

**САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М. А. БОНЧ-БРУЕВИЧА**

Факультет СС, СК и ВТ

Дипломная работа

на тему

**«Анализ протоколов маршрутизации в Интернет
на примере маршрутизатора Cisco»**

Дипломник Коваленко А. А.

Руководитель работы Доронин Е. М.

Санкт-Петербург

2013 г.

Реферат

Тема дипломной работы: «Анализ протоколов маршрутизации в Интернет на примере маршрутизатора Cisco».

Пояснительная записка включает в себя: 78 страниц текста, 21 рисунок, 9 таблиц.

Ключевые слова: Интернет, маршрутизатор, маршрутизация, протокол маршрутизации, таблица маршрутизации, RIP, OSPF, EIGRP, BGP, Cisco, IP-адрес, маска, локальные сети, глобальные сети, модель ISO.

Цель работы: для разрабатываемого на кафедре ОПДС учебного пособия «Интернет-технологии» выполнить анализ и описать заданные протоколы маршрутизации и на примере маршрутизаторов Cisco показать их настройку.

В дипломной работе был проведен анализ внутренних протоколов маршрутизации RIP и OSPF. Представлена их сравнительная характеристика. Рассмотрен протокол внешней маршрутизации BGP.

На оборудовании Cisco была выполнена упрощенная настройка протоколов маршрутизации. Как новый элемент учебно-методических материалов по дисциплине «Интернет-технологии» был разработан видеоурок. Видеоурок посвящен описанию принципов конфигурирования протоколов маршрутизации в ПО Cisco Packet Tracer, эмулирующем интерфейс встраиваемой сетевой ОС Cisco IOS.

Помимо настраиваемых протоколов маршрутизации в видео уроке наглядно представлена настройка DHCP и NAT.

Так же в дипломной работе рассмотрены следующие вопросы:

- ◆ маршрутизатор компании Cisco Systems серии 1800, его внутренние компоненты и возможности;
- ◆ серии маршрутизаторов компании Cisco Systems, которые представлены на рынке в настоящее время;
- ◆ конкурирующие компании по производству маршрутизаторов;
- ◆ кратко рассмотрена пакетная передача данных в сетях мобильных операторов с применением маршрутизаторов.

Содержание

| | |
|---|----|
| Введение..... | 6 |
| 1. Основные понятия | 10 |
| 1.1. Компьютерная сеть | 10 |
| 1.2. Маршрутизация | 15 |
| 2. Краткий обзор протоколов маршрутизации..... | 20 |
| 2.1. Протокол маршрутизации | 20 |
| на базе вектора расстояний | 20 |
| 2.2. Протокол маршрутизации | 24 |
| на основе состояния канала | 24 |
| 2.3. Усовершенствованный протокол маршрутизации на базе вектора расстояний | 29 |
| 2.4. Сравнительная характеристика внутренних протоколов маршрутизации..... | 33 |
| 2.5. Внешний протокол маршрутизации..... | 34 |
| 3. Структура и характеристики маршрутизаторов компании Cisco Systems .. | 37 |
| 3.1. Маршрутизатор Cisco 1811 | 39 |
| 3.2. Настройка маршрутизаторов Cisco | 50 |
| 4. Рекомендации по выбору маршрутизаторов | 58 |
| 4.1. Производители маршрутизаторов | 58 |
| 4.2. Серии маршрутизаторов Cisco | 68 |
| 4.3. Пакетная передача данных в сетях мобильных операторов..... | 75 |
| Заключение | 78 |
| Список использованной литературы..... | 79 |

Введение

Цель дипломной работы: для разрабатываемого на кафедре ОПДС учебного пособия «Интернет-технологии» выполнить анализ и описать заданные протоколы маршрутизации и на примере маршрутизаторов Cisco показать их настройку.

Для того чтобы понять, что такое Интернет, надо знать, что такое сеть в общем. Сеть – совокупность оконечных устройств связи, объединённых каналами передачи данных и коммутирующими устройствами (узлами сети), обеспечивающими обмен данных между всеми оконечными устройствами.

Различают локальные и глобальные сети. В локальных сетях компьютеры могут быть расположены в одной комнате или в одном здании. Глобальная сеть может объединять десятки тысяч локальных сетей, разбросанных по всему миру. Примером глобальной сети является Интернет (Internet).

Определение термина Интернет было дано 24.10.1995 года Федеральным советом США по компьютерным сетям (FNC - Federal Networking Council): «Internet - это глобальная информационная система, которая логически соединена посредством адресного пространства, основанного на протоколе IP (Internet Protokol) или заменяющих его протоколов, способна поддерживать передачу данных посредством протокола TCP (Transmission Control Protocol) или заменяющих его протоколов, обеспечивает, использует или делает доступными услуги по передаче данных и соответствующую инфраструктуру».

Устройства, которые обеспечивают передачу данных между различными сетями, называют маршрутизаторами, к тому же они определяют наилучший путь для передачи этих данных.

Для обмена информацией в Интернет необходимо знать адрес отправителя и адрес получателя. Обычно для этого используется протокол сетевого уровня – IP. Длина IP-адреса по версии 4 составляет 32 бита,

нетрудно посчитать, что количество адресов примерно равно 4,23 миллиарда. Довольно небольшое количество, учитывая, что если надо организовать обмен данными между всеми устройствами (компьютеры, принтеры, серверы и т.д.), то необходимо выделить IP-адрес каждому устройству, к тому же эти адреса платные.

Использование маршрутизатора позволяет более рационально назначать IP-адреса. Приведем самый простой пример. Есть локальная сеть, состоящая из N компьютеров, которым необходим выход в глобальную сеть. Каждому устройству присваивают частный IP-адрес (диапазон адресов, который не используется в глобальных сетях) и подключают к маршрутизатору. На WAN-интерфейсе прописывается только один внешний IP-адрес. К LAN-интерфейсам подключены все компьютеры. Далее включают механизм NAT – это процесс трансляции локальных адресов во внешние. Благодаря этому процессу компьютер получает доступ в Интернет.

Для маршрутизации используются таблицы маршрутизации и протоколы, которые реализуют алгоритмы маршрутизации, чтобы определить наиболее рациональный путь для пересылки пакета данных. Протоколы маршрутизации могут делиться по типу взаимодействия между сетями. Внутренний протокол маршрутизации – протокол, служащий для обмена данными внутри автономной системы, например: RIP, OSPF и EIGRP; внешний протокол маршрутизации – протокол, служащий для обмена данными между автономными системами, например: BGP. Внутренние протоколы маршрутизации могут использовать алгоритм маршрутизации на основе вектора расстояний или на основе состояния канала.

Есть множество компаний, которые занимаются производством сетевого оборудования. Приведу некоторые из них:

- ◆ Cisco Systems, Inc. – американская компания, основана в 1984 году. Мировой лидер в сфере телекоммуникационного оборудования. Представляет продукты и решения для IP-коммуникаций, сетевой безопасности, беспроводных сетей корпоративного уровня;

- ◆ D-link – тайваньская компания, основана в 1986 году, занимается производством сетевого и телекоммуникационного оборудования. Предлагает широкий набор продуктов и решений для домашних пользователей, корпоративного сегмента бизнеса и провайдеров интернет-услуг;
- ◆ Huawei Technologies Co. Ltd. – китайская компания, основана в 1987 году. Одна из крупнейших компаний в сфере телекоммуникаций;
- ◆ Juniper Networks – американская компания, основана в 1996 году. Является признанным мировым лидером в разработке и производстве комплексных сетевых решений для операторов связи;
- ◆ ZyXEL Communications Corp – тайваньская компания, основана в 1989 году, занимается производством сетевого и телекоммуникационного оборудования.

При выборе маршрутизатора необходимо знать, для каких целей он нужен, для организации домашней сети или организации корпоративной сети филиала компании и т.д. Например, для организации домашней сети не следует покупать маршрутизатор Cisco серии 7200, так как все возможности его попросту не будут реализованы в такой сети, и к тому же стоимость этой домашней сети будет дорогой.

Cisco является мировым лидером в предоставлении маршрутизаторов, коммутаторов и других сетевых устройств и производит различные серии маршрутизаторов. Серии варьируются в зависимости от возможностей, плотности портов и программного обеспечения. Управление маршрутизатором Cisco осуществляется в режиме командной строки программного обеспечения Cisco IOS.

Маршрутизаторы для филиалов.

- ◆ Серия Cisco 800 включает маршрутизаторы для широкополосных сетей, обеспечивающие защищенный доступ в Интернет или корпоративные сети для малых удаленных офисов или удаленно работающих сотрудников.

◆ Маршрутизаторы с интегрированными сервисами Cisco серии 1800 используют в сетях малых и средних компаний, а также в небольших филиалах предприятий. Устройства позволяют компаниям снизить издержки благодаря единой отказоустойчивой системе, обеспечивающей предоставление ряда важнейших деловых услуг, таких как: Передача данных, Безопасность, Унифицированные коммуникации, Беспроводные сети.

◆ Cisco серии 2800 применяют в сетях малых и средних компаний. Устройства предназначены для обеспечения одновременной работы различных сервисов с высоким уровнем защиты и скоростью физической линии. Архитектура обеспечивает необходимый уровень производительности, доступности и надежности для успешного масштабирования важнейших приложений в самых требовательных условиях.

◆ Маршрутизаторы с интегрированными сервисами Cisco серии 3800, идеально подходят для средних и крупных предприятий, а также филиалов, позволяют упростить развертывание и управление сетью, снизить расходы на ее создание и обслуживание, обеспечить поддержку важнейших деловых приложений. Устройства являются отличной защищенной платформой для работы каналов T3/E3 со скоростью физической линии.

Платформы для объединения центров обработки данных.

◆ Маршрутизаторы Cisco серии 7200 являются наиболее распространенными универсальными решениями для агрегации сервисов. Серия маршрутизаторов Cisco 7200 разработана как агрегирующее (объединяющее) устройство для сервис-провайдеров и идеально подходит в качестве центрального маршрутизатора или в качестве пограничного маршрутизатора ISP-компаний (поставщики интернет услуг). Оборудование серии Cisco 7200 гарантирует высокую надежность, отказоустойчивость, поддержку огромного спектра сред передачи данных.

❖ Маршрутизаторы Cisco ASR 1000 серии Сервисных Маршрутизаторов Агрегации спроектированы, чтобы оптимизировать границу системной службы и решения для соединения частей предприятия.

В дипломной работе рассмотрены следующие вопросы:

1. Что такое маршрутизация.
2. Сравнение внутренних протоколов маршрутизации. Обзор внешнего протокола маршрутизации.
3. Описание одного из маршрутизаторов компании Cisco и его базовые настройки.
4. Обзор компаний, производящих маршрутизаторы.

1. Основные понятия

1.1. Компьютерная сеть

Для уяснения понятия *маршрутизация*, введем начальные определения.

Компьютерная сеть – совокупность оборудования (компьютеры, серверы, средств коммутации и др.), соединенная каналами связи, представляющая единую систему для обмена информацией.

Сеть можно представить в виде графа, в котором узлы играют роль сетевого оборудования, а ребра, соединяющие узлы – каналы связи. Узлы могут быть оконечными, промежуточными или смежными. Оборудование может быть соединено друг с другом различными способами.

Соединение всех компонентов сети называют топологией.

Существует множество способов соединения оборудования. Примеры наиболее распространенных топологий:

❖ Шина (рис. 1.1). Все устройства соединяются с помощью одного кабеля, на концах находятся терминаторы, предотвращающие отражение сигнала. Сообщение, отосланное с одной машины, пересылается всем, и только та, которой оно адресовано, будет его обрабатывать. Такое построение сети отличается дешевизной и простой настройкой. Минус в

том, что при выходе из строя общего кабеля или терминатора система откажет в работе. Так же тяжело найти неисправность на сети;

❖ Кольцо (рис. 1.2). Оборудование подключается только к двум своим соседям. Данные передаются от устройства к устройству в одном направлении, вследствие чего не возникает коллизий пакетов данных. Каждое устройство ждет своей очереди для передачи данных. При отказе любого оборудования вся система выходит из строя, и найти неисправность сложно;

❖ Звезда (рис. 1.3). К центральному узлу подключаются все рабочие станции, при их отказе система не выйдет из строя. Но в случае отказа центрального узла вся сеть становится не работоспособной. Тем не менее, этот вид топологии отличается высокой производительностью, при правильном проектировании сети, и легкостью поиска неисправностей;

❖ Двойное кольцо (рис. 1.4). В этом варианте кольцевой топологии создается второе кольцо для передачи данных в обоих направлениях. Система становится более отказоустойчивой;

❖ Дерево (рис. 1.5). Разновидность топологии звезда. Отличия только в том, что схема более сложная и соблюдается иерархичность;

❖ Полносвязная (рис. 1.6). Все узлы соединяются друг с другом, поэтому система отказоустойчивая. Но такая топология очень дорогая и сложная, поэтому лучше создавать частично связанную топологию.

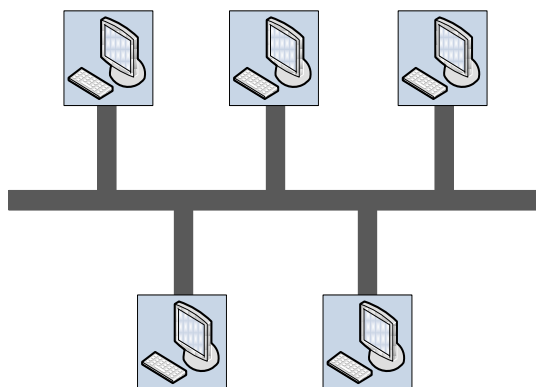


Рис. 1.1. Топология типа «Шина»

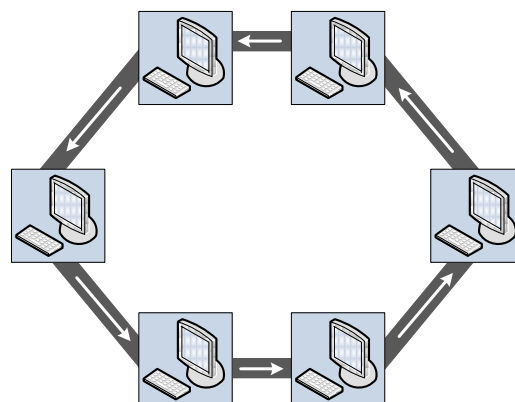


Рис. 1.2. Топология типа «Кольцо»

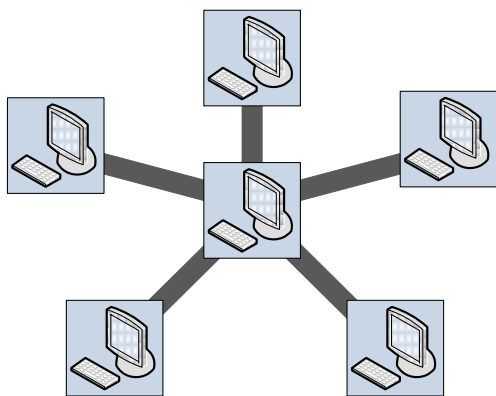


Рис. 1.3. Топология типа «Звезда»

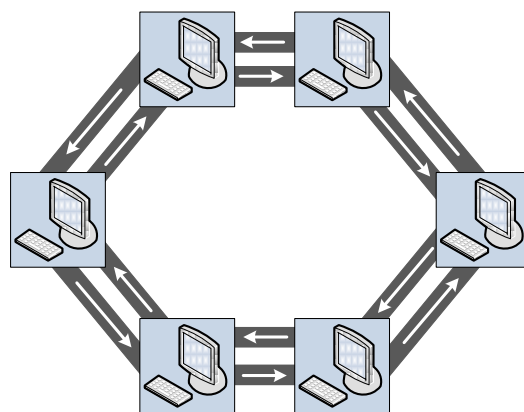


Рис. 1.4. Топология типа «Двойное кольцо»

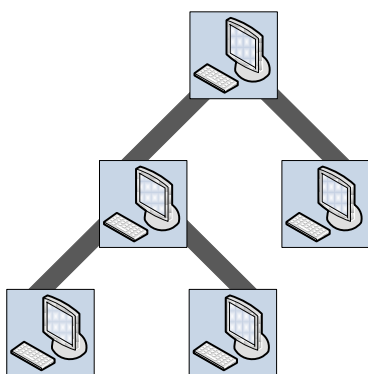


Рис. 1.5. Топология типа «Дерево»

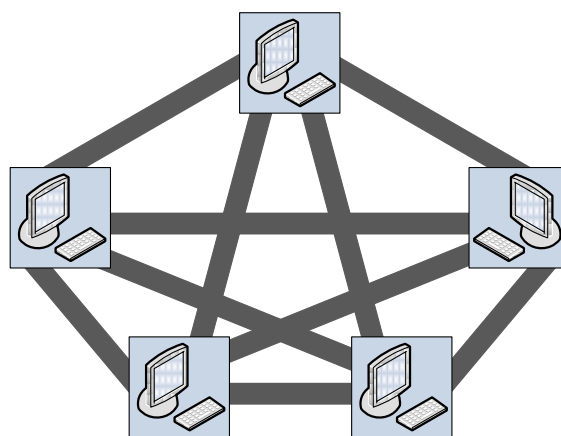


Рис. 1.6. Топология типа «Полносвязная»

Для организации передачи данных между узлами используют наборы правил – протоколы.

Все протоколы взаимодействуют друг с другом определенным образом. Международная организация по стандартам разработала модель, которая определяет функции уровней взаимодействующих систем. Это базовая эталонная модель взаимодействия открытых систем (OSI/ISO). Она включает в себя семь уровней.

В сети Интернет используется стек протоколов TCP/IP. Этот набор протоколов был разработан Министерством обороны США (Department of Defence, DoD) еще до появления модели OSI/ISO. Он включает в себя только

четыре уровня. Ниже представлено соответствие уровней модели OSI/ISO и стека TCP/IP (рис. 1.7).

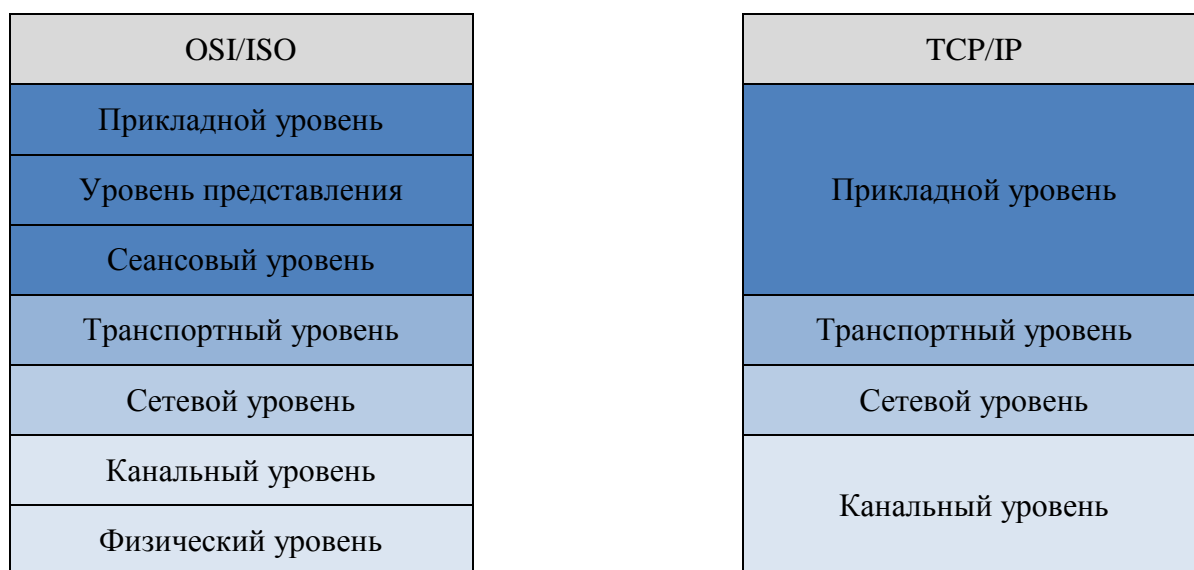


Рис. 1.7. Модель OSI/ISO и стек протоколов TCP/IP

Уровни модели OSI/ISO:

- ◆ прикладной уровень – уровень доступа приложений к сети. Отвечает за обмен данными между приложениями на устройстве пользователя и сетью. (Пример протокола: HTTP);
- ◆ представительный уровень – уровень, который отвечает за то, что данные, передаваемые на прикладном уровне, будут прочитаны и защищены;
- ◆ сеансовый уровень – осуществляет обмен между двумя приложениями. Основной элемент передачи – Protocol Data Unit (PDU) – Модуль данных протокола. (Пример протокола: RPTP);
- ◆ транспортный уровень – уровень отвечает за взаимодействие непосредственно двух точек, соединение которых уже установлено. Основной элемент передачи – сегмент. (Примеры протоколов: TCP, UDP);
- ◆ сетевой уровень – подключение и выбор пути между двумя точками для передачи данных. Основной элемент передачи – датаграмма. (Пример протокола: IP);

- ◆ канальный уровень – определяется формат данных для передачи и методы контроля доступа к физической среде. Основной элемент передачи данных – кадр. (Пример протокола: Ethernet);
- ◆ физический уровень – отвечает за физическое соединение между оборудованием. На этом уровне описываются электрические или оптические сигналы, необходимые для связывания двух конечных точек. (Примеры: электрический сигнал, модуляция, синхронизация).

При передаче данных информация «упаковывается» в пакет, начиная с верхнего уровня (прикладного) до нижнего (физического), этот процесс называется инкапсуляция. После этого пакет отправляется в сеть. При его получении происходит «распаковывание» от нижнего уровня к верхнему, и этот процесс называется деинкапсуляция.

Компьютерные сети делятся на:

- ◆ локальные сети (LAN, Local Area Network) – компьютерная сеть, покрывающая относительно небольшую территорию (комната, офис, здание);
- ◆ глобальные сети (WAN, Wide Area Network) – как правило, объединение большого количества локальных сетей.

Интернет (Internet) – глобальная сеть, состоящая из объединения тысяч корпоративных, научных, правительственных и домашних компьютерных сетей.

Для связи между сетевым оборудованием в локальных и глобальных сетях обычно используется протокол сетевого уровня – IP (Internet Protocol). На данный момент существует две версии протокола:

- ◆ IPv4 – каждому узлу присваивается IP-адрес длиной 32 бита (4 байта – 4 октета);
- ◆ IPv6 – каждому узлу присваивается IP-адрес длиной 128 бит (16 байт – 8 групп).

Формат IP-адреса (протокол IPv4) представляет собой 32-х битное двоичное число, для простоты это число разбивают на октеты по 8 бит

каждый и разделяют точкой. Двоичные числа в каждом октете преобразуют в десятичные от 0 до 255.

13 14 49 121
00001101.00001110.00110001.01111001

В локальных сетях используются особые IP адреса (протокол IPv4), называемые частными, внутренними (на сленге «серыми»), которые не используются в глобальной сети:

- ◆ 10.0.0.0 - 10.255.255.255;
- ◆ 172.16.0.0 - 172.31.255.255;
- ◆ 192.168.0.0 - 192.168.255.255.

Необходимость в таких адресах возникла из-за того, что не ожидали такого большого роста и использования сети. Конечно, проблему увеличения количества IP-адресов сейчас решает протокол IPv6, но на данный момент этот протокол еще широко не используется.

1.2. Маршрутизация

Маршрутизация – это процесс пересылки пакетов данных между сетями или подсетями с помощью устройств третьего уровня модели OSI/ISO.

Для маршрутизации используются таблицы маршрутизации и протоколы, которые реализуют алгоритмы маршрутизации, чтобы определить наиболее рациональный путь для пересылки пакета данных.

Устройство, которое определяет более приемлемый путь для передачи данных из одной сети в другую, называется маршрутизатор.

Для обмена данных в сетях маршрутизатор ведет таблицу маршрутизации. Она представляет собой список сетевых адресов, а так же хранит данные о местах назначения и связях со следующими переходами. С

помощью этих связей устройство понимает, можно ли добраться до пункта назначения напрямую или через другие маршрутизаторы. Таблица может хранить следующие виды записей (одна запись для каждой сети):

- ◆ статические – информация о маршруте заполняется вручную, но этот способ приводит к проблемам в случае изменения топологии сети или же отказа на каком-либо участке;
- ◆ динамические – заполнение происходит благодаря обмену данными маршрутизации между устройствами, полученных по протоколу маршрутизации, то есть маршрутизаторы обмениваются информацией друг с другом путем передачи сообщений об обновлении. В зависимости от протокола обновления могут поступать периодически или же только при изменении топологии.

Возникают ситуации, когда есть несколько путей передачи информации от источника до места назначения. Каждый протокол маршрутизации использует свои метрики для определения наилучшего пути. Если же используются различные протоколы, то приемлемый путь выбирается на основе административного расстояния – это число от 0 до 255 (рис. 1.8).

| Источник маршрутов | Расстояние по умолчанию |
|-------------------------------------|--|
| Подключенная сеть | 0 |
| Статический маршрут | 1 |
| EIGRP | 90 |
| OSPF | 110 |
| RIP | 120 |
| BGP | 200 |
| Не известный или не предусмотренный | 255 (не будет использоваться для передачи трафика) |

Рис. 1.8. Значения административного расстояния

Протокол с наименьшим значением выбирается как более надежный.

Протокол маршрутизации - это набор правил, которые маршрутизатор использует при «общении» с другими маршрутизаторами, чтобы определить пути к удаленным сетям, а так же для ведения записей об этих сетях в таблице маршрутизации. Существуют два понятия, которые нельзя путать:

- ◆ маршрутизируемый протокол – любой протокол с адресом сетевого уровня, который осуществляет пересылку пакетов между хостами. У этого протокола, как правило, нет информации обо всем маршруте от источника до места назначения. Например, протокол IP;
- ◆ протокол маршрутизации – позволяет обеспечить обмен данными маршрутизации между сетями, и позволяет создать динамические таблицы маршрутизации. Маршрутизатор должен знать, куда отправить пакет, но не его последующий путь от других маршрутизаторов.

Протоколы маршрутизации различаются по типу взаимодействия между сетями. Это различие связано с понятием автономная система (рис. 1.9).

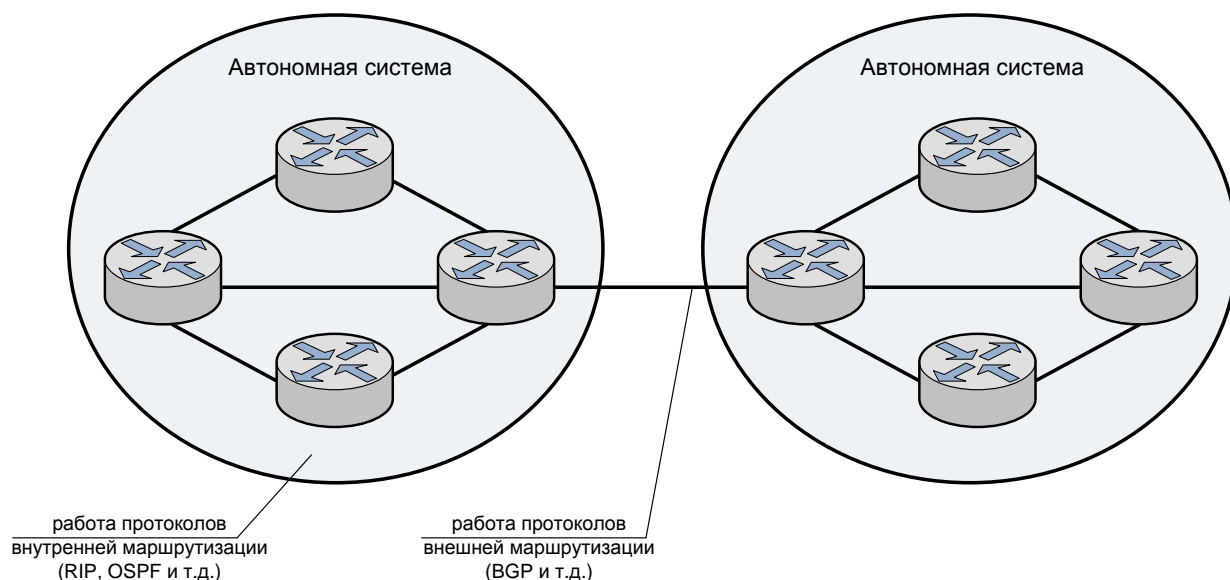


Рис. 1.9. Классификация протоколов по типу взаимодействия между сетями

Автономная система (АС) – это совокупность сетей с общим управлением, маршрутизаторы в АС имеют единые правила маршрутизации. В соответствии с этим понятием есть два типа протоколов маршрутизации:

- ◆ внутренний протокол маршрутизации – протокол, служащий для обмена информацией внутри АС. Например: RIP, OSPF, EIGRP и др.;
- ◆ внешний протокол маршрутизации – протокол, служащий для обмена информацией между автономными системами. Например: BGP.

Такое деление протоколов определяет иерархический метод маршрутизации.

Протоколы маршрутизации можно классифицировать по использованию определенного алгоритма маршрутизации, который необходим для определения оптимального пути прохождения пакетов от источника к месту назначения.

Требования, которым должны отвечать алгоритмы маршрутизации:

- ◆ оптимальность – способность алгоритма выбрать лучший путь;
- ◆ простота – алгоритм не должен требовать большой программной реализации;
- ◆ живучесть – алгоритм должен функционировать в случае непредвиденных обстоятельств, таких как отказ оборудования, высокие нагрузки на сети и т.д.;
- ◆ быстрая сходимость – процесс соглашения между всеми маршрутизаторами по наилучшим путям. Т.е., например, при отказе какого либо маршрутизатора, сообщения об обновлении топологии сети должны дойти до других маршрутизаторов с минимальной задержкой. В итоге маршрутизаторы пересчитывают пути и выбирают оптимальный. Алгоритмы, которые сходятся медленно, могут привести к нежелательным последствиям, таким как образование петель, выход из строя всей сети и т.д.;

◆ гибкость – алгоритм должен точно и быстро адаптироваться к изменениям в сети. Например, изменение топологии сети, полосы пропускания определенных линий, задержка и т.п.;

Различают следующие основные алгоритмы маршрутизации:

◆ статические. Системный администратор вручную прописывает записи в таблице маршрутизации. Такой метод маршрутизации непригоден для больших сетей. Так же его сложно настраивать при изменении топологии сети;

◆ динамические. Этот алгоритм учитывает изменения на сети, благодаря поступающим сообщениям. При изменении топологии произойдет пересчет путей, после чего осуществится новая рассылка сообщений об изменении маршрутов.

Протоколы внутренней маршрутизации можно классифицировать по использованию одного из следующих динамических алгоритмов маршрутизации:

◆ метод маршрутизации на основе вектора расстояний. Этот метод определяет направление и расстояние (например, количество переходов) к любому каналу другой сети, путем рассылки вектора. При получении вектора от соседа маршрутизатор увеличивает расстояние, а также добавляет информацию об известных ему сетях и рассылает новое значение вектора по сети. Минус этого метода в том, что в больших сетях широковещательная рассылка отрицательно скажется на работе сети;

◆ метод маршрутизации на основе состояние канала. Маршрутизаторы обмениваются сообщениями о состоянии канала со своими соседями, при этом каждый маршрутизатор создает базу данных топологии сети, на основе полученных сообщений. После этого алгоритм удаляет лишние пути и составляет свое дерево кратчайших путей.

Идеального алгоритма поиска пути для всей сети не существует.

В алгоритмах маршрутизации используется много различных показателей, называемых метрикой. Это число, которое генерирует алгоритм

для каждого пути. Чаще всего меньшая метрика означает наилучший путь. Сложные алгоритмы маршрутизации при выборе маршрута могут базироваться на множестве показателей или их комбинации. Ниже перечислены метрики, которые чаще всего используются в алгоритмах маршрутизации.

- ◆ Количество переходов. Число показывающее, сколько переходов через оборудование должен совершить пакет, чтобы добраться от источника к месту назначения.
- ◆ Скорость передачи данных в канале (полоса пропускания).
- ◆ Задержка. Время, необходимое для передачи пакета от источника до места назначения. Задержка может зависеть от многих факторов, таких как загрузка сети, пропускная способность каналов и т.п.
- ◆ Загрузка. Активность сетевого ресурса, маршрутизатора, канала и т.д.
- ◆ Надежность. Надежность, относится к надежности канала связи. Некоторые каналы сети могут отказывать чаще, чем другие. Отказы одних каналов сети могут быть устранены легче или быстрее, чем отказы других каналов. При назначении оценок надежности могут быть приняты в расчет любые факторы надежности.
- ◆ Стоимость. Настраиваемое значение.

2. Краткий обзор протоколов маршрутизации

2.1. Протокол маршрутизации на базе вектора расстояний

Одним из наиболее распространенных протоколов маршрутизации на базе вектора расстояний, является протокол RIP (Routing Information Protocol).

Основные характеристики протокола RIP:

- ◆ дистанционно-векторный протокол маршрутизации;
- ◆ метрика – число переходов;

- ◆ максимальное число переходов – 15;
- ◆ широковещательная рассылка обновлений маршрутизации по умолчанию – 30 секунд.

Эволюция протокола RIP заключалась в переходе от классового протокола маршрутизации (RIPv1) к бесклассовому протоколу (RIPv2). В соответствии с этим RIPv2:

- ◆ поддерживает маску переменной длины;
- ◆ отправляет маску подсети вместе с обновлением маршрутизации;
- ◆ групповая рассылка (RIPv1 – широковещательная рассылка);
- ◆ поддержка суммирования маршрутов вручную;
- ◆ поддержка аутентификации (процедура проверки подлинности).

В чем состоит основное отличие классовой маршрутизации от бесклассовой. Существует такое понятие как маска подсети – набор битов, определяющий, какая часть в IP-адресе показывает адрес сети, а какая показывает адрес узла в этой сети. Набор представляет собой непрерывную последовательность единиц и нулей.

```

IP Адрес – хоста  13.14.49.121
                  13    14    49    121
                  00001101.00001110.00110001.01111001

Маска
                255    255    255    0    = /24
                11111111.11111111.11111111.00000000
                └──────────────────┬──────────┘
                   сеть             хосты

Компактная запись
IP Адрес – хоста  13.14.49.121/24
IP Адрес – сети   13.14.49.0
  
```

Классовая адресация необходима для разделения сетей на подсети, при этом используются «стандартные» маски.

Для сетей класса А – маска 255.0.0.0, для сетей класса В – маска 255.255.0.0, для сетей класса С – маска 255.255.255.0.

Так как маленьких сетей намного больше, чем представлено в классе C, ввели бесклассовую адресацию. Для организации такой адресации используют маски переменной длины.

```

IP Адрес – хоста  13.14.49.121
                  13    14    49    121
                  00001101.00001110.00110001.01111001

Маска
                255    255    255    192    = /26
                11111111.11111111.11111111.11000000
                └──────────────────┬──────────┘
                              сеть   хосты

IP Адрес – сети
                  13    14    49    121
                  00001101.00001110.00110001.01111001
                  00001101.00001110.00110001.01000000
                  13    14    49    64

Компактная запись
IP Адрес – хоста  13.14.49.121/26
IP Адрес – сети  13.14.49.64
    
```

Учитывая это, можно сказать, что протокол RIPv2 с поддержкой бесклассовой маршрутизацией имеет больше возможностей.

Принцип работы протокола RIP. Маршрутизаторы обмениваются сообщениями о маршрутизации только со своими соседями (прямое подключение). Обновления эти происходят периодически, вне зависимости изменилась топология сети или нет, и включают в себя полную таблицу маршрутизации. Получив таблицу, маршрутизатор вносит определенные изменения в свою таблицу.

Существует ряд проблем, возникающих с работой протокола RIP.

Например, есть три маршрутизатора, которые соединены последовательно (рис. 2.1) . У каждого маршрутизатора уже составлена своя таблица маршрутизации до каждой сети. Неожиданно, сеть №4 отказала в доступе, соответственно маршрутизатор №3 прекращает отправлять пакеты в эту сеть. Но маршрутизаторы №1 и №2 не знают об отказе сети №4.

Маршрутизатор №1 видит, что сеть доступна через маршрутизатор №2, то есть в таблице маршрутизации указана сеть №4 с метрикой 2. Соответственно эта сеть так же записывается на втором маршрутизаторе, как известная. Таблица маршрутизации отправляется маршрутизатору №3, и он считает, что он имеет доступ к сети №4 через маршрутизатор №2.

Таким образом, метрика будет расти по кругу до бесконечности. Эта проблема решается путем задания максимума, в случае с протоколом RIP этот максимум равен 16 переходам.

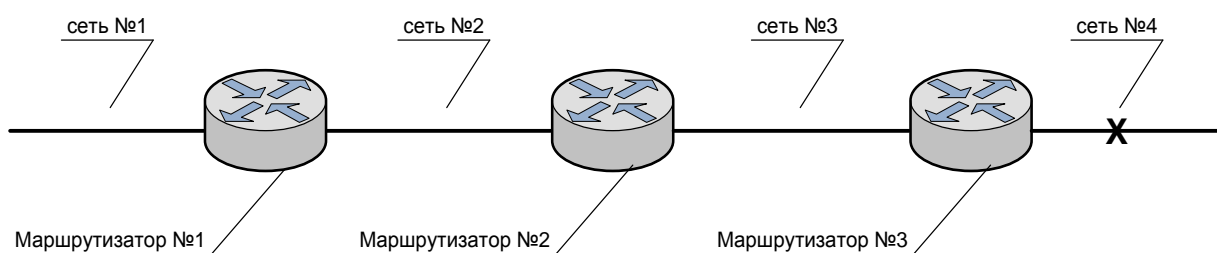


Рис. 2.1. Пример последовательного соединения маршрутизаторов

Иногда в сетях, использующих протокол RIP, возникают петли. Из рассмотренного примера видно, что при отказе сети №4 посланный пакет из сети №1 будет бесконечно блуждать между маршрутизаторами №2 и №3, то есть образуется петля. Есть несколько методов, которые не допускают образование петель.

1. Split Horizon.

Суть метода заключается в том, что маршрутизатор не будет отправлять данные о маршруте в обратную сторону.

2. Route Poisoning

При отказе сети №4 маршрутизатор №3 присваивает каналу в этом направлении метрику 16 переходов (то есть сеть недоступна). Благодаря этому маршрутизатор не будет воспринимать поступающие обновления (информация, что сеть доступна) от других маршрутизаторов.

3. Таймеры удержания.

Таймер удержания информации позволяет предотвратить петли, однако увеличивает время сходимости сети. Стандартное время удержания в

протоколе RIP составляет 180 секунд. Это время можно изменять. Идеальным решением является установка этого периода чуть большим максимального времени обновления маршрутов данной сети.

Так, если отказала сеть №4, сразу же на маршрутизаторе №3 запускается таймер удержания, и маршрут к сети №4 отмечается как недоступный. Если от соседних маршрутизаторов придет обновление с лучшей метрикой, то сеть станет доступна, и таймер будет удален. В ином случае обновления будут игнорироваться. Благодаря этому увеличится время, чтобы распространить обновления об изменении сети.

Вывод:

В современных сетях протокол RIP не самое лучшее решение для выбора в качестве протокола маршрутизации, так как его возможности уступают более современным протоколам, таким как EIGRP, OSPF. Ограничение на 15 переходов не позволяет применять его в больших сетях. Преимущество этого протокола – простота конфигурирования. Поэтому, если сеть небольшая, то протокол RIP вполне приемлем как протокол маршрутизации.

2.2. Протокол маршрутизации на основе состояния канала

Одним из распространенных протоколов на основе состояния канала является протокол OSPF. Это бесклассовый протокол маршрутизации. Технология работы протокола заключается в отслеживании состояния каналов и поиска кратчайших путей (Shortest Path First – SPF), используя алгоритм Дейкстры. Протокол поддерживает сложную топологическую базу данных. Если протоколы на базе вектора расстояний не содержат информацию об удаленных сетях, то протоколы на основе состояния канала поддерживают всю информацию об удаленных маршрутизаторах и их соединениях.

Состояние канала в этом протоколе подразумевает описание интерфейса (например, IP-адрес, маска, тип сети и т.п.) и его отношение с соседними маршрутизаторами. На основе выше указанных описаний интерфейсов формируется база данных состояния каналов.

База данных заполняется благодаря получению сообщений о состоянии канала (Link-State Advertisement – LSA), которые рассылаются регулярно или же сразу после изменения топологии сети, или при каких-либо изменениях на маршрутизаторах. Эти сообщения представляют собой небольшие пакеты. В LSA содержится информация о подключенных интерфейсах, метриках и других параметрах.

На основе полученных сообщений LSA маршрутизатор использует алгоритм SPF, который строит дерево кратчайших маршрутов. Алгоритм производит расчет над базой данных топологии сети, удаляя лишние ветви (ветви – все возможные пути). Полученные маршруты заносятся в таблицу маршрутизации.

Протокол OSPF – внутренний протокол маршрутизации и работает внутри одной автономной системы. Ее можно разбить на зоны (области), которые представляют собой логические разделы автономной системы.

Рассмотрим двухуровневую сетевую иерархию, в которой у всех маршрутизаторов свой принцип работы.

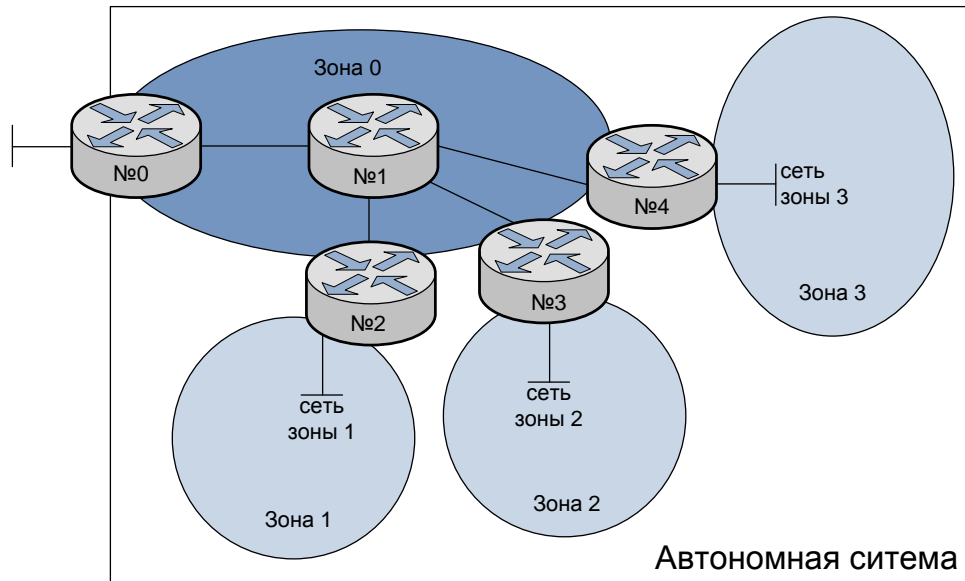


Рис. 2.2. Двухуровневая сетевая иерархия

На рис. 2.2 представлена одна автономная система, которая имеет один пограничный маршрутизатор (марш. №0), служащий для связи с внешней сетью (например, с другой автономной системой).

Автономная область включает в себя:

- ◆ зону 0 – область, отвечающую за соединение всех областей, иногда ее называют как магистральная область. Маршрутизатор №1 в этой области называют магистральным;
- ◆ зоны 1-3 – маршрутизаторы в этих областях называются не магистральные. Это маршрутизаторы, которые знают топологию области, в которых они находятся, и ведут базу данных состояний каналов только своих областей;
- ◆ на стыке зоны 0 и зон 1-3 находятся пограничные маршрутизаторы №2-4. Эти маршрутизаторы ведут базу данных состояний каналов всех областей, к которым они подключены;
- ◆ маршрутизатор №0 так же является пограничным, но уже для автономной системы.

OSPF выполняет следующие функции:

- ◆ формирует отношения с соседями;

- ◆ рассылает LSA для формирования на каждом маршрутизаторе базы данных;
- ◆ запускает SPF для расчёта наилучших маршрутов ко всем получателям;
- ◆ заполняет таблицы маршрутизации наилучшими маршрутами ко всем получателям.

Протокол OSPF формирует отношения с соседями следующим образом. Два маршрутизатора, т.е. маршрутизаторы-соседи, работающие по протоколу OSPF, должны «видеть» друг друга в сети, прежде чем будут обмениваться информацией. Этот процесс реализуется с помощью протокола Hello. Маршрутизаторы, в которых реализован протокол OSPF, со всех интерфейсов рассылают hello-пакеты (многоадресная рассылка – 224.0.0.6), которые содержат следующую информацию:

- ◆ Router ID – идентификатор маршрутизатора – 32-х битный уникальный номер для маршрутизатора. По умолчанию выбирается самый большой IP-адрес активного интерфейса. Эта идентификация важна для установления соседских отношений и устранения неполадок в них, а также для координации обмена данными маршрутизации;
- ◆ Hello и Dead интервалы – интервалы приветствия и простоя. Интервал приветствия определяет период отправки hello-пакетов маршрутизатором (по умолчанию – 10 секунд). Интервал простоя – это время, в течение которого маршрутизатор ожидает hello-пакет от соседнего маршрутизатора, прежде чем объявить его неисправным (по умолчанию интервал простоя в четыре раза превышает интервал приветствия). Эти интервалы должны быть одинаковыми на соседних маршрутизаторах, иначе соседские отношения не будут реализованы;
- ◆ Neighbors – соседи, в этом поле перечислены все соседние маршрутизаторы, с которыми установлено двусторонне соединение;
- ◆ Area ID – идентификатор области. Для взаимодействия между собой, маршрутизаторы должны находиться в одном сегменте и их интерфейсы

должны принадлежать к одной области OSPF в этом сегменте. Так же, соседние узлы должны использовать одинаковую подсеть и маску;

◆ Router priority – приоритет маршрутизатора – 8-ми битный номер, который необходим для выбора выделенного маршрутизатора (designated router, DR) и запасного выделенного маршрутизатора (backup designated router, BDR). Эти два типа маршрутизаторов необходимы для предотвращения проблемы рассылки копий LSA в сетях.

DR – управляет процессом рассылки LSA в сети. Информация об изменениях в сети рассылается всем маршрутизаторам от DR маршрутизатора, обнаружившего это изменение.

BDR – при выходе из строя DR, BDR становится DR и выполняет все его функции. DR и BDR также устанавливают отношения соседства и между собой. Роль DR (BDR) является свойством интерфейса, а не свойством всего маршрутизатора;

◆ DR и BDR ip-адреса – если известны;

◆ Authentication password – пароль для аутентификации, если аутентификация включена. Пароль на всех маршрутизаторах должен быть одинаковый;

◆ Stub area flag – флаг тупиковой области. Тупиковая область – особая область среды OSPF. Два маршрутизатора должны согласовать флаг тупиковой области в hello-пакетах.

Для формирования соседства поля hello-пакета – Hello interval, Dead interval, Area ID, Authentication Password и Stub Area Flag – должны совпадать.

Вывод:

Протокол OSPF имеет ряд преимуществ:

◆ маршруты, вычисленные протоколом OSPF, не могут быть циклическими;

◆ протокол обеспечивает масштабируемость для больших сетей;

◆ быстрая перенастройка при изменении топологии сети.

К недостатком же относится:

- ◆ иерархическая топология;
- ◆ отсутствует распределение нагрузки при неэквивалентных путях;
- ◆ метрика использует только стоимость маршрута.

2.3. Усовершенствованный протокол маршрутизации на базе вектора расстояний

Усовершенствованным протоколом маршрутизации на базе вектора расстояний является протокол EIGRP. Он был разработан компанией Cisco Systems, следовательно, часто используется на оборудовании этой компании.

Протокол обладает следующими качествами.

- ◆ Более быстрая сходимость в сравнении с другими протоколами на базе вектора расстояний, которая достигается благодаря алгоритму DUAL (Diffusing Update Algorithm). Алгоритм составляет таблицу топологий, в которой указано два лучших пути к сети назначения (основной и резервный). На обоих этих маршрутах не возникают петли.
- ◆ Снижение потребления полосы пропускания достигается за счет того, что при любых изменениях на сети, алгоритм DUAL отправляет только новые обновления, а не всю таблицу маршрутизации.
- ◆ Поддержка нескольких протоколов сетевого уровня (IP, IPX, AppleTalk).
- ◆ Бесклассовый протокол маршрутизации.
- ◆ Использование многоадресной (224.0.0.10) и одноадресной рассылки, вместо широковещательной. Благодаря этому обновления маршрутизации не затрагивают не нужные маршрутизаторы.

Принцип работы протокола EIGRP.

1. Протокол EIGRP сначала должен обнаружить своих соседей, для этого он использует протокол Hello, который в свою очередь рассылает hello-

пакеты (по умолчанию каждые 5 секунд). Для отправки пакетов используется многоадресная рассылка. Пока hello-пакеты приходят от соседа, маршрутизатор определяет его как функционирующий. Если в течение определенного времени (по умолчанию 15 секунд) от соседа не пришел hello-пакет, он считается недоступным.

2. После того, как соседи установлены, происходит обмен информацией о топологии сети. Сначала пересылается информация о полной топологии сети между маршрутизаторами. А далее, при изменении на сети, маршрутизаторы обмениваются следующими пакетами:

◆ Пакет обновления маршрутов (Update). В этих пакетах хранится информация об изменении маршрутов. Пакеты могут пересылаться по многоадресной или одноадресной рассылке.

◆ Пакет запросов (Query). Этот пакет необходим, когда маршрутизатор пересчитывает какой-либо маршрут, и у него нет резервного.

Маршрутизатор отправляет запрос соседям. Если у соседей есть маршрут, то они отвечают путем посылки пакета ответа на запрос (Reply). Если маршрута нет, то они отправляют запрос уже своим соседям.

◆ Помимо этого, при получении выше указанных пакетов (update, query, reply), ответно посылается пакеты подтверждения (Acknowledgment).

Для гарантированной доставки отправленных пакетов протокол EIGRP использует надежный транспортный протокол (Reliable Transport Protocol — RTP). Протокол повторно пересылает маршрутную информацию, если сообщение было потеряно. За счет использования протокола RTP уменьшается вероятность возникновения петель.

3. Далее происходит выбор наилучшего пути. Маршрутизаторы анализируют топологическую таблицу и выбирают из нее путь с наименьшей метрикой. Протокол считает ее с помощью весовых коэффициентов (по умолчанию $K1=1$; $K2=0$; $K3=1$; $K4=0$; $K5=0$), а также полосы пропускания (bandwidth) и задержки (delay).

Формула для расчета полосы пропускания выглядит так:

$$\text{bandwidth} = \frac{10000000}{\text{bandwidth(m)}} \cdot 256$$

bandwidth(m) – это минимальная пропускная способность канала на всем пути следования к сети назначения.

Формула для расчета задержки выглядит так:

$$\text{delay} = \text{delay (s)} \cdot 256$$

delay(s) – это суммарная задержка на всех маршрутизаторах по пути следования к сети назначения.

Полученные значения используются для подсчета метрики:

$$\text{Metric} = \left(K1 \cdot \text{bandwidth} + \frac{K2 \cdot \text{bandwidth}}{256 - \text{load}} + K3 \cdot \text{delay} \right) \cdot \frac{K5}{(\text{reliability} + K4)}$$

Если коэффициенты оставить по умолчанию, то:

$$\text{Metric} = K1 \cdot \text{bandwidth} + K3 \cdot \text{delay}$$

В таблице топологий находятся все известные маршрутизатору пути.

Приведем пример строки в таблице.

P 192.168.30.0/24, 1 successors, FD is 156160
via 10.0.0.1 (156160/128256), FastEthernet0/0

P – отвечает за состояние записи. Их два: Passive и Active. Первый значит, что маршрут используется и его пересчет не нужен. Состояние Active обозначает, что происходит пересчет маршрута. 192.168.30/24 IP-адрес сети и маска.

Successor – это маршрутизатор, через который проходит оптимальный маршрут в сеть.

FD (Feasible distance) – это метрика, которую будет использовать маршрутизатор. В данном случае она равна 156160.

10.0.0.1 – IP-адрес соседа. 128256 тоже метрика, называется она Advertised distance (AD) и показывает метрику маршрута в сеть для того маршрутизатора, который объявляет об этом маршруте.

Так же в таблице топологий могут встретиться следующие понятия:

FS (Feasible Successor) – это резервный маршрутизатор, через который можно попасть в некоторую сеть, если выйдет из строя Successor.

Feasible Condition (FC). Чтобы маршрутизатор мог стать резервным для какого-то маршрута, необходимо, чтобы значение Advertised distance (AD) для этого маршрутизатора было меньше, чем Feasible distance (FD) для основного маршрута.

Таким образом, маршрутизаторы, работающие на основе протокола EIGRP, поддерживают три таблицы.

- ◆ Таблица соседей, в которой указаны все соседи.
- ◆ Таблица топологии, в которой ведутся записи маршрутов до каждого места назначения, известные маршрутизатору.
- ◆ Таблица маршрутизации, куда заносятся лучшие маршруты из таблицы топологии.

Вывод:

К преимуществам протокола EIGRP относятся:


- ◆ быстрая сходимость в больших сетях;
- ◆ рнчительно меньшая загрузка каналов и CPU при работе протокола;
- ◆ Возможность балансировки трафика по неэквивалентным каналам.

Недостатком протокола EIGRP, является то что он ограничен количеством узлов равное 100 и является закрыты, то есть может быть реализован на оборудовании компании Cisco Systems.

2.4. Сравнительная характеристика внутренних протоколов маршрутизации

Таблица 2.1

Сравнение внутренних протоколов маршрутизации

| | RIPv2 | OSPF | EIGRP |
|--|---|--|---|
| Алгоритм | Вектор расстояний (Беллмана-Форда) | Состояние канала (Дейкстры) | Комбинированный (DUAL) |
| Обновление маршрутной информации | Вся таблица | Только изменения | Только изменения |
| Бесклассовый | да | да | да |
| Максимальное количество маршрутизаторов в сети | 15 | — | 255 |
| Открытый стандарт | да | да | нет |
| Метрика | Одна основная | Одна основная | Комбинированная |
| Планирование сети | нет | да (выбор зон) | нет |
| Балансировка нагрузки | нет | Одинаковые метрики | Разные метрики |
| Сложность конфигурации |  |  |  |

Можно сделать вывод (табл. 2.1): лучшими внутренними протоколами маршрутизации является OSPF и EIGRP. Особенно в применении к большим и сложным сетям. Но так же эти протоколы, не смотря на широкий спектр положительных качеств, имеют и свои минусы. Протокол OSPF имеет высокие требования к ресурсам маршрутизации из-за слишком сложного вычислительного расчета кратчайших путей. Хотя протокол EIGRP

выигрывает в этом плане, он все же является закрытым. Его реализация возможна только на оборудовании Cisco Systems. Но в наше время в сетях применяется оборудование разнообразных фирм. Поэтому в крупных сетях выгоднее применять протокол OSPF.

2.5. Внешний протокол маршрутизации

Внешним протоколом маршрутизации является протокол BGP (Border Gateway Protocol). На данный момент действует четвертая версия протокола, остальные считаются устаревшими. Протокол поддерживает бесклассовую адресацию.

Протокол функционирует поверх протокола транспортного уровня (TCP, порт 179) между автономными системами.

Как сказано выше, автономная система (Autonomous System, AS) – это совокупность сетей с общим управлением, то есть набор маршрутизаторов, имеющих единые правила маршрутизации. У каждой автономной системы есть свой номер. Организация, которая присваивает их, называется Internet Assigned Numbers Authority (IANA). Сам же номер представляет собой 16-битную комбинацию, то есть номер от 1 до 65535. Из них номера от 64512 до 65535 зарезервированы для частного пользования.

Маршрутизаторы, работающие на BGP, обмениваются информацией о сетевой доступности какой-либо сети, состоящей из атрибутов пути, что-то наподобие метрик для внутренних протоколов маршрутизации. Эти атрибуты включают в себя список всех автономных систем, которые необходимо пройти до сети назначения. А так же включают IP-адреса следующей автономной системы и обозначения, как сеть в конце пути была добавлена.

Протокол маршрутизации BGP соблюдает правила о маршрутизации только на уровне автономной системы. Вследствие чего маршрутизатор, работающий на этом протоколе, может передавать соседней автономной системе только те пути, которые использует сам.

К примеру, у нас есть несколько автономных систем (рис.2.3).

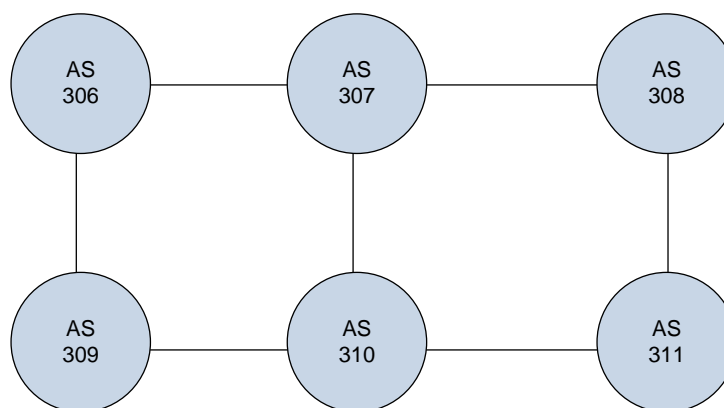


Рис. 2.3. Пример нескольких автономных систем

Необходимо отправить информацию из автономной системы 306 в автономную систему 311, и есть несколько вариантов путей:

- ◆ 306-307-308-311;
- ◆ 306-307-310-311;
- ◆ 306-309-310-311;
- ◆ 306-309-310-307-308-311.

Автономная система 306 не будет видеть все эти варианты, ей будут видны только те маршруты до системы 311, которые передадут автономные системы 307 и 309, причем наилучшие маршруты. К примеру, для маршрутизатора 307 лучший маршрут 307-308-311. Автономная система 306 при обращении к 307 будет видеть и отправлять трафик только по маршруту 306-307-308-311.

Автономная система 306 выберет наилучший вариант для отправки трафика к 307 или 309 автономной системе по правилам, принятым в своей автономной системе. Такой вид передачи данных, называется маршрутизация «шаг за шагом».

Принцип взаимодействия протокола BGP между автономными системами и внутри одной системы отличается. Если маршрутизаторы принадлежат одной автономной системе, то они работают по Internal BGP (IBGP), а если они находятся в разных АС, то работают по External BGP (EBGP).

В начале своей работы маршрутизаторы, работающие на основе протокола BGP, формируют TCP-соединения с каждым своим соседом, отправляя сообщение open. Это сообщение должно быть подтверждено сообщением keepalive. Потом устанавливается соединение. «Отношения» с соседом поддерживаются путем отправки сообщений keepalive с периодичностью в 60 секунд.

После установлений «отношений» маршрутизаторы обмениваются лучшими маршрутами, которые хранятся в их же таблицах маршрутизации. Далее каждый маршрутизатор собирает эти маршруты от каждого соседа и помещает их в базу данных топологии BGP. Лучшие маршруты для каждой сети выбираются из базы данных топологии процессом выбора маршрута BGP и записываются в таблицу маршрутизации. Внешние BGP маршруты имеют административное расстояние 20, а внутренние 200.

После составления таблицы маршрутизации маршрутизаторы обмениваются только обновлениями (сообщение Update) при изменениях на сети. Так же маршрутизаторы обмениваются сообщениями об ошибках и другой служебной информацией (notification messages).

Протокол BGP следует использовать в тех случаях, когда:

- ◆ автономная система является транзитной, через которую проходят пакеты, предназначенные для других автономных систем;
- ◆ автономная система имеет несколько подключений к другим автономным системам;
- ◆ политика маршрутизации между автономными системами должна быть управляемой, если надо повлиять на выбор пути для входящего и исходящего трафика.

Протокол BGP не следует использовать в тех случаях, когда:

- ◆ сеть имеет одно подключение к сети Интернет или к другой автономной системе;
- ◆ недостаточно ресурсов процессора и памяти на граничном маршрутизаторе для применения BGP маршрутизации;

- ◆ политика маршрутизации, применяемая в автономной системе, совместима с политикой в автономной системе провайдера.

3. Структура и характеристики маршрутизаторов компании Cisco Systems

Маршрутизатор – это устройство, которое определяет более приемлемый путь для передачи данных из одной сети в другую. Устройство работает на третьем уровне модели OSI/ISO (сетевом). Для определения лучшего пути маршрутизатор использует таблицы маршрутизации и протоколы, которые реализуют алгоритмы маршрутизации.

Рассмотрим компоненты маршрутизатора на примере маршрутизаторов компании Cisco Systems:

1. Оперативная память (ОЗУ, RAM). Ее основные функции – хранение таблиц маршрутизации, кеш протокола ARP (протокол канального уровня, предназначенный для определения соответствия между MAC и IP-адресом). Обеспечивает хранение пакетов на интерфейсах, пока они еще не начали обрабатываться центральным процессором (например, очередь захваченных пакетов). Обеспечивает временную и рабочую память для файлов конфигурации маршрутизатора при включенном питании. После выключения питания или перезагрузки содержимое оперативной памяти стирается.

2. Энергонезависимая память – NVRAM. Содержит резервную или старую копию файла конфигурации (startup-config). После выключения питания или перезагрузки содержимое памяти НЕ стирается.

3. Flash – память. Стираемая перепрограммируемая память. Содержит образ операционной системы. Позволяет обновлять ПО без извлечения чипа на процессоре.

4. Постоянное запоминающее устройство (ПЗУ, RAM). Содержит микрокод для начальной загрузки и обслуживания маршрутизатора, то есть

ПЗУ проверяет внутреннюю целостность маршрутизатора: процессор, память и т.д., какие присутствуют модули, определяет, в каком порядке и откуда загрузить операционную систему. Так же в ПЗУ хранится часть операционной системы Cisco, которая используется для восстановления файла образа операционной системы (например, если ее удалили с flash-памяти). Для обновления ПО в ПЗУ необходима замена чипа на системной плате устройства. После выключения питания или перезагрузки содержимое памяти НЕ стирается.

5. Интерфейс – сетевое соединение, через которые данные поступают и передаются с устройства. Размещается на сетевой плате или в отдельном модуле интерфейса.

6. Центральный процессор (ЦП). Процессор обеспечивает быструю обработку запросов приложений и служб безопасности.

При включении питания на маршрутизаторе Cisco выполняются следующие функции:

1. Проверяется работоспособность всех компонентов маршрутизатора. Так же проверяется состав оборудования. Проверка происходит на основе команд из ПЗУ.

2. Загрузка и выполнение кода загрузки (код используется для последующих действий). Код загрузки является микрокомандой ПЗУ.

3. Код загрузки определяет местонахождение запускаемого ПО операционной системы. Часто образ ПО храниться на flash-памяти.

4. Далее код загрузки распаковывает ПО в ОЗУ и запускается его. На некоторых маршрутизаторах ПО читается сразу с flash-памяти, без загрузки в ОЗУ, так как не хватает памяти ОЗУ.

5. Поиск конфигурации. По умолчанию (strtp-config) находится в энергозависимой памяти.

6. Загрузка конфигурации.

7. Запуск настроенного ПО операционной системы.

Основные функции маршрутизаторов:

1. Чтение заголовков пакетов сетевых протоколов, которые принимаются в буфер по каждому порту маршрутизатора;
2. Принятие решений о дальнейшем маршруте следования;
3. Подключение локальных сетей к глобальной сети.

3.1. Маршрутизатор Cisco 1811



В 1984 году была основана американская компания Cisco Systems, Inc., которая занимается разработкой и продажей сетевого оборудования. На рынке компанией представлен широкий спектр сетевого оборудования, и клиент имеет возможность закупить всё необходимое сетевое оборудование исключительно у Cisco Systems.

Помимо сетевого оборудования Cisco Systems создала многоуровневую разветвлённую систему сертификации инженеров по компьютерным сетям. Благодаря тому, что экзамены этой системы проверяют знание не только продукции Cisco, но и знание сетевых технологий, многие организации, даже работающие на сетевом оборудовании других фирм, признают ценность профессиональных сертификатов Cisco. В частности, сертификация на уровне эксперта (CCIE) является одной из самых известных и уважаемых в компьютерной индустрии.

Рассмотрим оборудование компании Cisco Systems – маршрутизатор с интегрированными сервисами Cisco серии 1800 - 1811. Маршрутизатор серии 1800 идеально подходят для сетей малых и средних компаний, а также для небольших филиалов предприятий.

Рассмотрим характеристики маршрутизаторов Cisco (табл. 3.1 – 3.7).

Технические характеристики маршрутизатора Cisco 1811

| Технические характеристики | Cisco 1811 |
|-------------------------------|---|
| WAN-интерфейсы | Два порта 10/100BASE-T |
| LAN-интерфейсы | Управляемый коммутатор на 8 портов 10/100BASE-T |
| Аналоговый модемный порт V.92 | Один аналоговый модемный порт |
| Порты USB 2.0 | 2 порта |
| Консольный порт | 1, скорость до 115.2 Кбит/с |
| AUX-порт | 1, скорость до 115.2 Кбит/с |
| ОЗУ (RAM) | Синхронный двухсторонний модуль памяти (DIMM) SDRAM (1 слот DIMM) по умолчанию 128 МБ максимум 384 МБ |
| Flash-память | Внешняя съемная flash-память формата Compact Flash, по умолчанию 32 МБ максимум 128 МБ |

WAN (Wide Area Network)-интерфейс – это внешний интерфейс маршрутизатора, используется для подключения к провайдеру или оборудованию доступа к провайдеру.

LAN (Local Area Network)-интерфейс – это интерфейс, отвечающий за выход в локальную сеть.

Консольный порт – порт, который используется для настройки оборудования с помощью управляющего терминала (консоли). В качестве консоли может выступать обычный компьютер.

AUX (auxiliary, вспомогательный) порт – необходим для подключения вспомогательного оборудования. После настройки подключения вспомогательное оборудование можно использовать как резервное.

Таблица 3.2

Физические параметры маршрутизатора Cisco 1811

| Параметры | Cisco 1811 |
|------------------------------|-------------------------------|
| Размер (ширина длина высота) | 32.36 см × 24.64 см × 4.80 см |
| Вес | 2.8 кг |
| Рабочая температура | от 0 до 40°C |
| Рабочая влажность | от 10 до 85% (без конденсата) |
| Температура хранения | от -25 до 65°C |
| Рабочая высота | до 3000 метров при 25°C |

Маршрутизатор Cisco 1811 может быть установлен на стену или в стандартную 19" стойку и займет 1 unit (44,45 мм).

Таблица 3.3

Обеспечение безопасности в маршрутизаторе Cisco 1811

| Сетевая безопасность | Cisco 1811 |
|--|--|
| Аппаратная поддержка шифрования | DES, 3DES, AES 128, AES 192, AES 256 |
| Поддержка IPSec-туннелей | 50 |
| Производительность IPSec VPN | 40 Мбит/с 3DES при размере пакета 1400 байт |
| Производительность межсетевого экрана Cisco IOS (Firewall) | 100 Мбит/с при размере пакета 1400 байт |

DES – симметричный алгоритм шифрования, разработанный в 1977 году. DES имеет блоки по 64 бита и 16 цикловую структуру сети Фейстеля. Для шифрования используется ключ длиной 56 бит.

3DES – алгоритм шифрования, разработанный на основе алгоритма DES, в 1978 году. Целью 3DES является устранение главного недостатка DES – малой длины ключа, который может быть взломан методом полного перебора ключа. Длина ключа 3DES – 168 бит.

AES 128, 192, 256 – симметричный алгоритм блочного шифрования имеет размер блока 128 бит, ключ 128, 192 или 256 бит.

VPN (Virtual Private Network) – это криптосистема, позволяющая защитить данные при передаче их по незащищенной сети (например, Интернет). VPN соединение состоит из канала типа точка-точка, также известного под названием туннель, и предоставляет прозрачный доступ к ресурсам сети, где пользователь может делать всё то, что он делает обычно независимо от того, насколько он удалён. По этой причине VPN приобрёл популярность среди работников офисов, которые работают удаленно, и нуждаются в совместном использовании ресурсов территориально разделённых сетей.

Стандарт IPSec был разработан для повышения безопасности протокола IP. Это достигается за счёт дополнительных протоколов, добавляющих к IP пакету собственные заголовки.

Так же защищенный доступ в сеть Интернет осуществляется благодаря динамическим управляемым спискам контроля доступа (Access Control List).

Таблица 3.4

Программное обеспечение маршрутизатора Cisco 1811

| Программное обеспечение | Cisco 1811 |
|------------------------------|---|
| Версия Cisco IOS | 12.4Т |
| Образ Cisco IOS по умолчанию | Продвинутые IP-сервисы (без голосовых служб) |

Программное обеспечение оборудования Cisco имеет следующее обозначения:

12.4 – показывают выпуск, после выпуска в скобках пишется цифра, которая показывает версию обновления.

Т – обозначает, что этот выпуск является не основным, а дополнением к основному выпуску, т.е. расширением.

Более старые выпуски часто работают более стабильно по сравнению с новыми, но предоставляют меньше возможностей.

Особенности маршрутизации в маршрутизаторе Cisco 1811

| Особенности маршрутизации | Cisco 1811 |
|--|--|
| Рекомендуемое количество пользователей | 50 |
| Поддержка технологий маршрутизации | Протокол динамической конфигурации узла (DHCP). Динамическая поддержка доменной системы имен. Сетевой протокол туннелирования канального уровня (L2TP). Технология трансляции порта адреса (PAT) скоростной пересылки Cisco (CEF). Асинхронный режим передачи данных по протоколу «точка-точка» (PPPoA). Протокол двухточечного соединения по сети Ethernet (PPPoE). Протокол связующего дерева (802.1d, STP). |
| Протоколы маршрутизации | BGP, EIGRP, OSPF, RIPv1, RIPv2 |
| Маршрутизируемые протоколы | IPv4, IPv6, IPX, IBM SNA, AppleTalk |

DHCP – сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

DNS – это протокол, при помощи которого символьные имена преобразуются в IP-адреса и наоборот.

L2TP – сетевой протокол туннелирования канального уровня в компьютерных сетях, использующийся для поддержки виртуальных частных сетей.

PAT – технология трансляции сетевого адреса в зависимости от TCP/UDP-порта получателя (частный случай NAT).

PPPoE – туннелирующий протокол, который позволяет настраивать (или инкапсулировать) IP или другие протоколы, которые настраиваются на PPP (Point to point protocol) через соединение Ethernet.

STP – сетевой протокол. Основной задачей STP является устранение петель в топологии произвольной сети Ethernet, в которой есть один или

более сетевых мостов, связанных избыточными соединениями. STP решает эту задачу, автоматически блокируя соединения, которые в данный момент для полной связности коммутаторов являются избыточными.

IPX – протокол сетевого уровня модели OSI в стеке протоколов SPX. Он предназначен для передачи датаграмм, являясь неориентированным на соединение (так же, как IP), и обеспечивает связь между NetWare-серверами и конечными станциями.

SNA – системная сетевая архитектура, разработанная компанией IBM в 1974 году. Представляет собой общее описание структуры, форматов, протоколов, используемых для передачи информации между программами IBM и оборудованием.

AppleTalk – стек протоколов, разработанный Apple Computer. Он был изначально включён в Macintosh (1984), сейчас компания отказалась от него в пользу TCP/IP.

Таблица 3.6

Особенности качества обслуживания в маршрутизаторе Cisco 1811

| Особенности QoS | Cisco 1811 |
|-----------------|---|
| Протоколы QoS | Weighted Fair Queuing (WFQ), Class-Based WFQ (CBWFQ), Weighted Random Early Detection (WRED), Committed Access Rate (CAR), Resource Reservation Protocol (RSVP), Network-Based Application Recognition (NBAR), Differentiated Services (DIFFSERV), Link fragmentation and interleaving (LFI), Low-Latency Queuing (LLQ) |

QoS (качество обслуживания) – способность сети обеспечить необходимый сервис заданному трафику в определенных технологических рамках.

Weighted Fair Queuing (WFQ) – взвешенная справедливая очередь. Механизм планирования пакетных потоков данных с различными приоритетами. Его задача – регулировать использования одного канала

передачи данных несколькими конкурирующими потоками. В данном случае под потоком понимается очередь пакетов данных.

Class-Based WFQ (CBWFQ) – соответствует механизму обслуживания очередей на основе классов. Весь трафик разбивается на 64 класса на основании следующих параметров: входной интерфейс, листы доступа (access list), протокол, значение DSCP (точка кода дифференцированных услуг), метка MPLS QoS.

Weighted Random Early Detection (WRED) – взвешенное произвольное раннее обнаружение. Алгоритм для управления переполнением очередей маршрутизаторов с возможностями предотвращения перегрузок.

Committed Access Rate (CAR) – механизм разработан для ограничения скорости.

Resource Reservation Protocol (RSVP) – протокол резервирования сетевых ресурсов (например, полосы пропускания для трафика).

Network-Based Application Recognition (NBAR) – распознавание сетевых приложений. Механизм, используемый в компьютерных сетях для распознавания потока данных по первому переданному пакету.

Differentiated Services (DIFFSERV) – дифференцированное обслуживание. Определяет обеспечение качества обслуживания на основе четко определенных компонентов, комбинируемых с целью предоставления требуемых услуг. DiffServ можно кратко охарактеризовать как приоритезацию трафика.

Link fragmentation and interleaving (LFI) – фрагментация и чередование в канале. Функция LFI операционной системы IOS Cisco сокращает задержку и уменьшает уровень «дребезжания» на медленных каналах путем разбиения (фрагментации) крупных дейтаграмм и чередования получившихся пакетов меньшего размера с пакетами с малой задержкой.

Low-Latency Queuing (LLQ) – очередность с низкой задержкой.

Технология PoE в маршрутизаторе Cisco 1811

| Особенности PoE | Cisco 1811 |
|--------------------------|--|
| Поддержка PoE | Поддержка на портах коммутатора 10/100 Ethernet с помощью опционального набора PoE |
| Стандарты PoE | IEEE 802.3af, Cisco Prestandard PoE |
| Внешний источник питания | Внешний источник питания на 80 Вт |

Power over Ethernet (PoE) — технология, позволяющая передавать удалённому устройству вместе с данными электрическую энергию через стандартную витую пару в сети Ethernet. Данная технология предназначена для IP-телефонии, точек доступа беспроводных сетей, IP-камер, сетевых концентраторов и других устройств, к которым нежелательно или невозможно проводить отдельный электрический кабель.

Рассмотрим более подробно маршрутизатор Cisco 1811 (рис. 3.1 – рис. 3.4, табл. 3.8).

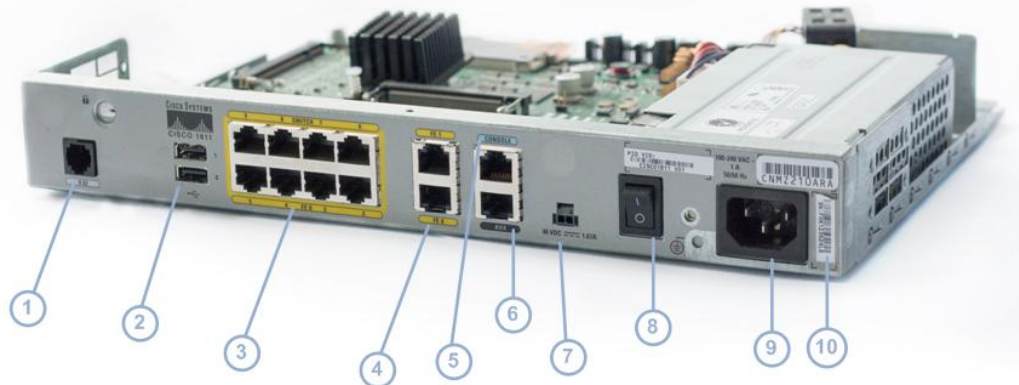


Рис. 3.1. Задняя панель маршрутизатора Cisco 1811

| №№ | Наименование |
|----|--|
| 1 | Порт модема V.92 |
| 2 | Порты USB 2.0 |
| 3 | Управляемый 8-портовый коммутатор |
| 4 | WAN-порты |
| 5 | Консольный порт |
| 6 | Вспомогательный (AUX) порт |
| 7 | POE разъем |
| 8 | Выключатель питания |
| 9 | Разъем питания |
| 10 | Серийный номер (серийный номер для маршрутизаторов Cisco серии 1800 состоит из 11-ти символов) |

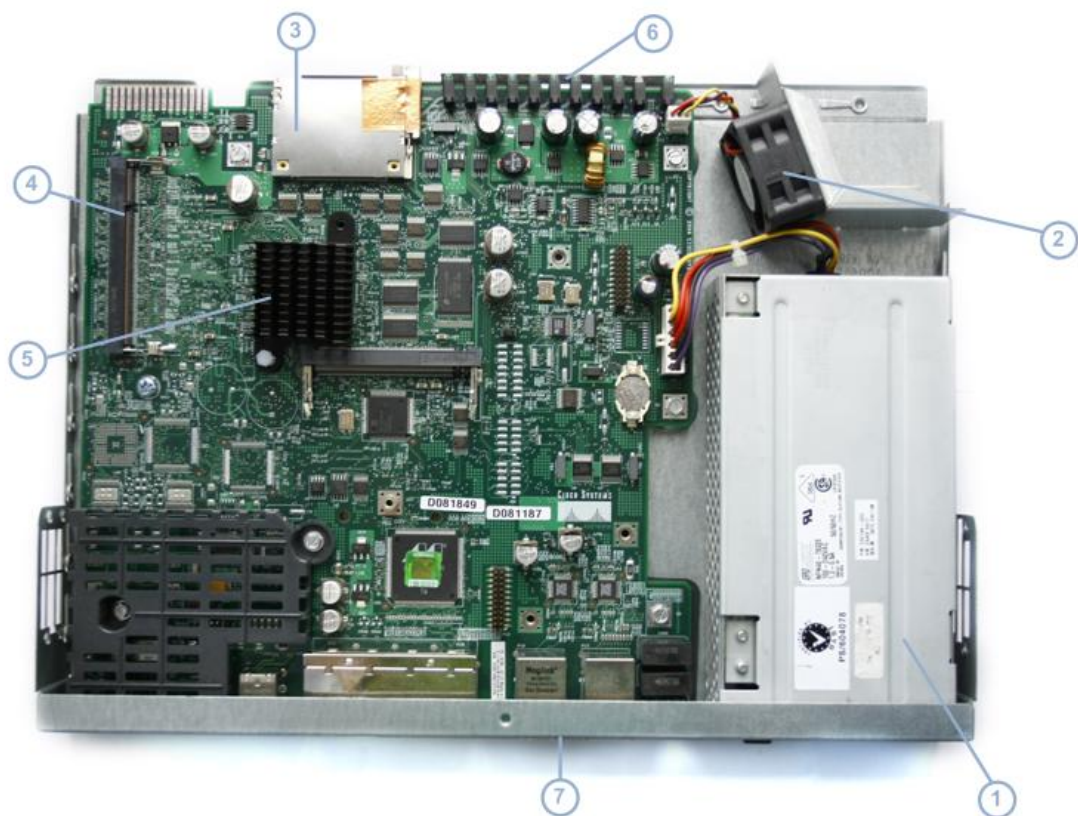


Рис. 3.2. Внутренние компоненты маршрутизатора Cisco 1811

| №№ | Наименование |
|----|------------------------------|
| 1 | Источник питания |
| 2 | Вентилятор |
| 3 | Слот для flash-памяти |
| 4 | Слот для RAM |
| 5 | Процессор |
| 6 | Светодиодные индикаторы |
| 7 | Задняя панель маршрутизатора |

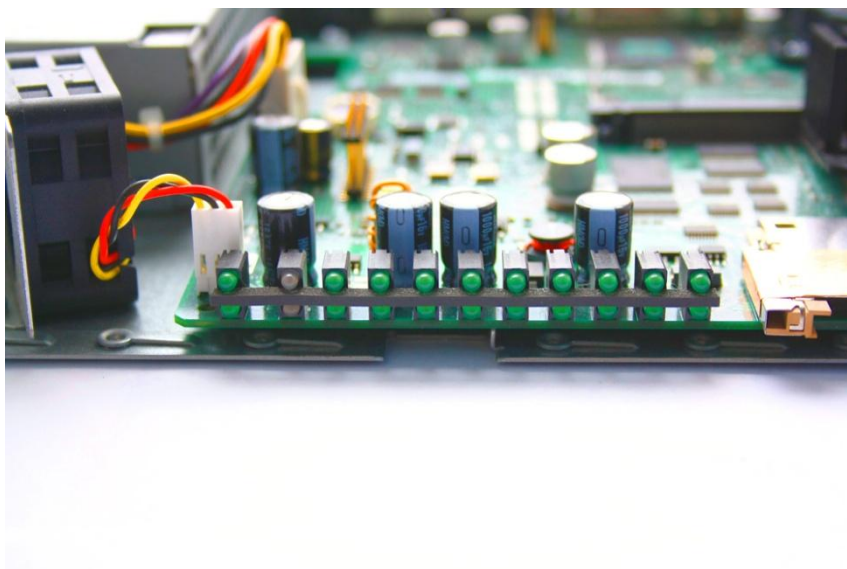


Рис. 3.3. Световые индикаторы маршрутизатора Cisco 1811



Рис. 3.4. Обозначение световых индикаторов маршрутизатора Cisco 1811

Таблица 3.8

Расшифровка световых индикаторов на маршрутизаторе Cisco 1811

| | | |
|------------------|------------------|---|
| SYS OK | Зеленый | Маршрутизатор успешно загрузился, и программное обеспечение работоспособно. Этот индикатор мигает при загрузке или в режиме мониторинга ROM. |
| POE | Зеленый / желтый | Зеленый цвет означает, что встроенный источник питания присутствует. Желтый цвет указывает на неисправность встроенного источника питания. |
| FE <port number> | Зеленый | Индикаторы показывают работоспособность портов Fast Ethernet WAN (2 порта FE № 0 и № 1) и портов коммутации (8 портов FE №№2-9). Зеленый цвет указывает, что интерфейс подключен. |

| | | |
|-------|---------|--|
| CD | Зеленый | Индикатор показывает, что модемное соединение установлено. |
| PPP | Зеленый | Индикатор показывает, что хотя бы одно PPP соединение установлено. |
| VPN | Зеленый | Индикатор показывает, что есть хотя бы один VPN туннель. |
| SPD 5 | Зеленый | Индикатор показывает подключение на высокой скорости (V.90/V.92). Если индикатор не горит, то установлена связь на низкой скорости (V.32/V.32b/V.34). Индикатор присутствует только на Cisco 1811. |
| BUSY | Зеленый | Мигание индикатора указывает на активность через модемную линию. Индикатор присутствует только на Cisco 1811 |
| CF | Зеленый | Индикатор указывает, что Flash память занята. Когда «горит» этот светодиод, память нельзя вынимать. |

3.2. Настройка маршрутизаторов Cisco

Маршрутизатор Cisco можно настраивать через интерфейс командной строки на консоли или удаленном терминале. Программное обеспечение Cisco IOS предоставляет интерпретатор, который называется EXEC (интерпретирует вводимые команды и выполняет соответствующие операции).

На маршрутизаторе можно работать в нескольких режимах.

Пользовательский режим. В этом режиме обычно проверяется состояние маршрутизатора. Для выхода используют команду `exit`.

RouterX>

Привилегированный режим. В этом режиме маршрутизатор настраивается. Для входа вводится команда `enable`, а так же пароль, если он есть. Для выхода используют команду `disable`.


```
RouterX>
RouterX>password
RouterX>enable
RouterX#
RouterX#disable
RouterX>
```

Для просмотра списка команд в каком-либо режиме можно ввести вопросительный знак. Так же Cisco IOS позволяет не вводить команды полностью, например, писать не полностью enable, а enab. Если нет другой команды с таким началом, маршрутизатор сразу поймет команду.

Существует режим глобальной конфигурации, который предоставляет доступ к специальным режимам конфигурации маршрутизатора (например, конфигурация интерфейса, линии, протокола и т.д.).

```
RouterX>
RouterX>enable
RouterX#configure terminal
RouterX(config)#
```

Пример настройки интерфейса на маршрутизаторе:

```
RouterX>
RouterX>enable
RouterX#configure terminal
RouterX(config)#interface fa 0/0 - настройка определенного интерфейса
RouterX(config-if)#ip address 192.168.1.1 255.255.255.0 - присваивание IP-адреса и маски
RouterX(config-if)#no shutdown - включение интерфейса
```

Для просмотра настройки на маршрутизаторе существует команда show interface.

При настройке локальной сети необходимо каждому компьютеру в этой сети присвоить IP-адрес. Это можно осуществить вручную, но чаще для этого применяют протокол DHCP. Сам протокол работает по принципу клиент-сервер. DHCP-сервер выделяет IP-адреса хостам автоматически (присваивает постоянный адрес клиенту), динамически (адрес выделяется на какой-то промежуток времени) или вручную.

```

RouterX(config)# service dhcp      - включение dhcp-сервера
RouterX(config)# ip dhcp pool LAN  - объявляем пул
RouterX(config-pool)#
network 192.168.20.0 255.255.255.0
RouterX(config-pool)# default-router  - указания шлюза по умолчанию
192.168.20.1

```

Исключение IP-адресов из предоставленного пула адресов.

```

RouterX(config-pool)# ip dhcp      - исключение одного адреса
excluded-addresses 192.168.0.2
RouterX(config-pool)# ip dhcp      - исключение диапазона адресов
excluded-addresses
192.168.0.128 192.168.0.255

```

Настройка маршрутизации.

Пример настройки статической маршрутизации.

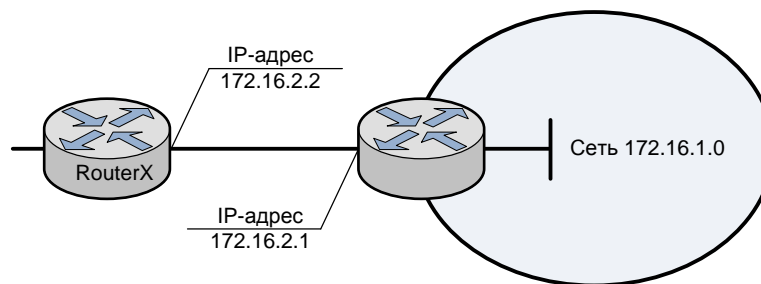


Рис. 3.5. Пример настройки статической маршрутизации

```

RouterX(config)#ip route      - Статический маршрут
172.16.1.0                    - адрес статического маршрута к сети назначения
255.255.255.0                - маска подсети
172.16.2.1                    - адрес след. перехода

```

Пример настройки протокола RIP (рис. 3.6)

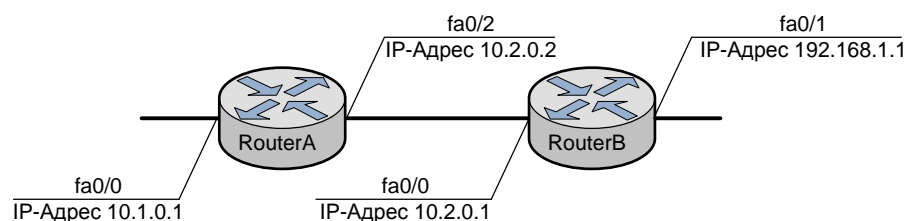


Рис. 3.6. Пример настройки протокола RIP

```
RouterB(config)#router rip
RouterB(config-router)#version 2
RouterB(config-router)#network 10.2.0.0
RouterB(config-router)#network 192.168.1.0
```

RIPv2 – бесклассовый протокол маршрутизации, но в команде `network` может быть указана только классическая сеть. Даже если указать сеть с маской, которая не соответствует классической, RIP автоматически преобразует её в классическую сеть. Команда `network` указывает только, на каких интерфейсах включить RIP, а фактическая сеть и маска будут взяты из настроек интерфейса.

Вывод таблицы маршрутизации производится командой `show ip route`. Сначала отображаются коды, указывающие на способ получения информации.

Коды: C – connected, S – static, R – RIP, M – mobile, B – BGP, D – EIGRP, EX – EIGRP external (внешний), O – OSPF, IA – OSPF inter area (межобластной), N1 – OSPF NSSA external type 1 (внешний маршрут NSSA первого типа), N2 – OSPF NSSA external type 2 (внешний маршрут NSSA второго типа), E1 – OSPF external type 1, E2 – OSPF external type 2, i – IS-IS, su – IS-IS summary, L1 – IS-IS level-1, L2 – IS-IS level-2, ia – IS-IS inter area, * – candidate default (указывает последний, использованный путь для пересылки маршрутов), U – per-user static route (пользовательский статический маршрут), o – ODR (маршрут по требованию), P – periodic downloaded static route (периодически загружаемый статический маршрут).

Далее отображается сама таблица маршрутизации. В ней указываются все записи обо всех известных сетях, которые так же помечаются буквой кода. В записях с удаленной сетью, так же есть поля с указанием административного расстояния источника данных, метрики маршрута, адреса следующего перехода, времени, прошедшего с момента последнего обновления, а так же интерфейса, через который можно получить доступ к удаленной сети.

```
RouterB#show ip route
```

```
...  
R 10.1.0.0 [120/1] via 10.2.0.2 00:00:08, fa0/2  
↓ ↓ ↓ ↓ ↓ ↓  
RIP админ.раст./Метрика время с последнего обновления  
адрес удаленной сети адрес маршрута след. перехода
```

Пример настройки протокола OSPF.

```
RouterB(config)#router ospf 101  
RouterB(config-router)#network 10.2.0.1 0.0.0.0 area 0  
RouterB(config-router)#network 192.168.1.1 0.0.0.0 area 1
```

101 – идентификатор процесса маршрутизации, случайный номер.

10.2.0.1 – адрес интерфейса (так же может быть записан адрес сети или подсети)

0.0.0.0 – wildcard mask, обратная маска, которая показывает, какая часть (сколько бит) IP-адреса могут меняться. 0.0.0.0 – все биты фиксированы.

Area 0 – идентификатор области.

```
RouterB(config-router)#ip ospf cost cost
```

Настройка стоимости (метрика от 1 до 65535) маршрута (для данного интерфейса) маршрутизации. При отсутствии данной команды стоимость для данного интерфейса рассчитывается исходя из его пропускной способности.

Пример настройки протокола EIGRP (рис. 3.7).

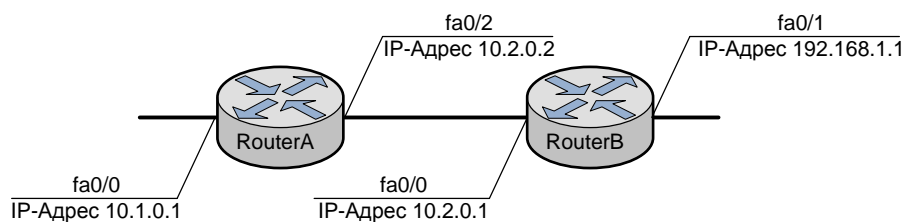


Рис. 3.7. Пример настройки протокола EIGRP

```
RouterB(config)#router eigrp 100  
RouterB(config-router)#network 10.2.0.0  
RouterB(config-router)#network 192.168.1.0
```

100 – номер автономной системы. Номер автономной системы может быть зарегистрированным или частным. Все маршрутизаторы, работающие в одной автономной системе, должны использовать один номер автономной системы для обмена информацией.

По умолчанию EIGRP выполняет балансировку нагрузки между 4 маршрутами с одинаковой метрикой. Для того, чтобы отключить балансировку нагрузки, надо установить количество маршрутов равным 1. Изменение количества маршрутов, между которыми выполняется балансировка нагрузки:

```
RouterX(config-router)# maximum-paths 6
```

В зависимости от того, как маршрутизатор обрабатывает пакет балансировка нагрузки, выполняется per-packet (для каждого пакета) или per-destination (для каждого адресата).

Балансировка нагрузки по адресату назначения означает, что маршрутизатор распределяет пакеты на основе адреса назначения. При наличии двух путей доступа к одной сети, все пакеты для назначения 1 в этой сети пересылаются по первому пути, а все пакеты для назначения 2 в этой сети пересылаются по второму пути и т.д. При этом сохраняется порядок пакетов с потенциально неравномерным использованием каналов.

Балансировка нагрузки по пакетам означает, что маршрутизатор отправляет один пакет для назначения 1 по первому пути, а второй пакет для этого же назначения 1 по второму пути и т.д. Балансировка нагрузки по пакетам гарантирует равномерное распределение нагрузки между всеми каналами. Однако существует вероятность нарушения порядка следования пакетов, когда они достигают адресата назначения, из-за возможного существования дифференциальной задержки в сети.

EIGRP может распределять трафик между несколькими маршрутами с различной метрикой. Это регулируется заданием variance:

```
RouterX(config-router)# variance 2
```

Значение `variance` может быть от 1 до 128. Это множитель, на который будет умножаться `FD` текущего маршрута для определения `feasible` маршрутов.

Балансировка нагрузки может выполняться только между `feasible routes`, когда они попадут в таблицу маршрутизации.

Маршрут считается `feasible` при выполнении двух условий:

- `FD` лучшего маршрута больше чем `AD`, которое анонсирует соседний маршрутизатор. Другими словами, следующий маршрутизатор на пути должен быть ближе к `destination`, чем локальный маршрутизатор (для предотвращения создания петель маршрутизации);

- `FD` лучшего маршрута, умноженное на `variance`, должно быть больше, чем `FD` альтернативного маршрута.

Пример настройки протокола BGP (рис. 3.8).

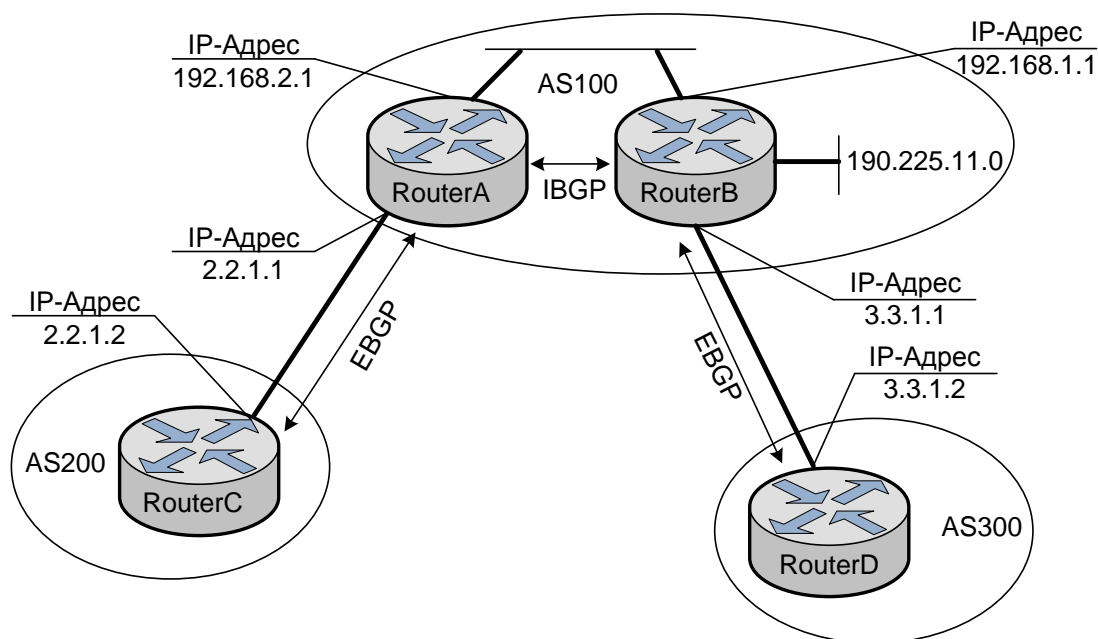


Рис. 3.8. Пример настройки протокола BGP

```
RouterA(config)#router bgp 100
RouterA(config-router)#neighbor 2.2.1.2 remote-as 200
RouterA(config-router)#neighbor 192.188.1.1 remote-as 100
```

Для проверки, работают ли (доступны ли) IBGP-соседи, можно использовать команду:

```
RouterA# show ip bgp neighbors
```

Loopback interfaces часто используются IBGP-соседями. Преимущество использования loopback interfaces заключается в том, что настройка маршрутизации перестает быть связана с IP-адресом физического интерфейса. И даже если физический интерфейс будет отключен, то это никоим образом не повлияет на маршрутизацию между автономными системами, т.к. он будет использовать некий псевдо IP-адрес интерфейса loopback, как идентифицирующий данный роутер.

Маршрутизаторы А и В обмениваются таблицами маршрутизации по IBGP в пределах AS 100. Если при конфигурировании маршрутизатора В в качестве IP-адреса соседа мы укажем IP-адрес одного из его интерфейсов, то все, конечно же, будет работать. До тех пор, пока этот интерфейс не «упадет». Если это случится, то обмен таблицами маршрутизации, равно как и трафиком, прекратится в результате того, что станет невозможным установить TCP-соединение между маршрутизаторами А и В.

```
RouterB(config)#router bgp 100
RouterB(config-router)#neighbor 150.212.1.1 remote-as 100

RouterA(config)#loopback interface 0
RouterA(config-if)#ip address 150.212.1.1 255.255.0.0
RouterA(config)#router bgp 100
RouterA(config-router)#neighbor 190.225.11.1 remote-as 100
RouterA(config-router)#neighbor 190.225.11.1 update-source
loopback 0
```

loopback интерфейсы редко используются на маршрутизаторах, которые работают по EBGP, поскольку они и так зависят от непосредственного физического соединения друг с другом.

4. Рекомендации по выбору маршрутизаторов

4.1. Производители маршрутизаторов

Существует несколько версий о том, кто изобрел маршрутизатор.

По одной из версий, маршрутизаторы были предложены компанией Cisco Systems. В начале 1980-х годов два сотрудника Стенфордского университета – Сэнди Лернер и Леонард Босак – решили провести исследование на тему, как пользователям одного сегмента сети получить доступ к ресурсам, расположенным в другом сегменте? Ответом стала необходимость организации маршрутизации. Через два года они разработали свой первый маршрутизатор и начали прокладывать сеть в кампусе Стенфорда. Их труд и новые идеи принесли результаты. Они успешно объединили оборудование Стенфордского университета при помощи своих маршрутизаторов, создав одну из крупнейших на то время университетских вычислительных сетей. Лернер и Босак обратились к руководству университета с предложением коммерческого использования их продукта, но университет отказался от продвижения новой технологии. В итоге им пришлось выходить на рынок самостоятельно. Была основана компания Cisco Systems, которая представила свой первый маршрутизатор широкой публике в октябре 1984 года.

Есть версия, что первый маршрутизатор был изобретен компанией Bridge Communications в 1983 году. Ее основала супружеская пара Джуди Эстрин и Билл Каррико, которая заявляла, что именно их компания является основными проводниками идеи о маршрутизации.

В конце 80-х годов компания Bridge Communications была приобретена компанией 3Com. Однако 3Com не захотела ориентировать свой бизнес на производство маршрутизаторов и бросила основные ресурсы на разработку и производство сетевых карт. Это был весьма серьезный просчет компании 3Com. Компания Cisco стала лидером.

Есть еще версия, что первый маршрутизатор изобрел Билл Ягер. Вот что он рассказывал.

В январе 1980 года руководитель Билла Ягера попросил его придумать что-нибудь для того, чтобы связать департамент электротехники, отдел теории вычислительных машин и медицинский центр. Все эти учреждения необходимо было соединить, потому что люди устали бегать туда и обратно с магнитными лентами. После некоторых раздумий Билл пришел к выводу, что то, в чем он нуждался для решения этой задачи, было операционной системой. И он начал разработку сетевой операционной системы и программы маршрутизации на PDP11/05. Необходим был очень компактный код и определение разумного числа входных буферов, поскольку это был бездисковый компьютер с ОЗУ объемом 56 КВ. Практически все лето было потрачено на надежность и оптимизацию алгоритма маршрутизации пакетов. Три последующих месяца ушло на сборку системы. Через шесть месяцев первый маршрутизатор был установлен в телефонном шкафу в здании, расположенном посередине между отделом теории вычислительных машин и медицинским центром.

Что же касается протоколов, то сначала маршрутизировались только пакеты PUP (Parc Universal Packet). Однако в конце 1981 года Биллу было указано, что все переходят на IP и необходимо это учесть. Тогда и добавился IP-маршрутизатор, но без поддержки протокола разрешения адресов ARP. Затем была создана более совершенная модель маршрутизатора на базе платы с процессором Motorola 68000, сконструированной Энди Бехтольшаймом, будущим основателем Sun Microsystems. По-настоящему же серьезная разработка завершилась к 1985 году.

Весной 1985 года Леонард Босак и его компаньон пришли в офис, где работал Билл Ягер. Они хотели узнать, могут ли получить доступ к исходным кодам ПО маршрутизатора. На вопрос Билла о причинах их интереса, они ответили, что хотят усовершенствовать его и добавить ряд новых функций. Билл сказал, что это замечательно, поскольку он уже не может дорабатывать

этот проект, так как занят другими исследованиями, и дал им пароль. Он в то время ничего не знал об образовании в 1984 г. компании Cisco.

Год спустя модифицированная версия кода Билла Ягера стала стандартом для маршрутизаторов в Стэнфорде. О компании Cisco все узнали в 1986 году. Именно тогда компания выпустила на рынок свой первый маршрутизатор, который назывался Advanced Gateway Server. Он был разработан на базе процессора Motorola 68000 10 MHz, имел 1 МВ памяти, восемь слотов для интерфейсных карт, к которым можно было подключить Ethernet, ARPAnet и низкоскоростные последовательные каналы. В первый год производительность маршрутизатора составляла 200 пакетов в секунду.

В конце 80-х – начале 90-х, на начальном этапе своего существования, маршрутизаторы в основном применялись для соединения сегментов локальных вычислительных сетей (ЛВС). Первые маршрутизаторы строились на базе относительно низкоскоростных компьютеров с очень ограниченным объемом памяти.

С середины 90-х годов корпоративные сети стали строиться по принципу: «использовать коммутаторы везде, где можно, маршрутизаторы – только там, где необходимо». Во многих ЛВС маршрутизаторы были отодвинуты на границу с глобальными сетями, но при этом они не стали менее важными.

Со временем функциональность корпоративных маршрутизаторов расширялась. Усложнение маршрутизаторов совпало по времени со стремительным ростом сети Интернет, выдвинувшей ряд принципиально новых требований. Оборудование для новых IP-сетей должно было поддерживать уже не сотни и тысячи, а миллионы пользователей, обеспечивая при этом для новых приложений реального времени гарантированное значение таких важных характеристик, как задержка, ее вариация (джиттер), процент потери пакетов. К тому же от нового оборудования требовалось быть максимально компактным и минимально

энергоемким, чтобы экономить такие ресурсы, как пространство и электричество в телекоммуникационных узлах.

На сегодняшний день рынок маршрутизаторов развивается довольно динамично. И на этом рынке присутствуют как лидирующие компании, так и второго плана. Так же есть и небольшие компании, чья продукция предназначена для совсем уж небольших сетей.

Различают три класса маршрутизаторов.

Маршрутизаторы первого (операторского) класса помогают объединять сети предприятий. Такой класс способен поддерживать огромное количество протоколов и интерфейсов. В основном эти маршрутизаторы предназначены для сетей операторов связи и сервис-провайдеров. Оборудование этого класса характеризуется очень высокой производительностью, наличием мощных средств обеспечения отказоустойчивости (как отдельного узла, так и сети в целом) и поддержкой таких ключевых протоколов, как BGP и MPLS (многопротокольная коммутация по меткам). Магистральные устройства этого класса имеют суперскоростные интерфейсы, вплоть до уровней OC-192/STM-64 (10 Гбит/с) и OC-768/STM-256 (40 Гбит/с).

С помощью маршрутизаторов второго класса формируются сетевые объединения в масштабе одного предприятия, то есть корпоративные сети. Во многих корпоративных сетях маршрутизаторы похожи на маршрутизаторы первого класса, но только производительность их (в части маршрутизации) ниже, интерфейсы менее скоростные, средства отказоустойчивости скромнее. Как правило, акцент в данном классе сделан на поддержку несколько иных протоколов маршрутизации: вместо BGP чаще используется RIP или OSPF. Зато функциональность корпоративных маршрутизаторов зачастую значительно шире. В частности, многие такие маршрутизаторы уже давно поддерживают широкий набор разнообразных телефонных стыков (FXS, FXO, E&M, BRI, PRI), а в настоящий момент становятся полнофункциональными телефонными станциями или «интеллектуальными» выносами центральной УАТС.

Третий класс маршрутизаторов предназначен для связи небольших офисов с сетью предприятия. Здесь функционируют маршрутизаторы (маршрутизаторы SOHO), ориентированные на домашних пользователей и небольшие компании. Их называют широкополосными Интернет-шлюзами. Маршрутизаторы имеют фиксированную архитектуру: набор жестко встроенных интерфейсов, таких, как Ethernet, xDSL, ISDN и др. Они просты в настройке, поскольку большинство функций у них предконфигурированы, а настройка остальных осуществляется с помощью простого графического интерфейса. Такие устройства являются относительно недорогими. Зачастую содержат дополнительные функциональные модули, необходимые в работе небольших офисов: серверы печати, точки беспроводного доступа, коммутаторы на четыре-восемь портов и т.д.

В последнее время конкуренция на рынке телекоммуникаций ощутимо ужесточилась. Лидирующей компанией остается Cisco Systems, но ее заметно теснят такие компании как Avaya, Juniper Networks, HP. В 2012 году Джон Чемберс (John Chambers), исполнительный директор Cisco Systems, высказался в одном интервью, что больше всего его беспокоит компания Huawei.



Juniper Networks – американская компания, занимающаяся производством высококачественного сетевого оборудования. Основана в 1996 году.

Маршрутизаторы Juniper предназначены для использования в тех случаях, когда требуется исключительно высокая производительность, а также надежность и доступность.

Это идеальное решение для центральных офисов крупных компаний, нескольких сетей внутри предприятия, а также центров обработки данных.

Компания Juniper с момента создания была нацелена на разработку маршрутизаторов первого класса. Компания является одним из основных конкурентов компании Cisco Systems.

У оборудования компании Juniper своя операционная система JunOS. Она построена на принципах модульности: каждый процесс выполняется в своем защищенном адресном пространстве, и его сбой не влияет на функционирование другого процесса, следовательно, не влечет за собой нарушения работы системы в целом. Организация операционной системы в виде ряда независимых модулей позволяет добавлять новую функциональность без остановки системы, а также дает возможность задействовать только необходимый набор функций, эффективно используя ресурсы оперативной памяти.

Что касается аппаратной части маршрутизаторов Juniper, то она реализована на принципиально ином подходе, чем оборудование, предлагаемое конкурентами. Основу аппаратной части маршрутизаторов составляют две подсистемы – одна из них отвечает за продвижение пакетов (forwarding), а другая – за маршрутизацию (routing). Первая реализована на основе специализированных быстродействующих интегральных микросхем ASIC, на которые возложена самая тяжелая работа – пересылка основного потока данных, а вторая выполнена на базе процессора Intel и участвует лишь в определении маршрута, по которому эти данные необходимо направлять.

Серии маршрутизаторов Juniper Networks.

Маршрутизаторы Juniper серии VX используются для транзитных соединений. Позволяют решить проблемы, связанные с текущими эксплуатационными расходами и пропускной способностью сети, а также полностью поддерживают возможность миграции на технологии 4G.

Маршрутизаторы серии J предоставляют набор гибких интерфейсов, обеспечивающих надежную и безопасную маршрутизацию подключений к удаленным подразделениям, филиалам и региональным офисам.

M-серия маршрутизаторов компании Juniper Networks предназначена для использования в ситуациях, когда требуется исключительно высокая производительность, надежность и доступность. Это идеальное решение для

центральных офисов крупных компаний, кампусных сетей и центров обработки данных.

Ethernet-маршрутизаторы Juniper серии MX обеспечивают маршрутизацию и коммутацию с высокой плотностью портов и предназначены для сетей поставщиков услуг и крупных предприятий. Такие устройства находят применение в Ethernet-сетях высокой плотности, на агрегационных и магистральных уровнях в центрах обработки данных, а также в периферийных Ethernet-сетях.

Маршрутизаторы Juniper серии T являются ведущими решениями среди платформ для опорных сетей IP/MPLS и способны обеспечить скорость передачи данных от 320 Гбит/с до 1,6 Тбит/с в одном шасси и до 25 Тбит/с в системах с несколькими шасси.



Huawei Technologies Co. Ltd. – одна из крупнейших китайских компаний в сфере телекоммуникаций, основана в 1988 году. Компания Huawei стремится занять ведущие позиции практически во всех сегментах телекоммуникационного рынка, и маршрутизаторы здесь не исключение, является конкурентов Cisco Systems.

В интервью, сделанном в начале апреля 2012 года, исполнительный директор Cisco назвал китайского гиганта вызывающим опасения конкурентом на длинной дистанции, который не всегда играет по правилам. В 2011 году Huawei развернула активную деятельность на территории США и теперь претендует на часть доли Cisco не только на телекоммуникационном, но и корпоративном ИТ-рынке.

Исполнительный директор Cisco не посчитал нужным вдаваться в детали и разьяснять, какие именно правила нарушает Huawei, уточнив только, что речь идет о правах на интеллектуальную собственность.

Официальная реакция Huawei на высказывания Cisco последовала незамедлительно. Уильям Пламмер, вице-президент по внешним связям, назвал комментарии Cisco «неуместными». Huawei располагает 50 тыс. собственных патентов, и поэтому всегда с уважением относилась к защите прав на интеллектуальную собственность, равно как и отстаивала собственные права. По аналогии с Cisco она сумела снискать доверие заказчиков к своей продукции на более чем 140 рынках мира. Пламмер добавил, что среди заказчиков его компании 500 операторов связи.

Оборудование HUAWEI, построенное на базе операционной системы VRP, имеет интерфейс командной строки, как и у Cisco. Принцип работы остается тем же самым, меняется только синтаксис.

На рынке компанией Huawei представлены маршрутизаторы разного уровня – от небольших и экономичных SOHO-маршрутизаторов до высокопроизводительных магистральных маршрутизаторов операторского класса.

Серии маршрутизаторов Huawei.

Маршрутизаторы серии NE – высокопроизводительное оборудование для построения IP/MPLS магистральных сетей сервис-провайдеров, операторов мобильной и фиксированной связи.

Маршрутизаторы серии AR – предназначены для второго и первого классов небольших операторов и организаций.



Основанная в 1986 году в Парке Шинчу (Тайвань) компания D-Link является всемирно известным разработчиком и производителем сетевого и телекоммуникационного оборудования и предлагает широкий набор решений для домашних пользователей и корпоративного сегмента.

Согласно исследованиям, проведенным аналитической компанией Synergy Research Group, D-Link занимает первое место в мире по объему продаж оборудования в потребительском секторе рынка сетевого оборудования.

D-Link предлагает законченные сетевые и коммуникационные решения для построения «цифрового дома», предприятий малого и среднего бизнеса, сетей масштаба рабочих групп и предприятий и провайдеров услуг Интернет. Кроме этого, компания производит полный спектр оборудования для создания проводных и беспроводных сетей, широкополосного доступа, IP-телефонии и мультимедиа-устройств.

D-Link обладает патентами и авторскими правами на ряд уникальных разработок, в числе которых компьютерные чипы ASIC, технологический дизайн, программное обеспечение и прочая интеллектуальная собственность.

Применение инновационных методик и высокие требования к качеству позволяют компании выпускать высокопроизводительные устройства, базирующиеся на современных стандартах. Идя навстречу требованиям потребителей, компания предлагает наилучшие цены на рынке систем связи в сочетании с высоким качеством устройств.



ZyXEL Communications Corp. – крупная тайваньская компания. Основана в 1989 году, один из лидеров на рынке оборудования для доступа в Интернет.

Сегодня приоритетные направления бизнеса компании – это абонентское и операторское оборудование для широкополосного доступа по технологиям xDSL, Metro Ethernet, LTE и PON, системы сетевой безопасности и профессиональные беспроводные сети.

Выводы:

На данный момент на рынке достаточно компаний, производящих телекоммуникационное оборудование, а том числе и маршрутизаторы.

Некоторые компании ориентируются на производство оборудования на определенный сегмент сети. Например, компания Cisco Systems предоставляет большой выбор продукции на любой сегмент сети, будь то малый офис или сеть операторского класса. Оборудование компании D-Link ориентировано на домашние и корпоративные сети.

Таблица 4.1

Возможности компаний по производству маршрутизаторов

| | Первый класс | Второй класс | Третий класс |
|---------------------|--------------|--------------|--------------|
| Cisco Systems | + | + | + |
| Juniper Networks | + | + | - |
| Huawei Technologies | + | + | + |
| D-Link | - | + | + |
| ZyXEL | - | + | + |

Операторам и сервис-провайдерам есть из чего выбирать. На рынке мощных маршрутизаторов сегодня представлена не только продукция компании Cisco Systems, но и продукция ее конкурентов – Huawei, Juniper, оборудование которых тоже выглядит весьма достойно.

Если же говорить о маршрутизаторах для корпоративных сетей, то число компаний на этом рынке еще больше. Помимо упомянутых выше компаний, большую активность проявляют фирмы D-Link и ZyXEL.

Конечно, есть и еще компании, производящие маршрутизаторы, такие как ASUS, HP, NETGEAR, Nortel и др.

Если сравнивать три фирмы операторского класса, то определить лидера среди них сложно. Многие выбирают оборудование Cisco, так как компания себя хорошо зарекомендовала на рынке. Компания разрабатывает сетевые решения в зависимости от того, что необходимо клиенту, т.е. сеть строится в зависимости от тех услуг, которые будут в ней реализованы.

Часто говорят, что другие компании при разработке сетевых решений предлагают только основной функционал, и для получения большего числа функций цена возрастает.

В то же время при всей своей практически идеальной репутации, решения от компании Cisco Systems многим просто не по карману, стоимость оборудования не маленькая. Другая сторона вопроса, чтобы связать несколько офисов, которые находятся в паре шагов друг от друга, продукция Cisco Systems может быть не нужна. Она попросту не оправдывает своих возможностей. Также после покупки оборудования далеко не каждый системный администратор обладает необходимой квалификацией, чтобы самостоятельно произвести грамотную настройку маршрутизатора Cisco, а услуги стороннего специалиста будут стоить дорого.

И, тем не менее, в средних и крупных компаниях, государственном секторе, а также везде, где требуется качественная и безотказная работа, сети используют оборудование Cisco, хоть это и весьма недешевое решение.

В России оборудование компании Cisco Systems установлено у многих операторов. Пользуется популярностью и оборудование других фирм. Так, например, в 2011 году компания ОАО «ВымпелКом» (Билайн) заявила о замене оборудования Cisco на Huawei Technologies.

4.2. Серии маршрутизаторов Cisco

Рассмотрим, какие линейки оборудования представлены на рынке в данный момент.

Для филиалов:

Маршрутизатор Cisco ISR серии 800



- ◆ настольный;
- ◆ безопасная передача данных, а также безопасное подключение к глобальной сети;
- ◆ подходит для сотрудников, работающих в

небольших офисах и в режиме удаленного доступа;

- ◆ возможность заказа с устанавливаемой на заводе точкой доступа 802.11n.

Маршрутизатор Cisco ISR серии 1900



- ◆ настольный;
- ◆ оптимальное решение для небольших офисов;
- ◆ экономичное решение начального уровня с высоким уровнем защищенности, предназначенное для подключения внутренней сети к глобальной сети;
- ◆ скорость коммутации глобальной сети до 25 Мбит/с.

Маршрутизатор Cisco ISR серии 2900



- ◆ модульный корпус. Занимает 1-2 Unit;
- ◆ скорость коммутации в глобальной сети до 75 Мбит/с;
- ◆ предоставляет интерактивные сервисы для работы с мультимедиа и средства виртуализации сервисов;
- ◆ является оптимальным решением для создания средних по размеру инфраструктур.

Маршрутизатор Cisco ISR серии 3900



- ◆ модульный корпус. Занимает 3 Unit;
- ◆ модернизируемая системная плата, скорость коммутации глобальной сети до 350 Мбит/с;
- ◆ предоставляет масштабируемые интерактивные сервисы для работы с мультимедиа, в том числе видеоконференцсвязи (TelePresence);

❖ является оптимальным решением для создания сложных ИТ-систем, для которых требуются непрерывность функционирования и возможности совместной работы.

Таблица 4.2

Сравнение моделей серии Cisco для филиалов

| | | 3945 | 2951 | 1941 | 1921 |
|---|---|--------------------|--------------------|--------------------|--------------------|
| Форма | | 3 Unit | 2 Unit | 2 Unit | 1 Unit |
| Комплексная WAN портов | | 3 Gigabit Ethernet | 3 Gigabit Ethernet | 2 Gigabit Ethernet | 2 Gigabit Ethernet |
| Расширение | Интерфейсные разъемы (Enhanced высокоскоростных WAN интерфейса карты [EHWIC]) | 4 | 4 | 2 | 2 |
| | Сервис-модуль Слоты | 4 | 2 | - | - |
| | Комплексное обслуживание модуля (ISM) слотами | 1 | 1 | 1 | - |
| | Пакет-голосовые данные-модуль (PVDM) слотами | 4 | 3 | 0 | 0 |
| Порты USB (v2.0) | | 2 | 2 | 2 | 1 |
| По умолчанию / максимальная флэш-памяти | | 256 МБ / 8 ГБ | 256 МБ / 8 ГБ | 256 МБ / 8 ГБ | 256 МБ / 256 МБ |
| По умолчанию / максимальная RAM | | 1 Гб / 2 Гб | 512 МБ / 2 Гб | 512 Мб / 2,5 Гб | 512 МБ / 512 МБ |
| Безопасность | | | | | |
| Firewall | | Да | Да | Да | Да |
| VPN (DES, 3DES и AES) | | Да | Да | Да | Да |
| Предотвращение вторжений | | Да | Да | Да | Да |
| Фильтрация содержимого | | Да | Да | Да | Да |
| Специализированная коммутация | | | | | |
| LAN конференции | | Да | Да | - | - |

| | | | | |
|--|--------------------------------|--------------------------------|---|---|
| Голос и видео-DSP | PVDM3 и PVDM2 | PVDM3 и PVDM2 | - | - |
| SRST ¹⁾ | До 1200 IP тел. | До 250 IP тел. | - | - |
| Cisco Unified Communications Manager Express (приложение для управление вызовами) | До 350 | До 150 | - | - |
| Cisco Unity Express (сетевой модуль [Нм], служебный модуль [SM] или ISM) ²⁾ | 32 портов, 300 почтовых ящиков | 32 портов, 300 почтовых ящиков | - | - |
| Session Initiation Protocol (SIP) сессий ³⁾ | 1000 | 600 | - | - |
| Цифровая поддержка голосовой связи | До 720 | До 400 | - | - |
| Максимальная поддержка голоса для аналоговых и Basic Rate Interface (BRI) | 112 FXS, FXO 64, 40 BRI | 64 FXS, FXO 40, 24 BRI | - | - |

1) Приложение Survivable Remote Site Telephony (SRST). Это решение используется для поддержки избыточности в централизованной корпоративной среде IP-телефонии. SRST гарантирует предоставление услуг в случае сбоя в глобальной сети за счет интеллектуальной перенастройки маршрутизаторов Cisco и резервирования обработки вызовов для IP-телефонов, установленных в удаленных отделениях корпоративной IP-сети. Таким образом, обработка вызовов поддерживается даже во время отказов и сбоев, обеспечивая постоянную готовность и доступность IP-телефонов.

2) Приложение Cisco Unity Express предоставляет функцию автосекретаря, которая помогает клиентам найти нужного сотрудника или подразделение и оставить голосовые сообщения.

3) Протокол передачи данных, который описывает способ установления и завершения пользовательского интернет-сеанса, включающего обмен мультимедийным содержимым (видео- и аудиоконференция, мгновенные сообщения и т.д.).

Для глобальных сетей:

Маршрутизатор серии 7200

Маршрутизаторы серии Cisco 7200 обеспечивают оптимальное решение задач в области организации центра коммутации крупного предприятия с сетью филиалов, подключение удаленных и региональных офисов к глобальным сетям и Интернет, создание мультисервисного узла коммутации.

В серии Cisco 7200 существует возможность выбора, в зависимости от потребностей, из 2-х, 4-х и 6-ти слотовых шасси, трех процессоров (до 200 МГц) и различных LAN и WAN портов до 48, одинарные или дублированные источники питания.

Благодаря модульной архитектуре маршрутизаторы Cisco 7200 позволяют создавать масштабируемые решения, отвечающие самым различным требованиям к плотности, производительности и ассортименту услуг, одновременно обеспечивая защиту инвестиций с учетом будущего развития сети.

Поддержка маршрутизаторами серии 7200 протокола Cisco IOSTM Hot Standby Router Protocol (HSRP) обеспечивает возможность быстрого перехода на резервное оборудование в случае отказа части сетевых устройств или соединений.

Основная задача протокола HSRP заключается в том, чтобы добиться практически 100% доступности и отказоустойчивости первого перехода от отправителя. Это достигается путем использования двух или более маршрутизаторов.

Маршрутизатор ASR серии 1000

Маршрутизатор серии 1000 подходит, как для корпоративных сетей, так может применяться и в сетях операторского класса.

В серию входят три модели: Cisco ASR 1002, 1004 и 1006, имеющие производительность до 20 Гбит/с. Все они используют инновационный процессор Cisco QuantumFlow, который обеспечивает не только высокую

производительность, но и поддержку таких сервисов, как шифрование и файрвол, QoS, NBAR, инспектирование пакетов на основе ПО, широкополосное подключение, контроль пограничных сессий и т.д.

Модульная архитектура позволяет подобрать конфигурацию оборудования в соответствии с необходимыми потребностями.

Функциональные особенности Cisco ASR 1000:

- ◆ параллельная обработка запросов обеспечивает быстрое предоставление сервисов;
- ◆ высокая доступность для сетевой периферии. Обеспечивает обновление ПО в процессе обслуживания;
- ◆ компактное исполнение. Позволяет снизить энергопотребление, занимаемые площади и затраты на комплектацию при обеспечении максимальной скорости работы интегрированных сервисов;
- ◆ объединение высокопроизводительных сервисов, включая шифрование, широкополосное подключение, брандмауэр 10 Гбит/с, NBAR и SBC (все на базе ПО, без необходимости подключения дополнительных сервисных модулей);
- ◆ мгновенное подключение новых сервисов;
- ◆ высокая отказоустойчивость благодаря поддержке удобной и экономичной функции обновления ПО без отключения сервисов (ISSU).

Маршрутизаторы Cisco ASR 1000 используют ПО Cisco IOS XE. Высочайшая гибкость и производительность встроенного процессора Cisco ASR 1000 обеспечивает безопасность сети, оптимизацию сетевого трафика, поддержку Cisco IOS Firewall и другие дополнительные функции Cisco IOS XE без необходимости подключения дополнительного оборудования.

Cisco ASR 1000 позволяют провайдерам объединить различные устройства и предоставить пользователям несколько мгновенно подключаемых управляемых сервисов. Для этого нет необходимости подключать специальные устройства и модули, что позволяет снизить операционные расходы за счет снижения затрат на обслуживание.

Провайдеры управляемых услуг могут задавать приоритетность трафика сервисных устройств, связанного с выполнением отдельных приложений, и повысить приоритетность трафика, требующего непрерывного и стабильного подключения, например, IP-телефонии или видео.

Для операторского класса:

Маршрутизатор Cisco XR серии 12000/12000

- ◆ Идеально подходит для крупных предприятий и операторов связи.
- ◆ Позволяет реализовать виртуализацию с высоким уровнем безопасности и согласованное предоставление доступа к сервисам.
- ◆ Использует архитектуру Cisco I-Flex, которая позволяет назначать приоритеты сервисам передачи голоса, видео и данных.
- ◆ Обеспечивает непрерывную работу системы и мультисервисное масштабирование.

Модельный ряд серии Cisco 12000 GSR представлен маршрутизаторами Cisco 12006, Cisco 12010, Cisco 12016, Cisco 12404, Cisco 12406, Cisco 12410, Cisco 12416, Cisco 12810, Cisco 12816.

Серия интеллектуальных маршрутизаторов Cisco 12000 GSR (Gigabit Switch Router) с производительностью от 2,5 Гбит/с до 10 Гбит/с (в расчете на один слот) предназначена для построения опорных и граничных сетей операторского класса на основе технологии IP/MPLS. Маршрутизаторы предназначены в первую очередь для построения высокопроизводительных магистралей с обеспечением гарантированного качества.

Серия Cisco 12000 GSR также широко используется в качестве магистральных маршрутизаторов в сети Интернет. Поддерживаемые интерфейсы включают в себя порты OC-12 (622 Мбит/с), OC-48 (2,4 Гбит/с) и OC-192 (10 Гбит/с). Оптическая несущая представляет собой стандартизированный набор скорости передачи. Расчет скорости: линия как OC-N обозначает скорость $N \times 51,84$ Мбит/с.

Маршрутизаторы серии Cisco 12000 GSR являются устройствами операторского класса с обеспечением резервирования всех функциональных элементов: коммутационной матрицы, процессоров, источников питания.

Маршрутизатор серии 7600

Серия маршрутизаторов Cisco 7600 – единственная в отрасли серия маршрутизаторов для граничных сегментов сетей, обеспечивающих широкий набор функций IP/MPLS для граничных сегментов операторских сетей и корпоративных городских и распределенных сетей.

Серия модульных маршрутизаторов Cisco 7600 включает модели: Cisco 7603, Cisco 7604, Cisco 7606, Cisco 7609 и Cisco 7613.

Например, маршрутизатор Cisco 7609 обеспечивает производительность коммутации на уровне 720 Гбит/с и пропускную способность 40 Гбит/с на слот. При этом маршрутизатор обеспечивает достаточную производительность для организации граничных сегментов сетей IP/MPLS. Оснащенная девятью вертикальными слотами и занимающая 1/2 стойки система централизованно обрабатывает 30 млн. пакетов/с, а также оснащена распределенной системой обработки, позволяющей обеспечить работу сетей Gigabit Ethernet и 10Gigabit Ethernet.

Поддерживая различные интерфейсы и технологию адаптивной обработки сетевого трафика, маршрутизаторы серии Cisco 7600 предлагают интегрированные услуги Ethernet, частных линий и агрегации абонентских подключений.

4.3. Пакетная передача данных в сетях мобильных операторов

GPRS (General Packet Radio Service) – сети с пакетной передачей данных, которые позволяют пользователям мобильных устройств производить обмен данными друг с другом в сети GSM и с внешними сетями (такими как Интернет). GPRS – своеобразная надстройка над

обычной сотовой сетью, которая позволяет передавать данные на существенно более высоких скоростях, чем в обычных GSM сетях.

Приведем пример построение сети сотового оператора с применением маршрутизаторов (рис. 4.1).

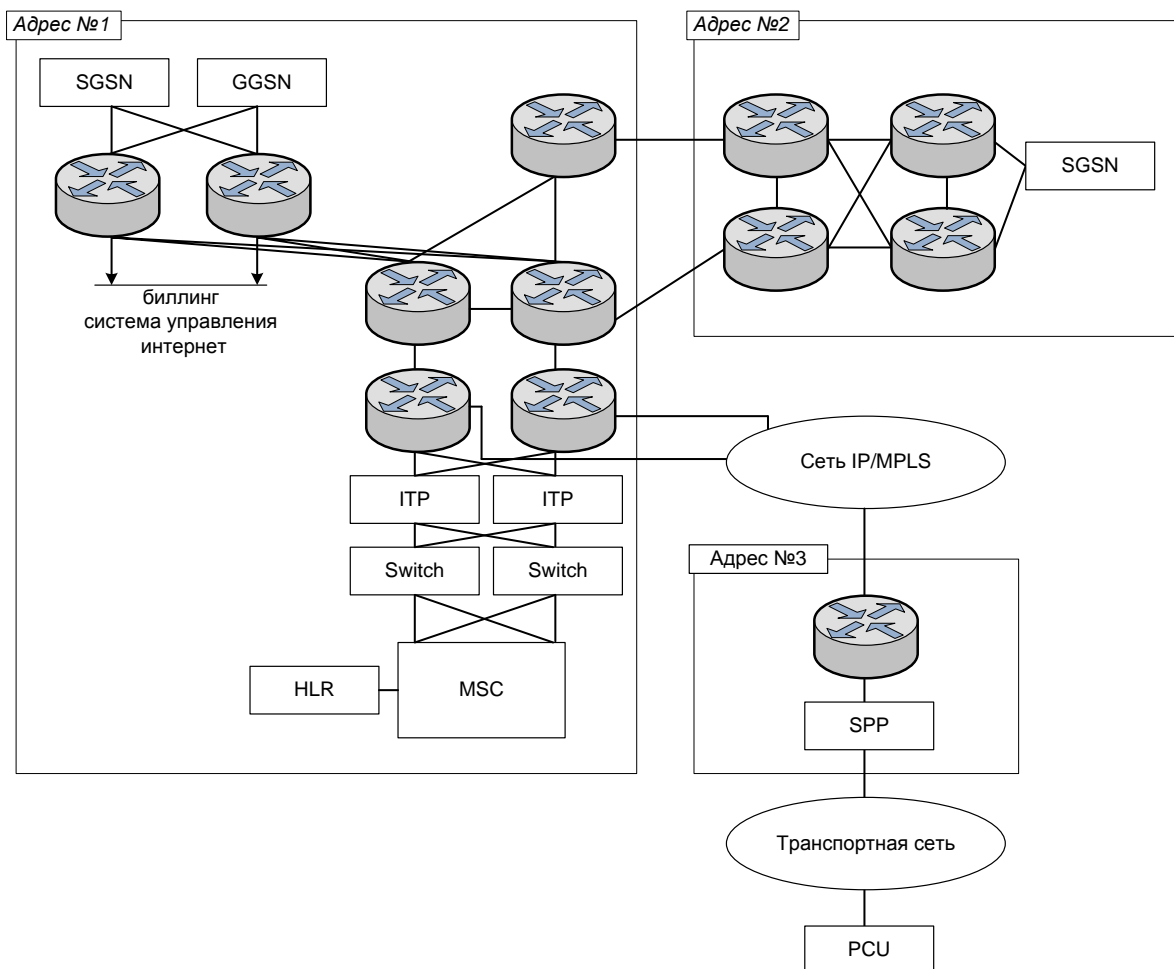


Рис. 4.1. Пример пакетной передачи данных в мобильных сетях

Основные компоненты сети:

HLR (Home Location Register) – база данных, которая содержит информацию об абонентах сети оператора.

MSC – автоматическая телефонная станция, обеспечивающая возможность связи (с коммутацией каналов) для управления и предоставления сервисов GSM, для мобильных телефонов внутри зоны своего обслуживания. Сервисы представляют собой голос, данные и факсимильную связь, а также SMS и переадресацию вызовов.

MGW (Media gateway) – элемент сети сотовой связи, предназначенный для коммутации абонентской нагрузки.

В архитектуре GPRS задействованы два новых основных сетевых узла.

Первый узел SGSN (Serving GPRS Support Node) обеспечивает поддержку услуг GPRS. SGSN имеет тот же уровень иерархии, что и MSC, и обеспечивает маршрутизацию пакетов, аутентификацию (контроль доступа) и шифрование, а так же отслеживает расположение мобильных передатчиков, находящихся в зоне его обслуживания.

Второй узел шлюзовой поддержки GPRS – GGSN (Gateway GPRS Support Node). SGSN обеспечивает маршрутизацию данных между GPRS Core network (протокол GTP) и внешними IP-сетями.

Так же добавляется управляющий блок пакетной коммутации PCU (Packet Controller Unit), который подключается к BSC и обеспечивает услуги пакетной радиопередачи на область охвата BSC.

Для подключения узлов SGSN и GGSN к некоторым элементам сети добавляются новые интерфейсы с обозначением G*, где * – буква, определяющая конкретный интерфейс.

IP/MPLS (Multiprotocol Label Switching) – это сеть, которая организована на базе технологии многопротокольной коммутации меток. Такая сеть имеет иерархическую двухуровневую архитектуру, которая включает в себя граничный слой, несущий основную нагрузку по обслуживанию абонентов, и составляет основной «интеллект» сети и опорный слой (ядро) MPLS-коммутации IP-трафика.

Механизм работы IP/MPLS отличается от работы протокола IP и заключается в том, что к пакету данных прикрепляется специальная метка, благодаря чему принципы управления передачей трафиком меняются.

Сначала с помощью динамических протоколов маршрутизации (OSPF и др.) определяется путь, по которому будет отправляться трафик. Каждому интерфейсу с помощью протокола LDP присваивается специализированная транспортная метка. Этот механизм определения топологии и раздачи меток

носит название управляющей компоненты MPLS. После того, как топология определена, трафик коммутируется внутри сети по независимым от типа передаваемого трафика меткам. Фактически устройства в сети MPLS являются коммутаторами трафика по меткам. Этот механизм носит название коммутационной компоненты MPLS.

Основные преимущества технологии IP/MPLS:

- ◆ более высокая скорость продвижения IP-пакетов по сети за счет сокращения времени обработки маршрутной информации;
- ◆ возможность организации информационных потоков в каналах связи. С помощью меток каждому информационному потоку (например, несущему телефонный трафик) может назначаться требуемый класс обслуживания. Потоки с более высоким классом получают приоритет перед всеми другими потоками;
- ◆ полное обособление друг от друга виртуальных корпоративных сетей за счет создания для каждой из них своеобразных туннелей;
- ◆ прозрачный пропуск через ядро IP/MPLS трафика протоколов Ethernet, Frame Relay или ATM, что позволяет подключать пользователей, использующих все эти разнообразные протоколы.

В такой сети для передачи данных между всем узлами коммутации (MGW, SGSN, GGSN и т.д.) используются маршрутизаторы. В этой сети необходимо применить маршрутизаторы операторского уровня. Например, маршрутизаторы серии Cisco 7600.

Заключение

В дипломной работе был проведен анализ и сравнение внутренних протоколов маршрутизации. Представлены их характеристики. Так же был рассмотрен протокол внешней маршрутизации.

Упрощенная настройка всех протоколов маршрутизации была наглядно продемонстрирована на оборудовании Cisco. На основе этого был снят

видеоурок. В видеоуроке представлена работа программы Cisco Packet Tracer – симулятора сети передачи данных, выпускаемой фирмой Cisco Systems. Программа позволяет делать работоспособные модели сети, настраивать с помощью команд Cisco IOS маршрутизаторы и коммутаторы.

Кроме настраиваемых протоколов маршрутизации в видеоурок включена настройка DHCP и NAT.

Так же в дипломной работе рассмотрены следующие пункты:

- ◆ маршрутизатор компании Cisco Systems серии 1800, его внутренние компоненты и возможности;
- ◆ серии маршрутизаторов компании Cisco Systems, которые представлены на рынке в настоящее время;
- ◆ конкурирующие компании по производству маршрутизаторов;
- ◆ кратко рассмотрена пакетная передача данных в сетях мобильных операторов с применением маршрутизаторов.

Список использованной литературы

1. Учебное пособие ISDN1 и ISDN2 компании Cisco Systems
2. С. Хелеби, Д. Мак-Ферсон. Принципы маршрутизации в Internet. 2-е издание, Москва-Санкт-Петербург-Киев, 2001.
3. www.cisco.com
4. <http://xgu.ru/>
5. <http://citforum.ru/>
6. <http://findotvet.ru/>
7. <http://www.opennet.ru/>
8. <http://it-notes.info/>