Маршрутизаторы Cisco

Выполнили студенты

Гр.3351 Ерёменок Андрей

Гр.3305 Свириденко Станислав

Содержание

1. Введение

В современной маршрутизации существует ряд проблем.

Ясно, что тот производитель, который сможет решить их наиболее приемлемым для пользователей образом, будет более востребован на рынке. Это экономический аспект.

Для нас же интерес представляет содержательный аспект – то, каким образом эти проблемы могут быть решены.

В данной лекции будут рассмотрены часть из этих проблем, а также решение их на примере концепции, разработанной компанией Cisco.

2. Проблемы современной маршрутизации

2.1 Проблема организации сетей

При проектировании сетей не всегда применяются системные решения. Вследствие этого возникают проблемы, описанные далее.

2.2 Недостатки маршрутизатора как устройства

Не все маршрутизаторы обеспечивают гибкую поддержку непрерывно изменяющихся требований к функциональности.

2.3 Недостатки протоколов маршрутизации

Традиционно используемые протоколы, основанные на алгоритмах вектора расстояний и состояния канала, имеют ряд недостатков.

2.1 Проблема организации сетей

Критические характеристики:

- Производительность
- Надёжность
- Безопасность
- Масштабируемость

2.1 Проблема организации сетей

Современные крупные сети очень сложны, поскольку определяются множеством протоколов, конфигурациями и технологиями.

На рынке представлено множество устройств с перекрывающимися функциями, принадлежащих при этом к разным ценовым диапазонам, что дополнительно усложняет выбор.

Главное, что следует отметить:

Применение спонтанных, несистемных решений при проектировании архитектуры сети не только затрудняет ее масштабируемость, но и ухудшает производительность. Также трудно поддерживать безопасность в такой сети.

2.2 Недостатки маршрутизатора как устройства

Критические характеристики:

- Безопасность
- Надёжность
- Масштабируемость

2.2 Недостатки маршрутизатора как устройства

Добавляют проблем и устаревшие устройства, заменить которые невозможно по финансовым либо другим причинам. Налаживать их взаимодействие с остальной сетью бывает порой весьма непросто.

В то же время, одно неправильно настроенное устройство (например, маршрутизатор) может существенно понизить производительность сети, а иногда и полностью парализовать её работу.

2.3 Недостатки протоколов маршрутизации

Критические характеристики:

- Производительность
- Масштабируемость
- Надежность

2.3 Недостатки протоколов маршрутизации

Протоколы маршрутизации базируются всего на двух простых алгоритмах, известных уже несколько десятилетий.

Для выполнения своей основной функции — переключения трафика — каждый маршрутизатор использует таблицу, в которой отражена топология сети на данный момент времени. В самом общем случае таблица маршрутизации содержит адрес сети назначения, адрес следующего узла на пути к этой сети и метрику (стоимость) пути. Создание и последующее обновление таблицы маршрутизации при изменении топологии сети осуществляется с помощью протоколов маршрутизации.

2.3 Недостатки протоколов маршрутизации

Алгоритм Беллмана-Форда (также известный как алгоритм Форда-Фулкерсона) был положен в основу первого протокола маршрутизации, созданного для сети ARPANET. Так называемые протоколы вектора расстояния (distance vector protocols), такие, как RIP, IGRP, BGP, используют те же принципы. В 1979 году на смену протоколу вектора расстояний пришел протокол состояния канала (link state protocol), ставший основным в ARPANET. Современные протоколы состояния канала включают OSPF, IS-IS, NLSP и др.

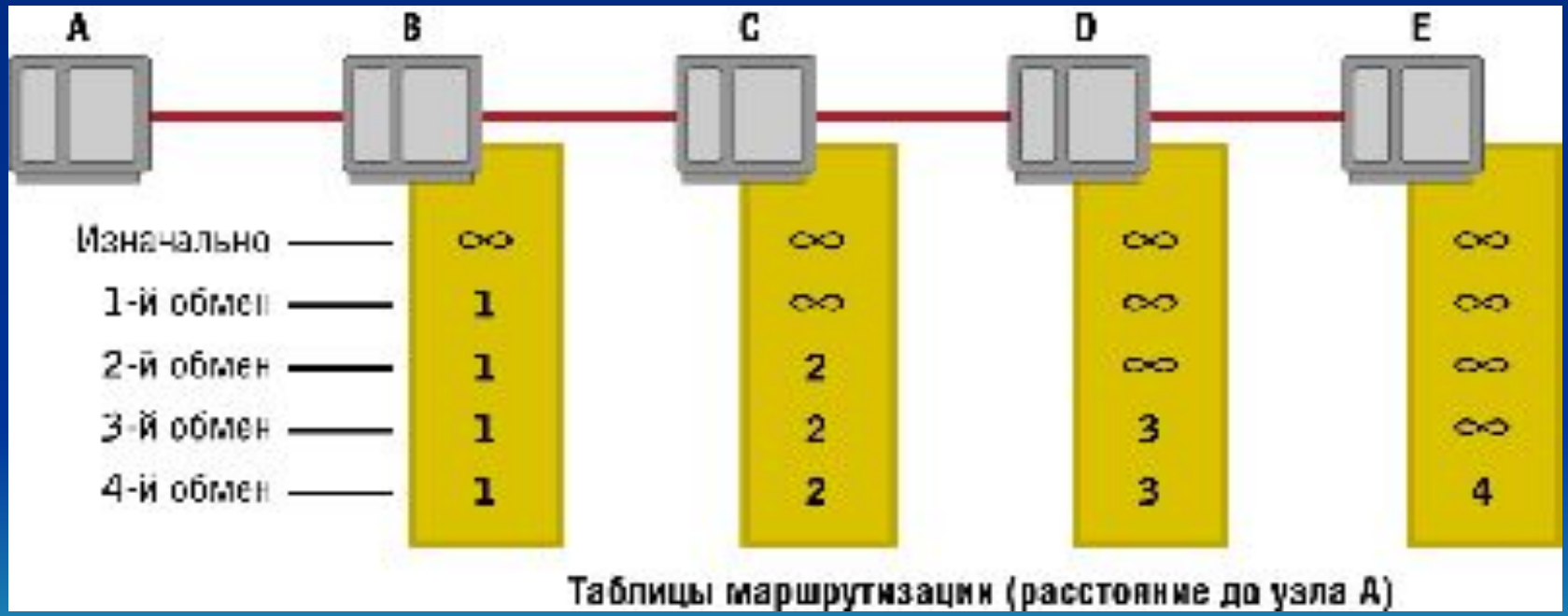
2.3 Недостатки протоколов маршрутизации

Основное преимущество алгоритма вектора расстояний — его простота. Действительно, в процессе работы маршрутизатор общается только с соседями, периодически обмениваясь с ними копиями своих таблиц маршрутизации. Получив информацию о возможных маршрутах от всех соседних узлов, маршрутизатор выбирает путь с наименьшей стоимостью и вносит его в свою таблицу.

Достоинство этого элегантного алгоритма — быстрая реакция на хорошие новости (появление в сети нового маршрутизатора), а недостаток — очень медленная реакция на плохие известия (исчезновение одного из соседей).

2.3 Недостатки протоколов маршрутизации

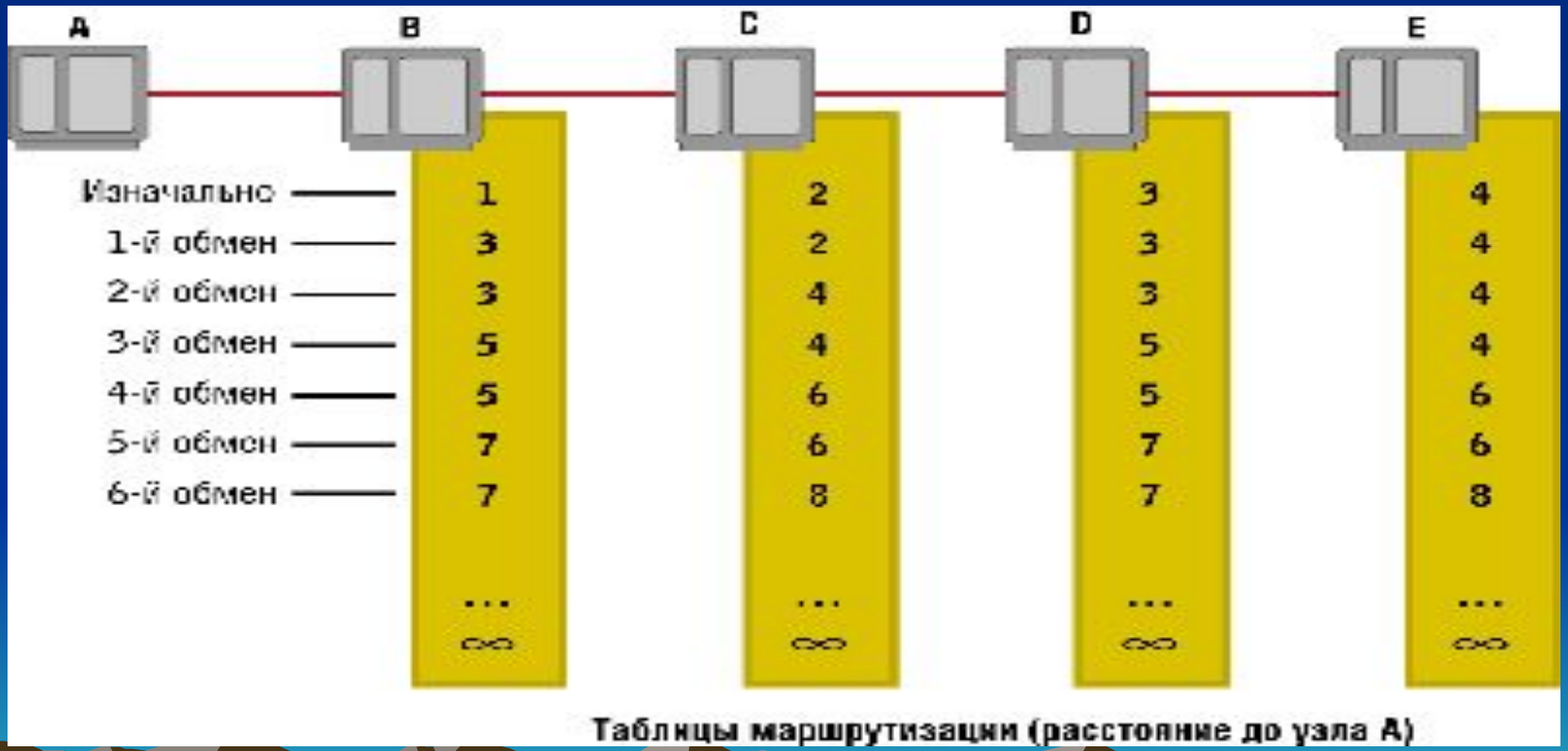
В качестве примера мы рассмотрим сеть из нескольких последовательно соединенных маршрутизаторов, где метрикой является число транзитных узлов на пути к точке назначения (как в протоколе RIP).



Таблицы маршрутизации (расстояние до узла A)

2.3 Недостатки протоколов маршрутизации

Теперь мы рассмотрим обратный случай, когда узел A перестает работать вследствие сбоя.



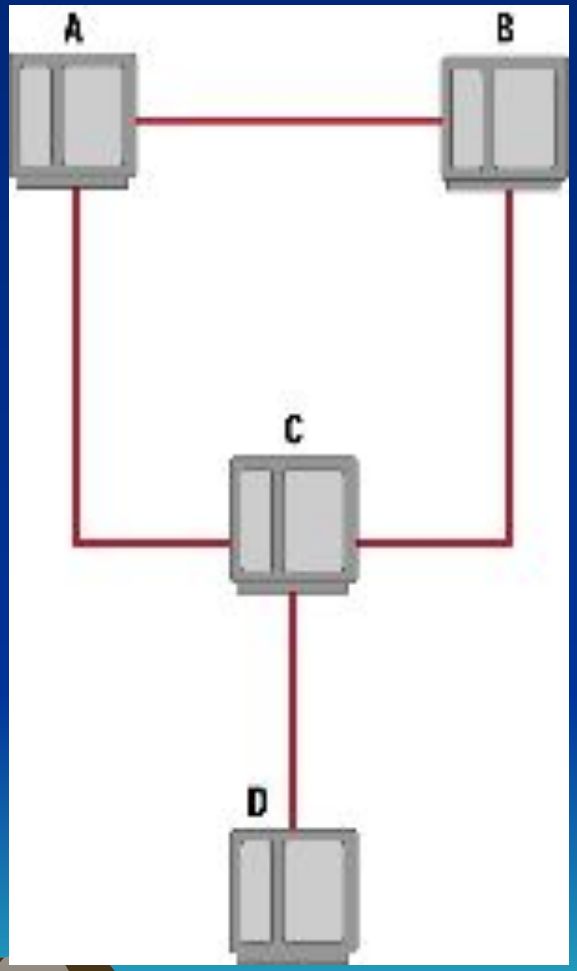
Таблицы маршрутизации (расстояние до узла A)

2.3 Недостатки протоколов маршрутизации

Для предотвращения образования ложных маршрутов используется несколько методов, один из них — метод расщепления горизонта (split-horizon). Данное правило не так сложно, как может показаться из названия: "Если известно, что путь до узла X лежит через соседний узел Y, то узлу Y не надо посылать объявления маршрута до X".

2.3 Недостатки протоколов маршрутизации

Рассмотрим пример сети с избыточной топологией. В начальный момент времени A и B знают, что расстояние до узла D равно "2". После выхода D из строя маршрутизатор C, не получив от D сообщения, определяет, что узел D недоступен. A и B продолжают считать D доступным, но правило расщепления горизонта запрещает им сообщать эту ложную информацию маршрутизатору C. При следующем обмене C уведомляет A и B о недоступности D. Но одновременно с этим узел A получает от B сообщение о пути до D стоимостью "2", а узел B получает аналогичное сообщение от A.



2.3 Недостатки протоколов маршрутизации

Подобную проблему помогает решить метод временного отказа от приема сообщений (hold-down), используемый современными протоколами вектора расстояний.

Правило отказа от приема запрещает маршрутизатору, получившему сообщение об отказе узла, принимать объявления маршрута до этого узла в течение некоторого времени. Получив от C уведомление о недоступности D, маршрутизатор A не должен доверять сообщению узла B, так как в момент обмена тот не имел достоверной информации о D. Лишь спустя некоторое время, когда можно быть уверенным, что информация об отказе D распространилась по всей сети, маршрутизатор A может вновь начинать принимать объявления о путях до D. (За это время и A и B сотрут информацию о маршруте до D, так как оно превышает время хранения записи в таблице маршрутизации.)

2.3 Недостатки протоколов маршрутизации

Если зацикливание в сети все же произошло, то образовавшаяся петля будет разорвана, когда метрика маршрута превысит максимально допустимую. Этот процесс может быть ускорен с помощью механизма принудительных объявлений (triggered updates).

Правило принудительных объявлений звучит следующим образом: "Узнав об изменении метрики маршрута, маршрутизатор обязан немедленно сообщить об этом соседям". В результате адаптация сети к изменившейся топологии произойдет значительно быстрее.

Однако при выходе из строя одного из каналов сети не все объявления дойдут до получателей. В этом случае маршрутизатор, так и не узнавший о произошедших изменениях, будет продолжать рекламировать устаревшие маршруты, а при отсутствии механизма отказа от приема проблема возрастания до бесконечности вновь спутает таблицы маршрутизации.

2.3 Недостатки протоколов маршрутизации

Развитие Internet привело к необходимости создания более гибкого и эффективного протокола маршрутизации для обслуживания крупных сетей. По замыслу создателей, протоколы состояния канала должны были решить характерные для протоколов вектора расстояний проблемы. Однако, в отличие от протоколов вектора расстояния, протоколы состояния канала сложны и требовательны к ресурсам маршрутизаторов. Основу протоколов состояния канала составляет алгоритм предпочтения кратчайшего пути, созданный в 1978 году.

2.3 Недостатки протоколов маршрутизации

В упрощенной форме принципы работы маршрутизаторов в соответствии с этим протоколом можно сформулировать в виде пяти несложных правил.

Итак, каждый маршрутизатор в сети должен:

1. при включении в сеть получить информацию о своих соседях;
2. узнать стоимость пути до каждого из соседей (т. е. узнать о состоянии каналов);
3. подготовить пакет–объявление, содержащий полученную информацию;
4. разослать этот пакет всем соседям;
5. построить дерево кратчайших расстояний до всех остальных маршрутизаторов.

2.3 Недостатки протоколов маршрутизации

При подключении сети, маршрутизатор первым делом должен "познакомиться" со своими соседями. Для этого он рассылает через все свои физические интерфейсы специальные пакеты с приветствием HELLO. Получив такой пакет, соседний узел должен ответить, сообщив данные о себе.

Узнав данные о соседях, маршрутизатор принимается за второй пункт программы — тестирование каналов связи с целью выяснения метрики каждого канала. Под метрикой может пониматься пропускная способность, время задержки, надежность (количество ошибок на единицу переданной информации), загрузка канала.

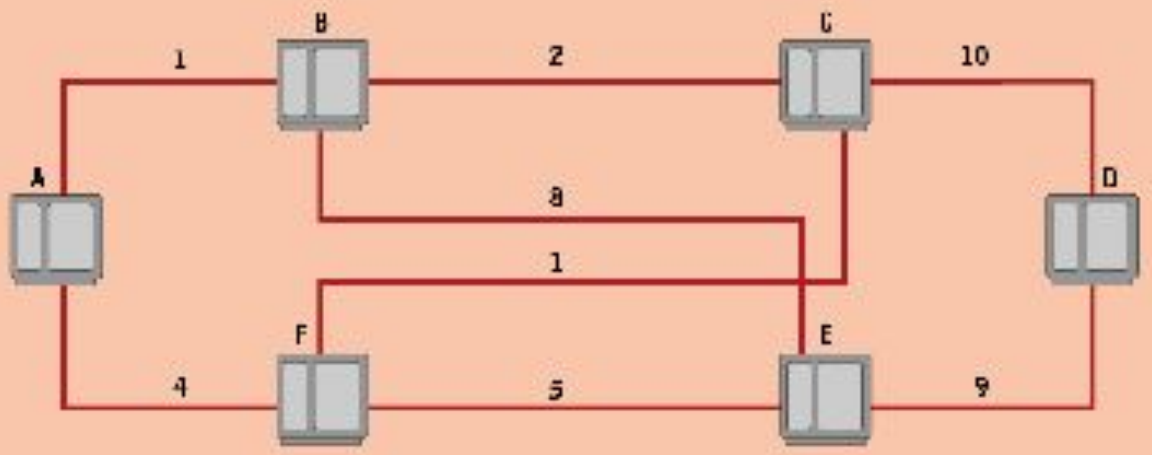
2.3 Недостатки протоколов маршрутизации

Загрузку канала несложно измерить. Однако ответ на вопрос о том, как использовать показатель загруженности канала при вычислении метрики, отнюдь не однозначен. Рассмотрим небольшой пример. При наличии нескольких альтернативных путей до точки назначения маршрутизатор, оценив загруженность каждого из них, переключает трафик на канал с меньшей загрузкой. Тем самым он максимально использует свободный канал, что вполне логично. Во время следующего измерения метрик предпочтение может быть отдано уже другому каналу, через который трафик уже не идет и который, следовательно, теперь менее загружен. В результате трафик будет переключен на него. Это приводит к тому, что трафик постоянно переводится с одного канала на другой, что, естественно, не способствует стабильности в работе сети.

2.3 Недостатки протоколов маршрутизации

Шаг номер три в программе маршрутизатора состоит в сообщении полученных знаний остальным. Информация о каналах должна быть разослана соседям. Однако пакеты с объявлениями о состоянии каналов (Link State Advertisement, LSA) могут затеряться при транспортировке или прибыть в ином порядке. Для того чтобы получатель мог разобраться в пришедшей информации, каждый пакет с объявлением о состоянии каналов снабжается полями source (адрес отправителя), sequence number (номер пакета в последовательности отправленных сообщений) и age (возраст).

2.3 Недостатки протоколов маршрутизации



Объявления о состоянии каналов, рассылаемые по сети

A		B		C		D		E		F	
Номер в послед-ти		Номер в послед-ти		Номер в послед-ти		Номер в послед-ти		Номер в послед-ти		Номер в послед-ти	
Возраст		Возраст		Возраст		Возраст		Возраст		Возраст	
B	1	C	2	D	10	C	10	D	9	E	5
F	4	A	1	B	2	E	9	F	5	A	4
		E	8	F	1			B	8	C	1

2.3 Недостатки протоколов маршрутизации

Обмен информацией осуществляется с помощью веерной рассылки, т. е., получив пакет, маршрутизатор LSA сохраняет копию в своей базе данных и посылает пакет дальше всем остальным соседям. В итоге пакет, отправленный одним из узлов сети, обязательно получат все остальные маршрутизаторы. В этом ключевое отличие данного алгоритма от алгоритма вектора расстояния, в котором каждый узел мог общаться только с непосредственно подключенными к нему маршрутизаторами, что часто приводит к эффекту "испорченного телефона", когда, сам не разобравшись в топологии, маршрутизатор сбивает с толку соседей

2.3 Недостатки протоколов маршрутизации

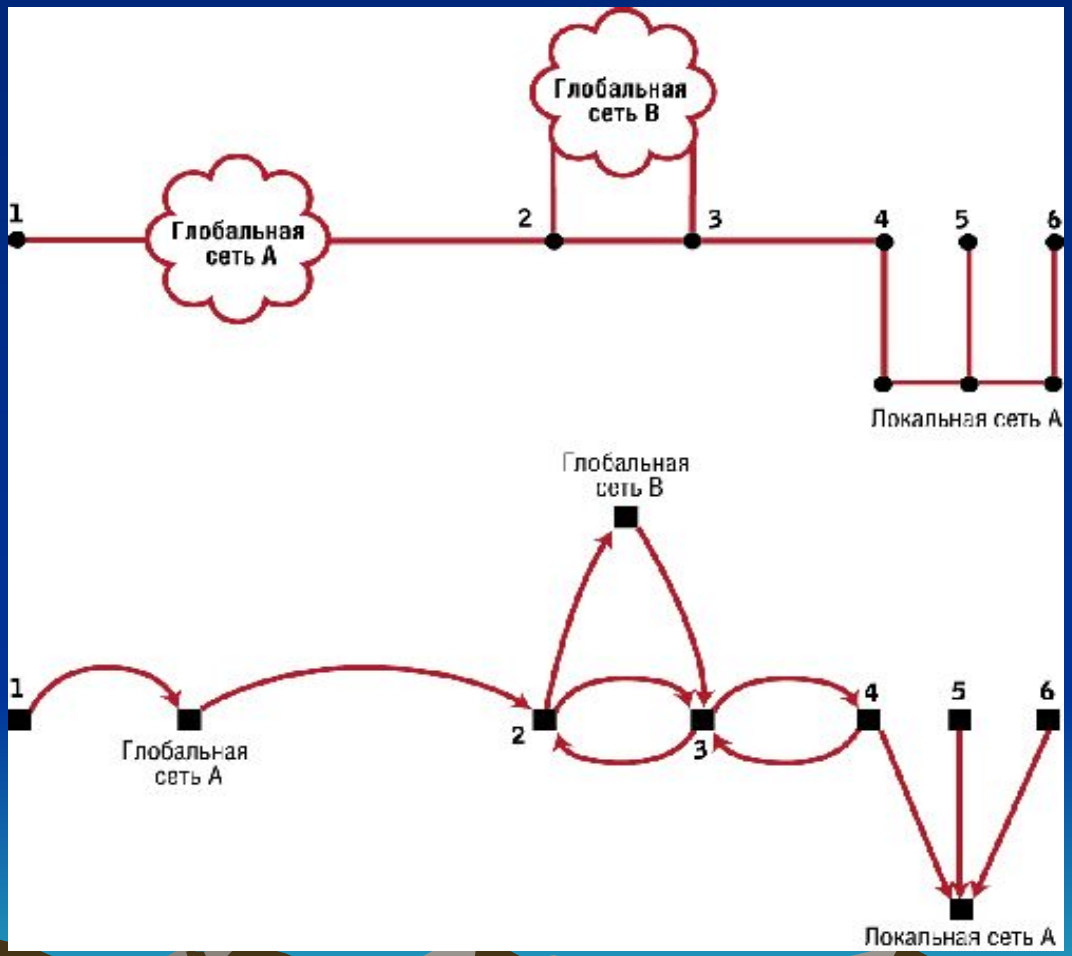
Получив пакет LSA, маршрутизатор проверяет пару (source, sequence), что позволяет отбросить устаревшие и дублированные объявления. Поле age задает время, по истечении которого не приславший новых объявлений узел считается недоступным.

В конкретных протоколах данные поля могут носить другие названия, в протоколе OSPF, например, поля age и sequence носят названия DeadInt и DD Sequence, а протокол IS-IS даже использует специальный тип пакета — порядковый пакет. Однако, независимо от протокола, наличие подобной информации обязательно для надежной работы алгоритма предпочтения кратчайшего пути.

2.3 Недостатки протоколов маршрутизации

После получения информации от всех узлов маршрутизатор может построить "карту" сети. Для этого он создает ориентированный граф, отражающий топологию сети. Соединение "точка-точка" между узлами представляется на графе парой дуг (по одной в каждом направлении), причем стоимости этих дуг могут отличаться друг от друга. Сети с множественным доступом (например, локальные сети) отображаются вершинами для каждого узла сети и дополнительной вершиной — "центром" этой сети. Дуги графа от "центра" до узлов сети не отображаются.

2.3 Недостатки протоколов маршрутизации



2.3 Недостатки протоколов маршрутизации

Протоколам маршрутизации традиционно не нравятся "облака" сетей X.25 и frame relay. Большое число медленных каналов, соответственно, требующих рассылки большого числа объявлений LSA, затрудняет работу. Рассылка объявлений производится по "веерному" методу, поэтому полносвязная (fully-meshed) топология сети нежелательна. Сети с частично связной (partial-meshed) топологией здесь более предпочтительны.

Несмотря на отсутствие строгого ограничения на максимальное количество узлов в сети, возможности протоколов все же не безграничны. Эксперименты с протоколом OSPF показали, что 50 маршрутизаторов на зону (area) — это верхний предел, превышение которого чревато неприятными "сюрпризами" со стороны сети. При большем количестве узлов лучший выход состоит в создании новой зоны.

2.3 Недостатки протоколов маршрутизации

Самой серьезной проблемой может стать нехватка памяти. Для системы из n узлов, каждый из которых имеет k соседей, необходимый объем памяти пропорционален k*n. Обычно подобные проблемы проявляются в больших сетях, с очень большим количеством внешних маршрутов. Определение одного маршрутизатора (шлюза) по умолчанию для всех внешних путей может значительно сэкономить память. Вообще, тщательное предварительное планирование сети способно значительно облегчить "жизнь" протоколам состояния канала.

3. Решения, предлагаемые Cisco

Проблемы:

- Со структурой организации сетей
- С конфигурацией маршрутизатора
- С протоколами маршрутизации

Решения:

- Трехуровневая иерархическая организация
- Системный подход к маршрутизатору как к совокупности программных и аппаратных средств
- «Фирменные» протоколы Cisco

3.1. Иерархическая организация сетей

Системный подход ставит несколько задач:

- *Передача ответственности за безопасность и надежность от отдельных компьютеров и пользователей к самой сети*
- *Создание сети, способной адаптироваться к меняющимся требованиям*
- *Рассмотрение сети в качестве упорядоченной и организованной системы, а не совокупности неравноправных, отдельно управляемых модулей*

3.1. Иерархическая организация сетей

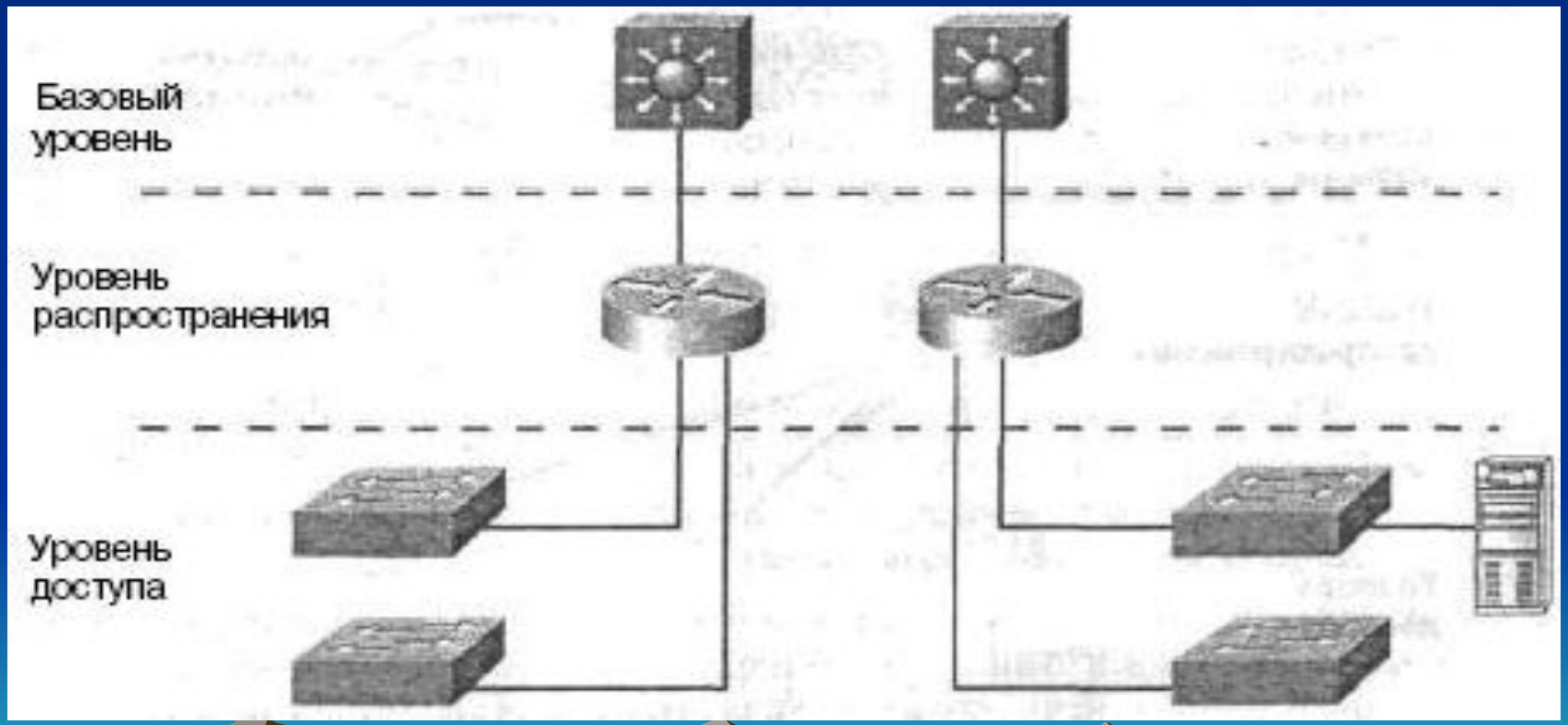
- *Системный подход* к маршрутизации и коммутации позволяет всем сотрудникам – даже находящимся на различных объектах – иметь одинаковый доступ к бизнес-приложениям, IP-коммуникациям и функциям видеоконференций, которые раньше были доступны только коллегам в штаб-квартире. Сетевые решения для филиалов чаще всего имеют модульную архитектуру, позволяя внедрять необходимые каждому конкретному офису функции.
- *Модульность* также позволяет модернизировать оборудование при изменении потребностей или расширении офиса.
- *Дополнительная выгода* этого системного подхода заключается в том, что технические сотрудники в штаб-квартирах получают возможность централизованного управления сетью, что позволяет уменьшить численность обслуживающего персонала и в то же время предоставлять надежное обслуживание сотрудников на всех объектах. Этот принцип действует вне зависимости от масштаба компании.

3.1. Иерархическая организация сетей

Современные крупные сети очень сложны, поскольку определяются множеством протоколов, конфигурациями и технологиями. С помощью иерархии можно упорядочить все компоненты в легко анализируемой модели. Причем, модель будет диктовать характеристики каждого иерархического уровня. Иерархическая модель помогает в разработке, внедрении и обслуживании масштабируемых, надежных и эффективных в стоимостном выражении объединенных сетей. Компания Cisco определила три иерархических уровня (см. рис), на каждом из которых выполняются специфические сетевые функций.

3.1. Иерархическая организация сетей

Трехуровневая Иерархическая модель



3.1. Иерархическая организация сетей

В модели определены три уровня:

- Базовый уровень (*Core layer*)
- Уровень распространения (*Distribution layer*)
- Уровень доступа (*Access layer*)

3.1. Иерархическая организация сетей

1) Базовый уровень

   Базовый уровень формирует ядро сети. На самом верху иерархии этот уровень отвечает за быструю и надежную пересылку больших объемов трафика. Единственным предназначением базового уровня является быстрая коммутация трафика. Трафик передается на базовом уровне совместно для нескольких пользователей. Однако на уровне распределения обрабатываются пользовательские данные, что может привести к дополнительным запросам в базовый уровень.

3.1. Иерархическая организация сетей

2) Уровень распространения

Уровень распространения иногда называют уровнем рабочих групп. Он расположен между базовым уровнем и уровнем доступа.

Основные функции уровня распространения состоят в маршрутизации, фильтрации и доступе к региональным сетям, а также (если необходимо) в определении правил доступа пакетов к базовому уровню. Уровень распространения обязан устанавливать наиболее быстрый способ обработки запросов к службам (например, метод файлового обращения к серверу). После определения на уровне распространения наилучшего пути доступа, запрос может быть передан на базовый уровень, где реализован скоростной транспорт запроса к нужной службе.

На уровне распространения устанавливается политика сети, а также обеспечиваются возможности гибкого описания сетевых операций. На уровне распространения выполняется несколько функций:

- Реализация инструментов, подобных спискам доступа, фильтрации пакетов или механизму запросов.
- Реализация системы безопасности и сетевых политик, включая трансляцию адресов и установку брандмауэров.
- Перераспределение между протоколами маршрутизации, включая использование статических путей.
- Маршрутизация между сетями VLAN и другие функции поддержки рабочих групп.
- Определение доменов широковещательных и многоадресных рассылок.

3.1. Иерархическая организация сетей

3) Уровень доступа

На *уровне доступа* реализовано управление пользователями и рабочими группами при обращении к ресурсам объединенной сети. Иногда уровень доступа называют уровнем настольных систем. Наибольшая часть необходимых пользователям сетевых ресурсов должна быть доступна локально. На уровне распределения выполняется перенаправление трафика к удаленным службам. Для уровня доступа характерны следующие функции:

- Постоянный контроль (из уровня распределения) за доступом и политиками
- Формирование независимых доменов конфликтов (сегментация)
- Соединение рабочих групп с уровнем распределения

Обычно на уровне доступа применяются технологии DDR или коммутация Ethernet. Здесь же можно увидеть статическую маршрутизацию (вместо протоколов динамической маршрутизации). Как уже отмечено выше, три отдельных уровня не связаны с тремя специальными типами маршрутизаторов. Этих устройств может быть меньше или больше, но нужно всегда помнить о разделении сетевых функций по уровням модели.

3.1. Иерархическая организация сетей

Итог:

Т.о., видно четкое разделение функций между уровнями. Это позволяет упростить процесс проектирования сети, сделать его более эффективным – таким, чтобы внимание уделялось только роли применяемого решения в пределах уровня, а не всей сети.

Применяя такое решение, Cisco удалось улучшить такие характеристики сетей, как производительность, надежность, безопасность, масштабируемость.

3.2. Комплексный подход к устройству маршрутизатора

Цель: добиться того, чтобы данный конкретный маршрутизатор выполнял свои функции наиболее эффективно.

Для этого надо определить набор этих функций и реализовать маршрутизатор так, чтобы он выполнял их и только их. Тогда его работа будет наиболее эффективна.

Ясно, что невозможно создать маршрутизатор для каждого из возможных наборов необходимых функций.

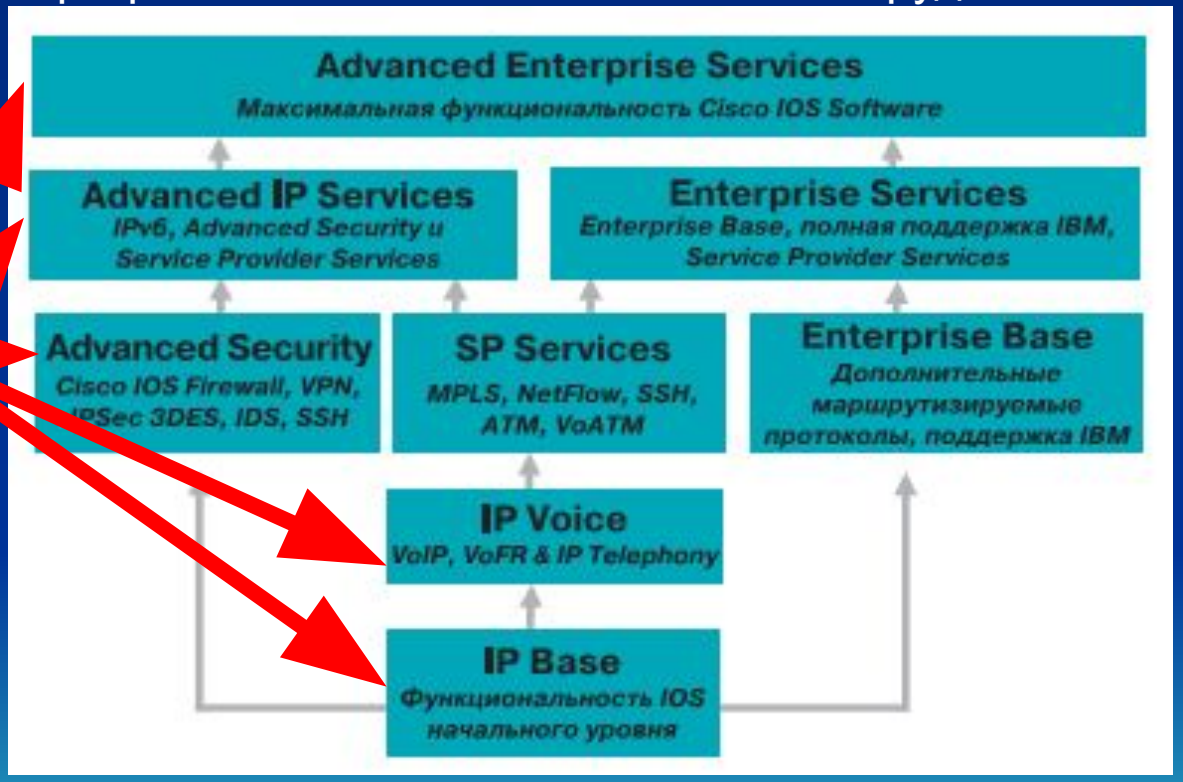
Решение: представить устройство маршрутизатора как совокупность аппаратной (материальной) и программной (идеальной) составляющих. Т.е. рассматривать взаимосвязь маршрутизатора и его операционной системы. При этом:

- развитие и появление новых моделей маршрутизаторов должно удовлетворять современным требованиям к проектированию сетей.
- развитие и появление новых версий ОС определяется современными требованиями к проектированию сетей и имеющимися моделями маршрутизаторов.

С появлением новой возможной функциональности необходимо создать новую версию ОС, поддерживающую ее. С накоплением большого количества новых функций маршрутизатор устаревает, т.к. поддержка их затрудняется. Необходимо создание качественно нового устройства.

3.2. Комплексный подход к устройству маршрутизатора

Т.о., подбирая необходимые маршрутизатор и ОС к нему, проектировщик сети может добиться наиболее точного обеспечения необходимой ему функциональности. Программной частью сетевого оборудования Cisco является Cisco IOS.



аппаратная часть

программная часть

3.2. Комплексный подход к устройству маршрутизатора

Программное обеспечение Cisco IOS (Internetwork Operating System) – это операционная система, обеспечивающая функционирование сетевого оборудования Cisco, являющегося основой сети Интернет и крупнейших частных сетей. Поддерживая широкий спектр оборудования Cisco, операционная система Cisco IOS обеспечивает общие программную платформу, набор функций и интерфейс командной строки в рамках всей сетевой инфраструктуры.

Cisco IOS реализует широкую функциональность в различных областях сетевых технологий.

Некоторые основные особенности Cisco IOS:

- поддержка широкого спектра сетевых протоколов;
- интеграция данных, голоса и видео в рамках единой IP сети;
- механизмы обеспечения качества обслуживания (QoS);
- средства обеспечения безопасности;
- поддержка протокола IPv6;
- поддержка мобильности пользователей;
- поддержка многоадресной рассылки (IP multicast);
- средства управления.

3.2. Комплексный подход к устройству маршрутизатора

Итог:

Применяя такое решение, Cisco удалось добиться улучшения таких характеристик, как надежность, масштабируемость и безопасность.

Т.е. возможно более гибкое изменение архитектуры сети без серьезных вложений, а также модификация сети в рамках работающей в ней технологии.

3.3. Протоколы Cisco

- IGRP
- EIGRP
- BGP

3.3.1 Протоколы Cisco. IGRP

IGRP представляет собой протокол, который позволяет большому числу маршрутизаторов координировать свою работу. Основные достоинства протокола:

- стабильность маршрутов даже в очень больших и сложных сетях;
- быстрый отклик на изменения топологии сети;
- минимальная избыточность. Поэтому IGRP не требует дополнительной пропускной способности каналов для своей работы;
- разделение потока данных между несколькими параллельными маршрутами, примерно равного достоинства;
- учет частоты ошибок и уровня загрузки каналов;
- возможность реализовать различные виды сервиса для одного и того же набора информации.

3.3.1 Протоколы Cisco. IGRP

IGRP используется в маршрутизаторах, которые имеют связи с несколькими сетями и выполняют функции переключателей пакетов.

Метрика, используемая в IGRP, учитывает:

- время задержки;
- пропускную способность самого слабого сегмента пути (в битах в сек);
- загруженность канала (относительную);
- надежность канала (определяется долей пакетов, достигших места назначения неповрежденными).

3.3.1 Протоколы Cisco. IGRP

Наилучший путь выбирается с использованием комбинированной метрики, вычисленной по формуле:

[(K1 / Be) + (K2 * Dc)] r [1], где:

K1, K2 - константы;

Be - пропускная способность канала (в отсутствии загрузки) * (1 - загрузка канала);

Dc - топологическая задержка;

r - относительная надежность. (% пакетов, успешно передаваемых по данному сегменту пути). Здесь загрузка измеряется как доля от 1.

Одним из преимуществ IGRP является простота реконфигурации. В IGRP маршрут по умолчанию не назначается, а выбирается из числа кандидатов.

3.3.1 Протоколы Cisco. IGRP

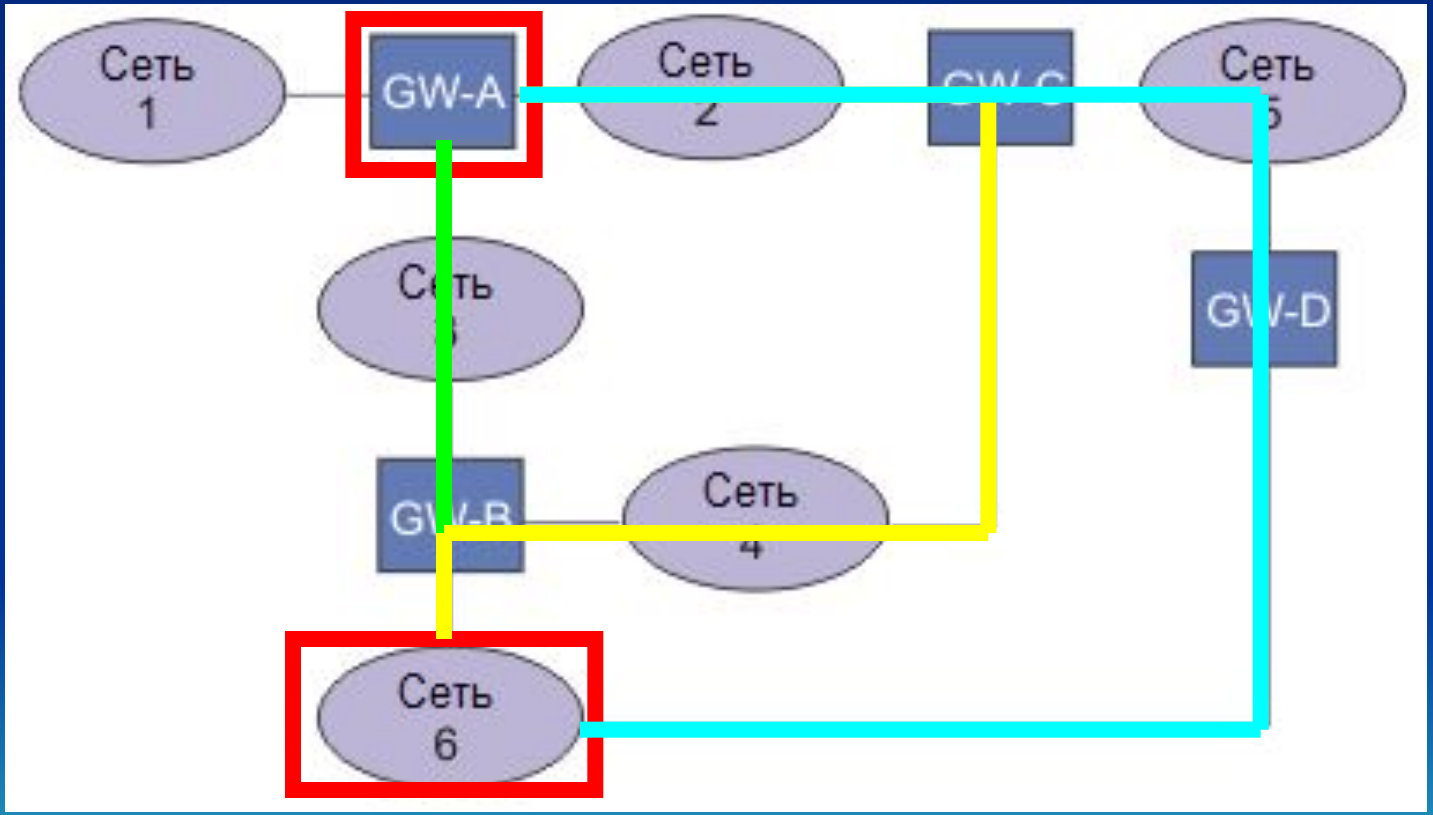
Распространение информации о новых маршрутах

Когда маршрутизатор включается, его маршрутные таблицы инициализируются оператором вручную или с использованием специальных файлов. Маршрутизатор S связан через соответствующие интерфейсы с сетями 2 и 3.

Таким образом, в исходный момент маршрутизатор S знает только о доступности сетей 2 и 3. За счет обмена информацией, полученной при инициализации и присланной позднее соседями, маршрутизаторы познают окружающий мир. Так S спустя некоторое время получит информацию от маршрутизатора R о доступности сети 1 и от T - о сети 4. В свою очередь S проинформирует T о доступе к сети 1. Очень быстро информация о доступности дойдет до всех маршрутизаторов и разрозненные сети станут единым целым.

3.3.1 Протоколы Cisco. IGRP

Построение маршрута



3.3.1 Протоколы Cisco. IGRP

Пример таблицы маршрутизации

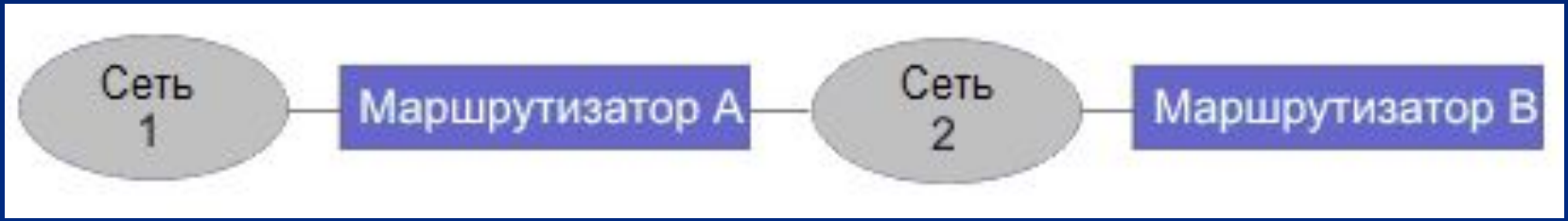
Номер сети	Интерфейс	Следующий Маршрутизатор	Метрика маршрута
Сеть 1	NW 1	Нет	Непосредственная связь
Сеть 2	NW 2	Нет	Непосредственная связь
Сеть 3	NW 3	Нет	Непосредственная связь
Сеть 4	NW 2	C	1270
	NW 3	B	1180
Сеть 5	NW 2	C	1270
	NW 3	B	2130
Сеть 6	NW 2	C	2040
	NW 3	B	1180

3.3.1 Протоколы Cisco. IGRP

Для того чтобы обеспечить работу с большими и сложными сетями, в IGRP введены усовершенствования алгоритма Белмана-Форда:

1) Для описания путей вместо простой, введена векторная метрика. Расчет комбинированной метрики проводится с использованием формулы [1]. Применение векторной метрики позволяет адаптировать систему с учетом различных видов сервиса.
2) Вместо выбора одного пути с минимальной метрикой, информационный поток может быть поделен между несколькими путями с метрикой, лежащей в заданном интервале. Распределение потоков определяется соотношением величин комбинированной метрики. Таким образом, используются маршруты с комбинированной метрикой меньше некоторого предельного значения M, а также с метрикой меньше V*M, где V - значение вариации M (обычно задается оператором сети).
3) Существуют определенные проблемы с вариацией. Трудно определить стратегию использования вариации V>1 и избежать зацикливания пакетов. В современных реализациях V=1.
4) Разработан ряд мер, препятствующих осцилляциям маршрутов при изменении топологии сети.

3.3.1 Протоколы Cisco. IGRP



Обеспечение стабильности топологии:

Маршрутизатор А сообщает В о маршруте к сети 1. Когда же В посылает сообщения об изменении маршрутов в А, он ни при каких обстоятельствах не должен упоминать сеть 1. Т.е. сообщения об изменении маршрута, направленные какому-то маршрутизатору, не должны содержать данных об объектах, непосредственно с ним связанных. Сообщения об изменении маршрутов должны содержать:

- адреса сетей, с которыми маршрутизатор связан непосредственно;
- пропускную способность каждой из сетей;
- топологическую задержку каждой из сетей;
- надежность передачи пакетов для каждой сети;
- загруженность канала для каждой сети;
- MTU для каждой сети.

3.3.1 Протоколы Cisco. IGRP

4 временные константы, управляющие процессом распространения маршрутной информации (эти константы определяются оператором сети):

- период широковещательных сообщений об изменении маршрутов (это время по умолчанию равно 90 сек);
- время существования - если за это время не поступило никаких сообщений о данном маршруте, он считается нерабочим. Это время в несколько раз больше периода сообщений об изменениях (по умолчанию в 3 раза).
- время удержания - когда какой-то адресат становится недостижим, он переходит в режим выдержки. В этом режиме никакие новые маршруты, ведущие к нему, не воспринимаются. Длительность этого режима и называется временем удержания. Обычно это время в три раза дольше периода сообщений об изменениях маршрутов.
- время удаления - если в течение данного времени не поступило сообщений о доступе к данному адресату, производится удаление записи о нем из маршрутной базы данных (по умолчанию это время в 7 раз больше периода сообщений об изменениях маршрутов)

3.3.1 Протоколы Cisco. IGRP

IGRP-сообщение вкладывается в IP-пакет, это сообщение имеет следующие поля:

- *version* номер версии протокола 4 байта
- *opcode* код операции
- *edition* код издания
- *asystem* номер автономной системы
- *Ninterior, Nsystem, Nexterior* числа субсетей в локальной сети, в автономной системе и вне автономной системы.
- *checksum* контрольная сумма IGRP-заголовка и данных
- *Version* - номер версии в настоящее время равен 1. Пакеты с другим номером версии игнорируются.
- *Opcode* - код операции определяет тип сообщения и может принимать значения:
- 1 - изменение; 2 - запрос
- *Edition* - (издание) является серийным номером, который увеличивается при каждом изменении маршрутной таблицы. Это позволяет маршрутизатору игнорировать информацию, которая уже содержится в его базе данных.
- *Asystem* - номер автономной системы. Согласно нормам Cisco маршрутизатор может входить в более чем одну автономную систему. В каждой AS работает свой протокол и они могут иметь совершенно независимые таблицы маршрутизации. Хотя в IGRP допускается "утечка" маршрутной информации из одной автономной системы в другую, но это определяется не протоколом, а администратором.
- Ninterior, nsystem и nexterior определяют числа записей в каждой из трех секций сообщения об изменениях.
- *Checksum* - контрольная сумма заголовка и маршрутной информации, для вычисления которой используется тот же алгоритм, что и в UDP, TCP и ICMP.

3.3.1 Протоколы Cisco. IGRP

IGRP запрос требует от адресата прислать свою маршрутную таблицу. Сообщение содержит только заголовок. Используются поля *version, opcode* и *asystem*, остальные поля обнуляются. IP-пакет, содержащий сообщение об изменении маршрутов, имеет 1500 байт (включая IP-заголовок). Для описанной выше схемы это позволяет включить в пакет до 104 записей. Если требуется больше записей, посылается несколько пакетов. Фрагментация пакетов не применяется.

Описание структуры для маршрута:

Number	3 октета IP-адреса
delay	задержка в десятках микросекунд 3 октета
bandwidth	Пропускная способность, в Кбит/с 3 октета
uchar mtu	MTU, в октетах 2 октета
reliability	процент успешно переданных пакетов tx/rx 1 октет
load	процент занятости канала 1 октет
hopcount	Число шагов 1 октет

3.3.1 Протоколы Cisco. IGRP

Пропускная способность измеряется в величинах, обратных бит/сек, умноженных на 1010. (Т.е., если пропускная способность равна N Кбит/с, то ее измерением в IGRP будет 10000000/N.). Надежность измеряется в долях от 255 (т.е. 255 соответствует 100%). Загрузка измеряется также в долях от 255, а задержка в десятках миллисекунд.

Комбинированная метрика в действительности вычисляется по следующей формуле (для версии Cisco 8.0(3)):

*Метрика = [K1*пропускная_способность + (K2*пропускная_способность)/(256 - загрузка) + K3*задержка] * [K5/(надежность + K4)].*

Если K5 == 0, член надежности отбрасывается. По умолчанию в IGRP

K1 == K3 == 1,

K2 == K4 == K5 == 0,

а загрузка лежит в интервале от 1 до 255.

3.3.2 Протоколы Cisco. EIGRP

1) улучшен алгоритм оптимизации маршрутов
2) сокращено временя установления
3) маски подсетей переменной длины.

Маршруты здесь делятся на внутренние и внешние - полученные от других протоколов или записанные в статических таблицах. Маршруты помечаются идентификаторами их начала.

Внешние маршруты помечаются следующей информацией:

- Идентификатор маршрутизатора EIGRP, который осуществляет рассылку информации о маршруте
- Номер AS, где расположен адресат маршрута
- Метка администратора
- Идентификатор протокола
- Метрика внешнего маршрута
- Битовые флаги маршрута по умолчанию

3.3. Протоколы Cisco. IGRP,EIGRP

Итог:

- IGRP был разработан для расширения возможностей RIP
- Количество переходов в IGRP ограничено 255
- IGRP и EIGRP выравнивают нагрузку для каналов с различными метриками
- Вместо того, чтобы обрабатывать все обновления при каждом поступлении, маршрутизаторы IGRP и EIGRP обрабатывают только обновления, противоречащие локальной таблице маршрутов
- EIGRP использует hello-пакеты для проверки существования соседних маршрутизаторов.

Т.о. применяя такое решение, Cisco удалось добиться улучшения таких характеристик, как производительность и надежность.

3.3.3 Протоколы Cisco. BGP

Главная цель BGP (*Border Gateway Protocol)* - сократить транзитный трафик. Местный трафик либо начинается, либо завершается в автономной системе (AS); в противном случае - это транзитный трафик.

Системы без транзитного трафика не нуждаются в BGP (им достаточно EGP для общения с транзитными узлами). Но не всякая ЭВМ, использующая протокол BGP, является маршрутизатором, даже если она обменивается маршрутной информацией с пограничным маршрутизатором соседней автономной системы. AS передает информацию только о маршрутах, которыми она сама пользуется. BGP-маршрутизаторы обмениваются сообщениями об изменении маршрутов (UPDATE-сообщения). Максимальная длина таких сообщений составляет 4096 октетов, а минимальная 19 октетов. Каждое сообщение имеет заголовок фиксированного размера. Объем информационных полей зависит от типа сообщения.

3.3.3 Протоколы Cisco. BGP

Автономной системой называют такую локальную сеть или систему сетей, которые имеют единую администрацию и общую маршрутную политику.

Пользователь, связанный только с одним сервис-провайдером, должен принадлежать к общей с ним AS. Автономная система должна обязательно создаваться, когда оператор сети связан с более чем одной AS с отличной от его маршрутной политикой. Если же пользователь обращается к услугам двух или более сервис-провайдеров, придерживающихся различных маршрутных политик, то он должен создать свою независимую AS. Общим правилом является использование максимально возможного числа маршрутов. Это повышает надежность и способствует перераспределению нагрузки между каналами.

3.3.3 Протоколы Cisco. BGP

Формат BGP-сообщений об изменениях маршрутов

Поле *маркер* содержит 16 октетов и его содержимое может легко интерпретироваться получателем. Если *тип* сообщения "OPEN", или если код идентификации в сообщении open равен нулю, то поле *маркер* должно быть заполнено единицами. Маркер может использоваться для обнаружения потери синхронизации в работе BGP-партнеров.

Поле *длина* имеет два октета и определяет общую длину сообщения в октетах, включая заголовок. Значение этого поля должно лежать в пределах 19-4096.

Поле *тип* представляет собой код разновидности сообщения.

3.3.3 Протоколы Cisco. BGP

Значения поля Тип

1	OPEN	(открыть)
2	UPDATE	(изменить)
3	NOTIFICATION	(внимание)
4	KEEPALIVE	(еще жив)

3.3.3 Протоколы Cisco. BGP

После того как связь на транспортном протокольном уровне установлена, первое сообщение, которое должно быть послано - это OPEN. При успешном прохождении этого сообщения партнер должен откликнуться сообщением KEEPALIVE ("Еще жив"). После этого возможны любые сообщения.

3.3.3 Протоколы Cisco. BGP

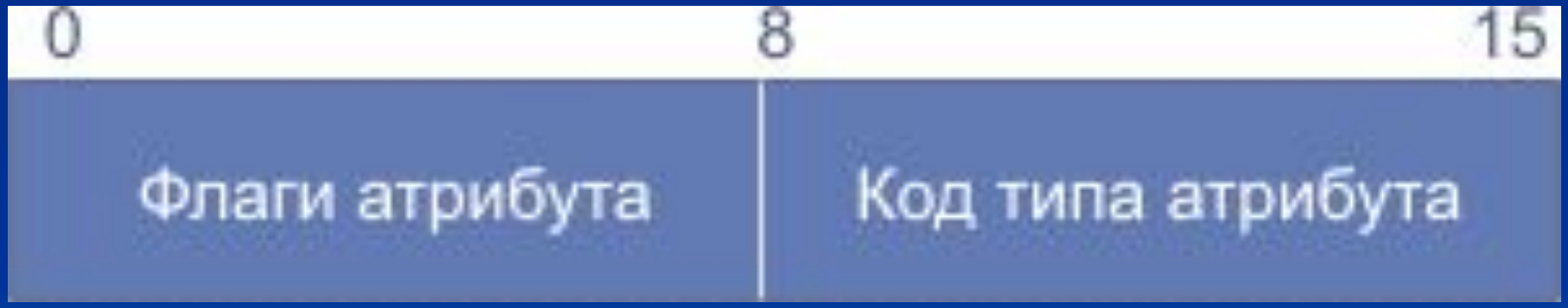
Поля сообщения Open:

3.3.3 Протоколы Cisco. BGP

Сообщения типа UPDATE (изменения) используются для передачи маршрутной информации между BGP-партнерами. Этот тип сообщения позволяет сообщить об одном новом маршруте или объявить о закрытии группы маршрутов, причем объявление об открытии нового и закрытии старых маршрутов возможно в пределах одного сообщения. Сообщение UPDATE всегда содержит стандартный заголовок и может содержать другие поля в соответствии со схемой:

3.3.3 Протоколы Cisco. BGP

Нулевое значение полной длины списка атрибутов пути говорит о том, что информация о доступности сетевого уровня в UPDATE-сообщении отсутствует. Список атрибутов пути присутствует в любом UPDATE-сообщении. Этот список имеет переменную длину, а каждый атрибут содержит три составные части: тип атрибута, длину атрибута и значение атрибута. Тип атрибута представляет собой двух-октетное поле со структурой:



3.3.3 Протоколы Cisco. BGP

Атрибуты пути бывают "стандартные обязательные" (well-known mandatory), "стандартные на усмотрение оператора", "опционные переходные" и "опционные непереходные". Стандартные атрибуты должны распознаваться любыми BGP-приложениями. Опционные атрибуты могут не распознаваться некоторыми приложениями. Обработка нераспознанных атрибутов задается битом 1 поля флагов. Пути с нераспознанными переходными опционными атрибутами должны восприниматься, как рабочие. Один и тот же атрибут может появляться в списке атрибутов пути только один раз.

Предусмотрены следующие разновидности кодов типа атрибута:

ORIGIN (код типа = 1) - стандартный обязательный атрибут, который определяет происхождение путевой информации. Генерируется автономной системой, которая является источником маршрутной информации.

3.3.3 Протоколы Cisco. BGP

Значение атрибута ORIGIN может принимать следующие значения:

Код атрибута	**Описание**
0	IGP - информация достижимости сетевого уровня является внутренней по отношению к исходной автономной системе;
1	EGP - информация достижимости сетевого уровня получена с помощью внешнего протокола маршрутизации;
2	Incomplete - информация достижимости сетевого уровня получена каким-то иным способом.

3.3.3 Протоколы Cisco. BGP

- **AS_PATH** (код типа = 2) также является стандартным обязательным атрибутом, который составлен из совокупности сегментов пути. Атрибут определяет автономные системы, через которые доставлена маршрутная информация. Когда BGP-маршрутизатор передает описание маршрута, которое он получил от своего BGP-партнера, он модифицирует AS_PATH-атрибут, соответствующий этому маршруту, если информация передается за пределы автономной системы. Каждый сегмент AS_PATH состоит из трех частей <тип сегмента пути, длина сегмента пути и оценка сегмента пути>. Тип сегмента пути представляет в свою очередь однооктетное поле, которое может принимать следующие значения:

Код типа сегмента	Описание
1	AS_set: неупорядоченный набор маршрутов в update сообщении;
2	AS_sequence: упорядоченный набор маршрутов автономной системы в UPDATE-сообщении.

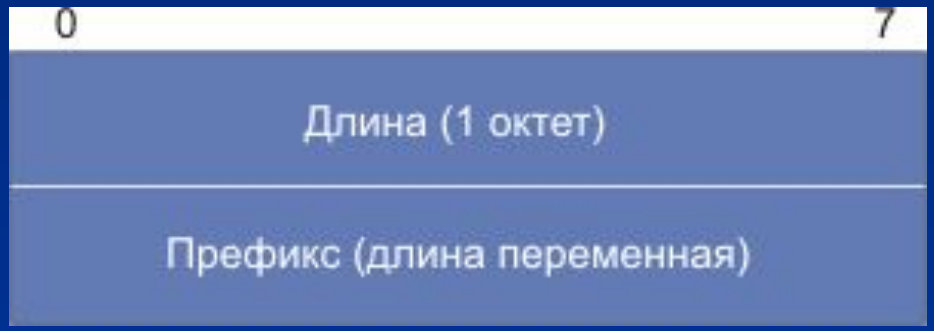
3.3.3 Протоколы Cisco. BGP

Длина сегмента пути представляет собой одно-октетное поле, содержащее число as, записанных в поле *оценка сегмента пути*. Последнее поле хранит один или более кодов автономной системы, по два октета каждый.

- **NEXT_HOP** (код типа = 3) - стандартный обязательный атрибут, определяющий IP-адрес пограничного маршрутизатора, который должен рассматриваться как цель следующего шага на пути к точке назначения.
- **MULTI_EXIT_DISC** (код типа = 4) представляет собой опционный непереходной атрибут, который занимает 4 октета и является положительным целым числом. Величина этого атрибута может использоваться при выборе одного из нескольких путей к соседней автономной системе.
- **LOCAL_PREF** (код типа = 5) является опционным атрибутом, занимающим 4 октета. Он используется BGP-маршрутизатором, чтобы сообщить своим BGP-партнерам в своей собственной автономной системе степень предпочтения объявленного маршрута.
- **ATOMIC_AGGREGATE** (код типа = 6) представляет собой стандартный атрибут, который используется для информирования партнеров о выборе маршрута, обеспечивающего доступ к более широкому списку адресов.
- **aggregator** (код типа = 7) - опционный переходной атрибут с длиной в 6 октетов. Атрибут содержит последний код автономной системы, который определяет агрегатный маршрут (занимает два октета), и IP-адрес BGP-маршрутизатора, который сформировал этот маршрут (4 октета). Объем информации о достижимости сетевого уровня равен (в октетах):

3.3.3 Протоколы Cisco. BGP

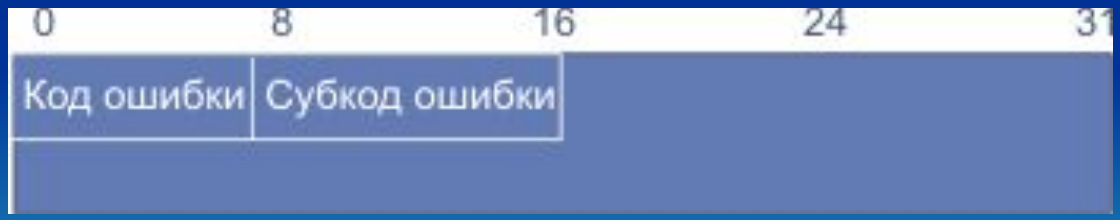
Длина сообщения UPDATE - 23 - полная длина атрибутов пути - длина списка отмененных маршрутов. Информация о достижимости кодируется в следующей форме:



Поле *длина* определяет длину IP-адресного префикса в битах. Если длина равна нулю, префикс соответствует всем IP-адресам. *Префикс* содержит IP-адресные префиксы и двоичные разряды, дополняющие код до целого числа октетов.

3.3.3 Протоколы Cisco. BGP

- Информация о работоспособности соседних маршрутизаторов получается из KEEPALIVE-сообщений, которые должны посылаться настолько часто, чтобы уложиться во время, отведенное таймером сохранения (hold). Обычно это время не должно превышать одной трети от времени сохранения, но не должно быть и меньше 1 секунды. Если выбранное значение времени сохранения равно нулю, периодическая посылка KEEPALIVE-сообщений не обязательна.
- NOTIFICATION-сообщения посылаются, когда обнаружена ошибка. BGP-связь при этом немедленно прерывается. Помимо заголовка NOTIFICATION-сообщение имеет следующие поля:



3.3.3 Протоколы Cisco. BGP

- Возможны следующие коды ошибки:

Код ошибки	Описание
1	Ошибка в заголовке сообщения.
2	Ошибка в сообщении open
3	Ошибка в сообщении update
4	Истекло время сохранения
5	Ошибка машины конечных состояний
6	Прерывание

3.3.3 Протоколы Cisco. BGP

- При отсутствии фатальной ошибки BGP-партнер может в любой момент прервать связь, послав NOTIFICATION-сообщение с кодом ошибки *прерывание*.
- Одно-октетное поле *субкод ошибки* предоставляет дополнительную информацию об ошибке. Каждый код ошибки может иметь один или более субкодов. Если поле содержит нуль, это означает, что никаких субкодов не определено

3.3.3 Протоколы Cisco. BGP

Ошибка	Субкод	Описание
Заголовок	1	Соединение не синхронизовано
	2	Неверная длина сообщения
	3	Неверный тип сообщения
Сообщения OPEN	1	Неверный код версии
	2	Ошибочный код as-партнера
	3	Ошибочный идентификатор BGP
	4	Ошибка в коде идентификации
	5	Ошибка при идентификации
	6	Неприемлемое время сохранения
Сообщения UPDATE	1	Ошибка в списке атрибутов
	2	Не узнан стандартный атрибут
	3	Отсутствует стандартный атрибут
	4	Ошибка в флагах атрибута
	5	Ошибка в длине атрибута
	6	Неправильный атрибут origin
	7	Циклический маршрут
	8	Ошибка в атрибуте next_hop
	9	Ошибка в опционном атрибуте
	10	Ошибка в сетевом поле
	11	Ошибка в as_path

3.3.3 Протоколы Cisco. BGP

- Вся маршрутная информация хранится в специальной базе данных RIB (routing information base). Маршрутная база данных BGP состоит из трех частей:

ADJ-RIBS-IN:	Запоминает маршрутную информацию, которая получена из update-сообщений. Это список маршрутов, из которого можно выбирать. (policy information base - PIB).
LOC-RIB:	Содержит локальную маршрутную информацию, которую BGP-маршрутизатор отобрал, руководствуясь маршрутной политикой, из ADJ-RIBS-IN.
ADJ-RIBS-OUT:	Содержит информацию, которую локальный BGP-маршрутизатор отобрал для рассылки соседям с помощью UPDATE-сообщений.

3.3.3 Протоколы Cisco. BGP

- Так как разные BGP-партнеры могут иметь разную политику маршрутизации, возможны осцилляции маршрутов. Для исключения этого необходимо выполнять следующее правило: если используемый маршрут объявлен не рабочим (в процессе корректировки получено сообщение с соответствующим атрибутом), до переключения на новый маршрут необходимо ретранслировать сообщение о недоступности старого всем соседним узлам.
- Протокол BGP позволяет реализовать маршрутную политику, определяемую администратором AS. Политика отражается в конфигурационных файлах BGP. Маршрутная политика это не часть протокола, она определяет решения, когда место назначения достижимо несколькими путями, политика отражает соображения безопасности, экономические интересы и пр. Количество сетей в пределах одной AS не лимитировано. Один маршрутизатор на много сетей позволяет минимизировать таблицу маршрутов.

3.3.3 Протоколы Cisco. BGP

BGP использует три таймера:

- **Connectretry** (сбрасывается при инициализации и коррекции; 120 сек),
- **Holdtime** (запускается при получении команд Update или Keepalive; 90сек) и
- **keepalive** (запускается при посылке сообщения Keepalive; 30сек).

3.3.3 Протоколы Cisco. BGP

- BGP отличается от RIP и OSPF тем, что использует TCP в качестве транспортного протокола. Две системы, использующие BGP, связываются друг с другом и пересылают посредством TCP полные таблицы маршрутизации. В дальнейшем обмен идет только в случае каких-то изменений. ЭВМ, использующая BGP, не обязательно является маршрутизатором. Сообщения обрабатываются только после того, как они полностью получены.
- BGP является протоколом, ориентирующимся на вектор расстояния. Вектор описывается списком AS по 16 бит на AS. BGP регулярно (каждые 30сек) посылает соседям TCP-сообщения, подтверждающие, что узел жив (это не тоже самое что "Keepalive" функция в TCP). Если два BGP-маршрутизатора попытаются установить связь друг с другом одновременно, такие две связи могут быть установлены. Такая ситуация называется столкновением, одна из связей должна быть ликвидирована. При установлении связи маршрутизаторов сначала делается попытка реализовать высший из протоколов (например, BGP-4), если один из них не поддерживает эту версию, номер версии понижается.

3.3.3 Протоколы Cisco. BGP

- Протокол BGP-4 является усовершенствованной версией (по сравнению с BGP-3). Эта версия позволяет пересылать информацию о маршруте в рамках одного IP-пакета. Концепция классов сетей и субсети находятся вне рамок этой версии. Для того чтобы приспособиться к этому, изменена семантика и кодирование атрибута AS_PASS. Введен новый атрибут **LOCAL_PREF** (степень предпочтительности маршрута для собственной AS), который упрощает процедуру выбора маршрута. Атрибут INTER_AS_METRICSпереименован в MULTI_EXIT_DISC (4 октета; служит для выбора пути к одному из соседей). Введены новые атрибуты **ATOMIC_AGGREGATE** и **AGGREGATOR**, которые позволяют группировать маршруты. Структура данных отражается и на схеме принятия решения, которая имеет три фазы:
- Вычисление степени предпочтения для каждого маршрута, полученного от соседней AS, и передача информации другим узлам местной AS.
- Выбор лучшего маршрута из наличного числа для каждой точки назначения и укладка результата в LOC-RIB.
- Рассылка информации из loc_rib всем соседним AS согласно политике, заложенной в RIB. Группировка маршрутов и редактирование маршрутной информации.

3.3.3 Протоколы Cisco. BGP

Поддержка CIDR

Бесклассовая интердоменная маршрутизация (CIDR- classless interdomain routing, RFC-1520, -1519) - способ избежать того, чтобы каждая С-сеть требовала свою таблицу маршрутизации.

- Основополагающий принцип CIDR заключается в группировке (агрегатировании) IP-адресов таким образом, чтобы сократить число входов в таблицах маршрутизации (RFC-1519, RFC-1518, RFC-1467, RFC-1466).
- Протокол совместим с RIP-2, OSPF и BGP-4. Основу протокола составляет идея бесклассовых адресов, где нет деления между полем сети и полем ЭВМ. Дополнительная информация, например 32-разрядная маска, выделяющая поле адреса сети, передается в рамках протокола маршрутизации.
- При этом выдерживается строгая иерархия адресов: провайдер > предприятие > отдел/здание > сегмент локальной сети. Групповой (агрегатный) адрес воспринимается маршрутизатором как один адрес.
- Группу может образовывать только непрерывная последовательность IP-адресов. Такой бесклассовый интернетовский адрес часто называется IP-префиксом. Так адрес 192.1.1.0/24 означает диапазон адресов 192.1.1.0 - 192.1.1.255, а адрес 192.1.128.0/17 описывает диапазон 192.1.128.0 - 192.1.255.255, таким образом, число, следующее после косой черты, задает количество двоичных разрядов префикса. Это представление используется при описании политики маршрутизации и самих маршрутов

3.3.3 Протоколы Cisco. BGP

Итог

- BGP, в отличие от других протоколов динамической маршрутизации, предназначен для обмена информацией о маршрутах не между отдельными маршрутизаторами, а между целыми автономными системами, и поэтому, помимо информации о маршрутах в сети, переносит также информацию о маршрутах на автономные системы. BGP не использует технические метрики, а осуществляет выбор наилучшего маршрута исходя из правил, принятых в сети.
- BGP поддерживает бесклассовую адресацию и использует суммирование маршрутов для уменьшения таблиц маршрутизации. С 1994 года действует четвёртая версия протокола, все предыдущие версии являются устаревшими.
- BGP является протоколом сетевого уровня, однако функционирует поверх протокола транспортного уровня TCP (порт 179).
- BGP, наряду с DNS, является одним из главных механизмов, обеспечивающих функционирование Internet.

Т.о. применяя такое решение, Cisco удалось добиться улучшения таких характеристик, как производительность и масштабируемость.

4. Выводы

- Из данной лекции видно, что принципы, составляющие идеологию Cisco, решают актуальные для проектировщиков сетей проблемы. Причем решают приемлемым для них образом. А именно:
- В рассмотренных решениях, которые применяются Cisco, было достигнуто улучшение следующих характеристик:
  - *Производительность*
  - *Надежность*
  - *Безопасность*
  - *Масштабируемость*

  Т.е. улучшение достигнуто по большинству из основных характеристик сетей.
- Это также объясняет востребованность продуктов данной компании на рынке маршрутизаторов.

5. Литература

- Дж. Ф. Димарцио «Маршрутизаторы Cisco»
- www.cisco.com
- http://book.itep.ru
- www.wikipedia.org
- http://network.xsp.ru/5_7.php
- http://www.osp.ru/text/302/133837/