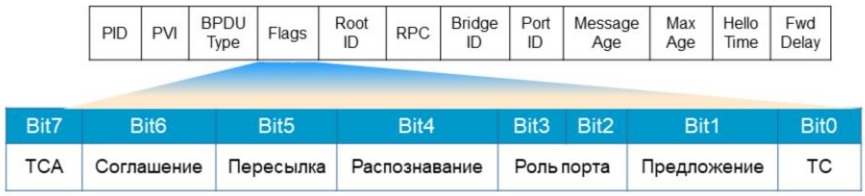
Состояния порта RSTP

STP	RSTP	Роль порта
Отключение	Отбрасывание	Отключенный
Блокировка	Отбрасывание	Альтернативный или резервный
Прослушивание	Отбрасывание	Корневой или назначенный
Изучение	Изучение	Корневой или назначенный
Пересылка	Пересылка	Корневой или назначенный

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

В RSTP изменились названия состояний портов, количество которых сокращено до трех типов. Тип порта зависит от того, пересылает ли порт пользовательский трафик и изучает ли MAC-адреса. Если порт не пересылает пользовательский трафик и не изучает MAC-адреса, порт находится в состоянии отбрасывания. Считается, что порт находится в состоянии изучения, когда порт не пересылает пользовательский трафик, но изучает MAC-адреса. Если порт пересылает пользовательский трафик и изучает MAC-адреса, значит, порт находится в состоянии пересылки.

RST BPDU



Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
TCA	Соглашение	Пересылка	Распознавание	Роль порта		Предложение	TC

Роль порта = 00 Неизвестный
01 Альтернативный/резервный порт
10 Корневой порт
11 Назначенный порт

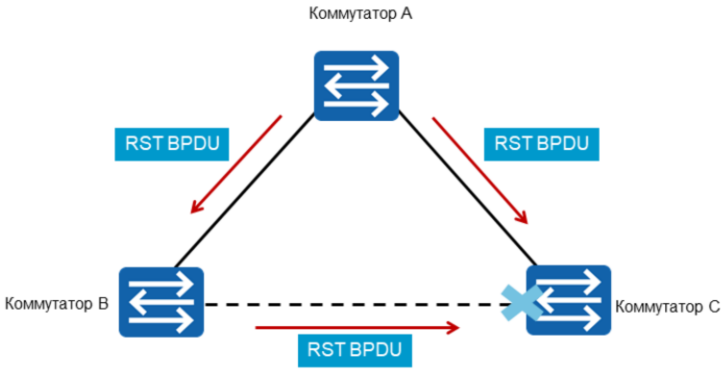
- Неиспользуемые поля STP BPDU активны в RSTP.
- В RSTP появляются новые возможности.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.
HUAWEI

Формат BPDU, используемый в STP, также используется в RSTP с небольшими изменениями некоторых общих параметров. Чтобы отличить конфигурационный BPDU STP от BPDU RST (BPDU быстрого связующего дерева), необходимо определить тип BPDU. STP устанавливает 0 (0x00) как тип конфигурационного BPDU, а 128 (0x80) как тип TCN BPDU (BPDU уведомления об изменении топологии), 2 (0x02) — тип RST BPDU. В поле flags BPDU RST дополнительные поля параметров назначаются полям BPDU.

В поле Flag BPDU протокола STP используются только два бита, которые определяют флаги изменения топологии TC и подтверждения TC (TCA), при этом другие поля являются резервными. BPDU RST использует эти поля для поддержки новых параметров. К ним относятся флаги процессов предложения и соглашения, используемые RSTP для быстрой конвергенции, определения роли и состояния порта.

RST BPDU

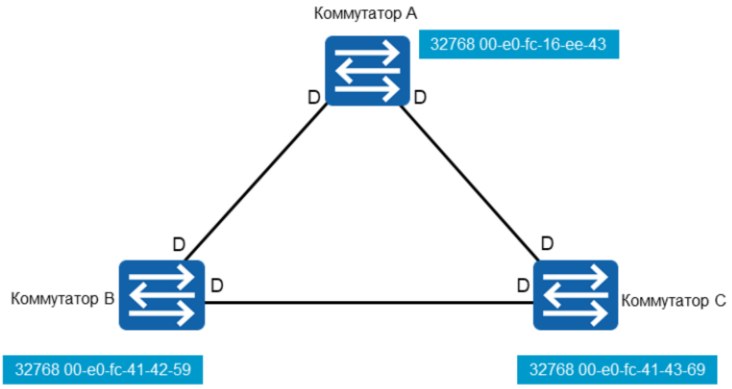


- Назначенные коммутаторы генерируют собственный BDPU с интервалом Hello, независимо от того, был ли принят RST BPDU.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

После того как топология становится стабильной в STP, корневой мост отправляет конфигурационный BPDU с интервалом, установленным таймером Hello. Некорневой мост не отправляет конфигурационный BPDU, пока не получит конфигурационный BPDU, отправленный с вышестоящего устройства. Это делает расчет STP сложным и трудоемким. В RSTP после того, как топология становится стабильной, некорневой мост отправляет конфигурационный BPDU с интервалами Hello, независимо от того, получил ли он конфигурационный BPDU, отправленный корневым мостом; такие операции выполняются на каждом устройстве независимо.

Конвергенция RSTP

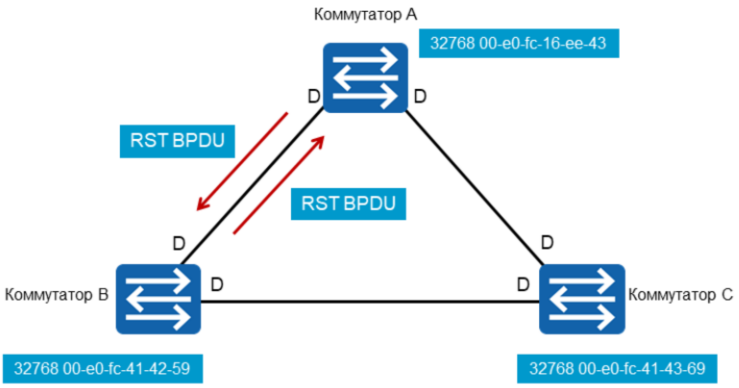


- Все коммутаторы с поддержкой RSTP начинают функционировать как корневые мосты и отправляют RST BPDU.
- Для портов установлены роли назначенного порта и состояние отбрасывания (discarding).

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Конвергенция RSTP строится на некоторых основных принципах STP, а именно на том, что все коммутаторы при инициализации принимают роль корневого моста, и, таким образом, каждому интерфейсу присваивается роль назначенного порта. Однако порт находится в состоянии отбрасывания до тех пор, пока взаимодействующие коммутаторы не смогут подтвердить состояние канала.

Предложение RST BPDU

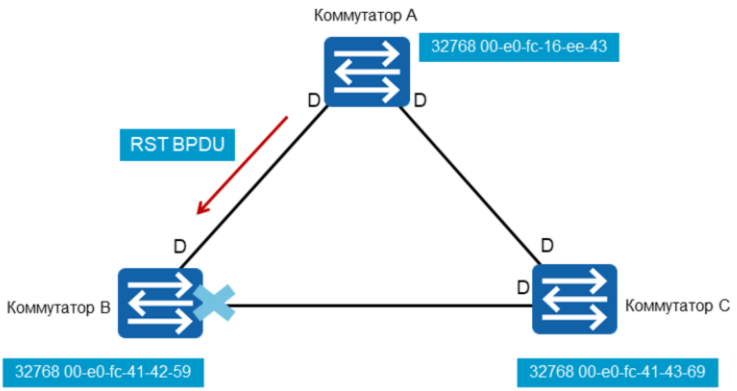


- Предложения отправляются в RST BPDU во время выбора корневого устройства.
- Коммутатор игнорирует предложение, если у него имеется лучший вариант ID моста.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Каждый коммутатор, объявляющий себя корневым мостом, будет согласовывать состояния портов для данного сегмента локальной сети, генерируя BPDU RST с битом предложения, установленным в поле flags. Когда порт получает RST BPDU от вышестоящего назначенного моста, порт сравнивает полученный RST BPDU с собственным RST BPDU. Если собственный RST BPDU обладает лучшими параметрами (Superior) по сравнению с принятым, порт отбрасывает принятый RST BPDU и немедленно отправляет на одноранговое устройство собственный RST BPDU, включающий в себя набор битов предложения.

Процесс синхронизации RSTP



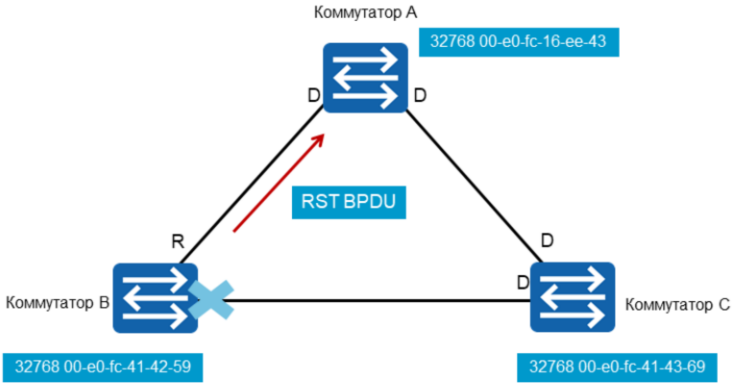
- При получении Superior BPDU (с наилучшими параметрами) коммутатор B прекращает отправку RST BDPU, содержащего предложение, и начинает синхронизацию.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.
HUAWEI

Поскольку таймеры не играют большую роль в процессе конвергенции топологии RSTP, как в случае с STP, важно ограничить возможность возникновения коммутационных петель во время согласования роли порта. Это достигается за счет процесса синхронизации, который определяет, что после получения Superior BPDU, содержащего бит предложения, коммутатор-получатель должен установить все нижестоящие назначенные порты в состояние отбрасывания.

Однако, если нижестоящий порт является альтернативным или граничным портом, статус роли порта остается неизменным. В данном примере показано временное изменение состояния назначенного порта нижестоящего сегмента LAN на состояние отбрасывания и, следовательно, блокирование пересылки любого кадра во время процесса предложения и соглашения в восходящем направлении.

Соглашение RST BPDU

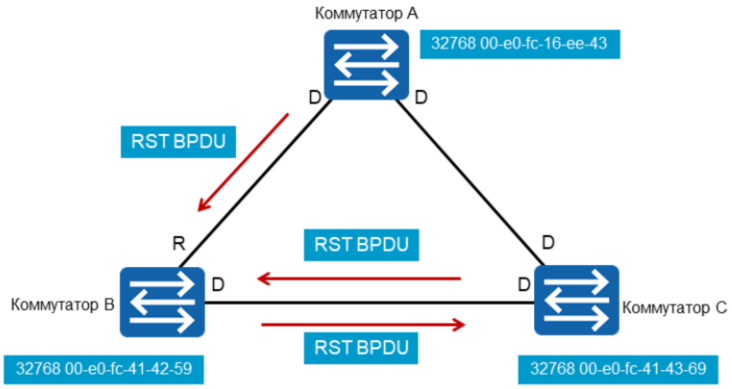


- После блокировки всех нижестоящих неграничных назначенных портов коммутатор B отправляет RST BPDU с битом соглашения.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Подтвержденное изменение состояния нижестоящего назначенного порта на состояние отбрасывания позволяет посылать RST BPDU в ответ на предложение, отправленное вышестоящим коммутатором. На данном этапе роль порта интерфейса определяется как корневой порт, и поэтому флаг соглашения и роль порта корневого устройства устанавливаются в поле flags RST BPDU, которое возвращается в ответ на предложение.

Конвергентный канал RSTP

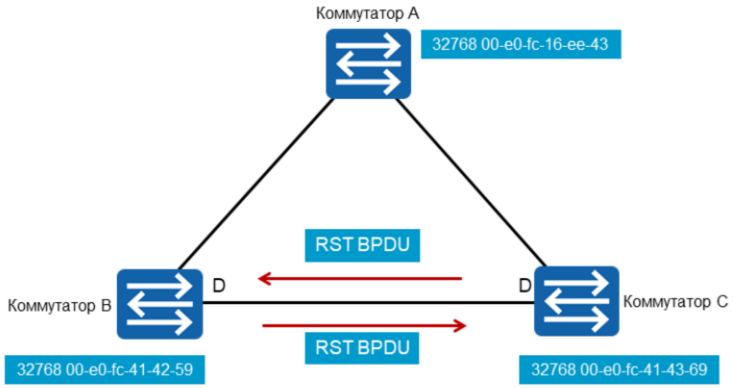


- Нисходящий порт снова разблокирован и между коммутатором B и коммутатором C начинается новый этап синхронизации.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

На заключительном этапе процесса предложения и соглашения вышестоящий коммутатор принимает RST BPDU, содержащий бит соглашения, и назначенный порт сразу же изменяет состояние отбрасывания на состояние пересылки. После этого нисходящие сегменты локальной сети начинают согласовывать роли портов интерфейсов, используя одни и те же процессы предложения и согласования.

Сбой канала/корневого устройства

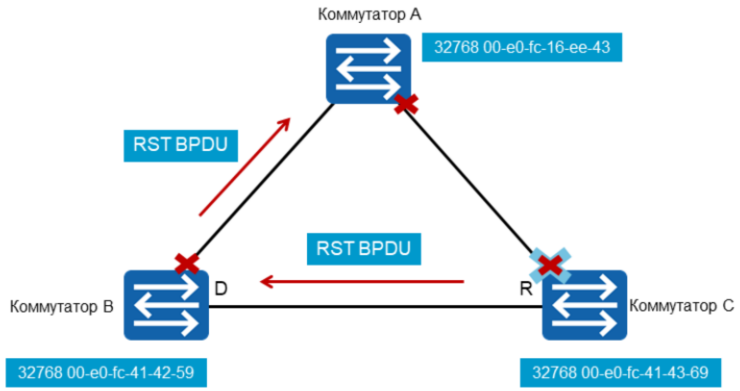


- Потеря восходящего RST BPDU сигнализирует о сбое канала/устройства.
  - Конвергенция на основе предложений и соглашений.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

В STP, прежде чем определять сбой согласования, устройство должно выждать период Max Age. В RSTP, если порт не получает конфигурационные BPDU, отправленные с вышестоящего устройства в течение трех последовательных интервалов Hello, происходит сбой связи между локальным устройством и одноранговым узлом, что приводит к инициализации процесса предложения и соглашения для обнаружения ролей порта для сегмента локальной сети.

Процесс изменения топологии



- Во время отправки соглашения выполняется сброс адресов для всех портов, за исключением порта, на котором был получен RST BPDU.

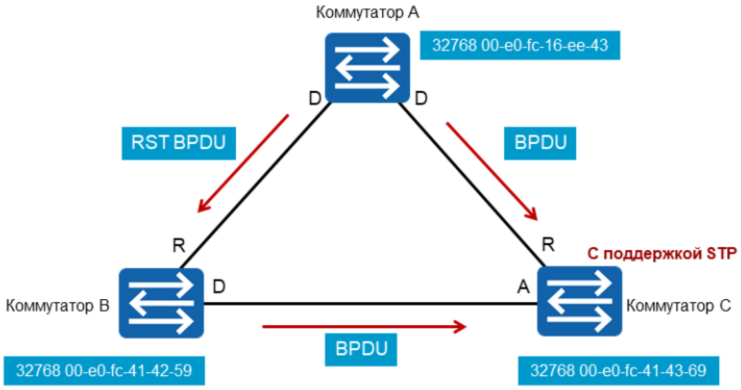
Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Изменения топологии влияют на RSTP так же, как влияют и на STP, однако между ними есть некоторые незначительные различия. В данном примере произошел сбой соединения на коммутаторе C. Коммутатор A и коммутатор C немедленно обнаруживают сбой соединения и сбрасывают записи адресов для портов, подключенных к этому каналу. BPDU RST начинает согласовывать состояния портов в рамках процесса предложения и соглашения, после чего будет получено уведомление об изменении топологии вместе с пересылкой BPDU RST, содержащим соглашение.

Этот RST BPDU будет иметь как бит Соглашения, так и бит TC, установленный в значение 1, чтобы проинформировать вышестоящие коммутаторы о необходимости сбросить записи MAC-адресов на всех интерфейсах портов, кроме интерфейса порта, на котором был получен RST BPDU, содержащий установленный бит TC.

Бит TC будет установлен в периодически отправляемом RST BPDU и переадресован в восходящем направлении в течение периода, эквивалентного времени Hello + 1 секунда, в течение которого все соответствующие интерфейсы будут сброшены и продолжат повторное заполнение записей MAC на основе новой топологии RSTP. Красный (темный) значок «x» в примере показывает, какие интерфейсы будут сброшены в результате изменения топологии.

Взаимодействие STP

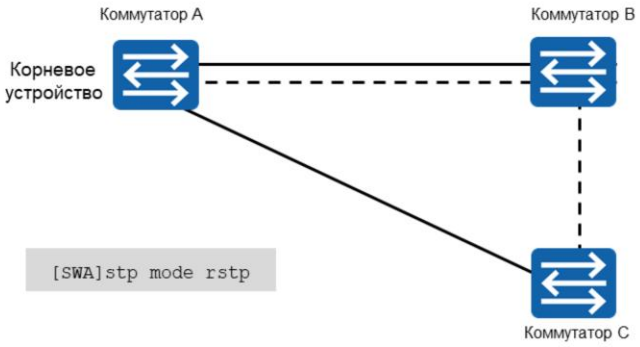


- Порты коммутатора RSTP возвращаются к STP при подключении к сегменту LAN, содержащему устройство с поддержкой STP.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Внедрение STP в топологию коммутации на основе RSTP возможна, однако не рекомендуется, поскольку любые ограничения, относящиеся к STP, становятся очевидными в рамках диапазона связи коммутатора с поддержкой STP. Порт, участвующий в процессе согласования для установления своей роли в STP, должен ждать в течение 50 секунд, прежде чем будет выполнена конвергенция, в результате преимущества RSTP становятся бесполезными.

Настройка режима



- Команда *stp mode rstp* позволяет всем портам коммутатора генерировать RST BPDU.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Конфигурация режима связующего дерева коммутаторов Sx7 требует использования команды stp mode для установки режима RSTP. При этом коммутатор серии Sx7 будет генерировать RST BPDU по отношению к RSTP, в отличие от других реализаций связующего дерева. Эта команда настраивается в режиме system-view и должна применяться ко всем коммутаторам, участвующим в топологии быстрого связующего дерева.

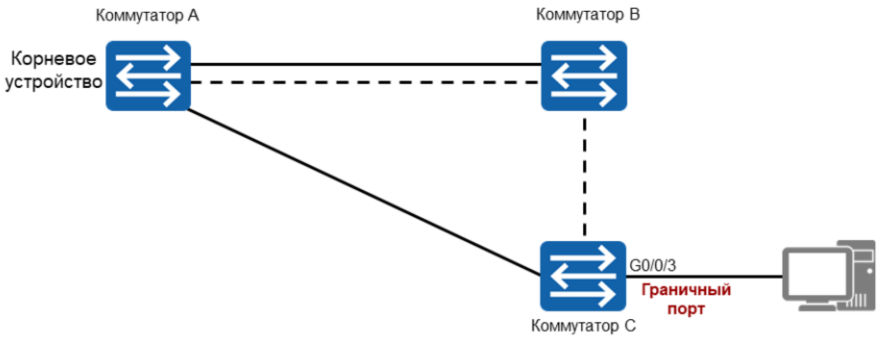
Проверка конфигурации

```
[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
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Команда display stp предоставляет соответствующую информацию о конфигурации RSTP, так как многие параметры поддерживают принципы архитектуры STP. Информация о режиме определяет, поддерживает ли коммутатор RSTP.

Настройка граничного порта




```
[SWC-GigabitEthernet0/0/3]stp edged-port enable
```

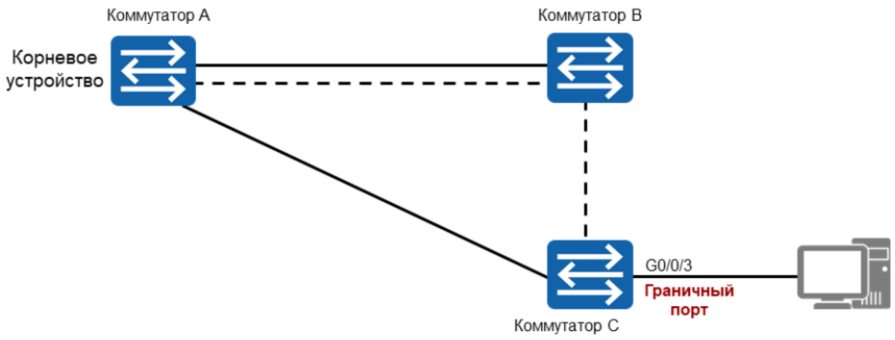
- Позволяет переводить граничный порт в состояние пересылки без задержек.
- Интерфейсы на S5700 являются неграничными портами по умолчанию.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Граничный интерфейс определяет порт, не участвующий в топологии связующего дерева. Эти интерфейсы используются конечными системами для подключения к коммутационной сети для пересылки кадров. Поскольку такие конечные системы не требуют согласования состояния интерфейса порта, предпочтительно, чтобы порт сразу переходил в состояние пересылки, чтобы можно было немедленно передать кадры через этот интерфейс.

Команда stp edged-port enable используется для переключения порта в состояние граничного порта, так как по умолчанию все порты считаются неграничными портами на коммутаторе. Для отключения граничного порта используется команда stp edged-port disable. Эти команды применяются только к одному порту на данном коммутаторе. Важно отметить, что поведение граничного порта связано с RSTP, как это определено в стандарте IEEE 802.1D-2004, однако вследствие специфического применения VRP базовой машины состояний (state machine) RSTP в STP (что также приводит к присутствию в STP состояний порта RSTP), также возможно применить настройки граничного порта RSTP к STP в рамках продуктов серии Sx7 Huawei.

Настройка граничного порта

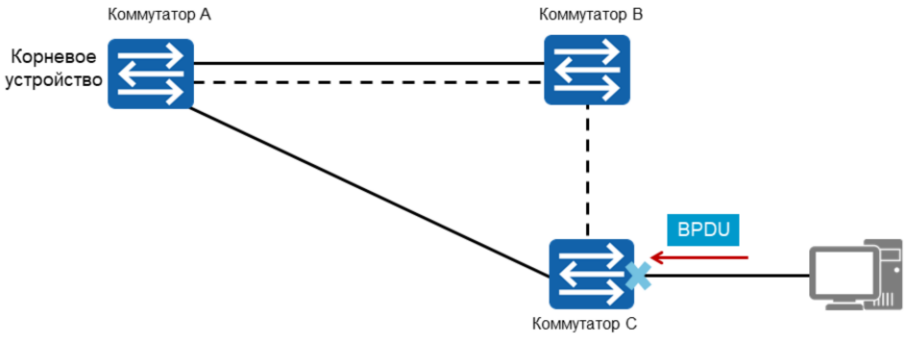


- Все порты коммутатора будут сконфигурированы как граничные порты.
- При использовании этой команды необходимо проявлять осторожность, чтобы избежать петель STP.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

В случае, если несколько портов на коммутаторе настраиваются как граничные порты, применяется команда stp edged-port default, которая обеспечивает, чтобы все интерфейсы портов на коммутаторе являлись граничными портами. Важно запустить команду stp edged-port disable на портах, которые должны участвовать в расчете STP между устройствами, чтобы избежать возникновения петель в результате вычисления топологии STP.

Защита BPDU




```
[SWC]stp bpdu-protection
```

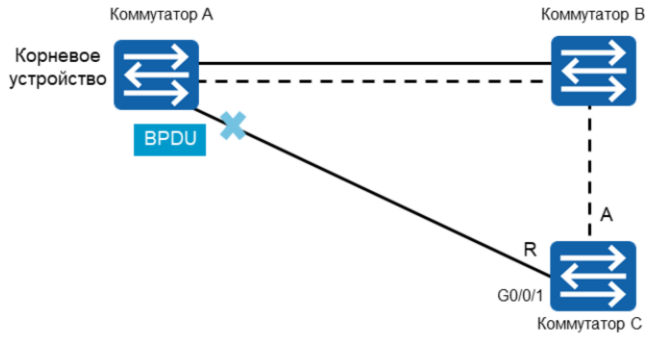
- Защита BPDU предотвращает умышленное внедрение BPDU в RSTP.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Порт, который напрямую подключен к пользовательскому терминалу, такому как ПК или файл-сервер, рассматривается как сконфигурированный граничный порт, предназначенный для обеспечения быстрого изменения состояния порта. Обычно никакие BPDU не отправляются на граничные порты, однако, если коммутатор подвергается атаке псевдо-BPDU, он устанавливает граничные порты в качестве негранничных. После того, как эти граничные порты получают BPDU, топология связующего дерева пересчитывается, и в результате сеть становится нестабильной.

Для защиты от атак псевдо-BPDU RSTP обеспечивает защиту BPDU. После включения защиты BPDU коммутатор отключает граничный порт, который получает BPDU, и сообщает об этом любой активной станции управления сетью (NMS). Граничные порты, которые отключены коммутатором, могут быть запущены вручную только сетевым администратором. Команда stp bpdu-protection должна использоваться для включения защиты BPDU и настраивается глобально в системном режиме.

Защита от петель



[SWC-GigabitEthernet0/0/1]stp loop-protection

- Если нижестоящий коммутатор не получает BDPU, корневой порт блокируется во избежание возникновения коммутационных петель.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

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

Коммутатор обеспечивает защиту от петель. После включения функции защиты от петель корневой порт блокируется, если он не может получить BPDU от вышестоящего коммутатора. Заблокированный порт остается в заблокированном состоянии и не пересылает пакеты, что позволяет предотвратить возникновение петель в сети. Если интерфейс сконфигурирован как граничный интерфейс или на интерфейсе включена защита корневого устройства, невозможно включить защиту от петель на интерфейсе. Необходимо применить команду stp loop-protection для включения этой функции в режиме интерфейса.

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
                            ......
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

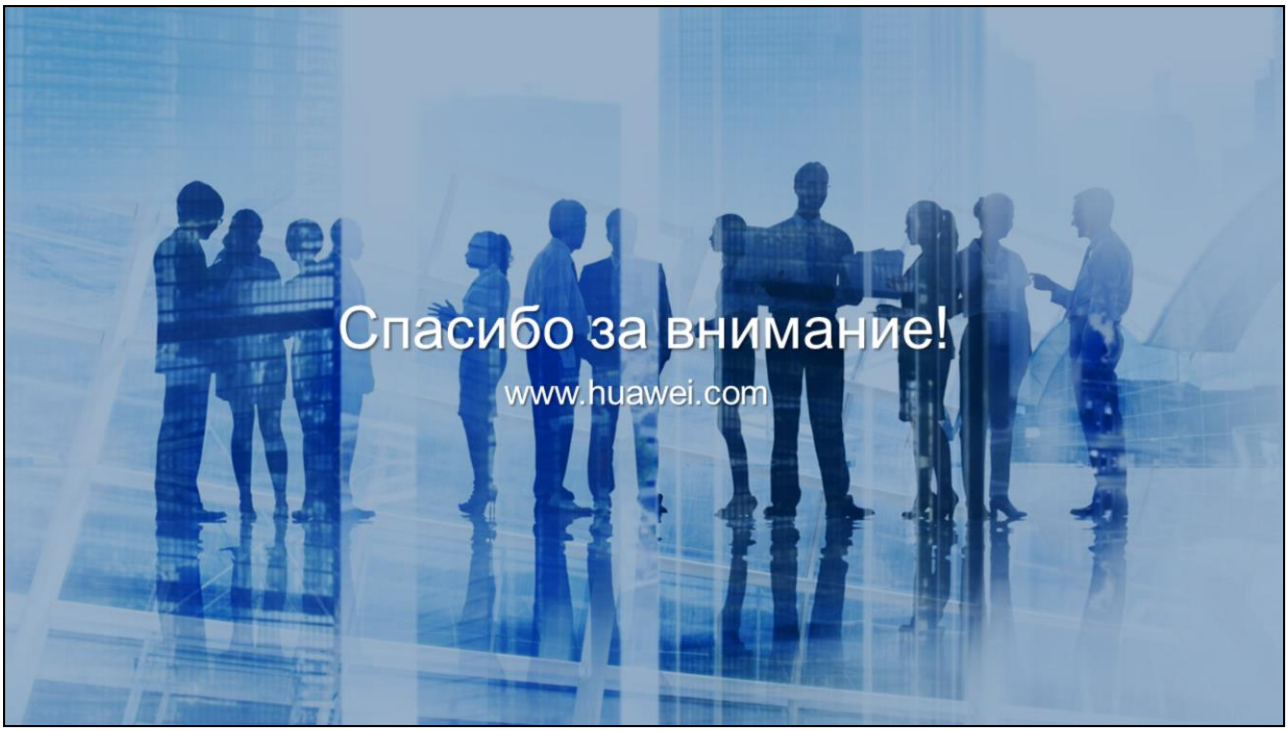
Проверка конфигурации RSTP для данного интерфейса выполняется с помощью команды display stp interface <interface>. Соответствующая информация идентифицирует состояние порта интерфейса как Discarding, Learning или Forwarding. Определяется соответствующая информация для интерфейса порта, включая приоритет порта, стоимость порта, статус порта в качестве граничного порта или поддерживающего передачу «точка-точка» и т.д.

Заключение

- Какова цель синхронизации, которая происходит во время процесса предложения и соглашения RSTP?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Синхронизация представляет собой этап процесса конвергенции, который включает блокировку назначенных портов, в то время как RST BPDU передаются с сообщениями предложения и соглашения для конвергенции сегмента коммутатора. Этот процесс предназначен для того, чтобы все интерфейсы согласовали свои роли порта, чтобы после разблокировки назначенного порта на любых нижестоящих коммутаторах не возникали коммутационные петли.


Спасибо за внимание!
www.huawei.com

Маршрутизация в IP-сетях

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

Пересылка кадров и коммутация определили операции, выполняемые на уровне канала передачи данных, а также роль стандартов семейства IEEE 802 как базовых механизмов связи, на основании которых работают протоколы верхнего уровня. Внедрение маршрутизации определило физические основы для протоколов верхнего уровня и межсетевого взаимодействия. Домен корпоративной сети, как правило, состоит из нескольких сетей, для которых требуются решения о выборе маршрута, чтобы гарантировать использование оптимальных маршрутов для пересылки IP-пакетов (или датаграмм) в пункт назначения. В этом разделе представлены основы такой маршрутизации.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

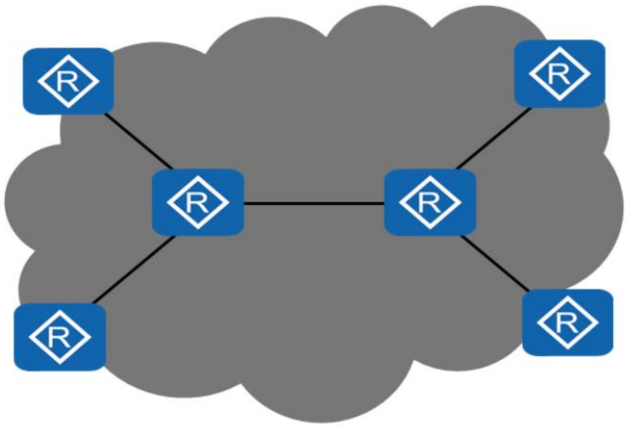
Цели

По окончании этого модуля слушатели смогут:

- Объяснить принципы принятия решений о выборе маршрутов в IP-сети.
- Объяснить основные требования к переадресации пакетов.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Автономные системы



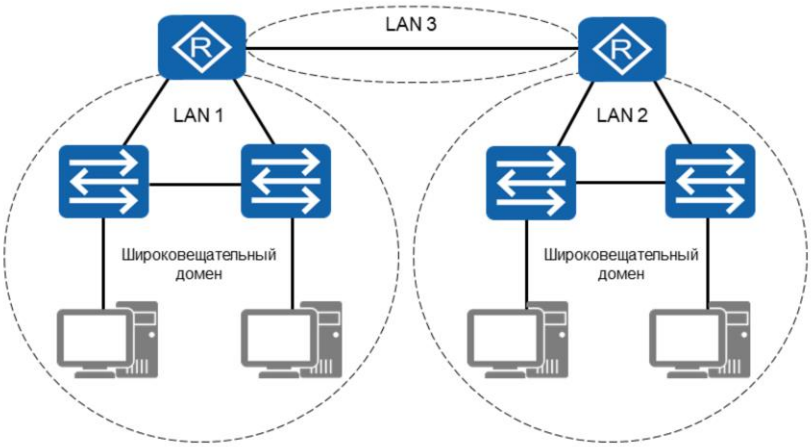
- IP-сеть или сети, управляемые одним или несколькими операторами с четкой политикой, определяющей порядок принятия решений о выборе маршрутов.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Корпоративную сеть обычно можно понимать как экземпляр автономной системы. Как определено в RFC 1030, автономная система или AS представляет собой группу из одного или нескольких префиксов IP, работающих у одного или нескольких сетевых операторов, которые имеют единую (SINGLE) и четко определенную (CLEARLY DEFINED) политику маршрутизации.

Концепция автономных систем изначально учитывала использование одного протокола маршрутизации, но со временем классическое определение было расширено, и в современном понимании AS может использовать несколько протоколов внутренней маршрутизации, которые взаимодействуют посредством внедрения маршрутов из одного протокола в другой. Под политикой маршрутизации можно понимать набор решений о пересылке, определяющих порядок администрирования трафика в автономной системе, которой должны придерживаться операторы.

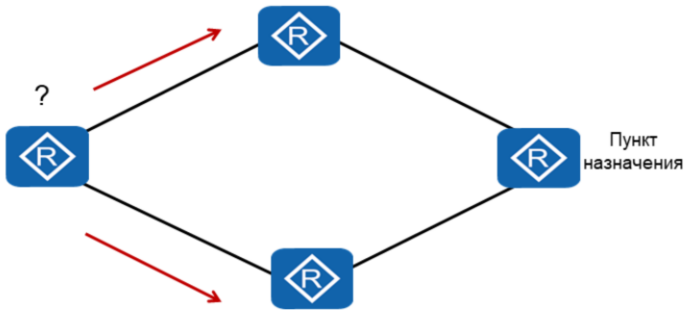
Локальная сеть и широковещательные домены



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Принципы, связанные с коммутацией, касались главным образом пересылки трафика в пределах локальной сети и шлюза, что до сих пор определяло границы широковещательного домена. Маршрутизаторы являются основной формой устройства сетевого уровня, используемого для определения шлюза каждой локальной сети и поддерживающие сегментации IP-сети. Маршрутизаторы являются средством маршрутизации пакетов из одной локальной сети в другую, использующими IP-адресацию для определения IP-сети, в которую направляются пакеты.

Решения о выборе маршрута



- Маршрутизаторы отвечают за процесс принятия решений, определяющий путь передачи пакетов.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Маршрутизатор отвечает за определение пути пересылки, по которому пакеты должны отправляться к указанному пункту назначения. Каждый маршрутизатор несет ответственность за принятие решения о том, как передаются данные. Если маршрутизатор имеет несколько путей к заданному пункту назначения, решения о маршруте принимаются на основе вычислений для определения следующего оптимального узла (перехода) к предполагаемому пункту назначения. Решения, определяющие выбор маршрута, могут варьироваться в зависимости от используемого протокола маршрутизации, и, в конечном счете, опираются на метрики каждого протокола при принятии решений в отношении изменяющихся 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 перечислены сети, доступные через определенный маршрутизатор. Пакеты, не имеющие маршрута, впоследствии отбрасываются.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Маршрутизаторы пересылают пакеты на основе таблиц маршрутизации и информационной базы пересылки (FIB) и поддерживают как минимум одну таблицу маршрутизации и одну FIB. Маршрутизаторы выбирают маршруты в таблицах маршрутизации и пересылают пакеты на основе FIB. Маршрутизатор использует локальную таблицу маршрутизации для хранения маршрутов и предпочтительных маршрутов. Затем маршрутизатор отправляет предпочтительные маршруты в FIB для управления пересылкой пакетов. Маршрутизатор выбирает маршруты в соответствии с приоритетами протоколов и стоимостью, хранящихся в таблице маршрутизации. Таблица маршрутизации содержит основные параметры каждого IP-пакета.

Сеть назначения и маска используются в комбинации для определения IP-адреса назначения или сегмента сети назначения, где находятся хост или маршрутизатор назначения.

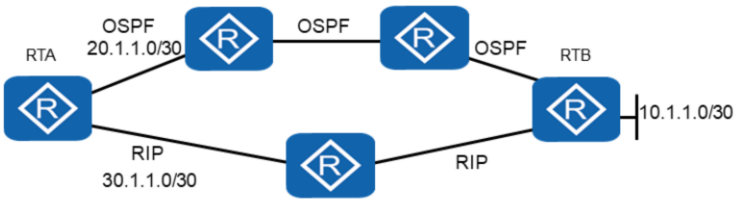
Поле Proto указывает протокол, по которому распознаются маршруты. Поле Pre указывает значение приоритета, которое связано с протоколом и используется для определения того, какой протокол будет применен к таблице маршрутизации, где два протокола предлагают аналогичные маршруты. В качестве оптимального маршрута маршрутизатор выбирает маршрут с наивысшим приоритетом (наименьшее значение).

Значение стоимости представляет собой метрику, которая используется для выбора маршрута в случае, когда несколько маршрутов к одному и тому же пункту назначения имеют одинаковые приоритеты. В качестве оптимального маршрута выбирается маршрут с наименьшей стоимостью.

Значение следующего перехода указывает IP-адрес следующего устройства или шлюза сетевого уровня, через который проходит IP-пакет. В приведенном примере следующий переход 127.0.0.1 – это локальный интерфейс устройства, являющегося следующим переходом.

Наконец, параметр интерфейса указывает исходящий интерфейс, через который пересылается IP-пакет.

Принятие решения о выборе маршрута – Приоритеты




```
[RTA]display ip routing-table
  Destination/Mask   Proto   Pre  Cost      Flags NextHop         Interface
  10.1.1.0/30        OSPF    10   60        RD    20.1.1.2        Ethernet0/0/0
                                  ......
```

Маршрут	Прямой	OSPF	Статический	RIP
Приоритет	0	10	60	100

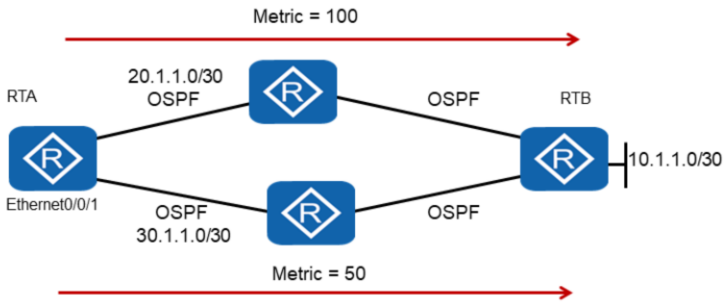
Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Таблица маршрутизации может содержать маршруты нескольких протоколов к данному пункту назначения. Не все протоколы маршрутизации считаются равными, и если самые длинные совпадения для нескольких маршрутов разных протоколов маршрутизации к одному пункту назначения равны, необходимо принять решение относительно того, какой протокол маршрутизации (включая статические маршруты) будет иметь приоритет.

Только один протокол маршрутизации в любой конкретный момент времени определяет оптимальный маршрут к пункту назначения. Чтобы выбрать оптимальный маршрут, каждый протокол маршрутизации (включая статический маршрут) настраивается с приоритетом (чем меньше значение, тем выше приоритет). Когда одновременно существуют несколько источников информации о маршрутизации, в качестве оптимального маршрута выбирается маршрут с наивысшим приоритетом и добавляется в локальную таблицу маршрутизации.

В этом примере определены два протокола, которые предоставляют средство обнаружения 10.1.1.0 по двум разным путям. Путь, определенный протоколом RIP, как видно, обеспечивает более прямой маршрут к предполагаемому месту назначения, однако из-за значения приоритета маршрут, определенный протоколом OSPF, является предпочтительным и поэтому устанавливается в таблице маршрутизации в качестве приоритетного маршрута. Для понимания порядка определения приоритета по умолчанию приведено краткое описание значений приоритетов по умолчанию для некоторых распространенных механизмов маршрутизации.

Принятие решения о выборе маршрута – Метрики



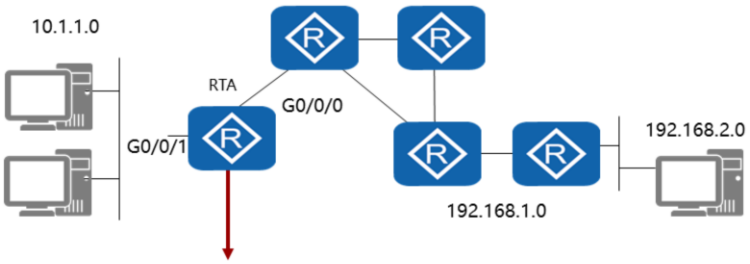

```
                    [RTA]display ip routing-table
 Destination/Mask  Proto   Pre  Cost      Flags NextHop         Interface
 10.1.1.0/30       OSPF    10   50        RD    30.1.1.2        Ethernet0/0/1
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Если же маршрут невозможно определить ни по самому длинному совпадению, ни по приоритету, то для принятия решения при определении маршрута, который должен быть указан в таблице маршрутизации, принимается метрика стоимости. Стоимость представляет длину пути к сети назначения.

Каждый сегмент предоставляет значение стоимости пути, которое учитывается для определения стоимости маршрута. Другим распространенным фактором является пропускная способность сети, на которой иногда основан механизм стоимости. Канал с более высокой скоростью (пропускной способностью) представляет собой более низкое значение стоимости, и определяет приоритет одного пути по отношению к другим, в то время как каналы с одинаковой скоростью получают сбалансированную стоимость для эффективного распределения нагрузки. Более низкая метрика всегда имеет приоритет, и поэтому метрика 50, как показано в примере, определяет оптимальный маршрут до заданного пункта назначения, для которого можно найти запись в таблице маршрутизации.

Создание таблицы IP-маршрутизации



Исходный маршрутизатор	Целевая сеть	Интерфейс
Прямой	10.1.1.0	G0/0/1
Статический	192.168.1.0	G0/0/0
OSPF	192.168.2.0	G0/0/0

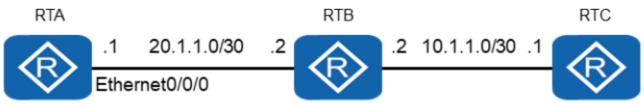
Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Создание таблицы IP-маршрутизации происходит путем использования «приоритета» и «стоимости».

Таблицы IP-маршрутизации можно разделить на три типа в зависимости от исходного маршрутизатора:

- Таблицы прямой маршрутизации;
- Таблицы статической маршрутизации;
- Таблицы динамической маршрутизации.

Принятие решения о выборе маршрута – Самые длинные совпадения




```
[RTA]display ip routing-table
  Destination/Mask  Proto   Pre  Cost      Flags NextHop         Interface
  10.1.1.0/24       Static  60   0           RD  20.1.1.2        Ethernet0/0/0
  10.1.1.0/30       Static  60   0           RD  20.1.1.2        Ethernet0/0/0
```

- Сравнение и выбор маршрута к одному пункту назначения выполняется на основе самого длинного совпадения.

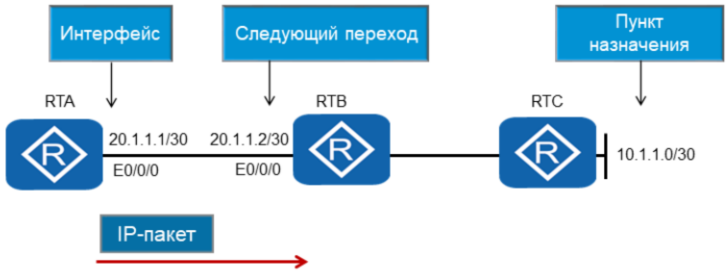
Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Чтобы пакеты могли достичь предполагаемого места назначения, маршрутизаторы должны принимать конкретные решения относительно изученных маршрутов и того, какой из этих маршрутов будет применен. Маршрутизатор узнает о пути к данному пункту назначения из информации о маршрутизации, анонсированной соседними маршрутизаторами. В качестве альтернативы можно вручную применить статические маршруты посредством вмешательства администратора.

Каждая запись в таблице FIB содержит физический или логический интерфейс, по которому отправляется пакет на следующий маршрутизатор. Запись также указывает, может ли пакет быть отправлен напрямую на хост назначения в сети с прямым подключением. Маршрутизатор выполняет операцию «AND» с адресом назначения в пакете и маской 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 наилучшим или «самым длинным» совпадением. В этом примере две записи в сети 10.1.1.0 существуют со следующим переходом 20.1.1.2. Пересылка в пункт назначения 10.1.1.1 приведет к применению принципа самого длинного совпадения, которое обеспечивает сетевой адрес 10.1.1.0/30.

Требования к пересылке по таблице маршрутизации



- Для пересылки пакетов необходимо иметь информацию о пункте назначения, интерфейсе пересылки и следующем переходе (узле).

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Способность маршрутизатора пересылать IP-пакет в заданный пункт назначения требует наличие определенной информации о пересылке. Любой маршрутизатор, пересылающий IP-пакет, должен знать действительный адрес назначения, на который должен быть переслан пакет. Это означает, что в таблице маршрутизации должна существовать запись, которую сможет использовать маршрутизатор. Эта запись также должна идентифицировать интерфейс, по которому будут передаваться IP-пакеты, и следующий переход, который должен получить пакет, прежде чем будет принято решение о следующей пересылке.

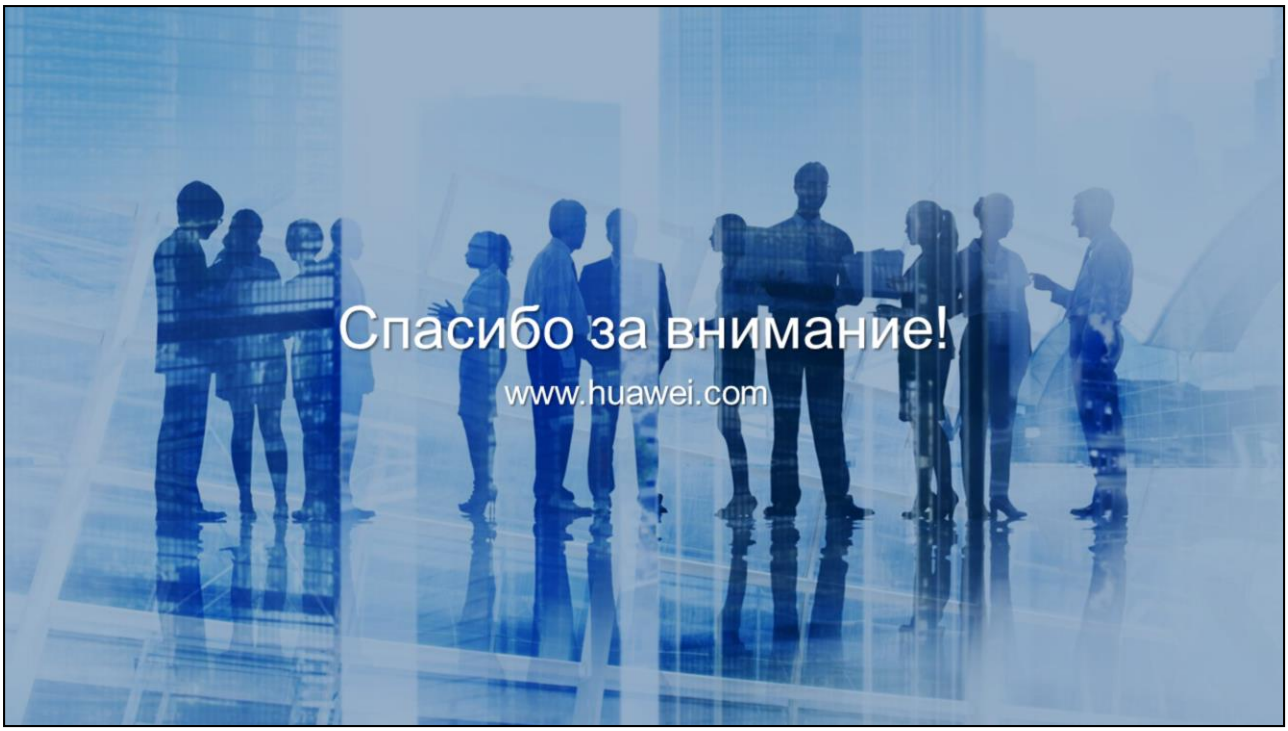
Заключение

- Каков порядок принятия решений о выборе маршрута?
- Что представляет собой приоритет?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Решения о выборе маршрута первоначально принимаются на основе самого длинного совпадения, независимо от значений приоритета, назначенных маршрутам в одной сети. Если значение самого длинного совпадения для двух маршрутов к одному пункту назначения равно, должно использоваться значение приоритета; если и они равны, то используется метрика. Если значения метрики также одинаковы, протоколы обычно применяют форму распределения нагрузки данных по каналам с одинаковой стоимостью.

Приоритет используется для обозначения надежности маршрута по отношению к маршрутам, которые считаются менее надежными. Однако поставщики оборудования для маршрутизации могут назначать разные значения приоритетов для протоколов, которые поддерживаются в каждом продукте каждого поставщика. Значения приоритетов некоторых распространенных протоколов маршрутизации, поддерживаемых устройствами маршрутизации Huawei, можно найти в этом разделе.


Спасибо за внимание!
www.huawei.com

Статические маршруты передачи по IP-сети

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

Маршруты в таблице IP-маршрутизации маршрутизатора можно определять вручную (статическая маршрутизация) или программно (посредством протоколов динамической маршрутизации). При ручной конфигурации маршруты указываются в явном виде, однако этот способ может привести к отказу маршрута в условиях сбоя перехода на следующий узел. Но все же статическая маршрутизация применяется часто, дополняя динамические протоколы маршрутизации и предоставляя альтернативные маршруты в случае, если динамически обнаруженные маршруты не обеспечивают действительный адрес следующего узла. Сетевой администратор должен уметь конфигурировать и применять статические маршруты.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

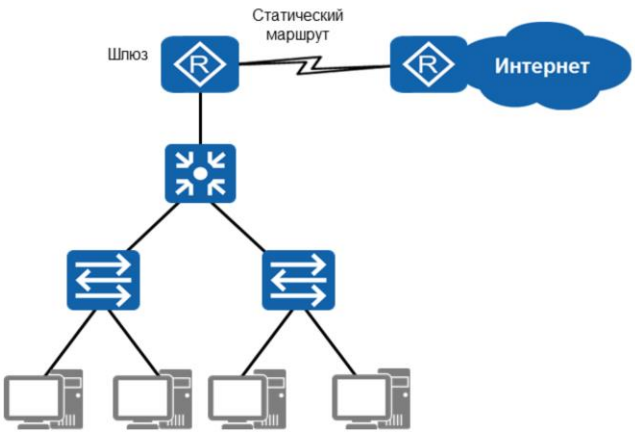
Цели

По окончании данного курса слушатели смогут:

- Объяснить различные режимы использования статических маршрутов.
- Успешно сконфигурировать статические маршруты в таблице IP-маршрутизации.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Применение статического маршрута

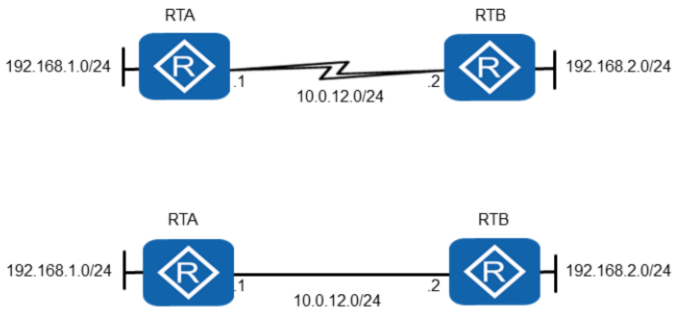


- Статический маршрут — это инструмент выбора пути к другим сетям.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Статический маршрут – это специальный маршрут, который вручную конфигурируется сетевым администратором. Недостатком статических маршрутов является то, что они не могут автоматически адаптироваться к изменениям в сети. Поэтому при изменениях в сети необходимо выполнять повторное конфигурирование. Статические маршруты подходят для сетей с относительно простой структурой. Не рекомендуется конфигурировать и обслуживать статические маршруты в сети со сложной структурой. Однако статические маршруты используют более узкую полосу пропускания и потребляют меньше ресурсов ЦП. Другие протоколы не дают этих преимуществ.

Поведение статического маршрута



- Передача пакетов через последовательный интерфейс требует определения исходящего интерфейса.

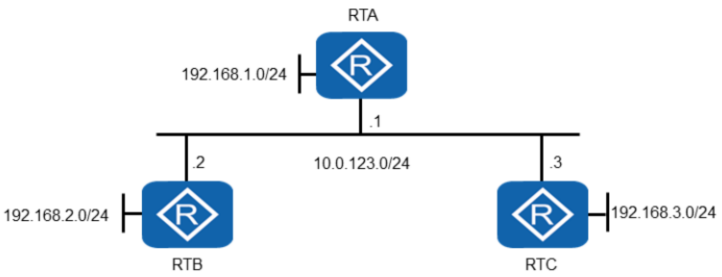
Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Статические маршруты могут применяться в сетях, использующих как среду последовательной передачи, так и Ethernet-среду, однако в каждой ситуации применения статического маршрута различаются условия, в которых необходимо определить либо исходящий интерфейс, либо IP-адрес следующего узла.

Среду последовательной передачи можно наблюдать в сети двухточечной связи (P2P), для которой должен быть сконфигурирован исходящий интерфейс. Для интерфейса P2P адрес следующего транзитного узла указывается после исходящего интерфейса. То есть адрес удаленного интерфейса (интерфейса на равноправном устройстве), подключенного к этому интерфейсу, является адресом следующего узла.

Например, протокол, используемый для инкапсуляции через среду последовательной передачи, является протоколом соединения «точка-точка» (PPP). Удаленный IP-адрес может быть получен после согласования PPP, поэтому необходимо указать только исходящий интерфейс. В этом примере также определяется такой вид двухточечного соединения, как Ethernet, однако поскольку Ethernet представляет собой технологию широковещательной передачи, то принципы технологии «точка-точка» здесь не применимы.

Поведение статического маршрута



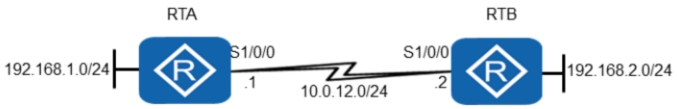
- Для передачи пакетов через широковещательные сети, например Ethernet, необходимо определить адрес следующего узла.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

В случае использования интерфейсов широковещательной передачи, например Ethernet, необходимо определить адрес следующего узла. Если в качестве исходящего интерфейса указан интерфейс Ethernet, то вероятно существует несколько следующих узлов, и система не сможет решить, какой следующий узел использовать. При определении адреса следующего узла маршрутизатор определяет локальное соединение, по которому должен быть получен пакет.

В данном примере пакеты, которые необходимо доставить в пункт назначения 192.168.2.0/24, необходимо перенаправить на адрес следующего узла 10.0.123.2. В другом варианте, для достижения адреса пункта назначения 192.168.3.0 необходимо определить адрес следующего узла 10.0.123.3.

Конфигурирование статического маршрута



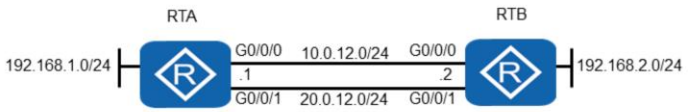

```
[RTB]ip route-static 192.168.1.0 255.255.255.0 10.0.12.1
[RTB]ip route-static 192.168.1.0 255.255.255.0 Serial 1/0/0
[RTB]ip route-static 192.168.1.0 24 Serial 1/0/0
```

- Статический маршрут может быть сконфигурирован одним из следующих способов.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.
HUAWEI

Для конфигурации статического маршрута необходимо выполнить команду *ip route-static ip-address* { *mask* | *mask-length* } *interface-type interface-number* [*nexthop-address*], где *ip-address* – это адрес сети или хоста назначения. В поле маски указывается значение маски или номер префикса. В случае использования интерфейсов широковещательной передачи, например Ethernet, используется адрес следующего узла. При использовании среды последовательной передачи необходимо указать тип и номер интерфейса (например, последовательный интерфейс 1/0/0) в команде для определения исходящего интерфейса.

Балансировка нагрузки 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 20.0.12.1
```

- Статические маршруты поддерживают распределение нагрузки трафика для одного пункта назначения и с одинаковой стоимостью маршрутов.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Если между исходной сетью и сетью назначения существуют маршруты с равной стоимостью, то можно применить механизм балансировки нагрузки, чтобы трафик передавался по обоим каналам. Для этого оба статических маршрута должны иметь одинаковые значения метрики, приоритета и совпадение с префиксом наибольшей длины. В случае использования среды последовательной передачи необходимо сконфигурировать несколько статических маршрутов, по одному для каждого следующего узла, или исходящий интерфейс.

В данном случае показан пример реализации двух команд *ip route-static*, каждая из которых определяет один и тот же IP-адрес и маску узла назначения, но с разными адресами следующих узлов. Это гарантирует совпадение самого длинного префикса (/24) и значения приоритета, так как оба маршрута являются статическими маршрутами со значением приоритета по умолчанию, равным 60. Стоимость путей будет также одинаковой, что позволяет сбалансировать нагрузку.

Проверка выполнения балансировки нагрузки статического маршрута

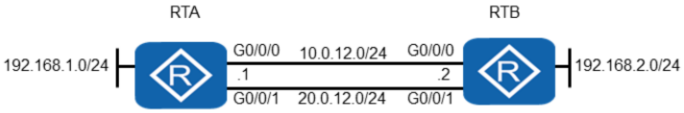
```
[RTB]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public         Destinations : 13        Routes : 14
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

                                ......
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
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Для проверки результатов выполнения команды *display ip routing-table* после конфигурирования статических маршрутов можно запросить таблицу маршрутизации, в которой будет отображен статический маршрут. В результате выполнения команды на экране появятся две записи для одного пункта назначения с соответствующими значениями приоритета и метрики. Различные адреса следующего узла и изменения в исходящем интерфейсе определяют два выбранных пути и подтверждают, что балансировка нагрузки достигнута.

Плавающие статические маршруты




```
[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 20.0.12.1
                    preference 100
```

- Плавающие статические маршруты обеспечивают альтернативный маршрут в случае отказа основного статического маршрута.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.
HUAWEI

Для достижения необходимых требований маршрутизации настройки статических маршрутов можно изменять. Например, изменить значение приоритета, чтобы конкретный статический маршрут имел предпочтение выбора перед другим, или при использовании с другими протоколами приоритет отдавался статическому маршруту или альтернативному протоколу маршрутизации.

Значение приоритета по умолчанию для статического маршрута равно 60, поэтому статический маршрут, у которого данное значение будет изменено, можно рассматривать как маршрут, приоритет которого не равен приоритету любого другого маршрута, включая другие статические маршруты. В приведенном примере два статических маршрута существуют в двух физических сегментах локальной сети. Обычно если оба статических маршрута считаются равными, то второму маршруту присваивается меньшее значение приоритета (более высокое значение), в результате чего он будет удален из таблицы маршрутизации. Основным принципом использования плавающего статического маршрута является то, что в случае сбоя основного маршрута, будет использоваться маршрут с меньшим значением приоритета в таблице маршрутизации.

Проверка плавающего 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       GigabitEthernet0/0/0
```

- До отказа основного маршрута в таблице маршрутизации будет указан только основной статический маршрут.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

С помощью команды *display ip routing-table* можно увидеть результаты изменения значения приоритета, которое приведет к использованию плавающего статического маршрута. Обычно в таблице маршрутизации отображаются два маршрута с одинаковой стоимостью, которые определяют один и тот же пункт назначения, но имеют разные значения адреса следующего транзитного узла и исходящие интерфейсы. Однако в данном случае можно увидеть только один экземпляр, содержащий значение приоритета статического маршрута по умолчанию, равное 60. Поскольку второй статический маршрут теперь имеет значение приоритета 100, он не сразу будет включен в таблицу маршрутизации, поскольку он больше не считается оптимальным маршрутом.

Проверка плавающего статического маршрута

```
[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
```

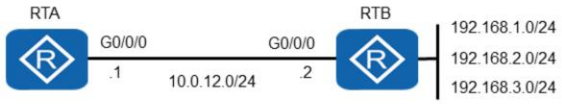
- При отключении основного маршрута в таблицу маршрутизации добавляется плавающий статический маршрут.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

В случае сбоя основного статического маршрута в результате неисправности физического канала или из-за отключения интерфейса, статический маршрут больше не сможет предоставлять маршрут к предполагаемому пункту назначения и поэтому будет удален из таблицы маршрутизации. Плавающий статический маршрут, вероятно, станет следующим оптимальным путем достижения планируемого пункта назначения и будет добавлен в таблицу маршрутизации в качестве второго альтернативного пути передачи пакетов к планируемому пункту назначения. Это гарантирует бесперебойность передачи в условиях любого отказа.

Как только физическое соединение для исходного маршрута будет восстановлено, активный статус текущего плавающего статического маршрута перейдет к данному исходному маршруту, запись которого будет восстановлена в таблице маршрутизации, в результате чего плавающий статический маршрут перейдет в резервный статус.

Статические маршруты по умолчанию




```
[RTA]ip route-static 0.0.0.0 0.0.0.0 10.0.12.2
```

- Маршрут по умолчанию является последним доступным ресурсом в том случае, если в таблице маршрутизации не будет найдено других маршрутов с префиксом наибольшей длины.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Статический маршрут по умолчанию – это специальный статический маршрут, который используется в сетях, в которых адрес назначения неизвестен. Это необходимо для того, чтобы обеспечить доступность пути передачи. Это эффективное средство направления трафика в неизвестный пункт назначения к маршрутизатору или шлюзу, которым может быть известно о пути передачи в корпоративной сети.

Маршрут по умолчанию основан на адресе «любой сети» 0.0.0.0 для поиска любой такой сети, в отношении которой не удалось найти совпадение в таблице маршрутизации, и предоставляет путь передачи по умолчанию, на который следует направлять пакеты для всех неизвестных сетевых пунктов назначения. В этом примере в RTA был реализован статический маршрут по умолчанию, который определяет, что в случае получения пакетов для неизвестной сети такие пакеты должны быть направлены в пункт назначения 10.0.12.2.

С точки зрения принятия решений в таблице маршрутизации, для маршрута по умолчанию, используемого в качестве статического маршрута, установлено значение приоритета 60. Это последний ресурс с точки зрения правила поиска совпадения с префиксом наибольшей длины в процессе поиска маршрута.

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
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

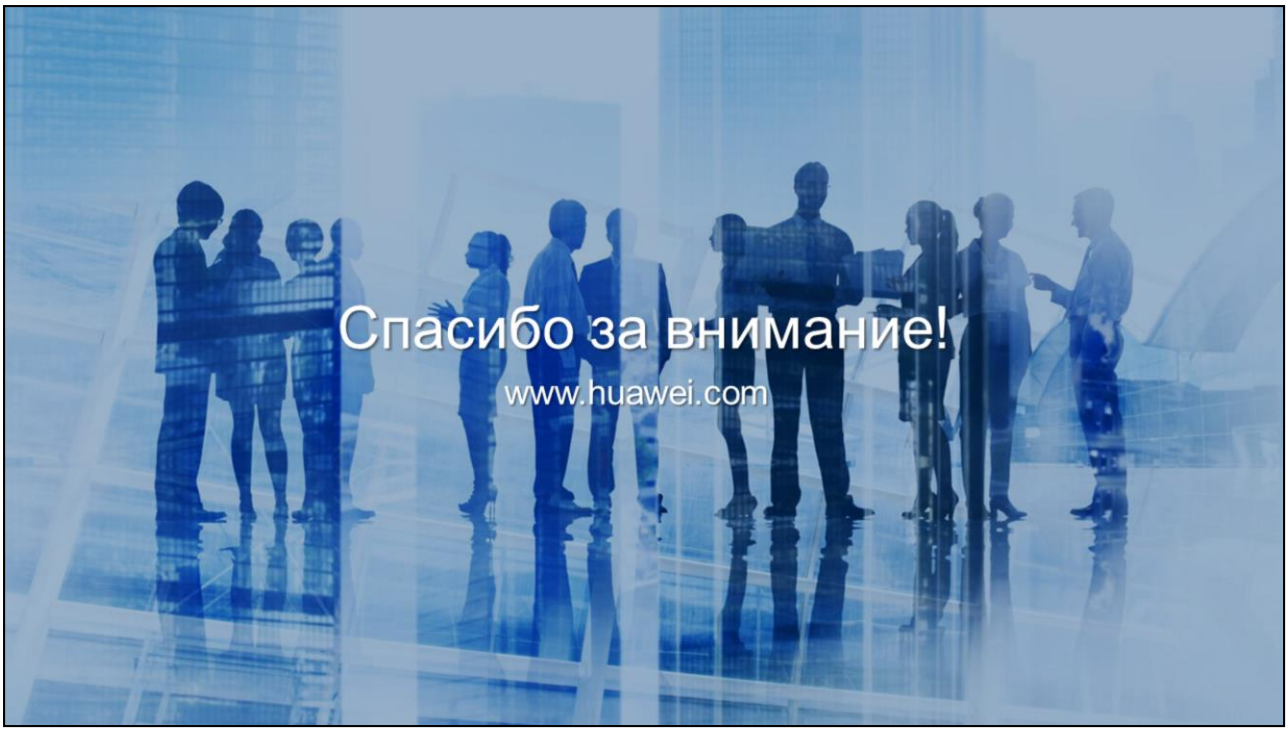
После конфигурации статический маршрут появится в таблице маршрутизации маршрутизатора. Для просмотра данной подробной информации используется команда *display ip routing-table*. В результате все маршруты в данном примере, которые не связаны с какими-либо другими маршрутами в таблице маршрутизации, будут перенаправлены в пункт назначения с адресом следующего транзитного узла 10.0.12.2 через интерфейс Gigabit Ethernet 0/0/0.

Вопросы

- Что следует изменить, чтобы статический маршрут стал плавающим статическим маршрутом?
- Какой сетевой адрес должен быть определен, чтобы статический маршрут по умолчанию был указан в таблице маршрутизации?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

1. Плавающий статический маршрут реализуется путем настройки значения приоритета статического маршрута, когда оба статических маршрута поддерживают механизм балансировки нагрузки.
2. Статический маршрут по умолчанию можно определить в таблице маршрутизации, указав адрес «любой сети» 0.0.0.0 в качестве адреса назначения вместе с адресом следующего транзитного узла интерфейса, на который должны пересылаться пакеты по этому статическому маршруту по умолчанию.


Спасибо за внимание!
www.huawei.com

Маршрутизация с учетом состояния канала с помощью протокола OSPF

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

OSPF — это протокол внутреннего шлюза (IGP), разработанный для IP-сетей и основанный на принципах маршрутизации с учетом состояния канала. Алгоритм учета состояния канала связи дает множество альтернативных преимуществ для средних и даже крупных корпоративных сетей. В данном разделе вы познакомитесь с применением алгоритма в IGP, а также узнаете принципы сходимости, применяемые в протоколе OSPF, принципы реализации OSPF. Эти знания необходимы для поддержки работы OSPF в корпоративных сетях.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

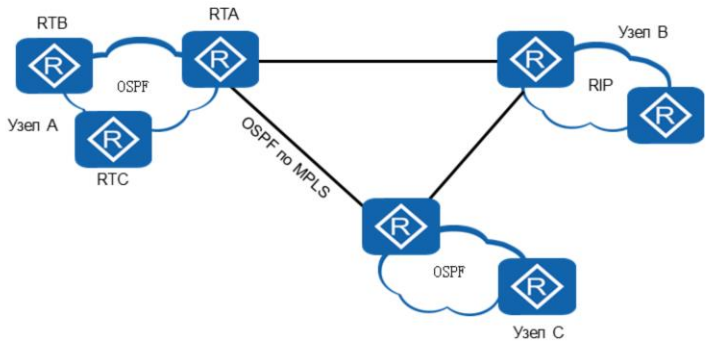
Цели

По окончании данного курса слушатели смогут:

- Объяснять процесс сходимости OSPF.
- Описывать различные типы сетей, поддерживаемые OSPF.
- Успешно конфигурировать сети в одной зоне OSPF.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Протокол выбора кратчайшего пути (OSPF)

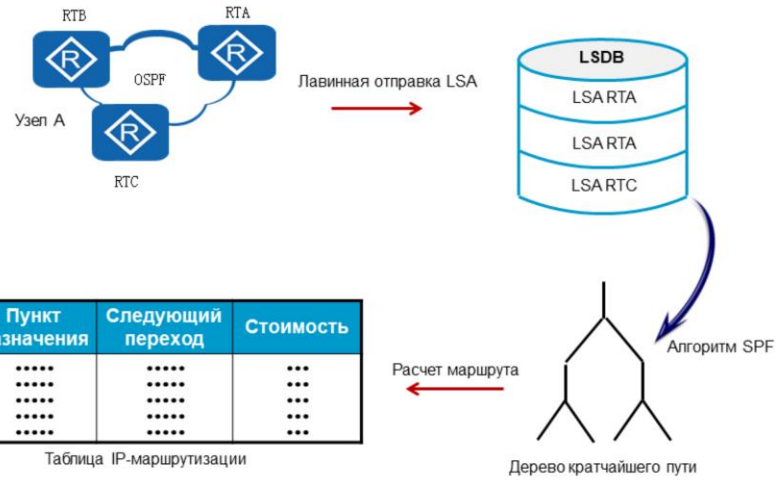


- Минимальный трафик маршрутизации
- Быстрая сходимость
- Масштабируемость
- Точные метрики маршрутов

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Протокол выбора кратчайшего пути или OSPF является протоколом, в котором применяется алгоритм маршрутизации с учетом состояния канала, который способен быстро обнаруживать топологические изменения в автономной системе и устанавливать маршруты без петель за короткий промежуток времени с задействованием минимального объема дополнительной служебной информации, необходимой для согласования изменений топологии между равноправными маршрутизаторами. OSPF также решает проблемы масштабируемости, которые возникают, когда число соединений между растущим числом маршрутизаторов становится настолько большим, что становится причиной нестабильности в автономной системе. Решение данной проблемы достигается за счет использования зон, ограничивающих возможность взаимодействия маршрутизатора (только с изолированной группой) в автономной системе, благодаря чему OSPF поддерживает малые, средние и даже большие сети. Протокол также может работать «поверх» других протоколов, таких как MPLS (протокол коммутации по меткам), чтобы обеспечить масштабируемость сети даже в отношении географически разнесенных узлов. С точки зрения определения оптимального пути, OSPF предоставляет расширенные метрики маршрутов, которые обеспечивают большую точность, чем метрики маршрутов, применяемые в таких протоколах, как RIP. Это необходимо для обеспечения оптимизации маршрутов в отношении не только расстояния, но и скорости канала.

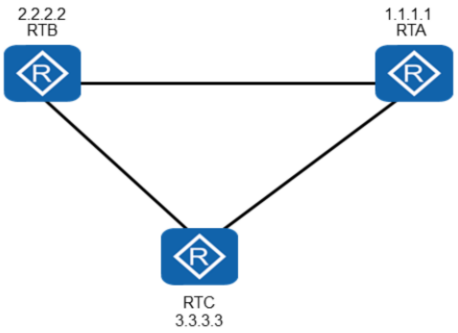
Сходимость в OSPF



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Для достижения сходимости OSPF необходимо, чтобы каждый и любой маршрутизатор, работающий по протоколу OSPF, имел информацию о состоянии всех интерфейсов и смежностей (отношения между подключенными маршрутизаторами), которая поможет установить наилучший путь к каждой сети. Изначально это достигается путем лавинной рассылки объявлений о состоянии канала (LSA), которые представляют собой блоки таких данных, как известные сети и состояния каналов для каждого интерфейса в домене маршрутизации. Каждый маршрутизатор будет использовать полученное LSA для формирования базы данных состояний каналов (LSDB), которая является основой создания дерева кратчайших путей к каждой сети, маршруты из которых, в конечном итоге, будут включены в таблицу IP-маршрутизации.

Идентификатор маршрутизатора



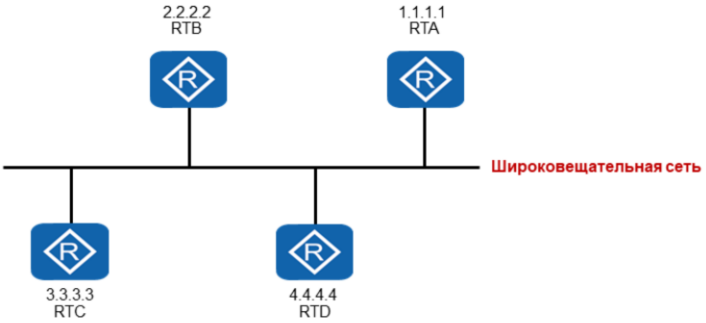
- Идентификатор маршрутизатора (Router ID) – это 32-битное значение, используемое для идентификации каждого маршрутизатора, работающего по протоколу OSPF.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Идентификатор, назначаемый каждому маршрутизатору, работающему по протоколу OSPF представляет собой 32-битное значение. Данное значение однозначно определяет маршрутизатор в автономной системе. Идентификатор маршрутизатора можно настроить вручную или получить из сконфигурированного адреса. Если логический (loopback) интерфейс сконфигурирован, то идентификатор маршрутизатора будет построен на базе IP-адреса сконфигурированного логического интерфейса самого высокого уровня, если существует несколько логических интерфейсов.

Если логические интерфейсы не сконфигурированы, то маршрутизатор будет использовать IP-адрес, сконфигурированный для физического интерфейса, самого высокого уровня. Перезапуск любого маршрутизатора, работающего по протоколу OSPF, можно выполнить с помощью функции «мягкого» перезапуска, чтобы обновить ID маршрутизатора, если будет сконфигурирован новый идентификатор. Настройку ID маршрутизатора рекомендуется выполнять вручную, чтобы избежать непредвиденных изменений идентификатора маршрутизатора в случае изменения адреса интерфейса.

Типы сетей, поддерживаемые OSPF

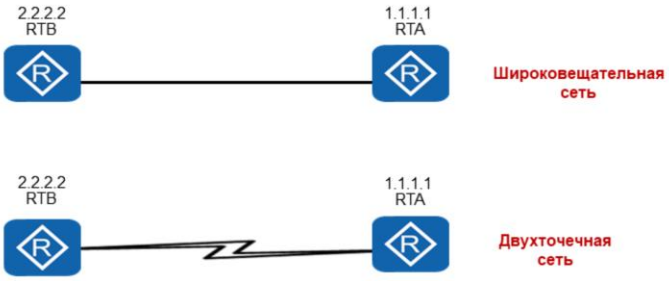


- Сети на базе Ethernet используют по умолчанию широковещательный тип передачи.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

OSPF поддерживает сети разного типа, в отношении которых применяются разные подходы к формированию отношений между соседями и организации связи. Ethernet – это форма широковещательной сети, в которой задействованы несколько маршрутизаторов, подключенных к одному сегменту сети. Одна из основных задач заключается в организации связи между соседними маршрутизаторами таким образом, чтобы минимизировать ресурсы маршрутизации OSPF, занимаемые служебными данными. Если Ethernet-сеть установлена, то в OSPF будет автоматически применяться тип широковещательной сети.

Типы сетей, поддерживаемые OSPF

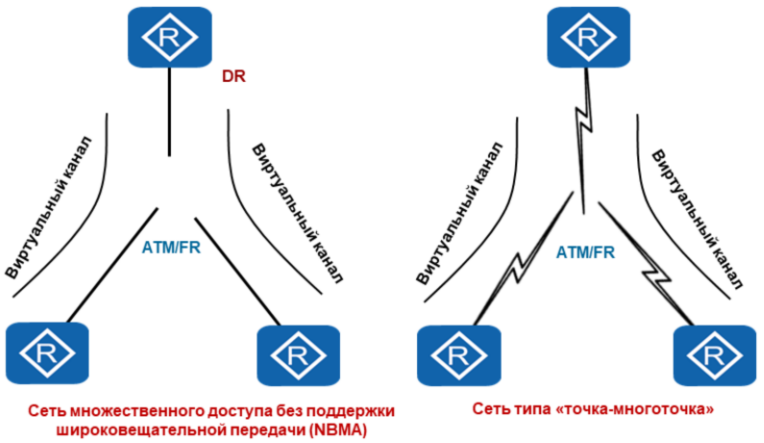


- Для двухточечной сети по умолчанию будут использоваться технологии последовательной передачи, такие как PPP и HDLC.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Если два маршрутизатора соединены с помощью топологии «точка-точка», то используемый тип сети будет зависеть от применяемой среды передачи и технологии, применяемой на канальном уровне. Как уже упоминалось, при использовании Ethernet-среды для OSPF будет автоматически назначен тип широковещательной сети. При использовании физической среды с последовательной передачей используется двухточечная сеть. Протоколы, которые работают в среде последовательной передачи на канальном уровне —протокол двухточечной связи (PPP) и высокоуровневый протокол управления каналом (HDLC).

Типы сетей, поддерживаемые OSPF



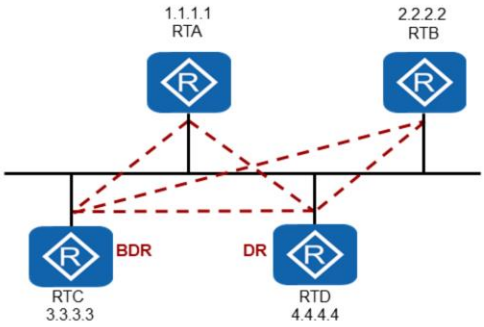
- По умолчанию в сети NBMA используются технологии ATM и Frame Relay.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

OSPF может работать в сетях множественного доступа, которые не поддерживают широковещательную передачу. Такими сетями являются Frame Relay и ATM, которые обычно организуются по топологии «звезда» (Hub-and-Spoke) с использованием виртуальных каналов. OSPF поддерживает два типа сетей, которые могут применяться к каналам, подключенным к таким средам. Тип сети NBMA (сеть множественного доступа без поддержки широковещательной передачи) эмулирует широковещательную сеть и поэтому требует, чтобы каждый интерфейс равноправного узла принадлежал тому же сегменту сети. В отличие от широковещательной сети, NBMA пересылает пакеты OSPF как одноадресные. Поэтому необходимо, чтобы для каждого пункта назначения было сгенерировано несколько экземпляров одного и того же пакета.

Для каждого интерфейса может также использоваться тип сети «точка-многоточка», и в этом случае применяется принцип соединения «точка-точка». Это означает, что каждый интерфейс равноправного узла должен быть связан с разными сетевыми сегментами. Выделенные маршрутизаторы (Designated Routers; DR) ассоциируются с широковещательными сетями и реализуются в сетях NBMA. Наиболее важным является позиционирование DR, которое должно быть назначено на узле-концентраторе архитектуры «звезда», чтобы все узлы могли обмениваться данными с таким DR.

Выделенный маршрутизатор и резервный выделенный маршрутизатор



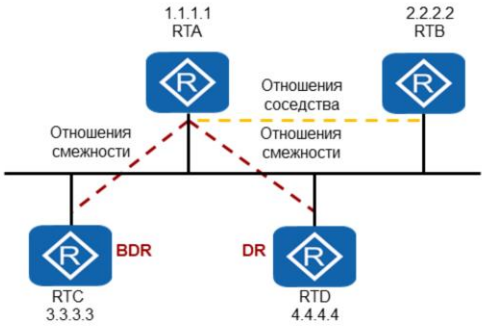
- Выделенные маршрутизаторы ограничивают количество отношений смежности в сетях широковещательной передачи (Ethernet).

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Для адресации и оптимизации OSPF-маршрутов в широковещательных сетях OSPF использует выделенный маршрутизатор (DR), который действует как центральная точка связи для всех остальных маршрутизаторов, ассоциированных с широковещательной сетью, по меньшей мере, на одном интерфейсе. В теоретической широковещательной сети, в которой не используется DR, маршрут рассчитывается по формуле: n(n-1)/2, где n – это количество интерфейсов маршрутизатора, участвующих в процессе OSPF. В приведенном примере используются 6 смежных соединений между всеми маршрутизаторами. При использовании DR, все маршрутизаторы устанавливают связь с таким DR, который функционирует в качестве центральной точки связи для всех соседних маршрутизаторов в широковещательной сети.

Резервный выделенный маршрутизатор (BDR) – это маршрутизатор, который выбирается для переключения с DR в случае сбоя. По существу, необходимо, чтобы BDR устанавливал базу данных состояния канала как DR для обеспечения синхронизации. Это означает, что все соседние маршрутизаторы также должны связываться с BDR в широковещательной сети. С применением DR и BDR количество ассоциаций уменьшается с 6 до 5, поскольку RTA и RTB должны связываться только с DR и BDR. Может показаться, что это не существенно, однако когда это используется в сети, содержащей, например, 10 маршрутизаторов, то есть (10*9)/2, то в результате эффективность использования такого подхода становится очевидной.

Состояния соседства



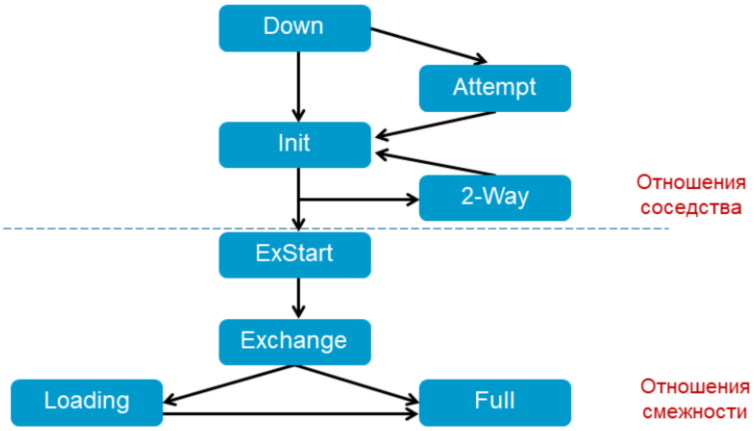
- Данное состояние определяет форму отношений между соседями.
- Возможны два типа отношений: отношения соседства и отношения смежности.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Для обмена маршрутной информацией OSPF создает отношения смежности между соседними маршрутизаторами. Не каждые два соседних маршрутизатора станут смежными, особенно если один из двух маршрутизаторов, устанавливающих отношения смежности, не является DR или BDR. Эти маршрутизаторы, называемые DROther, только уведомляют о своем присутствии, но не устанавливают полное соединение. Это называется отношение соседства. Однако маршрутизаторы DROther формируют отношения полной смежности с маршрутизаторами DR и BDR, чтобы обеспечить синхронизацию базы данных состояний каналов маршрутизаторов DR и BDR с каждым из маршрутизаторов DROther. Такая синхронизация достигается путем установления отношений соседства с каждым DROther.

Отношения смежности связаны с сетью, являющейся общей для двух маршрутизаторов. Если два маршрутизатора имеют несколько общих сетей, они могут иметь несколько отношений смежности между ними.

Установка состояния канала



- Изменение состояния позволяет достичь отношений соседства.

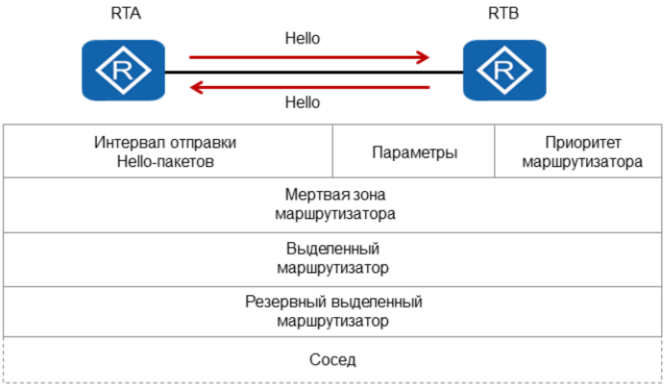
Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Для достижения отношений соседства или смежности каждый маршрутизатор, участвующий в OSPF, будет проходить через несколько состояний канала. Все маршрутизаторы после инициализации находятся в состоянии down и проходят процесс обнаружения соседей, который включает в себя, во-первых, информирование о присутствии маршрутизаторов в сети OSPF через отправку Hello-пакетов. При выполнении данного действия маршрутизатор перейдет в состояние init.

Как только маршрутизатор получит ответ в виде Hello-пакета, содержащего идентификатор маршрутизатора, получающего ответ, будет достигнуто состояние двустороннего обмена (2-Way) и сформированы отношения соседства. В сетях NBMA состояние attempt достигается, когда связь с соседом становится неактивной, и предпринимается попытка восстановить связь посредством периодической отправки Hello-пакетов. Маршрутизаторы, которые не достигли отношений смежности, останутся в состоянии соседства в режиме двустороннего обмена.

Маршрутизаторы, такие как DR и BDR, будут создавать отношения смежности со всеми другими соседними маршрутизаторами и поэтому должны обмениваться информацией о состоянии канала для создания полной базы данных состояния канала. Для этого необходимо, чтобы равноправные маршрутизаторы, которые устанавливают отношения смежности, сначала выполнили согласование для обмена информацией о состоянии канала (ExStart), прежде чем приступить к обмену сводной информацией о сетях, о которые им известно. Соседи могут идентифицировать маршруты, о которых они либо не знают, либо не имеют актуальной информации, и поэтому они запрашивают дополнительную информацию об этих маршрутах, что приводит к повышению нагрузки. Полностью синхронизированные отношения между соседями определяются состоянием full, при котором оба равноправных маршрутизатора могут считаться смежными.

Обнаружение соседей



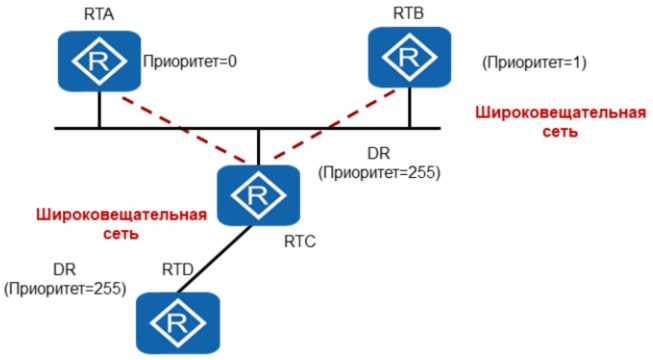
- Пакет Hello отвечает за обнаружение и обслуживание соседей с целью достижения двусторонней связи между соседями.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Обнаружение соседей достигается за счет отправки Hello-пакетов, которые генерируются с определенными интервалами, в зависимости от таймера, для которого по умолчанию установлено значение 10 секунд для широковещательных сетей и сетей типа «точка-точка»; в то время как для сетей NBMA и сетей типа «точка-многоточка» интервал отправки Hello-пакетов составляет 30 секунд. Hello-пакеты содержат этот интервал, а также поле приоритета маршрутизатора, по которому соседи могут найти соседа с наивысшим идентификатором для распознания DR и BDR в широковещательных сетях и сетях NBMA.

Также необходимо определить период срока действия Hello-пакетов, прежде чем отношение соседства будет считаться потерянным. Данный параметр определяется мертвой зоной маршрутизатора в Hello-пакете. Для данного интервала мертвой зоны по умолчанию установлено значение в четыре раза больше интервала отправки Hello-пакета. Он составляет 40 секунд для широковещательных сетей и двухточечных сетей и 120 секунд для сетей NBMA и сетей типа «точка-многоточка». Кроме того, если необходимо, передаются идентификаторы как DR, так и BDR на базе сети, для которой генерируется Hello-пакет.

Выбор выделенного маршрутизатора




```
[RTD]interface GigabitEthernet0/0/0
[RTD-GigabitEthernet0/0/0]ospf network-type p2p
```

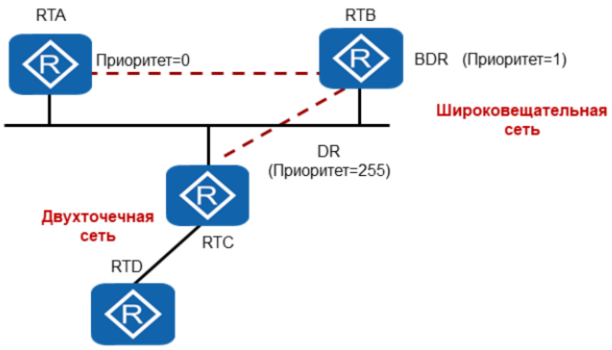
- Выделенный маршрутизатор выбирается в зависимости от значения приоритета.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

После обнаружения соседей может выполняться процедура выбора DR. Это зависит от типа сети сетевого сегмента — выбор осуществляют широковещательные сети и сети NMBA. Выбор DR зависит от приоритета, назначенного каждому интерфейсу, который участвует в данной процедуре. По умолчанию установлено значение приоритета 1, и чем выше приоритет, тем оптимальнее DR-кандидат.

Если установлен приоритет 0, то интерфейс больше не будет участвовать в выборе маршрутизатора в качестве DR или BDR. Может случиться так, что если двухточечные соединения (с использованием Ethernet в качестве физической среды передачи) настроены на поддержку широковещательного типа сети, то произойдет выбор ненужного DR, которое приведет к появлению избыточного трафика протокола. Поэтому рекомендуется сконфигурировать тип сети «точка-точка».

Выбор резервного выделенного маршрутизатора



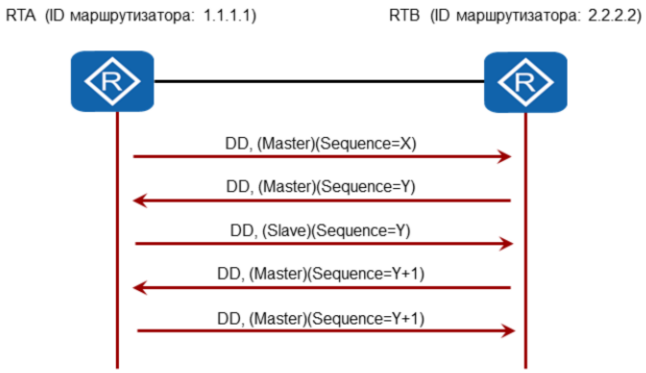
- Резервный выделенный маршрутизатор (BDR) формирует отношения смежности со всеми остальными маршрутизаторами и переходит в статус DR в случае сбоя активного DR.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Для повышения эффективности перехода к новому выделенному маршрутизатору (DR) в каждой широковещательной сети и сети NBMA назначается резервный маршрутизатор (BDR). Резервный выделенный маршрутизатор также является смежным для всех маршрутизаторов сети и переходит в статус DR в случае отказа текущего активного выделенного маршрутизатора. Без BDR пришлось бы формировать новые отношения смежности между новым выделенным маршрутизатором и всеми остальными маршрутизаторами, подключенными к сети.

Часть процесса формирования отношений смежности включает в себя синхронизацию баз данных состояний каналов, что потенциально может занять довольно много времени. В течение этого времени сеть не будет доступна для передачи данных. Резервный выделенный маршрутизатор устраняет необходимость формирования этих отношений смежности, поскольку они уже существуют. Это означает, что период прерывания передачи транзитного трафика будет длиться столько времени, сколько требуется для лавинной отправки новых LSA (которые объявляют о новом выделенном маршрутизаторе). Выбор резервного выделенного маршрутизатора также выполняется при помощи отправки Hello-пакетов. Каждый Hello-пакет имеет поле, в котором указывается резервный выделенный маршрутизатор для сети.

Синхронизация базы данных



- Соседние маршрутизаторы формируют отношения ведущий-ведомый.
- Пакеты Database Description содержат информацию заголовка LSA.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

В алгоритме маршрутизации с учетом состояния канала очень важно, чтобы базы данных состояния канала всех маршрутизаторов оставались синхронизированными. OSPF упрощает это, требуя синхронизации БД только соседних маршрутизаторов. Процесс синхронизации начинается, как только маршрутизаторы пытаются установить отношения смежности. Каждый маршрутизатор описывает свою базу данных, отправляя последовательность пакетов Database Description своему соседу. Каждый пакет Database Description описывает набор LSA, принадлежащих базе данных маршрутизатора.

Когда сосед видит более новый LSA, чем тот, который имеется в собственной копии базы данных, он отмечает, что необходимо запросить этот более новый LSA. Такая отправка и получение пакетов Database Description называется «процессом обмена базами данных». Во время этого процесса два маршрутизатора формируют отношения «ведущий-ведомый». Каждый пакет Database Description имеет порядковый номер. Пакеты Database Description, отправленные ведущим маршрутизатором, подтверждаются ведомым маршрутизатором путем отправки порядкового номера в ответном сообщении.

Установление полной смежности

- Запрос недостающих или новых экземпляров LSA выполняется с помощью LSR.
  - Вся запрошенные LSA отправляется в качестве обновленных данных.

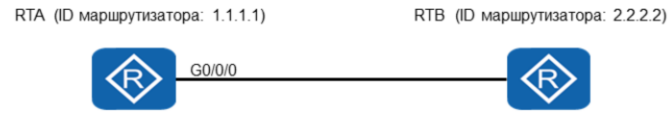
Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Во время и после процесса обмена базами данных каждый маршрутизатор имеет список тех LSA, для которых у соседа есть больше актуальных экземпляров. Пакет запроса состояния канала используется для запроса более актуальных экземпляров базы данных соседа. Может потребоваться использование нескольких пакетов запроса состояния канала.

Пакеты обновления состояния канала (Link State Update) выполняют лавинную отправку LSA. Каждый такой пакет передает набор LSA на один узел дальше от их узла-источника. В один пакет могут быть включены несколько LSA. В широковещательных сетях пакеты Link State Update являются многоадресными. IP-адрес пункта назначения, указанный для такого пакета, зависит от состояния интерфейса. Если состояние интерфейса DR или Backup, то используется адрес AllSPFRouters (224.0.0.5). В противном случае следует использовать адрес AllDRouters (224.0.0.6). В не широковещательных сетях отдельные пакеты обновления состояния канала должны отправляться одноадресной передачей каждому смежному соседу (т.е. находящемуся в состоянии Exchange или выше). IP-адреса пунктов назначения для этих пакетов являются IP-адресами соседей.

Когда процесс описания базы данных будет завершен, и все запросы состояния канала будут выполнены, базы данных будут считаться синхронизированными, а маршрутизаторы будут считаться полностью смежными. На данный момент смежность будет полностью функциональной и она объявляется в LSA двух маршрутизаторов.

Метрика OSPF




```
[RTA]interface GigabitEthernet 0/0/0
[RTA-GigabitEthernet0/0/0]ospf cost 20
```

```
[RTB]ospf
[RTB-ospf-1]bandwidth-reference 10000
```

- Стоимость метрики рассчитывается по формуле 10^8/полоса пропускания.
- Использование команды *bandwidth reference* повышает точность расчета метрики.

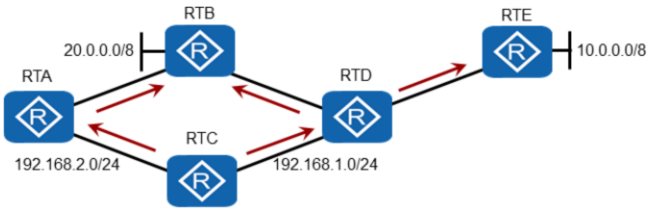
Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.
HUAWEI

OSPF вычисляет стоимость интерфейса на базе полосы пропускания интерфейса. Для расчета используется следующая формула: стоимость интерфейса = эталонное значение полосы пропускания/полоса пропускания. Эталонное значение полосы пропускания можно настроить. По умолчанию установлено значение 100 Мбит/с. При использовании формулы 100000000/полоса пропускания, метрика стоимости будет 1562 для последовательного порта 64 кбит/с, 48 для интерфейса E1 (2,048 Мбит/с) и 1 для Ethernet (100 Мбит/с) или выше.

Чтобы различать высокоскоростные интерфейсы, необходимо, чтобы метрика стоимости была скорректирована в соответствии с поддерживаемыми в настоящее время скоростями. Команды bandwidth-reference позволяют изменять метрику путем изменения эталонного значения полосы пропускания в формуле стоимости. Чем выше значение, тем более точной является метрика. Там, где поддерживаются скорости 10 Гб, рекомендуется увеличить эталонное значение полосы пропускания до «10000» или 1010/полоса пропускания, чтобы обеспечить метрики стоимости 1, 10 и 100 для каналов с полосой пропускания 10 Гб, 1 Гб и 100 Мб, соответственно.

Чтобы определить значение стоимости для данного интерфейса, метрику стоимости можно указать вручную с помощью команды ospf cost. Метрика стоимости находится в диапазоне от 1 до 65535, при этом по умолчанию установлено значение 1.

Дерево кратчайшего пути



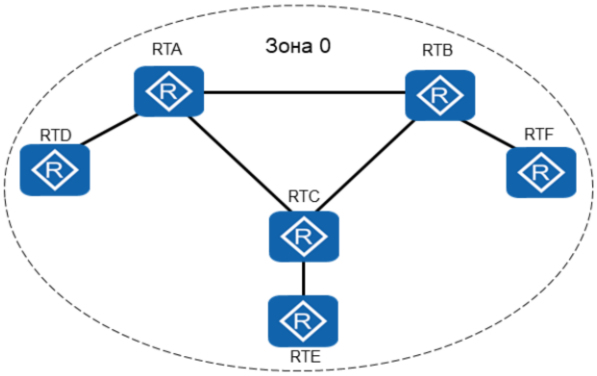

```
[RTC]display ip routing-table
......
Destination/Mask  Proto  Pre  Cost      Flags NextHop         Interface
      10.0.0.0/8  OSPF   10   20          D   192.168.1.4     G0/0/0
      20.0.0.0/8  OSPF   10   20          D   192.168.1.4     G0/0/0
                  OSPF   10   20          D   192.168.2.1     G0/0/1
```

- Каждый маршрутизатор вычисляет кратчайший путь ко всем другим сетям.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Считается, что маршрутизатор, который достиг статуса full, получил все объявления о состоянии канала (LSA) и синхронизировал свою базу данных состояний канала (LSDB) с базой данных смежных соседей. Информация о состоянии канала, собранная в базе данных состояний канала, затем используется для вычисления кратчайшего пути к каждой сети. Каждый маршрутизатор, чтобы выполнить независимый расчет кратчайшего пути к каждому пункту назначения, полагается только на информацию в LSDB, а не на информацию от равноправных узлов, которая по предположению является лучшим маршрутом к пункту назначения. Однако необходимость вычисления дерева кратчайшего пути означает, что каждый маршрутизатор должен использовать дополнительные ресурсы для выполнения этой операции.

OSPF в сети с одной зоной

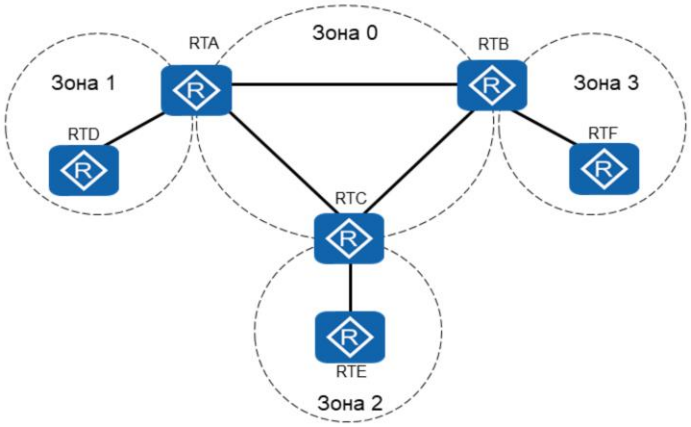


- Единая база данных состояния канала для административного домена.
  - Для зоны может быть назначен любой номер, но рекомендуется 0.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Небольшие сети могут выбирать количество маршрутизаторов, которые будут работать в составе домена OSPF. Эти маршрутизаторы считаются частью зоны, которая представлена идентичной базой данных состояния каналов для всех маршрутизаторов в домене. В сетях с одной зоной OSPF может быть назначен любой номер зоны, однако для будущей реализации рекомендуется, чтобы этой зоне был назначен номер 0.

OSPF в сети с несколькими зонами



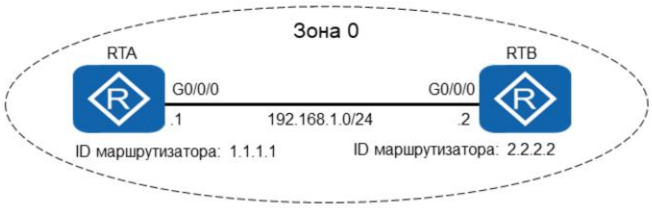
- В зонах создаются отдельные базы данных LS, что сводит к минимуму влияние каких-либо изменений.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Процессы передачи объявлений о состоянии канала и последующего вычисления кратчайшего пути на основе базы данных о состоянии канала все больше усложняются, поскольку все большее количество маршрутизаторов входят в состав домена OSPF. Для ограничения размера базы данных состояния канала и количества вычислений, которые должны быть выполнены при определении кратчайшего пути к данной сети, OSPF поддерживает иерархическую структуру.

Реализация нескольких зон позволяет разделить процесс вычисления в домене OSPF на основе базы данных состояния канала, которая формируется отдельно для каждой зоны, но предоставляет информацию для достижения всех пунктов назначения в домене OSPF. Некоторые маршрутизаторы, известные как пограничные маршрутизаторы зоны (ABR), работают между зонами и содержат базы данных состояний каналов отдельно для каждой зоны, к которой подключаются. Зона 0 должна быть сконфигурирована в месте пересечения всех зон OSPF, и весь трафик, передаваемый между зонами, обычно пересекает зону 0, что предупреждает возникновение петель маршрутов.

Объявление сети OSPF




```
[RTA]ospf 1 router-id 1.1.1.1
[RTA-ospf-1]area 0
[RTA-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255
```

- Команда *network* определяет сеть, которая будет объявлена.
- Объявления о маршруте передаются в соответствии с зоной.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

При установке OSPF в домене AS необходимо включить процесс OSPF на каждом маршрутизаторе, который будет участвовать в этом процессе. Это достигается с помощью команды ospf [process id], где process id – это указываемый идентификатор процесса, с которым связан маршрутизатор. Если маршрутизаторам будут назначены разные идентификаторы, то каждого отдельного идентификатора будут созданы отдельные базы данных состояний каналов. Если идентификатор процесса не будет назначен, будет использоваться значение по умолчанию, равное 1. ID маршрутизатора также можно назначить с помощью команды ospf [process id] [router-id <router-id>], где <router-id> – это значение идентификатора, при этом более высокие значения присваиваются выделенным маршрутизаторам (DR) в широковещательных сетях и сетях NBMA.

Информация в скобках означает процесс и уровень ospf, на которых можно сконфигурировать параметры ospf, включая зону, к которой привязан каждый канал (или интерфейс). Сети, которые должны быть объявлены в данной зоне, определяются с помощью сетевой команды. Маска представлена в виде шаблона, в котором битовое значение 0 означает, что биты являются фиксированными (например, идентификатор сети). Если битовое значение 1, в качестве адреса может быть установлено 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 ]
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Конфигурация отношений соседства между равноправными узлами OSPF проверяется с помощью команды display ospf peer. Для четкого понимания конфигурации представлены атрибуты, связанные с соединением между равноправными узлами. Атрибуты включают зону, в которой установлено соединение между равноправными узлами, статус установления соединения, ассоциацию главный-подчиненный для согласования смежности и достижения статуса full, а также DR и BDR, которые указывают на ассоциацию канала с сетью широковещательной передачи.

Аутентификация OSPF


```
[RTA]interface GigabitEthernet0/0/0
[RTA-GigabitEthernet0/0/0]ospf authentication-mode md5 1 huawei
```

- OSPF поддерживает два метода аутентификации: простой по паролю и с использованием криптографических средств.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

OSPF поддерживает обязательное прохождение процедуры аутентификации, обеспечивая защиту маршрутов от вредоносных действий, направленных на изменение или повреждения существующей топологии OSPF и маршрутов. OSPF позволяет использовать как простой метод аутентификации, так и так и сложный метод с использованием криптографических средств, который обеспечивает улучшенную защиту от потенциальных атак.

Аутентификация настраивается для каждого интерфейса. Для простого метода используется команда ospf authentication-mode { simple [[plain] <plain-text> | cipher <cipher-text >] | null }, где plain – это пароль в виде открытого текста, cipher – это пароль в виде зашифрованного текста, и null означает отсутствие аутентификации.

Для криптографического метода используется команда ospf authentication-mode { md5 | hmac-md5 } [key-id { plain <plain-text >| [cipher] <cipher-text >}]. MD5 представляет собой криптографический алгоритм для обеспечения аутентификации по каналу, и его настройки показаны в данном примере. Параметр key ID – это уникальный идентификатор ключа аутентификации при прохождении проверки по паролю в виде зашифрованного текста. Значение key ID должно соответствовать значению, указанному на равноправном устройстве.

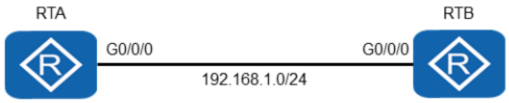
Проверка конфигурации

```
<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): * *
* * * * * *
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Для просмотра процесса аутентификации можно запустить отладку на терминале. Так как отладка может включать множество событий, должна использоваться команда debugging ospf packet, которая определяет, что данный процесс должен выполняться только в отношении определенных пакетов OSPF. Таким образом, просмотр процесса аутентификации выполняется, чтобы убедиться в успешной настройке данной процедуры.

Интерфейс silent в OSPF




```
[RTA]ospf
[RTA-ospf-1]silent-interface GigabitEthernet0/0/0
```

- Команда *silent-interface* не позволяет интерфейсу формировать отношения соседства с равноправными узлами.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Часто необходимо контролировать поток данных маршрутизации и ограничивать сферу влияния протоколов маршрутизации. Это в особенности необходимо в случае подключения к внешним сетям таким образом, чтобы внешние сети не получали информацию о внутренних маршрутах. Для этого применяется команда silent-interface, которая ограничивает все OSPF-связи через интерфейс, на котором реализована данная команда.

Установленный в режим silent OSPF-интерфейс сможет и дальше объявлять свои прямые маршруты, однако Hello-пакеты на интерфейсе, будут заблокированы, и установление отношений соседства не на интерфейсе будет невозможно. Команда silent-interface [interface-type interface-number] используется для определения конкретного интерфейса, на котором будут ограничены операции протокола OSPF, а для настройки ограничения на всех интерфейсах в рамках определенного процесса используется команда silent-interface all.

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
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

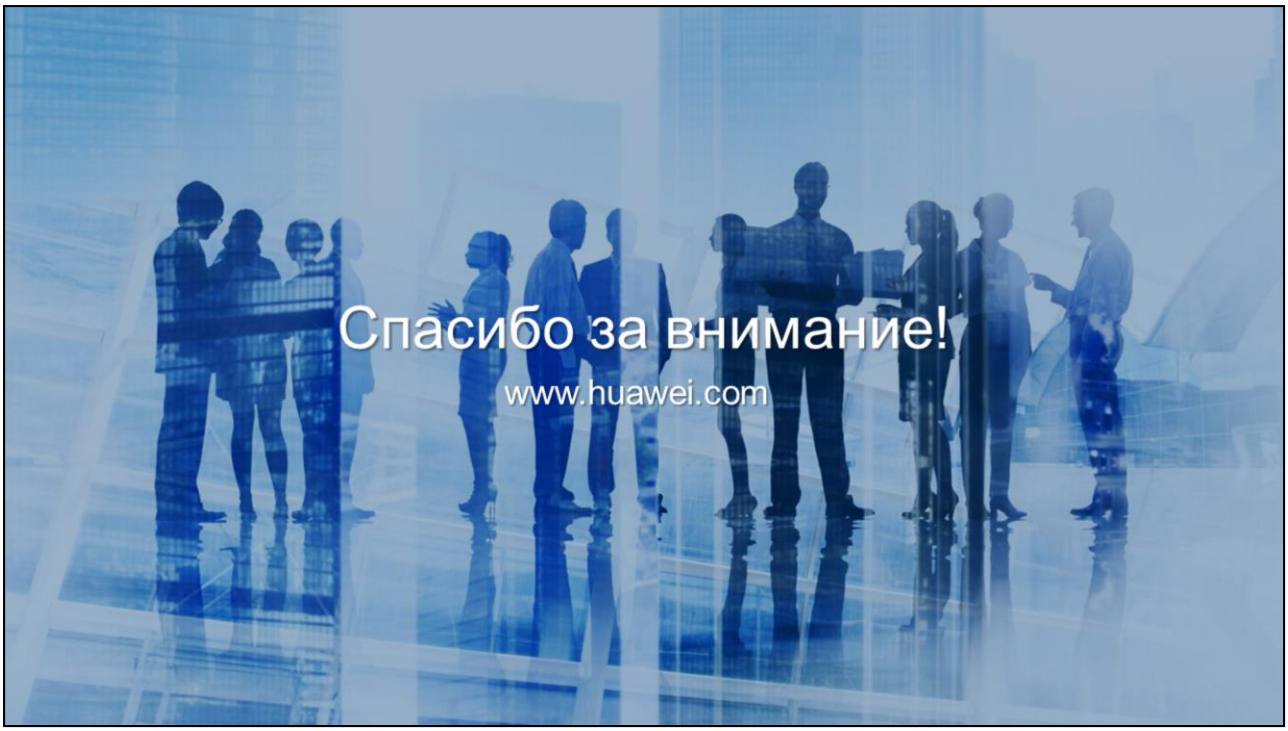
Проверка установки режима silent на каком-либо интерфейсе выполняется с помощью команды *display ospf <process_id> interface <interface>*, где interface – это интерфейс, к которому была применена команда *silent-interface*.

Вопросы

- Для чего используется интервал мертвой зоны в заголовке OSPF?
- Что такое адрес многоадресной передачи в широковещательной сети, который используется выделенным маршрутизатором (DR) и резервным выделенным маршрутизатором (BDR) для прослушивания информации об обновлении состояния канала?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

1. Интервал мертвой зоны – это значение таймера, который используется для определения остановки передачи Hello-пакетов OSPF. Данное значение эквивалентно четырехкратному интервалу Hello или 40 секундам по умолчанию в широковещательных сетях. В случае, если мертвая зона примет нулевое значение, то отношения соседства OSPF будут прекращены.
2. DR и BDR используют адрес многоадресной передачи 224.0.0.6 для прослушивания обновлений состояния канала, когда тип сети OSPF определен как широковещательный.


Спасибо за внимание!
www.huawei.com

Принципы работы протокола DHCP

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

Корпоративная сеть часто может состоять из значительного числа хост-устройств, и для каждого такого устройства необходимо настроить сетевые параметры — IP-адрес и дополнительные данные сети. Ручные операции назначения адреса утомительны и зачастую неточны, что приводит к появлению адресов-дубликатов на конечных станциях или недоступности служб, необходимых для бесперебойной работы сети. DHCP - это протокол прикладного уровня, предназначенный для автоматизации процесса предоставления такой информации о конфигурации клиентам в сети TCP/IP. Таким образом, DHCP помогает обеспечить правильное распределение адресов и снижает объем административных операций во всех корпоративных сетях. В данном разделе описываются методы применения DHCP в корпоративной сети.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

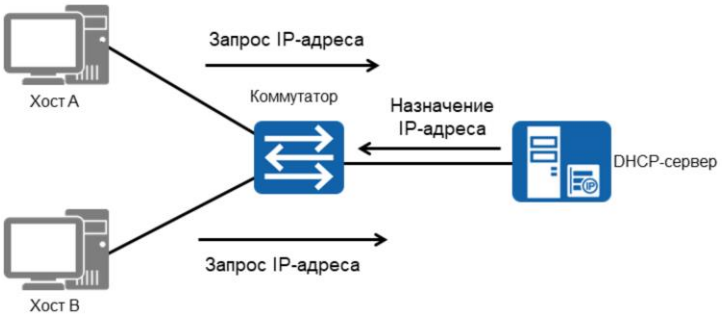
Цели

По окончании данного курса слушатели смогут:

- Описывать функцию DHCP в корпоративной сети.
- Объяснять процесс аренды DHCP.
- Конфигурировать пулы DHCP для аренды адресов.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Применение DHCP в корпоративной сети



- Сети, состоящие из большого числа пользователей, требуют централизованной системы управления, которая будет назначать IP-адреса.

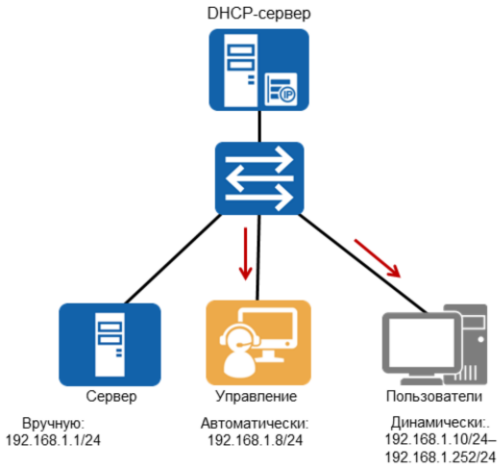
Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Корпоративные сети часто состоят из нескольких конечных систем, для которых необходимо назначить IP-адрес, чтобы такие системы могли подключаться к сегменту сети, к которому они привязаны. В небольших сетях с минимальным количеством конечных систем, подключенных к сети, легко управлять назначением адресов всем конечным системам.

Однако в сетях среднего и крупного масштаба становится все труднее вручную конфигурировать IP-адреса, так как существует большая вероятность их дублирования, а также внесения некорректных данных из-за человеческого фактора, и поэтому все более важной становится необходимость внедрения централизованного решения управления всей сетью. Протокол динамической конфигурации хоста (DHCP) реализован как решение, которое позволяет динамически назначать адреса существующим фиксированным и временным конечным системам, получающим доступ к сетевому домену.

В некоторых случаях в сети может быть больше хостов, чем доступных IP-адресов. В таких сетях фиксированный IP-адрес назначается небольшому числу хостов, а остальные получают их динамически с помощью DHCP-сервера.

Механизмы назначения адресов



- DHCP поддерживает три механизма назначения IP-адресов.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

DHCP поддерживает три механизма назначения IP-адресов. В автоматическом режиме протокол DHCP назначает постоянный IP-адрес клиенту. В динамическом режиме протокол DHCP выделяет IP-адрес клиенту на ограниченный периода времени или, по крайней мере, до тех пор, пока клиент в явной форме не откажется от использования IP-адреса.

Третий механизм подразумевает настройку адреса вручную. IP-адрес клиента назначает сетевой администратор, а DHCP используется только для обработки вручную назначенного клиенту адреса. Динамический режим является единственным из трех механизмов, который позволяет автоматически повторно использовать адрес, который больше не нужен клиенту, которому он был назначен. Таким образом, динамический режим будет оптимален при назначении 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.

Динамический режим также может стать хорошим решением для назначения IP-адреса новому клиенту, постоянно подключенному к сети, в которой количество IP-адресов достаточно ограничено, и восстановление адресов при удалении старых клиентов не выполняется. Ручной режим позволяет использовать DHCP для устранения ошибок в процессе настройки IP-адресов хостов вручную в тех средах, в которых необходимо более точное управление назначением IP-адресов.

Сообщения DHCP

Тип сообщений	Функция
DHCP DISCOVER	Сообщение посылается DHCP-клиентом в широковещательной рассылке в целях поиска доступных DHCP-серверов.
DHCP OFFER	Данное сообщение посылается сервером в ответ на сообщение DHCPDISCOVER и содержит параметры конфигурации.
DHCP REQUEST	Данное сообщение посылается клиентом серверу с целью a) запроса предлагаемых параметров от одного сервера и отказа от предложений от всех остальных, b) подтверждения правильности ранее назначенного адреса после, например, перезагрузки системы или (c) продления срока аренды определенного сетевого адреса.
DHCP ACK	Подтверждение сервера, отправляемое клиенту с параметрами конфигурации, включая назначенный сетевой адрес.
DHCP NAK	Сервер указывает клиенту, что запрашиваемый клиентом сетевой адрес не может быть назначен.
DHCP RELEASE	Клиент возвращает сетевой адрес серверу и отменяет оставшийся срок аренды.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

DHCP-сервер и DHCP-клиент обмениваются данными друг с другом путем обмена сообщениями различного типа. Обмен начинается с передачи сообщения DHCP Discover. DHCP-клиент осуществляет широковещательную рассылку данного сообщения, чтобы найти DHCP-сервер при попытке подключиться к сети в первый раз. В ответ на сообщение DHCP Discover DHCP-сервер отправляет сообщение DHCP Offer, в котором содержится информация о конфигурации.

Затем после инициализации DHCP-клиента отправляется сообщение DHCP Request в качестве ответа на сообщение DHCP Offer, отправленное DHCP-сервером. Такое сообщение также отправляется в широковещательной рассылке клиентом DHCP после его перезапуска и содержит подтверждение конфигурации, например назначенного IP-адреса. Сообщение DHCP Request также отправляется после того, как DHCP-клиент получит IP-адрес, чтобы продлить аренду этого IP-адреса.

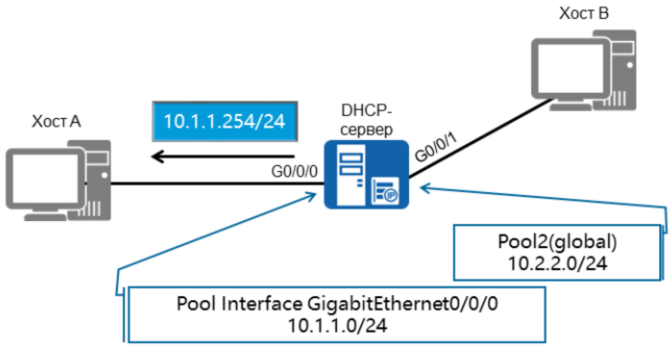
Сообщение DHCP ACK отправляется сервером DHCP для подтверждения сообщения DHCP Request от DHCP-клиента. После получения сообщения DHCP ACK клиент DHCP получает параметры конфигурации, включая IP-адрес. Однако не во всех случаях IP-адрес будет назначен клиенту. Сообщение DHCP NAK отправляется DHCP-сервером для того, чтобы отклонить сообщение DHCP Request, поступающее от DHCP-клиента, по истечении срока действия IP-адреса, назначенного DHCP-клиенту, или в случае, если DHCP-клиент переходит в другую сеть.

Сообщение DHCP Decline отправляется DHCP-клиентом, чтобы уведомить DHCP-сервер о том, что назначенный IP-адрес конфликтует с другим IP-адресом. После чего DHCP-клиент будет применять к DHCP-серверу другой IP-адрес.

Сообщение DHCP Release отправляется DHCP-клиентом для освобождения его IP-адреса. После получения сообщения DHCP Release DHCP-сервер назначает этот IP-адрес другому DHCP-клиенту.

Тип финального сообщения – это сообщение DHCP Inform, которое отправляется DHCP-клиентом для получения другой информации о конфигурации сети, например адреса шлюза и адреса сервера DNS, после того, как DHCP-клиент получит IP-адрес.

Адресные пулы



- Адресные пулы могут быть либо глобальными, либо интерфейсными.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Устройства серии AR2200 и S5700 могут работать в качестве DHCP-сервера для назначения IP-адресов пользователям в сети. Адресные пулы используются для определения адресов, которые должны быть выделены конечным системам. Существуют две основные формы адресных пулов, которые можно использовать для назначения адресов: глобальный адресный пул и интерфейсный адресный пул.

При использовании интерфейсного адресного пула IP-адреса из этого пула выделяются только конечным системам, подключенным к тому же сегменту сети, что и интерфейс. При настройке глобального адресного пула все конечные системы, связанные с сервером, смогут получать IP-адреса из этого пула. Настройка выполняется с помощью команды dhcp select global, в которой определяется глобальный адресный пул. В случае интерфейсного адресного пула команда dhcp select interface определяет интерфейс и сегмент сети, с которыми связан интерфейсный адресный пул.

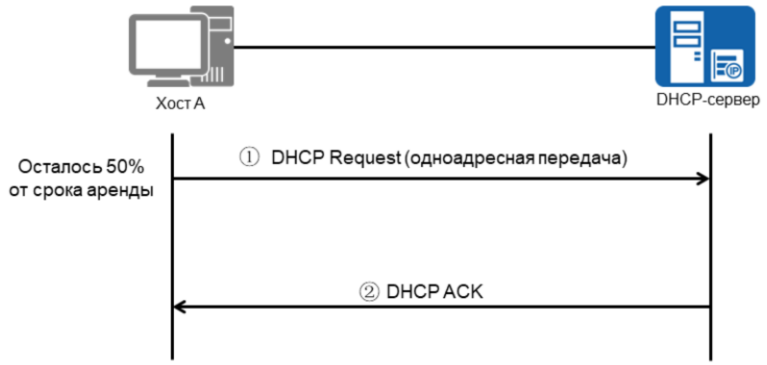
Интерфейсный адресный пул имеет приоритет над глобальным адресным пулом. Если на интерфейсе сконфигурирован адресный пул, то клиенты, подключенные к интерфейсу, получают IP-адреса из интерфейсного адресного пула, даже если сконфигурирован глобальный адресный пул. На коммутаторе S5700 только логические интерфейсы VLANIF могут быть сконфигурированы с интерфейсными адресными пулами.

Получение DHCP-адреса

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Для получения IP-адреса и другой информации о конфигурации необходимо, чтобы клиент установил связь с DHCP-сервером и через запрос получил адресную информацию, чтобы стать частью IP-домена. Этот процесс начинается с обнаружения IP-адреса, при котором DHCP-клиент ищет DHCP-сервер. DHCP-клиент осуществляет широковещательную передачу сообщения DHCP Discover, а DHCP-серверы отвечают на сообщение.
- Обнаружение одного или нескольких DHCP-серверов приводит к тому, что каждый DHCP-сервер предлагает IP-адрес DHCP-клиенту. После получения сообщения DHCP Discover каждый DHCP-сервер выбирает из пула IP-адресов тот адрес, который еще не выделен ни одному узлу, и отправляет клиенту сообщение DHCP Offer с назначенным IP-адресом и другой конфигурационной информацией.
- Если несколько DHCP-серверов отправляют сообщения DHCP Offer клиенту, клиент принимает первое полученное сообщение DHCP Offer. Затем клиент выполняет широковещательную передачу сообщения DHCP Request с выбранным IP-адресом. После получения сообщения DHCP Request сервер DHCP, который предлагает IP-адрес, отправляет сообщение DHCP ACK DHCP-клиенту. Сообщение DHCP ACK содержит предлагаемый IP-адрес и другую конфигурационную информацию.
- Получив сообщение DHCP ACK, DHCP-клиент передает в широковещательной рассылке пакеты gratuitous ARP, чтобы определить, использует ли какой-либо хост IP-адрес, выделенный DHCP-сервером. Если в течение указанного времени ответ не будет получен, то DHCP-клиент будет использовать этот IP-адрес. Если какой-либо хост использует этот IP-адрес, DHCP-клиент отправляет пакет DHCP Decline на DHCP-сервер, сообщая, что IP-адрес не может использоваться, после чего DHCP-клиент применяет другой IP-адрес.

Продление аренды DHCP



- DHCP инициирует процесс обновления аренды IP-адресов, когда оставшийся срок аренды составляет 50%.

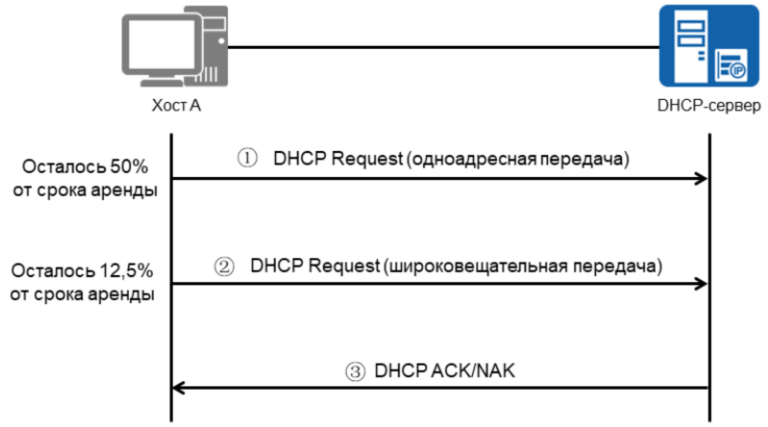
Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

После получения IP-адреса DHCP-клиент переходит в состояние привязки. На DHCP-клиенте установлены три таймера для управления обновлением аренды, повторной привязкой аренды и истечением срока аренды. При назначении IP-адреса DHCP-клиенту DHCP-сервер указывает значения для таймеров.

Если DHCP-сервер не устанавливает значения для таймеров, то DHCP-клиент использует значения по умолчанию. Значения по умолчанию определяют, что когда оставшийся срок аренды составляет 50%, должен начаться процесс обновления, после которого DHCP-клиент должен возобновить аренду своего IP-адреса. DHCP-клиент автоматически отправляет сообщение DHCP Request на DHCP-сервер, который выделил IP-адрес DHCP-клиенту.

Если IP-адрес является действительным, DHCP-сервер отвечает сообщением DHCP ACK, чтобы предоставить DHCP-клиенту право на новую аренду, а затем клиент повторно входит в состояние привязки. Если DHCP-клиент получает сообщение DHCP NAK от DHCP-сервера, то он переходит в состояние инициализации.

Истечение срока аренды DHCP



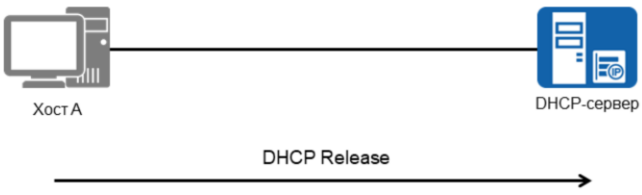
- Если срок аренды не будет продлен вовремя, то произойдет повторная привязка.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

После отправки DHCP-клиентом сообщения DHCP Request для продления аренды DHCP-клиент остается в статусе обновления и ожидает ответа. Если DHCP-клиент не получает сообщение DHCP Reply от DHCP-сервера после истечения времени ожидания повторной привязки DHCP-сервера, которая по умолчанию происходит, когда остается 12,5% от всего срока аренды, то DHCP-клиент предполагает, что исходный DHCP-сервер недоступен, и начинает широковещательную передачу сообщения DHCP Request, на которое любой DHCP-сервер в сети может ответить сообщением DHCP ACK или NAK.

При получении сообщения DHCP ACK DHCP-клиент возвращается в состояние привязки и сбрасывает таймер возобновления аренды и таймер привязки сервера. Если все полученные сообщения являются сообщениями DHCP NAK, то DHCP-клиент возвращается в состояние инициализации. В это время DHCP-клиент должен немедленно прекратить использование этого IP-адреса и запросить новый IP-адрес.

Освобождение IP-адреса

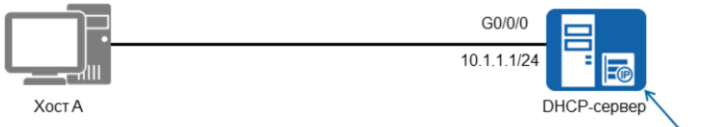


- Если клиент не сможет обновить IP-адрес до истечения срока аренды, IP-адрес освобождается.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Таймер аренды является конечным таймером в процессе истечения срока действия аренды, и если DHCP-клиент не получает ответ до истечения таймера срока аренды, то DHCP-клиент должен немедленно прекратить использование текущего IP-адреса и вернуться в состояние инициализации. Затем DHCP-клиент отправляет сообщение DHCP DISCOVER, чтобы подать заявку на новый IP-адрес, тем самым перезапуская цикл DHCP.

Конфигурация пула интерфейсов DHCP




```
[Huawei]dhcp enable
[Huawei]interface GigabitEthernet0/0/0
[Huawei-GigabitEthernet0/0/0]dhcp select interface
[Huawei-GigabitEthernet0/0/0]dhcp server dns-list 10.1.1.2
[Huawei-GigabitEthernet0/0/0]dhcp server excluded-ip-address
10.1.1.2
[Huawei-GigabitEthernet0/0/0]dhcp server lease day 3
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

В DHCP поддерживаются два типа настройки пула — определение глобального пула или пула на базе интерфейсов. Команда dhcp select interface используется для привязки интерфейса к интерфейсному адресному пулу для предоставления конфигурационной информации подключенным хостам. В данном примере интерфейс Gigabit Ethernet 0/0/0 привязан к интерфейсному адресному пулу.

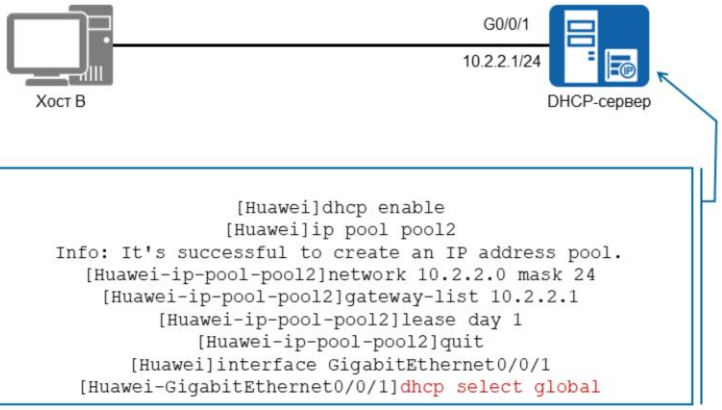
Проверка конфигурации DHCP

```
[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
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Каждый DHCP-сервер определяет один или несколько пулов, которые могут быть привязаны глобально или к определенному интерфейсу. 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 пула. Если поддерживаются другие атрибуты, передаваемые DNS-клиенту, например IP-шлюз, маска подсети и DNS-сервер, то они также будут отображаться.

Конфигурация глобального пула DHCP



- На DHCP-сервере создается адресный пул и настраиваются связанные с ним параметры.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

В данном примере показана конфигурация DHCP для глобального адресного пула, выделенного сети 10.2.2.0. Команда dhcp enable является необходимым условием для конфигурирования функций, связанных с DHCP. Конфигурация вступит в силу только после выполнения команды dhcp enable. Для DHCP-сервера необходимо сконфигурировать в системном представлении команду ip pool для создания пула IP-адресов и установки параметров пула IP-адресов, включая адрес шлюза, период аренды IP-адреса и т. д. После чего сконфигурированный DHCP-сервер сможет выделять клиентам IP-адреса из данного пула.

DHCP-сервер и его клиент могут находиться в разных сегментах сети. Чтобы клиент мог обмениваться данными с DHCP-сервером, для указания адреса выходного шлюза глобального адресного пула DHCP-сервера используется команда gateway-list. Затем DHCP-сервер сможет назначить клиенту как IP-адрес, так и указанный адрес выходного шлюза. Адрес указывается в виде десятичных чисел, разделённых точками, таким образом, можно сконфигурировать максимум восемь адресов шлюза, разделенных пробелами.

Проверка конфигурации DHCP

```
[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
```


Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

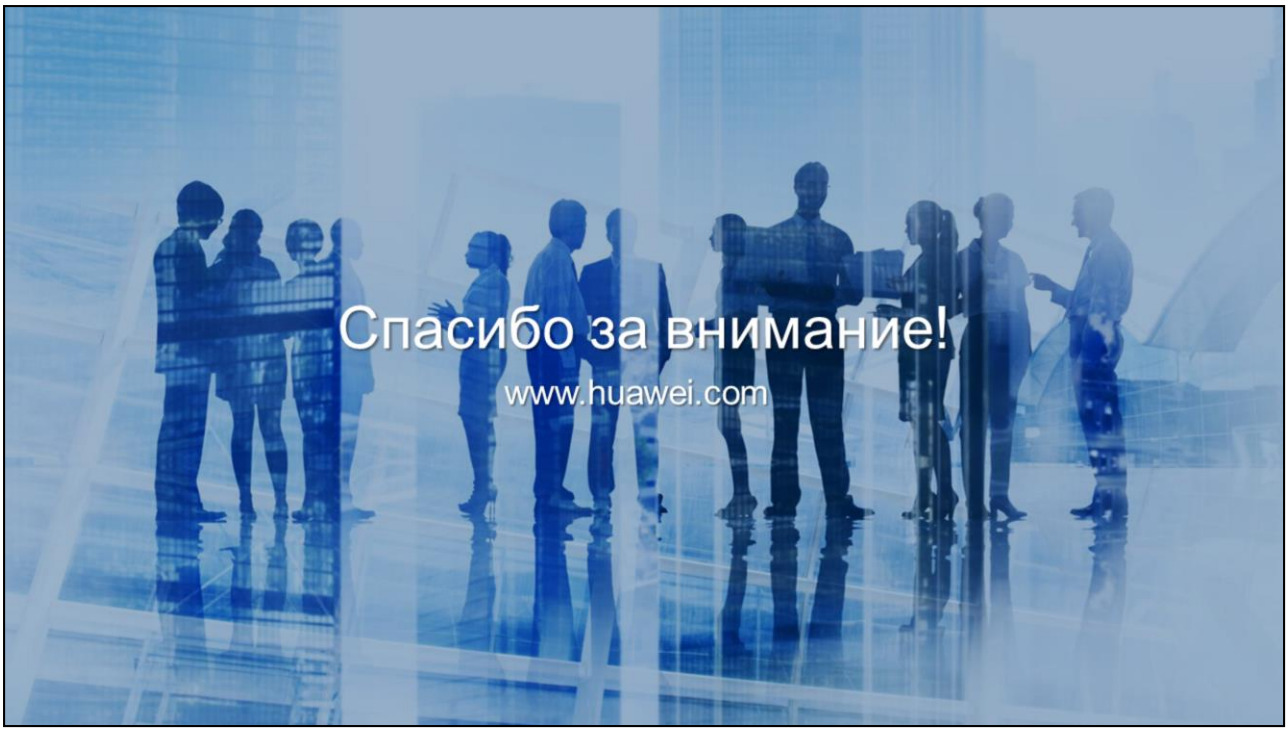
Информацию о пуле можно также просмотреть, использовав команду display ip pool. Эта команда предоставляет обзор общих параметров конфигурации, поддерживаемых сконфигурированным пулом, включая шлюз и маску подсети пула, а также общую статистику, которая позволяет администратору отслеживать текущее использование пула, чтобы определить количество выделенных адресов, наряду с другой статистикой использования.

Вопросы

- Какие IP-адреса обычно исключаются из адресного пула?
- Какой срок аренды IP-адреса по умолчанию?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

1. IP-адреса, которые используются для выделения серверам, например любым локальным DNS-серверам, во избежание конфликта адресов.
2. Срок аренды по умолчанию для назначенных IP-адресов DHCP устанавливается равным одному дню.


Спасибо за внимание!
www.huawei.com

Принципы работы протокола FTP

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

На ранних этапах разработки стандартов были заложены основы протокола передачи файлов для реализации обмена файлами между удаленными точками, на который не влияли бы различия в системах хранения файлов между хостами. Полученное в результате приложение FTP в конечном итоге было принято как часть набора протоколов TCP/IP. Сервис FTP остается неотъемлемой частью сети как приложение, которое обеспечивает надежную и эффективную передачу данных, обычно реализуемую для резервного копирования и извлечения файлов и данных журналов, а также оптимизирует общее управление сетью предприятия. Поэтому в данной презентации представлены средства, позволяющие инженерам и администраторам внедрять сервисы FTP в продуктах Huawei.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

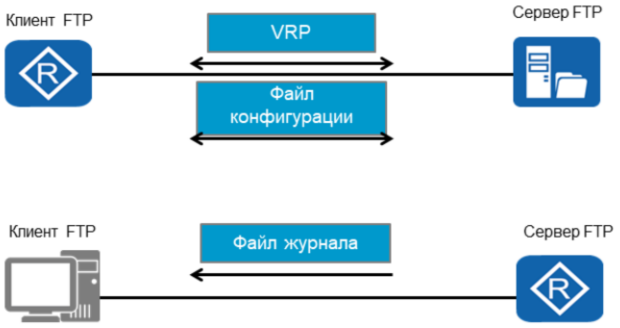
Цели

По окончании данного курса слушатели смогут:

- Объяснить процесс передачи файлов FTP.
- Сконфигурировать сервис FTP на устройствах Huawei.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Применение FTP в корпоративной сети



- FTP предоставляет эффективные средства для резервного копирования и извлечения важных файлов.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Применение FTP-сервера в корпоративной сети позволяет эффективно резервировать и извлекать важные системные и пользовательские файлы, которые могут использоваться для поддержки ежедневной работы корпоративной сети. Типичными примерами использования FTP-сервера являются резервное копирование и извлечение файлов VRP и конфигурационных файлов. Кроме того, FTP-сервер может использоваться для извлечения файлов журнала, необходимых при отслеживании активности FTP.

FTP: передача файлов

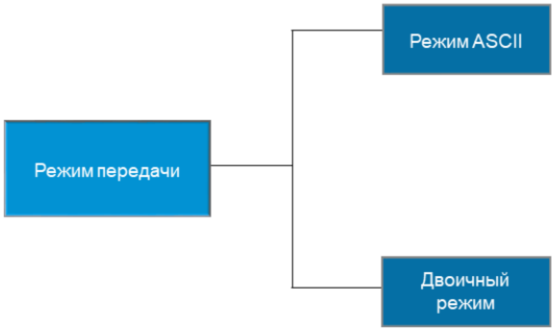
- Протокол FTP использует два типа TCP-соединений.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Протокол FTP использует два типа TCP-соединений. Одно из них называется управляющим соединением, которое устанавливается между клиентом FTP и сервером FTP для передачи команд. Сервер активирует заранее известный порт 21 и ожидает запроса на соединение от клиента. Затем клиент отправляет запрос на установку соединения с сервером. Управляющее соединение между клиентом и сервером остается на протяжении всего сеанса работы открытым, передает соответствующие команды от клиента к серверу, а также ответы от сервера клиенту.

Сервер со своей стороны использует TCP-порт 20 для передачи данных. Как правило, сервер осуществляет либо активное открытие, либо активное закрытие соединения для передачи данных. Однако что касается файлов, отправляемых с клиента на сервер в виде потоков, только клиент может закрыть соединение для передачи данных. FTP осуществляет передачу каждого файла в потоках. Для определения конца файла используется идентификатор EOF (End of File – конец файла). Поэтому для передачи каждого файла или списка каталогов требуется установить новое соединение для передачи данных. Передача файла между клиентом и сервером свидетельствует о том, что соединение для передачи данных установлено.

FTP: основные понятия

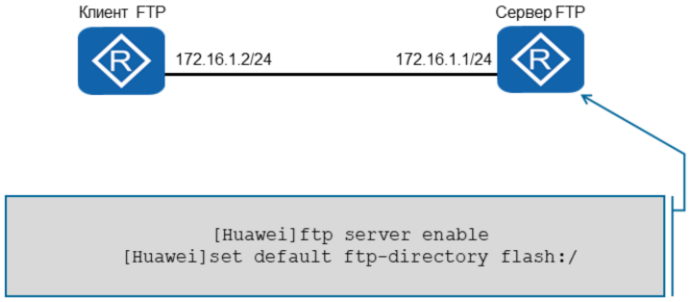


- Режимы передачи определяют формат данных перед их передачей между отправителем и получателем.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

- Протокол FTP поддерживает два режима передачи файлов: режим ASCII и двоичный режим. Режим ASCII используется для передачи текстовых файлов. В этом режиме перед передачей данные преобразуются из символьного представления на хосте-отправителе в «восьмибитный ASCII». Проще говоря, символы ASCII используются для замены служебных символов (возврата каретки и перевода строки), которые различаются в текстовых файлах различных операционных систем (ОС), для корректного отображения содержимого файла после передачи в ОС хоста-получателя. В двоичном режиме никакие преобразования символов не осуществляются — файл просто передается байт за байтом. Этот режим часто используется для передачи файлов изображений и программных файлов, символы которых могут передаваться без преобразования формата.

FTP: организация работы



- Для обработки файлов необходимо включить службу FTP и указать каталог FTP по умолчанию.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Служба FTP может быть реализована как на маршрутизаторах серии AR2200, так и на коммутаторах серии S5700. Включение данной службы выполняется с помощью команды *ftp server enable*. После включения функции FTP-сервера пользователи могут управлять файлами в режиме FTP. Для настройки рабочего каталога по умолчанию FTP-пользователей используется команда *set default ftp-directory*. Если рабочий каталог FTP по умолчанию не указан, пользователь не сможет войти в маршрутизатор и вместо этого получит сообщение с уведомлением о том, что у него нет прав доступа к рабочим каталогам.

FTP: доступ пользователя

- Для идентификации пользователей и определения объема прав каждого пользователя поддерживается создание аккаунтов пользователей.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Для управления доступом каждого пользователя к службе FTP каждому отдельному пользователю присваивается аккаунт. Для настройки локальной аутентификации и авторизации используется AAA. После перехода в режим AAA можно создать локального пользователя, назначив соответствующий аккаунт и пароль. Чтобы обеспечить возможность поддержки AAA для данного типа службы FTP, аккаунту настраивается привязка к различным службам, которые указываются с помощью команды *service-type*.

Если FTP-каталог пользователя должен отличаться от каталога по умолчанию, то для указания каталога пользователя используется команда *ftp-directory*. Для ограничения количества возможных активных соединений аккаунта локального пользователя используется команда *access-limit*. Данный параметр может принимать значения от 1 до 800 или может быть не задан, если ограничение доступа не применяется.

Для предотвращения несанкционированного доступа в случае, если окно сеанса не используется пользователем в течение некоторого периода времени, необходимо сконфигурировать время простоя. Значение команды *idle timeout* указывается в минутах и секундах. Команда со значением 0 0 означает, что время простоя не применяется. Наконец, уровень привилегий определяет уровень полномочий пользователя, с точки зрения того, какие команды он может использовать во время установления сеанса FTP. Для любого уровня привилегий может быть установлено значение от 0 до 15. Чем больше значение, тем более высокий уровень привилегий у пользователя.

FTP: конфигурация пользователя

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

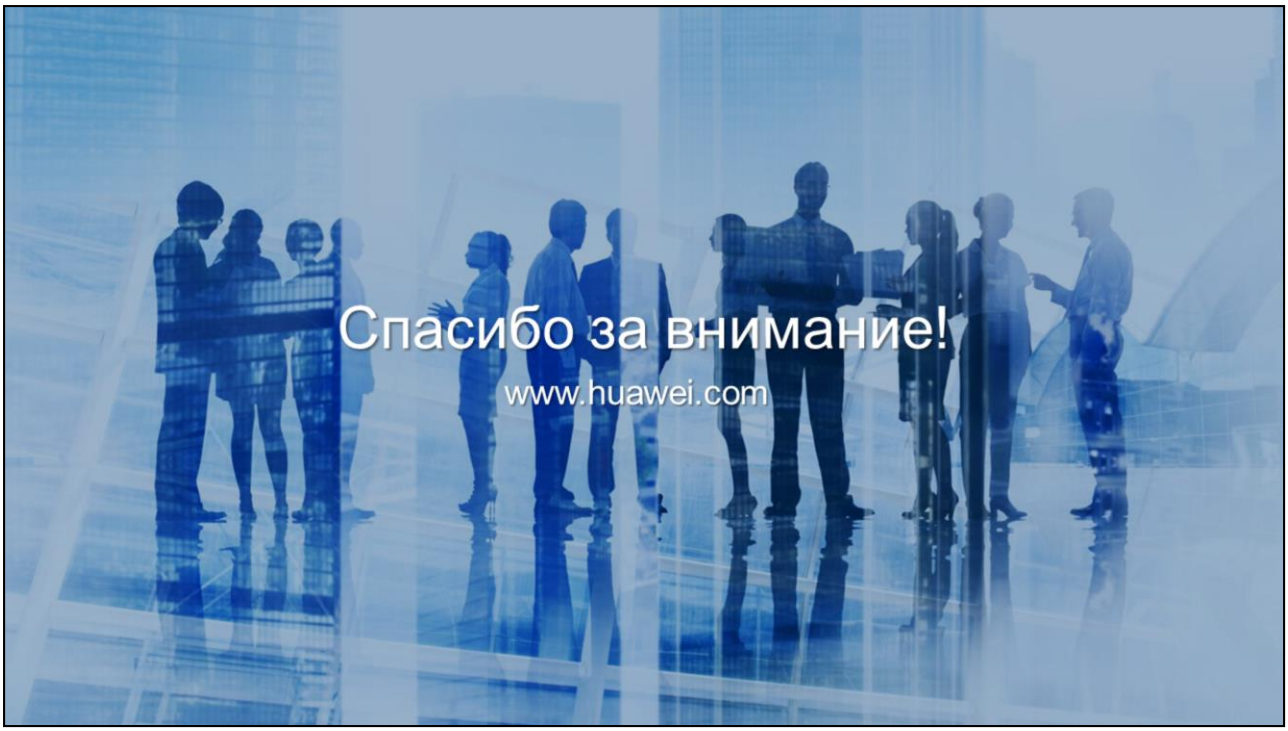
После конфигурирования службы FTP на FTP-сервере пользователи могут установить соединение между клиентом и сервером. Чтобы установить сеанс связи с поддержкой аутентификации AAA для проверки пользователя по паролю, выполните команду *ftp* на клиенте. После прохождения аутентификации клиент сможет выполнять конфигурирование, а также отправлять файлы с FTP-сервера или получать файлы на FTP-сервер.

Вопросы

- Какие порты должны быть открыты для работы сервиса FTP?
- Какие шаги необходимо выполнить, если пользователь не имеет полномочий на доступ к рабочему каталогу?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

1. Для успешного установления управляющего соединения и соединения для передачи данных сервиса FTP необходимо открыть TCP-порты 20 и 21.
2. Если пользователь не имеет полномочий на доступ к рабочему каталогу, то необходимо указать каталог FTP по умолчанию. Для этого необходимо выполнить команду *set default ftp-directory <directory location>*, где в качестве имени каталога может быть указана, например, флеш-память системы.


Спасибо за внимание!
www.huawei.com

Принципы работы протокола Telnet

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Введение

По мере расширения корпоративной сети, в связи с ростом количества филиалов, которые считаются частью корпоративного домена и требуют удаленного администрирования, увеличивается географическое расстояние между используемыми устройствами. Кроме того, управление сетью часто выполняется из центрального офиса, который контролирует работу всех устройств. Протокол Telnet позволяет упростить процесс администрирования и управления устройствами. В данной презентации представлены принципы работы протокола и его реализация.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Цели

По окончании данного курса слушатели смогут:

- Объяснить применение и принципы протокола Telnet.
- Включить сервис Telnet на используемых устройствах Huawei.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

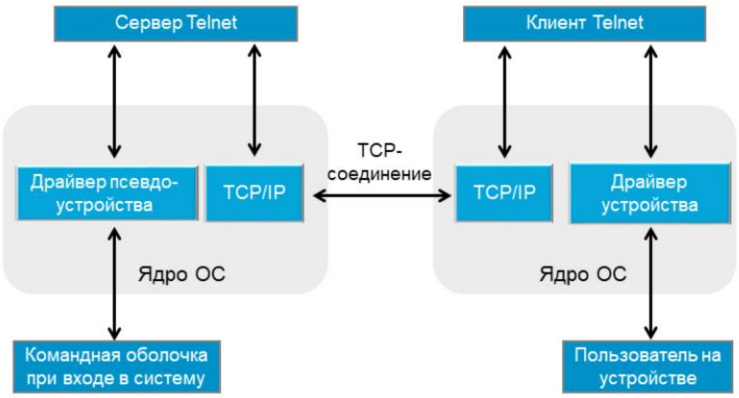
Применение Telnet

- Telnet представляет собой программу эмуляции терминалов для двунаправленного обмена текстом при использовании в локальных и удаленных сетях.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Протокол Telnet (Telecommunication Network Protocol – протокол телекоммуникационной сети) позволяет терминалу выполнить удаленный вход на любое устройство, способное работать в качестве сервера Telnet, и предоставляет интерактивный рабочий интерфейс, с помощью которого пользователь может выполнять операции так же, как это делается локально через консольное соединение. Удаленным хостам не требуется прямое подключение к аппаратному терминалу, что позволяет пользователям использовать повсеместно доступные возможности IP для удаленного управления устройствами практически из любой точки мира.

Архитектура «клиент-сервер» протокола Telnet



- Архитектура Telnet демонстрирует, как нажатие клавиш пользователем интерпретируется драйверами устройств перед передачей по TCP.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Telnet работает на базе архитектуры «клиент-сервер», для которой устанавливается TCP-соединение между портом-инициатором (клиентом) и портом с номером 23, закрепленным за протоколом Telnet на сервере. Сервер прослушивает этот заранее известный порт для обнаружения входящих TCP-соединений. TCP-соединения являются полнодуплексными и двухточечными (определяются портами источника и пункта назначения). Сервер поддерживает несколько одновременных соединений от заранее известного порта к целому диапазону заранее неизвестных пользовательских портов.

Драйверы устройств Telnet распознают нажатия клавиш пользователей и интерпретируют их в универсальный символьный стандарт на базе NVT (Network Virtual Terminal – сетевой виртуальный терминал), который работает в качестве виртуального посредника между системами, после чего происходит передача данных по TCP/IP-соединению на сервер. Сервер декодирует NVT-символы и передает их драйверу псевдо-устройства. Драйвер используется для того, чтобы операционная система могла принимать декодированные символы.

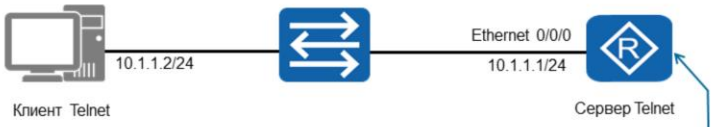
Режимы аутентификации

Режим аутентификации	Описание
Без аутентификации	Вход без аутентификации
AAA	Аутентификация AAA
Пароль	Аутентификация по паролю на интерфейсе пользовательского устройства

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

Для получения доступа к сервису Telnet пользователю, как правило, требуется пройти аутентификацию. Существует три основных режима аутентификации Telnet.

Конфигурация Telnet



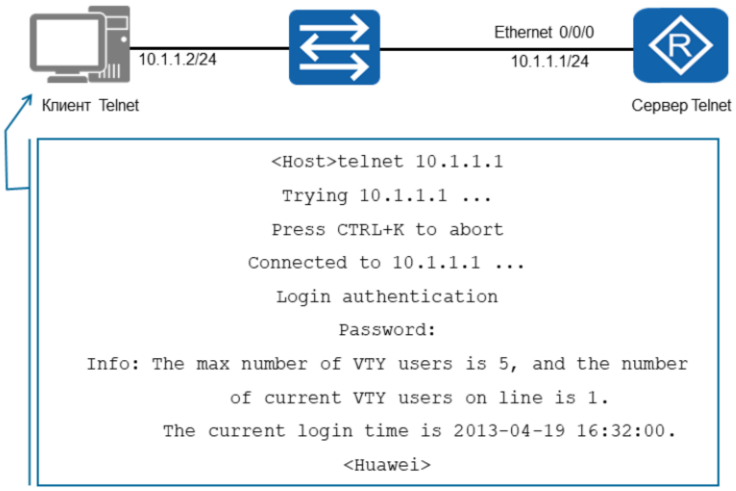

```
[Huawei]interface Ethernet 0/0/0
[Huawei-Ethernet0/0/0]ip address 10.1.1.1 24
[Huawei]user-interface vty 0 4
[Huawei-ui-vty0-4]authentication-mode password
[Huawei-ui-vty0-4]set authentication password cipher
Enter Password(<8-128>): huawei12
```

- Telnet требует, чтобы до установления соединения к интерфейсу виртуального телетайпа была применена аутентификация.

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

При выборе устройства, которое будет работать в качестве сервера Telnet, обычно используется общая схема аутентификации по паролю, которая применяется для всех пользователей, подключающихся к пользовательскому интерфейсу vty. Как только посредством реализации подходящей схемы адресации будет установлено IP-соединение, для диапазона vty выполняется набор команд authentication-mode password вместе с предназначенным паролем.

Конфигурация Telnet



Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.
HUAWEI

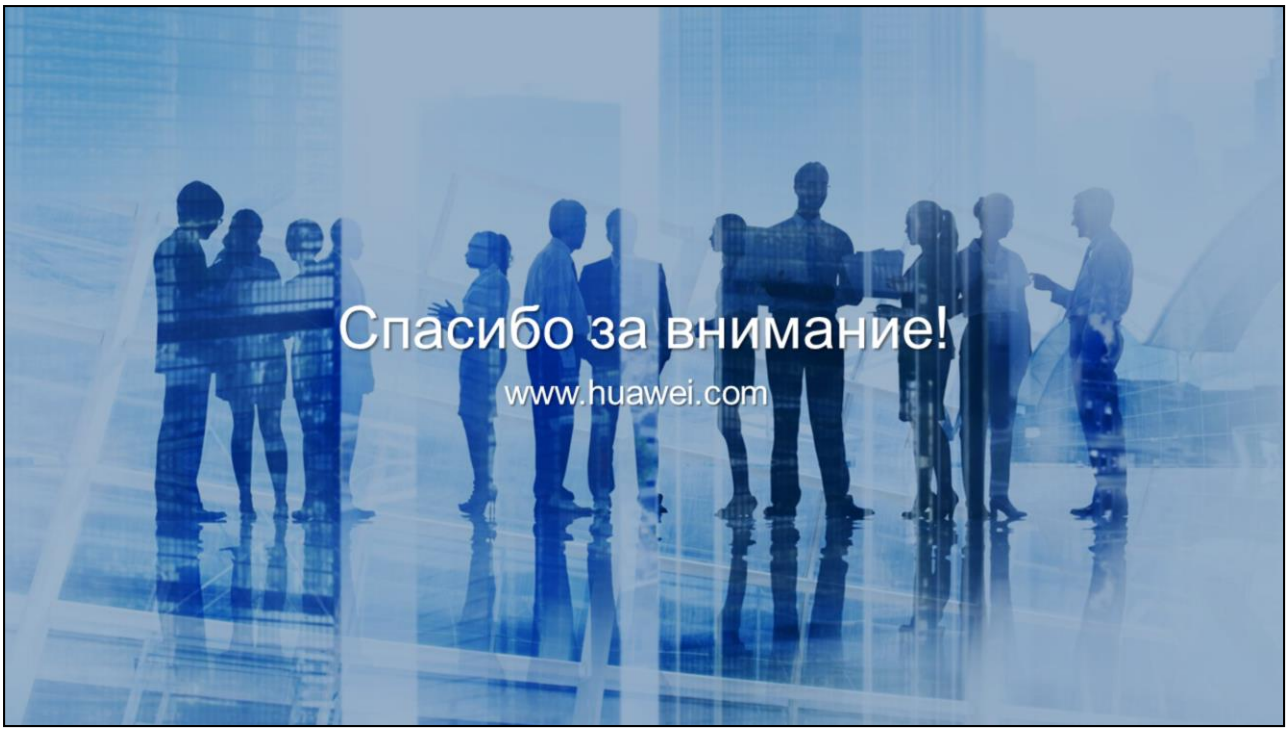
После настройки удаленного устройства в качестве сервера Telnet клиент может установить Telnet-соединение с помощью команды telnet и получить запрос на аутентификацию. Пароль аутентификации должен совпадать с паролем, который используется на сервере Telnet, как часть предыдущей конфигурации аутентификации по паролю. После этого пользователь сможет установить Telnet-соединение с удаленным устройством, работающим в качестве сервера Telnet, и запустить эмулятор командного интерфейса на локальном клиенте Telnet.

Вопросы

- Какие могут быть причины того, что пользователь не может установить Telnet-соединение, хотя сервис Telnet включен?

Copyright © 2019 Huawei Technologies Co., Ltd. Все права защищены.

1. Если пользователь не может установить Telnet-соединение, он должен убедиться, что устройство, поддерживающее сервис Telnet, достижимо. Если устройство достижимо, то необходимо выполнить проверку пароля. Если пароль используется правильный, следует проверить количество пользователей, которые в настоящее время обращаются к устройству через Telnet. Если необходимо увеличить количество пользователей, обращающихся к устройству через Telnet, используйте команду user-interface maximum-vty <0-15>, где 0-15 – это количество поддерживаемых пользователей.


Спасибо за внимание!
www.huawei.com