1. Преимущества динамической маршрутизации по сравнению со статической:

- Автоматизация: Динамическая маршрутизация обновляет маршруты автоматически, что устраняет необходимость вручную настраивать маршруты.

- Динамичное реагирование: Маршрутизаторы могут реагировать на изменения в топологии сети, перераспределяя трафик по оптимальным маршрутам.

- Устойчивость: Динамические протоколы могут быстро адаптироваться к сетевым изменениям, обеспечивая более стабильную сеть.

- Масштабируемость: При увеличении размера сети динамическая маршрутизация проявляет более высокую масштабируемость.

2. EIGRP (Enhanced Interior Gateway Routing Protocol):

EIGRP - это протокол маршрутизации внутри автономной системы (Interior Gateway Protocol), который используется для оптимизации маршрутов в сетях IP. Он разработан компанией Cisco и является проприетарным протоколом.

3. Основные характеристики, делающие EIGRP протоколом высокой производительности:

- Быстрая сходимость: EIGRP быстро реагирует на изменения в топологии сети.

- Минимизация трафика: Использует эффективные механизмы обмена информацией с минимальным количеством пересылаемых данных.

- Балансировка нагрузки: Распределяет трафик по нескольким маршрутам для более эффективного использования ресурсов сети.

4. Балансировка нагрузки в EIGRP:

EIGRP обеспечивает балансировку нагрузки, используя несколько маршрутов к одному месту назначения. Это достигается путем распределения трафика пропорционально стоимости маршрутов.

5. Принцип работы EIGRP DUAL (Diffusing Update Algorithm):

DUAL используется для обеспечения быстрой сходимости в случае изменения топологии. Он принимает решения о выборе оптимальных маршрутов, учитывая стоимости и метрики путей.

6. Метрики в EIGRP для оценки стоимости маршрутов:

EIGRP использует комплексную метрику, включающую пропускную способность, задержку, надежность и нагрузку, для расчета стоимости маршрутов.

7. Формирование таблицы маршрутизации EIGRP:

Таблица маршрутизации EIGRP, также известная как табличка DUAL, формируется на основе информации, полученной от соседних маршрутизаторов, и содержит оптимальные маршруты к различным сетям.

8. Критерии выбора лучшего маршрута в EIGRP:

Выбор лучшего маршрута в EIGRP зависит от метрики, которая включает в себя пропускную способность, задержку, надежность и нагрузку, а также наличие альтернативных путей.

9. Обнаружение и реагирование EIGRP на изменения в топологии:

EIGRP использует механизмы Hello и асинхронные обновления для обнаружения изменений в топологии и быстрого пересчета оптимальных маршрутов.

10. События, приводящие к передаче EIGRP обновлений маршрутов:

Изменения в топологии, события Hello таймеров, появление новых соседей или информации о маршрутах приводят к передаче EIGRP обновлений для синхронизации маршрутной информации между маршрутизаторами.

11. Роль "neighbor relationship" (отношение соседства) в EIGRP:

В EIGRP, "neighbor relationship" (отношение соседства) устанавливается между соседними маршрутизаторами для обмена информацией о маршрутах. Это отношение позволяет маршрутизаторам обмениваться копиями своих табличек маршрутизации (Topology Table), что важно для расчета оптимальных маршрутов.

12. Процесс аутентификации соседей EIGRP:

EIGRP поддерживает механизм аутентификации соседей с использованием ключей. Маршрутизаторы соседствуют между собой и обмениваются ключами, чтобы подтвердить свою подлинность перед обменом маршрутной информацией.

13. Типы сообщений в EIGRP для обмена информацией:

EIGRP использует следующие типы сообщений:

- Hello: Используется для обнаружения соседей.

- Update: Передача обновленной информации о маршрутах.

- Query: Запрос о дополнительной информации о маршрутах.

- Reply: Ответ на запрос.

14. Обработка асимметричных маршрутов в EIGRP:

EIGRP способен работать с асимметричными маршрутами, так как он учитывает пропускную способность и задержку в обоих направлениях при расчете метрик маршрута.

15. Настройка summarization (суммирование) в EIGRP и преимущества:

Суммирование в EIGRP позволяет объединять несколько подсетей в одну для более эффективного использования таблиц маршрутизации. Преимущества включают уменьшение размера таблицы маршрутизации и снижение объема передаваемой информации.

16. Обработка EIGRP запросов для разрешения асинхронных событий:

EIGRP использует запросы и ответы для разрешения асинхронных событий, таких как изменение топологии сети. Запросы отправляются для получения необходимой информации о маршрутах.

17. Поддержка переменных стоимости маршрутов в EIGRP:

EIGRP учитывает различные параметры, такие как пропускная способность и задержка, при расчете стоимости маршрута, что позволяет выбирать оптимальные маршруты.

18. Факторы, влияющие на принятие решения EIGRP о пересчете таблицы маршрутизации:

Факторы включают изменения в топологии, приход новой информации от соседей, а также события, такие как таймеры Hello и Hold.

19. Быстрая сходимость в EIGRP при изменениях:

EIGRP обеспечивает быструю сходимость благодаря множеству механизмов, таких как DUAL (Diffusing Update Algorithm) и асинхронному обмену информацией между соседями.

20. Роль Autonomous System (AS) в EIGRP и взаимодействие с другими AS:

EIGRP работает в пределах определенного Autonomous System (AS). Маршрутизаторы в одном AS могут обмениваться информацией EIGRP. Для взаимодействия с другими AS, могут использоваться механизмы, такие как redistribution, где маршрутизаторы могут обмениваться маршрутами с другими протоколами маршрутизации.

21. Настройка таймеров и таймаутов в EIGRP:

- Hello таймер Интервал между отправкой Hello пакетов. Настроить можно с помощью команды `ip hello-interval eigrp`.

- Hold таймер: Время ожидания до объявления соседа недействительным. Настраивается через `ip hold-time eigrp`.

- Active таймаут: Время ожидания завершения попыток установки маршрута в состоянии Active. Настраивается через `variance` команду.

22. Обработка асимметричных маршрутов в EIGRP

- EIGRP учитывает стоимость маршрутов в обоих направлениях, что позволяет эффективно работать с асимметричными маршрутами.

- В случае асимметрии, EIGRP использует симметричные данные для расчета метрик и принятия решений.

23. Аутентификация маршрутов в EIGRP:

- EIGRP может использовать аутентификацию для обеспечения безопасности. Это можно настроить с помощью команды `ip authentication mode` и указать метод аутентификации (`md5` или `sha-256`).

- Ключи для аутентификации маршрутов устанавливаются с использованием команды `ip authentication key-chain`.

24. Управление использованием bandwidth и delay в EIGRP:

- Значения bandwidth и delay могут быть изменены с использованием команды `bandwidth` и `delay` соответственно в конфигурационном режиме интерфейса.

- Изменение этих параметров влияет на расчет метрики EIGRP.

25. Влияние изменения сетевой топологии на EIGRP и обновление маршрутных таблиц:

- Изменения в топологии (добавление/удаление маршрутов) приводят к отправке EIGRP обновлений маршрутов.

- Соседние маршрутизаторы анализируют обновления и обновляют свои таблицы маршрутизации.

26. Различия между EIGRPv4 и EIGRPv6:

- EIGRPv4 используется для IPv4, а EIGRPv6 для IPv6.

- EIGRPv6 не поддерживает маршрутизацию между различными адресными семействами.

- EIGRPv6 не использует маску сети в обновлениях (аналогично OSPFv3).

27. Уменьшение количества EIGRP пакетов по сети:

- Можно использовать механизмы summarization и агрегации маршрутов для уменьшения объема пересылаемой информации.

- Настройка фильтрации маршрутов для уменьшения числа передаваемых EIGRP обновлений.

28. Маршрутизация в EIGRP через несколько путей (equal-cost load balancing):

- Включить равнозначное распределение нагрузки можно с помощью команды `maximum-paths` в конфигурационном режиме EIGRP.

- Это позволяет использовать несколько маршрутов с одинаковой стоимостью для достижения балансировки нагрузки.

Тема: IGRP EIGRP

Протокол динамической маршрутизации.

Предназначен для определения маршрута которые расположены внутри автономных систем, по способу сбора информации о маршрутах внутри системы – этот протокол относится к дистанционно векторным протоколам, комплексная метрика.

Наиболее существенным отличием протокола IGRP является наличие комплексного критерия оценки качества маршрута – метрики (стоимости маршрута) в данном протоколе используются доп., механизмы для построения маршрута их 2.

1. Задержка внасимая каналом
2. Готовность канала для отправки

Параллельные маршруты.

Использование протокола IGRP позволяет определять и обслуживать несколько параллельных маршрутов, связывающих источника и получателя. Существенной особенностью данного протокола является то, что эти маршруты необязательно должны иметь одинаковую метрику для их использования в качестве каналов.

Быстрая сходимость и предотвращение зацикливания

Для обеспечения минимального времени на реагирование, которое происходит в системе используются следующие решения:

1. Управляемые обновления передаются только в момент изменение сети
2. Таймеры, использующиеся для того, чтобы в сети при обновлении не возникали петли коммутации

Свежие маршруты не используются для передачи пакетов до истечения интервалов времени величина которого определяет таймером

1. Для предотвращения возникновения циклов обновления для маршрутизаторов, которые были получены с определенного направления не должны передаваться в этом же направлении.
2. Для блокирования маршрутов метрика которых начинает расти ей присваивается значение бесконечности.

В современных сетях бывает полезно выделять области, в которых должны быть использованы автономные процессы определения маршрута такие области называется доменами маршрутизации

Протокол EIGRP.

Это улучшенных протокола внутреннего шлюза, работает только на устройствах cisco, относятся к разряду улучшенного дистанционно-векторного протокола, этот протокол маршрутизации использует непростую метрику который вычитывает, основываясь на пропускной способности и задержках.

1. Быстрая сходимость
2. Происходит быстрое перестроение топологии сети при внезапных изменениях, падение канала добавления роутера и тд.
3. Обновления передаются частично таким образом сеть не нагружается лишним трафиком
4. Данный протокол имеет поддержку бесклассовой адресацией VLSM
5. Происходит балансировка трафика с различной метрикой
6. Взаимодействие между роутерами осуществляется с использование мульти каст адреса.

EIGRP таблицы

1. Таблица соседей строится строиться благодаря обмену Hello пакетов, если в течении 15 сек сосед не отвечает, то он удаляется из таблицы
2. Таблица в топологии содержат инфу о маршрутах и создан через протокол EIGRP.

Маршруты делятся на 2 типа:

* лучшие
* альтернативные маршруты добавляются в таблицу в случаи пропажи или удаления лучшего маршрута

EIGRP сообщения

Использует 5 типов пакетов

1. Hello пакет для проверки соседей
2. Update сообщение отправляется новому соседу чтобы он смог построить таблицу топологии также это сообщение отправляется когда происходят изменение в сети
3. Query это сообщение отправляется когда роутер потерял лучший маршрут а альтернативного маршрута не было, этот пакет спрашивает у соседей нет ли у них альтернативных маршрутов
4. Reply отправляется в ответ на query
5. Используются для подтверждения полученных данных но в себе данных не несет

**Тема:** протоколы верхнего (прикладного) уровня osi.

Протоколы верхнего уровня обеспечивают взаимодействие между человеком и сетью этих протоколов огромное кол-во.

**HTTP** – hypertext transport protocol – протокол передачи данных используется обычно для получения информации с веб сайтов. С каждым годом этот протокол становится более популярным и совершенствуется, он использует клиент серверную модель, тесть существуют клиенты, которые формируют и отправляют запрос, а серверы слушают данный запрос и отвечают на него.

**DNS** – domain name system – система доменных имен, хранит информацию о доменах, например ip адресу соответствует определенное имя, когда вы открываете сайт то вы обращаетесь к нему по имени. Не везде можно применять dns. Вот dns как раз и занимается сопоставлением ip адреса и имени.

**POP3/POP3s** – Post Office protocol v3 – почтовый протокол 3 версии, работает данный протокол по принципу загрузи и удали. Что клиент заходит на сервер и смотрит есть ли для него письмо, если оно присутствует он загружает его себе и ставит отметку об удалении на сервере. Порт 110. У данного протокола есть другая версия POP3s дополнительный криптографический протокол, защищенный способ передачи, использует 995 порт.

**Telnet** – terminal network – дынный протокол работает на 23 порту.

**SSH** – secure shell – использует 22 порт, используя зашифрованное соединение.

**FTP** – file transfer protocol – протокол передачи данных.

**TFTP** – trivial file transport protocol – простой протокол передачи данных. Не требует аутентификации пользователей используется для прихода обновления.

**IMAP** – Internet massage access port – протокол доступа к эл., почте, является более умным и сложным протоколом, главное различие с протоколом POP3 в том что клиент заходит на сервер не удаляет почту а копирует ее, таким образом у клиента отображается копия почтового ящика который хранится на почтовом сервер, и если клиент удалит письмо то оно удалится у него.

**DHCP** – динамическая конфигурация устройств – протокол динамической настройке узла, он позволяет узлам динамически получать шлюз, ip, маску, dns, при помощи dhcp можно обеспечить полный контроль над ip адресами. Создавать отдельные пулы для каждой сети, давать адреса в аренду и резервировать их.

**SMTP** – Simple mail transfer protocol – простой протокол передачи почты, используется для передачи почты на почтовый сервер использует 25 порт

Настройка статического и динамического NAT/PAT

Преобразование ip адресов

1. Настройка статического NAT:

Для настройки статического NAT на маршрутизаторе Cisco используется следующая команда:

ip nat inside source static <local\_ip> <global\_ip>

где:

- <local\_ip> - локальный IP-адрес устройства внутри сети

- <global\_ip> - глобальный IP-адрес, который будет использоваться для доступа к устройству извне

Пример:

ip nat inside source static 192.168.1.10 203.0.113.5

Эта команда настраивает статический NAT для устройства с локальным IP-адресом 192.168.1.10 и глобальным IP-адресом 203.0.113.5.

2. Настройка динамического NAT:

Для настройки динамического NAT на маршрутизаторе Cisco используется следующая команда:

ip nat inside source list <access\_list> interface <interface> overload

где:

- <access\_list> - список доступа, определяющий какие локальные IP-адреса будут переводиться в глобальные

- <interface> - интерфейс маршрутизатора, через который происходит выход в интернет

- overload - указывает на использование PAT (Port Address Translation) для перевода нескольких локальных адресов в один глобальный IP-адрес

Пример:

ip nat inside source list NAT\_ACL interface GigabitEthernet0/0 overload

Эта команда настраивает динамический NAT с использованием PAT для локальных адресов, определенных в списке доступа NAT\_ACL, через интерфейс GigabitEthernet0/0.

3. Команды для настройки PAT:

Для настройки PAT (Port Address Translation) используются те же команды, что и для динамического NAT, с добавлением ключевого слова overload. PAT позволяет использовать один глобальный IP-адрес для перевода нескольких локальных адресов, изменяя порты.

Пример настройки PAT:

ip nat inside source list PAT\_ACL interface GigabitEthernet0/0 overload

Эта команда настраивает PAT для локальных адресов, определенных в списке доступа PAT\_ACL, через интерфейс GigabitEthernet0/0 с использованием перегрузки портов.

FHRP Протокол резервирования 1 перехода

В случаи сбоя маршрутизатора (в который поступает в качестве шлюза по умолчанию) узел для которого настроена использование этого шлюза по умолчанию изолируется от внешних сетей, требуется механизм для предоставления альтернативных шлюзов в коммутируемых сетях где 2 или более маршрутизаторов подключены к одним и тем же сетям vlan, одним из способов устроения единой точки отказа на шлюзе по умолчанию является реализация виртуального маршрутизатора с виртуальным маршрутизатором несколько маршрутизаторов настроены для совместной работы. Чтобы предоставить иллюзию одного маршрутизатора хостам в локальной сети в случаи сбоя активного маршрутизатора протокол резервирования переводит резервный маршрутизатор на новые функции активного маршрутизатора происходит следующее:

1 резервный маршрутизатор перестает видеть сообщения приветствия от другого маршрутизатора

2 резервный марщрутизатор принимает роль передающего маршрутизатора

3 поскольку новый пересылающий маршрутизатор использует IPv4 так и MAC адрес виртуального маршрутизатора

4 хост устройства не замечает перебоев в обслуживании

FHRP – используется в производственной среде в значительной степени зависит от оборудования и потребности сети доступные:

HSRP и HSRP для IPv6

VRRP

GLBR

HSRP – является собственной разработкой cisco которое предназначено для обеспечения прозрачного переключение на резервное устройство первого периода, обеспечивает высокую доступность сети путем обеспечения избыточности маршрутизации первого перехода настроенных с адреса шлюза по умолчанию, используется группой маршрутизаторов для выбора активного и резервного устройства в группе интерфейсов устройств активным устройством является устройство которое используется для маршрутизации пакетов, резервное устройство – устройство которое берет на себя трафик когда активное устройство выходит из строя или когда предварительные условия сработали резервные функции заключается в контроле работоспособного состояния, и быстрого принятия роли, в случаи сбоя активного маршрутизатора.

HSRP IPv6 – это запатентованное компанией cisco технология которая обеспечивает туже функциональность но в среде IPv6, группа HSRP имеет виртуальный MAC адрес полученный из номера группы и виртуального канала IPv6 полученный из виртуального MAC адреса, периодические объявления маршрутизатора отправляются для локального адреса для канала виртуального IPv6 адресации, когда группа HSRP активна. Когда группа становится не активной, эти сообщения останавливаются после отправки последнего

VRRP – Протокол избыточного резервирования виртуальных маршрутизаторов v2 – открытых протокол выбора динамически назначающий VRRP маршрутизатором ответственность за 1 или несколько виртуальных маршрутизаторов в сети LAN таким образом маршрутизаторов в канале с множественным доступом могут использовать 1 виртуальный адрес, маршрутизатор VRRP настроен для запуска в сочетании с 1 или несколькими другими маршрутизаторами подключенных к локальной сети, в конфигурации VRRP один из маршрутизаторов выбирается в качестве основного виртуального маршрутизатора а другие выступают в роли резервных на случай сбоя основного виртуального маршрутизатора

VRRPv3 – предоставляет функции поддержки IPv4 и IPv6. VRRPv3 работает в неоднородных средах и предоставляет более широкие возможности масштабирования чем VRRPv2.

GLBP – протокол распределения нагрузки шлюза, используется только на cisco. GLBP для IPv6 обеспечивает защиту трафика от неисправного маршрутизатора или сети (предотвращает неисправность маршрутизатора в сети) одновременно обеспечивает балансировку нагрузки по группе избыточных маршрутизаторов протокол обеспечения маршрутизаторов с использование маршрутизаторов с использованием IСMP (IRTP) указанный IRDP является устаревшим решением FHRP позволяет определять место положения маршрутизаторов обеспечивающих подключения к другим нелокальным сетям.

Основные аспекты состояния протокола HSRP:

Активный маршрутизатор: Основной маршрутизатор, который обрабатывает весь трафик для HSRP-группы. Если активный маршрутизатор выходит из строя, резервный маршрутизатор берет на себя его функции.

Резервный маршрутизатор: Маршрутизатор находится в ожидании и готов взять на себя обработку трафика, если активный маршрутизатор выходит из строя.

Виртуальный IP-адрес: IP-адрес, который используется как шлюз по умолчанию для устройств в локальной сети. Этот IP-адрес настраивается на HSRP-группу, а не на конкретный физический интерфейс.

Приоритет: Значение, используемое для определения, какой маршрутизатор в группе будет активным. Маршрутизатор с самым высоким приоритетом становится активным маршрутизатором. Приоритет может быть изменен вручную для управления выбором активного маршрутизатора.

Преемпция: Функция, позволяющая маршрутизатору с более высоким приоритетом перехватить роль активного маршрутизатора у текущего активного маршрутизатора, когда тот становится доступным после восстановления после сбоя.

HSRP работает, отправляя сообщения Hello между маршрутизаторами в HSRP-группе для мониторинга их состояния. Если резервный маршрутизатор не получает Hello-сообщения от активного маршрутизатора в течение заданного времени, он предполагает, что активный маршрутизатор вышел из строя, и занимает его место, становясь новым активным маршрутизатором.

Этот механизм гарантирует, что пользовательские данные продолжают маршрутизироваться без значительных задержек или потерь в случае сбоя оборудования, тем самым повышая общую доступность и надежность сетевой инфраструктуры.

**PPP (сетевой протокол)**

**PPP** (англ. *Point-to-Point Protocol*) — двухточечный протокол [канального уровня](https://dic.academic.ru/dic.nsf/ruwiki/643650) (Data Link) [сетевой модели OSI](https://dic.academic.ru/dic.nsf/ruwiki/682146). Обычно используется для установления прямой связи между   двумя узлами сети, причем он может обеспечить аутентификацию соединения, шифрование (с использованием ECP, RFC 1968) и сжатие данных. Используется на многих типах физических сетей: нульмодемный кабель, телефонная линия сотовая связь и т. д.

Часто встречаются подвиды протокола PPP такие, как Point-to-Point Protocol over Ethernet (PPPoE), используемый для подключения по Ethernet, и иногда через DSL; и Point-to-Point Protocol over ATM (PPPoA), который используется для подключения по ATM Adaptation Layer 5 (AAL5), который является основной альтернативой PPPoE для DSL.

PPP представляет собой целое семейство протоколов: протокол управления линией связи (LCP), протокол управления сетью (NCP), протоколы аутентификации (PAP, CHAP), многоканальный протокол PPP (MLPPP).

**Основные характеристики**

PPP протокол был разработан на основе HDLC и дополнен некоторыми возможностями, которые до этого встречались только в проприетарных протоколах.

**Автоматическая настройка**

Link Control Protocol (LCP) обеспечивает автоматическую настройку интерфейсов на каждом конце (например, установка размера пакетов) и опционально проводит аутентификацию. Протокол LCP работает поверх PPP, то есть начальная PPP связь должна быть до работы LCP.

RFC 1994 описывает Challenge-handshake authentication protocol (CHAP)), который является предпочтительным для соединений с провайдерами.

Другим вариантом аутентификации через PPP является Extensible Authentication Protocol (EAP).[1]

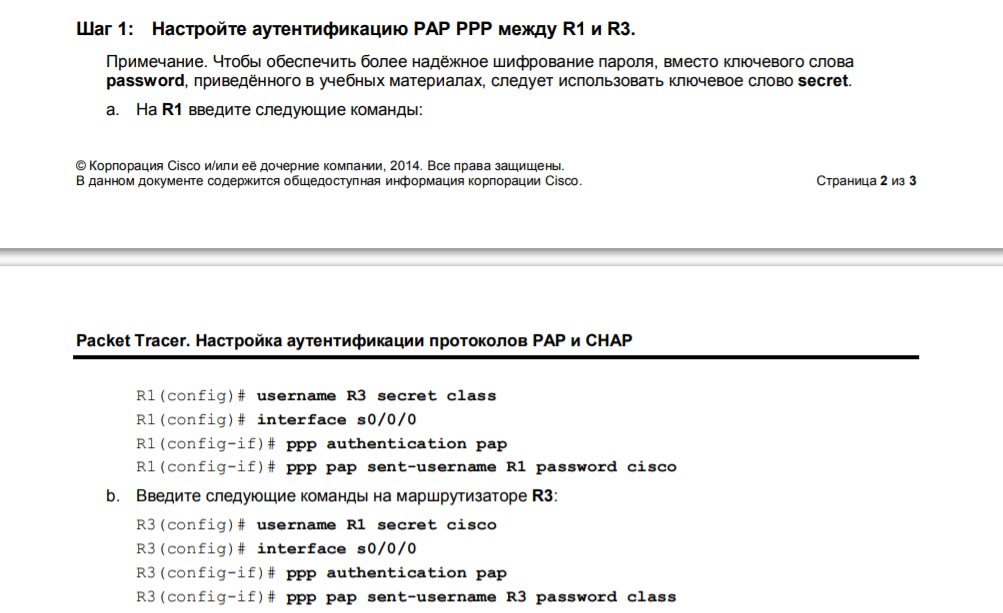
После того, как соединение было установлено, поверх него может быть настроена дополнительная сеть. Обычно, используется Internet Protocol Control Protocol (IPCP), хотя Internetwork Packet Exchange Control Protocol (IPXCP) и AppleTalk Control Protocol (ATCP) были когда-то популярны. Internet Protocol Version 6 Control Protocol (IPv6CP) получит большее распространение в будущем, когда IPv6 заменит IPv4 как основной протокол сетевого уровня.

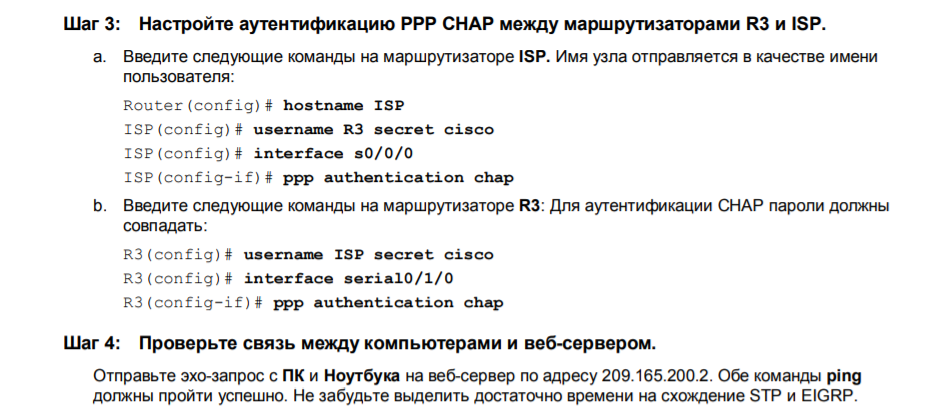
**Многопротокольная поддержка**

PPP позволяет работать нескольким протоколам сетевого уровня на одном канале связи. Другими словами, внутри одного PPP-соединения могут передаваться потоки данных различных сетевых протоколов (IP, Novell IPX и т. д.), а также данные протоколов канального уровня локальной сети. Для каждого сетевого протокола используется Network Control Protocol (NCP) который его конфигурирует (согласовывает некоторые параметры протокола).

Два производных PPP, протокол "Точка-точка" по Ethernet (PPPoE) и протокол "Точка-точка" по ATM (PPPoA), чаще всего используются интернет-провайдерами для установления интернет-соединения цифровой абонентской линии (DSL) с клиентами.

Настройка





Вопросы:

1.Список RFC: Это документы, опубликованные "Инженерной группой по сетевым запросам" (англ. Request for Comments), описывающие различные аспекты сетевых технологий, протоколов и стандартов. Они используются для разработки и определения интернет-стандартов. Примеры RFC включают RFC 791, который описывает протокол IP, и RFC 2616, который описывает протокол HTTP.

2. Описание протокола LCP: Протокол LCP (Link Control Protocol) используется в сетях PPP (Point-to-Point Protocol) для управления и настройки соединения между двумя устройствами. LCP устанавливает, тестирует и поддерживает логическое соединение между двумя удаленными устройствами.

3. Части протокола PPP:

- PPP Link Control Protocol (LCP): Устанавливает и контролирует соединение.

- PPP Network Control Protocol (NCP): Определяет протокол сети, используемый на PPP-соединении.

- PPP Data Link Layer Protocol: Определяет метод фреймования данных, такой как HDLC (High-Level Data Link Control), используемый для передачи данных.

4.Формирование PPP-кадра:

- Начало кадра: Флаг, обычно байт 01111110, указывает на начало кадра.

- Адрес: Обычно 1 байт, определяет адрес получателя.

- Управляющее поле: Обычно 1 байт, используется для контроля ошибок и управления передачей.

- Протокол: 2 байта, указывает на протокол верхнего уровня данных.

- Информация: Непосредственно данные, передаваемые по каналу.

- Контрольная сумма: 2 байта, используется для обнаружения ошибок.

5. Схема принципа алгоритма соединения протокола PPP\*\*: [Вставьте изображение схемы]

6. 3 класса LCP-пакетов:

- Configuration-Request (CR): Инициирует сеанс LCP и предлагает конфигурацию параметров.

- Configuration-Acknowledge (CA): Подтверждает успешное установление параметров конфигурации.

- Termination-Request (TR): Завершает сеанс LCP и закрывает соединение.

7. Правила передачи данных в канале Multilink:

- Равномерное распределение: Передача данных в канале происходит равномерно между доступными линиями.

- Ротация: Используется поочередное использование каждой линии для передачи данных.

- Сжатие: Данные могут быть сжаты перед передачей.

- Фрагментация: Большие пакеты данных могут быть разделены на более мелкие фрагменты для передачи.

- Обработка ошибок: Обработка ошибок на линиях и переключение на другую линию в случае неисправности.

- Балансировка нагрузки: Распределение нагрузки между доступными линиями для оптимизации производительности.

8. Назначение протокола PPTP: Протокол PPTP (Point-to-Point Tunneling Protocol) используется для создания виртуальных частных сетей (VPN) через общественные сети, такие как интернет.

**Port security**

Port security - это механизм безопасности, который

используется для ограничения доступа к сетевым

портам на сетевых коммутаторах или других сетевых

устройствах. Он предотвращает несанкционированный

доступ к сети путем контроля подключенных

устройств и их MAC-адресов.

Цели port security:

 Предотвращение несанкционированного доступа:

Главная цель port security состоит в том, чтобы

ограничить доступ к сетевым портам только для

авторизованных устройств.

 Защита от атак: Путем ограничения доступа к портам

можно предотвратить различные сетевые атаки, такие

как атаки переполнения буфера и атаки межсетевого

проникновения.

 Обеспечение целостности данных: Поскольку port

security позволяет идентифицировать и

аутентифицировать подключенные устройства, это

также способствует обеспечению целостности и

конфиденциальности передаваемых данных.

Принцип работы port security

Port security обычно реализуется путем привязки

определенных MAC-адресов к конкретным сетевым

портам. Это можно сделать следующими способами:

Статическая настройка: Администратор сети вручную

настраивает список разрешенных MAC-адресов для

каждого порта.

Динамическая настройка:

Сетевое устройство автоматически изучает MAC-

адреса устройств, подключенных к порту, и

динамически привязывает их к порту.

При достижении максимального количества

разрешенных MAC-адресов на порту либо новые

устройства блокируются, либо срабатывает механизм

уведомления администратора сети.

Port security является важным инструментом для

обеспечения безопасности компьютерных сетей. Этот

механизм помогает предотвратить

несанкционированный доступ, защитить сетевую

инфраструктуру от атак и обеспечить целостность

передаваемых данных. Внедрение и правильная

настройка port security играют ключевую роль в

создании надежной сетевой среды.

Настройка функции безопасности портов (Port Security) на оборудовании Cisco позволяет ограничить доступ к сети на основе MAC-адресов устройств, подключенных к портам коммутатора. Вот основные шаги для настройки port security на Cisco:

1. Включение функции безопасности портов на интерфейсе коммутатора:

```

Switch(config)# interface interface\_id

Switch(config-if)# switchport port-security

```

2. Установка максимального количества разрешенных MAC-адресов:

```

Switch(config-if)# switchport port-security maximum max\_addresses

```

3. Выбор метода обучения порта о MAC-адресах (необязательно):

```

Switch(config-if)# switchport port-security mac-address {sticky | static | dynamic}

```

4. Определение действия при нарушении безопасности:

```

Switch(config-if)# switchport port-security violation {shutdown | restrict | protect}

```

5. Необязательные настройки, такие как временные интервалы для обучения портов о MAC-адресах.

6. Сохранение настроек:

```

Switch# copy running-config startup-config

```

Пример:

```

Switch(config)# interface GigabitEthernet0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport port-security

Switch(config-if)# switchport port-security maximum 2

Switch(config-if)# switchport port-security violation restrict

Switch(config-if)# switchport port-security mac-address sticky

Switch(config-if)# end

Switch# copy running-config startup-config

```

Это простой пример настройки port security на Cisco. Важно учитывать особенности вашей сетевой инфраструктуры и требования к безопасности для корректной настройки функции безопасности портов.