Защита №5

Маршрутизация в глобальных сетях

1.Организация доступа к глобальной сети, типы операторов связи

Глобальная сеть (WAN) - система связанных между собой информационных сетей, предоставляющих доступ региональным сетям и оконечным устройствам, расположенных на удаленных расстояниях. Основная функция глобальной сети заключается в обеспечение взаимосвязи информационных сетей, маршрутизации трафика между ними, поддержание оптимальной пропускной способности. Доступ к глобальной сети предоставляется операторами связи, которые выделяют каналы определенной пропускной способности по установленному тарифному плану для подключения удалённых сетей и устройств. Если для подключения к глобальной сети организации требуется канал связи, то физическое подключение (арендованная линия) арендуется у оператора связи, которое подразумевает предоставление предустановленного канала связи глобальной сети, идущего от помещения заказчика к сети оператора связи.

Различают следующие типы операторов связи:

- Tier 1 ISP - провайдер, который имеет доступ ко всей региональной таблице маршрутизации исключительно через пиринговые взаимоотношения, не должен оплачивать транзит трафика;

- Tier 2 ISP - операторы, покупающие и продающие транзитный трафик в пределах интернет-региона;

- Tier-3 ISP - оператор, который для доступа к сети Интернет использует исключительно каналы, которые покупает у других операторов.

Пиринговые взаимоотношения - соглашение интернет-операторов об обмене трафиком между своими сетями, а также техническое взаимодействие, реализующее соединение сетей и обмен информацией о сетевых маршрутах по протоколу BGP.

Транзит трафика - услуга по предоставлению широкополосного доступа в глобальную сеть для операторов связи, через оптические сети передачи данных другого оператора на платной основе.

2. Автономная система, ее регистрация, типы регистраторов.

Для учета всех сетей операторов введены автономные системы.

Автономная система (AS) - система сетей и сетевых устройств, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации с глобальной сетью.

Номера автономных систем представляют собой 16-битные или 32-битные номера, которые выделяются локальным или региональным интернет-регистраторами.

Выделяют пять основных региональных регистраторов:

- American Registry for Internet Numbers (ARIN) - обслуживает сети Северной Америки;
- RIPE Network Coordination Centre (RIPE NCC) - обслуживает сети стран Европы, Ближнего Востока, Центральной Азии;

- Asia-Pacific Network Information Centre (APNIC) - обслуживает сети Азии, Тихоокеанского региона;
- Latin American and Caribbean Internet Addresses Registry (LACNIC) - обслуживает сети Латинской Америки, Карибского региона;
- African Network Information Centre (AfriNIC) – обслуживает сети Африканского континета.

Как правило статус локальных регистраторов имеют различные государственные и частные провайдеры.

Для регистрации автономной системы LIR или RIR необходимо предоставить следующую информацию:
- реквизиты организации;
- сведения (номера) о других автономных системах (минимум две), которые готовы с взаимодействовать с регистрируемой AS, как правило это AS операторов, которые предоставляют свои каналы связи;
- запрос определенного количества публичных IP-адресов;
- описать технические характеристики подключаемой сети, указать оборудование, которое будет обслуживать AS.

3. Принципы функционирования протокола BGP для внутренней и внешней маршрутизации.

Для маршрутизации между АС используется протокол BGP, который представляет собой протокол динамической маршрутизации передачи карты маршрутов до всех остальных маршрутизаторов в других АС. Протокол BGP может использоваться для внутренней маршрутизации – IGP или IBGP (Internal BGP), и для внешней - EGP или EBGP (External BGP). Принцип работы IBGP похож на алгоритм SPF в протоколе OSPF. Протокол EBGP основан на формирование атрибутов, включающих различные атрибуты для построения оптимального маршрута. Маршрутизатор, подключенный к глобальной сети (пограничный маршрутизатор) сообщает своим соседям, какие сети и АС достижимы через него. Обмен подобной информацией позволяет пограничным маршрутизаторам занести в таблицу маршрутизации записи о сетях, находящихся в других АС. При необходимости эта информация потом распространяется внутри автономной системы с помощью протоколов внутренней маршрутизации (OSPF, EIGRP, RIP).

Принципиальным отличием внешней маршрутизации от внутренней является наличие маршрутной политики, то сеть при расчете маршрута рассматривается не только метрики и математические расчеты, а множество других атрибутов. Алгоритмы расчета метрик в дистанционно-векторных протоколах и состояния каналов являются непригодными для глобальной маршрутизации, так как каждый узел передачи данных должен определять самостоятельно, не полагаясь на расчет метрики соседним устройством.

В протоколе BGP используется подход под названием «вектор пути», который в отличие от вектора расстояний, содержит адрес сети и список атрибутов пути, описывающих различные характеристики маршрута от маршрутизатора-отправителя в указанную сеть.

4. Список атрибутов BGP, расчет метрики.

Список атрибутов пути:

- **ASPATH** - список номеров AS, через которые должен пройти пакет на пути в указанную сеть;
- **NEXTHOP** - IP-адрес следующего маршрутизатора на пути достижения сети назначения;
- **ORIGIN** - обязательный атрибут, указывающий источник информации о маршруте: 0 (информация о достижимости сети получена от протокола внутренней маршрутизации или введена администратором); 1 (от протокола внешней маршрутизации), 2 — INCOMPLETE (из перераспределения, например, из RIP в OSPF, а затем в BGP);
- **MULTI _EXIT_DISC** - необязательный атрибут, представляющий собой приоритет использования объявляющего маршрутизатора для достижения через него анонсируемой сети, то есть фактически это метрика маршрута с точки зрения анонсирующего маршрут BGP-маршрутизатора. Используется не само значение, а разница значений, когда несколько маршрутизаторов одной AS объявляют о достижимости через себя одной и той же сети, предоставляя таким образом получателям несколько вариантов маршрутов в эту сеть. Пакеты в объявляемую сеть будут посылаться через маршрутизатор, заявивший меньшее значение MULTIEXITDISC.
- **LOCAL PREF** - необязательный атрибут, устанавливающий для данной AS приоритет данного маршрута среди всех маршрутов к заявленной сети;
- **ATOMIC AGGREGATE и AGGREGATOR-** необязательные атрибуты, связанные с операциями агрегирования нескольких маршрутов в один.

Атрибут ASPATH используется для:

- обнаружения петель, т. е. если номер одной и той же AS встречается в ASPATH дважды, значит маршрут неверно построен;
-вычисления метрики маршрута, *метрикой является число AS, через которые должен пройти пакет в сеть назначения*;
- применения маршрутной политики, если ASPATH содержит номера недоступных AS, то данный маршрут исключается из рассмотрения.

(Отличие IBGP от EBGP состоит в том, что при объявлении маршрута соседнему маршрутизатору, находящемуся в той же AS, маршрутизатор не должен добавлять в AS PATH номер своей автономной системы. Если номер AS будет добавлен, и соседний маршрутизатор анонсирует этот маршрут далее, то одна и та же AS будет указана в атрибуте AS_PATH дважды, что приведет к образованию петли. Также для исключения петель используются сервера маршрутной информации (аналог выделенного маршрутизатора в OSPF), которые обслуживают группу BGP-маршрутизаторов. Принцип работы сервера маршрутной информации заключается в получении маршрутов от одного маршрутизатора группы и их рассылка другим маршрутизаторам.)

5. Процесс отбора маршрутов по протоколу BGP, базы данных BGP.

Таблица 5.1 – Базы данных RIB (Routing Information Base) протокола BGP

Название	Описание
ADJ-RIBS-IN	Содержит маршрутную информацию, которая получена из сообщений UPDATE
LOC-RIB	Содержит локальную маршрутную информацию, которую маршрутизатор отобрал, руководствуясь маршрутной политикой, из ADJ-RIBS-IN
ADJ-RIBS-OUT	Содержит информацию, которую локальный маршрутизатор отобрал для рассылки соседям с помощью сообщений UPDATE

Маршрутизатор использует три базы данных и две политики: политика приема маршрутов и политика анонсирования маршрутов.

Для обработки маршрутов в базах данных в соответствии с имеющимися политиками маршрутизатор выполняет процедуру под названием процесс отбора (Decision Process), состоящий из следующих этапов:

1. Для полученных маршрутов из базы данных ADJ-RIBS-IN в соответствии с политикой приема вычисляется приоритет и значение атрибут LOCALPREF, в результате некоторые маршруты могут быть признаны неприемлемыми.

2. Для каждой сети из всех имеющихся (полученных и неприемлемых) вариантов выбирается маршрут с большим приоритетом, который заносятся в базу LOC-RIB и таблицу маршрутизации.

3. Из LocRIB выбираются маршруты, соответствующие политике анонсирования, и результат помещается в базу Adj-RIBsOut, содержимое которой рассылается соседям.

Отбор маршрутов из базы ADJ-RIBS-IN может производиться по следующим критериям:

- регулярное выражение для значения ASPATH (частные случаи: номер конечной AS маршрута, AS соседа, от которого получен маршрут);
- адрес сети, в которую ведет маршрут;
- адрес соседа, приславшего информацию о маршруте;
- происхождение маршрута (атрибут ORIGIN).

К маршруту, удовлетворяющему установленному критерию, можно применить следующие политики:

- не принимать маршрут, удалить из ADJ-RIBS-IN;
- установить административный вес маршрута,
- установить значение атрибута LOCAL PREF,
- установить маршрут в качестве маршрута по умолчанию.

Если после выполнения первого этапа отбора в базе ADJ-RIBS-IN имеется несколько альтернативных маршрутов, ведущих в одну сеть назначения, то отбор лучшего из них производится на втором этапе, исходя из следующих критериев:
- наибольшее административное расстояние;
- наибольшее значение LOCALPREF;
- кратчайший ASPATH (маршрут, порожденный в локальной AS, имеет самый короткий путь, а значит пустое значение атрибута AS PATH);
- наименьшее значение ORIGIN;
- наименьшее значение MULTIEXITDISC;
- маршрут, полученный по EBGP, против маршрута, полученного по IBGP;
- если все маршруты получены по IBGP, то выбирается маршрут через ближайшего соседа;
- маршрут, полученный от BGP-соседа с наименьшим идентификатором (1P-адресом).
Критерии последовательно применяются в указанном порядке, пока не останется единственный маршрут

Отбор маршрутов в базу ADJ-RIBS-OUT может производиться по следующим критериям:
- регулярное выражение для значения AS PATH (номер конечной AS маршрута, AS соседа, от которого получен маршрут);
- адрес сети, в которую ведет маршрут;
- адрес соседа, которому этот маршрут объявляется;
- происхождение маршрута (атрибут ORIGIN).

К маршруту, удовлетворяющему установленному критерию, можно применить следующие политики:
- не объявлять маршрут;
- не устанавливать значение MULTI_EXIT_DISC, установить указанное значение, взять в качестве значения метрику маршрута из IGP;
- произвести агрегирование сетей;
- модифицировать ASPATH;
- заменить маршрут на маршрут по умолчанию.

6. Типы сообщений BGP.

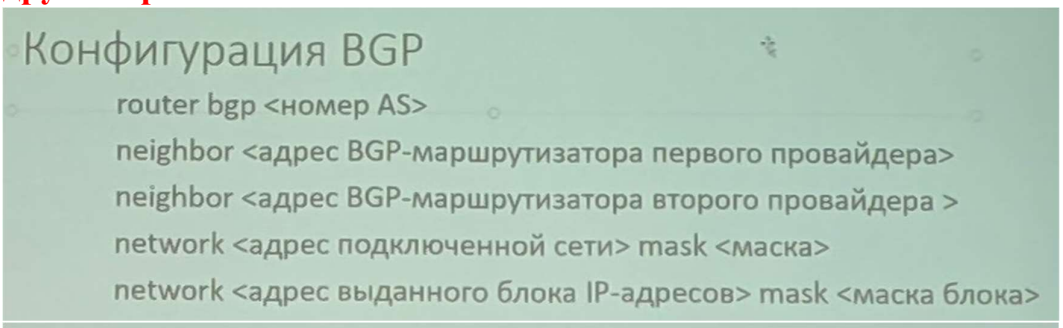
В протоколе BGP используются следующие типы сообщений:
- **OPEN** - посылается после установления TCP-соединения, ответом на которое является сообщение KEEPALIVE, если вторая сторона согласна стать соседом; иначе посылается сообщение NOTIFICATION с кодом, поясняющим причину отказа;
- **KEEPALIVE** - сообщение предназначено для подтверждения согласия установить соседские отношения, а также для мониторинга активности

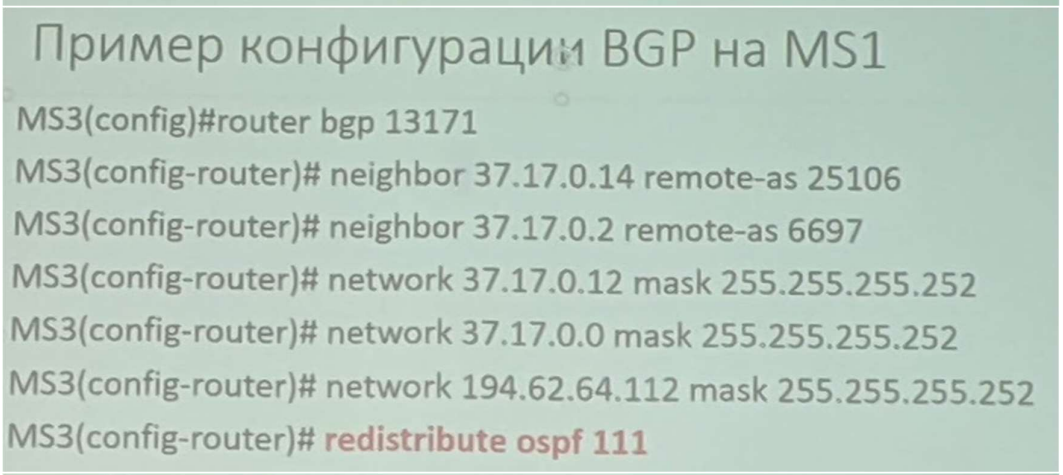
открытого соединения: BGP-соседи обмениваются KEEPALIVE-сообщениями через определенные интервалы времени.

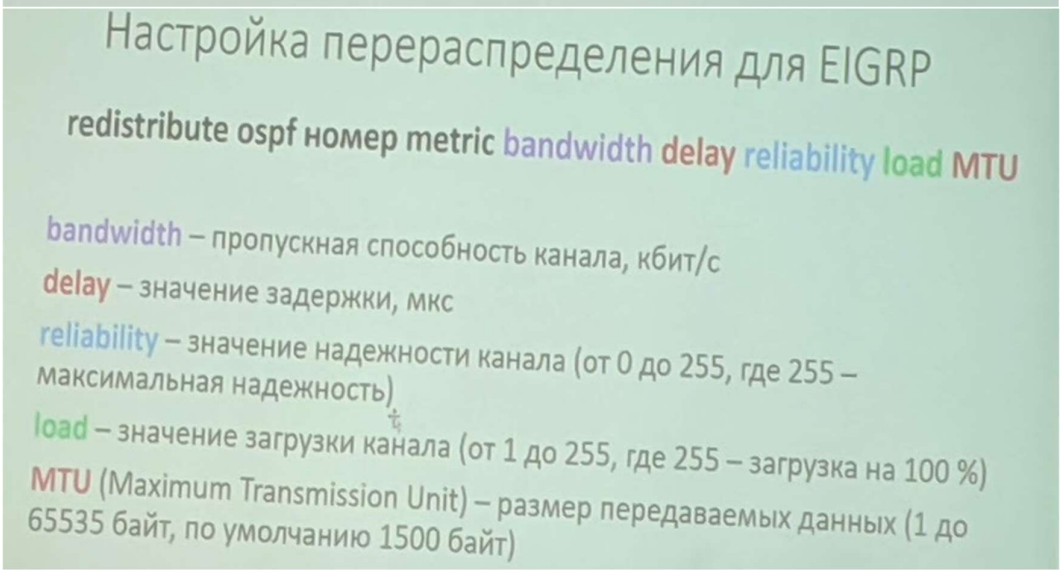
- UPDATE - сообщение предназначено для анонсирования и отзыва маршрутов. После установления соединения с помощью сообщений UPDATE пересылаются все маршруты, которые маршрутизатор хочет объявить соседу, после чего пересылаются только данные о добавленных или удаленных маршрутах по мере их появления;

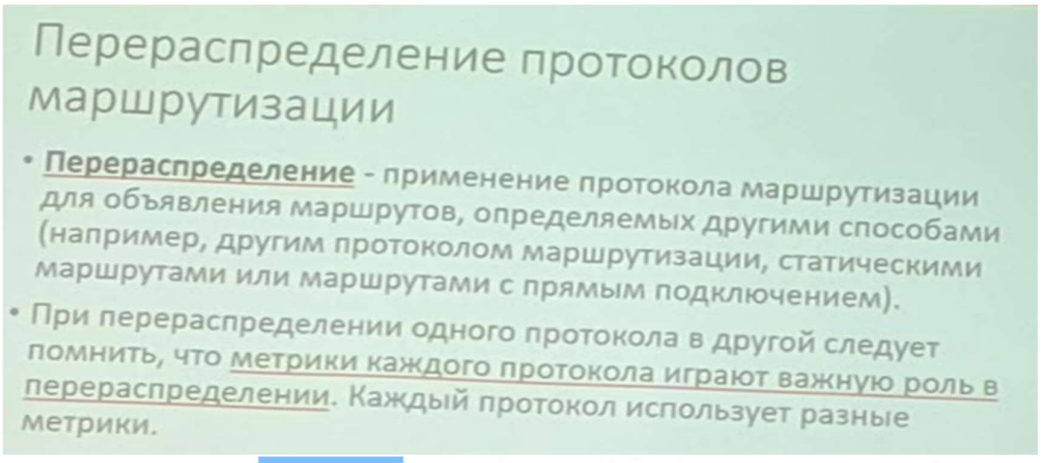
- NOTIFICATION - сообщение этого типа используется для информирования соседа о причине закрытия соединения.

7. Принцип конфигурации BGP и перераспределения маршрутов из других протоколов.









димо настроить перераспределение статических маршрутов следующим образом:

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

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
```

В представленных выше командах в OSPF 10 перераспределение внешних маршрутов (OE2) осуществляется с помощью команды `redistribute ospf 8 metric 10 match external 2`, в которой также задается и мет-

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
```

8. Доменное имя и домен. Распределение доменных имен.

Принцип работы протокола DNS в глобальных сетях имеет большие отличия. Доменные имена регистрируются в определенных доменах.

Доменное имя - символьное (буквенно-цифровое) обозначение, сформированное в соответствии с международными правилами адресации сети Интернет, предназначенное для поименованного обращения к интернет-ресурсу и связанное при его делегировании с определенным сетевым адресом.

Доменная зона (домен) - область иерархического пространства доменных имен глобальной сети, которая обозначается уникальным доменным именем.

Протокол DNS необходим не только для преобразования доменного имени в IP-адрес и наоборот, но и для поиска доменного имени в иерархической распределенной системе хранения и обработки информации о доменных зонах.

Распределение доменных имен в доменных зонах образует дерево имен со следующим уровнями:

- нулевой уровень или корневой домен, обычно обозначается точкой, которая обычно не указывается, регистратором корневого домена является организация и ICANN;

- первый уровень или национальные (региональные домены) или Top-Level Domain (TLD), принадлежат государственным организациям или крупным корпорациям, так например, администратором национальной доменной зоны .by является ОАЦ при Президенте РБ, а доменами .net и .com - компания VeriSign;

- второй уровень или Second-Level Domain (SLD), отражают название организации, владеющей веб-ресурсом или его тематику, регистраторами в РБ являются becloud.by, hoster.by, www.domain.by и др.;

-третий уровень или поддомены, представляют собой расширение доменного имени, необходимы для функционального расширения веб-ресурсов, обозначают дочерние веб-ресурсы.

Редко можно встретить доменные имена включающие четвертый и последующие уровни.

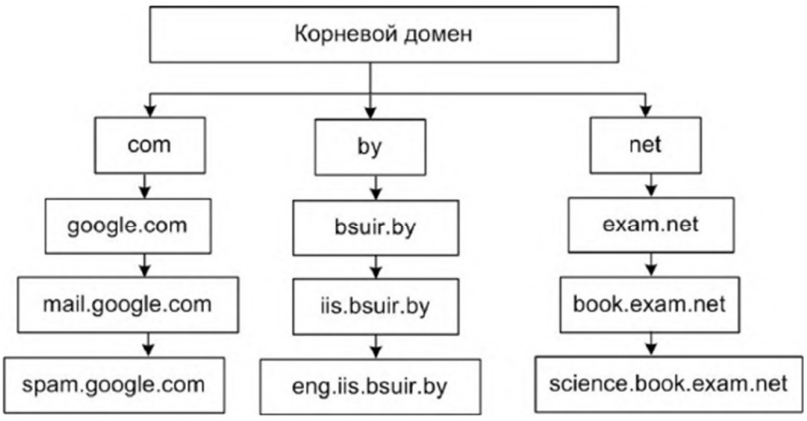


Рисунок 5.10 – Пример дерева доменных имен

9. Компоненты системы доменных имен. Этапы регистрации доменного имени.

Компоненты системы доменных имен:
- дерево серверов DNS;
- клиент DNS, ПО генерирующее запросы DNS на оконечном устройстве;
- DNS-резолвер или сервер разрешения имен DNS, предназначен для получения запросов от клиента и выполняет поиск необходимого IP-адреса в дереве доменных имен.

Для регистрации доменного имени сервера в глобальной сети необходимо зарегистрировать его у регистратора доменных имен, например hoster.by. Перед регистрацией можно проверить свободно ли доменное имя в Интернет пространстве на сайте регистратора доменных имен или с помощью утилиты ns lookup. Регистрация доменного имени является платной услугой на определенный период использования. После покупки и активации доменного имени необходимо приобрести хостинг-пространство (ресурсы для размещения веб-сайта).

10. Функции DNS-резолвера.

К основным функция DNS-резолвера относятся:
- рекурсия - модель обработки запросов DNS-сервером, при которой осуществляется поиск доменных имен посредством обращения к другим DNS- серверам;
- кэширование - временное хранение в памяти DNS-сервера информации, получаемой в DNS-ответах;
- TTL (Time To Live) - предельно допустимое время кэширования, содержится в поле TTL рекурсной записи.

Рассмотрим вышеописанные свойства на примере. Если пользователь вводит в браузере доменное имя iis.bsuir.by, изначально проверяется кеш DNS, который можно просмотреть с помощью команды ipconfig /displaydns в командной строке ОС Windows. Очистка DNS кеша осуществляется с помощью команды ipconfig /fUushdns.

В случае если к ресурсу iis.bsuir.by пользователь обращается впервые, то формируется DNS-запрос к DNS-резолверу. Если первичный сервер, IP-адрес которого внесен в сетевые настройки, будет недоступен, компьютер обратиться ко вторичному DNS-серверу. Однако это не означает, что, если первичный сервер не имеет информации о запрошенном доменном имени, он отправит запрос вторичному DNS-серверу. Когда к DNS-резолверу поступает запрос от клиента, он проверяет свой кеш, в случае если в кеше нет записи о доменном имени iis.bsuir.by, то DNS-резолвер формирует запрос к DNS серверу в корневом домене, который находится в регионе страны, например, домен .by. Как правило, корневой сервер имеет информацию о IP-адресах TLD-серверов в домене .by, IP-адрес одного из них и отправляется DNS-резолверу. Получив ответ от корневого сервера, DNS-резолвер формирует

новый запрос к TLD-серверу в домене .by. TLD-сервер по доменному имени определяет IP-адрес авторитетного сервера имен (Authoritative Name Server), который имеет базу данных для доменных имен bsuir.by. Авторитетным сервером имен является DNS-сервер, который удовлетворяет запросы из своих собственных баз данных без необходимости ссылаться на другой DNS-сервер. Получая ответ от TLD-сервера, DNS- резольвер направляет запрос авторитетному серверу, если сервер находит в базе данных доменное имя iis.bsuir.by, то он возвращает его IP-адрес DNS-резольверу. Допустим доменное имя не существует в глобальной сети, то будет отправлен отрицательный ответ. DNS-резольвер сохраняет полученную информацию в своем кеше и передает клиенту.

11. Способы конфигурации различных DNS-серверов.

Для настройки DNS-серверов используются следующие основные типы записей:

- запись A Record указывает точное соответствие IPvT-адреса и доменного имени сервера;
- запись AAAA (IPv6 Address Record) указывает точное соответствие IPv6-адреса и доменного имени сервера;
- запись NS (Name Server) указывает на DNS-сервер для данного домена, обычно для стабильной работы домена указывается не менее двух NS-записей, так как в случае недоступности одного из DNS-серверов отправляется запрос на другой DNS-сервер;
- запись CNAME (Canonical Name Record) - каноническая запись имени, используется для перенаправления на другое доменное имя;
- запись MX (Mail Exchange) указывает сервер обмена почтой для данного домена;
- SOA-запись (Start of Authority) - начальная запись зоны, указывает местоположение эталонной записи о домене, содержит в себе контактную информацию лица, ответственного за данную зону, время кэширования информации на серверах и данные о взаимодействии DNS.

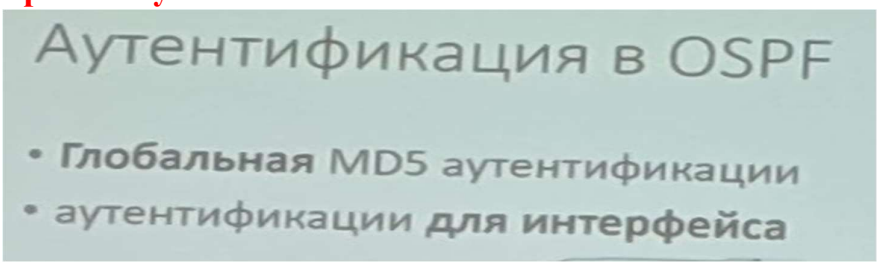
Порядок записей в базе данных DNS-сервсров не имеет значения за одним исключением: запись SOA должна идти первой. Дальнейшие записи считаются относящимися к той же зоне, пока не встретится новая запись SOA. Как правило, после записи зоны указывают записи DNS-серверов, а остальные записи располагают по алфавиту

12. Назначение аутентификации на маршрутизаторах глобальной сети.

Маршрутизаторы являются ключевыми компонентами сети, поэтому они часто становятся объектами сетевых атак. Поэтому важно помнить, что маршрутизаторы подвержены риску атак так же, как устройства конечных пользователей. Например, системы маршрутизации могут быть атакованы путем нарушения маршрутизации или фальсификации информации, передаваемой в протоколе маршрутизации. Информация о

фальсифицированной маршрутизации обычно может использоваться для того, чтобы заставить устройства дезинформировать друг друга, что может привести к атаке типа «отказ в обслуживании» (DoS), или заставить трафик следовать по пути отличному от установленного администратором маршрута. Можно выделить следующие последствия фальсификации маршрутной информации:
- перенаправление трафика для создания петель маршрутизации;
- перенаправление трафика, для его мониторинга;
- перенаправление трафика для его блокировки.

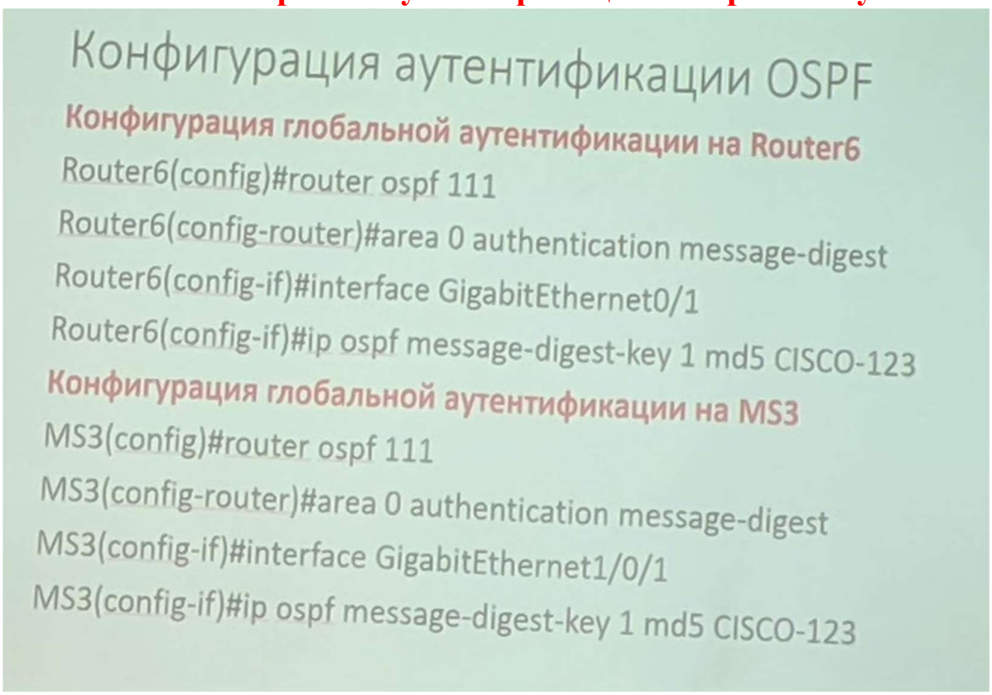
13. Типы аутентификации протокола OSPF. Процесс аутентификации по протоколу OSPF.



Протокол OSPF поддерживает **3 типа аутентификации:**
- **Null** - метод, установленный по умолчанию, который означает, что для OSPF аутентификация не используется;
- **простая аутентификация по паролю**, который отправляется в виде открытого текста в обновлении;
- **MD5** аутентификация - пароль шифруется алгоритмом MD5.

Сначала маршрутизатор Routerl объединяет сообщение маршрутизации с предварительно общим секретным ключом и вычисляет подпись, используя алгоритм MD5. Подпись также известна как хэш-значение.
Далее маршрутизатор Router 1 добавляет подпись к сообщению маршрутизации и отправляет его к маршрутизатору Router2. Алгоритм MD5 не шифрует сообщение; поэтому его содержание открыто. Маршрутизатор Router2 открывает пакет, объединяет сообщение маршрутизации с предварительно общим секретным ключом и вычисляет подпись с использованием алгоритма MD5. Если подписи совпадают, то маршрутизатор Router2 принимает обновление маршрутизации. Если подписи не совпадают, то маршрутизатор Router2 не использует полученную информацию для обновления.

14. Способы настройки аутентификации по протоколу OSPF и RIP.



Рассмотрим пример конфигурации аутентификации между маршрутизатором Router5 и коммутатором L3 MS3 (см. рисунок 5.1), на которых необходимо настроить глобальную аутентификацию OSPF MD5 для области 0. Конфигурация аутентификации на Router5 осуществляется следующим образом:

```
Router6(config)#router ospf 111
Router6(config-router)#area 0 authentication message-digest
Router6(config-if)#interface GigabitEthernet0/1
Router6(config-if)#shutdown
Router6(config-if)#ip ospf message-digest-key 1 md5 CISCO-123
```

Для аутентификации маршрутизаторов, работающих по протоколу RIP, также используется конфигурация цепочки ключей аналогично с протоколом BGP. Ключи протокола RIP быть зашифрованы с помощью алгоритма MD5. Отличие настройки цепочки ключей для протокола RIP заключается в том, что она активируется на интерфейсах соседних маршрутизаторов следующим образом:

```
interface <имя_номер>
ip rip authentication mode md5
ip rip authentication key-chain <имя_цепочки>.
```

15. Настройка аутентификации в протоколах EIGRP и BGP.

Протокол BGP поддерживает аутентификацию на основе использования криптографических алгоритмов и без шифрования. Кроме того, аутентификация может быть настроена двумя способами:

- с использованием цепочки ключей;
- на основе аутентификации соседа.

Аутентификация BGP (вариант 1)

```
Router (config)#key chain keychain_A
Router (config-keychain)#key 1
Router(config-keychain-key)#cryptographic-algorithm [HMAC-MD5 | HMAC-SHA1-12 | HMAC-SHA1-20 | MD5 | SHA-1] key
Router(config)#router bgp AS
Router(config-router)#neighbor 172.20.1.1 remote-as 1
Router(config-router)#keychain keychain_A
```

Аутентификация BGP (вариант 2)

```
Router(config)#router bgp 100
Router(config-router)# neighbor 10.1.1.1 remote-as 1
Router(config-router)#neighbor 10.1.1.1 password { clear | encrypted } password
```

Аутентификация EIGRP

Шаг 1. Создание цепочки ключей и ключа:

```
Router(config)#key chain NAME
Router(config-keychain)#key ID
Router(config-keychain-key)#key-string TEXT
```

Шаг 2. Настройка аутентификации EIGRP с помощью цепочки ключей и ключа:

```
Router(config-if)#ip authentication mode eigrp AS-NUMBER md5
Router(config-if)#ip authentication key-chain eigrp AS-NUMBER NAME
```

Конфигурация аутентификации EIGRP на MS5

MS5(config)#key chain **keyEIGRP**

MS5(config-keychain)# key 1

MS5(config-keychain-key)# key-string **EIGRP51365**

MS5(config)#interface GigabitEthernet1/1/4

MS5(config-if)# ip authentication mode eigrp 51365 md5

MS5(config-if)# ip authentication key-chain eigrp 51365 **keyEIGRP**