МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН
ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛ-ХОРАЗМИЙ

Факультет “Компьютерный инжиниринг”
Кафедра “Компьютерные системы”

Назаров А.И.

КОММУНИКАЦИЯ ДАННЫХ

Учебное пособие
для бакалавров, обучающихся по направлению:
5330500 – Компьютерный инжиниринг
5330600 – Программный инжиниринг

Ташкент 2018

МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛ-ХОРАЗМИЙ

Назаров А.И.

КОММУНИКАЦИЯ ДАННЫХ

Учебное пособие

Ташкент 2018

УДК 004.7(075.8)

Автор: доцент Назаров А.И. «Коммуникация данных»./ТУИТ.117с. Ташкент, 2018.

В пособии описаны принципы и способы коммуникации данных, методы доступа в среду передачи данных, приведено описание уровней коммуникации и маршрутизации данных.

Приведены практические примеры конфигурирования и администрирования маршрутизируемых сетей.

Адресовано студентам, обучающимся по направлению Компьютерный и программный инжиниринг», сетевым администраторам, специалистам
предприятий, внедряющие новые информационные технологии.

Рецензент (ы):
Доцент, к.т.н. кафедры
«Автоматизация технологических процессов
и управления производством» ТИТЛП
Каххаров А.А.
Профессор, д.т.н. кафедры
«Информационная технология» ТУИТ Турсунбаев Ф.К.

Ташкентский Университет Информационных Технологий
имени Мухаммада ал-Хоразмий, 2018

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В целях повышения эффективности реализации комплексных программ по внедрению современных IT технологий в Узбекистане уделяется большое внимание проектированию и практическому внедрению коммуникационных сетей передачи данных с целью оптимизации основных сетевых характеристик: пропускная способность, производительность, стоимость, временные задержки и топологическая реализация каналов связи[1].

Одной важнейшей функцией коммуникационной сети (КС) связи является создание оптимальных эффективных сетей коммуникации данных.

Коммутация — процесс соединения абонентов КС через сетевые узлы. Абонентами могут выступать пользовательские компьютеры, сетевые компоненты, сегменты локальных сетей, средства IP телефонии. В сети применяются определенные способы коммутации абонентов, которые разделяют имеющиеся физические каналы между несколькими сеансами связи и между абонентами сети.

В настоящее время коммутация данных осуществляется с помощью коммутации каналов, сообщений и пакетов.

Целью данного пособия является подготовка студентов к теоретическим и практическим знаниям, и умениям при использовании коммуникационного оборудования и программных средств в осуществлении коммуникации данных.

Изложение материала во всех главах опирается на примеры, после каждой главы представлены контрольные вопросы для закрепления изученного теоретического материала, тесты для самоконтроля, а также список рекомендуемой литературы для изучения курса.

В первой главе учебного пособия приведены компоненты коммуникации данных, три способа коммутации: коммутация каналов, коммутация пакетов и коммутация сообщений. В качестве методов доступа в сеть используются такие как, конкурентный (Ethernet) и маркерный доступ (Token Ring, Arcnet).

Во второй главе приводится коммутация данных на основе коммутаторов 2,3,4 уровней, позволяющих объединять сегменты разных технологий локальных сетей и фильтровать трафик пере-

[1] Постановление Президента Республики Узбекистан «О мерах по дальнейшему совершенствованию системы управления проектами в сфере информационно–коммуникационных технологий» № ПП–3415, 30.11. 2017.

дачи данных на уровне локальных групп и между сетями, показана трансляцией протоколов канального уровня в соответствии со спецификацией IEEE 802.1H и поддержкой разнообразных пользовательских фильтров, основанных на MAC - адресах.

В третьей главе показана IP маршрутизация на основе маршрутизаторов третьего уровня, позволяющая одновременно поддерживать сразу нескольких сетевых протоколов и нескольких протоколов маршрутизации, возможность приоритетной обработки трафика, разделение функций построения таблиц маршрутизации и продвижения пакетов между маршрутизаторами разного класса на основе готовых таблиц маршрутизации.

В четвертой главе описаны принципы работы дистанционно-векторных протоколов динамической маршрутизации OSPF, EIGRP, RIP, BGP в зависимости от размеров маршрутизируемой сети.

ГЛАВА 1. КОМПЬЮТЕРНЫЕ КОММУНИКАЦИИ

В целях обеспечения ускоренного инновационного развития всех отраслей экономики и социальной сферы на основе передового зарубежного опыта, современных достижений мировой науки, инновационных идей, разработок и технологий развитие коммуникационных сетей позволяют обеспечить эффективную передачу разнородной информационных данных.

1.1. Компоненты сети передачи данных

Основными компонентами сети являются рабочие станции, серверы, передающая среда и сетевое оборудование. Рабочей станцией называют каждый из компьютеров сети, на котором пользователи решают свои задачи, а сервером - аппаратно-программную систему, предназначенную для управления распределением сетевых ресурсов общего доступа.

Процесс передачи данных по сети определяют шесть компонент[2]:

1. Компьютер-источник;
2. Блок протокола;
3. Передатчик;
4. Физическая кабельная сеть;
5. Приемник;
6. Компьютер-адресат.

Компьютер-источник может быть рабочей станцией, файл-сервером, шлюзом или любым компьютером, подключенным к сети. Блок протокола состоит из набора микросхем и программного драйвера для платы сетевого интерфейса. Блок протокола отвечает за логику передачи по сети.

Передатчик посылает электрический сигнал через физическую топологическую схему. Приемник распознает и принимает сигнал, передающийся по сети, и направляет его для преобразования в блок протокола. Цикл передачи данных начинается с компьютера-источника, передающего исходные данные в блок протокола. Блок протокола организует данные в пакет передачи, содержащий соответ-

[2] Кульгин, Максим. Компьютерные сети. Практика построения. - СПб : Питер, 2003. - 462 с.

ствующий запрос к обслуживающим устройствам, информацию по обработке запроса (включая, если необходимо, адрес получателя) и исходные данные для передачи.

Пакет затем направляется в передатчик для преобразования в сетевой сигнал. Пакет распространяется по сетевому кабелю пока не попадает в приемник, где перекодируется в данные. Здесь управление переходит к блоку протокола, который проверяет данные на сбойность, передает «квитанцию» о приеме пакета источнику, переформировывает пакеты и передает их в компьютер-адресат. В ходе процесса передачи блок протокола управляет логикой передачи по сети через схему доступа.

Для соединения компьютеров в сети могут быть использованы различные проводящие среды, или линии связи. Основной характеристикой линии связи является пропускная способность, т.е. максимальная скорость передачи информации. Измеряется она в бит/с, Кбит/с, Мбит/с. Пропускная способность зависит от вида линии связи. Основными видами каналов связи являются:

1. Витая пара – проводной канал связи, содержащий две пары скрученных попарно проводников. Переплетение проводов необходимо для защиты от электрических помех, наводимых соседними проводами и иными внешними источниками. Различаются неэкранированная и экранированная витая пара. Витая пара обладает относительно малой пропускной способностью, ее нельзя использовать для передачи данных на большие расстояния. Безусловными достоинствами витой пары являются дешевизна и простота подключения.

2. Коаксиальный кабель обладает средней пропускной способностью, обеспечивает большую дальность по сравнению с витой парой. Он состоит из центрального цельного или витого проводника, окруженного слоем диэлектрика. Второй проводящий слой из металлической оплетки, алюминиевой фольги, или же их комбинации окружает диэлектрик и выполняет одновременно функцию экрана против электрических наводок. Внешнюю оболочку кабеля образует общий изолирующий слой.

4. Оптоволоконный кабель обладает самой высокой пропускной способностью. Носителем данных в нем является световой луч. Сигнал в кабеле практически не затухает, что позволяет передавать большие объемы данных с высокой скоростью. Помимо этого, такой вид связи устойчив к внешним электрическим помехам. С по-

мощью оптического волокна можно передавать данные только в одном направлении, поэтому кабель состоит из двух волокон с отдельными коннекторами. Одно из них используется для передачи, второе — для приема сигнала. Недостатками оптоволоконного кабеля являются высокая стоимость и сложность подсоединения.

Беспроводные локальные сети. В них информация передается в СВЧ-диапазоне, либо с помощью инфракрасных лучей. Беспроводные сети, безусловно, являются очень удобными, поскольку не требуют прокладки кабелей. Имеют они и свои недостатки. Так при удалении сетевых устройств друг от друга скорость работы сети довольно быстро падает. Помимо этого, защита передаваемых данных от перехвата требует дополнительной надежной системы безопасности сетевого взаимодействия.

Сети на телефонных линиях. При проектировании сетей такого типа следует учитывать, что далеко не все телефонные линии нашей страны отвечают стандартам качества западных стран, в расчете на которые разрабатывалось сетевое оборудование.

Сети на основе электропроводки. Для работы в таких сетях используются сетевые карты, подключающиеся к розеткам электропроводки с помощью специальных разъемов. Недостатками сетей на основе электропроводки являются электрические помехи, вызванные работой оборудования и слабая защищенность сообщений от перехвата с помощью постороннего компьютера.

Основные характеристики коммуникационной сети[3]:

1. Скорость передачи данных по каналу связи (измеряется количеством битов в единицу времени, для асинхронных модемов и телефонного канала — 300-9600 бит/сек, для синхронных — 1200-19200 бит/сек; волоконно-оптическая связь и технологии спектрального уплотнения каналов передают потоки 10 Гбит/с и более — до 100 Гбит, а поскольку в оптоволоконном световоде каналов можно «нарезать» более сотни, то можно говорить о переходе с терабитным системам цифровой связи.
2. Пропускная способность канала связи (количество знаков в секунду, включая служебные символы), измеряется количеством знаков в секунду);

[3] Компьютеры, сети, Интернет: энциклопедия / Новиков Ю., Новиков Д., Черепанов А., Чуркин В. - СПб : Питер, 2002. - 928 с:

3. Достоверность передачи информации (единица измерения — количество ошибок на знак, обычно в пределах 10^{-6} — 10^{-7} ошибок на знак).
4. Надежность канала связи и модемов (определяется либо долей времени исправного состояния в общем времени работы, либо средним временем безотказной работы, единица измерения — среднее время безотказной работы — в часах.

Основными видами сетевых компонент являются:

Сетевые карты (сетевые адаптеры) подключаются к слотам расширения материнской платы компьютера и предназначены для соединения компьютера с сетевым кабелем. С помощью сетевой карты осуществляется подготовка данных для их передачи в сеть, передача сигнала, прием сигналов из сети и их расшифровка, а также управление потоком данных между компьютером и сетью.

Концентраторы (Hub) используются для соединения сегментов локальной сети. Концентратор имеет несколько портов, к каждому из которых подключена своя линия. Когда на один из портов приходит пакет, он копируется и пересылается на все остальные порты, таким образом, все подключенные к хабу устройства сети могут видеть все передаваемые пакеты. Концентраторы подразделяются на активные и пассивные. Активные концентраторы усиливают полученные сигналы и передают их, в то время как пассивные концентраторы только пропускают через себя сигнал, не производя над ним никаких действий.

Коммутаторы (Switch) по своему назначению сходны с концентраторами. К ним подключается несколько линий. Принципиальное отличие состоит в том, что в концентраторе сигнал, поступивший на один порт, попадает во все остальные порты концентратора, а в коммутаторе происходит прямое связывание портов отправки и назначения через виртуальный канал. Все остальные порты не воспринимают этот сигнал. Таким образом, коммутатор является программно-управляемым устройством сети, позволяющим сократить сетевой трафик за счет анализа пришедшего пакета с целью определения адреса его назначения и передачи данных только получателю. Использование коммутаторов позволяет повысить пропускную способность сети и улучшить ее безопасность, поскольку перехват передаваемых данных может быть осуществлен только на отдельном маршруте сети.

Маршрутизаторы (Router) являются стандартными устройствами сети, обеспечивающими выбор маршрута передачи блоков данных между несколькими сетями, имеющими различную архитектуру или протоколы. Маршрутизаторы работают на сетевом уровне.

Повторители (repeater) предназначены для усиления и восстановления исходной формы сигнала с целью увеличения расстояния его передачи между станциями или сетевыми элементами. Повторитель работает на электрическом уровне для соединения двух сегментов сети.

Мосты (Bridge) используются для соединения двух отдельных сегментов одной сети, ограниченных своей физической длиной, или нескольких локальных сетей, использующих одинаковые протоколы. Помимо этого, мосты могут усиливать сигналы, что дает возможность увеличить размер сети, не нарушая ограничений на максимальную длину кабеля, количество подключенных устройств или количество повторителей на сегмент сети.

Шлюзы (Gateway) являются программно-аппаратными комплексами, обеспечивающими соединение разнородных сетей или сетевых устройств. Шлюз извлекает данные из пришедшего сигнала и затем преобразовывает их в формат, действующий на стороне получателя. Использование шлюзов позволяет решать проблемы, возникающие из-за различия протоколов или систем адресации.

Терминатор представляет собой резистор номиналом 50 Ом. Терминаторы используют для обеспечения затухания сигнала на концах сегмента сети.

Мультиплексоры обеспечивают совместное использование проводящей среды двумя и более каналами. Достигается это за счет группирования (мультиплексирования) сигналов от нескольких источников для их передачи по одному каналу. В настоящее время различают три вида мультиплексирования: пространственное, временное и частотное. При пространственном и временном мультиплексировании происходит последовательная циклическая передача сигналов нескольких каналов по общему каналу, а при частотном мультиплексировании осуществляется одновременная передача данных на различных частотах.

Брандмауэры (firewall, межсетевые экраны) предназначены для обеспечения информационной безопасности сетей и отдельных

компьютеров на основе контроля над передаваемой и принимаемой информацией и обеспечивают защиту посредством фильтрации данных на основе различных критериев (содержимого, адресов и т.д.). Брандмауэры могут быть программными и/или аппаратными. Как правило, функционирование брандмауэров основывается на традиционных моделях разграничения доступа, согласно которым субъекту (пользователю, программе, процессу или сетевому пакету) разрешается или запрещается доступ к какому-либо объекту (файлу или узлу сети) на основании некоторых заданных правил.

1.2. Способы коммутации

В любой сети связи всегда применяется какой-либо способ коммутации, обеспечивающий с помощью коммутаторов доступность имеющихся физических каналов одновременно для нескольких сеансов связи между абонентами сети, каждый из которых соединяется с ближайшим коммутатором индивидуальной линией связи. В любой момент времени эта линия используется только одним абонентом, а между коммутаторами линии связи используются совместно многими абонентами.

Используются три принципиально различных способа коммутации абонентов в сетях: коммутация каналов, коммутация сообщений и коммутация пакетов[4].

Сети с коммутацией сообщений и коммутацией пакетов относятся к типу сетей с промежуточным хранением передаваемой информации. Сети с коммутацией каналов и коммутацией пакетов разделяются, кроме того, на два класса - на сети с динамической коммутацией и сети с постоянной коммутацией.

В сетях с динамической коммутацией соединение абонента с любым другим устанавливается сетью по инициативе абонента, продолжается определенное время (от нескольких секунд до нескольких часов) и завершается также по инициативе абонента по окончании обмена информацией. Такой режим работы поддерживают телефонные сети общего пользования, локальные сети, сети TCP/IP.

[4] Мусаев М.М. “Компьютер тизимлари ва тармоқлари”. Тошкент.: “Aloqachi” нашриёти, 2013 йил. 8 боб. 394 бет. – Олий ўқув юртлари учун қўлланма.

В сетях с постоянной коммутацией соединение между взаимодействующими пользователями устанавливается персоналом сети на длительное время (несколько месяцев и более). Режим постоянной коммутации популярен в сетях технологии SDH, где создаются выделенные каналы связи с пропускной способностью в несколько Гбит/с.

Некоторые сети поддерживают оба режима работы, например сети X 25 и ATM.

Коммутация каналов. При коммутации каналов между связываемыми конечными пунктами на протяжении всего временного интервала соединения обеспечивается обмен в реальном масштабе времени, причем биты передаются с неизменной скоростью по каналу с постоянной полосой пропускания. Между абонентами устанавливается сквозной составной канал связи до начала передачи информации. Этот канал формируется из отдельных участков с одинаковой пропускной способностью. Прохождение отдельного сигнала вызова обеспечивается с помощью последовательного включения нескольких коммутационных устройств, размещаемых в центрах коммутации каналов (ЦКК). Каждое устройство резервирует за собой физическое соединение между одним входящим и одним исходящим каналами. Если при установлении сквозного канала связи занята вызываемая сторона или хотя бы одно из коммутационных устройств в цепочке прохождения сигнала вызова, последний будет блокироваться, и абонент, инициировавший вызов, должен спустя некоторое время его повторить.

Время установления сквозного канала связи обычно бывает большим из-за необходимости организации взаимодействия значительного числа устройств коммутации. После установления такого канала ЦКК выполняют минимальное число функций, хотя при этом может передаваться большой объем информации. Следовательно, при использовании метода коммутации каналов передача информации обеспечивается двумя основными составляющими в расходной части ресурсов: ресурсами для организации вызова и ресурсами для поддержания в ЦКК коммутационных устройств или для организации распределения временных каналов. Первая составляющая не зависит от объема передаваемой информации, а вторая прямо пропорциональна интервалу времени, в течение которого происходит соединение.

Коммутаторы и соединяющие их каналы должны обеспечивать одновременную передачу данных нескольких абонентских каналов, поэтому они должны быть высокоскоростными и поддерживать одну из двух техник мультиплексирования абонентских каналов:

• технику частотного мультиплексирования (FDM - Frequency Division Multiplexing - частотное уплотнение каналов), когда для разделения абонентских каналов используется модуляция высокочастотного несущего синусоидального сигнала низкочастотным сигналом, порождаемым звуковыми колебаниями (частотное разделение характерно для аналоговой модуляции сигналов);

• технику мультиплексирования с разделением времени (TDM - Time Division Multiplexing - мультиплексирование с разделением времени), когда аппаратура TDM-сетей (мультиплексоры, коммутаторы, демультиплексоры) работает в режиме разделения времени, поочередно обслуживая в течение цикла своей работы все абонентские каналы. Временное разделение характерно для цифрового кодирования. Сети TDM требуют синхронной работы всего оборудования, поэтому такая техника мультиплексирования имеет и другое название -техника синхронного режима передачи. В настоящее время практически все данные (голос, изображение, компьютерные данные) передаются в цифровой форме, поэтому выделенные каналы TDM-технологии, обеспечивающие нижний уровень для передачи цифровых данных, являются универсальными каналами для построения сетей любого типа: телефонных, компьютерных, телевизионных.

Виртуальные каналы в сетях с коммутацией пакетов. Существует режим работы сети - передача пакетов по виртуальному каналу (virtual circuit или virtual channel), где устанавливается виртуальный канал между двумя конечными узлами, который представляет собой единственный маршрут, соединяющий эти конечные узлы. Виртуальный канал может быть динамическим или постоянным.

Динамический виртуальный канал устанавливается путем запроса на установление соединения с помощью специального пакета, который проходит через коммутаторы и «прокладывает» виртуальный канал, т.е. коммутаторы запоминают маршрут для данного соединения и при поступлении последующих пакетов данного соединения отправляют их всегда по проложенному маршруту.

Постоянные виртуальные каналы создаются администраторами сети путем ручной настройки коммутаторов[5].

Каждый режим передачи пакетов имеет свои преимущества и недостатки. При передаче данных дейтаграммным методом, т.е. на основе пакета, передаваемого через сеть независимо от других пакетов без установления логического соединения и подтверждения приема, и поэтому работает без задержки перед передачей данных. Это особенно выгодно для передачи небольшого объема данных, когда время установления соединения может быть соизмеримым со временем передачи данных. Кроме того, дейтаграммный метод быстрее адаптируется к изменениям в сети.

При использовании метода виртуальных каналов время, затраченное на установление виртуального канала, компенсируется последующей быстрой передачей всего потока пакетов. Коммутаторы распознают принадлежность пакета к виртуальному каналу по специальной метке - номеру виртуального канала, а не анализируют адреса конечных узлов, как это делается при дейтаграммном методе.

В качестве недостатков метода коммутации каналов можно указать следующие:

- большое время установления сквозного канала связи из-за возможного ожидания освобождения отдельных его участков;
- необходимость повторной передачи сигнала вызова из-за занятости вызываемой стороны или какого-либо коммутационного устройства в цепочке прохождения этого сигнала (в связи с этим система, в которой реализуется метод коммутации каналов, относится к классу систем с потерей запросов на обслуживание);
- отсутствие возможности выбора скоростей передачи информации;
- наращивание функций и возможностей сети ограничено;
- не обеспечивается равномерность загрузки каналов связи (возможности по сглаживанию загрузки весьма ограничены).

Преимущества метода коммутации каналов:

- отработанность технологии коммутации каналов (первое коммутационное устройство появилось еще в конце XIX века);

[5] Велихов, А. В. Компьютерные сети]: уч. пособие по администрированию локальных и объединенных сетей / А. В. Велихов, К. С. Строчников, Б. К. Леонтьев. - М. : ЗАО "Новый изд. дом", 2005. - 304 с.

- возможность работы в диалоговом режиме и в реальном масштабе времени;
- обеспечение как битовой прозрачности, так и прозрачности по времени независимо от числа коммутаций между абонентами;
- гарантированная пропускная способность сети после установления соединения (это важно при передаче голоса, изображения, управления объектами в реальном масштабе времени);
- довольно широкая область применения. Сети с коммутацией каналов хорошо приспособлены для коммутации потоков данных постоянной скорости, когда единицей коммутации является долговременный синхронный поток данных между взаимодействующими абонентами.

Коммутация с промежуточным хранением. Сквозной канал между отправителем и получателем не устанавливается. Вызывающий объект посредством набора номера или через выделенную линию связывается только с ближайшим узлом сети и передает ему информационные биты. В каждом узле имеется коммутатор, построенный на базе коммуникационной ЭВМ с запоминающим устройством (ЗУ). Передаваемая информация должна храниться в каждом узле по пути к пункту назначения, причем задержка в хранении, как правило, будет различной для узлов. Наличие ЗУ в промежуточных узлах связи предотвращает потерю передаваемой информации, вследствие чего системы, реализующие рассматриваемые методы коммутации, относятся к классу систем без потерь запросов на обслуживание. Одним из показателей этих методов является возможность согласования скоростей передачи данных между пунктами отправления и назначения, которое обеспечивается наличием в сети эффективных развязок, реализуемых созданием буферных ЗУ в узлах связи. Наконец, для сетей с промежуточным хранением обязательным требованием является битовая прозрачность.

Коммутация сообщений. Этот метод передачи данных был преобладающим в 1960-х - 1970-х гг. и до сих пор используется в некоторых областях (в электронной почте, электронных новостях, телеконференциях, телесеминарах)[6]. Как и все методы коммутации с промежуточным хранением, технология коммутации сообщений

[6] Тарасов К. «Коммутаторы для сегмента передачи данных мультисервисной Metro-сети FTTB» журнал «Широкополосные мультисервисные сети», 2009.

относится к технологии типа «запомнить и послать». Кроме того, технология коммутации сообщений обычно предусматривает отношение «главный - подчиненный». Коммутатор (коммуникационная ЭВМ) в центре коммутации сообщений (ЦКС) выполняет регистрацию и выбор при управлении входящими и выходящими потоками. Здесь не рассматриваются интерактивный режим и работа в реальном масштабе времени, однако данные через коммутатор могут передаваться на очень высокой скорости с соответствующим определением уровней приоритетов для различных типов потоков данных. Высокоприоритетные потоки задерживаются в очереди на обслуживание на более короткое время по сравнению с низкоприоритетными потоками, что позволяет обеспечить интерактивные прикладные задачи.

Важно отметить, что при коммутации сообщений сообщение, независимо от его длины (разброс в длине сообщений может быть достаточно велик), целиком сохраняет свою целостность как единичный объект в процессе его прохождения от одного узла к другому вплоть до пункта назначения. Более того, транзитный узел не может начинать дальнейшую передачу части сообщения, если оно еще принимается. По своему влиянию на задержки это равноценно низкому уровню использования ресурсов сети.

Таким образом, коммутация сообщений предназначена для организации взаимодействия пользователей в режиме off-line, при котором не ожидается немедленной реакции на принятое сообщение.

Недостатки метода коммутации сообщений:

- необходимость реализации достаточно серьезных требований к емкости буферных ЗУ в узлах связи для приема больших сообщений, что обусловливается сохранением их целостности;
- недостаточные возможности по реализации диалогового режима и работы в реальном масштабе времени при передаче данных;
- выход из строя всей сети при отказе коммутатора, так как через него проходят все потоки данных (это характерно для структуры «главный - подчиненный»);
- коммутатор сообщений является потенциально узким местом по пропускной способности;
- каналы передачи данных используются менее эффективно по сравнению с другими методами коммутации с промежуточным хранением.

Преимущества метода:

- отсутствие необходимости в заблаговременном (до начала передачи данных) установлении сквозного канала связи между абонентами;
- возможность формирования маршрута из отдельных участков с различной пропускной способностью;
- реализация различных систем обслуживания запросов с учетом их приоритетов;
- возможность сглаживания пиковых нагрузок путем запоминания низкоприоритетных потоков в периоды этих нагрузок;
- отсутствие потерь запросов на обслуживание.

Коммутация пакетов. Появившаяся в 70-х гг. XX в. коммутация пакетов сочетает в себе преимущества коммутации каналов и коммутации сообщений[7]. Ее основные цели: обеспечение полной доступности сети и приемлемого времени реакции на запрос для всех пользователей, сглаживание асимметричных потоков между многими пользователями, обеспечение мультиплексирования возможностей каналов связи и портов компьютеров сети, рассредоточение критических компонентов (коммутаторов) сети.

При коммутации пакетов пользовательские данные (сообщения) перед началом передачи разбиваются на короткие пакеты фиксированной длины. Каждый пакет снабжается протокольной информацией: коды начала и окончания пакета, адреса отправителя и получателя, номер пакета в сообщении, информация для контроля достоверности передаваемых данных в промежуточных узлах связи и в пункте назначения. Будучи независимыми единицами информации, пакеты, принадлежащие одному и тому же сообщению, могут передаваться одновременно по различным маршрутам в составе дейтаграмм. Управление передачей и обработкой пакетов в узлах связи осуществляется центрами коммутации пакетов (ЦКП) с помощью компьютеров. Длительное хранение пакетов в ЦКП не предполагается, поэтому пакеты доставляются в пункт назначения с минимальной задержкой, где из них формируется первоначальное сообщение.

В отличие от коммутации сообщений технология коммутации пакетов позволяет:

[7] Shinder D.L.Osnovy of computer networks: - M.: Williams, 2002. - 656 with.

• увеличить количество подключаемых станций (терминалов), так как здесь больше коммутаторов;
• легче преодолеть трудности, связанные с подключением к коммутаторам дополнительных линий связи;
• осуществить альтернативную маршрутизацию (в обход поврежденных или занятых узлов связи и каналов), что создает повышенные удобства для пользователей;
• существенно сократить время на передачу пользовательских данных, повысить пропускную способность сети и эффективность использования сетевых ресурсов.

Одной из концепций коммутации пакетов является мультиплексирование с помощью разделения времени использования одного и того же канала многими пользователями, что повышает эффективность функционирования ТКС. Логика коммутации пакетов позволяет мультиплексировать многие пользовательские сеансы на один порт компьютера. Пользователь воспринимает порт как выделенный, в то-время как он используется как разделенный ресурс. Мультиплексирование порта и канала называют виртуальным каналом, а такой режим работы - передачей пакетов по виртуальному каналу. Коммутация пакетов и мультиплексирование обеспечивают сглаживание асимметричных потоков в каналах связи.

Стоимость организации вызова для пакетной коммутации ниже по сравнению с соответствующей характеристикой метода коммутации каналов. Но с увеличением объема передаваемой информации стоимостная характеристика для пакетной коммутации возрастает быстрее, чем для коммутации каналов, что объясняется необходимостью больших ресурсов для обработки пересылаемой информации.

В настоящее время пакетная коммутация является основной для передачи данных.

Символьная коммутация: субпакетная коммутация, или метод общего пакета представляет собой разновидность пакетной коммутации. Она применяется в случае, когда пакет содержит информационные биты, принадлежащие различным пользователям.

При пакетной коммутации приходится находить компромиссное решение, удовлетворяющее двум противоречивым требованиям. Первое из них - уменьшение задержки пакета в сети, обеспечиваемое уменьшением его длины, и второе - обеспечение повышения эффективности передачи информации, достигаемое, наобо-

рот, увеличением длины пакета (при малой длине пакета длина его заголовка становится неприемлемо большой, что снижает экономическую эффективность передачи). В сети с пакетной коммутацией максимально разрешенный размер пакета устанавливается на основе трех факторов: распределения длин пакетов, характеристики среды передачи (главным образом скорости передачи) и стоимости. Для каждой передающей среды выбирается свой оптимальный размер пакета.

При использовании символьной коммутации оптимальный размер пакета для конкретной передающей среды сохраняется с одновременным уменьшением времени задержки пакета в сети. Это достигается за счет приема от нескольких пользователей по небольшому количеству символов (информационных бит) и загрузки их в один пакет общего доступа.

Анализ рассмотренных коммутационных технологий позволяет сделать вывод о возможности разработки комбинированного метода коммутации, основанного на использовании в определенном сочетании принципов коммутации сообщений, пакетов и символьной коммутации и обеспечивающего более эффективное управление разнородным трафиком.

1.3. Методы доступа в компьютерных сетях

Каждая сетевая ОС использует определенную стратегию доступа от одного компьютера к другому. При конкурентном методе доступа абонент начинает передачу данных, если обнаруживает свободной линию, или откладывает передачу на некоторый промежуток времени, если линия занята другим абонентом. Широко используются маркерные методы доступа (называемые селективной передачей), когда компьютер-абонент получает от центрального компьютера сети так называемый маркер — сигнал передачи в течение определенного времени, после чего маркер передается другому абоненту.

Наиболее часто применяются две основные схемы[8]:

• конкурентная (Ethernet);

• с маркерным доступом (Token Ring, Arcnet).

[8] . Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы Питер, 2005. - 672 с.

Метод доступа CSMA/CD. В сетях Ethernet используется метод доступа к среде передачи данных, называемый методом коллективного доступа с опознаванием несущей и обнаружением коллизий (carrier-sense-multiply-access with collision detection, CSMA/CD).

Этот метод используется исключительно в сетях с общей шиной (к которым относятся и радиосети, породившие этот метод). Все компьютеры такой сети имеют непосредственный доступ к общей шине, поэтому она может быть использована для передачи данных между любыми двумя узлами сети. Простота схемы подключения - это один из факторов, определивших успех стандарта Ethernet. Говорят, что кабель, к которому подключены все станции, работает в режиме коллективного доступа (multiply-access, MA).

Все данные, передаваемые по сети, помещаются в кадры определенной структуры и снабжаются уникальным адресом станции назначения. Затем кадр передается по кабелю. Все станции, подключенные к кабелю, могут распознать факт передачи кадра, и та станция, которая узнает собственный адрес в заголовках кадра, записывает его содержимое в свой внутренний буфер, обрабатывает полученные данные и посылает по кабелю кадр-ответ.

Адрес станции-источника также включен в исходный кадр, поэтому станция-получатель знает, кому нужно послать ответ. При описанном подходе возможна ситуация, когда две станции одновременно пытаются передать кадр данных по общему кабелю (рис. 1.1.).

Для уменьшения вероятности этой ситуации непосредственно перед отправкой кадра передающая станция слушает кабель (то есть принимает и анализирует возникающие на нем электрические сигналы), чтобы обнаружить, не передается ли уже по кабелю кадр данных от другой станции.

Если опознается несущая (carrier-sense, CS), то станция откладывает передачу своего кадра до окончания чужой передачи, и только потом пытается вновь его передать. Но даже при таком алгоритме две станции одновременно могут решить, что по шине в данный момент времени нет передачи, и начать одновременно передавать свои кадры. При этом происходит *коллизия*, так как

содержимое обоих кадров сталкивается на общем кабеле, что приводит к искажению информации.

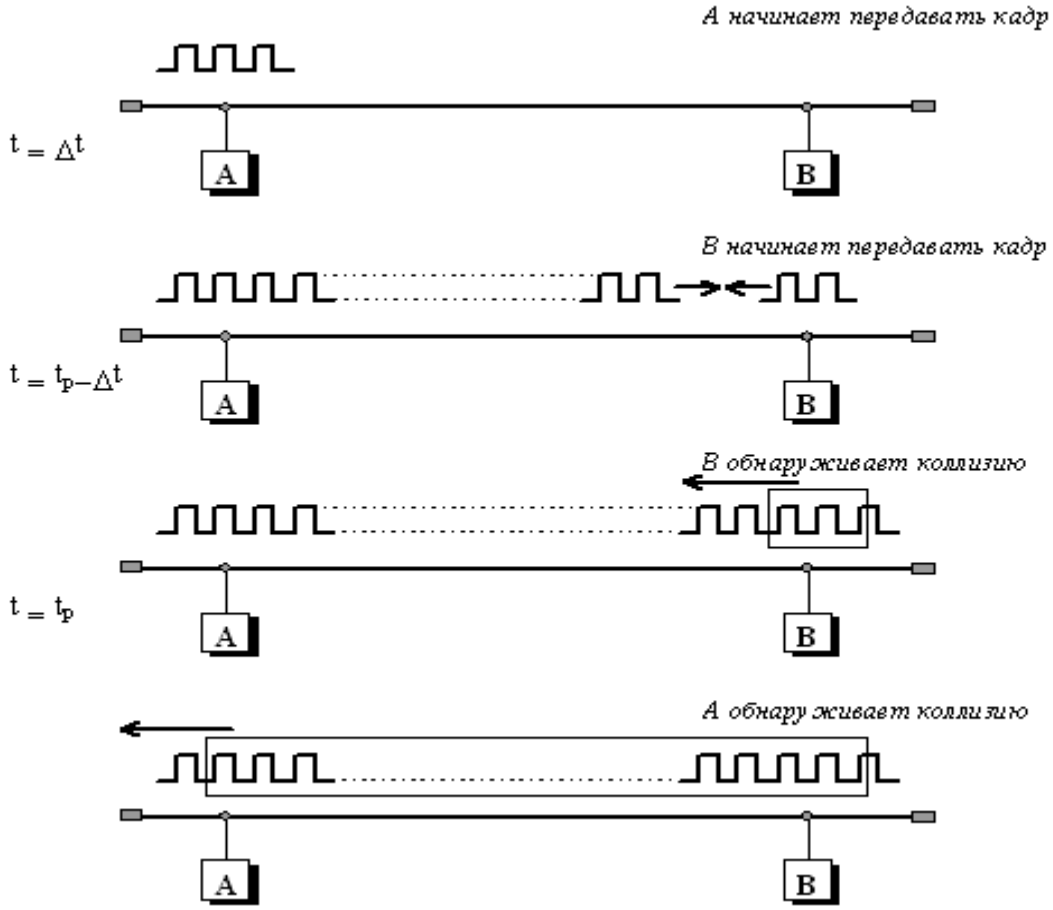

Рис. 1.1. Схема возникновения коллизии в методе случайного доступа CSMA/CD (tp - задержка распространения сигнала между станциями A и B)

Чтобы корректно обработать коллизию, все станции одновременно наблюдают за возникающими на кабеле сигналами. Если передаваемые и наблюдаемые сигналы отличаются, то фиксируется обнаружение коллизии (collision detection, CD). Для увеличения вероятности немедленного обнаружения коллизии всеми станциями сети, ситуация коллизии усиливается посылкой в сеть станциями, начавшими передачу своих кадров, специальной последовательности битов, которая называется jam-последовательностью.

После обнаружения коллизии передающая станция обязана прекратить передачу и ожидать в течение короткого случайного интервала времени, а затем может снова сделать попытку передачи кадра. Из описания метода доступа видно, что он носит вероятностный характер, и вероятность успешного получения в свое рас-

поряжение общей среды зависит от загруженности сети, то есть от интенсивности возникновения в станциях потребности передачи кадров. При разработке этого метода предполагалось, что скорость передачи данных в 10 Мб/с очень высока по сравнению с потребностями компьютеров во взаимном обмене данными, поэтому загрузка сети будет всегда небольшой.

Метод CSMA/CD определяет основные временные и логические соотношения, гарантирующие корректную работу всех станций в сети:

- Между двумя последовательно передаваемыми по общей шине кадрами информации должна выдерживаться пауза в 9.6 мкс; эта пауза нужна для приведения в исходное состояние сетевых адаптеров узлов, а также для предотвращения монопольного захвата среды передачи данных одной станцией.
- При обнаружении коллизии (условия ее обнаружения зависят от применяемой физической среды) станция выдает в среду специальную 32-х битную jam-последовательность, усиливающую явление коллизии для более надежного распознавания ее всеми узлами сети.
- После обнаружения коллизии каждый узел, который передавал кадр и столкнулся с коллизией, после некоторой задержки пытается повторно передать свой кадр. Узел делает максимально 16 попыток передачи этого кадра информации, после чего отказывается от его передачи. Величина задержки выбирается как равномерно распределенное случайное число из интервала, длина которого экспоненциально увеличивается с каждой попыткой. Такой алгоритм выбора величины задержки снижает вероятность коллизий и уменьшает интенсивность выдачи кадров в сеть при ее высокой загрузке.

Четкое распознавание коллизий всеми станциями сети является необходимым условием корректной работы сети Ethernet. Если какая-либо передающая станция не распознает коллизию и решит, что кадр данных ею передан верно, то этот кадр данных будет утерян, так как информация кадра исказится из-за наложения сигналов при коллизии, он будет отбракован принимающей станцией (из-за несовпадения контрольной суммы). Конечно, искаженная информация будет повторно передана каким-либо протоколом верхнего уровня, например, транспортным или прикладным, работающим с установлением соединения и нумерацией своих сообщений. Но по-

вторная передача сообщения протоколами верхних уровней произойдет через гораздо более длительный интервал времени (десятки секунд) по сравнению с микросекундными интервалами, которыми оперирует протокол Ethernet. Поэтому, если коллизии не будут надежно распознаваться узлами сети Ethernet, то это приведет к заметному снижению полезной пропускной способности данной сети.

Все параметры протокола Ethernet подобраны таким образом, чтобы при нормальной работе узлов сети коллизии всегда четко распознавались. Именно для этого минимальная длина поля данных кадра должна быть не менее 46 байт (что вместе со служебными полями дает минимальную длину кадра в 72 байта или 576 бит). Длина кабельной системы выбирается таким образом, чтобы за время передачи кадра минимальной длины сигнал коллизии успел бы распространиться до самого дальнего узла сети. Поэтому для скорости передачи данных 10 Мб/с, используемой в стандартах Ethernet, максимальное расстояние между двумя любыми узлами сети не должно превышать 2500 метров.

С увеличением скорости передачи кадров, что имеет место в новых стандартах, базирующихся на том же методе доступа CSMA/CD, например, Fast Ethernet, максимальная длина сети уменьшается пропорционально увеличению скорости передачи. В стандарте Fast Ethernet она составляет 210 м, а в гигабитном Ethernet ограничена 25 метрами.

Независимо от реализации физической среды, все сети Ethernet должны удовлетворять двум ограничениям, связанным с методом доступа:

- максимальное расстояние между двумя любыми узлами не должно превышать 2500 м,
- в сети не должно быть более 1024 узлов.

Кроме того, каждый вариант физической среды добавляет к этим ограничениям свои ограничения, которые также должны выполняться.

Станция, которая хочет передать кадр, должна сначала с помощью MAC-узла упаковать данные в кадр соответствующего формата. Затем для предотвращения смешения сигналов с сигналами другой передающей станции, MAC-узел должен прослушивать электрические сигналы на кабеле и в случае обнаружения несущей частоты 10 МГц отложить передачу своего кадра. После

окончания передачи по кабелю станция должна выждать небольшую дополнительную паузу, называемую межкадровым интервалом (interframe gap), что позволяет узлу назначения принять и обработать передаваемый кадр, и после этого начать передачу своего кадра.

Одновременно с передачей битов кадра приемно-передающее устройство узла следит за принимаемыми по общему кабелю битами, чтобы вовремя обнаружить коллизию. Если коллизия не обнаружена, то передается весь кадр, поле чего MAC-уровень узла готов принять кадр из сети либо от LLC-уровня.

Если же фиксируется коллизия, то MAC-узел прекращает передачу кадра и посылает jam-последовательность, усиливающую состояние коллизии. После посылки в сеть jam-последовательности MAC-узел делает случайную паузу и повторно пытается передать свой кадр.

В случае повторных коллизий существует максимально возможное число попыток повторной передачи кадра (attempt limit), которое равно 16. При достижении этого предела фиксируется ошибка передачи кадра, сообщение о которой передается протоколу верхнего уровня.

Для того, чтобы уменьшить интенсивность коллизий, каждый MAC-узел с каждой новой попыткой случайным образом увеличивает длительность паузы между попытками. Временное расписание длительности паузы определяется на основе усеченного двоичного экспоненциального алгоритма отсрочки (truncated binary exponential backoff). Пауза всегда составляет целое число так называемых интервалов отсрочки.

Интервал отсрочки (slot time) - это время, в течение которого станция гарантированно может узнать, что в сети нет коллизии. Это время тесно связано с другим важным временным параметром сети - окном коллизий (collision window). Окно коллизий равно времени двукратного прохождения сигнала между самыми удаленными узлами сети - наихудшему случаю задержки, при которой станция еще может обнаружить, что произошла коллизия. Интервал отсрочки выбирается равным величине окна коллизий плюс некоторая дополнительная величина задержки для гарантии:

интервал отсрочки = окно коллизий + дополнительная задержка

В стандартах 802.3 большинство временных интервалов измеряется в количестве межбитовых интервалов, величина которых

для битовой скорости 10 Мб/с составляет 0.1 мкс и равна времени передачи одного бита.

Величина интервала отсрочки в стандарте 802.3 определена равной 512 битовым интервалам, и эта величина рассчитана для максимальной длины коаксиального кабеля в 2.5 км. Величина 512 определяет и минимальную длину кадра в 64 байта, так как при кадрах меньшей длины станция может передать кадр и не успеть заметить факт возникновения коллизии из-за того, что искаженные коллизией сигналы дойдут до станции в наихудшем случае после завершения передачи. Такой кадр будет просто потерян.

Время паузы после N-ой коллизии полагается равным L интервалам отсрочки, где L - случайное целое число, равномерно распределенное в диапазоне [0, 2N]. Величина диапазона растет только до 10 попытки (напомним, что их не может быть больше 16), а далее диапазон остается равным [0, 210], то есть [0, 1024]. Значения основных параметров процедуры передачи кадра стандарта 802.3 приведены в таблице 1.1.

Таблица 1.1. Основные параметры кадра

Битовая скорость	10 Мб/с
Интервал отсрочки	512 битовых интервалов
Межкадровый интервал	9.6 мкс
Максимальное число попыток передачи	16
Максимальное число возрастания диапазона паузы	10
Длина jam-последовательности	32 бита
Максимальная длина кадра (без преамбулы)	1518 байтов
Минимальная длина кадра (без преамбулы)	64 байта (512 бит)
Длина преамбулы	64 бита

Учитывая приведенные параметры, нетрудно рассчитать максимальную производительность сегмента Ethernet в таких

единицах, как число переданных пакетов минимальной длины в секунду (packets-per-second, pps). Количество обрабатываемых пакетов Ethernet в секунду часто используется при указании внутренней производительности мостов и маршрутизаторов, вносящих дополнительные задержки при обмене между узлами. Поэтому интересно знать чистую максимальную производительность сегмента Ethernet в идеальном случае, когда на кабеле нет коллизий и нет дополнительных задержек, вносимых мостами и маршрутизаторами.

Так как размер пакета минимальной длины вместе с преамбулой составляет 64+8 = 72 байта или 576 битов, то на его передачу затрачивается 57.6 мкс. С учетом межкадрового интервала в 9.6 мкс период следования минимальных пакетов равен 67.2 мкс. Это соответствует максимально возможной пропускной способности сегмента Ethernet в 14880 п/с.

Маркерный метод доступа. Сети с маркерным доступом обычно более медленные, но они дают более предсказуемыми свойствами, чем конкурентные. По мере роста числа пользователей у сетей с маркерным доступом параметры ухудшаются медленнее, чем у конкурентных сетей. Эффективность сети зависит от величины потока сообщений, который необязательно связан с числом активных рабочих станций. По конкурентной схеме, когда много рабочих станций одновременно пытаются переслать данные, возникают наложения.

Таким образом, если большая часть обработки данных в сети выполняется локально (например, если рабочие станции заняты, главным образом, локальной подготовкой текстов), эффективность сети остается высокой, даже если к сети подключено много пользователей.

При схеме с маркерным доступом эффективность непосредственно определяем числом активных рабочих станций, а не полным потоком сообщений, передаваемым по сети. Каждый дополнительный пользователь добавляет еще один адрес, по которому будет передан маркер независимо от того, нуждается или нет рабочая станция в пересылке сообщения. Алгоритм доступа к среде иллюстрируется временной диаграммой (рис.1.2.).

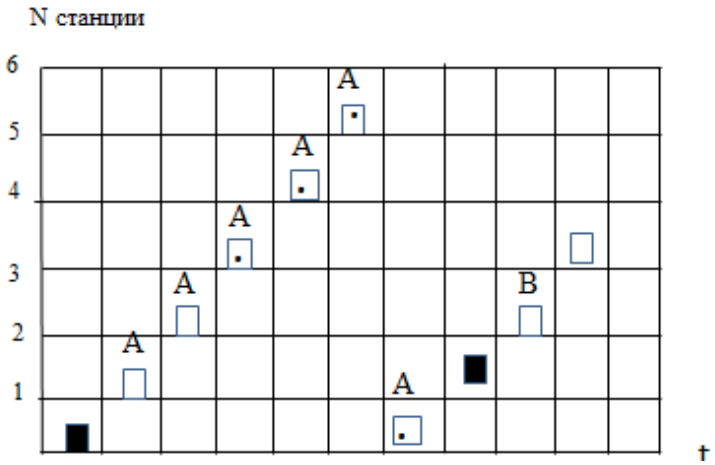

Рис.1.2. Алгоритм доступа к среде с маркерным доступом

Здесь показана передача пакета А в кольце, состоящем из 6 станций, от станции 1 к станции 3. После прохождения станции назначения 3 в пакете А устанавливаются два признака - признак распознавания адреса и признак копирования пакета в буфер (что на рисунке отмечено звездочкой внутри пакета). После возвращения пакета в станцию 1 отправитель распознает свой пакет по адресу источника и удаляет пакет из кольца. Установленные станцией 3 признаки говорят станции — отправителю о том, что пакет дошел до адресата и был успешно скопирован им в свой буфер.

Сеть Ethernet использует для управления передачей данных по сети конкурентную схему. Элементы сети Ethernet могут быть соединены по шинной или звездной топологии с использованием витых пар, коаксиальных или волоконно-оптических кабелей.

Основным преимуществом сетей Ethernet является их быстродействие. Обладая скоростью передачи от 10 до 100 Мбит/с, Ethernet является одной из самых быстрых среди существующих локальных сетей. Однако такое быстродействие, в свою очередь, вызывает определенные проблемы: из-за того, что предельные возможности тонкого медного кабеля лишь незначительно превышают указанную скорость передачи в 10 Мбит/с, даже небольшие электромагнитные помехи могут значительно ухудшить производительность сети.

Как показывает их наименование, сети Token Ring используют для передачи данных схему с маркерным доступом. Сеть Token Ring физически выполнена по схеме «звезда», но ведет себя как кольцевая. Другими словами, пакеты данных передаются с одной рабочей станции на другую последовательно (как в кольцевой

сети), но постоянно проходят через центральный компьютер (как в сетях типа «звезда»). Сети Token Ring могут осуществлять передачу как по незащищенным и защищенным витым проводным парам, так и по волоконно-оптическим кабелям.

Сети Token Ring существуют в двух версиях: со скоростью передачи в 4 и в 16 Мбит/с. Однако, хотя отдельные сети работают на скоростях либо 4, либо 16 Мбит/с, возможно соединение через мосты сетей с разными скоростями передачи. Сети Token Ring надежны, обладают высокой скоростью (особенно версия со скоростью передачи 16 Мбит/с) и просты для установки.

Сеть ARCnet использует схему с маркерным доступом и может работать как в шинной, так и в звездной топологии. Схема «звезда» обычно обеспечивает лучшую производительность, так как при этой топологии возникает меньше конфликта при передаче. ARCnet совместима с коаксиальными кабелями, витыми парами и волоконно-оптическими кабелями.

Системы ARCnet являются сравнительно медленными. Передача осуществляется на скорости лишь 2,5 Мбит/с, что значительно меньше, чем в других типах сетей. Несмотря на малое быстродействие, ARCnet сохраняет свою популярность. Ее маленькая скорость передачи является в своем роде компенсацией за эффективный метод передачи сигналов. ARCnet — сравнительно недорогая и гибкая система, которая легко устанавливается, расширяется и подвергается изменению конфигурации.

Выводы

В процессе передачи данных по сети задействованы: компьютер-источник, блок протокола, передатчик, физическая кабельная сеть, приемник, компьютер-адресат.

В сетях для соединения абонентов используются три метода коммутации: коммутация каналов, коммутация пакетов и коммутация сообщений.

В сетях с коммутацией каналов абонентов соединяет составной канал, образуемый коммутаторами сети по запросу одного из абонентов.

Для совместного разделения каналов между коммутаторами сети несколькими абонентскими каналами используются две технологии: частотного разделения канала (FDM) и разделения канала во времени (TDM). Частотное разделение характерно для аналого-

вой модуляции сигналов, а временное - для цифрового кодирования.

Сети с коммутацией каналов хорошо коммутируют потоки данных постоянной интенсивности, например потоки данных, создаваемые разговаривающими по телефону собеседниками, но не могут перераспределять пропускную способность магистральных каналов между потоками абонентских каналов динамически.

Сети с коммутацией пакетов были специально разработаны для эффективной передачи пульсирующего компьютерного трафика. Буферизация пакетов разных абонентов в коммутаторах позволяет сгладить неравномерности интенсивности трафика каждого абонента и равномерно загрузить каналы связи между коммутаторами.

Сети с коммутацией пакетов эффективно работают в том отношении, что объем передаваемых данных от всех абонентов сети в единицу времени больше, чем при использовании сети с коммутацией каналов. Однако для каждой пары абонентов пропускная способность сети может оказаться ниже, чем у сети с коммутацией каналов, за счет очередей пакетов в коммутаторах.

Сети с коммутацией пакетов могут работать в одном из двух режимов: дейтаграммном режиме или режиме виртуальных каналов.

В дейтаграммных протоколах отсутствует процедура предварительного установления соединения. Поэтому срочные данные отправляются в сеть без задержек.

Протоколы с установлением соединения могут обладать многими дополнительными свойствами, отсутствующими у дейтаграммных протоколов. Наиболее часто в них реализуется такое свойство, как способность восстанавливать искаженные и потерянные кадры.

Размер пакета существенно влияет на производительность сети. Обычно пакеты в сетях имеют максимальный размер в 1-4 Кбайт.

Коммутация сообщений предназначена для организации взаимодействия пользователей в режиме off-line, когда не ожидается немедленной реакции на сообщение. При этом методе коммутации сообщение передается через несколько транзитных компьютеров, где оно целиком буферизуется на диске.

Наиболее часто применяются два метода доступа в сеть: конкурентный (Ethernet) и маркерный доступ (Token Ring, Arcnet).

1.4. Вопросы и упражнения

1. Могут ли цифровые линии связи передавать аналоговые данные?
2. Определите пропускную способность канала связи для каждого из направлений дуплексного режима, если известно, что его полоса пропускания равна 600 кГц, а в методе кодирования используется 10 состояний сигнала.
3. Рассчитайте задержку распространения сигнала и задержку передачи данных для случая передачи пакета в 128 байт:
   - по кабелю витой пары длиной в 100 м при скорости передачи 100 Мбит/с;
   - коаксиальному кабелю длиной в 2 км при скорости передачи в 10 Мбит
4. Поясните, из каких соображений выбрана пропускная способность 64 Кбит/с элементарного канала цифровых телефонных сетей?
5. Сеть с коммутацией пакетов испытывает перегрузку. Для устранения этой ситуации размер окна в протоколах компьютеров сети нужно увеличить или уменьшить?
6. Как влияет надежность линий связи в сети на выбор размера окна?
7. В чем проявляется избыточность TDM-технологии?
8. Какой способ коммутации более эффективен: коммутация каналов или коммутация пакетов?
9. Объясните разницу между тремя понятиями:
   - логические соединения, на которых основаны некоторые протоколы;
   - виртуальные каналы в сетях с коммутацией пакетов;
   - составные каналы в сетях с коммутацией каналов.

ГЛАВА 2. ПОСТРОЕНИЕ ЛОКАЛЬНЫХ СЕТЕЙ НА КОММУТАТОРАХ

В целях повышения эффективности реализации комплексных программ по внедрению современных IT технологий в Узбекистане уделяется большое внимание проектированию и практическому внедрению оптимальных компьютерных сетей предприятия на коммутаторах, что позволит оптимизировать основные сетевые характеристики: пропускная способность, производительность, стоимость, временные задержки и топологическая реализация каналов связи.

2.1. Принципы работы коммутаторов локальной сети

Коммутатор (свитч) – основное устройство активного типа, применяемое в качестве центрального узла для подключения компьютеров в сетях, основанных на топологии «звезда»[9].

Функциональности коммутатор обязан протоколам, работающим на канальном уровне. Это позволяет избежать лишнего трафика, когда необходимо передать данные от отправителя конкретному компьютеру, не затрагивая при этом остальные компьютеры. За счет этого достигается высокая скорость передачи данных.

Коммутатор представляет собой достаточно интеллектуальное устройство, которое способно обучаться. Он использует MAC-адреса устройств, причем эти адреса коммутатор запоминает. Например, когда компьютер передает данные другому компьютеру, коммутатор запоминает MAC-адрес отправителя и отправляет данные сразу на все порты, то есть работает как концентратор. Однако это происходит только на первых порах. Как только коммутатор сможет определить MAC – адрес каждого компьютера, подключенного к его портам, данные сразу же будут отправляться на конкретный порт, тем самым уменьшая время доставки, а значит, увеличивая скорость передачи данных.

Коммутаторы – устройства канального уровня, соединяющие несколько физических сегментов локальной сети в одну большую сеть (см. рис.2.1.).

[9] Руководство пользователя. Коммутаторы локальных сетей D-Link. Учебное пособие 2004 г. 89 с.

Коммутация локальных сетей обеспечивает взаимодействие сетевых устройств по выделенной линии без возникновения коллизий, с параллельной передачей нескольких потоков данных путем одновременного соединений между разными парами портов коммутатора.

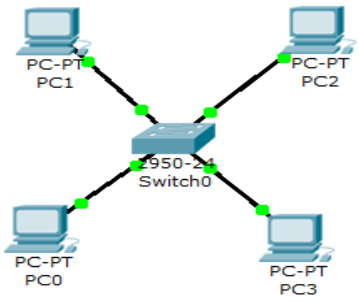

Рис. 2.1.Коммутатор локальной сети

При передаче пакета через коммутатор в нем создается отдельный виртуальный канал, по которому данные пересылаются напрямую от порта-источника к порту – получателю с максимально возможной для используемой технологии скоростью (рис.2.2.). Такой принцип работы получил название «микросегментация», коммутаторы получили возможность функционировать в режиме полного дуплекса (full duplex).

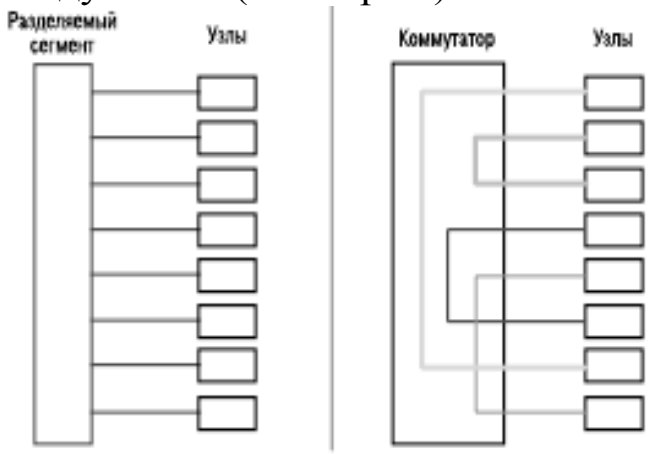

Рис. 2.2. Микросегментация

Это позволяет каждой рабочей станции одновременно передавать и принимать данные, используя всю полосу пропускания в обоих направлениях. Рабочей станции не конкурирует за полосу

пропускания с другими устройствами, в результате чего не происходит коллизия и повышается производительность сети.

Коммутаторы локальных сетей обрабатывают кадры на основе алгоритма прозрачного моста (transparent bridge), который определен стандартом IEEE 802.1D. Процесс работы алгоритма прозрачного моста начинается с построения таблицы коммутации (Forwarding DataBase). При включении питания коммутатор начинает изучать расположение рабочих станций всех присоединенных к нему сетей путем анализа MAC-адресов источников входящих кадров. Например, если на порт 1 коммутатора поступает кадр от узла 1, то он запоминает номер порта, на который этот кадр пришел и добавляет эту информацию в таблицу коммутации (forwarding database). Адреса изучаются динамически. Это означает, что, как только будет прочитан новый адрес, то он сразу будет занесен в контентно-адресуемую память (content-addressable memory, CAM). Каждый раз, при занесении адреса в таблицу коммутации, ему присваивается временной штамп. Это позволяет хранить адреса в таблице в течение определенного времени.

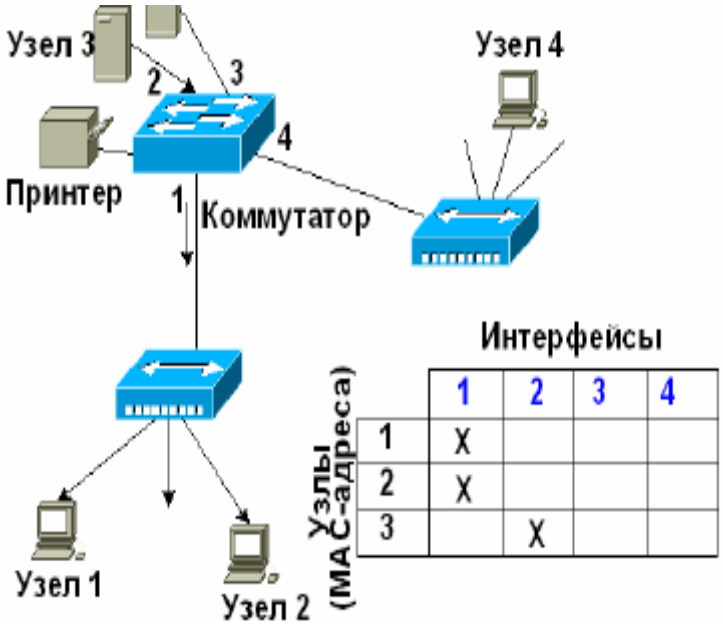

Рис.2.3. Построение таблицы коммутации

Каждый раз, когда идет обращение по этому адресу, он получает новый временной штамп. Адреса, по которым не обращались долгое время, из таблицы удаляются (рис. 2.3.).

Коммутатор использует таблицу коммутации для пересылки трафика. Когда на один из его портов поступает пакет дан-

ных, он извлекает из него информацию о MAC-адресе приемника с поиском этого MAC-адреса в своей таблице коммутации. При обнаружении в таблице записи MAC-адреса на одном из портов коммутатора, кадр пересылается через этот порт. Если такой ассоциации нет, кадр передается через все порты, за исключением того, на который он поступил. Это называется лавинным распространением (flooding), что является одной из проблем, ограничивающая применение коммутаторов. В случае, если в результате каких-либо программных или аппаратных сбоев протокол верхнего уровня или сам сетевой адаптер начнет работать не правильно, и будет постоянно генерировать широковещательные кадры, коммутатор в этом случае будет передавать кадры во все сегменты, затапливая сеть ошибочным трафиком.

Такая ситуация называется широковещательным штормом (broadcast storm). Коммутаторы надежно изолируют межсегментный трафик, уменьшая таким образом трафик отдельных сегментов. Этот процесс называется фильтрацией (filtering) и выполняется в случаях, когда MAC-адреса источника и приемника принадлежат одному сегменту. Обычно фильтрация повышает скорость отклика сети, ощущаемую пользователем.

Коммутаторы локальных сетей поддерживают два режима работы: полудуплексный режим и дуплексный режим.

Полудуплексный режим – это режим, при котором, только одно устройство может передавать данные в любой момент времени в одном домене коллизий.

Дуплексный режим – это режим работы, который обеспечивает одновременную двухстороннюю передачу данных между станцией-отправителем и станцией-получателем на MAC - подуровне. При работе в дуплексном режиме, между сетевыми устройствами повышается количество передаваемой информации. Это связано с тем, что дуплексная передача не вызывает в среде передачи коллизий, не требует составления расписания повторных передач и добавления битов расширения в конец коротких кадров. В результате не только увеличивается время, доступное для передачи данных, но и удваивается полезная полоса пропускания канала, поскольку каждый канал обеспечивает полноскоростную одновременную двустороннюю передачу.

Дуплексный режим работы требует наличия такой дополнительной функции, как управление потоком. Она позволяет принимающему узлу (например, порту сетевого коммутатора) в случае переполнения дать узлу-источнику команду (например, файловому серверу) приостановить передачу кадров на некоторый короткий промежуток времени. Управление осуществляется между MAC-уровнями с помощью кадра-паузы, который автоматически формируется принимающим MAC уровнем. Если переполнение будет ликвидировано до истечения периода ожидания, то для того, чтобы восстановить передачу, отправляется второй кадр-пауза с нулевым значением времени ожидания (см. рис. 2.4.).

Рис.2.4. Последовательность управления потоком IEEE 802.3x

Дуплексный режим работы и сопутствующее ему управление потоком являются дополнительными режимами для всех MAC-уровней Ethernet независимо от скорости передачи.

Дуплексный режим работы и сопутствующее ему управление потоком являются дополнительными режимами для всех MAC-уровней Ethernet независимо от скорости передачи.

Кадры-паузы идентифицируются, как управляющие MAC-кадры по индивидуальным (зарезервированным) значениям поля длины/типа. Им также присваивается зарезервированное значение адреса приемника, чтобы исключить возможность передачи входящего кадра-паузы протоколам верхних уровней или на другие порты коммутатора.

2.2. Технологии коммутации

Коммутаторы локальных сетей можно классифицировать в соответствии с уровнями модели OSI, на которых они передают, фильтруют и коммутируют кадры[10]. Различают коммутаторы уровня 2 (Layer 2 Switch), коммутаторы уровня 2 со свойствами уровня 3 (Layer 3 Switch) и многоуровневые коммутаторы.

Коммутаторы уровня 2 анализируют входящие кадры, принимают решение об их дальнейшей передаче и передают их пунктам назначения на основе MAC – адресов канального уровня модели OSI. Основное преимущество коммутаторов уровня 2 – прозрачность для протоколов верхнего уровня. Поскольку коммутатор функционирует на 2-м уровне, ему нет необходимости анализировать информацию верхних уровней модели OSI.

Коммутация 2-го уровня – аппаратная. Она обладает высокой производительностью, поскольку пакет данных не претерпевает изменений. Передача кадра в коммутаторе может осуществляться специализированным контроллером, называемым Application-Specific Integrated Circuits (ASIC). Эта технология, разработанная для коммутаторов, позволяет обеспечивать высокие скорости коммутации с минимальными задержками. Существуют 2 основные причины использования коммутаторов 2-го уровня – сегментация сети и объединение рабочих групп. Высокая производительность коммутаторов позволяет разработчикам сетей значительно уменьшить количество узлов в физическом сегменте. Деление крупной сети на логические сегменты повышает производительность сети (за счет уменьшения объема передаваемых данных в отдельных сегментах), а также гибкость построения сети, увеличивая степень защиты данных, и облегчает управление сетью.

Несмотря на преимущества коммутации 2-го уровня, она все же имеет некоторые ограничения. Наличие коммутаторов в сети не препятствует распространению широковещательных кадров (broadcast) по всем сегментам сети, сохраняя ее прозрачность.

---

[10] Kubilinskas E. Designing Resilient and Fair Multi-layer Telecommunication Networks. / Kubilinskas E. – Lund Institute of Technology, 2005

Таким образом, очевидно, что для повышения производительности сети необходима функциональность 3-го уровня OSI модели. Коммутатор локальной сети уровня 2 с функциями уровня 3 (или коммутатор 3-го уровня) принимает решение о коммутации на основании большего количества информации, чем просто MAC-адрес.

Коммутаторы 3-го уровня осуществляют коммутацию и фильтрацию на основе адресов канального (уровень 2) и сетевого (уровень 3) уровней OSI модели. Такие коммутаторы динамически решают, коммутировать (уровень 2) или маршрутизировать (уровень 3) входящий трафик. Коммутаторы 3 уровня выполняет коммутацию в пределах рабочей группы и маршрутизацию между рабочими группами.

Коммутаторы 3-го уровня выполняют функции:

• определение оптимальных путей передачи данных на основе логических адресов (адресов сетевого уровня, традиционно IP-адресов);
• управление широковещательным и многоадресным трафиком;
• фильтрация трафика на основе информации 3-го уровня;
• IP- фрагментация.

Основное отличие между маршрутизаторами и коммутаторами 3-го уровня заключается в том, что в маршрутизаторах общего назначения

принятие решения о пересылке пакетов обычно выполняется программным образом, а в коммутаторах обрабатывается специализированными контроллерами ASIC. Это позволяет коммутаторам выполнять маршрутизацию пакетов на скорости канала связи.

Коммутация 4-го уровня считается технологией аппаратной коммутации уровня 3, которая может учитывать используемое приложение (Telnet или FTP), а также используют номера портов, находящиеся в заголовке транспортного уровня при создании списков доступа для фильтрации данных протоколов верхнего уровня, программ и приложений.

Многоуровневые коммутаторы сочетают в себе технологии коммутации уровней 2, 3 и 4. Принятие решения о передаче данных осуществляется в таких коммутаторах на основе следующей информации:

• MAC - адресе источника/приемника кадра данных;

• IP-адресе источника/приемника из заголовка сетевого (3-го) уровня;
• типа протокола в заголовке сетевого уровня;
• номера порта источника/приемника в заголовке транспортного уровня.

Коммутаторы высокого класса должны обеспечивать высокую производительность и плотность портов, а также поддерживать широкий спектр функций управления. Такие устройства зачастую кроме традиционной коммутации на MAC-уровне выполняют функции маршрутизации. Коммутаторы, реализующие также функции сетевого уровня (маршрутизацию), оснащены, как правило, RISC-процессорами для выполнения ресурсоемких программ маршрутизации.

Контроллеры ASIC для коммутаторов ЛС делятся на 2 класса – большие ASIC, способные обслуживать множество коммутируемых портов (один контроллер на устройство) и небольшие контроллеры ASIC, обслуживающие несколько портов и объединяемые в матрицы коммутации.

Существует 3 варианта архитектуры коммутаторов:
• на основе коммутационной матрицы (cross-bar);
• с разделяемой многовходовой памятью (shared memory);
• на основе общей высокоскоростной шины.

Часто эти три способа взаимодействия комбинируются в одном коммутаторе.

Коммутационная матрица (cross-bar) - основной и самый быстрый способ взаимодействия процессоров портов. Однако, реализация матрицы возможна только для определенного числа портов, причем сложность схемы возрастает пропорционально квадрату количества портов коммутатора.

В любой момент такой коммутатор может обеспечить организацию только одного соединения (пара портов). При невысоком уровне трафика не требуется хранение данных в памяти перед отправкой в порт назначения. Однако, коммутаторы cross-bar требуют буферизации на входе от каждого порта, поскольку в случае использования единственного возможного соединения коммутатор блокируется.

Коммутационная матрица работает по принципу коммутации каналов. При поступлении кадра в какой-либо порт процессор EPP (Ethernet Packet Processor) буферизует несколько первых байт

кадра, чтобы прочитать адрес назначения. После получения адреса назначения процессор сразу же принимает решение о передаче пакета, не дожидаясь прихода остальных байт кадра. Для этого он просматривает свой собственный кэш адресной таблицы, а если не находит там нужного адреса, обращается к системному модулю, который работает в многозадачном режиме, параллельно обслуживая запросы всех процессоров EPP.

Системный модуль производит просмотр общей адресной таблицы и возвращает процессору найденную строку, которую тот буферизует в своем кэше для последующего использования. После нахождения адреса назначения процессор EPP знает, что нужно дальше делать с поступающим кадром (во время просмотра адресной таблицы процессор продолжал буферизацию поступающих в порт байтов кадра). Если кадр нужно отфильтровать, процессор просто прекращает записывать в буфер байты кадра, очищает буфер и ждет поступления нового кадра. Если же кадр нужно передать на другой порт, то процессор обращается к коммутационной матрице и пытается установить в ней путь, связывающий его порт с портом, через который идет
маршрут к адресу назначения.

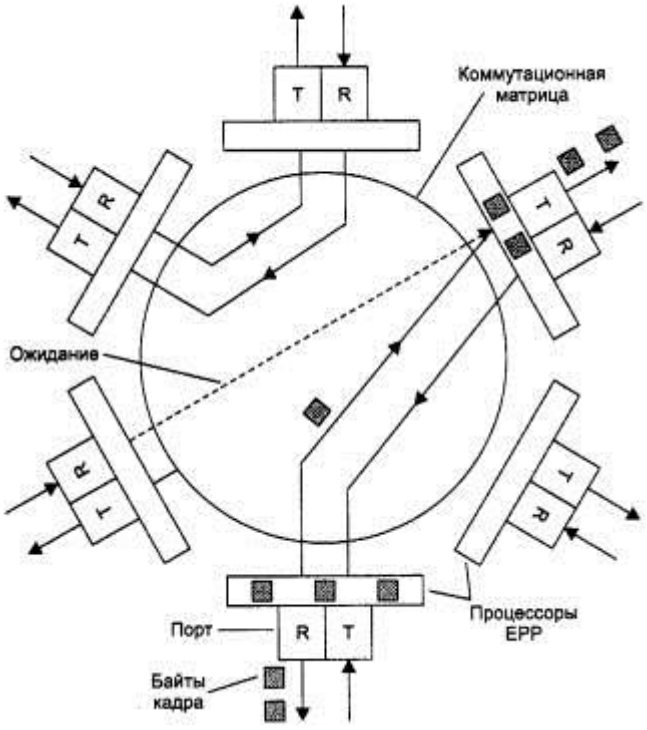

Рис.2.5. Передача кадра через коммутационную матрицу

Коммутационная матрица может это сделать только в том случае, когда порт адреса назначения в этот момент свободен, то есть

не соединен с другим портом. Если же порт занят, то, как и в любом устройстве с коммутацией каналов, матрица в соединении отказывает. В этом случае кадр полностью буферизуется процессором входного порта, после чего процессор ожидает освобождения выходного порта и образования коммутационной матрицей нужного пути (см. рис.2.5.).

После того как нужный путь установлен, в него направляются буферизованные байты кадра, которые принимаются процессором выходного порта. Как только процессор выходного порта получает доступ к подключенному к нему сегменту Ethernet по алгоритму CSMA/CD, байты кадра сразу же начинают передаваться в сеть. Процессор входного порта постоянно хранит несколько байт принимаемого кадра в своем буфере, что позволяет ему независимо и асинхронно принимать и передавать байты кадра.

Коммутаторы с разделяемой памятью (shared memory switch) имеют общий входной буфер для всех портов. Буферизация данных перед их рассылкой приводит к возникновению задержки. Однако, коммутаторы с разделяемой памятью, как показано на рисунке 5 не требуют организации специальной внутренней магистрали для передачи данных между портами, что обеспечивает им более низкую цену по сравнению с коммутаторами на базе высокоскоростной внутренней шины.

Коммутаторы с общей шиной (backplane) используют для связи процессоров портов высокоскоростную шину, используемую в режиме разделения времени. После того, как данные преобразуются в приемлемый для передачи по шине формат, они помещаются на шину и далее передаются в порт назначения.

Для того чтобы шина не была узким местом коммутатора, ее производительность должна быть выше скорости поступления данных во входные блоки процессоров портов.

$$\sum_{i}^{N} C_i \times 2 \text{ Мбит/с} \qquad (2.1.)$$

где: N – количество портов, Cpi - максимальная производительность протокола, поддерживаемого i-м портом коммутатора. Кроме этого, кадр должен передаваться по шине небольшими частями, по несколько байт, чтобы передача кадров между несколькими портами происходила в псевдопараллельном режиме, не внося задержек в передачу кадра в целом. Размер такой ячейки дан-

ных определяется производителем коммутатора. Поскольку шина может обеспечивать одновременную передачу потока данных от всех портов, такие коммутаторы часто называют «неблокируемыми» (non-blocking) - они не создают пробок на пути передачи данных.

2.3. Характеристики коммутаторов

Производительность коммутатора – характеристика, на которую сетевые интеграторы и опытные администраторы обращают внимание в первую очередь при выборе устройства.

Основными показателями коммутатора, характеризующими его производительность, являются[11]:

- скорость фильтрации кадров;
- скорость продвижения кадров;
- пропускная способность;
- задержка передачи кадра.

Несколько характеристик коммутатора, которые в наибольшей степени влияют на указанные характеристики производительности:

- тип коммутации;
- размер буфера (буферов) кадров;
- производительность внутренней шины;
- производительность процессора или процессоров;
- размер внутренней адресной таблицы.

Скорость фильтрации и скорость продвижения. Скорость фильтрации и продвижения кадров - это две основные характеристики производительности коммутатора. Эти характеристики являются интегральными показателями и не зависят от технической реализации коммутатора.

Скорость фильтрации (filtering) определяет скорость, с которой
коммутатор выполняет следующие этапы обработки кадров:

- прием кадра в свой буфер;
- просмотр адресной таблицы с целью нахождения порта для адреса назначения кадра;

[11] Руководство пользователя. Коммутаторы локальных сетей D-Link. Учебное пособие 2004 г. 89 с.

• уничтожение кадра, если его порт назначения и порт источника принадлежат одному логическому сегменту;
• Скорость фильтрации практически у всех коммутаторов является неблокирующей - коммутатор успевает отбрасывать кадры в темпе их поступления.

Скорость продвижения (forwarding) определяет скорость, с которой коммутатор выполняет следующие этапы обработки кадров:
• прием кадра в свой буфер;
• просмотр адресной таблицы с целью нахождения порта для адреса назначения кадра;
• передача кадра в сеть через найденный по адресной таблице порт назначения.

Как скорость фильтрации, так и скорость продвижения измеряется обычно в кадрах в секунду. Если в характеристиках коммутатора не уточняется, для какого протокола и для какого размера кадра приведены значения скоростей фильтрации и продвижения, то по умолчанию считается, что эти показатели даются для протокола Ethernet и кадров минимального размера, то есть кадров длиной 64 байт (без преамбулы) с полем данных в 46 байт. Применение в качестве основного показателя скорости обработки коммутатором кадров минимальной длины объясняется тем, что такие кадры всегда создают для коммутатора наиболее тяжелый режим работы по сравнению с кадрами другого формата при равной пропускной способности передаваемых пользовательских данных. Поэтому при проведении тестирования коммутатора режим передачи кадров минимальной длины используется как наиболее сложный тест, который должен проверить способность коммутатора работать при наихудшем сочетании параметров трафика.

Пропускная способность коммутатора это количество пользовательских данных (в мегабитах или гигабитах в секунду), которые передаются в единицу времени через его порты. Так как коммутатор работает на канальном уровне, для него пользовательскими данными являются те данные, которые переносятся в поле данных кадров протоколов канального уровня – Ethernet, Fast Ethernet и т.д. Максимальное значение пропускной способности коммутатора всегда достигается на кадрах максимальной длины, так как при этом доля накладных расходов на

служебную информацию кадра гораздо ниже, чем для кадров минимальной длины, а время выполнения коммутатором операций по обработке кадра, приходящееся на один байт пользовательской информации, существенно меньше. Поэтому коммутатор может быть блокирующим для кадров минимальной длины, но при этом иметь очень хорошие показатели пропускной способности.

Задержка передачи кадра измеряется как время, прошедшее с момента прихода первого байта кадра на входной порт коммутатора до момента появления этого байта на его выходном порту. Задержка складывается из времени, затрачиваемого на буферизацию байт кадра, а также времени, затрачиваемого на обработку кадра коммутатором, - просмотра адресной таблицы, принятия решения о продвижении и получения доступа к среде выходного порта. Величина вносимой коммутатором задержки зависит от режима его работы. Если коммутация осуществляется без буферизации, то задержки обычно невелики и составляют от 5 до 40 мкс, а при полной буферизации кадров - от 50 до 200 мкс (для кадров минимальной длины).

Размер адресной таблицы. Максимальная емкость адресной таблицы определяет предельное количество MAC-адресов, с которыми может одновременно оперировать коммутатор. В таблице коммутации для каждого порта хранятся только те наборы адресов, с которыми он работал в последнее время. Значение максимального числа MAC - адресов, которое может храниться в таблице коммутации, зависит от области применения коммутатора, измеряется в тысячах записей, например 4К – 4 тысячи адресов. Коммутаторы D-Link для рабочих групп и малых офисов обычно поддерживают таблицу MAC адресов емкостью от 4К до 8К. Коммутаторы крупных рабочих групп поддерживают таблицу MAC адресов емкостью от 8К до 16К, а коммутаторы магистралей сетей – как правило, от 16К до 32 К адресов и более.

Недостаточная емкость адресной таблицы может служить причиной замедления работы коммутатора и засорения сети избыточным трафиком. Если адресная таблица коммутации полностью заполнена, а порт встречает новый адрес источника в поступившем пакете, коммутатор должен вытеснить из таблицы какой-либо старый адрес и поместить на его место новый. Эта операция сама по себе отнимет часть времени, но главные потери

производительности будут наблюдаться при поступлении кадра с адресом назначения, который пришлось удалить из адресной таблицы. Так как адрес назначения кадра неизвестен, то коммутатор должен передать этот кадр на все остальные порты. Эта операция будет создавать лишнюю работу для многих процессоров портов, кроме того, копии этого кадра будут попадать и на те сегменты сети, где они совсем не обязательны.

Объем буфера кадров. Внутренняя буферная память коммутатора нужна для временного хранения кадров данных в тех случаях, когда их невозможно немедленно передать на выходной порт. Буфер предназначен для сглаживания кратковременных пульсаций трафика. Например, трафик может в течение нескольких десятков миллисекунд поступать одновременно на все входы коммутатора, не давая ему возможности передавать принимаемые кадры на выходные порты.

При кратковременном многократном превышении среднего значения интенсивности трафика (для локальных сетей часто встречаются значения коэффициента пульсации трафика в диапазоне 50-100) возможны потери кадров. Одним из методов борьбы с этим служит буфер большого объема. Чем больше объем этой памяти, тем менее вероятны потери кадров при перегрузках. Другой метод – управление потоком (Flow control). Обычно коммутаторы, предназначенные для работы в ответственных частях сети, имеют буферную память в несколько десятков или сотен килобайт на порт. Дополнительным средством защиты может служить общий для всех портов буфер в модуле управления коммутатором. Такой буфер обычно имеет объем в несколько мегабайт.

Коммутация «на лету» или с буферизацией. Производительность коммутатора также зависит от способа передачи пакетов - «на лету» или с буферизацией. Коммутаторы, передающие пакеты «на лету», вносят меньшие задержки передачи кадров на каждом промежуточном коммутаторе, поэтому общее уменьшение задержки доставки данных может быть значительным, что является важным для мультимедийного трафика. Кроме того, выбранный способ коммутации оказывает влияние на возможности реализации некоторых полезных дополнительных функций, например трансляцию протоколов канального уровня. В табл. 2.2 дается сравнение возможностей двух способов коммутации.

Таблица 2.2. Сравнение способов коммутации

Функция	На лету	С буферизацией
Защита плохих кадров	Нет	Да
Поддержка разнородных сетей (Ethernet, Token Ring, FDDI, ATM	Нет	Да
Задержка передачи пакетов	Низкая (5-40 мкс, средняя при высокой нагрузке	
Поддержка резервных связей	Нет	Да
Функции анализа трафика	Нет	Да

Средняя величина задержки коммутаторов, работающих «на лету», при высокой нагрузке объясняется тем, что в этом случае выходной порт часто бывает занят приемом другого пакета, поэтому вновь поступивший пакет для данного порта все равно приходится буферизовать. Коммутатор, работающий «на лету», может выполнять проверку некорректности передаваемых кадров, но не может изъять плохой кадр из сети, так как часть его байт (и, как правило, большая часть) уже переданы в сеть.

Так как каждый способ имеет свои достоинства и недостатки, в тех моделях коммутаторов, которым нужно транслировать протоколы, иногда применяется механизм адаптивной смены режима работы коммутатора. Основной режим такого коммутатора - коммутация «на лету», но коммутатор постоянно контролирует трафик и при превышении интенсивности появления плохих кадров некоторого порога переходит на режим полной буферизации. Затем коммутатор может вернуться к коммутации «на лету».

Возможности коммутаторов по фильтрации трафика.

Многие коммутаторы позволяют администраторам задавать дополнительные условия фильтрации кадров. Пользовательские фильтры предназначены для создания дополнительных барьеров на пути кадров, которые ограничивают доступ определенных групп пользователей к определенным службам сети.

Наиболее простыми являются пользовательские фильтры на основе MAC – адресов станций. Так как MAC – адреса – это та информация, с которой работает коммутатор, то он позволяет задавать такие фильтры в удобной для администратора форме. При этом пользователю, работающему на компьютере с данным MAC -

адресом, полностью запрещается доступ к ресурсам другого сегмента сети.

Часто администратору требуется задать более тонкие условия фильтрации, например, запретить некоторому пользователю печатать свои документы на определенном сервере печати NetWare чужого сегмента, а остальные ресурсы этого сегмента сделать доступными. Для реализации такого фильтра нужно запретить передачу кадров с определенным MAC – адресом, в которых вложены пакеты IPX, в поле «номер сокета» которых будет указано значение, соответствующее службе печати NetWare.

Коммутаторы не анализируют протоколы верхних уровней, такие как IPX, поэтому администратору приходится для задания условий такой фильтрации вручную определять поле, по значению которого нужно осуществлять фильтрацию, в виде пары «смещение - размер» относительно начала поля данных кадра канального уровня, а затем еще указать в шестнадцатеричном формате значение этого поля для службы печати.

Обычно условия фильтрации записываются в виде булевых выражений, формируемых с помощью логических операторов AND и OR. Наложение дополнительных условий фильтрации может снизить производительность коммутатора, так как вычисление булевых выражений требует проведения дополнительных вычислений процессорами портов

Приоритетная обработка кадров. Построение сетей на основе коммутаторов позволяет использовать приоритетность обработки трафика независимо от технологии сети. Эта новая возможность является следствием того, что коммутаторы буферизуют кадры перед их отправкой на другой порт. Коммутатор обычно ведет для каждого входного и выходного порта не одну, а несколько очередей, причем каждая очередь имеет свой приоритет обработки. При этом коммутатор может быть сконфигурирован, например, так, чтобы передавать один низкоприоритетный пакет на каждые 10 высокоприоритетных пакетов.

Поддержка приоритетной обработки может использоваться для приложений, предъявляющих различные требования к допустимым задержкам кадров и к пропускной способности сети для потока кадров.

Более приоритетные кадры будут обрабатываться раньше менее приоритетных, поэтому все показатели качества обслуживания

у них будут выше, чем у менее приоритетных. Гарантии качества обслуживания дают другие схемы, которые основаны на предварительном резервировании качества обслуживания. Например, такие схемы используются в технологиях глобальных сетей frame relay и ATM или в протоколе RSVP для сетей TCP/IP. Основным вопросом при приоритетной обработке кадров коммутаторами является вопрос назначения кадру приоритета. Так как не все протоколы канального уровня поддерживают поле приоритета кадра, например у кадров Ethernet оно отсутствует, то коммутатор должен использовать какой-либо дополнительный механизм для связывания кадра с его приоритетом. Наиболее распространенный способ - приписывание приоритета портам коммутатора. При этом способе коммутатор помещает кадр в очередь кадров соответствующего приоритета в зависимости от того, через какой порт поступил кадр в коммутатор. Способ несложный, но недостаточно гибкий - если к порту коммутатора подключен не отдельный узел, а сегмент, то все узлы сегмента получают одинаковый приоритет.

Более гибким является назначение приоритетов кадрам в соответствии с достаточно новым стандартом IEEE 802.1p. Этот стандарт разрабатывался совместно со стандартом 802.10, который рассматривается в следующем разделе, посвященном виртуальным локальным сетям. В обоих стандартах предусмотрен общий дополнительный заголовок для кадров Ethernet, состоящий из двух байт. В этом дополнительном заголовке, который вставляется перед полем данных кадра, 3 бита используются для указания приоритета кадра. Существует протокол, по которому конечный узел может запросить у коммутатора один из восьми уровней приоритета кадра. Если сетевой адаптер не поддерживает стандарт 802.1p, то коммутатор может назначать приоритеты кадрам на основе порта поступления кадра. Такие помеченные кадры будут обслуживаться в соответствии с их приоритетом всеми коммутаторами сети, а не только тем коммутатором, который непосредственно принял кадр от конечного узла. При передаче кадра сетевому адаптеру, не поддерживающему стандарт 802.1p, дополнительный заголовок должен быть удален.

Программное обеспечение коммутаторов. Вторым компонентом коммутируемой межсетевой модели является программное обеспечение коммутаторов [18]. Программное обеспечение коммутаторов D-Link предоставляет полный набор программных сервисов, необходимых для выполнения в условиях современ-

ных сетей таких функций, как управление сетевой безопасностью, QoS и предоставление дополнительных сервисов, обеспечивающих отказоустойчивость сети. Кроме того, программное обеспечение коммутаторов взаимодействует с приложениями сетевого мониторинга и управления использующих протокол SNMP, например D-Link D-View. Эти управляющие программы поддерживаются всей линейкой управляемых коммутаторов D-Link.

Системное программное обеспечение располагается во Flash-памяти коммутатора, размер которой варьируется в зависимости от модели, обычно 8-16 Мб. Эта память может содержать несколько образов системного программного обеспечения, каждый из которых может быть выборочно загружен в устройство. Также во Flash-памяти хранится загрузочный модуль, отвечающий за первичное тестирование функциональных компонентов коммутатора после подачи питания, обеспечение загрузки и запуска исполняемого файла. Текущая конфигурация устройства хранится в энергонезависимой памяти NV-RAM, сохраняющей информацию при отключении питания.

Третий и последний компонент коммутируемой межсетевой модели – средства и приложения сетевого управления. Поскольку коммутаторы интегрированы в сеть, сетевое управление становится актуально как для рабочей группы, так и для магистрали сети.

2.4. Виртуальные локальные сети

Всем коммутируемым сетям присуще одно ограничение. Поскольку коммутатор является устройством канального уровня, он не может знать, куда направлять широковещательные пакеты протоколов сетевого уровня. Хотя трафик с конкретными адресами (соединения "точка-точка") изолирован парой портов, широковещательные пакеты передаются во всю сеть (на каждый порт). Широковещательные пакеты – это пакеты, передаваемые на все узлы сети. Они необходимы для работы многих сетевых протоколов, таких как ARP, BOOTP или DHCP, с их помощью рабочая станция оповещает другие компьютеры о своем появлении в сети, так же широковещательные пакеты могут возникать из-за некорректно работающего сетевого адаптера.

Широковещательные пакеты могут привести к насыщению полосы пропускания, особенно в крупных сетях. Для того, чтобы этого не происходило важно ограничить область распространения широковещательного трафика (эта область называется широковещательным доменом) - организовать небольшие широковещательные домены или виртуальные ЛВС (Virtual LAN, VLAN)[12].

Виртуальной сетью называется логическая группа узлов сети, трафик которой, в том числе и широковещательный, на канальном уровне полностью изолирован от других узлов сети. Это означает, что передача кадров между разными виртуальными сетями на основании MAC-адреса невозможна, независимо от типа адреса - уникального, группового или широковещательного. В то же время, внутри виртуальной сети кадры передаются по технологии коммутации, то есть только на тот порт, который связан с адресом назначения кадра. Таким образом, с помощью виртуальных сетей решается проблема распространения широковещательных пакетов и вызываемых ими следствий, которые могут развиться в широковещательные штормы и существенно снизить производительность сети.

VLAN обладают следующими преимуществами:

• Гибкость внедрения. VLAN являются эффективным способом группировки сетевых пользователей в виртуальные рабочие группы, несмотря на их физическое размещение в сети;

• VLAN обеспечивают возможность контроля широковещательных сообщений, что увеличивает полосу пропускания, доступную для пользователя;

• VLAN позволяют усилить безопасность сети, определив с помощью фильтров, настроенных на коммутаторе или маршрутизаторе, политику взаимодействия пользователей из разных виртуальных сетей.

В коммутаторах могут использоваться три типа VLAN:

• VLAN на базе портов;

• VLAN на базе MAC-адресов;

[12] Фортенбери Т. Проектирование виртуальных частных сетей в среде Windows 2000. Вильямс. [RUS,320.,2002].

• VLAN на основе меток в дополнительном поле кадра – стандарт IEEE 802.1Q.

При использовании VLAN на базе портов, каждый порт назначается в определенную VLAN, независимо от того, какой пользователь или компьютер подключен к этому порту. Это означает, что все пользователи, подключенные к этому порту, будут членами одной VLAN. Конфигурация портов статическая и может быть изменена только вручную (см. рис.2.6).

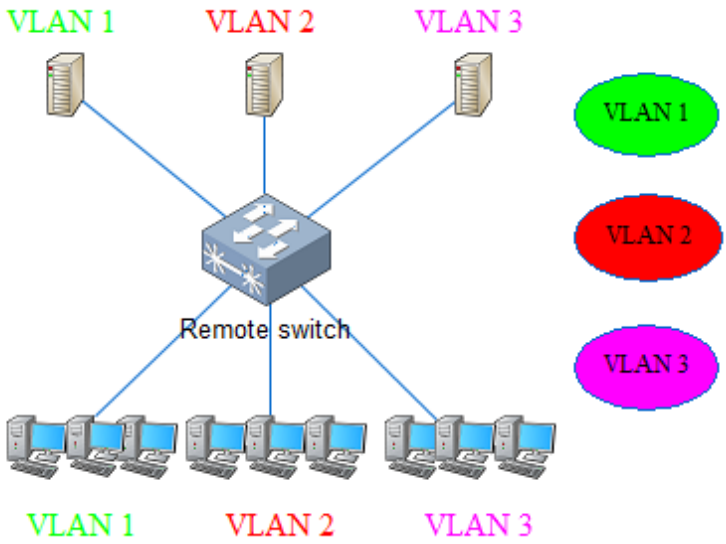

Рис.2.6. VLAN на базе портов

Если необходимо организовать несколько рабочих групп в пределах небольшой сети на основе одного коммутатора, то решение VLAN на базе портов оптимально подходит для данной задачи.

Простота настройки. Создание виртуальных сетей на основе группирования портов не требует от администратора большого объема ручной работы - достаточно каждому порту, находящемуся в одной VLAN, присвоить один и тот же идентификатор VLAN (VLAN ID) .

Возможность изменения логической топологии сети без физического перемещения станций – достаточно всего лишь изменить настройки порта, с одной VLAN (например, VLAN технического отдела) на другую (VLAN отдела продаж) и рабочая станция сразу же получает возможность совместно использовать ресурсы с членами новой VLAN.

Таким образом, VLAN обеспечивают гибкость при перемещениях, изменениях и наращивании сети. Каждый порт

может входить только в один VLAN. Поэтому для объединения виртуальных подсетей – как внутри одного коммутатора, так и между двумя коммутаторами, нужно использовать сетевой уровень (третий уровень модели ISO/OSI). Один из портов каждой VLAN подключается к интерфейсу маршрутизатора, который создает таблицу маршрутизации для пересылки пакетов из одной подсети в другую, при этом IP адреса подсетей должны быть разными (см. рис. 2.7.).

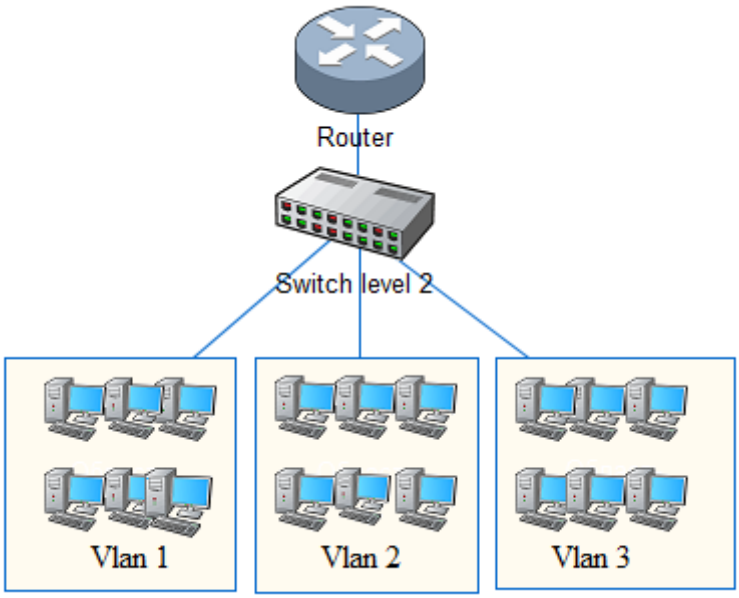

Рис.2.7. Объединение VLAN на базе портов на основе маршрутизатора

Недостатком такого решения является то, что один порт каждой VLAN необходимо подключать к маршрутизатору. Это приводит к дополнительным расходам на покупку кабелей и маршрутизатор, плюс порты коммутатора используются очень расточительно. Решить данную проблему можно двумя способами: использовать коммутаторы, которые на основе фирменного решения позволяют включать порт в несколько VLAN или использовать коммутаторов уровня 3.

VLAN на базе MAC-адресов. Следующий способ, который используется для образования виртуальных сетей, основан на группировке MAC-адресов. При существовании в сети большого количества узлов этот способ требует выполнения большого количества ручных операций от администратора. Однако он оказывается более гибким при построении виртуальных сетей на основе нескольких коммутаторов, чем способ группировки пор-

тов. Группирование MAC-адресов в сеть на каждом коммутаторе избавляет от необходимости их связи несколькими портами, однако, требует выполнения большого количества ручных операций по маркировке MAC-адресов на каждом коммутаторе сети.

Широковещательные домены на базе MAC-адресов, позволяют физически перемещать станцию (подключать к любому порту коммутатора), позволяя оставаться ей в одном и том же широковещательном домене без каких-либо изменений в настройках конфигурации.

Настройка виртуальной сети на основе MAC-адресов может отнять много времени - представьте себе, что вам потребуется связать с VLAN адреса 1000 устройств. Кроме того, MAC-адреса «наглухо зашиты» в оборудование, и может потребоваться много времени на выяснение адресов устройств в большой, территориально распределенной сети (см. рис.2.8.).

VLAN на базе меток – стандарт IEEE 802.1Q. Описанные два подхода основаны только на добавлении дополнительной информации к адресным таблицам коммутатора и не используют возможности встраивания информации о принадлежности кадра к виртуальной сети в передаваемый кадр.

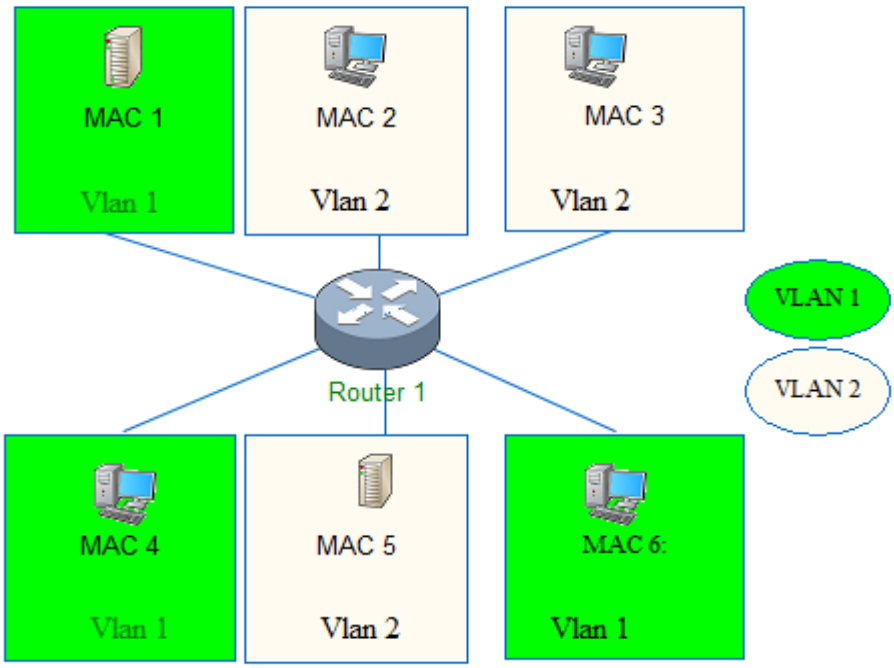

Рис.2.8. VLAN на базе MAC-адресов

Метод организации VLAN на основе меток – тэгов, использует дополнительные поля кадра для хранения информации о принадлежности кадра при его перемещениях между коммутаторами сети.

Стандарт IEEE 802.1Q определяет изменения в структуре кадра Ethernet, позволяющие передавать информацию о VLAN по сети. С точки зрения удобства и гибкости настроек, VLAN на основе меток является лучшим решением, по сравнению с ранее описанными подходами.

Его основные преимущества: гибкость и удобство в настройке и изменении – можно создавать необходимые комбинации VLAN как в пределах одного коммутатора, так и во всей сети, построенной на коммутаторах с поддержкой стандарта IEEE 802.1Q. Способность добавления меток позволяет VLAN распространяться через множество 802.1Q-совместимых коммутаторов по одному физическому соединению. Позволяет активизировать алгоритм покрывающего дерева (Spanning Tree) на всех портах и работать в обычном режиме. Протокол Spanning Tree оказывается весьма полезным для применения в крупных сетях, построенных на нескольких коммутаторах, и позволяет коммутаторам автоматически определять древовидную конфигурацию связей в сети при произвольном соединении портов между собой. Для нормальной работы коммутатора требуется отсутствие замкнутых маршрутов в сети. Эти маршруты могут создаваться администратором специально для образования резервных связей или же возникать случайным образом, что вполне возможно, если сеть имеет многочисленные связи, а кабельная система плохо структурирована или документирована. С помощью протокола Spanning Tree коммутаторы после построения схемы сети блокируют избыточные маршруты, таким образом, автоматически предотвращается возникновение петель в сети.

Способность VLAN 802.1Q добавлять и извлекать метки из заголовков пакетов позволяет VLAN работать с коммутаторами и сетевыми адаптерами серверов и рабочих станций, которые не распознают метки. Устройства разных производителей, поддерживающие стандарт могут работать вместе, не зависимо от какого-либо фирменного решения. Чтобы связать подсети на сетевом уровне, достаточно включить нужные порты в несколько VLAN, что обеспечит возможность обмена трафиком. Например, для

организации доступа к серверу из различных VLAN, нужно включить порт коммутатора, к которому подключен сервер во все подсети. Единственное ограничение – сетевой адаптер сервера должен поддерживать стандарт IEEE 802.1Q.

2.5 . Дополнительные функции коммутаторов

Так как коммутатор представляет собой сложное вычислительное устройство, имеющее несколько процессорных модулей, то естественно нагрузить его помимо выполнения основной функции передачи кадров с порта на порт по алгоритму моста и некоторыми дополнительными функциями, полезными при построении надежных и гибких сетей.

Поддержка алгоритма Spanning Tree. Алгоритм покрывающего дерева - Spanning Tree Algorithm (STA) позволяет коммутаторам автоматически определять древовидную конфигурацию связей в сети при произвольном соединения портов между собой. Как уже отмечалось, для нормальной работы коммутатора требуется отсутствие замкнутых маршрутов в сети. Эти маршруты могут создаваться администратором специально для образования резервных связей или же возникать случайным образом, что вполне возможно, если сеть имеет многочисленные связи, а кабельная система плохо структурирована или документирована.

Поддерживающие алгоритм STA коммутаторы автоматически создают активную древовидную конфигурацию связей на множестве всех связей сети. Такая конфигурация называется покрывающим деревом - Spanning Tree, который описан в стандарте IEEE 802.1D.

Коммутаторы находят покрывающее дерево адаптивно, с помощью обмена служебными пакетами. Реализация в коммутаторе алгоритма STA очень важна для работы в больших сетях - если коммутатор не поддерживает этот алгоритм, то администратор должен самостоятельно определить, какие порты нужно перевести в заблокированное состояние, чтобы исключить петли. К тому же при отказе какого-либо кабеля, порта или коммутатора администратор должен, во-первых, обнаружить факт отказа, а во-вторых, ликвидировать последствия отказа, переведя резервную связь в рабочий режим путем активизации некоторых портов. При поддержке коммутаторами сети протокола Spanning Tree отказы обнаружива-

ются автоматически, за счет постоянного тестирования связности сети служебными пакетами. После обнаружения потери связности протокол строит новое покрывающее дерево и сеть автоматически восстанавливает работоспособность.

Алгоритм Spanning Tree определяет активную конфигурацию сети за три этапа.

1. Сначала в сети определяется корневой коммутатор (root switch), от которого строится дерево. Корневой коммутатор может быть выбран автоматически или назначен администратором. При автоматическом выборе корневым становится коммутатор с меньшим значением MAC - адреса его блока управления.
2. Для каждого коммутатора определяется корневой порт (root port) - это порт, который имеет по сети кратчайшее расстояние до корневого коммутатора.
3. Для каждого сегмента сети выбирается так называемый назначенный порт (designated port) - это порт, который имеет кратчайшее расстояние от данного сегмента до корневого коммутатора. После определения корневых и назначенных портов каждый коммутатор блокирует остальные порты, которые не попали в эти два класса портов.

Понятие расстояния играет важную роль в построении покрывающего дерева. Именно по этому критерию выбирается единственный порт, соединяющий каждый коммутатор с корневым коммутатором, и единственный порт, соединяющий каждый сегмент сети с корневым коммутатором.

На рис. 2.9 показан пример построения конфигурации покрывающего дерева для сети, состоящей из 5 сегментов и 5 коммутаторов[13]. Корневые порты закрашены темным цветом, назначенные порты не закрашены, а заблокированные порты перечеркнуты. В активной конфигурации коммутаторы 2 и 4 не имеют портов, передающих кадры данных, поэтому они закрашены как резервные.

Расстояние до корня это суммарное условное время на передачу одного бита данных от порта данного коммутатора до порта корневого коммутатора. Условное время сегмента рассчитывается как время, затрачиваемое на передачу одного бита информации в 10

[13] Тарасов К. «Коммутаторы для сегмента передачи данных мультисервисной Metro-сети FTTB» журнал «Широкополосные мультисервисные сети», 2009.

наносекундных единицах между непосредственно связанными по сегменту сети портами.

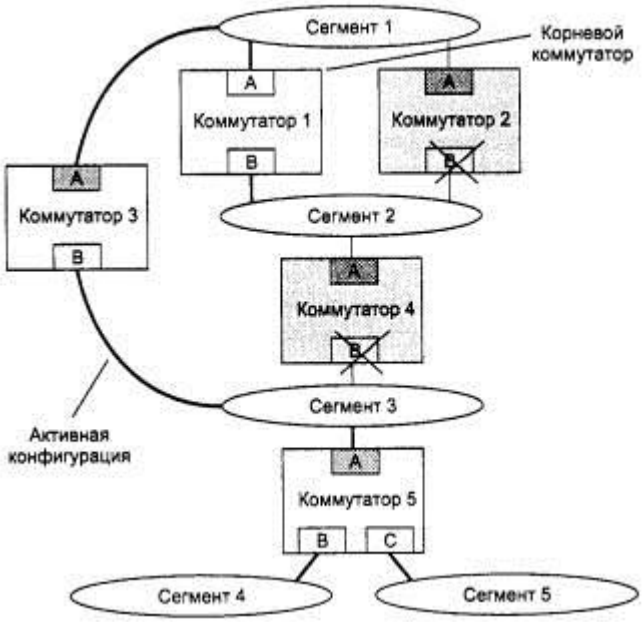

Рис. 2.9. Построение покрывающего дерева сети по алгоритму STA

Так, для сегмента Ethernet это время равно 10 условным единицам, а для сегмента Token Ring 16 Мбит/с - 6,25. (Все сегменты работают на одной скорости, поэтому они имеют одинаковые условные расстояния.)

Для автоматического определения начальной активной конфигурации дерева все коммутаторы сети после их инициализации начинают периодически обмениваться специальными пакетами, называемыми протокольными блоками данных моста - BPDU (Bridge Protocol Data Unit), что отражает факт первоначальной разработки алгоритма STA для мостов.

Пакеты BPDU помещаются в поле данных кадров канального уровня, например кадров Ethernet или FDDI. Для одновременной рассылки кадров BPDU всем коммутаторам сети все коммутаторы должны поддерживать общий групповой адрес. Поля пакета BPDU перечислены ниже.

- Идентификатор версии протокола STA - 2 байта. Коммутаторы должны поддерживать одну и ту же версию протокола STA или может установиться активная конфигурация с петлями.
- Тип BPDU - 1 байт. Существуют два типа BPDU - конфигурационный BPDU, то есть заявка на возможность стать

корневым коммутатором, на основании которой происходит определение активной конфигурации, и BPDU уведомления о реконфигурации, которое посылается коммутатором, обнаружившим событие, требующее проведения реконфигурации - отказ линии связи, отказ порта, изменение приоритетов коммутатора или портов.

- Флаги - 1 байт. Один бит содержит флаг изменения конфигурации, второй -флаг подтверждения изменения конфигурации.
- Идентификатор корневого коммутатора - 8 байт.
- Расстояние до корня - 2 байта.
- Идентификатор коммутатора - 8 байт.
- Идентификатор порта - 2 байта.
- Время жизни сообщения - 2 байта. Измеряется в единицах по 0,5 с, служит для выявления устаревших сообщений. Когда пакет BPDU проходит через коммутатор, тот добавляет ко времени жизни пакета время его задержки данным коммутатором.
- Максимальное время жизни сообщения - 2 байта. Если пакет BPDU имеет время жизни, превышающее максимальное, то он игнорируется коммутаторами.
- Интервал hello, через который посылаются пакеты BPDU.
- Задержка смены состояний - 2 байта. Задержка определяет минимальное время перехода портов коммутатора в активное состояние.

Такая задержка необходима, чтобы исключить возможность временного возникновения петель при неодновременной смене состояний портов во время реконфигурации. У пакета BPDU уведомления о реконфигурации отсутствуют все поля, кроме двух первых.

Идентификаторы коммутаторов состоят из 8 байт, причем младшие 6 являются MAC – адресом блока управления коммутатора. Старшие 2 байта в исходном состоянии заполнены нулями, но администратор может изменить значение этих байтов, тем самым назначив определенный коммутатор корневым.

После инициализации каждый коммутатор сначала считает себя корневым. Поэтому он начинает через интервал hello генерировать через все свои порты сообщения BPDU конфигурационного типа. В них он указывает свой идентификатор в качестве идентификатора корневого коммутатора (и в качестве идентификатора данного коммутатора также), расстояние до корня устанавливается в 0, а в качестве идентификатора порта указывается идентификатор

того порта, через который передается BPDU. Как только коммутатор получает BPDU, в котором имеется идентификатор корневого коммутатора, со значением, меньшим его собственного, он перестает генерировать свои собственные кадры BPDU, а начинает ретранслировать только кадры нового претендента на звание корневого коммутатора. При ретрансляции кадров каждый коммутатор наращивает расстояние до корня, указанное в пришедшем BPDU, на условное время сегмента, по которому принят данный кадр. Тем самым в кадре BPDU, по мере прохождения через коммутаторы, накапливается расстояние до корневого коммутатора. Если считать, что все сегменты рассматриваемого примера являются сегментами Ethernet, то коммутатор 2, приняв от коммутатора BPDU по сегменту 1 с расстоянием, равным 0, наращивает его на 10 единиц.

Ретранслируя кадры, каждый коммутатор для каждого своего порта запоминает минимальное расстояние до корня, встретившееся во всех принятых этим портом кадрах BPDU. При завершении процедуры установления конфигурации покрывающего дерева (по времени) каждый коммутатор находит свой корневой порт - это порт, для которого минимальное расстояние до корня оказалось меньше, чем у других портов. Так, коммутатор 3 выбирает порт А в качестве корневого, поскольку по порту А минимальное расстояние до корня равно 10 (BPDU с таким расстоянием принят от корневого коммутатора через сегмент 1). Порт В коммутатора 3 обнаружил в принимаемых кадрах минимальное расстояние в 20 единиц - это соответствовало случаю прохождения кадра от порта В корневого моста через сегмент 2, затем через мост 4 и сегмент 3.

Кроме корневого порта коммутаторы распределенным образом выбирают для каждого сегмента сети назначенный порт. Для этого они исключают из рассмотрения свой корневой порт (для сегмента, к которому он подключен, всегда существует другой коммутатор, который ближе расположен к корню), а для всех своих оставшихся портов сравнивают принятые по ним минимальные расстояния до корня с расстоянием до корня своего корневого порта. Если у какого-либо своего порта принятые им расстояния до корня больше, чем расстояние маршрута, пролегающего через свой корневой порт, то это значит, что для сегмента, к которому подключен данный порт, кратчайшее расстояние к корневому коммутатору ведет именно через данный порт. Коммутатор делает все свои порты, у которых такое условие выполняется, назначенными.

Если в процессе выбора корневого порта или назначенного порта несколько портов оказываются равными по критерию кратчайшего расстояния до корневого коммутатора, то выбирается порт с наименьшим идентификатором.

В качестве примера рассмотрим выбор корневого порта для коммутатора 2 и назначенного порта для сегмента 2. Мост 2 при выборе корневого порта столкнулся с ситуацией, когда порт A и порт B имеют равное расстояние до корня – по 10 единиц (порт A принимает кадры от порта B корневого коммутатора через один промежуточный сегмент – сегмент 1, а порт B принимает кадры от порта A корневого коммутатора также через один промежуточный сегмент – через сегмент 2). Идентификатор A имеет меньшее числовое значение, чем B (в силу упорядоченности кодов символов), поэтому порт A стал корневым портом коммутатора 2. При проверке порта B на случай, не является ли он назначенным для сегмента 2, коммутатор 2 обнаружил, что через этот порт он принимал кадры с указанным в них минимальным расстоянием 0 (это были кадры от порта B корневого коммутатора 1). Так как собственный корневой порт у коммутатора 2 имеет расстояние до корня 10, то порт B не является назначенным для сегмента 2.

Затем все порты, кроме корневого и назначенных, переводятся каждым коммутатором в заблокированное состояние. На этом построение покрывающего дерева заканчивается. В процессе нормальной работы корневой коммутатор продолжает генерировать служебные кадры BPDU, а остальные коммутаторы продолжают их принимать своими корневыми портами и ретранслировать назначенными. Если у коммутатора нет назначенных портов, как у коммутаторов 2 и 4, то они все равно продолжают принимать участие в работе протокола Spanning Tree, принимая служебные кадры корневым портом. Если по истечении тайм-аута корневой порт любого коммутатора сети не получает служебный кадр BPDU, то он инициализирует новую процедуру построения покрывающего дерева, оповещая об этом другие коммутаторы BPDU уведомления о реконфигурации. Получив такой кадр, все коммутаторы начинают снова генерировать BDPU конфигурационного типа, в результате чего устанавливается новая активная конфигурация.

Выводы

Логические сегменты, построенные на основе коммутаторов, являются строительными элементами более крупных сетей, объединяемых маршрутизаторами.

Коммутаторы – наиболее быстродействующие современные коммуникационные устройства, они позволяют соединять высокоскоростные сегменты без блокирования (уменьшения пропускной способности) межсегментного трафика.

Пассивный способ построения адресной таблицы коммутаторами – с помощью слежения за проходящим трафиком – приводит к невозможности работы в сетях с петлевидными связями. Другим недостатком сетей, построенных на коммутаторах, является отсутствие защиты от широковещательного шторма, который эти устройства обязаны передавать в соответствии с алгоритмом работы.

Применение коммутаторов позволяет сетевым адаптерам использовать полнодуплексный режим работы протоколов локальных сетей (Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI). В этом режиме отсутствует этап доступа к разделяемой среде, а общая скорость передачи данных удваивается.

В полнодуплексном режиме для борьбы с перегрузками коммутаторов используется метод управления потоком, описанный в стандарте 802.3x. Он повторяет алгоритмы полной приостановки трафика по специальной команде, известной из технологий глобальных сетей.

При полудуплексном режиме работы коммутаторы используют для управления потоком при перегрузках два метода: агрессивный захват среды и обратное давление на конечный узел. Применение этих методов позволяет достаточно гибко управлять потоком, чередуя несколько передаваемых кадров с одним принимаемым.

Коммутаторы связывают процессоры портов по трем основным схемам – коммутационная матрица, общая шина и разделяемая память.

Для поддержания неблокирующего режима работы коммутатора общая шина или разделяемая память должны обладать производительностью, превышающей сумму производительностей всех портов максимально высокоскоростного набора модулей, которые устанавливаются в шасси.

Основными характеристиками производительности коммутатора являются: скорость фильтрации кадров, скорость продвижения кадров, общая пропускная способность по всем портам в мегабитах в секунду, задержка передачи кадра.

На характеристики производительности коммутатора влияют: тип коммутации – «на лету» или с полной буферизацией, размер адресной таблицы, размер буфера кадров.

Для автоматического поддержания резервных связей в сложных сетях в коммутаторах реализуется алгоритм покрывающего дерева - Spanning Tree Algorithm. Этот алгоритм основан на периодической генерации служебных кадров, с помощью которых выявляются и блокируются петлевидные связи в сети.

Коммутаторы могут объединять сегменты разных технологий локальных сетей, транслируя протоколы канального уровня в соответствии со спецификацией IEEE 802.1H.

Коммутаторы поддерживают разнообразные пользовательские фильтры, основанные на MAC – адресах, а также на содержимом полей протоколов верхних уровней.

Коммутаторы обеспечивают поддержку качества обслуживания с помощью приоритетной обработки кадров. Стандарт 802.1p определяет дополнительное поле, состоящее из 3 бит, для хранения приоритета кадра независимо от технологии сети.

Технология виртуальных локальных сетей (VLAN) позволяет в сети, построенной на коммутаторах, создать изолированные группы узлов, между которыми не передается любой тип трафика, в том числе и широковещательный.

2.6. Вопросы и упражнения

1. Каким образом мост/коммутатор строит свою внутреннюю таблицу?
2. Что случится, если во время работы моста/коммутатора произойдет реконфигурация сети, например, будут подключены новые компьютеры?
3. В области сетевых технологий явно наметилась тенденция к использованию индивидуальных связей компьютеров с коммуникационными устройствами (в отличие от подключения к портам сегментов). С чем это связано?

4. Почему полнодуплексный Ethernet не поддерживается в концентраторах?
5. Каким образом коммутатор может управлять потоком пакетов, поступающих от сетевых адаптеров станций сети?
6. Можно ли создать коммутатор, который способен работать в режиме концентратора на тех же портах, на которых выполняется маршрутизация?
7. Можно ли соединить транслирующим коммутатором сегменты, в которых установлено разное максимальное значение поля данных?
8. Имеется ли специфика в использовании мостов и коммутаторов? Приведите примеры, когда замена моста коммутатором не повышает производительности сети.
9. Почему недорогие коммутаторы, выполняющие ограниченное число функций, обычно работают по быстрому алгоритму обработки пакетов «на лету», а дорогие коммутаторы, с большим числом функций - по более медленному алгоритму буферизации пакетов?
10. Какая информация содержится в таблицах мостов/коммутаторов и маршрутизаторов?
11. Поясните определение: «Виртуальная локальная сеть - это домен распространения широковещательных сообщений».
12. В каких случаях появляется необходимость в создании виртуальных сегментов? Приведите примеры.

ГЛАВА 3. IP - МАРШРУТИЗАЦИЯ

В целях повышения эффективности реализации комплексных программ по внедрению современных инфокоммуникационных технологий уделяется большое внимание практическому внедрению сложной инфокоммуникационной сети, объединенной маршрутизаторами. что позволит организовать и четко отладить взаимодействие между разными ее составными частями, превратив их в единую систему.

3.1. Принципы маршрутизации

Маршрутизация — процесс определения в сети наилучшего пути, по которому пакет может достигнуть адресата. В основе маршрутизации лежит коммутация пакетов — это перемещение пакетов через роутер.

Маршрутизатор или роутер (router) объединяет персональные компьютеры в локальную вычислительную сеть, пересылает пакеты данных между различными сегментами сети и работает на третьем (сетевом) уровне модели OSI (open systems interconnection basic reference model — базовая эталонная модель взаимодействия открытых систем)[14] [3,5].

Существует 2 вида маршрутизации: статическая и динамическая маршрутизация. Статическая маршрутизация используется редко в ЛВС, так как маршруты настраиваются вручную (администратором сети) и любые изменения сетевой топологии требуют участия администратора для корректировки таблиц маршрутизации, а в больших сетях подобная ручная работа становится громоздкой.

При настройке статического маршрута указывается:

- адрес сети, на которую маршрутизируется трафик;
- маска сети, позволяющая узнать какая часть IP-адреса принадлежит сети, а какая — хосту;
- адрес шлюза (узла).

Динамическая маршрутизация — вид маршрутизации, при котором

[14] Димарцио Д.Ф. «Маршрутизаторы Cisco. Пособие для самостоятельного изучения», 2005.

таблица маршрутизации редактируется программным способом и используются протоколы динамической маршрутизации, которые обменивают своей маршрутной информацией по определенным правилам.

IP-маршрутизация – это процесс продвижения IP-трафика соответствующему адресату в составной IP-сети с произвольной топологией, т.е. это процесс продвижения пакетов от хоста-источника к хосту-адресату через ряд промежуточных маршрутизаторов.

Для упрощения процесса продвижения хост-источник и каждый маршрутизатор принимают решение о продвижении на основе содержимого своих локальных таблиц IP-маршрутизации. Записи таблицы IP-маршрутизации создаются тремя основными источниками:

- программным обеспечением стека TCP/IP (Transmission Control Protocol – протокол управления передачей), представляющая собой записи о непосредственно подключенных сетях и основных шлюзах, информация о которых вводится при ручной настройке сетевых подключений компьютера администратором путем конфигурирования статических маршрутов;
- протоколами маршрутизации, например протоколом передачи маршрутной информации (RIP; Routing Information Protocol).

Существуют два типа IP-маршрутизации – прямая и косвенная:

Прямая маршрутизация. Если хост-источник и хост назначения находятся в одной физической сети, то IP – пакет может быть послан непосредственно путем упаковки в кадр физической сети. Это называется прямой доставкой или прямой маршрутизацией.

Косвенная маршрутизация. Такая маршрутизация выполняется тогда, когда хост назначения не находится в сети, непосредственно подключенной к хосту-источнику. Единственный способ достичь адресата – передать пакет через один или более IP-маршрутизаторов. Адрес первого из этих маршрутизаторов (адрес первого перехода) называется косвенным маршрутом и – это единственная информация, необходимая хосту-источнику. Иногда одна сеть делится на несколько подсетей. Если хост назначения и хост-источник относятся к одной сети, но расположены в разных подсетях, то используется косвенная маршрутизация. При этом трафик между подсетями должен продвигаться маршрутизатором.

Таблица маршрутизации – это база данных маршрутов, хранящаяся в памяти всех IP-узлов. Каждая запись, или маршрут, который содержится в таблице маршрутизации, содержит информацию о продвижении для некоторой области IP-адресов назначения.

Цель таблицы IP – маршрутизации – предоставить для IP-адреса назначения каждого продвигаемого пакета информацию об интерфейсе следующего перехода и IP – адресе следующего перехода:

Интерфейс следующего перехода – это адрес интерфейса, через который должен быть послан IP-пакет.

IP-адрес следующего перехода – это IP-адрес узла, которому должен быть направлен IP – пакет. Для прямой доставки IP-адрес следующего перехода является IP-адресом назначения передаваемого IP-пакета. Для косвенной доставки IP – адрес следующего перехода – это IP-адрес непосредственно достижимого промежуточного маршрутизатора, которому должен быть направлен IP – пакет.

Каждая запись в таблице IP-маршрутизации содержит достаточно информации для идентификации соответствующего адресата, интерфейса следующего перехода и IP – адреса следующего перехода, а также для выбора наилучшего маршрута при наличии нескольких маршрутов к одному адресату.

Протокол IP, центральной частью которого является таблица маршрутов, использует эту таблицу при принятии всех решений о маршрутизации IP – пакетов. Содержание таблицы маршрутов определяется администратором сети.

Рассмотрим простую IP – сеть на рис.3.1., состоящая из 3 компьютеров: A, B и C. Для передачи пакетов используется прямая маршрутизация. Каждая сетевая карта этих компьютеров имеет свой Ethernet – адрес. Менеджер сети должен присвоить им уникальные IP адреса.

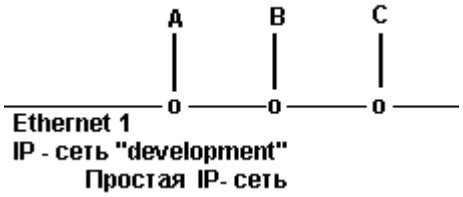

Рис.3.1. Простая IP-сеть

Когда A посылает IP – пакет B, то заголовок IP-пакета содержит в поле отправителя IP – адрес узла A, а заголовок Ethernet

– кадра (MAC адрес) содержит в поле отправителя Ethernet-адрес A. Кроме этого, IP-заголовок содержит в поле получателя IP–адрес узла B, а Ethernet – заголовок содержит в поле получателя Ethernet-адрес B.

Табл.3.1. Адреса в Ethernet-кадре, передающие IP-пакет от A к B

Поле отправителя	Поле получателя
IP-заголовок A Ethernet-заголовок A	IP-заголовок B Ethernet-заголовок B

Когда получатель B получает IP-пакет от A, он сопоставляет IP-адрес места назначения со своим и, если адреса совпадают, то передает дейтаграмму протоколу верхнего уровня. В данном случае при взаимодействии A с B используется прямая маршрутизация.

Косвенная маршрутизация. На рис. 3.2. представлена сеть, состоящая из трех сетей Ethernet, на базе которых работают три IP-сети, объединенные шлюзом D. Каждая IP – сеть включает четыре компьютера, которые имеют свои собственные IP– и Ethernet –адреса.

Модуль – это программа, взаимодействующая с драйвером, сетевыми прикладными программами или другими модулями. Драйвер сетевого адаптера и, возможно, другие модули, специфичные для физической сети передачи данных, предоставляют сетевой интерфейс для протокольных модулей семейства TCP/IP. Шлюз D соединяет все три сети и, следовательно, имеет три IP – адреса и три Ethernet – адреса, а также имеет стек протоколов TCP/IP состоящий из трех модулей ARP (Address Resolution Protocol адресный протокол) и трех драйверов Ethernet. Менеджер сети присваивает каждой сети Ethernet уникальный номер, называемый IP-номером сети. На рис.3.2. IP – номера не показаны, вместо них используются имена сетей. Когда компьютер A посылает IP – пакет компьютеру B, то процесс передачи идет в пределах одной сети.

Маршрутизация IP – пакетов выполняется модулями IP и является прозрачной для модулей TCP, UDP и прикладных процессов. Если компьютер A посылает компьютеру E IP – пакет, то IP-адрес и Ethernet – адрес отправителя соответствуют адресам A. IP-адрес места назначения является адресом E, но поскольку модуль IP в A посылает IP – пакет через D, Ethernet – адрес места назначения является адресом D.

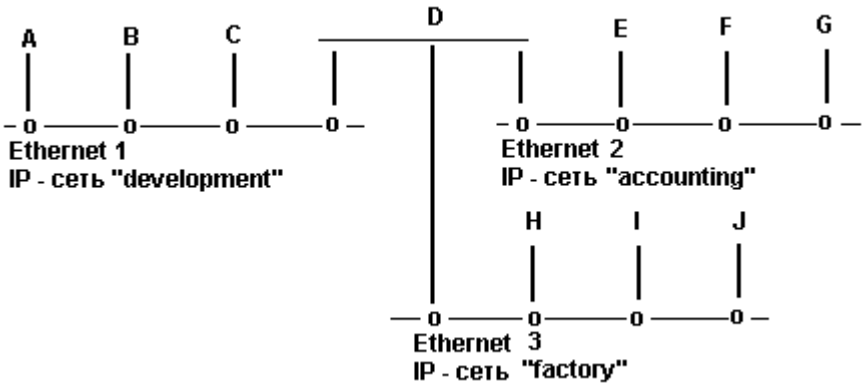

Рис.3.2. Сеть, состоящая из трех IP-сетей

Табл.3.2. Адреса в Ethernet-кадре с IP-пакет от A к E (до шлюза D)

Поле отправителя	Поле получателя
IP-заголовок A Ethernet-заголовок A	IP-заголовок E Ethernet-заголовок D

Модуль IP в шлюзе D получает IP – пакет и проверяет IP – адрес места назначения. Определив, что это не его IP – адрес, шлюз D посылает этот IP – пакет прямо к E.

Табл.3.3. Адреса в Ethernet – кадре с IP – пакет от A к E (после шлюз D)

Поле отправителя	Поле получателя
IP-заголовок A Ethernet-заголовок A	IP-заголовок E Ethernet-заголовок E

Итак, при прямой маршрутизации IP– и Ethernet – адреса отправителя соответствуют адресам того узла, который послал IP-пакет, а IP – и Ethernet – адреса места назначения соответствуют адресам получателя. При косвенной маршрутизации IP – и Ethernet-адреса не образуют таких пар. Реальные сети могут быть гораздо сложнее, так как могут содержать несколько шлюзов и несколько типов физических сред передачи. В приведенном примере несколько сетей Ethernet объединяются шлюзом для того, чтобы локализовать широковещательный трафик в каждой сети.

3.2. Правила маршрутизации в модуле IP

Название блока данных, передаваемого по сети, зависит от того, на каком уровне стека протоколов он находится. Блок данных, с которым имеет дело сетевой интерфейс, называется кадром; если

блок данных находится между сетевым интерфейсом и модулем IP, то он называется IP-пакетом; если он – между модулем IP и модулем UDP, то – UDP-дейтаграммой; если между модулем IP и модулем TCP, то – TCP – сегментом (или транспортным сообщением); если блок данных находится на уровне сетевых прикладных процессов, то он называется прикладным сообщением[15].

Для отправляемых IP-пакетов, поступающих от модулей верхнего уровня, модуль IP должен определить способ доставки - прямой или косвенный и выбрать сетевой интерфейс. Этот выбор делается на основании результатов поиска в таблице маршрутов. Для принимаемых IP-пакетов, поступающих от сетевых драйверов, модуль IP должен решить, нужно ли ретранслировать IP-пакет по другой сети или передать его на верхний уровень. Если модуль IP решит, что IP-пакет должен быть ретранслирован, то дальнейшая работа с ним осуществляется также, как с отправляемыми IP-пакетами. Входящий IP-пакет никогда не ретранслируется через тот же сетевой интерфейс, через который он был принят. Решение о маршрутизации принимается до того, как IP – пакет передается сетевому драйверу, и до того, как происходит обращение к ARP-таблице.

Подсети. Адресное пространство сети может быть разделено на непересекающиеся подпространства – "подсети", с каждой из которых можно работать как с обычной сетью TCP/IP. Таким образом, единая IP – сеть организации может строиться как объединение подсетей. Как правило, подсеть соответствует одной физической сети, например, одной сети Ethernet. Конечно, использование подсетей необязательно. Можно просто назначить для каждой физической сети свой сетевой номер, например, номер класса C. Однако такое решение имеет два недостатка. Первый, и менее существенный, заключается в пустой трате сетевых номеров. Более серьезный недостаток состоит в том, что если имеется несколько сетевых номеров, то машины вне ее должны поддерживать записи о маршрутах доступа к каждой из этих IP – сетей.

Таким образом, структура IP-сети организации становится видимой для всего мира. При каких-либо изменениях в IP-сети информация о них должна быть учтена в каждой из машин, поддер-

[15] . Руководство Cisco по междоменной многоадресной маршрутизации. . — М.: «Вильямс», 2004. — 320с.

живающих маршруты доступа к данной IP-сети. Подсети позволяют избежать этих недостатков. Необходимо получить один сетевой номер, например, номер класса B. Стандарты TCP/IP определяют структуру IP – адресов. Для IP – адресов класса B первые два октета являются номером сети. Оставшаяся часть IP-адреса может использоваться для третьего октета – это номер подсети, а четвертого октета – номер узла в ней. Необходимо описать конфигурацию подсетей в файлах, определяющих маршрутизацию IP – пакетов. Это описание является локальным и не видно вне ее, т.е. все машины видят одну большую IPсеть. Следовательно, они должны поддерживать только маршруты доступа к шлюзам, соединяющим IP – сеть с остальным миром.

Как назначать номера сетей и подсетей. При использовании подсети или множество IP-сетей необходимо назначить им номера. Каждой физической сети, например, Ethernet или Token Ring, назначается отдельный номер подсети или номер сети. В некоторых случаях имеет смысл назначать одной физической сети несколько подсетевых номеров. Например, предположим, что имеется сеть Ethernet, охватывающая три здания. При увеличении числа машин, подключенных к этой сети, придется ее разделить на несколько отдельных сетей Ethernet. Для того, чтобы избежать необходимости менять IP-адреса, когда это произойдет, можно заранее выделить для этой сети три подсетевых номера - по одному на здание. (Такая адресация позволяет сразу определить, где находится та или иная машина.) Однако прежде, чем выделять три различных подсетевых номера одной физической сети, необходимо проверить, что все программы способны работать в такой среде, а также выбрать "маску подсети". Она используется сетевым программным обеспечением для выделения номера подсети из IP-адресов. Биты IP-адреса, определяющие номер IP-сети, в маске подсети должны быть равны 1, а биты, определяющие номер узла, в маске подсети должны быть равны 0. Как уже отмечалось, стандарты TCP/IP определяют количество октетов, задающих номер сети. Часто в IP-адресах класса B третий октет используется для задания номера подсети. Это позволяет иметь 256 подсетей, в каждой из которых может быть до 254 узлов. Маска подсети в такой системе равна 255.255.255.0. Но, если в сети должно быть больше подсетей, а в каждой подсети будет 60 узлов, то можно использовать маску 255.255.255.192. Это позволяет иметь 1024 подсети и до 62 узлов в

каждой. Протоколы TCP/IP позволяют также запрашивать эту информацию по сети.

Имена. В маленьких сетях информация о соответствии имен IP-адресам хранится в файлах "hosts" на каждом узле. В больших сетях эта информация хранится на сервере и доступна по сети. Несколько строк из файла "hosts" могут выглядеть примерно так:

223.1.2.1 alpha
223.1.2.2 beta
223.1.2.3 gamma
223.1.2.4 delta
223.1.3.2 epsilo
223.1.4.2 iota

В первом столбце – IP-адрес, во втором – название машины.

В большинстве случаев файлы "hosts" могут быть одинаковы на всех узлах. В узле delta в этом файле есть всего одна запись, хотя он имеет три IP – адреса. Узел delta доступен по любому из этих IP–адресов. Какой из них используется, не имеет значения. Когда узел delta получает IP-пакет и проверяет IP – адрес места назначения, то он опознает любой из трех своих IP – адресов. IP – сети также могут иметь имена. Если у вас есть три IP – сети, то файл "networks" может выглядеть примерно так:

223.1.2 development
223.1.3 accounting
223.1.4 factory

В первой колонке - сетевой номер, во второй - имя сети.

В данном примере alpha является узлом номер 1 в сети development, beta является узлом номер 2 в сети development и т.д. Показанный выше файл hosts удовлетворяет потребности пользователей, но для управления сетью internet удобнее иметь названия всех сетевых интерфейсов. Менеджер сети, возможно, заменит строку, относящуюся к delta:

223.1.2.4 devnetrouter delta
223.1.3.1 accnetrouter
223.1.4.1 facnetrouter

Эти три строки файла hosts задают каждому IP-адресу узла delta символьные имена. Фактически, первый IP-адрес имеет два имени: "devnetrouter" и "delta", которые являются синонимами. На практике имя "delta" используется как общеупотребительное имя машины, а остальные три имени – для администрирования сети.

Файлы hosts и networks используются командами администрирования и прикладными программами.

IP-таблица маршрутов. Как модуль IP узнает, какой именно сетевой интерфейс нужно использовать для отправления IP-пакета, осуществляет поиск в таблице маршрутов. Ключом поиска служит номер IP–сети, выделенный из IP–адреса места назначения IP–пакета. Таблица маршрутов содержит по одной строке для каждого маршрута. Основными столбцами таблицы маршрутов являются номер сети, флаг прямой или косвенной маршрутизации, IP–адрес шлюза и номер сетевого интерфейса. Эта таблица используется модулем IP при обработке каждого отправляемого IP–пакета. В большинстве систем таблица маршрутов может быть изменена с помощью команды "route". Содержание таблицы маршрутов определяется менеджером сети, поскольку менеджер сети присваивает машинам IP–адреса[16].

Рассмотрим более подробно, как происходит прямая маршрутизация в одной физической сети.

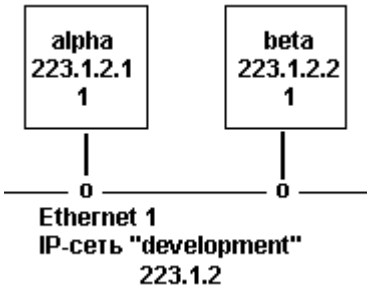

Рис.3.3. Одна физическая сеть

Табл.3.4. Пример таблицы маршрутов

Сеть флаг вида	Development (223.1.2)
маршрутизации	прямая
шлюз	<пусто>
номер интерфейса	1

Порядок прямой маршрутизации. Узел alpha посылает IP–пакет узлу beta, находящийся в модуле IP узла alpha. IP–адрес места назначения равен IP–адресу beta (223.1.2.2). Модуль IP с помощью маски подсети выделяет номер сети из IP–адреса и ищет соответ-

[16] Леинванд А., Пински Б Конфигурирование маршрутизаторов Cisco. — 2-е изд— М:Изд.дом«Вильямс», 2004. — 368с.

ствующую ему строку в таблице маршрутов (первая строка). Остальная информация в найденной строке указывает на то, что машины этой сети доступны напрямую через интерфейс номер 1. С помощью ARP–таблицы выполняется преобразование IP–адреса в соответствующий Ethernet–адрес и через интерфейс 1 Ethernet–кадр посылается узлу beta. Если прикладная программа пытается послать данные по IP–адресу, который не принадлежит сети development, то модуль IP отбрасывает IP–пакет.

Порядок косвенной маршрутизации. Узел alpha посылает IP–пакет узлу epsilon, изображенной на рис.3.4.

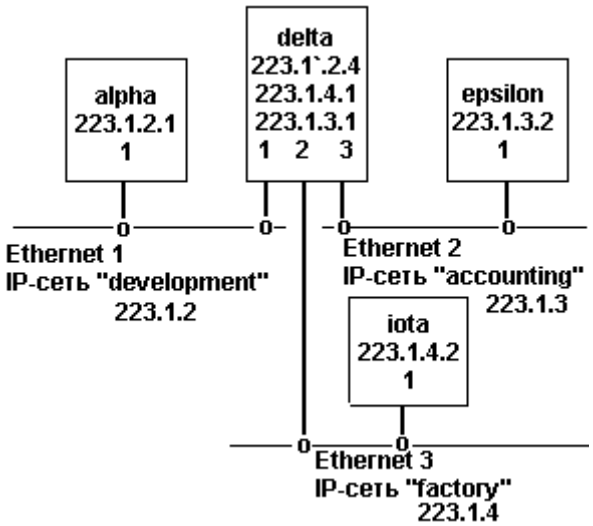

Рис.3.4. Подробная схема трех сетей

Этот пакет находится в модуле IP узла alpha, и IP–адрес места назначения равен IP–адресу узла epsilon (223.1.3.2). Модуль IP выделяет сетевой номер из IP–адреса (223.1.3) и ищет соответствующую ему строку в таблице маршрутов. Соответствие находится во второй строке. Запись в этой строке указывает на то, что машины требуемой сети доступны через шлюз devnetrouter (таблица 3.5, 3.6).

Таблица 3.5. Таблица маршрутов в узле alpha

Сеть	development	accounting	factory
маршрутизация	прямая	косвенная	косвенная
шлюз	<пусто>	devnetrouter	devnetrouter
номер интерфейса	1	1	1

Табл.3.6. Таблица маршрутов в узле alpha с номерами

Сеть	223.1.2	223.1.3	223.1.4
маршрутизация	прямая	косвенная	косвенная
шлюз	<пусто>	223.1.2.4	223.1.2.4
номер интерфейса	1	1	1

В столбце "шлюз" таблицы маршрутов узла alpha указывается IP–адрес точки соединения узла delta с сетью development. Модуль IP в узле alpha осуществляет поиск в ARP–таблице, с помощью которого определяет Ethernet–адрес, соответствующий IP–адресу devnetrouter. Затем IP–пакет, содержащий IP–адрес места назначения epsilon, посылается через интерфейс 1 шлюзу devnetrouter. IP–пакет принимается сетевым интерфейсом в узле delta и передается модулю IP. Проверяется IP–адрес места назначения, и, поскольку он не соответствует ни одному из собственных IP–адресов delta, шлюз решает ретранслировать IP–пакет. Модуль IP в узле delta выделяет сетевой номер из IP–адреса места назначения IP–пакета (223.1.3) и ищет соответствующую запись в таблице маршрутов (таблица 3.7., 3.8).

Табл.3.7. Таблица маршрутов в узле delta

Сеть флаг вида	development	accounting	factory
маршрутизация	прямая	косвенная	косвенная
шлюз	<пусто>	<пусто>	<пусто>
номер интерфейса	1	2	3

Табл.3.8. Таблица маршрутов в узле delta (с номерами)

Сеть флаг вида	223.1.2	223.1.3	223.1.4
маршрутизация	прямая	косвенная	косвенная
шлюз	<пусто>	<пусто>	<пусто>
номер интерфейса	1	2	3

Соответствие находится во второй строке. Теперь модуль IP напрямую посылает IP–пакет узлу epsilon через интерфейс номер 2. Пакет содержит IP– и Ethernet–адреса места назначения равные

epsilon. Узел epsilon принимает IP–пакет, и его модуль IP проверяет IP–адрес места назначения. Он соответствует IP–адресу epsilon, поэтому содержащееся в IP–пакете сообщение передается протокольному модулю верхнего уровня.

3.3. Функции маршрутизатора

Основная функция маршрутизатора – чтение заголовков пакетов сетевых протоколов, которые принимаются каждым его портом (IPX, IP, AppleTalk) с последующим принятием решения о дальнейшем маршруте следования пакета по его сетевому адресу, имеющие номер сети и номер узла. Функции маршрутизатора могут быть разбиты на 3 группы в соответствии с уровнями модели OSI (рис. 3.5).

Уровень интерфейсов. На нижнем уровне маршрутизатор обеспечивает физический интерфейс со средой передачи, включая согласование уровней электрических сигналов, линейное и логическое кодирование.

С каждым интерфейсом для подключения локальной сети неразрывно связан определенный протокол канального уровня – например, Ethernet, Token Ring, FDDI.

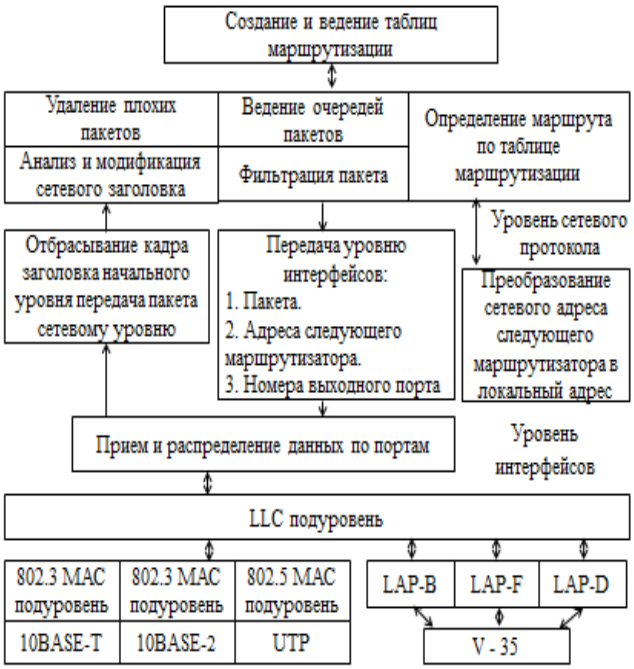

Рис. 3.5. Функциональная модель маршрутизатора

Интерфейсы маршрутизатора выполняют полный набор функций физического и канального уровней по передаче кадра, включая получение доступа к среде, формирование битовых сигналов, прием кадра, подсчет его контрольной суммы и передачу поля данных кадра верхнему уровню, в случае если контрольная сумма имеет корректное значение.

Маршрутизатор должен поддерживать все протоколы канального и физического уровней, используемые в каждой из сетей, к которым он будет непосредственно присоединен. На рис. 3.5 показана функциональная модель маршрутизатора с четырьмя портами, реализующими следующие физические интерфейсы: 10Base–T и 10Base–2 для двух портов Ethernet, UTP для Token Ring и V.35, над которым могут работать протоколы LAP–B, LAP–D или LAP–F, обеспечивая подключение к сетям X.25, ISDN или frame relay.

Кадры, которые поступают на порты маршрутизатора, после обработки соответствующими протоколами физического и канального уровней, освобождаются от заголовков канального уровня. Извлеченные из поля данных кадра пакеты передаются модулю сетевого протокола.

Уровень сетевого протокола. Сетевой протокол в свою очередь извлекает из пакета заголовок сетевого уровня и анализирует содержимое его полей: проверяется контрольная сумма, и если пакет пришел поврежденным, то он отбрасывается. Выполняется проверка время жизни пакета, при превышении допустимого времени пакет также отбрасывается. На этом этапе вносятся корректировки в содержимое некоторых полей, например, наращивается время жизни пакета, пересчитывается контрольная сумма.

На сетевом уровне выполняется одна из важнейших функций маршрутизатора – фильтрация трафика. Маршрутизатор, обладая более высоким интеллектом, чем коммутаторы, позволяет задавать и более сложные правила фильтрации. Маршрутизаторы, программное обеспечение которых содержит модуль сетевого протокола, производят разбор и анализ отдельных полей пакета. Они оснащаются развитыми средствами пользовательского интерфейса, которые позволяют администратору без особых усилий задавать сложные правила фильтрации. Они, например, могут запретить прохождение в корпоративную сеть всех пакетов, кроме пакетов, поступающих из подсетей этого же предприятия. Фильтрация в

данном случае производится по сетевым адресам, и все пакеты, адреса которых не входят в разрешенный диапазон, отбрасываются.

Программное обеспечение маршрутизатора может реализовать различные дисциплины обслуживания очередей пакетов: в порядке поступления по принципу «первый пришел – первым обслужен» (First Input First Output, FIFO), случайное раннее обнаружение, когда обслуживание идет по правилу FIFO, но при достижении длиной очереди некоторого порогового значения вновь поступающие пакеты отбрасываются (Random Early Detection, RED), а также различные варианты приоритетного обслуживания.

К сетевому уровню относится основная функция маршрутизатора – определение маршрута пакета. По номеру сети, извлеченному из заголовка пакета, модуль сетевого протокола находит в таблице маршрутизации строку, содержащую сетевой адрес следующего маршрутизатора, и номер порта, на который нужно передать данный пакет. Если в таблице отсутствует запись о сети назначения пакета и записи о маршрутизаторе, то данный пакет отбрасывается.

Перед тем как передать сетевой адрес следующего маршрутизатора на канальный уровень, необходимо преобразовать его в локальный адрес той технологии, которая используется в сети, содержащей следующий маршрутизатор. Для этого сетевой протокол обращается к протоколу разрешения адресов. Таблица соответствия локальных адресов сетевым адресам строится отдельно для каждого сетевого интерфейса. Протоколы разрешения адресов занимают промежуточное положение между сетевым и канальным уровнями.

С сетевого уровня пакет, локальный адрес следующего маршрутизатора и номер порта маршрутизатора передаются вниз, канальному уровню. На основании указанного номера порта осуществляется коммутация с одним из интерфейсов маршрутизатора, средствами которого выполняется упаковка пакета в кадр соответствующего формата. В поле адреса назначения заголовка кадра помещается локальный адрес следующего маршрутизатора. Готовый кадр отправляется в сеть.

Уровень протоколов маршрутизации. Сетевые протоколы активно используют в своей работе таблицу маршрутизации, но ни ее построением, ни поддержанием ее содержимого не занимаются. Эти функции выполняют протоколы маршрутизации. На основании этих протоколов маршрутизаторы обмениваются информацией о

топологии сети, а затем анализируют полученные сведения, определяя наилучшие по тем или иным критериям маршруты. Результаты анализа и составляют содержимое таблиц маршрутизации.

Помимо перечисленных выше функций, на маршрутизаторы могут быть возложены и другие обязанности, например операции, связанные с фрагментацией.

Выводы

- Типичный маршрутизатор представляет собой сложный специализированный компьютер, который работает под управлением специализированной операционной системы, оптимизированной для выполнения операций построения таблиц маршрутизации и продвижения пакетов на их основе.
- Маршрутизатор часто строится по мультипроцессорной схеме, причем используется симметричное мультипроцессирование, асимметричное мультипроцессирование и их сочетание. Наиболее рутинные операции обработки пакетов выполняются программными– специализированными процессорами или аппаратными большими интегральными схемами (БИС/ASIC). Более высокоуровневые действия выполняют программные универсальные процессоры.
- По областям применения маршрутизаторы делятся на: магистральные маршрутизаторы, маршрутизаторы региональных подразделений, маршрутизаторы удаленных офисов и маршрутизаторы локальных сетей – коммутаторы 3–го уровня.
- Основными характеристиками маршрутизаторов являются: общая производительность в пакетах в секунду, набор поддерживаемых сетевых протоколов и протоколов маршрутизации, набор поддерживаемых сетевых интерфейсов глобальных и локальных сетей.
- К числу дополнительных функций маршрутизатора относится одновременная поддержка сразу нескольких сетевых протоколов и нескольких протоколов маршрутизации, возможность приоритетной обработки трафика, разделение функций построения таблиц маршрутизации и продвижения пакетов между маршрутизаторами разного класса на основе готовых таблиц маршрутизации.
- Основной особенностью коммутаторов 3–го уровня является высокая скорость выполнения операций маршрутизации за счет их перенесения на аппаратный уровень – уровень БИС/ASIC.

- Многие фирмы разработали собственные протоколы ускоренной маршрутизации долговременных потоков в локальных сетях, которые маршрутизируют только несколько первых пакетов потока, а остальные пакеты коммутируют на основе MAC – адресов.

3.4. Вопросы и упражнения

1. Сравните таблицу коммутатора с таблицей маршрутизатора. Каким образом они формируются? Какую информацию содержат? От чего зависит их объем?
2. Таблица маршрутизации содержит записи о сетях назначения. Должна ли она содержать записи обо всех сетях составной сети или только о некоторых?
3. Какие из следующих утверждений верны всегда?

A. Каждый порт коммутатора имеет MAC – адрес.
B. Каждый коммутатор имеет сетевой адрес.
C. Каждый порт коммутатора имеет сетевой адрес.
D. Каждый маршрутизатор имеет сетевой адрес.
E. Каждый порт маршрутизатора имеет MAC – адрес.
F. Каждый порт маршрутизатора имеет сетевой адрес.

4. Пусть поставщик услуг Internet имеет в своем распоряжении адрес сети класса B. Для адресации узлов своей собственной сети он использует 254 адреса. Определите максимально возможное число абонентов этого поставщика услуг, если размеры требуемых для них сетей соответствуют классу C? Какая маска должна быть установлена на маршрутизаторе поставщика услуг, соединяющем его сеть с сетями абонентов?
5. Почему даже в тех случаях, когда используются маски, в IP–пакете маска не передается?
6. Отличается ли обработка поля MAC – адреса кадра маршрутизатором и коммутатором?
7. Сравните функции маршрутизаторов, которые поддерживают маршрутизацию от источника, с функциями маршрутизаторов, поддерживающих протоколы адаптивной маршрутизации.
8. Какие метрики расстояния могут быть использованы в алгоритмах сбора маршрутной информации?
9. Какие элементы сети могут выполнять фрагментацию?

A. только компьютеры;
B. только маршрутизаторы;

C. компьютеры, маршрутизаторы, коммутаторы;
D. компьютеры и маршрутизаторы.
10. Что произойдет, если при передаче пакета он был фрагментирован и один из фрагментов не дошел до узла назначения после истечения тайм–аута?
A. модуль IP узла–отправителя повторит передачу недошедшего фрагмента;
B. модуль IP узла–отправителя повторит передачу всего пакета, в состав которого входил недошедший фрагмент;
C. модуль IP узла–получателя отбросит все полученные фрагменты пакета, в котором потерялся один фрагмент; модуль IP узла–отправителя не будет предпринимать никаких действий по повторной передаче пакета данного пакета.
11. Каким образом должен быть сконфигурирован маршрутизатор, чтобы он предотвращал «широковещательный шторм»?
12. За счет чего коммутаторы третьего уровня ускоряют процесс маршрутизации?

ГЛАВА 4. ПРОТОКОЛЫ ВНУТРЕННЕЙ ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИИ

Протоколы маршрутизации разрабатываются для эффективной передачи пульсирующего компьютерного трафика. Таблицы маршрутизации позволяют оптимизировать неравномерность интенсивности трафика каждого абонента и равномерно загрузить каналы связи между маршрутизаторами.

4.1. Протокол маршрутизации OSPF

OSPF (Open Shortest Path First — выбор кратчайшего пути первым) — внутренний протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала LSA (Link–State Technology), использующий для нахождения кратчайшего пути с помощью алгоритма Дейкстры для эффективной маршрутизации IP–пакетов в больших сетях со сложной топологией, включающей петли[17].

Алгоритм Дейкстры — алгоритм на графах, находит кратчайшие пути от одной из вершин графа до всех остальных. Протокол OSPF был разработан как замена дистанционно–векторного протокола маршрутизации RIP. На данный момент существует три версии протокола. Вторая версия OSPF поддерживает IPv4, а третья поддерживает IPv6.

OSPF протокол ориентирован на применение в больших гетерогенных сетях. Гетерогенные сети — это сети, состоящие из различных операционных систем и приложений, имеющие смешанную топологию и работающие по различным сетевым протоколам. OSPF не использует протокол транспортного уровня, так как пакеты OSPF отправляются посредством IP. Протокол OSPF использует hello–пакеты, чтобы обнаружить соседей, установить смежность с соседними узлами, распространять параметры и т. д. Пакеты отправляются каждые 10 секунд в сегмент мультидоступа и в сегмент точка–точка, и каждые 30 секунд в сегмент нешироковещательного мультидоступа.

[17] Фейт С. TCP/IP. Архитектура, протоколы, реализация. – М.: Лори, 2015. – 424 с. 5.

Мертвый интервал — это ожидание маршрутизатора SPF разрыва смежности с соседом. Мертвый интервал в четыре раза превышает интервал hello по умолчанию (интервал составляет 120 секунд). Для сегментов мультидоступа и сегментов точка–точка, этот период составляет 40 секунд.

Алгоритм работы протокола основан на использовании всеми маршрутизаторами единой базы данных, описывающей, с какими сетями связан каждый маршрутизатор. Описывая каждую связь, маршрутизаторы связывают с ней метрику.

Метрика — это значение, характеризующее «качество» канала связи, которые позволяет более объективно оценивать маршруты, а при наличии выбора, принимать эффективное и целесообразное решение. Это позволяет маршрутизаторам OSPF учитывать реальную пропускную способность канала, надежность, загруженность, величина задержки распространения сигнала в канале и выявлять наилучшие маршруты. Важной особенностью протокола OSPF является то, что используется групповая, то есть, нагрузка каналов меньше.

LSA сообщения отправляются, только если произошли какие–либо изменения в сети, но раз в 30 минут LSA сообщения отправляются в принудительном порядке.

Существует 7 типов LSA:

1. Router LSA — объявление о состоянии каналов маршрутизатора.
2. Network LSA — объявление о состоянии каналов сети.
3. Network Summary LSA — суммарное объявление о состоянии кана–лов сети.
4. ASBR Summary LSA — суммарное объявление о состоянии каналов пограничного маршрутизатора автономной системы.
5. AS External LSA — объявления о состоянии внешних каналов авто–номной системы.
6. AS External LSA for NSSA — объявления о состоянии внешних каналов автономной системы в NSSA зоне.

Для преодоления недостатка быстрого увеличения сети, протокол реализует деление автономной системы на зоны (areas). Использование зон позволяет снизить нагрузку на сеть и процессоры маршрутизаторов и уменьшить размер таблиц маршрутизации.

В OSPF процесс построения таблицы маршрутизации разбивается на два крупных этапа. На первом этапе каждый маршрутиза-

тор строит граф связей сети, в котором вершинами графа являются маршрутизаторы и IP–сети, а ребрами – интерфейсы маршрутизаторов. Все маршрутизаторы для этого обмениваются со своими соседями той информацией о графе сети, которой они располагают к данному моменту времени. Этот процесс похож на процесс распространения векторов расстояний до сетей в протоколе RIP, однако сама информация качественно другая – это информация о топологии сети. Эти сообщения называются router links advertisement – объявление о связях маршрутизатора. Кроме того, при передаче топологической информации маршрутизаторы ее не модифицируют, как это делают RIP–маршрутизаторы, а передают в неизменном виде. В результате распространения топологической информации все маршрутизаторы сети располагают идентичными сведениями о графе сети, которые хранятся в топологической базе данных маршрутизатора.

Второй этап состоит в нахождении оптимальных маршрутов с помощью полученного графа. Каждый маршрутизатор считает себя центром сети и ищет оптимальный маршрут до каждой известной ему сети. В каждом найденном таким образом маршруте запоминается только один шаг – до следующего маршрутизатора, в соответствии с принципом одношаговой маршрутизации. Данные об этом шаге и попадают в таблицу маршрутизации. Задача нахождения оптимального пути на графе является достаточно сложной и трудоемкой. В протоколе OSPF для ее решения используется итеративный алгоритм Дейкстры. Если несколько маршрутов имеют одинаковую метрику до сети назначения, то в таблице маршрутизации запоминаются первые шаги всех этих маршрутов.

После первоначального построения таблицы маршрутизации необходимо отслеживать изменения состояния сети и вносить коррективы в таблицу маршрутизации. Для контроля состояния связей и соседних маршрутизаторов OSPF–маршрутизаторы не используют обмен полной таблицей маршрутизации. Вместо этого они передают специальные короткие сообщения HELLO. Если состояние сети не меняется, то OSPF–маршрутизаторы корректировкой своих таблиц маршрутизации не занимаются и не посылают соседям объявления о связях. Если же состояние связи изменилось, то ближайшим соседям посылается новое объявление, касающееся только данной связи, что, конечно, экономит пропускную способность сети. Получив новое объявление об изменении состояния связи,

маршрутизатор перестраивает граф сети, заново ищет оптимальные маршруты (не обязательно все, а только те, на которых отразилось данное изменение) и корректирует свою таблицу маршрутизации. Одновременно маршрутизатор ретранслирует объявление каждому из своих ближайших соседей (кроме того, от которого он получил это объявление). При появлении новой связи или нового соседа маршрутизатор узнает об этом из новых сообщений HELLO. В сообщениях HELLO указывается достаточно детальная информация о том маршрутизаторе, который послал это сообщение, а также о его ближайших соседях, чтобы данный маршрутизатор можно было однозначно идентифицировать. Сообщения HELLO отправляются через каждые 10 секунд, чтобы повысить скорость адаптации маршрутизаторов к изменениям, происходящим в сети. Небольшой объем этих сообщений делает возможной такое частое тестирование состояния соседей и связей с ними. Так как маршрутизаторы являются одними из вершин графа, то они обязательно должны иметь идентификаторы.

Протокол OSPF обычно использует метрику, учитывающую пропускную способность сетей. Кроме того, возможно использование двух других метрик, учитывающих требования к качеству обслуживания в IP–пакете, задержки передачи пакетов и надежности передачи пакетов сетью. Для каждой из метрик протокол OSPF строит отдельную таблицу маршрутизации. Выбор нужной таблицы происходит в зависимости от требований к качеству обслуживания пришедшего пакета (см. рис. 4.1).

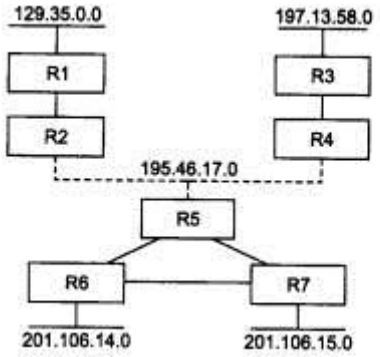

Рис.4.1. Построение таблицы маршрутизации по протоколу OSPF

Маршрутизаторы соединены как с локальными сетями, так и непосредственно между собой глобальными каналами типа «точка–точка». Данной сети соответствует граф, приведенный на рис. 4.2.

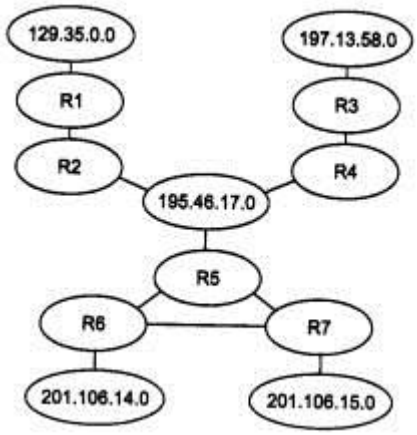

Рис. 4.2. Граф сети, построенный протоколом OSPF

Протокол OSPF в своих объявлениях распространяет информацию о связях двух типов: маршрутизатор – маршрутизатор и маршрутизатор – сеть. Примером связи первого типа служит связь «R3 – R4», а второго – связь «R4 – 195.46.17.0». Если каналам «точка–точка» дать IP–адреса, то они станут дополнительными вершинами графа, как и локальные сети. Вместе с IP–адресом сети передается также информация о маске сети.

После инициализации OSPF–маршрутизаторы знают только о связях с непосредственно подключенными сетями, как и RIP–маршрутизаторы. Они начинают распространять эту информацию своим соседям. Одновременно они посылают сообщения HELLO по всем своим интерфейсам, так что почти сразу же маршрутизатор узнает идентификаторы своих ближайших соседей, что пополняет его топологическую базу новой информацией, которую он узнал непосредственно. Далее топологическая информация начинает распространяться по сети от соседа к соседу и через некоторое время достигает самых удаленных маршрутизаторов.

Каждая связь характеризуется метрикой. Протокол OSPF поддерживает стандартные для многих протоколов (например, для протокола Spanning Tree) значения расстояний для метрики, отражающей производительность сетей: Ethernet – 10 единиц, Fast Ethernet – 1 единица, канал T1 – 65 единиц, канал 56 Кбит/с – 1785 единиц и т. д.

При выборе оптимального пути на графе с каждым ребром графа связана метрика, которая добавляется к пути, если данное ребро в него входит. Пусть на приведенном примере маршрутизатор R5 связан с .R6 и R7 каналами Tl, а R6 и R7 связаны между собой каналом 56 Кбит/с. Тогда R7 определит оптимальный маршрут

до сети 201.106.14.0 как составной, проходящий сначала через маршрутизатор R5, а затем через R6, поскольку у этого маршрута метрика будет равна 65+65 = 130 единиц. Непосредственный маршрут через R6 не будет оптимальным, так как его метрика равна 1785.

Протокол OSPF разрешает хранить в таблице маршрутизации несколько маршрутов к одной сети, если они обладают равными метриками. Если такие записи образуются в таблице маршрутизации, то маршрутизатор реализует режим баланса загрузки маршрутов (load balancing), отправляя пакеты попеременно по каждому из маршрутов.

У каждой записи в топологической базе данных имеется срок жизни, как и у маршрутных записей протокола RIP. С каждой записью о связях связан таймер, который используется для контроля времени жизни записи. Если какая–либо запись топологической базы маршрутизатора, полученная от другого маршрутизатора, устаревает, то он может запросить ее новую копию с помощью специального сообщения Link–State Request протокола OSPF, на которое должен поступить ответ Link–State Update от маршрутизатора, непосредственно тестирующего запрошенную связь. При инициализации маршрутизаторов, а также для более надежной синхронизации топологических баз маршрутизаторы периодически обмениваются всеми записями базы, но этот период существенно больше, чем у RIP–маршрутизаторов.

Периоды нестабильной работы в OSPF–сетях могут возникать. Например, при отказе связи, когда информация об этом не дошла до какого–либо маршрутизатора и он отправляет пакеты сети назначения, считая эту связь работоспособной. Однако эти периоды продолжаются недолго, причем пакеты не зацикливаются в маршрутных петлях, а просто отбрасываются при невозможности их передать через неработоспособную связь.

К недостаткам протокола OSPF следует отнести его вычислительную сложность, которая быстро растет с увеличением размерности сети, то есть количества сетей, маршрутизаторов и связей между ними. Для преодоления этого недостатка в протоколе OSPF вводится понятие *области сети (area*). Маршрутизаторы, принадлежащие некоторой области, строят граф связей только для этой области, что сокращает размерность сети. Между областями информация о связях не передается, а пограничные для областей

маршрутизаторы обмениваются только информацией об адресах сетей, имеющихся в каждой из областей, и расстоянием от пограничного маршрутизатора до каждой сети. При передаче пакетов между областями выбирается один из пограничных маршрутизаторов области, а именно тот, у которого расстояние до нужной сети меньше. Этот стиль напоминает стиль работы протокола RIP, но нестабильность здесь устраняется тем, что петлевидные связи между областями запрещены. При передаче адресов в другую область OSPF–маршрутизаторы агрегируют несколько адресов в один, если обнаруживают у них общий префикс.

OSPF–маршрутизаторы могут принимать адресную информацию от других протоколов маршрутизации, например от протокола RIP, что полезно для работы в гетерогенных сетях. Такая адресная информация обрабатывается так же, как и внешняя информация между разными областями.

В оборудовании Cisco приходится использовать обратную маску (wildcard mask). При описании сетей в протоколе OSPF используется обратная маска, то есть не 255.255.255.0, а 0.0.0.255. Для получения обратной маски производится перевод из 10 системы счисления в 2–ю:

255.255.255.252 = 11111111.11111111.11111111.11111100.

Далее производится инверсия:

00000000.00000000.00000000.00000011.

После полученный результат переводится в 10 систему счисления и получается обратная маска, которая заносится в протокол OSPF: 0.0.0.3.

Прямая маска оперирует сетями, а обратная — хостами. Например, используя обратную маску выделить хосты с конкретными адресами и разрешить им доступ в Интернет.

4.2. Протокол маршрутизации EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol) — усовершенствованный внутренний дистанционно–векторный протокол динамической маршрутизации. Практически неиспользуемый протокол IGRP был переработан и улучшен после появления OSPF, компания Cisco представила протокол EIGRP. Существуют

две основные версии протокола EIGRP — версия 0 и 1[18]. Протокол EIGRP версии 1 более стабилен и эффективен. Для того чтобы EIGRP–протокол хорошо масштабировался и обеспечивал очень быстрое время конвергенции при минимальном сетевом трафике, он должен быть использован в хорошо спроектированной сети.

Протокол EIGRP более прост в реализации и менее требователен к вычислительным ресурсам маршрутизатора, чем протокол OSPF. У EIGRP более продвинутый алгоритм вычисления метрики (используется минимальная пропускная способность, что позволяет определять более точно выгодный маршрут и усовершенствованная формула вычисления метрики позволяет учитывать загрузку и надежность интерфейсов на пути).

Протокол EIGRP в отличии от OSPF не использует выделенный маршрутизатор для рассылки маршрутной информации в локальной сети, но позволяет суммировать маршруты вручную на любом маршрутизаторе в сети и балансировать нагрузку как по маршрутам с равной, так и по маршрутам с отличающейся метрикой.

Недостатком протокола EIGRP является его ограниченность в его использовании только на оборудовании компании Cisco. EIGRP–маршрутизаторы пересылают друг другу как полные, так и частичные обновления маршрутной информации.

Протокол EIGRP включает функции, которые обычно отсутствуют в других дистанционно–векторных протоколах маршрутизации, как RIP и IGRP. Эти функции включают:

• RTP (Real–time Transport Protocol) — работает на прикладном уровне и используется при передаче трафика реального времени;
• ограниченные обновления;
• DUAL (англ. Diffusing Update Algorithm) — диффузионный алго–
ритм обновления;
• установление смежности;
• таблицы соседей;
• таблица топологии.

Для расчета метрик маршрутизации протокол EIGRP использует минимальную пропускную способность маршрута до ко-

[18] Руководство Cisco по междоменной многоадресной маршрутизации. . — М.: «Вильямс», 2004. — 320с.

нечного адреса, а также суммарную задержку. Можно также настроить и другие метрики.

Метрики пропускной способности и задержки определяются на основе значений, установленных на интерфейсах маршрутизаторов, которые являются частью маршрута к сети назначения.

Метрика протокола EIGRP рассчитывается по формуле:

Метрика = ((10000000/МПП) + КЗ) х 256.

МПП — это минимальная полоса пропускания (Кб/сек),

КЗ — кумулятивная задержка на маршруте.

Три основных этапа работы протокола:

1. Обнаружение соседних устройств. EIGRP–маршрутизаторы (маршрутизаторы, в которых запущен процесс EIGRP–маршрутизации и которые подключены к одной и той же подсети) рассылают hello–сообщения, чтобы обнаружить соседние маршрутизаторы и проверить их основные конфигурационные параметры.

2. Обмен топологической информацией. Соседние часто называемые смежными устройства обмениваются полной информацией о топологии сети при включении, а впоследствии пересылают друг другу только частичные анонсы, содержащие информацию об изменениях в сетевой топологии.

3. Выбор оптимальных маршрутов. Каждый EIGRP–маршрутизатор анализирует топологическую таблицу и выбирает из нее маршруты с наименьшей метрикой к каждой подсети [28]. В маршрутизаторе хранятся таблицы маршрутизации соседних устройств (англ. neighbor table), топологии и маршрутизации. Оптимальная таблица маршрутизации соседних устройств обеспечивает надежную и упорядоченную доставку пакетов.

Потенциальными EIGRP–соседями считаются устройства, от которых получено hello–сообщение, а далее проверяются следующие параметры:

- аутентификацию (совпадение пароля);
- совпадение номера автономной системы;
- IP адрес устройства EIGRP–соседа должен находиться в той же подсети.

По умолчанию hello–пакеты отправляются каждые 5 секунд для установления отношений соседства, но с небольшим случайным отклонением, которое используется для того, чтобы между маршрутизаторами не было синхронизации в отправке

пакетов. Если за период удержания от соседнего маршрутизатора не пришел ни один hello–пакет, то он считается недоступным.

В таблице соседних устройств содержаться следующие поля:

• address — IP–адрес соседнего устройства, например, 192.168.0.5;

• interface — интерфейс к которому подключено соседнее устройство, например, FastEthernet 0/0;

• hold uptime (время удержания) — время по истечении, которого при отсутствии каких–либо сообщений от соседнего устройства, канал рассматривается как неработоспособный, например, 00:00:30 (сек);

• SRTT (таймер цикла обмена сообщениями) — среднее время, требуемое для отправки пакета соседнему устройству и получению ответного пакета от него. С помощью этого интервала определяется интервал повторной передачи RTI (Retransmit Interval), например, 40 (миллисекунды);

• RTO (retransmission timeout) — интервал между отправкой unicast–пакетов, которые отправляются после того как от соседа не было получено подтверждение о получении multicast–пакета, например, 1000;

• queue count (счетчик очереди) — показывает число пакетов, которые находятся в очереди и ожидают передачи. Обычно это число равно нулю, если нет, то значит маршрутизатор испытывает перегрузку, например, 0;

• sec num (sequence number, номер последовательности) — номер последнего пакета, полученного от соседнего устройства, используется в протоколе EIGRP для подтверждения приема пакета, например, 25.

В протоколе EIGRP используются обновления маршрутов для обмена топологической информацией. Такие сообщения рассылаются по broadcast адресу 224.0.0.10, если устройство передает информацию маршрутизаторам в той же самой подсети; если же обновление маршрутов передается устройству в другой подсети, то оно пересылается на unicast адрес конкретного маршрутзатора.

4.3. Протокол маршрутизации RIP

RIP (Routing Information Protocol) — наиболее распространенный внутренний протокол, основанный на дистанционно–векторной маршрутизации, широко используемый в сетях малого раз-

мера, использует алгоритм Беллмана–Форда, является одним из самых простых протоколов маршрутизации. Каждые 30 секунд он передает в сеть свою таблицу маршрутизации.

Преимущество протокола это простота конфигурирования. Недостатки — увеличение трафика при периодической рассылке широковещательных пакетов и не оптимальность найденного маршрута.

Версии RIP — RIPv1 и RIPv2, а также для работы в среде IPv6 была разработана версия RIPng.

Принцип действия дистанционно–векторного алгоритма: каждый маршрутизатор периодически и широковещательно рассылает по сети вектор, компонентами которого является расстояния от данного маршрутизатора до всех известных ему метрик.

RIP не является универсальным протоколом внутренней маршрутизации. Дистанционно–векторные алгоритмы хорошо работают только в небольших сетях, так как в больших сетях они засоряют линии связи интенсивным трафиком. Протокол RIP заменяет запись о какой–либо сети только, если новая информация имеет лучшую метрику (с меньшим расстоянием), чем уже существующий.

Маршрутизаторы RIP адаптируется сложнее к изменениям, связанным с потерей какого–либо маршрута (длительные периоды нестабильной работы), чем к появлению новых маршрутов. Все это происходит из–за того, что в формате сообщений протокола нет поля для указания отсутствия сети.

Протокол имеет несколько методов для решения проблем, образующихся между соседними петлями.

1. Split horizon. Метод split horizon заключается в том, что маршрутная информация о некоторой сети, хранящаяся в таблице маршрутизации, никогда не передается маршрутизатору, от которого она получена.

2. Triggered update. Triggered update получив данные об изменении метрики до какой–либо сети, маршрутизатор не ждет истечения периода передачи таблицы маршрутизации, а передает данные об изменившемся маршруте немедленно.

3. Hold down. Hold down вводит тайм–аут на принятие новых данных о только что ставшей недоступной сети и предотвращает принятие устаревших сведений в отличии от triggered update и передает устаревшие сведения о ее работоспособности. В течение

тайм–аута замораживания изменений эти маршрутизаторы вычеркнут данный маршрут из своих таблиц, так как не получат о нем новых записей и не будут распространять устаревшую информацию.

RIP использует широковещательные User Datagram Protocol (UDP) пакеты данных для обмена маршрутной информацией. Программное обеспечение Cisco IOS посылает маршрутные обновления каждые 30 секунд, это называется вещанием или рассылкой. Если маршрутизатор не получает обновления от другого маршрутизатора в течение 180 секунд или более, он помечает маршруты, обслуживаемые не обновляемым маршрутизатором как непригодные. Если через 240 секунд до сих пор нет обновления, маршрутизатор удаляет все записи в таблице маршрутизации не обновляемого маршрутизатора[19].

Протокол RIPv2 отличается от RIPv1 тем, что может работать по мультикасту, т.е. по мультикаст адресу, а также передает данные о масках сетей. RIPv1 распространяет между маршрутизаторами информацию только о номерах сетей и расстояниях до них. В улучшенной версии протокола RIPv2 повышена безопасность т.к. была введена дополнительная маршрутная информация.

В качестве расстояния до сети стандарты протокола RIP допускают различные виды метрик, учитывающие пропускную способность T, вносимые задержки D и надежность сетей R (то есть соответствующие признакам D, T и R в поле «Качество сервиса» IP–пакета), а также любые комбинации этих метрик. Метрика должна обладать свойством аддитивности – метрика составного пути должна быть равна сумме метрик составляющих этого пути. В большинстве реализации RIP используется простейшая метрика – количество хопов, то есть количество промежуточных маршрутизаторов, которые нужно преодолеть пакету до сети назначения.

Рассмотрим процесс построения таблицы маршрутизации с помощью протокола RIP на примере составной сети, изображенной на рис. 4.3.

Этап 1 – создание минимальных таблиц. В этой сети имеется восемь IP–сетей, связанных четырьмя маршрутизаторами с идентификаторами: Ml, M2, M3 и M4.

[19] Sosinsky, Barrie. "TCP - UDP Port Assignments". Networking Bible. Wiley Publishing. p. 851. ISBN 978-0-470-43131-3. OCLC 471462746 – via Google Books.

В исходном состоянии в каждом маршрутизаторе стеком TCP/IP автоматически создается минимальная таблица маршрутизации, где учитываются непосредственно подсоединенные сети. На рис.4.3. адреса портов маршрутизаторов в отличие от адресов сетей помещены в овалы.

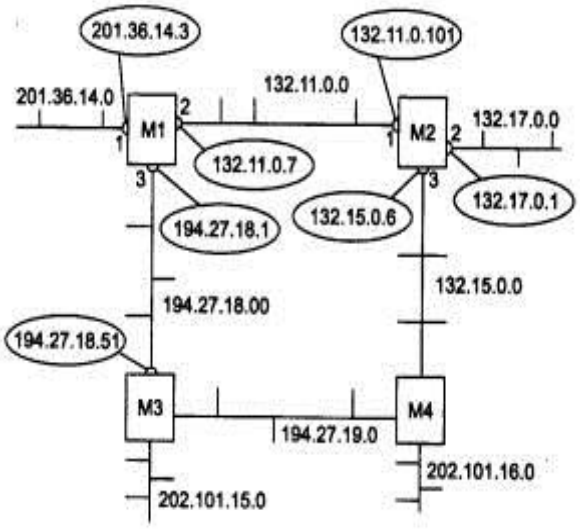

Рис. 4.3. Сеть, объединенная RIP–маршрутизаторами

Таблица 4.1. Минимальная таблица маршрутизации Ml

Номер сети	Адрес следующего маршрутизатора	Порт	Расстояние
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1

Этап 2–рассылка минимальных таблиц. После инициализации каждого маршрутизатора он начинает посылать своим соседям сообщения протокола RIP, в которых содержится его минимальная таблица.

RIP–сообщения передаются в пакетах протокола UDP и включают два параметра для каждой сети: ее IP–адрес и расстояние до нее от передающего сообщение маршрутизатора.

Соседями являются те маршрутизаторы, которым данный маршрутизатор непосредственно может передать IP–пакет по какой–либо своей сети, не пользуясь услугами промежуточных маршрутизаторов. Например, для маршрутизатора Ml соседями являются маршрутизаторы М2 и М3, а для маршрутизатора М4 – маршрутизаторы М2 и М3.

Таким образом, маршрутизатор Ml передает маршрутизатору М2 и М3 следующее сообщение:
сеть 201.36.14.0, расстояние 1;
сеть 132.11.0.0, расстояние 1;
сеть 194.27.18.0, расстояние 1.

Этап 3 – получение RIP–сообщений от соседей и обработка полученной информации. После получения аналогичных сообщений от маршрутизаторов М2 и М3 маршрутизатор Ml наращивает каждое полученное поле метрики на единицу. Маршрутизатор запоминает, через какой порт и от какого маршрутизатора получена новая информация (адрес этого маршрутизатора будет адресом следующего маршрутизатора, если эта запись будет внесена в таблицу маршрутизации). Маршрутизатор начинает сравнивать новую информацию с той, которая хранится в его таблице маршрутизации (табл. 4.2).

Таблица 4.2. Таблица маршрутизации M1

Номер сети	Адрес следующего маршрутизатора	Порт	Расстояние
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1
132.17.0.0	132.11.0.101	2	2
194.27.19.0	194.27.18.51	3	2
202.101.15.0	194.27.18.51	3	2
132.11.0.0	132.11.0.101	2	1
194.27.18.0	194.27.18.51	3	2

Записи с четвертой по девятую получены от соседних маршрутизаторов, и они претендуют на помещение в таблицу. Однако только записи с четвертой по седьмую попадают в таблицу, а записи восьмая и девятая – нет. Это происходит потому, что они содержат данные об уже имеющихся в таблице Ml сетях, а расстояние до них хуже, чем в существующих записях.

Протокол RIP замещает запись о какой–либо сети только в том случае, если новая информация имеет лучшую метрику (расстояние в хопах меньше), чем имеющаяся. В результате в таблице маршрутизации о каждой сети остаётся только одна запись; если же имеется несколько равнозначных в отношении расстояния путей к одной и той же сети, то все равно в таблице остается одна запись,

которая пришла в маршрутизатор первая по времени. Для этого правила существует исключение – если худшая информация о какой–либо сети пришла от того же маршрутизатора, на основании сообщения которого была создана данная запись, то худшая информация замещает лучшую. Аналогичные операции с новой информацией выполняют и остальные маршрутизаторы сети.

Этап 4 – рассылка новой таблицы соседям. Каждый маршрутизатор отсылает новое RIP–сообщение всем своим соседям. В этом сообщении он помещает данные о всех известных ему сетях – как непосредственно подключенных, так и удаленных, о которых маршрутизатор узнал из RIP–сообщений.

Этап 5 – получение RIP–сообщений от соседей и обработка полученной информации. Этап 5 повторяет этап 3 – маршрутизаторы принимают RIP–сообщения, обрабатывают содержащуюся в них информацию и на ее основании корректируют свои таблицы маршрутизации. Рассмотрим последовательность работы маршрутизатора Ml (табл. 4.3).

На этом этапе маршрутизатор Ml получил от маршрутизатора М3 информацию о сети 132.15.0.0, которую тот в свою очередь на предыдущем цикле работы получил от маршрутизатора М4. Маршрутизатор знает о сети 132.15.0.0, старая информация имеет лучшую метрику, чем новая, новая информация об этой сети отбрасывается. О сети 202.101.16.0 маршрутизатор Ml узнает на этом этапе впервые, причем данные о ней приходят от двух соседей – от М3 и М4. Поскольку метрики в этих сообщениях указаны одинаковые, то в таблицу попадают данные, которые пришли первыми.

Таблица 4.3. Таблица маршрутизации маршрутизатора М1

Номер сети	Адрес следующего маршрутизатора	Порт	Расстояние
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1
132.17.0.0	132.11.0.101	2	2
132.15.0.0	132.11.0.101	3	2
~~132.15.0.0~~	~~194.27.18.51~~	~~3~~	~~3~~
~~202.101.15.0.0~~	~~194.27.18.51~~	~~3~~	~~2~~
202.101.16.0.	132.11.0.101	2	3
~~202.101.16.0.~~	~~194.27.18.51~~	~~3~~	~~3~~

В нашем примере считается, что маршрутизатор М2 опередил маршрутизатор М3 и первым переслал свое RIP–сообщение маршрутизатору Ml.

Если маршрутизаторы периодически повторяют этапы рассылки и обработки RIP–сообщений, то за конечное время в сети установится корректный режим маршрутизации. Под корректным режимом маршрутизации здесь понимается такое состояние таблиц маршрутизации, когда все сети будут достижимы из любой сети с помощью некоторого рационального маршрута. Пакеты будут доходить до адресатов и не зацикливаться в петлях, которая образуется маршрутизаторами М1–М2–М3–М4.

Для адаптации к изменениям в сети протокол RIP использует ряд механизмов. К новым маршрутам RIP–маршрутизаторы приспосабливаются просто – они передают новую информацию в очередном сообщении своим соседям и постепенно эта информация становится известна всем маршрутизаторам сети. А вот к отрицательным изменениям, связанным с потерей какого–либо маршрута, RIP–маршрутизаторы приспосабливаются сложнее. Это связано с тем, что в формате сообщений протокола RIP нет поля, которое бы указывало на то, что путь к данной сети больше не существует.

Вместо этого используются два механизма уведомления о том, что некоторый маршрут недействителен:

- истечение времени жизни маршрута;
- указание специального расстояния (бесконечности) до сети, ставшей недоступной.

Для отработки первого механизма каждая запись таблицы маршрутизации (как и записи таблицы продвижения моста/коммутатора), полученная по протоколу RIP, имеет время жизни (TTL). При поступлении очередного RIP–сообщения, которое подтверждает справедливость данной записи, таймер TTL устанавливается в исходное состояние, а затем из него каждую секунду вычитается единица. Если за время тайм–аута не придет новое маршрутное сообщение об этом маршруте, то он помечается как недействительный.

Время тайм–аута связано с периодом рассылки векторов по сети. В RIP IP период рассылки выбран равным 30 секундам, а в качестве тайм–аута выбрано шестикратное значение периода рассылки, то есть 180 секунд. Выбор достаточно малого времени

периода рассылки объясняется несколькими причинами. Шестикратный запас времени нужен для уверенности в том, что сеть действительно стала недоступна, а не просто произошли потери RIP–сообщений (а это возможно, так как RIP использует транспортный протокол UDP, который не обеспечивает надежной доставки сообщений).

Если какой–либо маршрутизатор отказывает и перестает слать своим соседям сообщения о сетях, которые можно достичь через него, то через 180 секунд все записи, которые породил этот маршрутизатор, станут недействительными у его ближайших соседей. После этого процесс повторится уже для соседей ближайших соседей – они вычеркнут подобные записи уже через 360 секунд, так как первые 180 секунд ближайшие соседи еще передавали сообщения об этих записях.

Рассмотрим случай зацикливания пакетов на примере сети, изображенной на рис. 4.3. Пусть маршрутизатор Ml обнаружил, что его связь с непосредственно подключенной сетью 201.36.14.0 потеряна (например, по причине отказа интерфейса 201.36.14.3). Ml отметил в своей таблице маршрутизации, что сеть 201.36.14.0 недоступна. В худшем случае он обнаружил это сразу же после отправки очередных RIP–сообщений, так что до начала нового цикла его объявлений, в котором он должен сообщить соседям, что расстояние до сети 201.36.14.0 стало равным 16, остается почти 30 секунд.

Каждый маршрутизатор работает на основании своего внутреннего таймера, не синхронизируя работу по рассылке объявлений с другими маршрутизаторами. Поэтому весьма вероятно, маршрутизатор М2 опередил маршрутизатор Ml и передал ему свое сообщение раньше, чем Ml успел передать новость о недостижимости сети 201.36.14.0. А в этом сообщении имеются данные, порожденные следующей записью в таблице маршрутизации М2 (табл. 4.4).

Таблица 4.4. Таблица маршрутизации маршрутизатора М2

Номер сети	Адрес следующего маршрутизатора	Порт	Расстояние
201.36.14.0	132.11.0.7	1	2

Эта запись была получена от маршрутизатора Ml и корректна до отказа интерфейса 201.36.14.3, а теперь она устарела, но маршрутизатор М2 об этом не узнал.

Теперь маршрутизатор Ml получил новую информацию о сети 201.36.14.0 – эта сеть достижима через маршрутизатор М2 с метрикой 2. Раньше Ml также получал эту информацию от М2. Но игнорировал ее, так как его собственная метрика для 201.36.14.0 была лучше. Теперь Ml должен принять данные о сети 201.36.14.0, полученные от М2, и заменить запись в таблице маршрутизации о недостижимости этой сети (табл. 4.5.).

Таблица 4.5.Таблица маршрутизации маршрутизатора М1

Номер сети	Адрес следующего маршрутизатора	Порт	Расстояние
201.36.14.0	132.11.0.101	2	3

В результате в сети образовалась маршрутная петля: пакеты, направляемые узлам сети 201.36.14.0, будут передаваться маршрутизатором М2 маршрутизатору Ml, а маршрутизатор Ml будет возвращать их маршрутизатору М2. IP–пакеты будут циркулировать по этой петле до тех пор, пока не истечет время жизни каждого пакета.

Маршрутная петля будет существовать в сети достаточно долго. Рассмотрим периоды времени, кратные времени жизни записей в таблицах маршрутизаторов.

- Время 0–180 с. После отказа интерфейса в маршрутизаторах Ml и М2 будут сохраняться некорректные записи, приведенные выше. Маршрутизатор М2 по–прежнему снабжает маршрутизатор Ml своей записью о сети 201.36.14.0 с метрикой 2, так как ее время жизни не истекло. Пакеты зацикливаются.
- Время 180–360 с. В начале этого периода у маршрутизатора М2 истекает время жизни записи о сети 201.36.14.0 с метрикой 2, так как маршрутизатор Ml в предыдущий период посылал ему сообщения о сети 201.36.14.0 с худшей метрикой, чем у М2, и они не могли подтверждать эту запись. Теперь маршрутизатор М2 принимает от маршрутизатора Ml запись о сети 201.36.14.0 с метрикой 3 и трансформирует ее в запись с метрикой 4. Маршрутизатор Ml не получает новых сообщений от маршрутизатора М2 о сети 201.36.14.0 с метрикой 2, поэтому время жизни его записи начинает уменьшаться. Пакеты продолжают зацикливаться.

- Время 360–540 с. Теперь у маршрутизатора Ml истекает время жизни записи о сети 201.36.14.0 с метрикой 3. Маршрутизаторы Ml и М2 опять меняются ролями – М2 снабжает Ml устаревшей информацией о пути к сети 201.36.14.0, уже с метрикой 4, которую Ml преобразует в метрику 5. Пакеты продолжают зацикливаться. Если бы в протоколе RIP не было выбрано расстояние 16 в качестве недостижимого, то описанный процесс длился бы до бесконечности.

В результате маршрутизатор М2 на очередном этапе описанного процесса получает от маршрутизатора Ml метрику 15, которая после наращивания, превращаясь в метрику 16, фиксирует недостижимость сети. Период нестабильной работы сети длился 36 минут.

Ограничение в 15 хопов сужает область применения протокола RIP до сетей, в которых число промежуточных маршрутизаторов не может быть больше 15. Для более масштабных сетей нужно применять другие протоколы маршрутизации или разбивать сеть на автономные области.

Приведенный пример хорошо иллюстрирует главную причину нестабильной работы маршрутизаторов, работающих по протоколу RIP. Эта причина коренится в самом принципе работы дистанционно–векторных протоколов – пользовании информацией, полученной из вторых рук. Действительно, маршрутизатор М2 передал маршрутизатору Ml информацию о достижимости сети 201.36.14.0, за достоверность которой он сам не отвечает.

Методы борьбы с ложными маршрутами в протоколе RIP.

Протокол RIP не в состоянии полностью исключить переходные состояния в сети, имеется несколько методов, которые во многих случаях решают подобные проблемы.

Ситуация с петлей, образующейся между соседними маршрутизаторами, описанная в предыдущем разделе, надежно решается с помощью метода, получившем название расщепления горизонта (split horizon). Метод заключается в том, что маршрутная информация о некоторой сети, хранящаяся в таблице маршрутизации, никогда не передается тому маршрутизатору, от которого она получена (это следующий маршрутизатор в данном маршруте). Если маршрутизатор М2 в рассмотренном выше примере поддерживает технику расщепления горизонта, то он не передаст маршрутизатору Ml

устаревшую информацию о сети 201.36.14.0, так как получил ее именно от маршрутизатора Ml.

Практически все сегодняшние маршрутизаторы, работающие по протоколу RIP, используют технику расщепления горизонта.

Однако расщепление горизонта не помогает в тех случаях, когда петли образуются не двумя, а несколькими маршрутизаторами. Рассмотрим более детально ситуацию, которая возникнет в сети, приведенной на рис. 4.1, в случае потери связи маршрутизатора 2 с сетью А. Пусть все маршрутизаторы этой сети поддерживают технику расщепления горизонта. Маршрутизаторы М2 и М3 не будут возвращать маршрутизатору в этой ситуации данные о сети 201.36.14.0 с метрикой 2, так как они получили эту информацию от маршрутизатора Ml. Однако они будут передавать маршрутизатору информацию о достижимости сети 201.36.14.0 с метрикой 4 через себя, так как получили эту информацию по сложному маршруту, а не от маршрутизатора Ml непосредственно. Например, маршрутизатор М2 получил эту информацию по цепочке М4–М3–М1. Поэтому маршрутизатор Ml снова может быть обманут, пока каждый из маршрутизаторов в цепочке М3–М4–М2 не вычеркнет запись о достижимости сети 1 (а это произойдет через период 3 х 180 секунд).

Для предотвращения зацикливания пакетов по составным петлям при отказах связей применяются два других приема, называемые триггерными обновлениями (triggered updates) и замораживанием изменений (hold down).

Способ триггерных обновлений состоит в том, что маршрутизатор, получив данные об изменении метрики до какой–либо сети, не ждет истечения периода передачи таблицы маршрутизации, а передает данные об изменившемся маршруте немедленно. Этот прием может во многих случаях предотвратить передачу устаревших сведений об отказавшем маршруте, но он перегружает сеть служебными сообщениями, поэтому триггерные объявления также делаются с некоторой задержкой. Поэтому возможна ситуация, когда регулярное обновление в каком–либо маршрутизаторе чуть опередит по времени приход триггерного обновления от предыдущего в цепочке маршрутизатора и данный маршрутизатор успеет передать по сети устаревшую информацию о несуществующем маршруте.

Второй прием позволяет исключить подобные ситуации. Он связан с введением тайм–аута на принятие новых данных о сети,

которая только что стала недоступной. Этот тайм–аут предотвращает принятие устаревших сведений о некотором маршруте от тех маршрутизаторов, которые находятся на некотором расстоянии от отказавшей связи и передают устаревшие сведения о ее работоспособности.

Протокол BGP. Border Gateway Protocol (BGP) предназначен для маршрутизации между автономными системами[20]. Этот протокол включает в себя защиту от "зацикливания". Автономная система (АС) – это набор роутеров, которые работают под управлением одного администратора, или одной группы администраторов, и используют общую стратегию маршрутизации.

Общая схема работы BGP такова. BGP–маршрутизаторы соседних АС, решившие обмениваться маршрутной информацией, устанавливают между собой соединения по протоколу BGP и становятся BGP–соседями (BGP–peers). Далее BGP использует подход под названием path vector, являющийся развитием дистанционно–векторного подхода. BGP–соседи рассылают друг другу векторы путей (path vectors). Вектор путей, в отличие от вектора расстояний, содержит не просто адрес сети и расстояние до нее, а адрес сети и список атрибутов (path attributes), описывающих различные характеристики маршрута от маршрутизатора–отправителя в указанную сеть.

Данных, содержащихся в атрибутах пути, должно быть достаточно, чтобы маршрутизатор–получатель, проанализировав их с точки зрения политики своей АС, мог принять решение о приемлемости или неприемлемости полученного маршрута.

Пара BGP–соседей устанавливает между собой соединение по протоколу TCP, порт 179. Соседи, принадлежащие разным АС, должны быть доступны друг другу непосредственно; для соседей из одной АС такого ограничения нет, поскольку протокол внутренней маршрутизации обеспечит наличие всех необходимых маршрутов между узлами одной автономной системы.

Поток информации, которым обмениваются BGP–соседи по протоколу TCP, состоит из последовательности BGP–сообщений. Максимальная длина сообщения 4096 октетов, минимальная – 19. Имеется 4 типа сообщений.

[20] Хелд Г. Технологии передачи данных. СПб.: Питер, 2003. 720 с.

Типы BGP–сообщений. OPEN – посылается после установления TCP–соединения[21]. Ответом на OPEN является сообщение KEEPALIVE, если вторая сторона согласна стать BGP–соседом; иначе посылается сообщение NOTIFICATION с кодом, поясняющим причину отказа, и соединение разрывается.

KEEPALIVE – сообщение предназначено для подтверждения согласия установить соседские отношения, а также для мониторинга активности открытого соединения: для этого BGP–соседи обмениваются KEEPALIVE–сообщениями через определенные интервалы времени.

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

NOTIFICATION – сообщение этого типа используется для информирования соседа о причине закрытия соединения. После отправления этого сообщения BGP–соединение закрывается.

Выводы

Протокол маршрутизации OSPF– это протокол динамической маршрутизации, который основан на технологии отслеживания состояния канала LSA и использовании алгоритма Дейкстры, ориентированного на применение в больших гетерогенных сетях. OSPF не использует протокол транспортного уровня, так как пакеты OSPF отправляются посредством IP. Протокол OSPF использует hello–пакеты для обнаружения соседних компонентов сети и распространения параметров и т. д.

Протокол реализует деление автономной системы на зоны, что позволяет снизить нагрузку на сеть.

Протокол EIGRP– это внутренний дистанционно–векторный протокол динамической маршрутизации, имеет простую реализацию, менее требователен к вычислительным ресурсам маршрутизатора, чем протокол OSPF, а также использует более продвинутый алгоритм вычисления метрики: минимальная пропускная способ-

[21] 1. Филимонов А.Ю. Построение мультисервисных сетей Ethernet. СПб.: БХВ-Петербург, 2007. – 592 с.,

2. Barr, M., Massa, A.N. Programming embedded systems: with C and GNU

development tools / M. Barr, A.N Massa. – Sebastopol: O'Reilly Media Inc., 2006. – 301 p. – ISBN 0596009836.

ность. Это позволяет определять более точно оптимальный маршрут с учетом загрузки и надежности интерфейсов сети.

Недостатком протокола EIGRP является его ограниченность в его использовании только на оборудовании компании Cisco.

Для расчета метрик маршрутизации протокол EIGRP использует минимальную пропускную способность маршрута до конечного адреса, а также суммарную задержку.

RIP внутренний протокол, основанный на дистанционно–векторной маршрутизации, широко используемый в сетях малого размера, использует алгоритм Беллмана–Форда, является одним из самых простых протоколов маршрутизации. Каждые 30 секунд он передает в сеть свою таблицу маршрутизации.

Преимущество протокола — простота конфигурирования. Недостатки — увеличение трафика при периодической рассылке широковещательных пакетов и не оптимальность найденного маршрута.

BGP – внешний протокол предназначен для маршрутизации между автономными системами на основе дистанционно–векторного подхода. Вектор путей, в отличие от вектора расстояний, содержит адрес сети и список атрибутов, описывающих различные характеристики маршрута от маршрутизатора–отправителя в указанную сеть.

4.4. Вопросы и упражнения

1. В чем состоит отличие задач, решаемых протоколами сетевого уровня в локальных и глобальных сетях?
2. Сравните таблицу коммутатора с таблицей маршрутизатора. Каким образом они формируются? Какую информацию содержат? От чего зависит их объем?
3. Таблица маршрутизации содержит записи о сетях назначения. Должна ли она содержать записи обо всех сетях составной сети или только о некоторых? Если только о некоторых, то о каких именно?
4. Может ли в таблице маршрутизации иметься несколько записей о маршрутизаторах по умолчанию?

A. Каждый порт коммутатора имеет MAC – адрес.
B. Каждый коммутатор имеет сетевой адрес.
C. Каждый порт коммутатора имеет сетевой адрес.
D. Каждый маршрутизатор имеет сетевой адрес.

E. Каждый порт маршрутизатора имеет MAC – адрес.
F. Каждый порт маршрутизатора имеет сетевой адрес.
5. Отличается ли обработка поля MAC – адреса кадра маршрутизатором и коммутатором?
6. Сравните функции маршрутизаторов, которые поддерживают маршрутизацию от источника, с функциями маршрутизаторов, поддерживающих протоколы адаптивной маршрутизации.
7. Какие метрики расстояния могут быть использованы в алгоритмах сбора маршрутной информации?
8. Сравните интенсивность широковещательного трафика, порождаемого протоколами RIP и OSPF.
9. Какие элементы сети могут выполнять фрагментацию?
G. только компьютеры;
H. только маршрутизаторы;
I. компьютеры, маршрутизаторы, мосты, коммутаторы;
J. компьютеры и маршрутизаторы.
10. Что произойдет, если при передаче пакета он был фрагментирован и один из фрагментов не дошел до узла назначения после истечения тайм–аута?
K. модуль IP узла–отправителя повторит передачу недошедшего фрагмента;
L. модуль IP узла–отправителя повторит передачу всего пакета, в состав которого входил недошедший фрагмент;
M. модуль IP узла–получателя отбросит все полученные фрагменты пакета, в котором потерялся один фрагмент; модуль IP узла–отправителя не будет предпринимать никаких действий по повторной передаче пакета данного пакета.
11. Каким образом должен быть сконфигурирован маршрутизатор, чтобы он предотвращал «широковещательный шторм»?

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Постановление Президента Республики Узбекистан «О мерах по дальнейшему совершенствованию системы управления проектами в сфере информационно–коммуникационных технологий» № ПП–3415, 30.11. 2017.
2. Постановление Кабинета Министров Республики Узбекистан «О по дальнейшему улучшению качества услуг связи, информатизации и телекоммуникаций, N 185, 07.03.2018.
3. Аллан Леинванд, Брюс Пински, «Конфигурирование маршрутизаторов Cisco», 2001.
4. Велихов А.В. Компьютерные сети: уч. пособие по администрированию локальных и объединенных сетей /А.В.Велихов, К.С. Строчников Б.К. Леонтьев. — М.: ЗАО "Новый изд. дом", 2005. —– 304 с.
5. Димарцио Д.Ф. «Маршрутизаторы Cisco. Пособие для самостоятельного изучения», 2005.
6. Kubilinskas E. Designing Resilient and Fair Multi–layer Telecommunication Networks. / Kubilinskas E. – Lund Institute of Technology, 2005.
7. Кульгин М. Компьютерные сети. Практика построения. — СПб.: Питер, 2003. — 462 с.
8. Компьютеры, сети, Интернет: энциклопедия / Новиков Ю., Новиков Д., Черепанов А., Чуркин В. — СПб.: Питер, 2002. — 928с.
9. Леинванд А., Пински Б. Конфигурирование маршрутизаторов Cisco. — 2–е изд –М:Изд.дом«Вильямс», 2004. — 368с.
10. Мусаев М.М.“Компьютер тизимлари ва тармоқлари”. Тошкент.: “Aloqachi” нашриёти, 2013.—394б. — Олий ўқув юртлари учун қўлланма.
11. Новиков Ю.В. Локальные сети: архитектура, алгоритмы, проектирование. / Ю. В. Новиков. — М.: ЭКОМ, 2000. — 312 с.
12. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы Питер, 2005. — 672 с.
13.Руководство Cisco по междоменной многоадресной маршрутизации.— М.: «Вильямс», 2004. — 320с.
14. Руководство пользователя. Коммутаторы локальных сетей D–Link. Учебное пособие, 2004. — 89с.

15.Тарасов К. «Коммутаторы для сегмента передачи данных мультисервисной Metrocети FTTB» журнал «мультисервисные сети», 2009.
16.Стивенс У. Протоколы TCP/IP в подлиннике. Практическое руководство. – М.: BHV, 2003. — 672 с.
17. Фейт С. TCP/IP: Архитектура, протоколы, реализация (включая IP версии 6 и IP Security) — 2–е изд. Copyright © 1997, 1993 by The McGraw–Hill Companies, Inc. ISBN 0–07– 021389–5 McGraw–Hill Издательство "Лори", 2000. ─ 450 с.
18. Флинт Д. Локальные сети ПК: принципы построения, реализаци я/Д. Флинт. — М.: Финансы и статистика, 2001. — 359 с.
19. Филимонов А.Ю. Построение мультисервисных сетей Ethernet. СПб.: БХВ–Петербург, 2007. —592 с.
20. Фейт С. TCP/IP. Архитектура, протоколы, реализация. – М.: Лори, 2015. — 424с.5.
21. Фортенбери Т. Проектирование виртуальных частных сетей в среде Windows 2000. Вильямс. [RUS,320.,2002].
22. Хелд Г. Технологии передачи данных. СПб.: Питер, 2003. — 720 с.
23. Shinder D.L.Osnovy of computer networks: – M.: Williams, 2002. – 656 with.
24. Sosinsky, Barrie. "TCP – UDP Port Assignments". Networking Bible. Wiley Publishing. p. 851. ISBN 978–0–470–43131–3. OCLC 471462746 – via Google Books.
25. Barr, M., Massa, A.N. Programming embedded systems: with C and GNU development tools / M. Barr, A.N Massa. – Sebastopol: O'Reilly Media Inc., 2006. – 301 p. — ISBN 0596009836.

ГЛОССАРИЙ

Адрес Ethernet. 48–битовое значение, являющееся уникальным идентификатором устройства (порта Ethernet) в сети. Обычно записывается 12 шестнадцатеричными цифрами.

Авторизация – процесс определения прав пользователя в системе или сети.

Администратор сети – пользователь, ответственный за планирование, настройку и управление ежедневной работой сети. Администратор сети называется также системным администратором.

Адрес памяти – часть памяти компьютера, которая может быть выделена устройству или использоваться программой или операционной системой.

Алгоритм построения связующего дерева STA (Spanning Tree Algorithm). Алгоритм, используемый протоколом связующего дерева для построения связующего дерева.

Базовая система ввода–вывода – набор базовых программ для проверки оборудования во время запуска, для загрузки операционной системы, а также для поддержки обмена данными между устройствами.

База управляющей информации MIB (Management Information Base). База данных, где хранится информация для управления сетью, которая используется и поддерживается протоколом сетевого управления SNMP. Значение MIB–объекта может быть изменено или извлечено с помощью команд SNMP и сетевой системы управления (например, D–Link D –View) с GUI–интерфейсом. MIB–объекты образуют древовидную структуру с открытыми (стандартными) и закрытыми (частными) ветвями.

Базовый диск – физический диск, к которому может обращаться MS–DOS и все операционные системы семейства Windows.

Беспроводная связь – связь между компьютером и другим компьютером или устройством без использования кабелей.

Бит в секунду – число битов, передаваемых за секунду; используется в качестве единицы измерения скорости, с которой устройство, такое как модем, может передавать данные.

Буфер – область ОЗУ, предназначенная для временного размещения данных при переносе из одного места в другое, например между областью данных приложения и устройством ввода/вывода.

Веб–сервер – компьютер, обслуживаемый системным администратором или поставщиком услуг Интернета (ISP) и предназначенный для обработки запросов клиентских обозревателей.

Виртуальная локальная сеть – логическое объединение узлов одной или нескольких локальных сетей, позволяющее организовать взаимодействие между узлами так, как если бы они находились в одной физической сети.

Виртуальная память – временное хранилище, используемое компьютером для выполнения программ, превышающих размер доступной оперативной памяти.

Виртуальный IP–адрес – IP–адрес, совместно используемый узлами компонента «Балансировка нагрузки сети».

Внешний компьютер – компьютер, использующий другую систему очереди сообщений, однако, благодаря приложению–коннектору, способный обмениваться сообщениями с компьютерами, работающими под управлением системы «Очередь сообщений».

Выделение ресурсов – процесс распределения вычислительных средств системы между ее компонентами, обеспечивающий выполнение задания.

Групповой адрес (Multicast address). Общий адрес, который относится к некоторой группе нескольких сетевых устройств.

Гигабайт (Гбайт) – 1 024 мегабайта, хотя часто принимается приблизительно за один миллиард байтов.

Главный сервер – официальный сервер DNS для зоны. В зависимости от порядка получения данных зоны различают два типа главных серверов — основные и дополнительные.

Глобальная сеть – коммуникационная сеть, соединяющая географически удаленные компьютеры, принтеры и другие устройства.

Группа – совокупность пользователей, компьютеров, контактов и других групп. Группы могут использоваться для управления доступом или в качестве списков рассылки. Группы распространения применяются только в электронной почте.

Датаграмма – один пакет (или единица) данных, включающий сведения о доставке, такие как адрес места назначения, передаваемый по сетям с коммутацией пакетов.

Драйвер сетевой платы – драйвер устройства, обеспечивающий работу сетевой платы (является посредником между платой и драйвером протокола).

Драйвер устройства – программа, позволяющая конкретному устройству, такому как модем, сетевой адаптер или принтер, взаимодействовать с операционной системой.

Дуплексная передача (Full duplex). Одновременная передача данных между станцией–отправителем и станцией– получателем.

Жесткий диск – устройство, содержащее одну или несколько жестких пластин, покрытых магнитным материалом, на который могут быть записаны (или считаны) данные при помощи магнитных головок**.**

Заголовок пакета – предусмотренное сетевыми протоколами специальное поле фиксированной длины, находящееся в начале пакета и содержащее управляющие данные.

Загрузка системы – процесс запуска или перезапуска компьютера. При включении («холодная» загрузка) или сбросе («теплая» загрузка) компьютер выполняет программное обеспечение, загружающее и запускающее его операционную систему, подготавливая ее для дальнейшего использования.

Институт инженеров по электротехнике и радиоэлектронике. IEEE (Institute of Electrical and Electronic Engineers). Профессиональная организация, основанная в 1963 году для координации разработки компьютерных и коммуникационных стандартов. Институт подготовил группу стандартов 802 для локальных сетей. Подкомитет 802 является частью технического комитета по компьютерным коммуникациям (Technical Committee for Computer Communications), основанного в 1980 году для обеспечения совместимости оборудования и программ различных фирм. Членами IEEE являются ANSI и ISO.

Изучение MAC–адресов (MAC address learning). Служба самообучающегося моста, в котором хранится MAC–адрес источника для каждого полученного пакета. Затем эти адреса используются для передачи следующих пакетов только через те мостовые интерфейсы, где расположены эти адреса. Пакеты с нераспознанным адресом передаются через все мостовые интерфейсы. Эта схема позволяет уменьшить трафик через присоединенные локальные сети. Служба изучения MAC–адресов определена в стандарте IEEE 802.1.

IP– протокол (Internet Protocol). Часть стека протоколов TCP/IP, определенного в RFC 791 . Описывает программную маршрутизацию пакетов и адресацию устройств. Стандарт используется для

передачи через сеть базовых блоков данных и дейтаграмм IP. Обеспечивает передачу пакетов без организации соединений и гарантии доставки.

IP–адрес (IP address). Адрес для протокола IP – 32 битовое (4 байта) значение, определенное в STD 5 (RFC 791) и используемое для представления точек подключения в сети TCP/IP. IP–адрес состоит из номера сети (network portion) и номера хоста (host portion) – такое разделение позволяет сделать маршрутизацию более эффективной. Обычно для записи IP–адресов используют десятичную нотацию с разделением точками. Новая версия протокола IPv6 использует 128–разрядные адреса, позволяющие решить проблему нехватки адресного пространства.

Инкапсуляция. Метод, используемый многоуровневыми протоколами, в которых уровни добавляют заголовки в модуль данных протокола (protocol data unit – PDU) из вышележащего.

Кадр (Frame). Единица информации на канальном уровне сетевой модели. В ЛВС кадр представляет собой единицу данных подуровня MAC, содержащую управляющие данные и пакет сетевого уровня.

Коммутатор (Switch). Сетевое устройство, которое фильтрует, пересылает и направляет кадры в зависимости от их адреса приемника. Коммутатор работает на канальном уровне модели OSI.

Коммутируемая сеть (Switched LAN). Локальная сеть с коммутаторами.

Коллизия. Возникает в сети Ethernet, когда два узла одновременно ведут передачу. Передаваемые ими по физическому носителю кадры сталкиваются и разрушаются.

Коллизионный домен. Часть сети Ethernet, все узлы которой распознают коллизию независимо от того, в какой части сети эта коллизия возникла.

Класс обслуживания. CoS (Class of Service). Характеристика, позволяющая определить, как протокол верхнего уровня использует протокол нижнего уровня для обработки его сообщений. Другое название ToS.

Лавинная передача (Flooding) Способ передачи трафика, используемый в коммутаторах и мостах, при котором полученный интерфейсом трафик пересылается всем другим интерфейсам этого устройства.

Локальная сеть LAN (Local Area Network). Высокоскоростная

компьютерная сеть, покрывающая относительно небольшую площадь. Локальные сети объединяют рабочие станции, периферийные устройства, терминалы и другие устройства, находящиеся в одном здании или на другой небольшой территории.

LLC (Logical Link Control) подуровень управления логическим соединением. Высший из двух подуровней канального уровня, определенный IEEE. Управляет обработкой ошибок, потоками, кадрированием, а также адресацией MAC–подуровня. Наиболее распространенным LLC–протоколом является IEEE 802.2. Существуют варианты IEEE 802.2 с подтверждением и без подтверждения.

Межсетевой протокол управления группами IGMP (Internet Group Management Protocol). Протокол, используемый IP–узлами для уведомления смежных широковещательных маршрутизаторов об их участии в широковещательных группах.

MAC (Media Access Control) управление доступом к передающей среде. Низший из двух подуровней канального уровня, определенный IEEE. MAC–подуровень управляет доступом к совместно используемым носителям.

MAC–адрес (MAC address). Стандартный адрес канального уровня, который требуется задавать для каждого порта или устройства, подключенного к локальной сети. Другие устройства используют эти адреса для обнаружения специальных сетевых портов, а также для создания и обновления таблиц маршрутизации и структур данных. Длина MAC–адреса составляет 6 байтов, а их содержимое регламентируется IEEE. MAC–адреса также называют аппаратными или физическими адресами.

Маршрутизация (Routing). Процесс выбора оптимального пути для передачи сообщения.

Модуль передачи максимального размера MTU (Maximum Transmission Unit). Максимальный размер (в байтах) пакета данных, который можно передать через данный интерфейс.

Многоадресная рассылка (Multicast). Режим копирования одиночных пакетов и их передачи заданному подмножеству сетевых адресов. Эти адреса задаются в поле адреса приемника (Destination address field).

Многоадресная группа (Multicast group). Динамически определенная группа IP–узлов, идентифицируемая одним групповым IP–адресом.

Многоадресный маршрутизатор (Multicast router). Маршрутизатор, используемый для передачи IGMP–запросов для присоединенных локальных сетей. Узлы, принадлежащие к многоадресной группе, отвечают на запрос посылкой IGMP–отчетов с обозначением тех широковещательных групп, к которым они относятся. Многоадресный маршрутизатор отвечает за передачу дейтаграмм от данной группы ко всем сетям, которые содержат членов этой группы.

Ethernet. Стандарт организации локальных сетей (ЛВС), описанный в спецификациях IEEE и других организаций.

ETTH (Ethernet to the Home). Цель решения ETTH заключается в передаче данных, речи и видео по простой и недорогой сети Ethernet.

Пакет – единичный набор двоичных данных сетевого уровня OSI (Open Systems Interconnection), состоящий из передаваемых данных и заголовка, содержащего идентификационный номер, адреса источника и назначения, а также данные для контроля ошибок.

Пакет данных – единица информации, передаваемая как целое между двумя устройствами в сети.

Параллельный порт – разъем ввода/вывода для подключения устройств параллельного интерфейса. Большинство принтеров подключаются к параллельному порту.

Периферийное устройство – устройство (такое как дисковый накопитель, принтер, модем или джойстик), подключенное к компьютеру и управляемое процессором компьютера.

ПЗУ – постоянное запоминающее устройство, полупроводниковая память с программами и данными, размещенная в компьютере на стадии его изготовления. ПЗУ доступно для чтения, но не для записи.

Подсеть – подразделение сети IP. Каждая подсеть имеет собственный уникальный номер сети.

Полное имя узла – уникальное доменное имя DNS, однозначно определяющее некоторое место в дереве пространства имен домена.

Пользователи – специальная группа, содержащая всех пользователей, имеющих разрешения пользователя на сервере.

Порт – разъем, к которому подключаются устройства, передающие данные с компьютера и на него.

Последовательный порт – порт компьютера для организации побайтной асинхронной связи.
Приемопередатчик – устройство, способное передавать и принимать сигналы.
Пропускная способность – Разность между максимальной и минимальной частотой для конкретного диапазона в устройстве связи.
Простые службы TCP/IP – четыре службы TCP/IP: Character Generator, Daytime Discard, Echo и Quote of the Day.
Протокол – набор правил и соглашений для передачи данных по сети.
Протокол ARP – в протоколе TCP/IP этот протокол использует широковещательный трафик в локальной сети для разрешения логически назначеного IP–адреса в аппаратный адрес.
Протокол DHCP – протокол службы TCP/IP, обеспечивающий динамическое распределение IP–адресов и других параметров конфигурации между клиентами сети.
Протокол FTP – один из протоколов TCP/IP, используемый для копирования файлов с одного компьютера на другой через Интернет.
Протокол IP – маршрутизируемый протокол семейства TCP/IP, отвечающий за IP–адресацию, маршрутизацию, а также за разбиение на сегменты и повторную сборку пакетов IP.
Протокол TCP/IP – набор широко используемых в Интернете сетевых протоколов, поддерживающий связь между объединенными сетями, состоящими из компьютеров различной архитектуры и с разными операционными системами.
Протокол UDP – дополнительный компонент протокола TCP, поддерживающий выполняющуюся без подключений службу датаграмм, не гарантирующую ни доставку, ни правильную последовательность доставленных пакетов (аналогично протоколу IP).
Простой протокол SNMP (Simple Network Management Protocol) управления сетью. Протокол управления сетью, используемый почти исключительно в сетях TCP/IP. SNMP предоставляет средства контроля и управления сетевыми устройствами, конфигурациями, производительностью
и безопасностью, а также сбора статистической информации.
Протокол связующего дерева STP(Spanning Tree Protocol). Мостовой протокол, использующий алгоритм связующего дерева и позволяющий самообучающемуся мосту динамически обрабаты-

вать петли в сетевой топологии путем создания связующего дерева. Мосты обнаруживают петли путем обмена сообщениями BPDU с другими мостами и ликвидируют их посредством блокирования выбранных мостовых интерфейсов.

Сегмент (Segment).

1. Секция сети, ограниченная мостами, маршрутизаторами или коммутаторами.
2. В LAN с шинной топологией – непрерывная электрическая цепь, часто соединенная с другими сегментами при помощи повторителей.
3. Термин, используемый в спецификации TCP для описания одиночного модуля транспортного уровня.

Сеансовый уровень (Session Layer). Уровень 5 модели OSI, обеспечивающий способы ведения управляющего диалога между системами.

Связующее дерево (Spanning Tree). Нециклическая часть сетевой топологии. Методика коммутации пакетов, согласно которой кадры полностью обрабатываются перед их отправкой через соответствующий порт. Обработка включает расчет CRC и проверку адреса приемника. Кроме того, кадры необходимо временно хранить до тех пор, пока не станут доступными сетевые ресурсы (например, свободный канал) для передачи сообщения. Эта технология противоположна коммутации пакетов без буферизации (cut–through packet switching).

Сетевой уровень (Network Layer). Уровень 3 модели OSI, отвечающий за маршрутизацию, переключение и доступ к подсетям через всю среду OSI.

CSMA/CD (Carrier sense multiple access/collision detection) множественный доступ к среде с обнаружением конфликтов и распознаванием несущей. Механизм доступа, при котором устройства, готовые для передачи данных, сначала проверяют наличие частоты. Если ее нет в течении некоторого заданного промежутка времени, то устройства могут приступать к передаче данных. При одновременной передаче со стороны двух устройств возникает коллизия, которая может быть обнаружена всеми вызвавшими ее устройствами. Такая коллизия, в свою очередь, задерживает повторную передачу данных этими устройствами на некоторое произвольное время. CSMA/CD –доступ используется в Ethernet и IEEE

Сквозная коммутация пакетов (Cut–through packet switching). Способ коммутации, при котором данные проходят через коммутатор таким образом, что ведущий край пакета покидает коммутатор на выходном порте еще до того, как закончится прием пакета на входном порте. Устройство со сквозной коммутацией пакетов считывает, обрабатывает и передает пакеты сразу после определения адреса приемника и выходного порта. Этот способ также называется оперативной коммутацией пакетов.

Рабочая группа – объединение компьютеров, предназначенное для упрощения поиска пользователями таких объектов, как принтеры и общие папки.

Терминал – устройство, состоящее из монитора и клавиатуры, используемое для обмена данными с компьютером.

Тип коммутатора – тип интерфейса, к которому подключено устройство ISDN. Тип коммутатора называется также просто коммутатором.

Топология – система отношений между компонентами сети Windows.

Транспортный уровень (Transport Layer). Уровень 4 модели OSI, отвечающий за надежную передачу данных между конечными системами.

Таблица пересылки (Forwarding table). Таблица, содержащая идентификаторы и адреса, а также пределы рассылки адресов.

Удаленный компьютер – компьютер, доступный пользователю только с применением коммуникационных линий и устройств, таких как сетевая плата или модем.

Узел сети – компьютер с операционной системой Windows, выполняющий программу сервера или службу, используемую сетью или удаленными клиентами.

Устройство – любое оборудование, которое может быть подсоединено к локальной сети или компьютеру.

Управление потоком (Flow control). Методы, используемые для контроля за передачей данных между двумя точками сети и позволяющие избегать потери данных в результате переполнения приемных буферов.

Хорошо организованная сеть – уровень связи, обеспечивающий удобную работу клиентов в сети и с Active Directory.

Фильтрация (Filtering) Процесс проверки пакетов данных в сети и определения адресатов для принятия решения о даль-

нейшей пересылке (данная ЛВС, удаленная ЛВС) или отбрасывании пакета. Фильтрация пакетов выполняется мостами, коммутаторами и маршрутизаторами.

Шлюз – устройство, соединяемое с несколькими физическими сетями TCP/IP и обеспечивающее маршрутизацию и доставку пакетов IP между этими сетями.

Учебное пособие по предмету Коммуникация данных» для бакалавров по направлению 5330500 – «Компьютерный инжиниринг»

Рассмотрено на заседании кафедры «Компьютерные системы»
от «15» мая 2018г. Протокол № 22

Рассмотрено на заседании факультета «Компьютерный инжиниринг»
от «22» мая 2018г. Протокол № 34

Рассмотрено и рекомендовано к изданию на заседании научно–методического Совета ТУИТ
от «___»___2018г. Протокол № _____

Составитель Назаров А.И.

Рецензенты: Каххаров А.А.

Турсунбаев Ф.К.

Ответственный редактор: Кабильджанов А.С.

Корректор: Доспанова Д.У.