Защита № 6

МНОГОУРОВНЕВАЯ OSPF. МЕТОДЫ АУТЕНТИФИКАЦИИ В ПРОТОКОЛАХ МАРШРУТИЗАЦИИ

1. Обоснование применения OSPF с несколькими областями. Типы областей Multiarea OSPF.

Для обеспечения большей эффективности маршрутизации и масштабируемости сетей протокол OSPF поддерживает иерархическую маршрутизацию с разделением на области.

Область OSPF - группа маршрутизаторов, использующих одинаковые данные о состоянии канала в своих базах данных.

Протокол OSPF с одной областью чаще используется в небольших сетях, где сеть соединений маршрутизаторов не является сложной, и стоимости маршрутов быстро вычисляются. При этом если область становится слишком большой, возникают следующие проблемы:

- большое число записей в таблице маршрутизации;
- большая база данных состояния канала, т. к. каждый маршрутизатор должен иметь запись о каждой сети в области;
- частые вычисления алгоритма SPF могут привести в большой сети к тому, что маршрутизаторы будут тратить много ресурсов на пересчет стоимостей маршрутов по алгоритму SPF и, следовательно, обновление таблицы маршрутизации даже при незначительных изменениях.

Многоуровневой OSPF (Multiarea OSPF) – это разделение области OSPF на более мелкие области. Основная область называется областью магистрали (область 0,ядро), все остальные области должны соединяться с областью магистрали.

Можно выделить следующие основные иерархии областей:

- магистральная область (Backbone area) - область, соединяющая все области, осуществляет межзонную маршрутизацию, формирует суммарные маршруты и др., для передачи информации за границу автономной системы и области используется маршруты полученные по разным протоколам маршрутизанни:
- тупиковая область (Stub area) - область, через которую не проходят пакеты маршрутизации, не принимаются пакеты с внешними маршрутами для автономной системы, но обрабатываются маршруты из других зон, для передачи информации за границу автономной системы используется маршрут по умолчанию;
- полностью тупиковая область (Totally stubby area) - область, через которую не проходят пакеты маршрутизации, не принимаются пакеты с внешними маршрутами для автономной системы и маршруты из других зон, для передач информации за границу автономной системы и области используется маршрут по умолчанию;
- NSSA (Not-so-stubby-areas) - область, через которую проходят пакеты маршрутизации разных протоколов, не принимаются пакеты с внешними маршрутами для автономной системы, но обрабатываются маршруты из других зон и протоколов, для передачи информации за границу автономной системы используется маршрут по умолчанию.
- транзитная область (Transit area) - область, соединяющая несколько областей, через эту область проходят пакеты маршрутизации OSPF, принимаются и передаются пакеты с внешними маршрутами для автономной системы и маршруты из других зон, для передачи информации за границу автономной системы используется маршрут по умолчанию.

Магистральные области соединяются с другими типами областей OSPF. Как правило, конечные пользователи не находятся в магистральной области. Базовая область также называется нулевой областью OSPF. Обычно номер магистральной области равен нулю.

2. Требования к планированию областей OSPF.

При планировании областей следует придерживаться следующих требований:

- в области должно быть не более 50 маршрутизаторов;
- маршрутизатор не должен быть более чем в трех областях;
- у любого отдельного маршрутизатора не должно быть более 60 соседей.

3. Типы маршрутизаторов OSPF.

Существует четыре различных типа маршрутизаторов OSPF:

- внутренний маршрутизатор (IR, Internal Router) - это маршрутизатор,все интерфейсы которого относятся к одной области;
- магистральный маршрутизатор (BR, Backbone Router) - маршрутизатор, у которого хотя бы один интерфейс относиться к магистральной области;
- пограничный маршрутизатор (ABR, Area Border Router) - это маршрутизатор, интерфейсы которого подключены к нескольким областям.
- пограничный маршрутизатор автономной системы (ASBR, Autonomous System Boundary Router) - это маршрутизатор, у которого по крайней мере один интерфейс подключен к внешней сети (другой автономной системе).

Пограничный маршрутизатор должен поддерживать разные базы данных для каждой области. ABR являются точками выхода для области, что означает, что информация о маршрутизации, предназначенная для другой области, может попасть туда только через ABR локальной области. Таким образом, ABR распространяют информацию о маршрутизации в магистральную область. Магистральные маршрутизаторы затем пересылают информацию другим ABR.

ASBR может импортировать информацию о сети, работающей по другому протоколу и в сеть OSPF, используя процесс, называемый перераспределением маршрутов. Перераспределение в OSPF происходит, когда ASBR соединяет разные домены маршрутизации (например, EIGRP и OSPF) и настраивает их для обмена и объявления информации о маршрутизации между этими доменами маршрутизации.

4. Особенности конфигурации OSPF для нескольких областей. Принципы использования переадресации для разных типов областей OSPF.

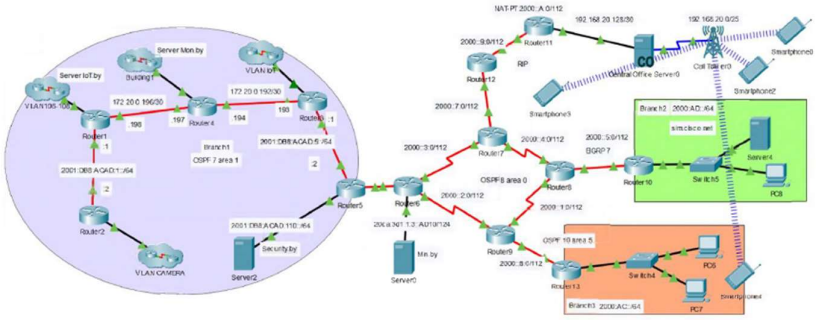

Рисунок 6.1 – Пример сети с применением нескольких областей OSPF

Рассмотрим пример конфигурации протокола OSPF для разных областей на примере сети, представленной на рисунке 6.1.Все сети соединяются посредством подсети соединений маршрутизаторов с маршрутизацией OSPF со значением Process ID, равным 8, и областью 0. Все остальные подсети сгруппированы в кластеры, между подсетями настроена маршрутизация OSPF с Process ID, равным 7, и областью 1.

Маршрутизаторы области 0 соединены между собой последовательным соединением. Связь через последовательное соединение - это метод передачи данных, при котором данные передаются последовательно по одному каналу. В параллельной связи биты могут передаваться одновременно по нескольким проводам. Тем не менее, параллельные соединения имеют проблемы с перекрестными помехами между проводами, особенно с увеличением длины провода. Другой проблемой параллельного соединения является ресинхронизация данных, которая происходит, когда данные по различным проводам не поступают одновременно. Наконец, большинство параллельных соединений поддерживает только однонаправленную, исходящую связь.

Благодаря своей двунаправленной способности последовательная связь значительно дешевле в реализации. Последовательная связь использует меньше проводов, более дешевые кабели и меньше контактов разъема.

Конфигурация последовательных интерфейсов осуществляется аналогично со всеми другими интерфейсами маршрутизатора. Для входа в режим конфигурации используется команда interface Serial_номер. Команды для конфигурации IP-адреса или маршрутизации аналогичные.

Основной задачей в сети, представленой на риснуке 6.1, является настройка и передача данных из одной области OSPF в другую. На маршрутизаторе Router6 настроен суммарный статический маршрут в область 1 OSPF 7, для того чтобы передавать в другие области и протоколы данный маршрут в конфигурации протокола OSPF необходимо настроить перераспределение статических маршрутов следующим образом:

```
Router6(config)#ipv6 router ospf 8
Router6(config-rtr)#redistribute static
Router6(config-rtr)#redistribute connected
```

Интерфейсы маршрутизатора Router9 также подключены к разным областям и процессам OSPF и настраиваются аналогично примеру на рисунке 6.5. Однако на маршрутизаторе Router9 не настроен статический маршрут в подсеть Branch3, поэтому здесь необходимо осуществить перераспределение маршрутов из одной области в другую следующим образом:

```
Router9(config)#ipv6 router ospf 10
Router9(config-rtr)#default-information originate
Router9(config-rtr)#redistribute ospf 8 metric 10 match
external 2
Router9(config-rtr)#ipv6 router ospf 8
Router9(config-rtr)#default-information originate
Router9(config-rtr)#redistribute ospf 10 metric 3
```

На маршрутизаторе Router10 интерфейсы подключены к домену маршрутизации OSPF и EIGRP, для которых перераспределение настраивалось следующим образом:

```
Router8(config)#ipv6 router ospf 8
Router8(config-rtr)# redistribute eigrp 7 metric 10000 20
255 1 1500
Router8(config-rtr)#ipv6 router eigrp 7
Router8(config-rtr)# redistribute ospf 8  metric 10000 20
255 1 1500 match external 2
```

5. Стандарты последовательной связи и типы соединения DTE-DCE, DTE-DTE.

Можно выделить следующих три основных стандарта последовательной связи:

- RS-232 - интерфейс общего назначения, который можно использовать практически для любых типов устройств;
- V.35 - это стандарт интерфейса, используемый большинством маршрутизаторов для высокоскоростного синхронного обмена данными, объединяет полосу пропускания нескольких телефонных цепей.
- HSSI (High-Speed Serial Interface) - высокоскоростной последовательный интерфейс поддерживает скорость передачи до 52 Мбит/с, используется для соединения маршрутизаторов в локальных сетях с глобальными сетями по высокоскоростным линиям, таким как линии Т3.

Интерфейс RS-232 обеспечивает соединение двух устройств, одно из которых называется DTE (Data Terminal Equipment) или ООД (Оконечное Оборудование Данных),

второе - DCE (Data Communications Equipment) или ОПД (Оборудование Передачи Данных).

С точки зрения подключения к глобальной сети с использованием последовательного соединения должно быть устройство DTE на одном конце соединения и устройство DCE на другом конце. Иначе говоря, устройство DTE соединяет клиентское оборудования с сетью WAN, DCE - устройство для преобразования пользовательских данных в форму, приемлемую для линии передачи поставщика услуг WAN. DTE также может быть маршрутизатором, компьютером, принтером, т. е. любым устройством, которое подключается напрямую к сети поставщика услуг. Первоначально концепция DCE и DTE основывалась на двух типах оборудования: оконечное оборудование, которое генерировало или получало данные, и оборудование связи, которое только передавало данные.

Изначально стандарт RS-232 определял только соединение DTE и DCE, которые были модемами. Однако для подключения двух DTE, например, двух маршрутизаторов, специальный кабель, называемый нуль-модемом, устраняет необходимость в DCE. Другими словами, два устройства могут быть подключены без модема. Нуль-модем - это способ связи, позволяющий напрямую подключить два DTE с помощью последовательного кабеля RS-232. Для нульмодемного соединения линии передачи (Tx) и приема (Rx) организуются, как показано на рисунке 6.2. При использовании нуль-модемного кабеля в соединении маршрутизатор-маршрутизатор один из последовательных интерфейсов должен быть настроен как конец DCE для обеспечения тактового сигнала для соединения.

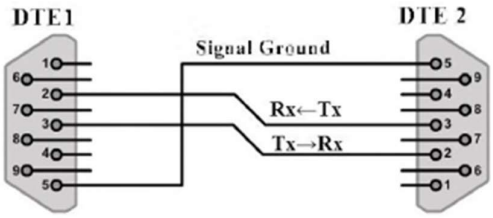

Рисунок 6.2 – Соединение линии передачи (Tx) и приема (Rx) с помощью последовательного кабеля RS-232

Кабель для подключения DTE к DCE представляет собой экранированный последовательный переходный кабель. Конец маршрутизатора экранированного последовательного переходного кабеля может быть разъемом DB-60,который подключается к порту DB-60 на последовательной интерфейсной карте WAN. Другой конец последовательного переходного кабеля имеет разъем, подходящий под необходимый стандарт. Для поддержки более высокой плотности портов используется кабель Smart Serial. Конец интерфейса маршрутизатора кабеля Smart Serial представляет собой 26-контактный разъем, который значительно компактнее, чем DB-60.

6. Сравнение протоколов инкапсуляции для передачи данных через последовательные интерфейсы.

Перед передачей данных по последовательному интерфейсу используются следующие протоколы инкапсуляции:

- HDLC - используется по умолчанию для соединений точка-точка, является основой для синхронного PPP, используемого многими серверами для подключения к глобальной сети;
- PPP - обеспечивает соединение маршрутизатор-маршрутизатор и оконечное устройство-сеть по синхронным и асинхронным каналам, работает с протоколами сетевого уровня (IPv4 и IPv6), использует протокол инкапсуляции HDLC, но также имеет встроенные механизмы безопасности, такие как PAP и CHAP;
- SLIP (Serial Line Internet Protocol) - стандартный протокол для последовательных соединений с использованием TCP/IP, считается устаревшим и заменен протоколом PPP;

- X.25 - стандарт, который определяет, как поддерживаются соединения между DTE и DCE для удаленного доступа в сетях общего пользования, является предшественником Frame Relay.
- Frame Relay - промышленный стандарт, коммутируемый протокол канального уровня, который обрабатывает несколько виртуальных каналов;
- ATM - международный стандарт для ретрансляции, в котором устройства отправляют несколько типов данных (голос, видео, данные) в ячейках фиксированной длины (53 байта), позволяющие выполнять обработку на оборудовании сокращать транзитные задержки.

7. Описание протокола HDLC и типы поддерживаемых кадров, описание полей.

HDLC - это бит-ориентированный протокол синхронного канального уровня, разработанный ISO. HDLC использует синхронную последовательную передачу для обеспечения безошибочной связи между двумя точками, определяет структуру кадра, которая позволяет управлять потоком и контролем ошибок посредством использования подтверждений. Каждый кадр имеет одинаковый формат, будь то кадр данных или кадр управления. Когда кадры передаются по синхронным или асинхронным каналам связи, эти каналы не имеют механизма для маркировки начала или конца кадров. По этой причине HDLC использует разделитель или флаг кадра, чтобы отметить начало и конец каждого кадра. HDLC определяет три типа кадров (рисунок 6.9), каждый из которых имеет свой формат поля управления.

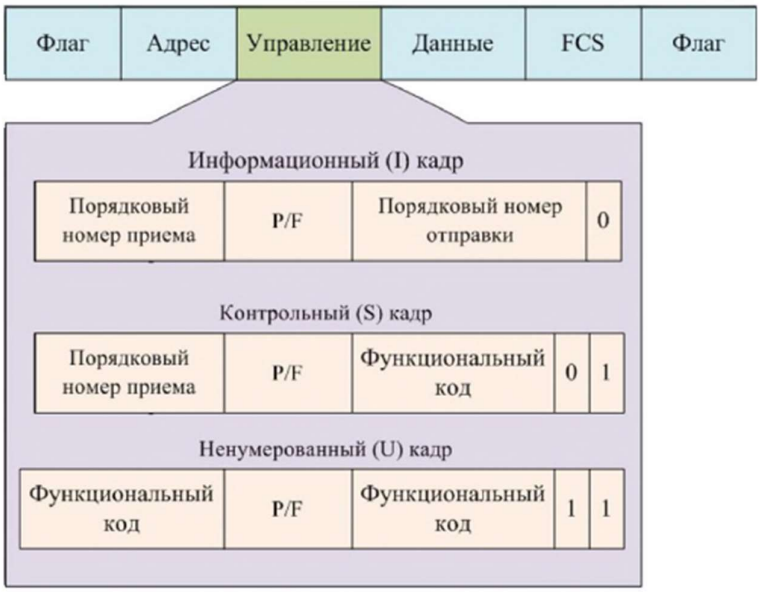

Рисунок 6.9 – Форматы кадров протокола HDLC

Поле флага инициирует и завершает проверку ошибок. Кадр всегда начинается и заканчивается 8-битным полем флага, битовый шаблон которого представляется в двоичном формате 01111110. Поскольку существует вероятность того, что этот шаблон встречается в реальных данных, отправитель HDLC всегда вставляет бит 0 после каждых пяти последовательных единиц в поле данных. Получатель удаляет вставленные биты. Когда кадры передаются последовательно, флаг окончания первого кадра используется в качестве флага начала следующего кадра.
Поле адреса содержит адрес HDLC. Этот адрес может содержать конкретный адрес, групповой адрес или широковещательный адрес. Основной адрес является либо источником, либо назначения. 0x0F-одноадресные, 0x8F-широковещательные пакеты.
Поле управления использует три различных формата в зависимости от типа используемого кадра HDLC:
- информационный (1) кадр - 1-кадры несут информацию управления.

Кадр содержит порядковые номер отправки и приема, бит опроса (P/F), который выполняет управление потоком и ошибками. Порядковый номер отправки относится к номеру кадра, который должен быть отправлен следующим. Порядковый номер приема предоставляет номер кадра, который должен быть получен следующим. И отправитель, и получатель поддерживают порядковые номера отправки и приема. Отправитель использует бит P/F, чтобы сообщить, требуется ли немедленный ответ. Получатель – чтобы сообщить отправителю, является ли текущий кадр последним в текущем ответе.
- контрольный (S) кадр - S-кадры предоставляют управляющую информацию. S-кадр может запрашивать и приостанавливать передачу, сообщать о состоянии и подтверждать получение 1-кадров. S-кадры не имеют информационного поля.
- ненумерованный (U) кадр - U-кадры поддерживают управление и не передают данные порядковых номеров. В зависимости от функции U-кадра его поле управления составляет 1 или 2 байта. Некоторые U-кадры имеют информационное поле.
Поле данных содержит информацию блока информации о пути (PIU) или идентификации (XID).
Последовательность проверки кадра (Frame Check Sequence, FCS) предшествует конечному разделителю флага и обычно является остатком вычисления циклического избыточного кода (Cyclic Redundancy Check, CRC). Расчет CRC повторяется получателем. Если результат отличается от значения в исходном кадре, значит, присутствует ошибка передачи.

8. Компоненты протокола PPP и их назначение.

Протокол PPP также инкапсулирует кадры данных для передачи по физическим каналам уровня 2. PPP устанавливает прямое соединение, используя последовательные кабели, телефонные линии, магистральные линии, радио или оптоволоконные каналы.

PPP содержит три основных компонента:

- инкапсуляцию подобную протоколу HDLC для транспортировки многопротокольных пакетов по каналам точка-точка;
- расширяемый протокол управления каналом (Link Control Protocol, LCP) для установления, настройки и тестирования соединения канала передачи данных:
- семейство протоколов управления сетью (Network Control Protocols, NCP) для установления и настройки различных протоколов сетевого уровня.

LCP функционирует на канальном уровне и играет роль в установлении, настройке и тестировании соединения. LCP устанавливает связь точка-точка, а также согласовывает и устанавливает параметры управления в канале передачи данных WAN, которые обрабатываются на сетевом уровне. LCP обеспечивает автоматическую настройку интерфейсов на каждом интерфейсе, включая:
- обработку различных ограничений на размер пакета;
- обнаружение распространенных ошибок в конфигурации;
- завершение соединения;
- определение того, работает ли соединение правильно или когда оно выходит из строя.

После установления связи PPP также использует LCP для автоматического согласования форматов инкапсуляции, таких как аутентификация, сжатие и обнаружение ошибок.

NCP включают функциональные поля, содержащие стандартизированные коды для указания протокола сетевого уровня, который инкапсулирует PPP. Каждый NCP управляет конкретными функциями, необходимыми для соответствующих протоколов сетевого уровня. Различные компоненты NCP инкапсулируют и

согласовывают параметры для нескольких протоколов сетевого уровня.

Таблица 6.1 – Коды полей протокола PPP

Код	Название протокола
8021	Протокол IPv4
8057	Протокол IPv6
8023	Протокол сетевого уровня модели OSI
8029	AppleTalk
802b	Novell IPX
c021	Протокол канального уровня модели OSI
c023	Протокол парольной аутентификации PAP
c223	Протокол парольной аутентификации PHAP

9. Формат кадра PPP, описание полей.

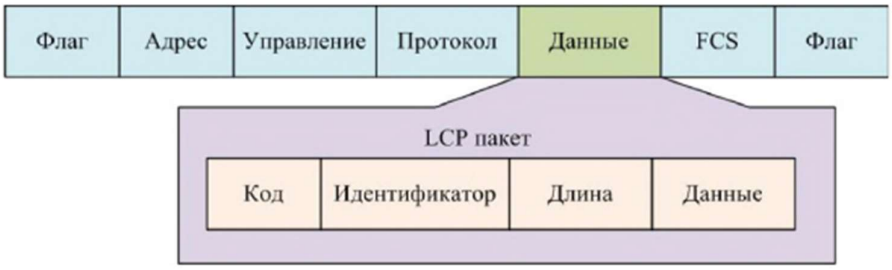

Рисунок 6.12 – Структура кадра PPP

Кадр PPP состоит из шести полей:

- флаг - одиночный байт, указывающий начало или конец кадра, состоит из двоичной последовательности 01111110;
- адрес - один байт, содержащий двоичную последовательность 11111111 (стандартный широковещательный адрес);
- управление - один байт, содержащий двоичную последовательность 00000011, которая требует передачи пользовательских данных в неупорядоченном кадре, что обеспечивает услугу связи без установления соединения;
- протокол - два байта, которые идентифицируют протокол, инкапсулированный в информационном поле кадра;
-данные - ноль или более байтов, которые содержат дейтаграмму для протокола, указанного в поле протокола;
- последовательность проверки кадра (FCS) - обычно 16 бит (2 байта).

10. Описание этапов установления соединения PPP.

Существует три этапа установления соединения PPP.

Этап 1. Установление соединения и согласование конфигурации. Прежде чем PPP обменивается дейтаграммами сетевого уровня, такими как IP, LCP должен сначала открыть соединение и согласовать параметры конфигурации. Эта фаза завершается, когда принимающий маршрутизатор отправляет кадр подтверждения конфигурации обратно в маршрутизатор, инициирующий соединение.

Этап 2. Определение качества канала (необязательно). LCP проверяет канал, чтобы определить, является ли качество канала достаточным для запуска. протоколов сетевого уровня. LCP может задержать передачу информации протокола сетевого уровня до завершения этой фазы.

Этап 3. Согласование конфигурации протокола сетевого уровня. После того, как LCP завершил фазу определения качества соединения, соответствующий NCP может отдельно настроить протоколы сетевого уровня, а также в любое время активировать и отключить их. Если LCP закрывает канал, он информирует протоколы сетевого уровня, чтобы они могли предпринять соответствующие действия. Канал остается сконфигурированным для связи до тех пор, пока кадры LCP или NCP не закроют канал, или пока не произойдет какое-либо внешнее событие, например, истечение таймера бездействия или

вмешательство администратора.
Работа LCP включает в себя установление соединения, обслуживание канала и закрытие соединения (рисунок 6.13).

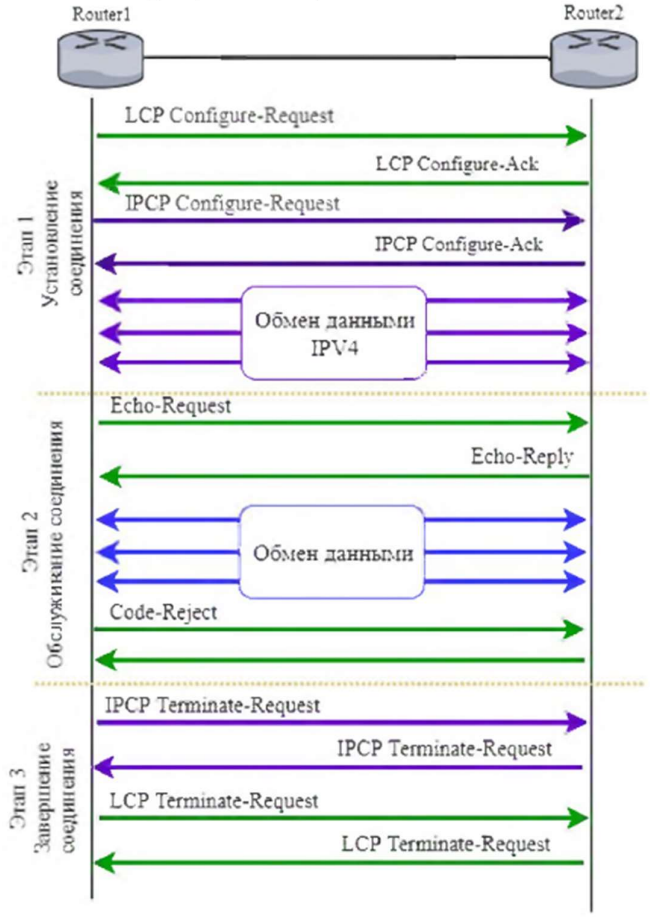

Рисунок 6.13 – Этапы установления соединения PPP

Таблица 6.2 – Коды пакета LCP

LCP код	Тип пакета LCP	Описание
1	Configure-Request	Отправляется для открытия или сброса соединения PPP, содержит список параметров LCP.
2	Configure-Ack	Отправляется, когда все значения параметров LCP в последнем полученном запросе настройки распознаны и приняты.
3	Configure-Nak	Отправляется, когда все параметры LCP распознаны, но значения некоторых параметров не принимаются. Configure-Nak включает параметры несоответствия и их допустимые значения.
4	Configure-Reject	Отправляется, когда параметры LCP не распознаны или неприемлемы для установления соединения. Configure-Reject включает нераспознанные или необоротные параметры.
5	Terminate-Request	Отправляется для закрытия PPP-соединения.
6	Terminate-Ack	Отправляется в ответ на Terminate-Request.
7	Code-Reject	Отправляется, когда код LCP неизвестен. Code-Reject включает в себя отклоненный пакет LCP.
8	Protocol-Reject	Отправляется, когда кадр PPP содержит неизвестный идентификатор протокола. Сообщение Protocol-Reject включает в себя отклоненный пакет LCP.
9	Echo-Request	Отправляется для тестирования PPP-соединения.
10	Echo-Reply	Отправлено в ответ на Echo-Request. Echo-Request и Echo-Reply не связаны с сообщениями ICMP.
11	Discard-Request	Отправляется для осуществления соединения в исходящем направлении.

11. Отличия типов аутентификации протокола PPP, особенности их конфигурации.

Методы аутентификации PPP

- **По паролю (PAP, Password Authentication Protocol)** – это простой процесс обмена сообщениями, содержащими имя пользователя и пароль, без шифрования
- **По вызову (CHAP, Challenge Handshake Authentication Protocol)** – обеспечивает защиту, используя переменное значение, которое является уникальным и непредсказуемым, т. к. результирующее значение хеша является уникальным и случайным

Конфигурация PAP для Router8-Router7

На маршрутизаторе Router8:

```
Router8(config)#username Router7 password 0 pass-router7
Router8(config)#interface Serial0/0/0
Router8(config-if)#shutdown
Router8(config-if)#ppp authentication pap
Router8(config-if)#ppp pap sent-username Router8 password 0 pass-router8
Router8(config-if)#no shutdown
Router8(config-if)#exit
```

На маршрутизаторе Router7:

```
Router7(config)#username Router8 password 0 pass-router8
Router7(config)#interface Serial0/0/1
Router7(config-if)#shutdown
Router7(config-if)#ppp pap sent-username Router7 password 0 pass-router7
Router7(config-if)#no shutdown
Router7(config-if)#exit
```

Конфигурация CHAP для Router8-Router7

На маршрутизаторе Router6:

```
Router6(config)#username Router7 password chap-312
Router6(config)#interface Serial0/0/0
Router6(config-if)#shutdown
Router6(config-if)#ppp authentication chap
Router6(config-if)#no shutdown
```

На маршрутизаторе Router7:

```
Router(config)#hostname Router7
Router7(config)#username Router6 password chap-312
Router7(config)#interface Serial0/0/0
Route7(config-if)#shutdown
Route7(config-if)#ppp authentication chap
Router7(config-if)#no shutdown
```

Когда PPP завершает фазу установления соединения, удаленный узел повторно отправляет сообщение с именем пользователя и паролем и ожидает подтверждение. Необходимо отметить, что после завершения аутентификации PAP не требуется повторного подтверждения подлинности, что может привести к атакам. В отличие от аутентификации PAP в процессе аутентификации CHAP проводит периодические проверки подтверждения подлинности. При аутентификации CHAP после завершения этапа установления соединения PPP маршрутизатор отправляет сообщение вызова на удаленный узел, который должен отправить значение, рассчитанное с использованием однонаправленной хеш-функции по алгоритму MD5 на основе пароля и сообщения вызова. Локальный маршрутизатор проверяет ответ по собственному расчету значения хеш-функции. Если значения совпадают, инициирующий узел подтверждает аутентификацию. Если значение не совпадает, инициирующий узел немедленно прерывает соединение.

12. Особенности сопряжения сетей с технологией LTE с глобальной сетью.

Технология LTE является самой перспективной технологией широкополосной мобильной связи с точки зрения производительности. Для операторов мобильной связи увеличение производительности заключается в возможности увеличения емкости сети и пропускной способности в совокупности с большими скоростями передачи трафика и меньшими задержками передачи пакетов. Это позволяет быстро развивающимся беспроводным средствам телекоммуникаций поддерживать мультимедийные приложения и обеспечивать максимальное расширение использования в сети протокола 1P. Переход на IP-платформу позволяет оператору связи без проблем наращивать пропускную способность и предоставлять новые сервисы. В то же время вследствие масштабируемости и гибкости сети, операторы мобильной связи сталкиваются с экономическими проблемами, так как их магистральные сети испытывают сложности, связанные с сокращением расходов. Поэтому, в настоящее время многие операторы связи переводят свои опорные сети на сети, построенные на основе технологии Ethernet, позволяющей обеспечить качество и продолжительность связи сетей 4G и Интернета. В иерархии мобильной связи можно выделить опорную сеть (backhaul), выполняющую роль в предоставлении мобильных услуг и относящуюся к той части иерархической сети, которая является связующим звеном между глобальной сетью и любой базовой сетью. Backhaul принимает на себя основную нагрузку по организации связи между элементами сети мобильного доступа и магистральной сетью оператора. Это означает, что ее роль заключается в транспортировке данных от мобильного абонента к сетевому оборудованию оператора мобильной связи и через него к другим операторам. То есть, опорная сеть является связующим компонентом между магистральной сетью и сетями передачи данных. На рисунке 6.1 опорная сеть для передачи данных к абонентам мобильной связи представлена базовой станцией мобильной связи (Cell Tower) и сервером, принимающем вызовы абонентов (Central Office Server), которые соединяются коаксиальным кабелем. Далее сервер подключается к маршрутизатору Routerl 1 с использованием интерфейса FastEthernet. Между маршрутизаторами Router7, Routerl 1, Routerl2 настроена маршрутизация RIP.