ВОПРОСЫ И ОТВЕТЫ К ЭКЗАМЕНУ ПО КУРСУ «РАСПРЕДЕЛЕННЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ»

Часть 1 (зима 2009-2010 г.) билеты №№1-2
Часть 2 (весна 2010 г.) билеты №№27-43 (17 билетов)

Дополнительный материал части 2:

1. Исторические аспекты развития коммуникаций. Эволюция телекоммуникационных систем от древнего мира до наших дней. Примеры наиболее значимых исторических коммуникационных систем. Развитие коммуникаций в XX веке.

системы коммуникаций: органы зрения, слуха и голосовой аппарат.
письменность.
символьный язык для описания не только объектов реального мира, но и абстрактных понятий.
Сигнальные костры (зона видимости, разжигались по очереди).
Почтовые голуби

в 19-ом веке стали появляться железные дороги, пароходы, электрический телеграф и телефон. Связь с применением азбуки Морзе в 1840-ых годах позволяла передать до 10 бит/сек на расстояние десятки и сотни километров. Азбука Морзе, пожалуй, была первым широко распространенным телекоммуникационным кодом

Телевидение. 1907 году Б. Г. Розингом было предложено использовать для приема изображения электронно-лучевую трубку (ЭЛТ), Устройство отображения на принимающей стороне также предполагало применение ЭЛТ. Электронное телевидение возникло в 30-х годах двадцатого века (усилиями В. К. Зворыкина и Ф. Франсуорта).

Состояние телекоммуникаций к концу 20-го века: (К 1950 годам: 1,2,3)

1. Телеграфная сеть, которая просуществовала до конца 20-го века.
2. Телефонная сеть (аналоговая), имеющая полосу 4 кГц и почти не менявшаяся по принципам работы с 1880 годов. Импульсная сигнальная система практически не изменялась с 1910 года.
3. Телексная сеть, которая применялась в основном для делового обмена.
4. Первые компьютеры 50-х годов - большие, громоздкие и дорогие - предназначались для очень небольшого числа избранных пользователей. Системы пакетной обработки, как правило, строились на базе мэйнфрейма - мощного и надежного компьютера универсального назначения.
5. в начале 60-х годов появились новые способы организации вычислительного процесса, которые позволили учесть интересы пользователей. Начали развиваться интерактивные многотерминальные системы разделения времени
6. В начале 70-х годов появились большие интегральные схемы. Их сравнительно невысокая стоимость и высокие функциональные возможности привели к созданию мини-компьютеров, которые стали реальными конкурентами мэйнфреймов.
   — Шло время, потребности пользователей, им уже хотелось получить возможность обмена данными с другими близко расположенными компьютерами.
   — Предприятия и организации стали соединять свои мини-компьютеры вместе и разрабатывать ПО, необходимое для их взаимодействия.
   В результате появились первые локальные вычислительные сети
7. В середине 80-х годов утвердились стандартные технологии объединения компьютеров в сеть - Ethernet, Arcnet, Token Ring. Мощным стимулом для их развития послужили персональные компьютеры.

Интернет является сетью виртуальных сетей. В 1991 году у нас (тогда еще в СССР) о нем знали неск. десятков человек

8. Сегодня ВС продолжают развиваться достаточно быстро. Разрыв между локальными и глобальными сетями сокращается из-за появления высокоскоростных территориальных каналов связи. В глобальных сетях появляются службы доступа к ресурсам, такие же удобные и прозрачные, как и службы локальных сетей. Подобные примеры в большом количестве демонстрирует самая популярная глобальная сеть - Internet.

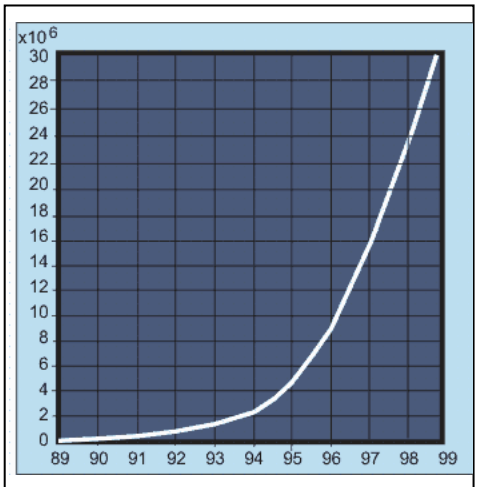


Рис. 1.1. Рост числа ЭВМ, подключенных к Интернет в период 1989-98 годы (по вертикальной оси отложено число ЭВМ в миллионах)

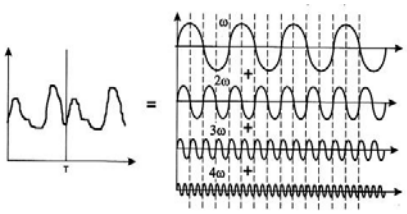
2. Основы теории передачи данных по линиям связи. Спектральная теория и ее применение к линиям связи. АЧХ.

Линия связи

проводные (воздушные);
кабельные (медные и волоконно-оптические);
радиоканалы наземной и спутниковой связи.

Спектральный анализ сигналов на линиях связи

1. Из теории гармонического анализа известно: любой периодический процесс можно представить в виде суммы синусоидальных колебаний различных частот и различных амплитуд



2. Для некоторых сигналов, (напр., для последовательности прямоугольных импульсов одинаковой длительности и амплитуды), спектр легко вычисляется на основании формул Фурье.

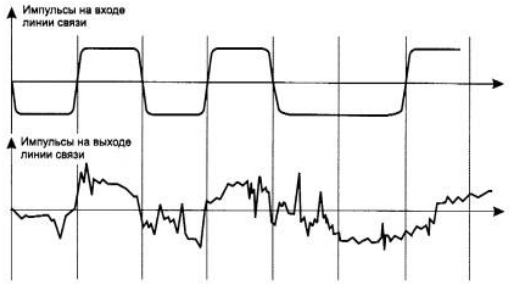
3. Представив значение напряжения или силы тока в виде однозначной периодической функции времени g(t) с периодом T, можно разложить её в **ряд Фурье.**.где $f = 1/T$— основная частота (гармоника), a_n и b_n — амплитуды синусов и косинусов *n-й* **гармоники**, а c — константа.

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \sin(2\pi nft) + \sum_{n=1}^{\infty} b_n \cos(2\pi nft);$$

4. Информационный сигнал, имеющий конечную длительность (все информационные сигналы имеют конечную длительность), может быть разложен в **ряд Фурье**, если представить, что весь сигнал бесконечно повторяется снова и снова (то есть интервал от T до *2T* полностью повторяет интервал от 0 до T, и т. д.).
Амплитуды a_n могут быть вычислены для любой заданной функции *g(t)*.

$$a_n = \frac{2}{T}\int_0^T g(t)\sin(2\pi nft)\,dt;\ b_n = \frac{2}{T}\int_0^T g(t)\cos(2\pi nft)\,dt;\ c = \frac{2}{T}\int_0^T g(t)\,dt.$$

Для сигналов произвольной формыспектр можно найти с помощью спектральных анализаторов, которые измеряют спектр реального сигнала и отображают амплитуды составляющих гармоник.

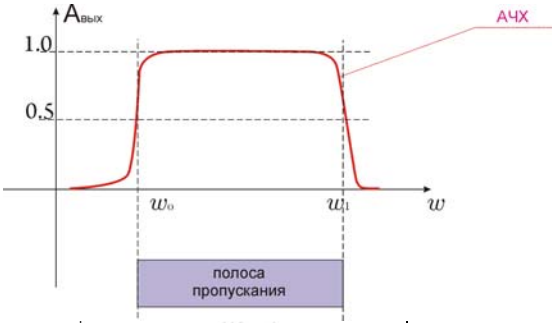


5. Ни один канал связи не может передавать сигналы без потери мощности. **Искажение** передающим каналом синусоиды какой-либо частоты приводит к искажению передаваемого сигнала любой формы (синусоиды различных частот искажаются неодинаково).

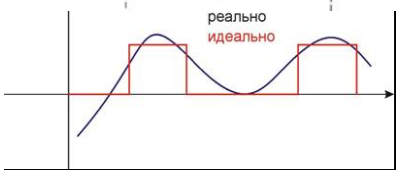
- Линия связи искажает сигналы из-за того, что ее физические параметры отличаются от идеальных.
- Кроме того, существуют и внешние помехи, которые создают различные электрические двигатели, электронные устройства, атмосферные явления и т. д.

Амплитудно-частотная характеристика (АЧХ) показывает, как затухает амплитуда синусоиды на выходе линии связи по сравнению с амплитудой на ее входе для всех возможных частот передаваемого сигнала. Вместо амплитуды в этой характеристике часто используют также такой параметр сигнала, как его мощность.

Все каналы связи уменьшают гармоники ряда Фурье в разной степени, искажая передаваемый сигнал. Как правило, амплитуды передаются без уменьшения в некотором частотном диапазоне, который наз. **полосой пропускания**. Обычно в полосу пропускания включают частоты, которые передаются с потерей мощности, не превышающей 50 %.

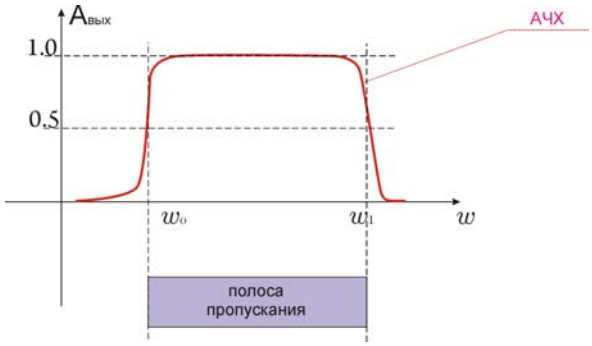


Знание АЧХ позволяет определить форму вых. сигнала практически для любого вх. сигнала. Для этого необходимо найти спектр вх. сигнала, преобразовать амплитуду составляющих его гармоник в соответствии с АЧХ, а затем найти форму вых. сигнала, сложив преобразованные гармоники



3. Характеристики линий связи. Полоса пропускания, затухание, мощность сигнала. Примеры линий связи. Помехоустойчивость, NEXT, BER.

Характеристики линий связи



амплитудно-частотная характеристика;
полоса пропускания;
затухание;
помехоустойчивость;
перекрестные наводки на ближнем конце линии;
пропускная способность;
достоверность передачи данных;
удельная стоимость.

Полоса пропускания *(bandwidth)* - это непрерывный диапазон частот, для которого отношение амплитуды выходного сигнала ко входному превышает некоторый заранее заданный предел, обычно 0,5. То есть полоса пропускания определяет диапазон частот синусоидального сигнала, при которых этот сигнал передается по линии связи без значительных искажений.

Затухание *(attenuation)* – относительное уменьшение амплитуды или мощности сигнала при передаче по линии сигнала определенной частоты. Т. образом, затухание представляет собой одну точку из АЧХ линии.

Затухание А обычно измеряется в децибелах (дБ, decibel - dB):

$$A = 10 \log_{10} P_{вых} / P_{вх},$$

где $P_{вых}$ ~ мощн. сигнала на выходе линии, $P_{вх}$ – мощн. сигнала на входе линии.

Так как мощность вых. сигнала кабеля без промежут. усилителей всегда меньше, чем мощность вх. сигнала, затухание кабеля всегда является отрицат. величиной.

Абсолютный **уровень мощности**, напр. ур. мощн. передатчика, также измеряется в дБ. При этом в кач. базового значения мощн. сигнала, отн. которого измеряется текущая мощность, принимается значение в 1 мВт.:

$$p = 10 \log_{10} P/1мВт \ [дБм],$$

где P - мощность сигнала в милливаттах, а дБм (dBm) - это единица измерения уровня мощности (децибел на 1 мВт).

Помехоустойчивость(ПУ) линии определяет ее способность уменьшать уровень помех, создаваемых во внешней среде, на внутренних проводниках. ПУ линии зависит от типа использ. физ. среды, а также от экранирующих и подавляющих помехи средств самой линии.

— Наименее помехоустойчивыми являются радиолинии,

— хорошей устойчивостью обладают кабельные линии и отличной - волоконно-оптические линии, малочувствительные ко внешнему электромагнитному излучению. Обычно для уменьшения помех, появляющихся из-за внешних электромагнитных полей, проводники экранируют и/или скручивают.

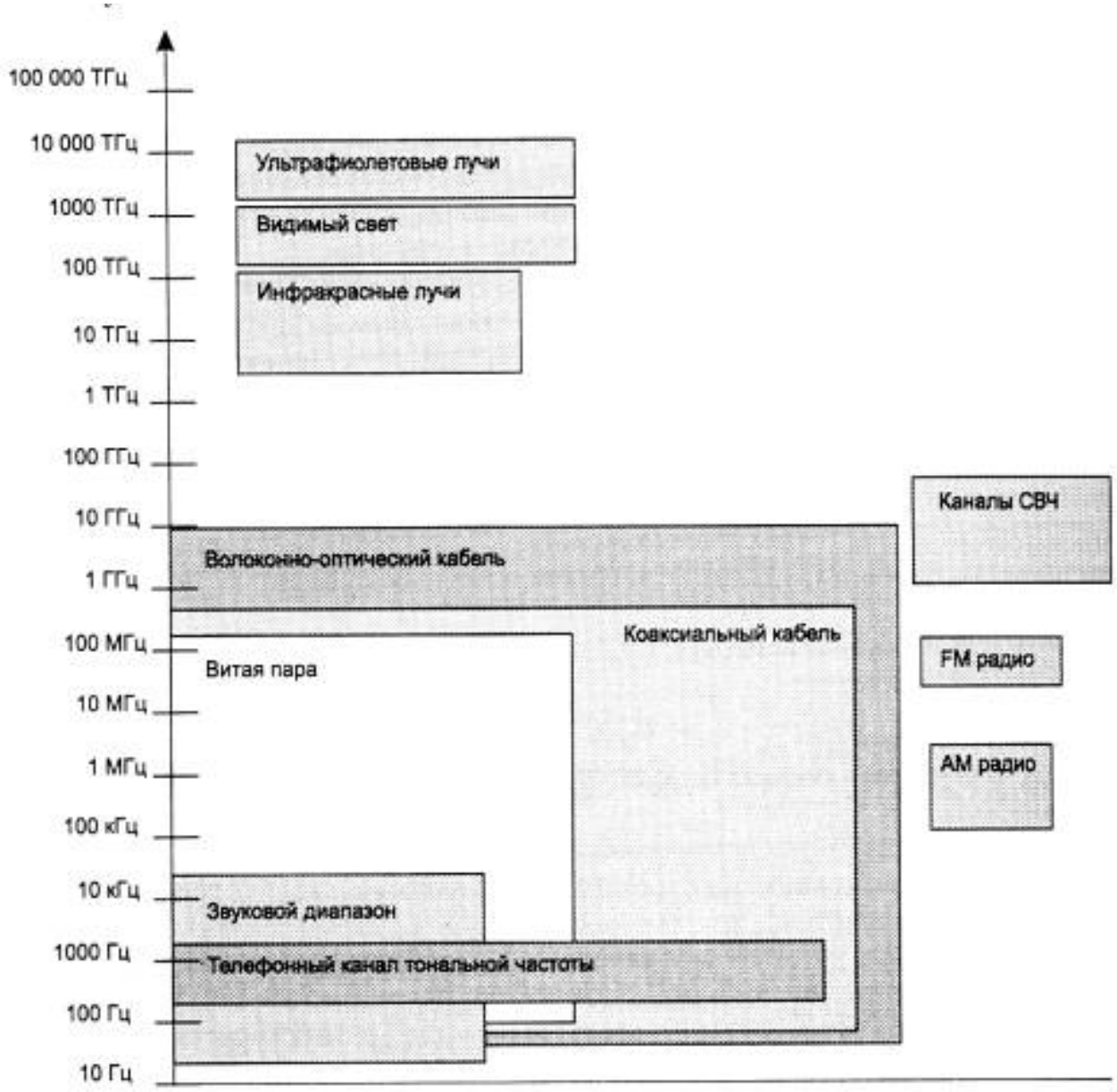
Перекрестные наводки на ближнем конце *(Near End Cross Talk - **NEXT**)* определяют ПУ кабеля к внутр. источникам помех, когда электромагнитное поле сигнала, передаваемого выходом передатчика по одной паре проводников, наводит на другую пару проводников сигнал помехи. Если ко второй паре будет подключен приемник, то он может принять наведенную внутреннюю помеху за полезный сигнал. Показатель NEXT, выраженный в децибелах, равен 10 $\log P_{вых}/P_{нав}$, где $P_{вых}$ - мощность выходного сигнала, $P_{нав}$ - мощность наведенного сигнала.

Чем меньше значение **NEXT**, тем лучше кабель. Так, для витой пары категории 5 показатель NEXT должен быть меньше -27 дБ на частоте 100 МГц.

Показатель NEXT обычно используется применительно к кабелю, состоящему из нескольких витых пар, так как в этом случае взаимные наводки одной пары на другую могут достигать значительных величин. Для одинарного коаксиального кабеля (то есть состоящего из одной экранированной жилы) этот показатель не имеет смысла, а для двойного коаксиального кабеля он также не применяется вследствие высокой степени защищенности каждой жилы. Оптические волокна также не создают сколь-нибудь заметных помех друг для друга.

Достоверность передачи данных характеризует вероятность искажения для каждого передаваемого бита данных. Иногда этот же показатель называют **интенсивностью битовых ошибок** *(Bit Error Rate, BER)*. Величина **BER** для каналов связи без дополнительных средств защиты от ошибок (например, самокорректирующихся кодов или протоколов с повторной передачей искаженных кадров) составляет, как правило, 10^{-4} - 10^{-6}, в оптоволоконных линиях связи - 10^{-9}. Значение достоверности передачи данных, например, в 10^{-4} говорит о том, что в среднем из 10000 бит искажается значение одного бита.

Искажения бит происходят как из-за наличия помех на линии, так и по причине искажений формы сигнала ограниченной полосой пропускания линии. Поэтому для повышения достоверности передаваемых данных нужно повышать степень помехозащищенности линии, снижать уровень перекрестных наводок в кабеле, а также использовать более широкополосные линии связи..



Пример ЛС:
полосы пропускания линий связи различных типов
(телефонный канал тональной частоты, витая пара, коаксиальный кабель, волоконно-оптический кабель),
а также наиболее часто используемые в технике связи частотные диапазоны
(звуковой диапазон, AM радио, FM –радио, каналы СВЧ, ИК-лучи, видимый свет УФ-лучи).

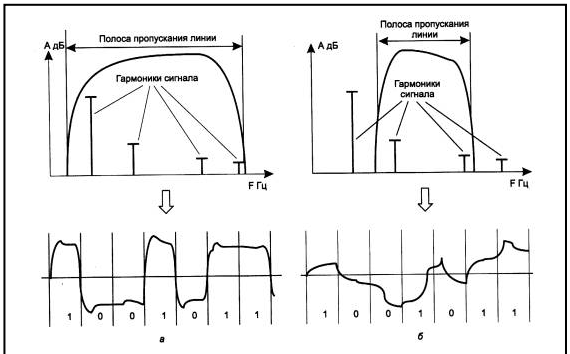
4. Линейное кодирование. Пропускная способность линий связяи. Связь меду полосой пропускания и пропускной способностью (теорема Шеннона, критерий Найквиста).

Выбор способа представления дискретной информации в виде сигналов, подаваемых на линию связи, называется **физическим** или **линейным кодированием**. От выбранного способа кодирования зависит спектр сигналов и, соответственно, пропускная способность линии. Таким образом, для одного способа кодирования линия может обладать одной пропускной способностью, а для другого - другой.

На пропускную способность линии оказывает влияние не только физическое, но и логическое кодирование. **Логическое кодирование** выполняется до физического кодирования и подразумевает замену бит исходной информации новой последовательностью бит, несущей ту же информацию, но обладающей, кроме этого, дополнительными свойствами, например возможностью для приемной стороны обнаруживать ошибки в принятых данных.

Пропускная способность *(throughput)* **линии** характеризует максимально возможную скорость передачи данных по линии связи. Пропускная способность измеряется в битах в секунду - бит/с, а также в производных единицах, таких как килобит в секунду (Кбит/с), мегабит в секунду (Мбит/с), гигабит в секунду (Гбит/с) и т. д. (то есть килобит - это 1000 бит, а мегабит - это 1 000 000 бит, а не 2^{10} =1024, а «мега» - 2^{20} = 1 048576)

Пропускная способность линии связи зависит не только от ее характеристик, таких как АЧХ, но и от спектра передаваемых сигналов..



Соответствие между полосой пропускания линии связи и спектром сигнала

Связь между проп. способностью линии и ее полосой пропускания

Чем выше частота несущего периодического сигнала, тем больше информации в единицу времени передается по линии и тем выше пропускная способность линии при фиксированном способе физического кодирования..

Связь между полосой пропускания линии и ее **максимально возможной пропускной способностью**, вне зависимости от принятого способа физического кодирования, установил **Клод Шеннон (теорема Шеннона):**

$C = F \log2 (1 + P_c/P_ш)$,

где C - максимальная пропускная способность линии в битах в секунду, F - ширина полосы пропускания линии в герцах, P_c - мощность сигнала, $P_ш$ - мощность шума.

Близким по сути к формуле Шеннона является следующее соотношение, полученное **Найквистом**, которое также определяет максимально возможную пропускную способность линии связи, но без учета шума на линии:

$C = 2F \log_2 M$,

где M - количество различимых состояний информационного параметра.

Теорема 1 (Шенона).

$$C_{[bod]} = F_{[Gc]} \cdot \log_2(1 + \frac{P_c}{P_u})$$

- C – *пропускная способность*
- P_c – *мощность сигнала*
- P_u – *мощность шума*

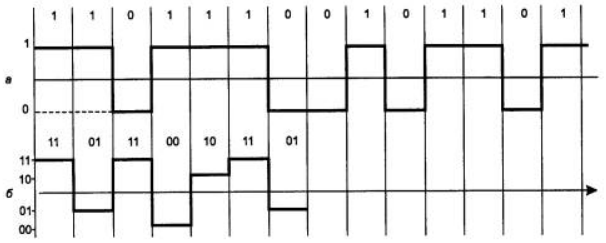
Теорема 2 (Найквист-Котельников).

$$C_{[bod]} = 2 \cdot F_{[Gc]} \cdot \log_2(M)$$

- C – *пропускная способность*
- M – *число состояний*

```
    1 -
   -- 11
   -- 01
   -- 10
   -- 00
  0 -
   -- ??
```

Если сигнал имеет 2 различимых состояния, то пропускная способность равна удвоенному значению ширины полосы пропускания линии связи (рис. 2.10, а). Если же передатчик использует более чем 2 устойчивых состояния сигнала для кодирования данных, то пропускная способность линии повышается, так как за один такт работы передатчик передает несколько бит исходных данных, например 2 бита при наличии четырех различимых состояний сигнала (рис. 2.10, б).



Повышение скорости передачи за счет дополнительных состояний сигнала

5. Методы передачи дискретных данных по линиям связи. Аналоговая модуляция, цифровое кодирование и их особенности.

При передаче дискретных данных применяются два осн. типа физического кодирования:
на основе синусоидального несущего сигнала (**аналоговой модуляцией**)
на основе последовательности прямоугольных импульсов (**цифр. кодированием**).

Первый – наз. также **модуляцией** или **аналоговой модуляцией**, т.к., кодирование осущ. за счет изменения параметров аналогового сигнала.

Второй – наз. цифровым кодированием.

Эти способы отличаются:
- шириной спектра
- сложностью аппаратуры.

При использ. прямоугольных имп-сов спектр результирующего сигнала получается весьма широким. Применение синусоиды приводит к спектру гораздо меньшей ширины при той же скорости передачи инф-ции. Однако для реализации синусоидальной модуляции требуется более сложная и дорогая аппаратура, чем для реализации прямоуг. имп-сов.

В наст. время все чаще данные, изначально имеющие аналоговую форму - речь, телевизионное изображение, - передаются по каналам связи в дискретном виде, то есть в виде послед-сти “1» и «0». Процесс представления аналоговой информации в дискретной форме наз. **дискретной модуляцией**. Термины «модуляция» и «кодирование» часто используют как синонимы.

Аналоговая модуляция (Факс –классический модем)

Аналоговая модуляция применяется для передачи дискретных данных по каналам с узкой полосой частот, (канал тональной частоты – телефонные сети). Этот канал передает частоты в диапазоне от 300 до 3400 Гц, таким образом, его полоса пропускания 3100 Гц

Методы аналоговой модуляции: (АМ, ЧМ, ФМ, и т.д.)

АМ (амплитудная модуляция) : для лог. единицы выбирается один уровень амплитуды синусоиды несущей частоты, а для логического нуля – другой. + простота, – помехи

ЧМ (частотная модуляция): значения 0 и 1 исходных данных передаются синусоидами с различной частотой - f0 и f1

ФМ (**фазовая модуляция):** значениям данных 0 и 1 соотв. сигналы одинаковой частоты, но с различной фазой, напр. 0 и 180° или 0,90,180 и 270 °.

В скоростных модемах часто используются **комбинированные методы модуляции**, как правило, амплитудная в сочетании с фазовой. Например **QAM**

QAM – квадратурная амплитудно-фазовая модуляция При квадратурной модуляции изменяется как фаза, так и амплитуда сигнала, что позволяет увеличить количество информации, передаваемой одним состоянием (отсчётом) сигнала.

Цифровое кодирование

Цифровой метод имеет целый ряд преимуществ перед аналоговым:

Высокую надежность. Если шум ниже входного порога, его влияние не ощущается, возможна повторная посылка кода.

Отсутствие зависимости от источника информации (звук, изображение или цифровые данные).

Возможность шифрования, что повышает безопасность передачи.

Независимость от времени. Можно передавать не тогда, когда информация возникла, а когда готов канал.

При цифровом кодировании дискретной информации применяют потенциальные и импульсные коды.

В потенциальных кодах для представления логических “1» и «0» используется только значение потенциала сигнала, а его перепады, формирующие законченные импульсы, во внимание не принимаются. Импульсные коды позволяют представить двоичные данные либо импульсами определенной полярности, либо частью импульса - перепадом потенциала определенного направления

Требования к методам цифрового кодирования

При использовании прямоугольных импульсов для передачи дискретной информации необходимо выбрать такой способ кодирования, который одновременно достигал бы нескольких целей:

- имел при одной и той же битовой скорости наименьшую ширину спектра результирующего сигнала;
- обеспечивал синхронизацию между передатчиком и приемником;
- обладал способностью распознавать ошибки;
- обладал низкой стоимостью реализации.

6. Аналоговая модуляция. Модемы. Способы модуляции и их спектральные характеристики..

Аналоговая модуляция (Факс –классический модем)

Анал. мод-ция применяется для передачи дискретных данных по каналам с узкой полосой частот, (канал тональной частоты – телефонные сети). Этот канал передает частоты в диапазоне от 300 до 3400 Гц, таким образом, его полоса пропускания 3100 Гц

Модемы. Устройство, которое выполняет функции модуляции несущей синусоиды на передающей стороне и демодуляции на приемной стороне, носит название **модем** (модулятор - демодулятор).

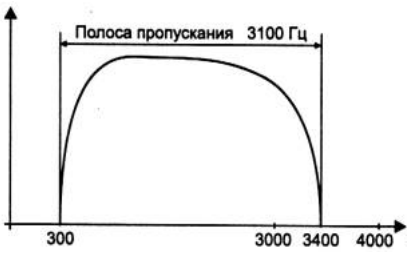


Рис. 2.12. АЧХ канала тональной частоты

Методы аналоговой модуляции: (АМ, ЧМ, ФМ, QAM и т.д.)

Информация кодируется изменением амплитуды, частоты или фазы синусоидального сигнала несущей частоты

При **амплитудной модуляции (АМ)** для логической единицы выбирается один уровень амплитуды синусоиды несущей частоты, а для логического нуля - другой

\+ простота

– помехи

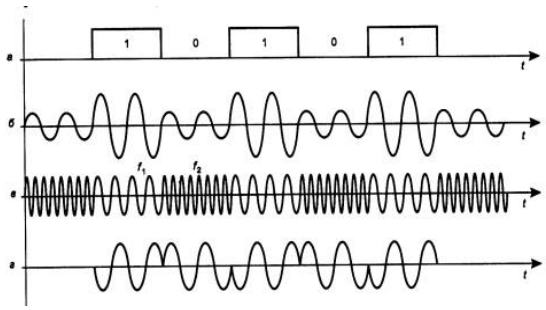


Рис. 2.13. Различные типы модуляции

При **частотной модуляции (ЧМ)** значения 0 и 1 исходных данных передаются синусоидами с различной частотой - f0 и f1

При **фазовой модуляции** (**ФМ**) значениям данных 0 и 1 соотв. сигналы одинаковой частоты, но с различной фазой, напр. 0 и 180° или 0,90,180 и 270 °.

Спектр модулированного сигнала

Спектр результирующего модулированного сигнала зависит от типа модуляции и скорости модуляции, то есть желаемой скорости передачи бит исходной информации.

Спектр ***потенциального кода*** требует для качественной передачи широкую полосу пропускания. Кроме того, реально спектр сигнала постоянно меняется в зависимости от того, какие данные передаются по линии связи. В результате потенциальные коды на каналах тональной частоты никогда не используются.

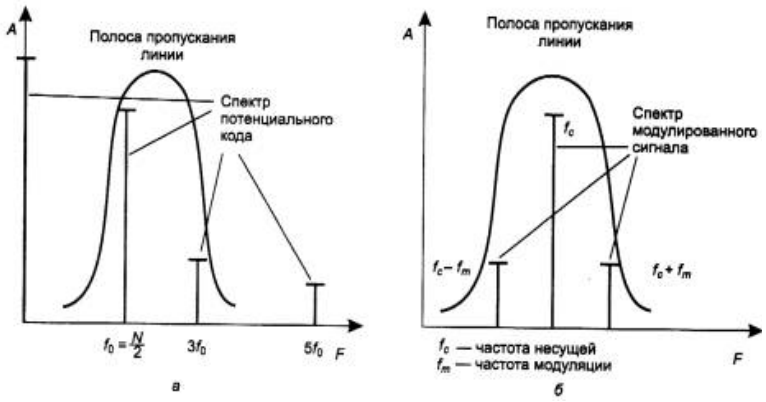


Рис. 2.14. Спектры сигналов при потенциальном кодировании (а) и амплитудной модуляции (б)

При **амплитудной модуляции** спектр состоит из синусоиды несущей частоты fc и двух боковых гармоник: (fc + fm) и (fc - fm), где fm - частота изменения информационного параметра синусоиды, которая совпадает со скоростью передачи данных при использовании двух уровней амплитуды (рис. 2.14, б). Частота fm определяет пропускную способность линии при данном способе кодирования. При небольшой частоте модуляции ширина спектра сигнала будет также небольшой (равной 2fm), поэтому сигналы не будут искажаться линией, если ее полоса пропускания будет больше или равна 2fm. Для канала тональной частоты такой способ модуляции приемлем при скорости передачи данных не больше 3100/2=1550 бит/с. Если же для представления данных используются 4 уровня амплитуды, то пропускная способность канала повышается до 3100 бит/с.

При **фазовой и частотной модуляции** спектр сигнала получается более сложным, чем при амплитудной модуляции, так как боковых гармоник здесь образуется более двух, но они также симметрично расположены относительно основной несущей частоты, а их амплитуды быстро убывают. Поэтому эти виды модуляции также хорошо подходят для передачи данных по каналу тональной частоты.

В скоростных модемах, для повыш. скор. передачи данных используют **комбинированные методы мод-ции**, как правило, амплитудная в сочетании с фазовой.. Наиболее распрост. Явл. *методы квадратурной амплитудной модуляции* (Quadrature Amplitude Modulation, **QAM**).

QAM – квадратурная амплитудно-фазовая модуляция При квадратурной модуляции изменяется как фаза, так и амплитуда сигнала, что позволяет увеличить количество информации, передаваемой одним состоянием (отсчётом) сигнала.

7. Цифровое кодирование. Особенности и проблемы цифрового кодирования, характеристики цифровых кодов. Основные типы кодирования и их спектральные характеристики.

Цифровое кодирование

При цифровом кодировании дискретной информации применяют потенциальные (используется только значение потенциала) и импульсные коды(либо импульсами определенной полярности, либо частью импульса - перепадом потенциала).

Требования к методам цифрового кодирования:

- имеет при одной и той же битовой скорости наименьшую ширину спектра результирующего сигнала;
- обеспечивает синхронизацию между передатчиком и приемником;
- обладает способностью распознавать ошибки;
- обладает низкой стоимостью реализации.

Более узкий спектр сигналов позволяет на одной и той же линии (с одной и той же полосой пропускания) добиваться более высокой скорости передачи данных.

Синхронизация передатчика и приемника нужна для того, чтобы приемник точно знал, в какой момент времени необходимо считывать новую информацию с линии связи.

В сетях применяются так называемые **самосинхронизирующиеся коды**, сигналы которых несут для передатчика указания о том, в какой момент времени нужно осуществлять распознавание очередного бита (фронт имп. - может служить синхр., синусоид в качестве несущего).

Распознавание и коррекцию искаженных данных сложно осуществить средствами физического уровня, поэтому чаще всего эту работу берут на себя протоколы, лежащие выше: канальный, сетевой, транспортный или прикладной.

Схемы кодирования:

(Информация) → <Логическое кодирование> → <Физическое кодирование> → [Передатчик]

Потенциальный код без возвращения к нулю (Non Return to Zero, **NRZ**). При передаче последовательности единиц сигнал не возвращается к нулю в течение такта. Метод NRZ:
+ прост в реализации,
+ хорошая распознаваемость ошибок (из-за двух резко отличающихся потенциалов),
– не обладает свойством самосинхронизации.
– наличие низкочастотной составляющей, которая приближается к нулю при передаче длинных последовательностей единиц или нулей. В результате в чистом виде код NRZ в сетях не используется. (используются его модификации, в которых устраняют эти недостатки).

Привлекательность кода NRZ, , состоит в достаточно низкой частоте основной гармоники f_0, которая равна N/2 Гц

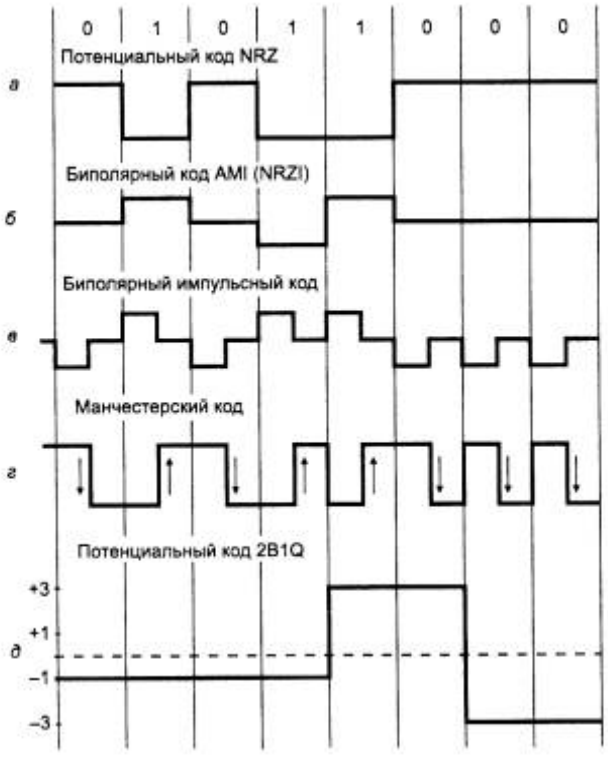


Рис. 2.16. Способы дискретного кодирования данных

Метод биполярного кодирования с альтернативной инверсией (Bipolar Alternate Mark Inversion, **AMI**, модификация NRZ) Используются три уровня потенциала – отрицат., нулевой и положит. Для кодирования логического нуля используется нулевой потенциал, а логическая единица кодируется либо положительным потенциалом, либо отрицательным, при этом потенциал каждой новой единицы противоположен потенциалу предыдущей.

Код AMI частично ликвидирует проблемы постоянной составляющей и отсутствия самосинхронизации,

Потенциальный код с инверсией при единице (Non Return to Zero with ones Inverted, **NRZI**), похожий на AMI, но только с двумя уровнями сигнала. При передаче нуля он передает потенциал, который был установлен в предыдущем такте (то есть не меняет его), а при передаче единицы потенциал инвертируется на противоположный. Он удобен в тех случаях, когда использование третьего уровня сигнала весьма нежелательно, например в оптических кабелях, где устойчиво распознаются два состояния сигнала - свет и темнота.

В **импульсных. кодах** данные представлены полным импульсом или же его частью – фронтом:

Биполярный импульсный код: единица представлена импульсом одной полярности, а ноль – другой. Каждый импульс длится половину такта.

+ отличные самосинхронизирующие свойства,

– постоянная составляющая, может присутствовать, (напр., при передаче длинной последовательности 1 или 0).

– спектр у него шире, чем у потенциальных кодов.

Из-за слишком широкого спектра биполярный импульсный код используется редко.

Манчестерский код в локальных сетях до недавнего времени самым распространенным методом кодирования (применяется в технологиях Ethernet и Token Ring).

В манчестерском коде для кодирования “1» и «0» используется перепад потенциала, то есть фронт импульса. При манчестерском кодировании каждый такт делится на две части. Информация кодируется перепадами потенциала, происходящими в середине каждого такта. Единица кодируется перепадом от низкого уровня сигнала к высокому, а ноль - обратным перепадом. В начале каждого такта может происходить служебный перепад сигнала, если нужно представить несколько единиц или нулей подряд.

+ Так как сигнал изменяется по крайней мере один раз за такт передачи одного бита данных, то манчестерский код обладает хорошими самосинхронизирующими свойствами.

+ Полоса пропускания манчестерского кода уже, чем у биполярного импульсного.

+ Нет постоянной составляющей, а основная гармоника в худшем случае (при передаче последовательности единиц или нулей) имеет частоту N Гц, а в лучшем (при передаче чередующихся “1» и «0») она равна N/2 Гц, как и у кодов AMI или NRZ.

В среднем ширина полосы манчестерского кода в полтора раза уже, чем у биполярного импульсного кода, а основная гармоника колеблется вблизи значения 3N/4.

+ используются два уровня сигнала. (у биполярного — три уровня сигнала).

Потенциальный код 2B1Q (с четырьмя уровнями сигнала для кодирования данных) — каждые два бита (2B) передаются за один такт сигналом, имеющим четыре состояния (1Q), Паре бит 00 соответствует потенциал -2,5 В, паре бит 01 соответствует потенциал -0,833 В, паре 11 - потенциал +0,833 В, а паре 10 - потенциал +2,5 В.

– требуются дополнительные меры по борьбе с длинными последовательностями одинаковых пар бит, так как при этом сигнал превращается в постоянную составляющую.

+ При случайном чередовании бит спектр сигнала в два раза уже, чем у кода NRZ, так как при той же битовой скорости длительность такта увеличивается в два раза.

Таким образом, с помощью кода 2B1Q можно по одной и той же линии передавать данные в два раза быстрее, чем с помощью кода AMI или NRZI.

– Однако мощность передатчика должна быть выше, чтобы четыре уровня четко различались приемником на фоне помех.

Спектральные характеристики типов кодирования

Улучшенные потенциальные коды обладают достаточно узкой полосой пропускания для любых последовательностей “1» и «0», которые встречаются в передаваемых данных. На рис. 2.18 приведены спектры сигналов разных кодов, полученные при передаче произвольных данных, в которых различные сочетания нулей и единиц в исходном коде равновероятны. При построении графиков спектр усреднялся по всем возможным наборам исходных последовательностей. Естественно, что результирующие коды могут иметь и другое распределение нулей и единиц. Из рис. видно, что потенциальный код NRZ обладает хорошим спектром с одним недостатком - у него имеется постоянная составляющая. Коды, полученные из потенциального путем логического кодирования, обладают более узким спектром, чем манчестерский, даже при повышенной тактовой частоте (на рисунке спектр кода 4B/5B должен был бы примерно совпадать с кодом B8ZS, но он сдвинут в область более высоких частот, так как его тактовая частота повышена на 1/4 по сравнению с другими кодами). Этим объясняется применение потенциальных избыточных и скрэмблированных кодов в современных технологиях, подобных FDDI, Fast Ethernet, Gigabit Ethernet, ISDN и т. п. вместо манчестерского и биполярного импульсного кодирования.

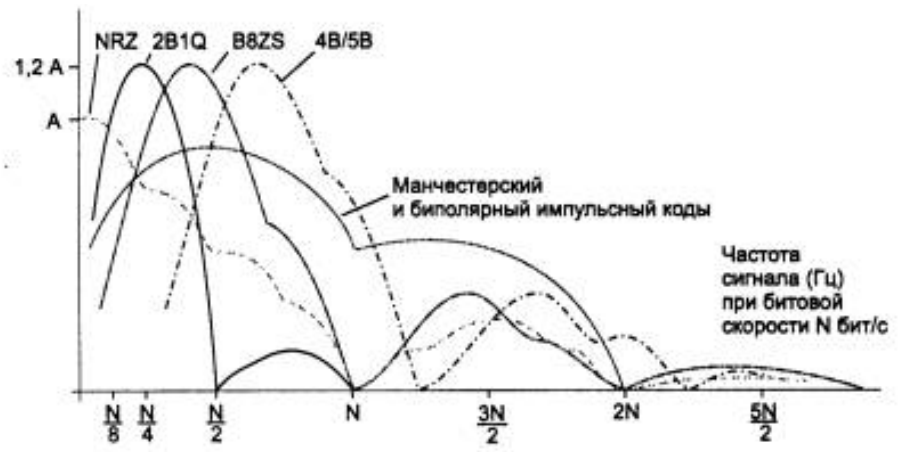


Рис. 2.18. Спектры потенциальных и импульсных кодов

8. Логическое кодирование. Необходимость и особенности логического кодирования. Наиболее популярные методы логического кодирования.

Логическое кодирование выполняется до физического кодирования и подразумевает замену бит исходной информации новой последовательностью бит, несущей ту же информацию, но обладающей, кроме этого, дополнительными свойствами, например возможностью для приемной стороны обнаруживать ошибки в принятых данных. Сопровождение каждого байта исходной информации одним битом четности - это пример очень часто применяемого способа логического кодирования при передаче данных с помощью модемов. Другим примером логического кодирования может служить шифрация данных, обеспечивающая их конфиденциальность при передаче через общественные каналы связи. При логическом кодировании чаще всего исходная последовательность бит заменяется более длинной последовательностью, поэтому пропускная способность канала по отношению к полезной информации при этом уменьшается.

Схемы кодирования:

(Информация) → <Логическое кодирование> → <Физическое кодирование> → [Передатчик]

Логическое кодирование используется для улучшения потенциальных кодов типа AMI, NRZI или 2Q1B. Логическое кодирование должно заменять длинные последовательности бит, приводящие к постоянному потенциалу, вкраплениями единиц. Как уже отмечалось выше, для логического кодирования характерны два метода:

избыточные коды (4B/5B, 8B/6T)

скрэмблирование.

Избыточные коды основаны на разбиении исходной последовательности бит на порции, которые часто наз. символами. Затем каждый исходный символ заменяется на новый, который имеет большее количество бит, чем исходный. Например, логический код 4B/5B, используемый в технологиях FDDI и Fast Ethernet, заменяет исходные символы длиной в 4 бита на символы длиной в 5 бит. Так как результирующие символы содержат избыточные биты, то общее количество битовых комбинаций в них больше, чем в исходных. Так, в **коде 4B/5B** результирующие символы могут содержать 32 битовых комбинации, в то время как исходные символы - только 16. Поэтому в результирующем коде можно отобрать 16 таких комбинаций, которые не содержат большого количества нулей, а остальные считать запрещенными кодами (code violation). Кроме устранения постоянной составляющей и придания коду свойства самосинхронизации, избыточные коды позволяют приемнику распознавать искаженные биты. Если приемник принимает запрещенный код, значит, на линии произошло искажение сигнала.

Соответствие исходных и результирующих кодов 4B/5B представлено ниже.

Исходный код	Результирующий код	Исходный код	Результирующий код
0000	11110	1000	10010
0001	01001	1001	10011
0010	10100	1010	10110
0011	10101	1011	10111
0100	01010	1100	11010
0101	01011	1101	11011
0110	01110	1110	11100
0111	01111	1111	11101

Код 4B/5B затем передается по линии с помощью физ. кодирования по одному из методов потенциального кодирования, чувствительному только к длинным послед-стям нулей. Символы кода 4B/5B длиной 5 бит гарантируют, что при любом их сочетании на линии не могут встретиться более трех нулей подряд.

Буква B в названии кода означает, что элементарный сигнал имеет 2 состояния - от английского binary - двоичный. Имеются также коды и с тремя состояниями сигнала, например, в коде 8B/6T для кодирования 8 бит исходной информации используется код из 6 сигналов, каждый из которых имеет три состояния. Избыточность кода 8B/6T выше, чем кода 4B/5B, так как на 256 исходных кодов приходится 36=729 результирующих символов.

\+ Перекодировка (таблицы) является очень простой операцией,→ этот подход не усложняет сетевые адаптеры и интерфейсные блоки коммутаторов и маршрутизаторов.

– Для обеспечения зад. проп. способности линии передатчик, использующий избыточный код, должен работать с повыш. тактовой частотой. Так, для передачи кодов 4B/5B со скоростью 100 Мб/с передатчик должен работать с тактовой частотой 125 МГц. При этом спектр сигнала на линии расширяется по сравнению со случаем, когда по линии передается чистый, не избыточный код.

\+ Тем не менее спектр избыточного потенциального кода оказывается уже спектра манчестерского кода, что оправдывает дополнительный этап логического кодирования, а также работу приемника и передатчика на повышенной тактовой частоте.

Скрэмблирование

Перемешивание данных **скрэмблером** перед передачей их в линию с помощью потенциального кода является другим способом логического кодирования.

Методы скрэмблирования заключаются в побитном вычислении результирующего кода на основании бит исходного кода и полученных в предыдущих тактах бит результирующего кода. Например, скрэмблер может реализовывать следующее соотношение:

$$B_i = A_i \oplus B_{i-3} \oplus B_{i-5},$$

где Bi - двоичная цифра результирующего кода, полученная на i-м такте работы скрэмблера, Ai - двоичная цифра исходного кода, поступающая на i-м такте на вход скрэмблера, Bi-3 и Bi-5 - двоичные цифры результирующего кода, полученные на предыдущих тактах работы скрэмблера, соответственно на 3 и на 5 тактов ранее текущего такта, - операция исключающего ИЛИ (сложение по модулю 2). Например, для исходной последовательности 110110000001 скрэмблер даст следующий результирующий код: B1 = A1 = 1 (первые три цифры результирующего кода будут совпадать с исходным, так как еще нет нужных предыдущих цифр)

Таким образом, на выходе скрэмблера появится последовательность 110001101111, в которой нет последовательности из шести нулей, присутствовавшей в исходном коде.

$$B_2 = A_2 = 1$$
$$B_3 = A_3 = 0$$
$$B_4 = A_4 \oplus B_1 = 1 \oplus 1 = 0$$
$$B_5 = A_5 \oplus B_2 = 1 \oplus 1 = 0$$
$$B_6 = A_6 \oplus B_3 \oplus B_1 = 0 \oplus 0 \oplus 1 = 1$$
$$B_7 = A_7 \oplus B_4 \oplus B_2 = 0 \oplus 0 \oplus 1 = 1$$
$$B_8 = A_8 \oplus B_5 \oplus B_3 = 0 \oplus 0 \oplus 0 = 0$$
$$B_9 = A_9 \oplus B_6 \oplus B_4 = 0 \oplus 1 \oplus 0 = 1$$
$$B_{10} = A_{10} \oplus B_7 \oplus B_5 = 0 \oplus 1 \oplus 0 = 1$$
$$B_{11} = A_{11} \oplus B_8 \oplus B_6 = 0 \oplus 0 \oplus 1 = 1$$
$$B_{12} = A_{12} \oplus B_9 \oplus B_7 = 1 \oplus 1 \oplus 1 = 1$$

После получения результирующей последовательности приемник передает ее дескрэмблеру, который восстанавливает исходную последовательность на основании обратного соотношения:

$$C_i = B_i \oplus B_{i-3} \oplus B_{i-5} = (A_i \oplus B_{i-3} \oplus B_{i-5}) \oplus B_{i-3} \oplus B_{i-5} = A_i.$$

Различные алгоритмы скрэмблирования отличаются количеством слагаемых, дающих цифру результирующего кода, и сдвигом между слагаемыми. Так, в сетях ISDN при передаче данных от сети к абоненту используется преобразование со сдвигами в 5 и 23 позиции, а при передаче данных от абонента в сеть - со сдвигами 18 и 23 позиции.

Существуют и более простые методы борьбы с последовательностями единиц, также относимые к классу скрэмблирования.

Для улучшения кода Bipolar AMI используются два метода, основанные на искусственном искажении последовательности нулей запрещенными символами.

На рис. 2.17 показано использование метода B8ZS (Bipolar with 8-Zeros Substitution) и метода HDB3 (High-Density Bipolar 3-Zeros) для корректировки кода AMI. Исходный код состоит из двух длинных последовательностей нулей: в первом случае - из 8, а во втором - из 5.

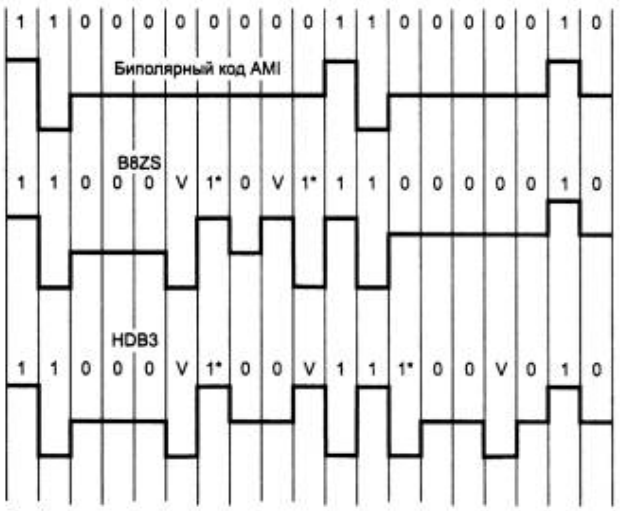


Рис. 2.17. Коды B8ZS и HDB3. V - сигнал единицы запрещенной полярности; 1*-сигнал единицы корректной полярности, но заменившей 0 в исходном коде

Код B8ZS исправляет только последовательности, состоящие из 8 нулей. Для этого он после первых трех нулей вместо оставшихся пяти нулей вставляет пять цифр: V-1*-0-V-1*. V здесь обозначает сигнал единицы, запрещенной для данного такта полярности, то есть сигнал, не изменяющий полярность предыдущей единицы, 1* - сигнал единицы корректной полярности, а знак звездочки отмечает тот факт, что в исходном коде в этом такте была не единица, а ноль. В результате на 8 тактах приемник наблюдает 2 искажения - очень маловероятно, что это случилось из-за шума на линии или других сбоев передачи. Поэтому приемник считает такие нарушения кодировкой 8 последовательных нулей и после приема заменяет их на исходные 8 нулей. Код B8ZS построен так, что его постоянная составляющая равна нулю при любых последовательностях двоичных цифр.

Код HDB3 исправляет любые четыре подряд идущих нуля в исходной последовательности. Правила формирования кода HDB3 более сложные, чем кода B8ZS. Каждые четыре нуля заменяются четырьмя сигналами, в которых имеется один сигнал V. Для подавления постоянной составляющей полярность сигнала V чередуется при последовательных заменах. Кроме того, для замены используются два образца четырехтактовых кодов. Если перед заменой исходный код содержал нечетное число единиц, то используется последовательность 000V, а если число единиц было четным - последовательность 1*00V.

9. Передача аналоговых сигналов по цифровым линиям связи. Дискретная модуляция. Теорема Найквиста-Котельникова и ее применение к кодированию человеческой речи. Способы улучшения дискретной модуляции для разных типов сигналов.

Передача в одной сети как дискретных, так и аналоговых данных (телефоны, видеокамеры, звуко- и видеовоспроизводящая аппаратура) основана на дискретизации непрерывных процессов как по амплитуде, так и по времени с пом. **импульсно-кодовой модуляции, ИКМ** (*Pulse Amplitude Modulation, PAM*),

Амплитуда исходной непрерывной функции измеряется с заданным периодом - за счет этого происходит дискретизация по времени. Затем каждый замер представляется в виде двоичного числа определенной разрядности, что означает дискретизацию по значениям функции - непрерывное множество возможных значений амплитуды заменяется дискретным множеством ее значений. Устройство, которое это выполняет, называется **аналого-цифровым преобразователем (АЦП)**. После этого замеры передаются по каналам связи в виде послед-сти «1» и «0».

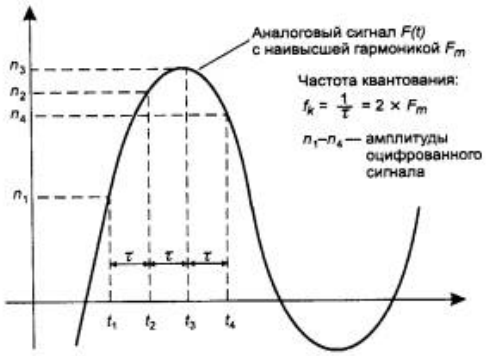


Рис. 2.19. Дискретная модуляция непрерывного процесса

На приемной стороне коды преобразуются в исходную последовательность бит, а спец. аппаратура, наз. **цифро-аналоговым преобразователем (ЦАП)**, производит демодуляцию оцифрованных амплитуд непрерывного сигнала, восстанавливая исходную непрерывную функцию времени.

Дискретная модуляции основана на **теории отображения Найквиста - Котельникова**. В соответствии с этой теорией, **аналоговая непрерывная функция, переданная в виде последовательности ее дискретных по времени значений, может быть точно восстановлена, если частота дискретизации была в два или более раз выше, чем частота самой высокой гармоники спектра исходной функции**.

+ Преимуществом цифровых методов записи, воспроизведения и передачи аналоговой информации является возможность контроля достоверности считанных с носителя или полученных по линии связи данных. Для этого применяются те же методы, которые применяются для компьютерных данных.

Для качественной передачи голоса в методе ИКМ используется частота квантования амплитуды звуковых колебаний в 8000 Гц. Это связано с тем, что в аналоговой телефонии для передачи голоса был выбран диапазон от 300 до 3400 Гц, который достаточно качественно передает все основные гармоники собеседников. В соответствии с теоремой Найквиста - Котельникова для качественной передачи голоса достаточно выбрать частоту дискретизации, в два раза превышающую самую высокую гармонику непрерывного сигнала, то есть 2 * 3400 = 6800 Гц. Выбранная в действительности частота дискретизации 8000 Гц обеспечивает некоторый запас качества. В методе ИКМ обычно используется 7 или 8 бит кода для представления амплитуды одного замера. Соответственно это дает 127 или 256 градаций звукового сигнала, что оказывается вполне достаточным для качественной передачи голоса.

При использовании метода ИКМ для передачи одного голосового канала необходима пропускная способность 56 или 64 Кбит/с в зависимости от того, каким количеством бит представляется каждый замер. Если для этих целей используется 7 бит, то при частоте передачи замеров в 8000 Гц получаем:

8000 * 7 = 56000 бит/с или 56 Кбит/с;

а для случая 8-ми бит:

8000 * 8 = 64000 бит/с или 64 Кбит/с.

Стандартным является цифровой канал 64 Кбит/с, который также называется элементарным каналом цифровых телефонных сетей.

Передача непрер. сигнала в дискретном виде требует от сетей жесткого соблюдения временного интервала в 125 мкс (соответствующего частоте дискретизации 8000 Гц) между соседними замерами, то есть требует **синхронной** передачи данных между узлами сети.

На качество сигнала после ЦАП влияет не только синхронность поступления на его вход замеров, но и погрешность дискретизации амплитуд этих замеров. **В теореме Найквиста - Котельникова** предполагается, что амплитуды функции измеряются точно, в то же время использование для их хранения двоичных чисел с ограниченной разрядностью несколько искажает эти амплитуды. Соответственно искажается восстановленный непрерывный сигнал, что называется шумом дискретизации (по амплитуде).

Существуют и другие методы дискретной модуляции, позволяющие представить замеры голоса в более компактной форме, напр. в виде послед-сти 4-битных или 2-битных чисел. При этом один голосовой канал требует меньшей пропускной способности, напр. 32 Кбит/с, 16 Кбит/с или еще меньше. С 1985 года применяется **стандарт CCITT кодирования голоса, называемый Adaptive Differential Pulse Code Modulation (ADPCM)**. Коды ADPCM основаны на нахождении разностей между последовательными замерами голоса, которые затем и передаются по сети. В коде ADPCM для хранения одной разности используются 4 бит и голос передается со скоростью 32 Кбит/с. Более современный метод, **Linear Predictive Coding (LPC)**, делает замеры исходной функции более редко, но использует методы прогнозирования направления изменения амплитуды сигнала. При помощи этого метода можно понизить скорость передачи голоса до 9600 бит/с.

Представленные в цифровой форме непрерывные данные легко можно передать через компьютерную сеть. Для этого достаточно поместить несколько замеров в кадр какой-нибудь стандартной сетевой технологии, снабдить кадр правильным адресом назначения и отправить адресату. Адресат должен извлечь из кадра замеры и подать их с частотой квантования (для голоса - с частотой 8000 Гц) на цифро-аналоговый преобразователь. По мере поступления следующих кадров с замерами голоса операция должна повториться. Если кадры будут прибывать достаточно синхронно, то качество голоса может быть достаточно высоким. Однако, кадры в компьютерных сетях могут задерживаться как в конечных узлах (при ожидании доступа к разделяемой среде), так и в промежуточных коммуникационных устройствах - мостах, коммутаторах и маршрутизаторах. Поэтому качество голоса при передаче в цифровой форме через компьютерные сети обычно бывает невысоким. **Для качественной передачи оцифрованных непрерывных сигналов - голоса, изображения - сегодня используют специальные цифровые сети, такие как ISDN, ATM, и сети цифрового телевидения.** Тем не менее для передачи внутрикорпоративных телефонных разговоров сегодня характерны сети frame relay, задержки передачи кадров которых укладываются в допустимые пределы.

Асинхронная и синхронная передачи

При обмене данными достаточно обеспечить синхронизацию на битовом и кадровом уровне, - чтобы передатчик и приемник смогли обеспечить устойчивый обмен инф-цией. Однако при плохом качестве линии связи вводят дополнительные средства синхронизации на уровне байт.

Такой режим работы называется **асинхронным или старт-стопным**. Другой причиной использ-я этого режима является наличие устройств, которые генерируют байты данных в случайные моменты времени (клавиатура дисплея или другого терминального устр-ва, с к-рого человек вводит данные).

В асинхронном режиме каждый байт данных сопровождается специальными сигналами «старт» и «стоп» (рис. 2.20, а). Назначение этих сигналов: 1) известить приемник о приходе данных, 2) дать приемнику достаточно врем. для выполнения нек-рых функций, связанных с синхронизацией, до поступления след. байта. Сигнал «старт» имеет продолжительность в один тактовый интервал, а сигнал «стоп» может длиться один, полтора или два такта, поэтому говорят, что используется один, полтора или два бита в качестве стопового сигнала, хотя пользовательские биты эти сигналы не представляют.

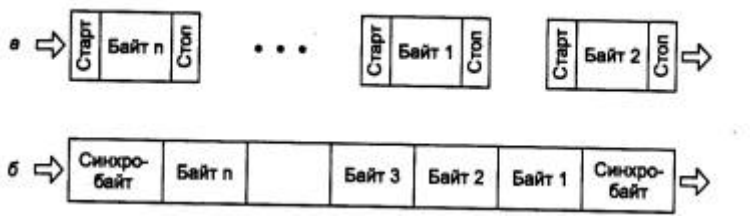


Рис. 2.20. Асинхронная (а) и синхронная (б) передачи на уровне байт

Асинхронным описанный режим называется потому, что каждый байт может быть несколько смещен во времени относительно побитовых тактов предыдущего байта. Такая асинхронность передачи байт не влияет на корректность принимаемых данных, так как в начале каждого байта происходит дополнительная синхронизация приемника с источником за счет битов «старт». Более «свободные» временные допуски определяют низкую стоимость оборудования асинхронной системы.

При **синхронном режиме передачи** старт-стопные биты между каждой парой байт отсутствуют. Пользовательские данные собираются в кадр, который предваряется байтами синхронизации (рис. 2.20, б). **Байт синхронизации** - это байт, содержащий заранее известный код, напр. 0111110, который оповещает приемник о приходе кадра данных. При его получении приемник должен войти в байтовый синхронизм с передатчиком, то есть правильно понимать начало очередного байта кадра. Иногда применяется несколько синхробайт для обеспечения более надежной синхронизации приемника и передатчика. Так как при передаче длинного кадра у приемника могут появиться проблемы с синхронизацией бит, то в этом случае используются самосинхронизирующиеся коды.

Выводы к главе 2.2. (вопросы 5 - 9)

- При передаче дискретных данных по узкополосному каналу тональной частоты, используемому в телефонии, наиболее подходящими оказываются способы аналоговой модуляции, при которых несущая синусоида модулируется исходной последовательностью двоичных цифр. Эта операция осуществляется специальными устройствами - модемами.
- Для низкоскоростной передачи данных применяется изменение частоты несущей синусоиды. Более высокоскоростные модемы работают на комбинированных способах квадратурной амплитудной модуляции (QAM), для которой характерны 4 уровня амплитуды несущей синусоиды и 8 уровней фазы. Не все из возможных 32 сочетаний метода QAM используются для передачи данных, запрещенные сочетания позволяют распознавать искаженные данные на физическом уровне.
- На широкополосных каналах связи применяются потенциальные и импульсные методы кодирования, в которых данные представлены различными уровнями постоянного потенциала сигнала либо полярностями импульса или его фронта.
- При использовании потенциальных кодов особое значение приобретает задача синхронизации приемника с передатчиком, так как при передаче длинных последовательностей нулей или единиц сигнал на входе приемника не изменяется и приемнику сложно определить момент съема очередного бита данных.
- Наиболее простым потенциальным кодом является код без возвращения к нулю (NRZ), однако он не является самосинхронизирующимся и создает постоянную составляющую.
- Наиболее популярным импульсным кодом является манчестерский код, в котором информацию несет направление перепада сигнала в середине каждого такта. Манчестерский код применяется в технологиях Ethernet и Token Ring.
- Для улучшения свойств потенциального кода NRZ используются методы логического кодирования, исключающие длинные последовательности нулей. Эти методы основаны:
    - на введении избыточных бит в исходные данные (коды типа 4B/5B);
    - скрэмблировании исходных данных (коды типа 2B 1Q).
- Улучшенные потенциальные коды обладают более узким спектром, чем импульсные, поэтому они находят применение в высокоскоростных технологиях, таких как FDDI, Fast Ethernet, Gigabit Ethernet.

10. Кабели связи. Характеристики кабелей связи, стандарты кабельной продукции.

Кабель - это изделие, состоящее из проводников, слоев экрана и изоляции. В некоторых случаях в состав кабеля входят разъемы. Кроме этого, для перекоммутации кабелей и оборудования используются различные электромеханические устройства (кроссовые секции, кроссовые коробки или шкафы).

Характеристики кабелей связи (электромагнитные характеристики)**.**

- Затухание (Attenuation) измер. в дБ/м для определенной частоты или диапазона частот.
- Перекрестные наводки на ближнем конце (Near End Cross Talk, NEXT). Измеряются в дБ для определенной частоты сигнала.
- Импеданс (волновое сопротивление) - это полное (активное и реактивное) сопротивление в электрической цепи. Импеданс измеряется в Омах и является относительно постоянной величиной для кабельных систем (например, для коаксиальных кабелей, используемых в стандартах Ethernet, импеданс кабеля должен составлять 50 Ом). Для неэкранированной витой пары наиболее часто используемые значения импеданса - 100 и 120 Ом. В области высоких частот (100-200 МГц) импеданс зависит от частоты.
- Активное сопротивление - это сопротивление постоянному току в электрической цепи. В отличие от импеданса активное сопротивление не зависит от частоты и возрастает с увеличением длины кабеля.
- Емкость - это свойство металлических проводников накапливать энергию. Два электрических проводника в кабеле, разделенные диэлектриком, представляют собой конденсатор, способный накапливать заряд. Емкость является нежелательной величиной, поэтому следует стремиться к тому, чтобы она была как можно меньше (иногда применяют термин «паразитная емкость»). Высокое значение емкости в кабеле приводит к искажению сигнала и ограничивает полосу пропускания линии.
- Уровень внешнего электромагнитного излучения или электрический шум (ЭШ), мВ. ЭШ - это нежелательное переменное напряжение в проводнике. ЭШ бывает двух типов: фоновый и импульсный. ЭШ можно также разделить на низко-, средне- и высокочастотный. Источниками фонового ЭШ в диапазоне до 150 кГц являются линии электропередачи, телефоны и лампы дневного света; в диапазоне от 150 кГц до 20 МГц - компьютеры, принтеры, ксероксы; в диапазоне от 20 МГц до 1 ГГц - телевизионные и радиопередатчики, микроволновые печи. Основными источниками импульсного ЭШ являются моторы, переключатели и сварочные агрегаты. ЭШ измеряется в милливольтах.
- Диаметр или площадь сечения проводника. Для медных проводников достаточно употребительной является американская система AWG (American Wire Gauge), которая вводит некоторые условные типы проводников, например 22 AWG, 24 AWG, 26 AWG. Чем больше номер типа проводника, тем меньше его диаметр. В вычислительных сетях наиболее употребительными являются типы проводников, приведенные выше в качестве примеров. В европейских и международных стандартах диаметр проводника указывается в миллиметрах.

Помимо электромагнитных хар-к есть ещё механические и конструктивные хар-ки, определяющие тип изоляции, конструкцию разъема и т. п. Существуют хар-ки, которые применимы только к определенному типу кабеля. Напр., параметр шаг скрутки проводов используется только для характеристики витой пары, а параметр NEXT применим только к многопарным кабелям на основе витой пары.

Стандарты определены для **четырех типов кабеля**:

- на основе неэкранированной витой пары,
- на основе экранированной витой пары,
- коаксиального
- волоконно-оптического кабелей

Стандарты кабелей:

- Американский стандарт EIA/TIA-568A
- Международный стандарт ISO/IEC 11801.
- Европейский стандарт EN50173.

Кроме этих открытых стандартов, многие компании в свое время разработали свои фирменные стандарты, из которых до сих пор имеет практическое значение только один - стандарт компании IBM.

При стандартизации кабелей принят протокольно-независимый подход. Это означает, что в стандарте оговариваются электрические, оптические и механические характеристики, которым должен удовлетворять тот или иной тип кабеля или соединительного изделия - разъема, кроссовой коробки и т. п. Однако для какого протокола предназначен данный кабель, стандарт не оговаривает. Поэтому нельзя приобрести кабель для протокола Ethernet или FDDI, нужно просто знать, какие типы стандартных кабелей поддерживают протоколы Ethernet и FDDI.

Выводы (альтернативный ответ на билет №10)

В компьютерных сетях применяются кабели, удовлетворяющие определенным стандартам. Современные стандарты определяет характеристики не отдельного кабеля, а полного набора элементов, необходимого для создания кабельного соединения, например шнура от рабочей станции до розетки, самой розетки, основного кабеля, жесткого кроссового соединения и шнура до концентратора.
Сегодня наиболее употребительными **стандартами** являются:

- американский стандарт EIA/TIA-568A,
- международный стандарт ISO/IEC 11801,
- европейский стандарт EN50173,
- а также фирменный стандарт компании IBM.

Стандарты определены для четырех типов кабеля:

- на основе неэкранированной витой пары,
- на основе экранированной витой пары,
- коаксиального и волоконно-оптического кабелей.

Кабель на основе неэкранированной витой пары в зависимости от электрических и механических характеристик разделяется на 5 категорий.

- Кабели *категории 1* применяются там, где требования к скорости передачи минимальны.
- Главная особенность кабелей *категории 2* - способность передавать сигналы со спектром до 1 МГц.
- Кабели *категории 3* широко распространены и предназначены как для передачи данных, так и для передачи голоса.
- Кабели *категории 4* представляют собой несколько улучшенный вариант кабелей категории 3 и на практике используются редко.
- Кабели *категории 5* были специально разработаны для поддержки высокоскоростных протоколов FDDI, Fast Ethernet, 100VG-AnyLAN, ATM и Gigabit Ethernet.

Кабель на основе экранированной витой пары хорошо защищает передаваемые сигналы от внешних помех, а пользователей сетей - от вредного для здоровья излучения. Наличие заземляемого экрана удорожает кабель и усложняет его прокладку. Экранированный кабель применяется только для передачи данных. Основным стандартом, определяющим параметры экранированной витой пары, является фирменный стандарт IBM. В этом стандарте кабели делятся на типы: Type 1, Type 2,..., Type 9, из которых основным является кабель Type 1.

Коаксиальные кабели существует в большом количестве вариантов:

- «толстый» коаксиальный кабель,
- различные разновидности «тонкого» коаксиального кабеля, которые обладают худшими механическими и электрическими характеристиками по сравнению с «толстым» коаксиальным кабелем, зато за счет своей гибкости более удобны при монтаже, сюда же относится телевизионный кабель.

Волоконно-оптические кабели обладают отличными электромагнитными и механическими характеристиками, недостаток их состоит в сложности и высокой стоимости монтажных работ.

Дополнительные сведения (вопр. №10)

Основное внимание в современных стандартах уделяется кабелям на основе витой пары и волоконно-оптическим кабелям.

1. Кабели на основе неэкранированной витой пары

Медный неэкранированный кабель **UTP** в зависимости от электрических и механических характеристик разделяется на 5 категорий (Category 1 - Category 5). Кабели категорий 1 и 2 были определены в стандарте EIA/TIA-568, но в стандарт 568A уже не вошли, как устаревшие.

Кабели категории 1 применяются там, где требования к скорости передачи минимальны. Обычно это кабель для цифровой и аналоговой передачи голоса и низкоскоростной (до 20 Кбит/с) передачи данных. До 1983 года это был основной тип кабеля для телефонной разводки.

Кабели категории 2 были впервые применены фирмой IBM при построении собственной кабельной системы. Главное требование к кабелям этой категории - способность передавать сигналы со спектром до 1 МГц.

Кабели категории 3 были стандартизованы в 1991 году, когда был разработан ***Стандарт телекоммуникационных кабельных систем для коммерческих зданий*** (EIA-568), на основе которого затем был создан действующий стандарт EIA-568A. Стандарт EIA-568 определил электрические характеристики кабелей категории 3 для частот в диапазоне до 16 МГц, поддерживающих, таким образом, высокоскоростные сетевые приложения. Кабель категории 3 предназначен как для передачи данных, так и для передачи голоса. Шаг скрутки проводов равен примерно 3 витка на 1 фут (30,5 см). Кабели категории 3 сейчас составляют основу многих кабельных систем зданий, в которых они используются для передачи и голоса, и данных.

Кабели категории 4 представляют собой несколько улучшенный вариант кабелей категории 3. Кабели категории 4 обязаны выдерживать тесты на частоте передачи сигнала 20 МГц и обеспечивать повышенную помехоустойчивость и низкие потери сигнала. Кабели категории 4 хорошо подходят для применения в системах с увеличенными расстояниями (до 135 метров) и в сетях Token Ring с пропускной способностью 16 Мбит/с. На практике используются редко.

Кабели категории 5 были специально разработаны для поддержки высокоскоростных протоколов. Поэтому их характеристики определяются в диапазоне до 100 МГц. Большинство новых высокоскоростных стандартов ориентируются на использование витой пары 5 категории. На этом кабеле работают протоколы со скоростью передачи данных 100 Мбит/с - FDDI (с физическим стандартом TP-PMD), Fast Ethernet, l00VG-AnyLAN, а также более скоростные протоколы - ATM на скорости 155 Мбит/с, и Gigabit Ethernet на скорости 1000 Мбит/с (вариант Gigabit Ethernet на витой паре категории 5 стал стандартом в июне 1999 г.). Кабель категории 5 пришел на замену кабелю категории 3, и сегодня все новые кабельные системы крупных зданий строятся именно на этом типе кабеля (в сочетании с волоконно-оптическим).

Наиболее важные электромагнитные хар-ки кабеля категории 5 имеют след. значения:

- полное волновое сопротивление в диапазоне частот до 100 МГц равно 100 Ом (стандарт ISO 11801 допускает также кабель с волновым сопротивлением 120 Ом);
- величина перекрестных наводок NEXT в зависимости от частоты сигнала должна принимать значения не менее 74 дБ на частоте 150 кГц и не менее 32 дБ на частоте 100 МГц;
- затухание имеет предельные значения от 0,8 дБ (на частоте 64 кГц) до 22 дБ (на частоте 100 МГц);
- активное сопротивление не должно превышать 9,4 Ом на 100 м;
- емкость кабеля не должна превышать 5,6 нф на 100 м.

Все кабели UTP независимо от их категории выпускаются в 4-парном исполнении. Каждая из четырех пар кабеля имеет определенный цвет и шаг скрутки. Обычно две пары предназначены для передачи данных, а две - для передачи голоса.

Для соединения кабелей с оборудованием используются вилки и розетки RJ-45, представляющие 8-контактные разъемы, похожие на обычные телефонные разъемы. RJ-11.

Особое место занимают кабели категорий 6 и 7, которые промышленность начала выпускать сравнительно недавно. Для кабеля категории 6 характеристики определяются до частоты 200 МГц, а для кабелей категории 7 - до 600 МГц. Кабели категории 7 обязательно экранируются, причем как каждая пара, так и весь кабель в целом. Кабель категории 6 может быть как экранированным, так и неэкранированным. Основное назначение этих кабелей - поддержка высокоскоростных протоколов на отрезках кабеля большей длины, чем кабель UTP категории 5. Некоторые специалисты сомневаются в необходимости применения кабелей категории 7, так как стоимость кабельной системы при их использовании получается соизмеримой по стоимости сети с использованием волоконно-оптических кабелей, а характеристики кабелей на основе оптических волокон выше.

2. Кабели на основе экранированной витой пары

Экранированная витая пара **STP** хорошо защищает передаваемые сигналы от внешних помех, а также меньше излучает электромагнитных колебаний вовне, что защищает, в свою очередь, пользователей сетей от вредного для здоровья излучения. Наличие заземляемого экрана удорожает кабель и усложняет его прокладку, так как требует выполнения качественного заземления. Экранированный кабель применяется только для передачи данных, а голос по нему не передают.

Основным стандартом, определяющим параметры экранированной витой пары, является фирменный стандарт **IBM**. В этом стандарте кабели делятся не на категории, а на типы: **Type I, Type 2,..., Type 9**.

Основным типом экранированного кабеля является кабель **Type 1** стандарта **IBM**. Он состоит из 2-х пар скрученных проводов, экранированных проводящей оплеткой, которая заземляется. Электрические параметры кабеля Type 1 примерно соответствуют параметрам кабеля UTP категории 5. Однако волновое сопротивление кабеля Type 1 равно 150 Ом (UTP категории 5 имеет волновое сопротивление 100 Ом), поэтому простое «улучшение» кабельной проводки сети путем замены неэкранированной пары UTP на STP Type 1 невозможно. Трансиверы, рассчитанные на работу с кабелем, имеющим волновое сопротивление 100 Ом, будут плохо работать на волновое сопротивление 150 Ом. Поэтому при использовании STP Type 1 необходимы соответствующие трансиверы. Такие трансиверы имеются в сетевых адаптерах Token Ring, так как эти сети разрабатывались для работы на экранированной витой паре. Некоторые другие стандарты также поддерживают кабель STP Type I - например, l00VG-AnyLAN, а также Fast Ethernet (хотя основным типом кабеля для Fast Ethernet является UTP категории 5). В случае если технология может использовать UTP и STP, нужно убедиться, на какой тип кабеля рассчитаны приобретаемые трансиверы. Сегодня кабель STP Type 1 включен в стандарты EIA/TIA-568A, ISO 11801 и EN50173, то есть приобрел международный статус.

Экранированные витые пары используются также в кабеле IBM **Type 2**, который представляет кабель Type 1 с добавленными 2 парами неэкранированного провода для передачи голоса.

Для присоединения экранированных кабелей к оборудованию используются разъемы конструкции IBM.

Не все типы кабелей стандарта IBM относятся к экранированным кабелям - некоторые определяют характеристики неэкранированного телефонного кабеля (Type 3) и оптоволоконного кабеля (Type 5).

3. Коаксиальные кабели

Существует большое количество типов коаксиальных кабелей, используемых в сетях различного типа - телефонных, телевизионных и компьютерных. Ниже приводятся основные типы и характеристики этих кабелей.

- **RG-8** и **RG-11** - «толстый» коаксиальный кабель, разработанный для сетей Ethernet l0Base-5. Имеет волновое сопротивление 50 Ом и внешний диаметр 0,5 дюйма (около 12 мм). Этот кабель имеет достаточно толстый внутренний проводник диаметром 2,17 мм, который обеспечивает хорошие механические и электрические характеристики (затухание на частоте 10 МГц - не хуже 18 дБ/км). Зато этот кабель сложно монтировать - он плохо гнется.
- **RG-58/U**, **RG-58 A/U** и **RG-58 C/U** - разновидности «тонкого» коаксиального кабеля для сетей Ethernet l0Base-2. Кабель RG-58/U имеет сплошной внутренний проводник, а кабель RG-58 A/U - многожильный. Кабель RG-58 C/U проходит «военную приемку». Все эти разновидности кабеля имеют волновое сопротивление 50 Ом, но обладают худшими механическими и электрическими характеристиками по сравнению с «толстым» коаксиальным кабелем. Тонкий внутренний проводник 0,89 мм не так прочен, зато обладает гораздо большей гибкостью, удобной при монтаже. Затухание в этом типе кабеля выше, чем в «толстом» коаксиальном кабеле, что приводит к необходимости уменьшать длину кабеля для получения одинакового затухания в сегменте. Для соединения кабелей с оборудованием используется разъем типа BNC.
- **RG-59** - телевизионный кабель с волновым сопротивлением 75 Ом. Широко применяется в кабельном телевидении.
- **RG-62** - кабель с волновым сопротивлением 93 Ома, использовался в сетях ArcNet, оборудование которых сегодня практически не выпускается. Коаксиальные кабели с волновым сопротивлением 50 Ом (то есть «тонкий» и «толстый») описаны в стандарте EIA/TIA-568. Новый стандарт EIA/TIA-568A коаксиальные кабели не описывает, как морально устаревшие.

4. Волоконно-оптические кабели

Волоконно-оптические кабели состоят из центрального проводника света (сердцевины) - стеклянного волокна, окруженного другим слоем стекла - оболочкой, обладающей меньшим показателем преломления, чем сердцевина. Распространяясь по сердцевине, лучи света не выходят за ее пределы, отражаясь от покрывающего слоя оболочки. В зависимости от распределения показателя преломления и от величины диаметра сердечника различают:

- многомодовое волокно со ступенчатым изменением показателя преломления (рис. 2.11, а);
- многомодовое волокно с плавным изменением показателя преломления (рис. 2.11,6);
- одномодовое волокно (рис. 2.11, в).

Понятие «мода» описывает режим распространения световых лучей во внутреннем сердечнике кабеля. В одномодовом кабеле (Single Mode Fiber, SMF) используется центральный проводник очень малого диаметра, соизмеримого с длиной волны света - от 5 до 10 мкм. При этом практически все лучи света распространяются вдоль оптической оси световода, не отражаясь от внешнего проводника. Полоса пропускания одномодового кабеля очень широкая - до сотен гигагерц на километр. Изготовление тонких качественных волокон для одномодового кабеля представляет сложный технологический процесс, что делает одномодовый кабель достаточно дорогим. Кроме того, в волокно такого маленького диаметра достаточно сложно направить пучок света, не потеряв при этом значительную часть его энергии.

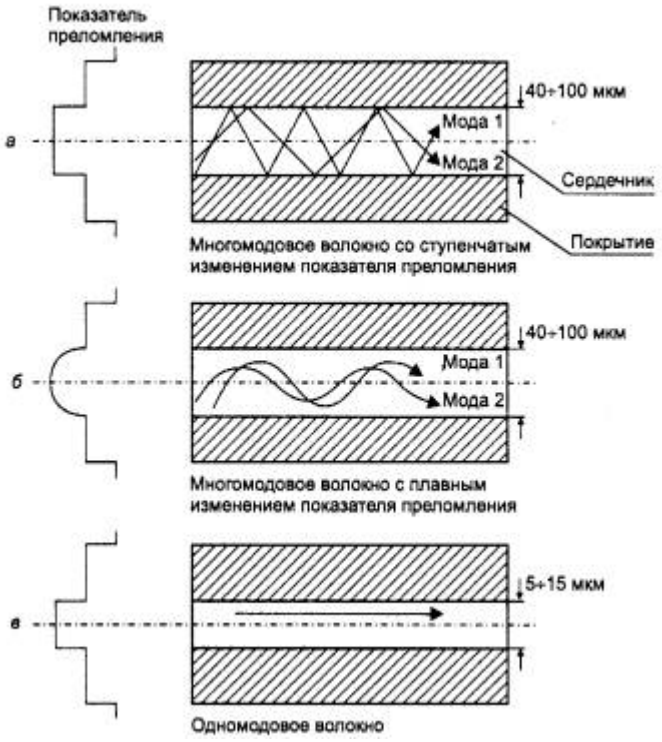


Рис. 2.11. Типы оптического кабеля

В многомодовых кабелях (Multi Mode Fiber, MMF) используются более широкие внутренние сердечники, которые легче изготовить технологически. В стандартах определены два наиболее употребительных многомодовых кабеля: 62,5/125 мкм и 50/125 мкм, где 62,5 мкм или 50 мкм - это диаметр центрального проводника, а 125 мкм - диаметр внешнего проводника.

В многомодовых кабелях во внутреннем проводнике одновременно существует несколько световых лучей, отражающихся от внешнего проводника под разными углами. Угол отражения луча называется модой луча. В многомодовых кабелях с плавным изменением коэффициента преломления режим распространения каждой моды имеет более сложный характер.

Многомодовые кабели имеют более узкую полосу пропускания - от 500 до 800 МГц/км. Сужение полосы происходит из-за потерь световой энергии при отражениях, а также из-за интерференции лучей разных мод.

В качестве источников излучения света в волоконно-оптических кабелях применяются:

- светодиоды;
- полупроводниковые лазеры.

Для одномодовых кабелей применяются только полупроводниковые лазеры, так как при таком малом диаметре оптического волокна световой поток, создаваемый светодиодом, невозможно без больших потерь направить в волокно. Для многомодовых кабелей используются более дешевые светодиодные излучатели.

Для передачи информации применяется свет с длиной волны 1550 нм (1,55 мкм), 1300 нм (1,3 мкм) и 850 нм (0,85 мкм). Светодиоды могут излучать свет с длиной волны 850 нм и 1300 нм. Излучатели с длиной волны 850 нм существенно дешевле, чем излучатели с длиной волны 1300 нм, но полоса пропускания кабеля для волн 850 нм уже, например 200 МГц/км вместо 500 МГц/км.

Лазерные излучатели работают на длинах волн 1300 и 1550 нм. Быстродействие современных лазеров позволяет модулировать световой поток с частотами 10 ГГц и выше. Лазерные излучатели создают когерентный поток света, за счет чего потери в оптических волокнах становятся меньше, чем при использовании некогерентного потока светодиодов.

Использование только нескольких длин волн для передачи информации в оптических волокнах связанно с особенностью их амплитудно-частотной характеристики. Именно для этих дискретных длин волн наблюдаются ярко выраженные максимумы передачи мощности сигнала, а для других волн затухание в волокнах существенно выше.

Волоконно-оптические кабели присоединяют к оборудованию разъемами MIC, ST и SC.

Волоконно-оптические кабели обладают отличными характеристиками всех типов: электромагнитными, механическими (хорошо гнутся, а в соответствующей изоляции обладают хорошей механической прочностью). Однако у них есть один серьезный недостаток - сложность соединения волокон с разъемами и между собой при необходимости наращивания длины кабеля.

Сама стоимость волоконно-оптических кабелей ненамного превышает стоимость кабелей на витой паре, однако проведение монтажных работ с оптоволокном обходится намного дороже из-за трудоемкости операций и высокой стоимости применяемого монтажного оборудования. Так, присоединение оптического волокна к разъему требует проведения высокоточной обрезки волокна в плоскости строго перпендикулярной оси волокна, а также выполнения соединения путем сложной операции склеивания, а не обжатия, как это делается для витой пары. Выполнение же некачественных соединений сразу резко сужает полосу пропускания волоконно-оптических кабелей и линий.

11. Структурированные кабельные сети (системы)

Структурированная кабельная система

(Structured Cabling System, **SCS**) – это:

- набор коммутационных элементов (кабелей, разъемов, коннекторов, кроссовых панелей и шкафов),
- а также методика их совместного использования, которая позволяет создавать регулярные, легко расширяемые структуры связей в вычислительных сетях.

Зачем это нужно:

При построении больших сетей возникают различные ограничения:

- огр. на длину связи между узлами;
- огр. на кол-во узлов в сети;
- огр. на интенсивность трафика, порождаемого узлами сети.

Для снятия этих ограничений используются специальные методы структуризации сети и специальное структурообразующее оборудование - повторители, концентраторы, мосты, коммутаторы, маршрутизаторы. Оборудование такого рода также называют коммуникационным

Структурированная кабельная система (далее SCS) представляет своего рода «**конструктор**», с помощью которого проектировщик сети строит нужную ему конфигурацию из стандартных кабелей, соединенных стандартными разъемами и коммутируемых на стандартных кроссовых панелях. При необходимости конфигурацию связей можно легко изменить - добавить компьютер, сегмент, коммутатор, изъять ненужное оборудование, а также поменять соединения между компьютерами и концентраторами.

При построении SCS подразумевается, что каждое рабочее место на предприятии должно быть оснащено розетками для подключения телефона и компьютера. То есть хорошая SCS строится **избыточной**.

Кабели, представляющие собой набор витых пар, прокладываются в каждом здании, разводятся между этажами, на каждом этаже используется специальный .кроссовый шкаф, от которого провода в трубах и коробах подводятся к каждой комнате и разводятся по розеткам.

SCS планируется и строится **иерархически**, с главной магистралью и многочисленными ответвлениями от нее (рис. 4.1).

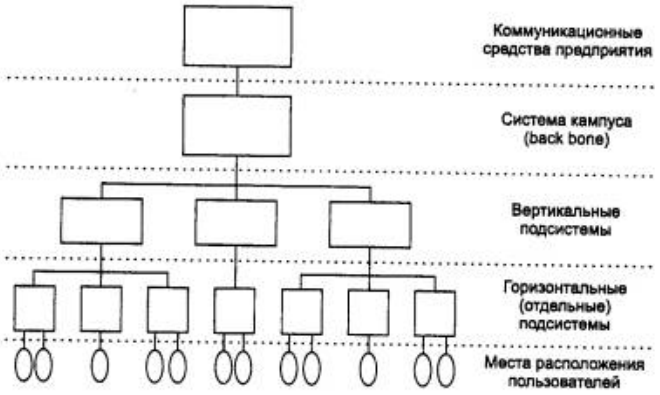


Рис. 4.1. Иерархия структурированной кабельной системы

Типичная иерархическая структура SCS (рис. 4.2) включает:

- **Горизонтальная подсистема** (в пределах этажа) соединяет кроссовый шкаф этажа с розетками пользователей. Подсистемы этого типа соответствуют этажам здания.
- **Вертикальная подсистема** (внутри здания); соединяет кроссовые шкафы каждого этажа с центральной аппаратной здания.
- **Подсистема кампуса** (в пределах одной территории с несколькими зданиями)соединяет неск. зданий с главной аппаратной всего кампуса. Эта часть каб. сист. обычно называется магистралью (**backbone**).

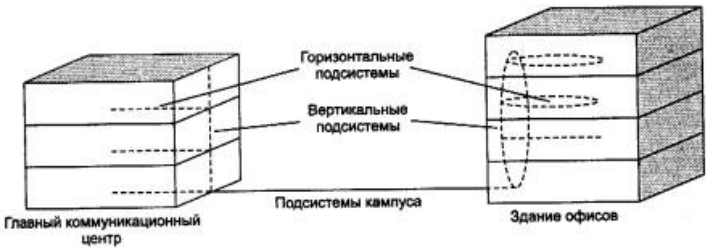


Рис. 4.2. Структура кабельных подсистем

Преимущества использования SCS (коротко):

- Универсальность.
- Увеличение срока службы.
- Уменьшение стоимости добавления новых пользователей и изменения их мест размещения.
- Возможность легкого расширения сети.
- Обеспечение более эффективного обслуживания.
- Надежность.

Подробнее см. на след. Стр.

Преимущества использования SCS (подробно):

- Универсальность. (единая среда для передачи комп. данных в лок. выч. сети, лок. телеф. сети, передачи видеоинф., сигналов от датчиков пож. безоп. или охр. систем позволяет автоматизировать многие процессы контроля, мониторинга и управления хоз. службами и системами жизнеобеспечения предприятия).
- Увеличение срока службы. (Срок морального старения SCS. – 10-15 лет.)
- Уменьшение стоимости добавления новых пользователей и изменения их мест размещения. (более выгодно провести однократную работу по прокладке кабеля, возможно, с большим запасом по длине, чем несколько раз выполнять прокладку, наращивая длину кабеля.)
- Возможность легкого расширения сети. SCS является модульной, поэтому ее легко расширять. (к магистрали можно добавить новую подсеть, не оказывая никакого влияния на существующие подсети. Можно заменить в отдельной подсети тип кабеля независимо от остальной части сети. SCS является основой для деления сети на легко управляемые логические сегменты, так как она сама уже разделена на физические сегменты).
- Обеспечение более эффективного обслуживания. SCS облегчает обслуживание и поиск неисправностей по сравнению с шинной кабельной системой. При шинной организации кабельной системы отказ одного из устройств или соединительных элементов приводит к трудно локализуемому отказу всей сети. В SCS отказ одного сегмента не действует на другие, так как объединение сегментов осуществляется с помощью концентраторов. Концентраторы диагностируют и локализуют неисправный участок.
- Надежность. SCS имеет повышенную надежность, поскольку производитель такой системы гарантирует не только качество ее отдельных компонентов, но и их совместимость.

Первой структурированной кабельной системой, имеющий все современные черты такого типа систем, была система SYSTIMAX SCS компании Lucent Technologies (ранее - подразделение AT&T). И сегодня компании Lucent Technologies принадлежит основная доля мирового рынка. Многие другие компании также выпускают качественные структурированные кабельные системы, например AMP, BICC Brand-Rex, Siemens, Alcatel, MOD-TAP. На российском рынке успешно завоевывает себе место под солнцем отечественная структурированная кабельная система АйТи-СКС московской компании «АйТи».

ВЫВОДЫ к главе 4.1 (альтернативный ответ на билет)

Кабельная система составляет фундамент любой компьютерной сети. От ее качества зависят все основные свойства сети.

Структурированная кабельная система представляет собой набор коммуникационных элементов - кабелей, разъемов, коннекторов, кроссовых панелей и шкафов, которые удовлетворяют стандартам и позволяют создавать регулярные, легко расширяемые структуры связей.

Структурированная кабельная система состоит из трех подсистем:

- горизонтальной (в пределах этажа),
- вертикальной (между этажами)
- и подсистемы кампуса (в пределах одной территории с несколькими зданиями).

Для горизонтальной подсистемы характерно наличие большого количества ответвлений и перекрестных связей. Наиболее подходящий тип кабеля - неэкранированная витая пара категории 5.

Вертикальная подсистема состоит из более протяженных отрезков кабеля, количество ответвлений намного меньше, чем в горизонтальной подсистеме. Предпочтительный тип кабеля - волоконно-оптический.

Для подсистемы кампуса характерна нерегулярная структура связей с центральным зданием. Предпочтительный тип кабеля - волоконно-оптический в специальной изоляции.

Кабельная система здания строится избыточной, так как стоимость последующего расширения кабельной системы превосходит стоимость установки избыточных элементов

12. Проблемы совместного использования линий связи. Мультиплексирование и демультиплексирование. TDM и цифровая телефония.

При совместном использовании линий связи (далее ЛС) возникает комплекс проблем, к-рый вкл.:
- чисто электрические проблемы;
- логические проблемы разделения во врем. доступа.

Для реш. этих и др. проблем, наряду с разл. методами используют методы коммутации
Существуют три принципиально различные схемы коммутации абонентов в сетях:
- **коммутация каналов** (circuit switching),
- **коммутация пакетов** (packet switching)
- **коммутация сообщений** (message switching).

Коммутация каналов подразумевает образование непрерывного составного физ. канала из последовательно соединенных отдельных канальных участков для прямой передачи данных между узлами. Отдельные каналы соединяются между собой специальной аппаратурой - **коммутаторами**, которые могут устанавливать связи между любыми конечными узлами сети.

Коммутаторы, а также соединяющие их каналы должны обеспечивать одновременную передачу данных нескольких абонентских каналов. Для этого они должны быть высокоскоростными и поддерживать какую-либо **технику мультиплексирования** абонентских каналов.

В настоящее время для мультиплексирования абонентских каналов используются две техники:
- **техника частотного мультиплексирования** (Frequency Division Multiplexing, **FDM**); разрабатывалась в расчете на передачу непрер. сигналов (голос).
- **техника мультиплексирования с разделением времени** (Time Division Multiplexing, **TDM**). Эта новая техника мультиплексирования, ориентирующаяся на дискретный характер передаваемых данных, была разработана, при переходе к цифр. форме представления голоса

Аппаратура TDM-сетей - мультиплексоры, коммутаторы, демультиплексоры -работает в режиме разделения времени, поочередно обслуживая в теч. цикла своей работы все абонентские каналы. Цикл работы оборудования TDM равен 125 мкс, что соответствует периоду следования замеров голоса в цифровом абонентском канале. Это значит, что мультиплексор или коммутатор успевает вовремя обслужить любой абонентский канал и передать его очередной замер далее по сети. Каждому соединению выделяется один квант времени цикла работы аппаратуры, называемый также **тайм-слотом**. Длительность тайм-слота зависит от числа абонентских каналов, обслуживаемых мультиплексором TDM или коммутатором.

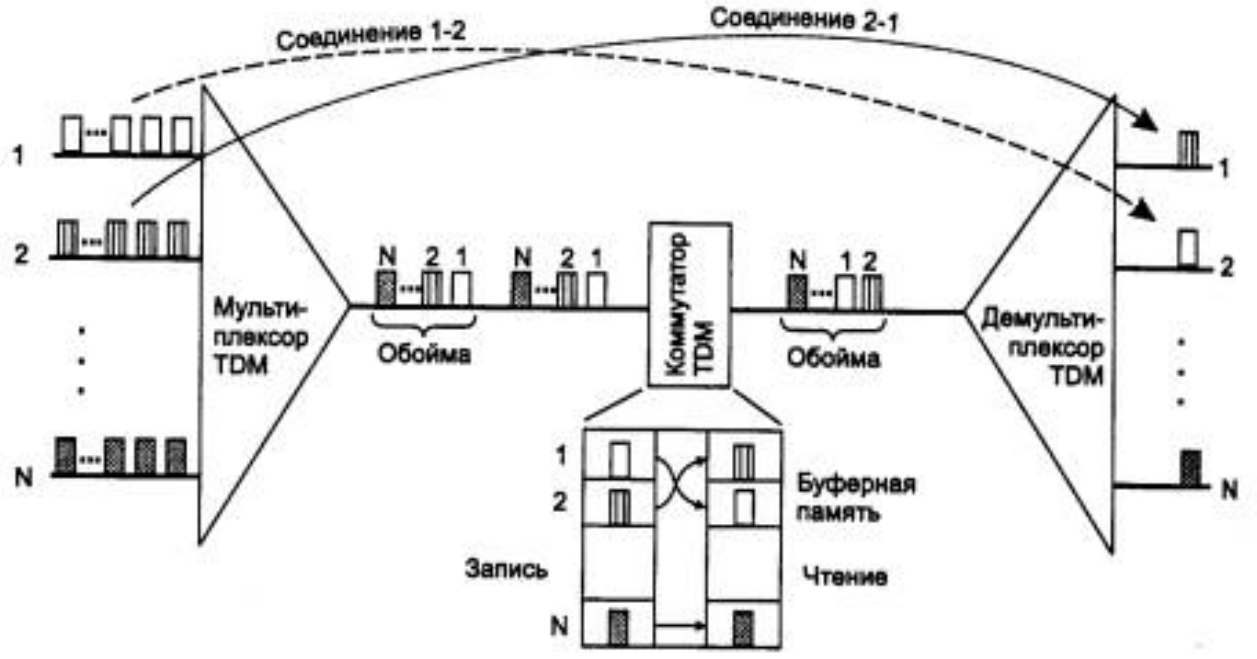


Рис. 2.28. Коммутация на основе разделения канала во времени

Мультиплексор принимает инф-цию по N входным каналам от конечных абонентов, каждый из к-рых передает данные по абонентскому каналу со скоростью 64 Кбит/с - 1 байт каждые 125 мкс. В каждом цикле мультиплексор выполняет следующие действия:

прием от каждого канала очередного байта данных;
составление из принятых байтов уплотненного кадра, называемого также обоймой;
передача уплотненного кадра на выходной канал с битовой скоростью, равной N*64 Кбит/с.

Порядок байт в обойме соответствует номеру входного канала, от которого этот байт получен. Количество обслуживаемых мультиплексором абонентских каналов зависит от его быстродействия. Например, мультиплексор T1, представляющий собой первый промышленный мультиплексор, работавший по технологии TDM, поддерживает 24 входных абонентских канала, создавая на выходе обоймы стандарта T1, передаваемые с битовой скоростью 1,544 Мбит/с.

Демультиплексор выполняет обратную задачу - он разбирает байты уплотненного кадра и распределяет их по своим нескольким выходным каналам, при этом он считает, что порядковый номер байта в обойме соответствует номеру выходного канала.

Коммутатор принимает уплотненный кадр по скоростному каналу от мультиплексора и записывает каждый байт из него в отдельную ячейку своей буферной памяти, причем в том порядке, в котором эти байты были упакованы в уплотненный кадр. Для выполнения операции коммутации байты извлекаются из буферной памяти не в порядке поступления, а в таком порядке, который соответствует поддерживаемым в сети соединениям абонентов. Так, например, если первый абонент левой части сети рис. 2.28 должен соединиться со вторым абонентом в правой части сети, то байт, записанный в первую ячейку буферной памяти, будет извлекаться из нее вторым. «Перемешивая» нужным образом байты в обойме, коммутатор обеспечивает соединение конечных абонентов в сети.

Однажды выделенный номер тайм-слота остается в распоряжении соединения «входной канал-выходной слот» в течение всего времени существования этого соединения, даже если передаваемый трафик является пульсирующим и не всегда требует захваченного количества тайм-слотов. Это означает, что соединение в сети TDM всегда обладает известной и фиксированной пропускной способностью, кратной 64 Кбит/с.

Сети, использующие технику TDM, требуют синхронной работы всего оборудования, что и определило второе название этой техники - синхронный режим передач (STM). Нарушение синхронности разрушает требуемую коммутацию абонентов, так как при этом теряется адресная информация..

ВЫВОДЫ к главе 2.4 (альтернативный ответ на билет 12)

- В сетях для соединения абонентов используются три метода коммутации: коммутация каналов, коммутация пакетов и коммутация сообщений.
- Как коммутация каналов, так и коммутация пакетов может быть либо динамической, либо постоянной.
- 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 аналоговой 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.

13. Сети с коммутацией каналов и сети с коммутацией пакетов. Основные отличия и характеристики. Применения и примеры сетей с различными способами коммутации.

Существуют три принципиально различные схемы коммутации абонентов в сетях:

- **коммутация каналов** (circuit switching),
- **коммутация пакетов** (packet switching)
- **коммутация сообщений** (message switching).

Каждая из этих схем имеет свои «+» и «—» , но по долгосрочным прогнозам будущее принадлежит технологии коммутации пакетов, как более гибкой и универсальной.

Как сети с коммутацией пакетов, так и сети с Коммутацией каналов можно разделить на два класса по другому признаку:

- на сети с динамической коммутацией (соединение по инициативе пользователя на время сеанса связи)
- и сети с постоянной коммутацией. (сеть разрешает паре пользователей заказать соединение на длительный период времени,. соединение устанавливается персоналом, обслуживающим сеть)

Примерами сетей, поддерживающих режим динамической коммутации, являются телефонные сети общего пользования, локальные сети, сети TCP/IP

Некоторые типы сетей поддерживают оба режима работы. Например, сети X.25 и ATM

Коммутация каналов подразумевает образование непрерывного составного физ. канала из последовательно соединенных отдельных канальных участков для прямой передачи данных между узлами. Подразделяется на **FDM** и **TDM**

Общие свойства сетей с коммутацией каналов (FDM и TDM):

Если соединение установлено, то ему выделяется фиксированная полоса частот в FDM-сетях или же фиксированная пропускная способность в TDM-сетях. Эти величины остаются неизменными в течение всего периода соединения. Т.е.

+ **гарантированная пропускная способность** является важным свойством, необходимым для таких приложений, как передача голоса, изображения или управления объектами в реальном масштабе времени.

– Однако динамически **изменять пропускную способность** канала по требованию абонента сети с коммутацией каналов не могут, что делает их неэффективными в условиях пульсирующего трафика.

–невозможность применения пользовательской аппаратуры, работающей с разной скоростью, так как сети с коммутацией каналов не буферизуют данные пользователей.

+ Сети с коммутацией каналов хорошо приспособлены для коммутации потоков данных постоянной скорости, когда единицей коммутации является не отдельный байт или пакет данных, а долговременный синхронный поток данных между двумя абонентами

Рис. 2.29. Разбиение сообщения на пакеты

Коммутация пакетов - все передаваемые пользователем сети сообщения разбиваются в исходном узле на сравнительно небольшие части, называемые пакетами (была спец. разработана для эфф. передачи компьютерного трафика). Каждый пакет снабжается заголовком, в котором указывается адресная информация, необходимая для доставки пакета узлу назначения, а также номер пакета, который будет использоваться узлом назначения для сборки сообщения. Пакеты транспортируются в сети как независимые информационные блоки. Коммутаторы сети принимают пакеты от конечных узлов и на основании адресной информации передают их друг другу, а в конечном итоге - узлу назначения

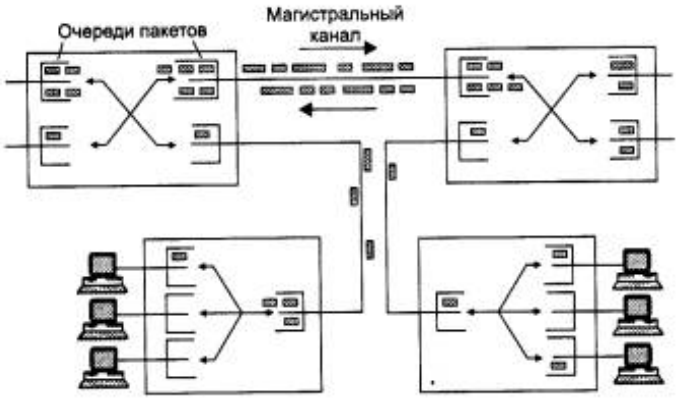


Рис. 2.30. Сглаживание пульсаций трафика в сети с коммутацией пакетов

Коммутаторы пакетной сети отличаются от коммутаторов каналов тем, что они имеют внутреннюю буферную память для временного хранения пакетов, если выходной порт коммутатора в момент принятия пакета занят передачей другого пакета (рис. 2.30). В этом случае пакет находится некоторое время в очереди

пакетов в буферной памяти выходного порта, а когда до него дойдет очередь, то он передается следующему коммутатору. Такая схема передачи данных позволяет сглаживать пульсации трафика на магистральных связях между коммутаторами и тем самым использовать их наиболее эффективным образом для повышения пропускной способности сети в целом

Одним из отличий метода коммутации пакетов от метода коммутации каналов является неопределенность пропускной способности соединения между двумя абонентами. В методе коммутации каналов после образования составного канала пропускная способность сети при передаче данных между конечными узлами известна - это пропускная способность канала.

процесс передачи для определенной пары абонентов в сети с коммутацией пакетов является более медленным, чем в сети с коммутацией каналов.

Неопределенная пропускная способность сети с коммутацией пакетов - это плата за ее общую эффективность при некотором ущемлении интересов отдельных абонентов.

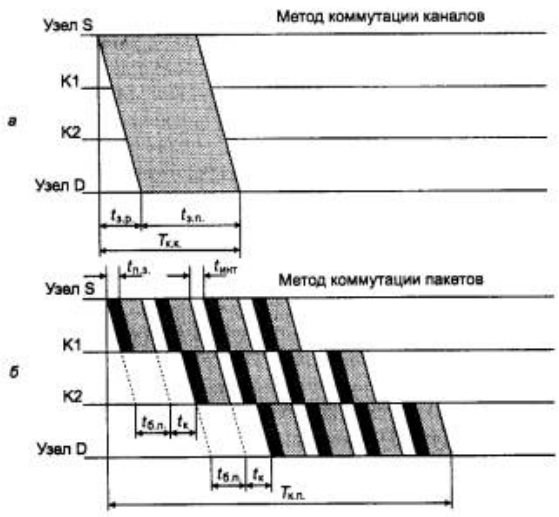


Рис. 2.31. Задержки передачи данных в сетях с коммутацией каналов и пакетов

На эффективность работы сети существенно влияют размеры пакетов, которые передает сеть. Слишком большие размеры пакетов приближают сеть с коммутацией пакетов к сети с коммутацией каналов, поэтому эффективность сети при этом падает. Слишком маленькие пакеты заметно увеличивают долю служебной информации, так как каждый пакет несет с собой заголовок фиксированной длины, а количество пакетов, на которые разбиваются сообщения, будет резко расти при уменьшении размера пакета. Существует некоторая золотая середина, которая обеспечивает максимальную эффективность работы сети, однако ее трудно определить точно, так как она зависит от многих факторов, некоторые из них к тому же постоянно меняются в процессе работы сети.

ВЫВОДЫ к главе 2.4 (альтернативный ответ на билет)

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

14. Методы доступа к среде передачи и их применение в локальных сетях ЭВМ.

Локальные вычислительные сети (ЛВС) – группа компьютеров, сосредоточенная на небольшой территории, объединенная одним или несколькими высокоскоростными каналами передачи данных, общем случае, коммуникационная система, принадлежащая одной организации**.**

Метод доступа регулирует доступ узлов к кабелю (среде передачи) и определяет порядок, по которому узлы получают право доступа к среде.

Методы доступа:

Централизованные. Управление обменом сосредоточенно в одном месте.

– 1. Неустойчивость к отказам центра

– 2. Малая гибкость управления (центр обычно не может оперативно реагировать на все события в сети).

+ 1. Отсутствие конфликтов.

+ 2. Простота реализации.

Децентрализованные. Вопросами управления, в т.ч. разрешением конфликтов, занимаются все абоненты сети.

+ Высокая устойчивость к отказам и большая гибкость.

Случайные. Случайное чередование передающих абонентов. Возможны конфликты, но предполагаются способы их разрешений.

– Плохо работают при больших информационных потоках и не гарантируют абоненту величину времени доступа.

+ Более устойчивы к отказам сетевого оборудования и более эффективно используют сеть при малой интенсивности обмена.

Основные принципы:

1. Слушай, прежде чем говорить

2. Слушай пока говоришь.

Пример: CSMA/CD (сеть Ethernet)

Детерминированые. Определяют четкие правила, по которым чередуются захватывающие сеть абоненты. Имеется систему приоритетов, причем приоритеты эти различны для всех абонентов.

+ Конфликты полностью исключены (или маловероятны).

Пример: Маркерный доступ (сети Token-Ring, FDDI). Право передачи имеет сетевое устройство владеющее специальным сообщением (маркером).

Комбинированые.

Были разработаны теоретически, но на практике не применяются.

(альтернативный ответ на билет №14)

Для упрощения и, соответственно, удешевления аппаратных и программных решений разработчики **первых локальных сетей** остановились на совместном использовании кабелей всеми компьютерами сети в режиме разделения времени, то есть режиме TDM. Наиболее явным образом режим совместного использования кабеля проявляется в классических сетях Ethernet, где коаксиальный кабель физически представляет собой неделимый отрезок кабеля, общий для всех узлов сети. Но и в сетях Token Ring и FDDI, где каждая соседняя пара компьютеров соединена, казалось бы, своими индивидуальными отрезками кабеля с концентратором, эти отрезки не могут использоваться компьютерами, которые непосредственно к ним подключены, в произвольный момент времени. Эти отрезки образуют логическое кольцо, доступ к которому как к единому целому может быть получен только по вполне определенному алгоритму, в котором участвуют все компьютеры сети. Использование кольца как общего разделяемого ресурса упрощает алгоритмы передачи по нему кадров, так как в каждый конкретный момент времени кольцо занято только одним компьютером.

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 применяется исключительно в сетях с логической 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. Одновременно все компьютеры сети имеют возможность немедленно (с учетом задержки распространения сигнала по физической среде) получить данные, которые любой из компьютеров начал передавать на общую шину (рис. 3.3). 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).

Рис. 3.3. Метод случайного доступа CSMA/CD

Почти все виды технологий Ethernet используют один и тот же метод разделения среды передачи данных - метод случайного доступа CSMA/CD, который определяет облик технологии в целом.

Важным явлением в сетях Ethernet является **коллизия** - ситуация, когда две станции одновременно пытаются передать кадр данных по общей среде. Наличие коллизий - это неотъемлемое свойство сетей Ethernet, являющееся следствием принятого случайного метода доступа. Возможность четкого распознавания коллизий обусловлена правильным выбором параметров сети, в частности соблюдением соотношения между минимальной длиной кадра и максимально возможным диаметром сети.

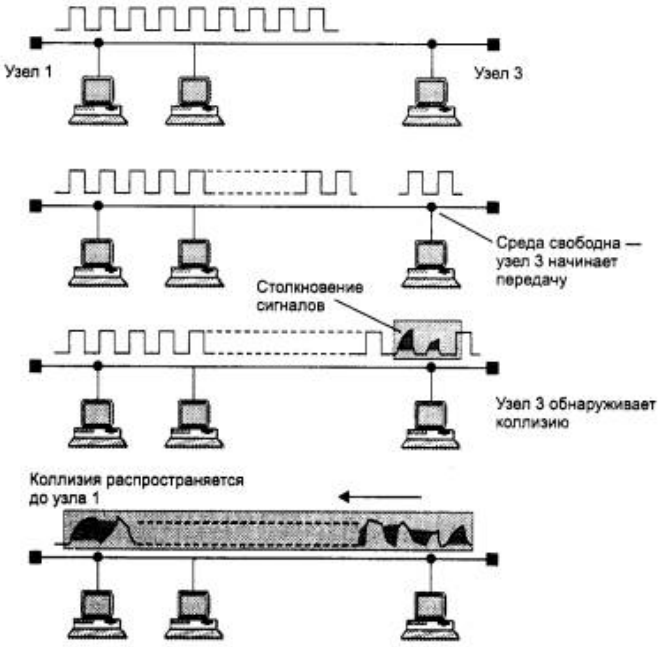


Рис. 3.4. Схема возникновения и распространения коллизии

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 скорейшего обнаружения коллизии всеми станциями сети станция, которая обнаружила коллизию, прерывает передачу своего кадра (в произвольном месте, возможно, и не на границе байта) и усиливает ситуацию коллизии посылкой в сеть специальной последовательности из 32 бит, называемой jam-последовательностью.После этого обнаружившая коллизию передающая станция обязана прекратить передачу и сделать паузу в течение короткого случайного интервала времени. Затем она может снова предпринять попытку захвата среды и передачи кадра

15. Сетевые топологии физического уровня и их связь с методами доступа к среде. Топология физических связей

Под **топологией** вычислительной сети понимается конфигурация графа, вершинам которого соответствуют компьютеры сети (иногда и другое оборудование, например концентраторы), а ребрам - физические связи между ними. Компьютеры, подключенные к сети, часто называют станциями или узлами сети

Конфигурация физических связей определяется электрическими соединениями компьютеров между собой и может отличаться от конфигурации логических связей между узлами сети. Логические связи представляют собой маршруты передачи данных между узлами сети и образуются путем соответствующей настройки коммуникационного оборудования.

Выбор топологии электрических связей существенно влияет на многие характеристики сети.

Полносвязная топология (рис. 1.10, а) соответствует сети, в которой каждый компьютер сети связан со всеми остальными. Для каждой пары компьютеров должна быть выделена отдельная электрическая линия связи.

Ячеистая топология (mesh) получается из полносвязной путем удаления некоторых возможных связей (рис. 1.10, б). В сети с ячеистой топологией непосредственно связываются только те компьютеры, между которыми происходит интенсивный обмен данными, а для обмена данными между компьютерами, не соединенными прямыми связями, используются транзитные передачи через промежуточные узлы. Ячеистая топология допускает соединение большого количества компьютеров и **характерна**, как правило, **для глобальных сетей**.

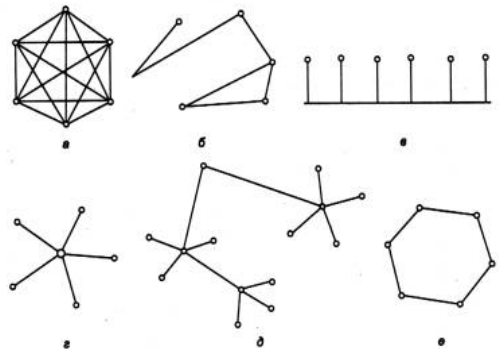


Рис. 1.10. Типовые топологии сетей

Общая шина(рис. 1.10, в) является очень распространенной (а до недавнего времени самой распространенной) топологией **для локальных сетей**. В этом случае компьютеры подключаются к одному коаксиальному кабелю по схеме «монтажного ИЛИ». Передаваемая информация может распространяться в обе стороны.

Основными преимуществами такой схемы являются дешевизна и простота разводки кабеля по помещениям. Самый серьезный недостаток общей шины заключается в ее низкой надежности: любой дефект кабеля или какого-нибудь из многочисленных разъемов полностью парализует всю сеть. Другим недостатком общей шины является ее невысокая производительность, так как при таком способе подключения в каждый момент времени только один компьютер может передавать данные в сеть. Поэтому пропускная способность канала связи всегда делится здесь между всеми узлами сети.

Топология звезда (рис. 1.10, г). В этом случае каждый компьютер подключается отдельным кабелем к общему устройству, называемому **концентратором,** который находится в центре сети. В функции концентратора входит направление передаваемой компьютером информации одному или всем остальным компьютерам сети. Главное преимущество этой топологии перед общей шиной - существенно большая надежность. Любые неприятности с кабелем касаются лишь того компьютера, к которому этот кабель присоединен, и только неисправность концентратора может вывести из строя всю сеть. Кроме того, концентратор может играть роль интеллектуального фильтра информации, поступающей от узлов в сеть, и при необходимости блокировать запрещенные администратором передачи.

К недостаткам топологии типа звезда относится более высокая стоимость сетевого оборудования из-за необходимости приобретения концентратора. Кроме того, возможности по наращиванию количества узлов в сети ограничиваются количеством портов концентратора.

В настоящее время иерархическая звезда является самым распространенным типом топологии связей как в локальных, так и глобальных сетях.

В сетях с **кольцевой конфигурацией** (рис. 1.10, е) данные передаются по кольцу от одного компьютера к другому, как правило, в одном направлении. Если компьютер распознает данные как «свои», то он копирует их себе во внутренний буфер. В сети с кольцевой топологией необходимо принимать специальные меры, чтобы в случае выхода из строя или отключения какой-либо станции не прервался канал связи между остальными станциями. Кольцо представляет собой очень удобную конфигурацию для организации обратной связи - данные, сделав полный оборот, возвращаются к узлу-источнику. Поэтому этот узел может контролировать процесс доставки данных адресату. Часто это свойство кольца используется для тестирования связности сети и поиска узла, работающего некорректно.

В то время как небольшие сети, как правило, имеют типовую топологию - звезда, кольцо или общая шина, для крупных сетей характерно наличие произвольных связей между компьютерами. В таких сетях можно выделить отдельные произвольно связанные фрагменты (подсети), имеющие типовую топологию, поэтому их называют **сетями со смешанной топологией** (рис. 1.11).

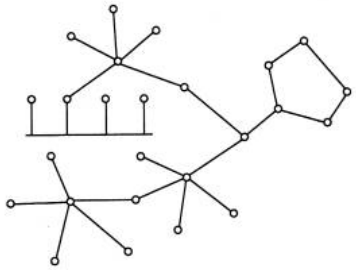


Рис. 1.11. Смешанная топология

Только в сети с полносвязной топологией для соединения каждой пары компьютеров имеется отдельная линия связи. Во всех остальных случаях неизбежно возникает вопрос о том, как организовать совместное использование линий связи несколькими компьютерами сети

В вычислительных сетях используют как индивидуальные линии связи между компьютерами, так и разделяемые (shared), когда одна линия связи попеременно используется несколькими компьютерами. В случае применения разделяемых линий связи (часто используется также термин разделяемая среда передачи данных - shared media) возникает комплекс проблем, связанных с их совместным использованием, который включает как чисто электрические проблемы обеспечения нужного качества сигналов при подключении к одному и тому же проводу нескольких приемников и передатчиков, так и логические проблемы разделения во времени доступа к этим линиям.

Классическим примером сети с разделяемыми линиями связи являются сети с топологией «**общая шина»,** в которых один кабель совместно используется всеми компьютерами сети. Ни один из компьютеров сети в принципе не может индивидуально, независимо от всех других компьютеров сети, использовать кабель, так как при одновременной передаче данных сразу несколькими узлами сигналы смешиваются и искажаются. В топологиях «кольцо» или «звезда» индивидуальное использование линий связи, соединяющих компьютеры, принципиально возможно, но эти кабели часто также рассматривают как разделяемые для всех компьютеров сети, так что, например, только один компьютер кольца имеет право в данный момент времени отправлять по кольцу пакеты другим компьютерам.

Несмотря на все эти сложности, в локальных сетях разделяемые линии связи используются очень часто. Этот подход, в частности, реализован в широко распространенных классических технологиях Ethernet и Token Ring.

Сеть с разделяемой средой при большом количестве узлов будет работать всегда медленнее, чем аналогичная сеть с индивидуальными линиями связи, так как пропускная способность индивидуальной линии связи достается одному компьютеру, а при ее совместном использовании - делится на все компьютеры сети.

Основной принцип, положенный в основу Ethernet, - случайный метод доступа к разделяемой среде передачи данных. В качестве такой среды может использоваться толстый или тонкий коаксиальный кабель, витая пара, оптоволокно или радиоволны

В стандарте Ethernet строго зафиксирована топология электрических связей. Компьютеры подключаются к разделяемой среде в соответствии с типовой структурой «общая шина» (рис. 1.13). С помощью разделяемой во времени шины любые два компьютера могут обмениваться данными. Управление доступом к линии связи осуществляется специальными контроллерами - сетевыми адаптерами Ethernet. Каждый компьютер, а более точно, каждый сетевой адаптер, имеет уникальный адрес. Передача данных происходит со скоростью 10 Мбит/с. Эта величина является пропускной способностью сети Etherne

16. Локальные и глобальные сети. Основные характеристики и отличия. Структура крупных локальных и глобальных сетей.

Локальные сети - Local Area Networks (LAN) (или **Локальные вычислительные сети (ЛВС)**) - сети компьютеров, сосредоточенные на небольшой территории (обычно в радиусе не более 1-2 км) объединенные одним или несколькими высокоскоростными каналами передачи данных (порядка 100 Мбит/с),. в общем случае локальная сеть это коммуникационная система, принадлежащая одной организации.

Предоставляемые услуги отличаются широким разнообразием и обычно предусматривают реализацию в режиме on-line.

Глобальные сети (ГС) - Wide Area Networks (WAN) - объединяют территориально рассредоточенные компьютеры, которые могут находиться в различных городах и странах. В глобальных сетях часто используются уже существующие линии связи, (телефон – телеграф). Более низкие, чем в локальных сетях, скорости передачи данных (десятки килобит в секунду) ограничивают набор предоставляемых услуг передачей файлов, преимущественно не в оперативном, а в фоновом режиме, с использованием электронной почты. Для устойчивой передачи дискретных данных применяются более сложные методы и оборудование, чем в локальных сетях.

Отличия локальных сетей от глобальных (коротко) Подробно –см. на обороте

- Протяженность, качество и способ прокладки линий связи.
- Сложность методов передачи и оборудования.
- Скорость обмена данными. ЛС (10,16и100 Мбит/с) ГС (2400,9600,28800,33600 бит/с),
- Разнообразие услуг. ЛС – широкие, ГС — ограниченные (почта)
- Оперативность выполнения запросов. ЛС – неск. мсек, режим on-line ГС – неск. сек.
- Разделение каналов. В ЛС совместно сразу неск. узлами сети, а в ГС - индивидуально.
- Использование метода коммутации пакетов. В ЛС - применяется (неравн. нагрузка) В ГС – в осн. метод коммутации каналов,
- Масштабируемость. ЛС – плохая, ГС – хорошая.

Структура крупных локальных и глобальных сетей

Классификация по масштабу производственного подразделения, в пределах к-рого действует сеть:

- **сети отделов**, (небольшая группа сотрудников/ разделение локальных ресурсов)
- **сети кампусов** (мн-во сетей разл. отделов одного предприятия в пределах отдельного здания или в пределах одной территории)
- **корпоративные сети** объединяют большое количество компьютеров на всех территориях отд. предприятия. Они могут быть сложно связаны и покрывать город, регион или даже континент. Число пользователей и комп-ов может измеряться тысячами, а число серверов - сотнями, расстояния между сетями отдельных территорий могут оказаться такими, что необходимо использование глобальных связей.

Для соединения удаленных локальных сетей и отдельных компьютеров применяются разнообразные телекоммуникационные средства, в (телефонные каналы, радиоканалы, спутниковая связь). Корпоративную сеть можно представить в виде «островков локальных сетей», плавающих в телекоммуникационной среде

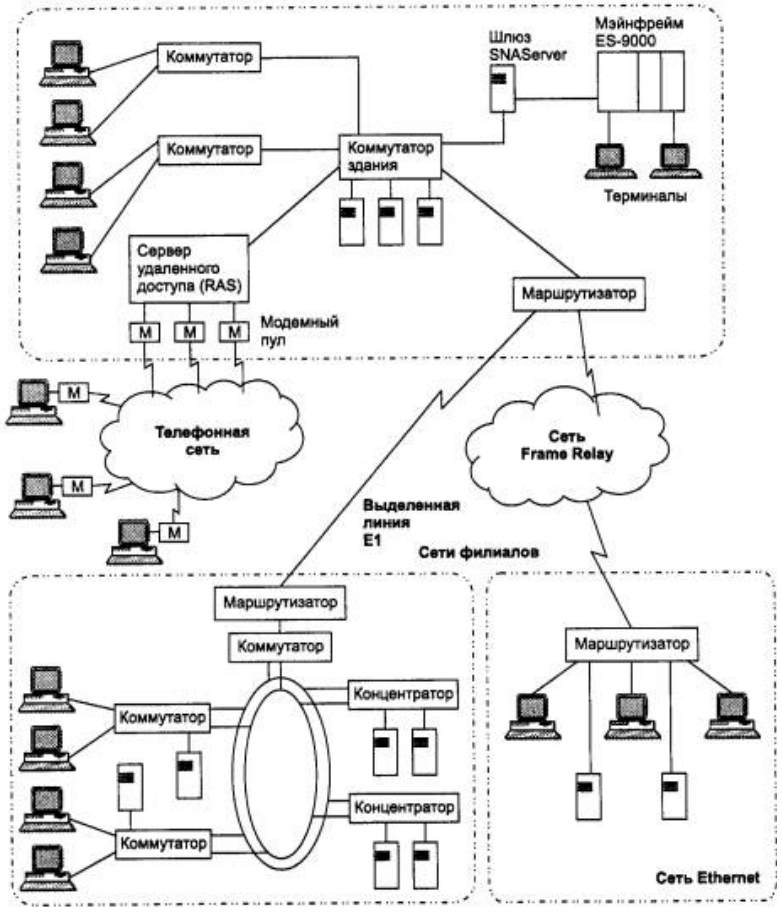


Рис. 1.33. Пример корпоративной сети

Для такой сложной и крупномасштабной сети как корпоративная сеть характерно:

- **масштабность** - тысячи пользовательских компьютеров, сотни серверов, огромные объемы хранимых и передаваемых по линиям связи данных, множество разнообразных приложений;
- **высокая степень гетерогенности** - типы компьютеров, коммуникационного оборудования, операционных систем и приложений различны;
- **использование глобальных связей** - сети филиалов соединяются с помощью телекоммуникационных средств, в том числе телефонных каналов, радиоканалов, спутниковой связи.

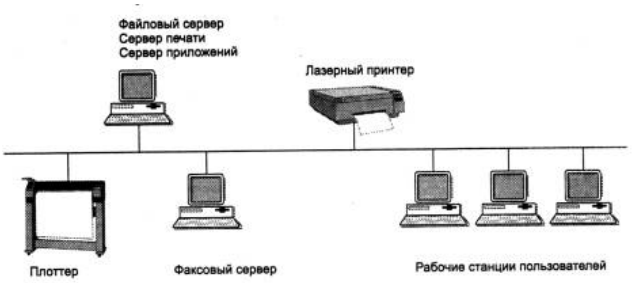


Рис. 1.31. Пример сети масштаба отдела

Отличия локальных сетей от глобальных (подробно)

- **Протяженность, качество и способ прокладки линий связи.** ЛВС отличается от ГС небольшим расстоянием между узлами сети. Это делает возможным использование в ЛВС качественных линий связи: коаксиального кабеля, витой пары, оптоволоконного кабеля, которые не всегда доступны (из-за экономических ограничений) на больших расстояниях, свойственных ГС, В ГС часто применяются уже существующие линии связи (телеграфные или телефонные), а в локальных сетях они прокладываются заново.
- **Сложность методов передачи и оборудования**. В условиях низкой надежности физ. каналов в ГС требуются более сложные, чем в ЛС, методы передачи данных и оборудование. Так, в ГС широко применяются модуляция, асинхронные методы, сложные методы контрольного суммирования, квитирование и повторные передачи искаженных кадров. С другой стороны, качественные линии связи в ЛС позволили упростить процедуры передачи данных за счет применения немодулированных сигналов и отказа от обязательного подтверждения получения пакета.
- **Скорость обмена данными.** Скорость высокоскоростных каналов ЛС (10,16и100 Мбит/с) сравнима со скоростями работы устройств и узлов компьютера - дисков, внутренних шин обмена данными и т. п. Для ГС типичны гораздо более низкие скорости передачи данных - 2400,9600,28800,33600 бит/с, 56 и 64 Кбит/с и только на магистральных каналах - до 2 Мбит/с.
- **Разнообразие услуг.** ЛС сети предоставляют широкий набор услуг - это различные виды услуг файловой службы, услуги печати, услуги службы передачи факсимильных сообщений, услуги баз данных, электронная почта и другие, в то время как ГС в основном предоставляют почтовые услуги и иногда файловые услуги с ограниченными возможностями - передачу файлов из публичных архивов удаленных серверов без предварительного просмотра их содержания.
- **Оперативность выполнения запросов.** Время прохождения пакета через ЛС обычно составляет несколько миллисекунд, время же его передачи через ГС может достигать нескольких секунд. Низкая скорость передачи данных в ГС затрудняет реализацию служб для режима on-line, который является обычным для ЛС.
- **Разделение каналов.** В ЛС каналы связи используются, как правило, совместно сразу несколькими узлами сети, а в ГС - индивидуально.
- **Использование метода коммутации пакетов**. Важной особенностью ЛС является неравномерное распределение нагрузки. Отношение пиковой нагрузки к средней может составлять 100:1 и даже выше. Такой трафик обычно называют пульсирующим. Из-за этого в ЛС для связи узлов применяется метод коммутации пакетов, который оказывается гораздо более эффективным, чем традиционный для глобальных сетей метод коммутации каналов. Эффективность метода коммутации пакетов состоит в том, что сеть в целом передает в единицу времени больше данных своих абонентов. В ГС метод коммутации пакетов также используется, но наряду с ним часто применяется и метод коммутации каналов, а также некоммутируемые каналы - как унаследованные технологии некомпьютерных сетей.
- **Масштабируемость.** «Классические» локальные сети обладают плохой масштабируемостью из-за жесткости базовых топологий, определяющих способ подключения станций и длину линии. При использовании многих базовых топологий характеристики сети резко ухудшаются при достижении определенного предела по количеству узлов или протяженности линий связи. Глобальным же сетям присуща хорошая масштабируемость, так как они изначально разрабатывались в расчете на работу с произвольными топологиями

17. Локальные сети на основе технологии Ethernet. Физический и канальный уровни. Основные характеристики и отличия. Различные реализации и их особенности.

При организации взаимодействия узлов в локальных сетях основная роль отводится классическим технологиям **Ethernet, Token Ring, FDDI**,

В начале 80-х **Ethernet** был стандартизован рабочей группой **IEEE 802.3**, и с тех пор он является международным стандартом.

Стандарты семейства **IEEE 802.X** охватывают только два нижних уровня семи-уровневой модели OSI - физический и канальный. Это связано с тем, что именно эти уровни в наибольшей степени отражают специфику локальных сетей.

Канальный уровень (Data Link Layer) делится в локальных сетях на два подуровня:

- логической передачи данных (Logical Link Control, **LLC**);
- управления доступом к среде (Media Access Control, **MAC**).

Уровень MAC появился из-за существования в локальных сетях разделяемой среды передачи данных. Именно этот уровень обеспечивает корректное совместное использование общей среды, предоставляя ее в соответствии с определенным алгоритмом в распоряжение той или иной станции сети. После того как доступ к среде получен, ею может пользоваться более высокий уровень - **уровень LLC**, организующий передачу логических единиц данных, кадров информации, с различным уровнем качества транспортных услуг.

Уровень LLC отвечает за передачу кадров данных между узлами с различной степенью надежности, а также реализует функции интерфейса с прилегающим к нему сетевым уровнем. Именно через уровень LLC сетевой протокол запрашивает у канального уровня нужную ему транспортную операцию с нужным качеством. На уровне LLC существует несколько режимов работы, отличающихся наличием или отсутствием на этом уровне процедур восстановления кадров в случае их потери или искажения, то есть отличающихся качеством транспортных услуг этого уровня.

Протоколы уровней MAC и LLC взаимно независимы - каждый протокол уровня MAC может применяться с любым протоколом уровня LLC, и наоборот.

протокол уровня MAC может применяться с любым протоколом уровня LLC, и наоборот.

Стандарты IEEE 802 имеют достаточно четкую структуру, приведенную на рис. 3.1:

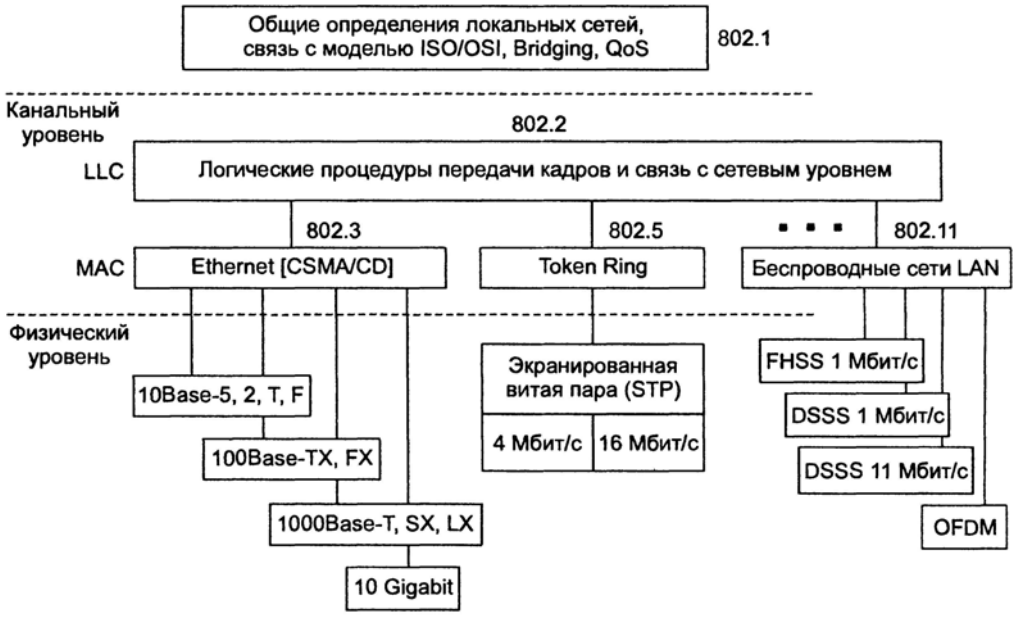
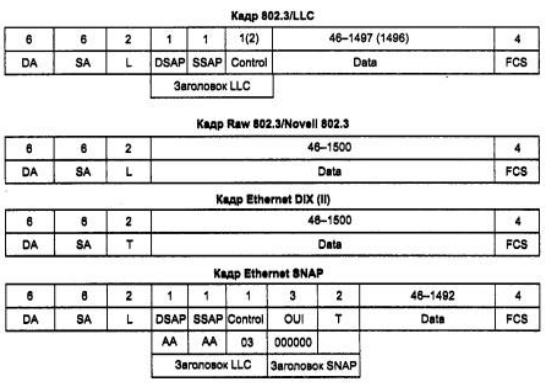


Рис. 3.1. Структура стандартов IEEE 802.X

Форматы кадров Ethernet (рис.)**:**

- кадр 802.3/LLC (кадр 802.3/802.2 или кадр Novell 802.2);
- кадр Raw 802.3 (или кадр Novell 802.3);
- кадр Ethernet DIX (или кадр Ethernet II);
- кадр Ethernet SNAP.



Параметры уровня **MAC** Ethernet

Параметры	Значения
Битовая скорость	10 Мбит/с
Интервал отсрочки	512 битовых интервала
Межкадровый интервал (IPG)	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 байт
Минимальная длина кадра (без преамбулы)	64 байт (512 бит)
Длина преамбулы	64 бит
Минимальная длина случайной паузы после коллизии	0 битовых интервалов
Максимальная длина случайной паузы после коллизии	524 000 битовых интервала
Максимальное расстояние между станциями сети	2500 м
Максимальное число станций в сети	1024

Физические спецификации технологии Ethernet на сегодняшний день включают следующие среды передачи данных.

- **l0Base-5** - коаксиальный кабель диаметром 0,5 дюйма, называемый «толстым» коаксиалом. Имеет волновое сопротивление 50 Ом. Максимальная длина сегмента - 500 метров (без повторителей).
- **l0Base-2** - коаксиальный кабель диаметром 0,25 дюйма, называемый «тонким» коаксиалом. Имеет волновое сопротивление 50 Ом. Максимальная длина сегмента - 185 метров (без повторителей).
- **l0Base-T** - кабель на основе неэкранированной витой пары (Unshielded Twisted Pair, UTP). Образует звездообразную топологию на основе концентратора. Расстояние между концентратором и конечным узлом - не более 100 м.
- **l0Base-F** - волоконно-оптический кабель. Топология аналогична топологии стандарта l0Base-T. Имеется несколько вариантов этой спецификации - FOIRL (расстояние до 1000 м), l0Base-FL (расстояние до 2000 м), l0Base-FB (расстояние до 2000 м).

Число 10 в указанных выше названиях обозначает битовую скорость передачи данных этих стандартов - 10 Мбит/с, а слово Base - метод передачи на одной базовой частоте 10 МГц (в отличие от методов, использующих несколько несущих частот, которые называются Broadband - широкополосными). Последний символ в названии стандарта физического уровня обозначает тип кабеля.

Параметры спецификаций **физического уровня для стандарта Ethernet**

	10Base-5	10Base-2	10Base-T	10Base-F
Кабель	Толстый коаксиальный кабель RG-8 или RG-11	Тонкий коаксиальный кабель RG-58	Неэкраниро-ванная витая пара категорий 3, 4, 5	Многомодовый волоконно-оптический кабель
Максимальная длина сегмента, м	500	185	100	2000
Максимальное расстояние между узлами сети (при использо-вании повторителей), м	2500	925	500	2500 (2740 для 10Base-FB)
Максимальное число станций в сегменте	100	30	1024	1024
Максимальное число повторителей между любыми станциями сети	4	4	4	4 (5 для 10 Base-FB)

18. Коммутируемые сети Ethernet. Концепции коммутации и бриджинга, различные типы коммутаторов и мостов.

Технология Ethernet наиболее чувствительна к перегрузкам разделяемого сегмента . Ограничения, возникающие из-за использования общей разделяемой среды, можно преодолеть, разделив сеть на несколько разделяемых сред и соединив отдельные сегменты сети такими устройствами, как мосты, коммутаторы или маршрутизаторы

Сеть, разделенная на логические сегменты, обладает более высокой производительностью и надежностью. Взаимодействие между логическими сегментами организуется с помощью мостов и коммутаторов.

Сеть можно разделить на логические сегменты с помощью устройств двух типов - мостов (bridge) и/или коммутаторов (switch, switching hub).

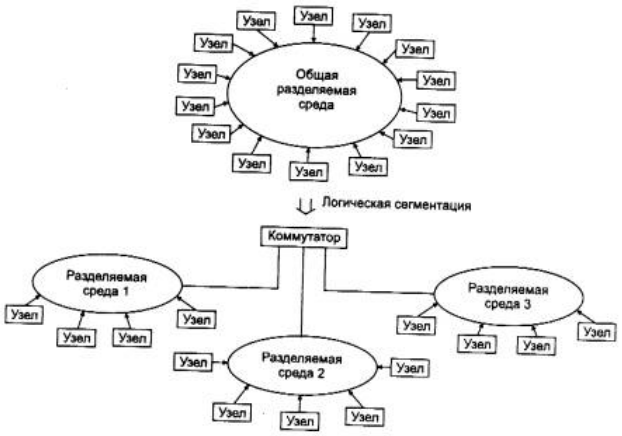
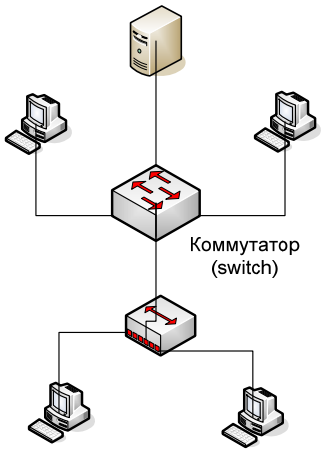


Рис. 4.16. Логическая структуризация сети

Коммутатор ЛВС (switch) – многопортовое устройство-мост, каждый порт которого связан со своим сегментом сети.

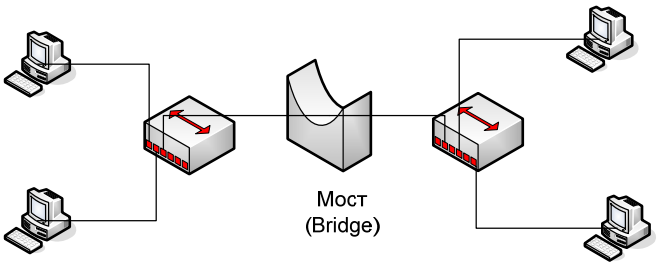
- Внешне похож на концентратор, но в отличие от последнего коммутатор направляет входящий трафик на один порт, необходимый для достижения места назначения.
- Коммутатор функционирует на 2 уровне модели OSI, поддерживая различные протоколы сетевого уровня



Мост (bridge) – устройство, используемое для объединения сегментов кабеля ЛВС, но в отличие от концентраторов функционирующее на физическом и канальном уровнях.

- Мост позволяет осуществлять фильтрацию передаваемых пакетов по физическому адресу. Мост не изменяет содержимое кадров и не учитывает данные протоколов сетевого и более высокого уровней.

Тем не менее мост и коммутатор - это функциональные близнецы. Оба эти устройства продвигают кадры на основании одних и тех же алгоритмов. Мосты и коммутаторы используют два типа алгоритмов: алгоритм прозрачного моста (transparent bridge), описанного в стандарте IEEE 802. ID, либо алгоритм моста с маршрутизацией от источника (source routing bridge) компании IBM для сетей Token Ring.



Выводы

- Для логической структуризации сети применяются мосты и их современные преемники - коммутаторы и маршрутизаторы. Первые два типа устройств позволяют разделить сеть на логические сегменты с помощью минимума средств - только на основе протоколов канального уровня. Кроме того, эти устройства не требуют конфигурирования.
- 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.
- 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.

Технология коммутации сегментов Ethernet была предложена фирмой Kalpana в 1990 году в ответ на растущие потребности

Структурная схема **коммутатора EtherSwitch**, предложенного фирмой Kalpana, представлена на рис. 4.23.

Каждый из 8 портов 10Base-T обслуживается одним процессором пакетов Ethernet - EPP (Ethernet Packet Processor). Кроме того, коммутатор имеет системный модуль, который координирует работу всех процессоров EPP. Системный модуль ведет общую адресную таблицу коммутатора и обеспечивает управление коммутатором по протоколу SNMP. Для передачи кадров между портами используется коммутационная матрица, подобная тем, которые работают в телефонных коммутаторах или мультипроцессорных компьютерах, соединяя несколько процессоров с несколькими модулями памяти.

Коммутационная матрица работает по принципу коммутации каналов. Для 8 портов матрица может обеспечить 8 одновременных внутренних каналов при полудуплексном режиме работы портов и 16 - при полнодуплексном, когда передатчик и приемник каждого порта работают независимо друг от друга.

Рис. 4.23. Структура коммутатора EtherSwitch компании Ka1pana

Прозрачные мосты незаметны для сетевых адаптеров конечных узлов, так как они самостоятельно строят специальную адресную таблицу, на основании которой можно решить, нужно передавать пришедший кадр в какой-либо другой сегмент или нет. Сетевые адаптеры при использовании прозрачных мостов работают точно так же, как и в случае их отсутствия, то есть не предпринимают никаких дополнительных действий, чтобы кадр прошел через мост. Алгоритм прозрачного моста не зависит от технологии локальной сети, в которой устанавливается мост, поэтому прозрачные мосты Ethernet работают точно так же, как прозрачные мосты FDDI.

Мосты с маршрутизацией от источника применяются для соединения колец Token Ring и FDDI, хотя для этих же целей могут использоваться и прозрачные мосты. Маршрутизация от источника (Source Routing, SR) основана на том, что станция-отправитель помещает в посылаемый в другое кольцо кадр всю адресную информацию о промежуточных мостах и кольцах, которые должен пройти кадр перед тем, как попасть в кольцо, к которому подключена станция-получатель. Хотя в название этого способа входит термин «маршрутизация», настоящей маршрутизации в строгом понимании этого термина здесь нет, так как мосты и станции по-прежнему используют для передачи кадров данных только информацию MAC - уровня, а заголовки сетевого уровня для мостов данного типа по-прежнему остаются неразличимой частью поля данных кадра.

19. Технологии, специфика адаптации технологии Ethernet к сетям доступа..

MetroEthernet это Metropolitan Area Network, **MAN** - сети мегаполисов

Стандарт 802.6 (Metropolitan Area Network – городские сети) описывает рекомендации для региональных сетей.

Из Олифера, глава 3

Сегодня комитет 802 включает следующий ряд подкомитетов, в который входят как уже упомянутые, так и некоторые другие:

- 802.1 - Internetworking - объединение сетей;
- 802.2 - Logical Link Control, LLC - управление логической передачей данных;
- 802.3 - Ethernet с методом доступа CSMA/CD;
- 802.4 - Token Bus LAN - локальные сети с методом доступа Token Bus;
- 802.5 - Token Ring LAN - локальные сети с методом доступа Token Ring;
- 802.6 - **Metropolitan Area Network**, MAN - сети мегаполисов;
- 802.7 - Broadband Technical Advisory Group - техническая консультационная группа по широкополосной передаче;
- 802,8 - Fiber Optic Technical Advisory Group - техническая консультационная группа по волоконно-оптическим сетям;
- 802.9 - Integrated Voice and data Networks - интегрированные сети передачи голоса и данных;
- 802.10 - Network Security - сетевая безопасность;
- 802.11 - Wireless Networks - беспроводные сети;
- 802.12 - Demand Priority Access LAN, l00VG-AnyLAN - локальные сети с методом доступа по требованию с приоритетами.

Из Википедии

Коммутация IP-пакетов — технология, использующаяся для оптимизации работы маршрутизаторов при использовании неизменных или редко меняющихся маршрутов.

Суть технологии — обработка IP-пакета без участия центрального процессора маршрутизатора. Первый пакет заданного типа (адрес отправителя, получателя, порт получателя) обрабатывается процессором в полном объёме (с проверкой на ACL, обработкой таблицы маршрутизации, определение нужного интерфейса), все последующие аналогичные (те же адреса, порты) уже не обрабатываются процессором, а коммутируются, как в устройствах второго уровня (чаще всего с использованием аппаратных средств коммутации, вроде коммутационной матрицы).

Подобная технология позволяет существенно снизить нагрузку на процессор маршрутизатора и уменьшить задержку в прохождении пакета. Самым существенным недостатком этой технологии является проблема смены маршрута, которая обнаруживается не сразу после изменения. Так же подобная технология используется в коммутаторах с поддержкой маршрутизации (L3 коммутаторы).

Дальшейшим развитием идеи коммутации IP-пакетов является MPLS и **MetroEthernet**, подразумевающие отказ от маршрутизации и переход к коммутации данных внутри обслуживаемого периметра (обычно, трафика абонентов).

20. Локальные сети на основе технологии FDDI. Физический и канальный уровни. Основные характеристики и отличия. Различные реализации и их особенности.

Технология FDDI (Fiber Distributed Data Interface)- оптоволоконный интерфейс распределенных данных - это первая технология локальных сетей, в которой средой передачи данных является волоконно-оптический кабель.

Технология FDDI во многом основывается на технологии Token Ring, развивая и совершенствуя ее основные идеи. Разработчики технологии FDDI ставили перед собой в качестве наиболее приоритетных следующие цели:

- повысить битовую скорость передачи данных до 100 Мбит/с;
- повысить отказоустойчивость сети за счет стандартных процедур восстановления ее после отказов различного рода - повреждения кабеля, некорректной работы узла, концентратора, возникновения высокого уровня помех на линии и т. п.;
- максимально эффективно использовать потенциальную пропускную способность сети как для асинхронного, так и для синхронного (чувствительного к задержкам) трафиков.

Сеть FDDI строится на основе двух оптоволоконных колец, которые образуют основной и резервный пути передачи данных между узлами сети. Наличие двух колец - это основной способ повышения отказоустойчивости в сети FDDI, и узлы, которые хотят воспользоваться этим повышенным потенциалом надежности, должны быть подключены к обоим кольцам.

Канальный уровень технологии FDDI

Кольца в сетях FDDI рассматриваются как общая разделяемая среда передачи данных, поэтому для нее определен специальный метод доступа. Этот метод очень близок к методу доступа сетей Token Ring и также называется методом маркерного (или токенного) кольца - token ring.

Отличия метода доступа заключаются в том, что время удержания маркера в сети FDDI не является постоянной величиной, как в сети Token Ring. Это время зависит от загрузки кольца - при небольшой загрузке оно увеличивается, а при больших перегрузках может уменьшаться до нуля. Эти изменения в методе доступа касаются только асинхронного трафика, который не критичен к небольшим задержкам передачи кадров. Для синхронного трафика время удержания маркера по-прежнему остается фиксированной величиной. Механизм приоритетов кадров, аналогичный принятому в технологии Token Ring, в технологии FDDI отсутствует.

Как и во многих других технологиях локальных сетей, в технологии FDDI используется протокол подуровня управления каналом данных LLC, определенный в стандарте IEEE 802.2. Таким образом, несмотря на то что технология FDDI была разработана и стандартизована институтом ANSI, а не комитетом IEEE, она полностью вписывается в структуру стандартов 802.

Особенности метода доступа FDDI

Для передачи синхронных кадров станция всегда имеет право захватить маркер при его поступлении. При этом время удержания маркера имеет заранее заданную фиксированную величину.

Для обеспечения отказоустойчивости в стандарте FDDI предусмотрено создание двух оптоволоконных колец - первичного и вторичного. В стандарте FDDI допускаются два вида подсоединения станций к сети. Одновременное подключение к первичному и вторичному кольцам называется двойным подключением - Dual Attachment, DA. Подключение только к первичному кольцу называется одиночным подключением - Single Attachment, SA.

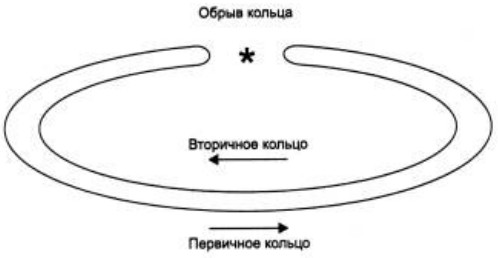


Рис. 3.16. Реконфигурация колец FDDI при отказе

Физический уровень технологии FDDI

В технологии FDDI для передачи световых сигналов по оптическим волокнам реализовано логическое кодирование 4B/5B в сочетании с физическим кодированием NRZI. Эта схема приводит к передаче по линии связи сигналов с тактовой частотой 125 МГц.

Физический уровень разделен на два подуровня: независимый от среды подуровень PHY (Physical) и зависящий от среды подуровень PMD (Physical Media Dependent)

Характеристики технологий FDDI, Ethernet, Token Ring

Характеристика	FDDI	Ethernet	Token Ring
Битовая скорость	100 Мбит/с	10 Мбит/с	16 Мбит/с
Топология	Двойное кольцо деревьев	Шина/звезда	Звезда/кольцо
Метод доступа	Доля от времени оборота маркера	CSMA/CD	Приоритетная система резервирования
Среда передачи данных	Оптоволокно, неэкранированная витая пара категории 5	Толстый коаксиал, тонкий коаксиал, витая пара категории 3, оптоволокно	Экранированная и неэкранированная витая пара, оптоволокно
Максимальная длина сети (без мостов)	200 км (100 км на кольцо)	2500 м	4000 м
Максимальное расстояние между узлами	2 км (не больше 11 дБ потерь между узлами)	2500 м	100 м
Максимальное количество узлов	500 (1000 соединений)	1024	260 для экранированной витой пары, 72 для неэкранированной витой пары
Тактирование и восстановление после отказов	Распределенная реализация тактирования и восстановления после отказов	Не определены	Активный монитор

Выводы

- Технология FDDI является наиболее отказоустойчивой технологией локальных сетей. При однократных отказах кабельной системы или станции сеть, за счет «сворачивания» двойного кольца в одинарное, остается вполне работоспособной.
- Маркерный метод доступа FDDI работает по-разному для синхронных и асинхронных кадров (тип кадра определяет станция). Для передачи синхронного кадра станция всегда может захватить пришедший маркер на фиксированное время. Для передачи асинхронного кадра станция может захватить маркер только в том случае, когда маркер выполнил оборот по кольцу достаточно быстро, что говорит об отсутствии перегрузок кольца. Такой метод доступа, во-первых, отдает предпочтение синхронным кадрам, а во-вторых, регулирует загрузку кольца, притормаживая передачу несрочных асинхронных кадров.
- В качестве физической среды технология FDDI использует волоконно-оптические кабели и UTP категории 5 (этот вариант физического уровня называется TP-PMD).
- Максимальное количество станций двойного подключения в кольце - 500, максимальный диаметр двойного кольца - 100 км. Максимальные расстояния между соседними узлами для многомодового кабеля равны 2 км, для витой пары UPT категории 5-100 м, а для одномодового оптоволокна зависят от его качества

21. Локальные сети на основе технологии Token Ring. Физический и канальный уровни. Основные характеристики и отличия. Различные реализации и их особенности..

Сети Token Ring, так же как и сети Ethernet, характеризует разделяемая среда передачи данных, которая в данном случае состоит из отрезков кабеля, соединяющих все станции сети в кольцо. Кольцо рассматривается как общий разделяемый ресурс, и для доступа к нему требуется не случайный алгоритм, как в сетях Ethernet, а детерминированный, основанный на передаче станциям права на использование кольца в определенном порядке. Это право передается с помощью кадра специального формата, называемого маркером или токеном (token).

Технология Token Ring был разработана компанией IBM в 1984 году, а затем передана в качестве проекта стандарта в комитет IEEE 802, который на ее основе принял в 1985 году стандарт 802.5. Компания IBM использует технологию Token Ring в качестве своей основной сетевой технологии

Сети Token Ring работают с двумя битовыми скоростями - 4 и 16 Мбит/с. Смешение станций, работающих на различных скоростях, в одном кольце не допускается. Сети Token Ring, работающие со скоростью 16 Мбит/с, имеют некоторые усовершенствования в алгоритме доступа по сравнению со стандартом 4 Мбит/с.

Технология Token Ring является более сложной технологией, чем Ethernet. Она обладает свойствами отказоустойчивости. В сети Token Ring определены процедуры контроля работы сети, которые используют обратную связь кольцеобразной структуры - посланный кадр всегда возвращается в станцию - отправитель. В некоторых случаях обнаруженные ошибки в работе сети устраняются автоматически, например может быть восстановлен потерянный маркер. В других случаях ошибки только фиксируются, а их устранение выполняется вручную обслуживающим персоналом.

В сетях с **маркерным методом доступа** (а к ним, кроме сетей Token Ring, относятся сети FDDI, а также сети, близкие к стандарту 802.4, - ArcNet, сети производственного назначения MAP) право на доступ к среде передается циклически от станции к станции по логическому кольцу.

Для контроля сети одна из станций выполняет роль так называемого активного монитора. Активный монитор выбирается во время инициализации кольца как станция с максимальным значением MAC-адреса, Если активный монитор выходит из строя, процедура инициализации кольца повторяется и выбирается новый активный монитор. Чтобы сеть могла обнаружить отказ активного монитора, последний в работоспособном состоянии каждые 3 секунды генерирует специальный кадр своего присутствия. Если этот кадр не появляется в сети более 7 секунд, то остальные станции сети начинают процедуру выборов нового активного монитора.

В сети Token Ring кольцо образуется отрезками кабеля, соединяющими соседние станции. Таким образом, каждая станция связана со своей предшествующей и последующей станцией и может непосредственно обмениваться данными только с ними. Для обеспечения доступа станций к физической среде по кольцу циркулирует кадр специального формата и назначения - **маркер**. В сети Token Ring любая станция всегда непосредственно получает данные только от одной станции - той, которая является предыдущей в кольце. Такая станция называется ближайшим активным соседом, расположенным выше по потоку (данных) - Nearest Active Upstream Neighbor, NAUN. Передачу же данных станция всегда осуществляет своему ближайшему соседу вниз по потоку данных.

Получив маркер, станция анализирует его и при отсутствии у нее данных для передачи обеспечивает его продвижение к следующей станции. Станция, которая имеет данные для передачи, при получении маркера изымает его из кольца, что дает ей право доступа к физической среде и передачи своих данных. Затем эта станция выдает в кольцо кадр данных установленного формата последовательно по битам. Переданные данные проходят по кольцу всегда в одном направлении от одной станции к другой. Кадр снабжен адресом назначения и адресом источника.

В Token Ring существуют три различных формата кадров:

- маркер;
- кадр данных;
- прерывающая последовательность.

Физический уровень технологии Token Rin

Стандарт Token Ring фирмы IBM изначально предусматривал построение связей в сети с помощью концентраторов, называемых MAU (Multistation Access Unit) или MSAU (Multi-Station Access Unit), то есть устройствами многостанционного доступа (рис. 3.15). Сеть Token Ring может включать до 260 узлов.

Концентратор Token Ring может быть активным или пассивным. Пассивный концентратор просто соединяет порты внутренними связями так, чтобы станции, подключаемые к этим портам, образовали кольцо.

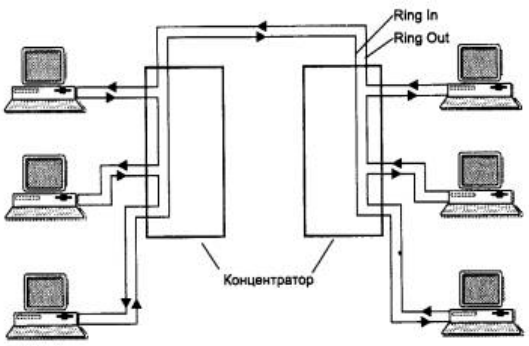


Рис. 3.15. Физическая конфигурация сети Token Ring

Активный концентратор выполняет функции регенерации сигналов и поэтому иногда называется повторителем, как в стандарте Ethernet.

В общем случае сеть Token Ring имеет комбинированную звездно-кольцевую конфигурацию. Конечные узлы подключаются к MSAU по топологии звезды, а сами MSAU объединяются через специальные порты Ring In (RI) и Ring Out (RO) для образования магистрального физического кольца.

Все станции в кольце должны работать на одной скорости - либо 4 Мбит/с, либо 16 Мбит/с. Кабели, соединяющие станцию с концентратором, называются ответвительными (lobe cable), а кабели, соединяющие концентраторы, - магистральными (trunk cable).

Технология Token Ring позволяет использовать для соединения конечных станций и концентраторов различные типы кабеля: STP Type I, UTP Type 3, UTP Type 6, а также волоконно-оптический кабель.

При использовании экранированной витой пары STP Type 1 из номенклатуры кабельной системы IBM в кольцо допускается объединять до 260 станций при длине ответвительных кабелей до 100 метров, а при использовании неэкранированной витой пары максимальное количество станций сокращается до 72 при длине ответвительных кабелей до 45 метров.

Расстояние между пассивными MSAU может достигать 100 м при использовании кабеля STP Type 1 и 45 м при использовании кабеля UTP Type 3. Между активными MSAU максимальное расстояние увеличивается соответственно до 730 м или 365 м в зависимости от типа кабеля.

Максимальная длина кольца Token Ring составляет 4000 м.

Выводы

- Технология Token Ring развивается в основном компанией IBM и имеет также статус стандарта IEEE 802.5, который отражает наиболее важные усовершенствования, вносимые в технологию IBM.
- В сетях Token Ring используется маркерный метод доступа, который гарантирует каждой станции получение доступа к разделяемому кольцу в течение времени оборота маркера. Из-за этого свойства этот метод иногда называют детерминированным.
- Метод доступа основан на приоритетах: от 0 (низший) до 7 (высший). Станция сама определяет приоритет текущего кадра и может захватить кольцо только в том случае, когда в кольце нет более приоритетных кадров.
- Сети Token Ring работают на двух скоростях: 4 и 16 Мбит/с и могут использовать в качестве физической среды экранированную витую пару, неэкранированную витую пару, а также волоконно-оптический кабель. Максимальное количество станций в кольце - 260, а максимальная длина кольца - 4 км.
- Технология Token Ring обладает элементами отказоустойчивости. За счет обратной связи кольца одна из станций - активный монитор - непрерывно контролирует наличие маркера, а также время оборота маркера и кадров данных. При некорректной работе кольца запускается процедура его повторной инициализации, а если она не помогает, то для локализации неисправного участка кабеля или неисправной станции используется процедура beaconing.
- Максимальный размер поля данных кадра Token Ring зависит от скорости работы кольца. Для скорости 4 Мбит/с он равен около 5000 байт, а при скорости 16 Мбит/с - около 16 Кбайт. Минимальный размер поля данных кадра не определен, то есть может быть равен 0.
  • В сети Token Ring станции в кольцо объединяют с помощью концентраторов, называемых MSAU. Пассивный концентратор MSAU выполняет роль кроссовой панели, которая соединяет выход предыдущей станции в кольце со входом последующей. Максимальное расстояние от станции до MSAU - 100 м для STP и 45 м для UTP.
- Активный монитор выполняет в кольце также роль повторителя - он ресинхронизирует сигналы, проходящие по кольцу.
- Кольцо может быть построено на основе активного концентратора MSAU, который в этом случае называют повторителем.
- Сеть Token Ring может строиться на основе нескольких колец, разделенных мостами, маршрутизирующими кадры по принципу «от источника», для чего в кадр Token Ring добавляется специальное поле с маршрутом прохождения колец.

В сетях с МД. Право передачи имеет сетевое устройство, владеющее специальным сообщением (маркером). Пример: FDDI, Token Ring.

Билет №21

Token Ring. Все станции сети объединены в кольцо, отрезками кабеля (витая пара, оптоволокно). Кольцо рассматривается как общий разделяемый ресурс. Право на использование кольца передается с помощью кадра спец.формата (маркер, токен). Любая станция в TR всегда получает данные от ближайшего активного соседа (станции, расположенной выше по потоку данных) и передает своему ближайшему соседу вниз по потоку данных. Станция которая имеет данные для передачи при получении маркера изымает его из кольца и выдает в кольцо кадр данных. Кадр данных снабжен адресом источника и адресом назначения и флагом подтверждения приема. Далее кадр идет по сети. И если он проходит ч/з станцию назначения, то она выставляет флаг подтверждения приема и отправляет кадр далее. Когда кадр возвращается в к станции источнику она проверяет флаг, изымает кадр из кольца и формирует новый маркер. Время владения кольцом ограничивается временем удержания маркера, после истечения которого станция обязана прекратить передачу данных и передать маркер далее по кольцу. TR работают с 2-мя битовыми скоростями – 4 и 16 Мб/с Работа станций на разных скоростях не допускается. В TR 16Мб/с также используется алгоритм раннего освобожденияя маркера: станция передает маркер не дожидаясь возвращения по кольцу кадра с битом подтверждения приема. Одна станция обозначается как активный монитор, она осуществляет управление тайм-аутом в кольце, порождает новые маркеры, генерирует диагностические кадры. Если монитор отказал, то среди станций выбирается новый монитор.

Билет №20

FDDI. Основывается на TR. Строится на основе двух оптоволоконных колец (основное и резервное). В нормальном режиме данные проходят ч/з все участки первичного (Primary) кольца. В случае отказа первичное кольцо объединяется со вторичным, образуя вновь единое кольцо. Этот режим работы называется Wrap (свертывание). Свертывание производится силами концентраторов или сетевых адаптеров. Для упрощения этой процедуры, данные в первичном кольце передаются против часовой стрелки, а по вторичному - против. Скорость передачи составляет до 100Мб/с.

+ 1.Обладает элементами отказоустойчивости
+ 2. Отсутствие коллизий.
– 1. Высокая стоимость оборудования
– 2. Сложность построения больших сете

22. Глобальные сети связи. Различные типы глобальных сетей, особенности и характеристики

Глобальные сети (Wide Area Networks, WAN), которые также называют территориальными компьютерными сетями, служат для того, чтобы предоставлять свои сервисы большому количеству конечных абонентов, разбросанных по большой территории - в пределах области, региона, страны, континента или всего земного шара. Ввиду большой протяженности каналов связи построение глобальной сети требует очень больших затрат, в которые входит стоимость кабелей и работ по их прокладке, затраты на коммутационное оборудование и промежуточную усилительную аппаратуру, обеспечивающую необходимую полосу пропускания канала, а также эксплуатационные затраты на постоянное поддержание в работоспособном состоянии разбросанной по большой территории аппаратуры сети.

Рис. 6.1. Абоненты глобальной сети

Типы глобальных сетей

Принято различать корпоративные сети, построенные с использованием:

- выделенных каналов;
- коммутации каналов;
- коммутации пакетов.

Выделенные каналы

Выделенные (или арендуемые - leased) каналы можно получить у телекоммуникационных компаний, которые владеют каналами дальней связи (таких, например, как «РОСТЕЛЕКОМ»), или от телефонных компаний, которые обычно сдают в аренду каналы в пределах города или региона.

Использовать выделенные линии можно двумя способами.

- Построение с их помощью территориальной сети определенной технологии, например frame relay, в которой арендуемые выделенные линии служат для соединения промежуточных, территориально распределенных коммутаторов пакетов, как в случае, приведенном на рис. 6.2.
- Соединение выделенными линиями только объединяемых локальных сетей или конечных абонентов другого типа, например мэйнфреймов, без установки транзитных коммутаторов пакетов, работающих по технологии глобальной сети

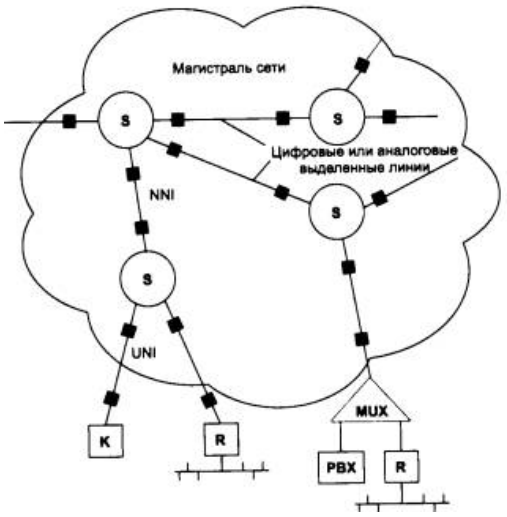


Рис. 6.2. Пример структуры глобальной сети

Глобальные сети с коммутацией каналов двух типов

- традиционные аналоговые телефонные сети (АТС)
- цифровые сети с интеграцией услуг ISDN. Достоинством сетей с коммутацией каналов является их распространенность, что характерно особенно для аналоговых телефонных сетей..

Недостаток АТС — низкое качество составного канала из-за использования телефонных коммутаторов устаревших моделей, работающих по принципу частотного уплотнения каналов (FDM-технологии). На такие коммутаторы сильно воздействуют внешние помехи (например, грозовые разряды или работающие электродвигатели), которые трудно отличить от полезного сигнала. Правда, в аналоговых телефонных сетях все чаще используются цифровые АТС, которые между собой передают голос в цифровой форме. Аналоговым в таких сетях остается только абонентское окончание. Чем больше цифровых АТС в телефонной сети, тем выше качество канала

Глобальные сети с коммутацией пакетов (технологии: X.25, frame relay, SMDS и ATM)

Кроме этих технологий, можно воспользоваться услугами территориальных сетей TCP/IP, которые доступны сегодня как в виде недорогой и очень распространенной сети Internet, качество транспортных услуг которой оставляет желать лучшего, так и в виде коммерческих глобальных сетей TCP/IP, изолированных от Internet и предоставляемых в аренду телекоммуникационными компаниями.

Характеристики сетей с коммутацией пакетов

Тип сети	Скорость доступа	Трафик	Примечания
X.25	1,2–64 Кбит/с	Терминальный	Большая избыточность протоколов, хорошо работают на каналах низкого качества
Frame Relay	от 64 Кбит/с до 2 Мбит/с	Компьютерный	Сравнительно новые сети, хорошо передают пульсации трафика, в основном поддерживают службу постоянных виртуальных каналов
SMDS	1,544–45 Мбит/с	Компьютерный, графика, голос, видео	Сравнительно новые сети, распространены в крупных городах Америки, вытесняются сетями ATM
ATM	1,544–155 Мбит/с	Компьютерный, графика, голос, видео	Новые сети, коммерческая эксплуатация началась с 1996 года, пока используются в основном для передачи компьютерного трафика
TCP/IP	1,2–2,048 Кбит/с	Терминальный, компьютерный	Широко распространены в некоммерческом варианте — сети Internet, коммерческие услуги пока слабые

Магистральные сети и сети доступа

Целесообразно делить территориальные сети, используемые для построения корпоративной сети, на две большие категории:

- магистральные сети;
- сети доступа.

Магистральные территориальные сети (backbone wide-area networks) используются для образования одноранговых связей между крупными локальными сетями, принадлежащими большим подразделениям предприятия. Магистральные территориальные сети должны обеспечивать высокую пропускную способность, так как на магистрали объединяются потоки большого количества подсетей. Кроме того, магистральные сети должны быть постоянно доступны,.

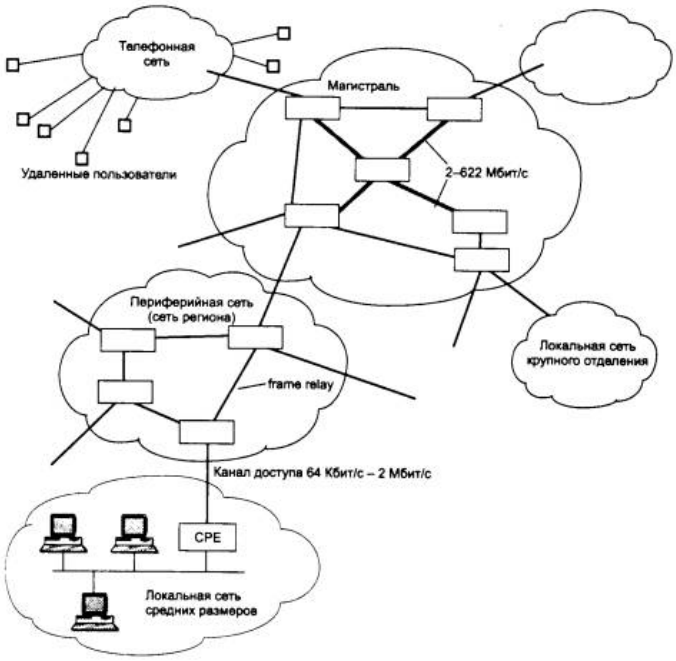


Рис. 6.5. Структура глобальной сети предприятия

Обычно в качестве магистральных сетей используются цифровые выделенные каналы со скоростями от 2 до 622 Мбит/с, по которым передается трафик IP, IPX или протоколов архитектуры SNA компании IBM, сети с коммутацией пакетов frame relay, ATM, X.25 или TCP/IP. При наличии выделенных каналов для обеспечения высокой готовности магистрали используется смешанная избыточная топология связей, как это показано на рис. 6.5.

Под **сетями доступа** понимаются территориальные сети, необходимые для связи небольших локальных сетей и отдельных удаленных компьютеров с центральной локальной сетью предприятия. Если организации магистральных связей при создании корпоративной сети всегда уделялось большое внимание, то организация удаленного доступа сотрудников предприятия перешла в разряд стратегически важных вопросов только в последнее время. Быстрый доступ к корпоративной информации из любой географической точки определяет для многих видов деятельности предприятия качество принятия решений его сотрудниками. Важность этого фактора растет с увеличением числа сотрудников, работающих на дому (telecommuters - телекоммьютеров), часто находящихся в командировках, и с ростом количества небольших филиалов предприятий, находящихся в различных городах и, может быть, разных странах.

Выводы к билету №22 (альтернативный ответ)

- Глобальные компьютерные сети (WAN) используются для объединения абонентов разных типов: отдельных компьютеров разных классов - от мэйнфреймов до персональных компьютеров, локальных компьютерных сетей, удаленных терминалов.
- Ввиду большой стоимости инфраструктуры глобальной сети существует острая потребность передачи по одной сети всех типов трафика, которые возникают на предприятии, а не только компьютерного: голосового трафика внутренней телефонной сети, работающей на офисных АТС (PBX), трафика факс-аппаратов, видеокамер, кассовых аппаратов, банкоматов и другого производственного оборудования.
- Для поддержки мультимедийных видов трафика создаются специальные технологии: ISDN, B-ISDN. Кроме того, технологии глобальных сетей, которые разрабатывались для передачи исключительно компьютерного трафика, в последнее время адаптируются для передачи голоса и изображения. Для этого пакеты, переносящие замеры голоса или данные изображения, приоритезируются, а в тех технологиях, которые это допускают, для их переноса создается соединение с заранее резервируемой пропускной способностью. Имеются специальные устройства доступа - мультиплексоры «голос - данные» или «видео - данные», которые упаковывают мультимедийную информацию в пакеты и отправляют ее по сети, а на приемном конце распаковывают и преобразуют в исходную форму - голос или видеоизображение.
- Глобальные сети предоставляют в основном транспортные услуги, транзитом перенося данные между локальными сетями или компьютерами. Существует нарастающая тенденция поддержки служб прикладного уровня для абонентов глобальной сети: распространение публично-доступной аудио-, видео- и текстовой информации, а также организация интерактивного взаимодействия абонентов сети в реальном масштабе времени. Эти службы появились в Internet и успешно переносятся в корпоративные сети, что называется технологией intranet.

- Все устройства, используемые для подключения абонентов к глобальной сети, делятся на два класса: DTE, собственно вырабатывающие данные, и DCE, служащие для передачи данных в соответствии с требованиями интерфейса глобального канала и завершающие канал.
- Технологии глобальных сетей определяют два типа интерфейса: «пользователь-сеть» (UNI) и «сеть-сеть» (NNI). Интерфейс UNI всегда глубоко детализирован для обеспечения подключения к сети оборудования доступа от разных производителей. Интерфейс NNI может быть детализирован не так подробно, так как взаимодействие крупных сетей может обеспечиваться на индивидуальной основе.
- Глобальные компьютерные сети работают на основе технологии коммутации пакетов, кадров и ячеек. Чаще всего глобальная компьютерная сеть принадлежит телекоммуникационной компании, которая предоставляет службы своей сети в аренду. При отсутствии такой сети в нужном регионе предприятия самостоятельно создают глобальные сети, арендуя выделенные или коммутируемые каналы у телекоммуникационных или телефонных компаний.
- На арендованных каналах можно построить сеть с промежуточной коммутацией на основе какой-либо технологии глобальной сети (X.25, frame relay, ATM) или же соединять арендованными каналами непосредственно маршрутизаторы или мосты локальных сетей. Выбор способа использования арендованных каналов зависит от количества и топологии связей между локальными сетями.
- Глобальные сети делятся на магистральные сети и сети доступа.

23. Сети на основе Frame Relay. Особенности технологии и ее расширения.

Коротко

Frame Relay предназначен для межсетевого общения, ориентирован на соединение и использует два протокольных уровня модели OSI. Остальные уровни должны реализоваться программно. Такая схема заметно удешевляет интерфейс. Сеть работает по технологии, которая передает кадры только по протоколу канального уровня LAP-F, кадры при передаче ч/з коммутатор не преобразуется. Протокол вводит понятие committed information rates (CIR - оговоренные скорости передачи), обеспечивая каждому приложению гарантированную полосу пропускания. Если приложение не использует полностью выделенную полосу, другие приложения могут поделить между собой свободный ресурс. Frame Relay гарантирует большее быстродействие, чем X.25. и синхронную передачу данных. Применение инкапсуляции гарантирует транспортировку пакетов других протоколов через сети Frame Relay. Особенностью Frame Relay является отказ от коррекции обнаруженных в кадрах искажений

***

Сети frame relay - сравнительно новые сети, которые гораздо лучше подходят для передачи пульсирующего трафика локальных сетей по сравнению с сетями X.25, правда, это преимущество проявляется только тогда, когда каналы связи приближаются по качеству к каналам локальных сетей, а для глобальных каналов такое качество обычно достижимо только при использовании волоконно-оптических кабелей.

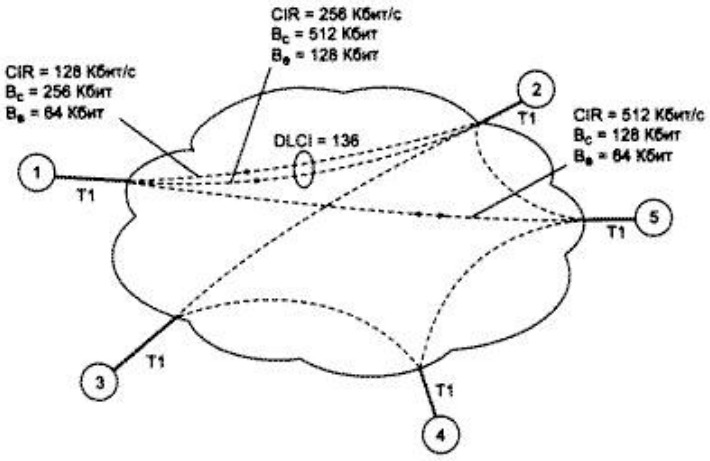


Рис. 6.28. Пример использования сети frame relay

Преимущество сетей frame relay заключается в их низкой протокольной избыточности и дейтаграммном режиме работы, что обеспечивает высокую пропускную способность и небольшие задержки кадров. Надежную передачу кадров технология frame relay не обеспечивает. Сети frame relay специально разрабатывались как общественные сети для соединения частных локальных сетей. Они обеспечивают скорость передачи данных до 2 Мбит/с.

Особенностью технологии frame relay является гарантированная поддержка основных показателей качества транспортного обслуживания локальных сетей - средней скорости передачи данных по виртуальному каналу при допустимых пульсациях трафика. Кроме технологии frame relay гарантии качества обслуживания на сегодня может предоставить только технология ATM, в то время как остальные технологии предоставляют требуемое качество обслуживания только в режиме «с максимальными усилиями» (best effort), то есть без гарантий.

Технология frame relay в сетях ISDN стандартизована как служба. В рекомендациях 1.122, вышедших в свет в 1988 году, эта служба входила в число дополнительных служб пакетного режима, но затем уже при пересмотре рекомендаций в 1992-93 гг. она была названа службой frame relay и вошла в число служб режима передачи кадров наряду со службой frame switching. Служба frame switching работает в режиме гарантированной доставки кадров с регулированием потока. На практике поставщики телекоммуникационных услуг предлагают только службу frame relay.

Технология frame relay сразу привлекла большое внимание ведущих телекоммуникационных компаний и организаций по стандартизации. В ее становлении и стандартизации помимо CCITT (ITU-T) активное участие принимают Frame Relay Forum и комитет T1S1 института ANSI.

Выводы к билету №23 (альтернативный ответ)

- Сети frame relay работают на основе весьма упрощенной, по сравнению с сетями X.25, технологией, которая передает кадры только по протоколу канального уровня - протоколу LAP-F. Кадры при передаче через коммутатор не подвергаются преобразованиям, из-за чего технология и получила свое название.
- Важной особенностью технологии frame relay является концепция резервирования пропускной способности при прокладке в сети виртуального канала. Сети frame relay создавались специально для передачи пульсирующего компьютерного трафика, поэтому при резервировании пропускной способности указывается средняя скорость трафика CIR и согласованный объем пульсаций Bc.
- Сеть frame relay гарантирует поддержку заказанных параметров качества обслуживания за счет предварительного расчета возможностей каждого коммутатора, а также отбрасывания кадров, которые нарушают соглашение о трафике, то есть посылаются в сеть слишком интенсивно.
- Большинство первых сетей frame relay поддерживали только службу постоянных виртуальных каналов, а служба коммутируемых виртуальных каналов стала применяться на практике только недавно.

24. Сети ISDN. Концепция сети с интеграцией услуг. Характеристики, применение к передаче голоса и данных.

ISDN (Integrated Services Digital Network - цифровые сети с интегральными услугами) относятся к сетям, в которых основным режимом коммутации является режим коммутации каналов, а данные обрабатываются в цифровой форме. (Идеи перехода телефонных сетей общего пользования на полностью цифровую обработку данных.

Архитектура сети ISDN предусматривает **несколько видов служб** (рис. 6.16):

- некоммутируемые средства (выделенные цифровые каналы);
- коммутируемая телефонная сеть общего пользования;
- сеть передачи данных с коммутацией каналов;
- сеть передачи данных с коммутацией пакетов;
- сеть передачи данных с трансляцией кадров (frame relay);
- средства контроля и управления работой сети.

Как видно из приведенного списка, транспортные службы сетей ISDN действительно покрывают **очень широкий спектр услуг**, включая популярные услуги frame relay. Кроме того, большое внимание уделено средствам контроля сети, которые позволяют маршрутизировать вызовы для установления соединения с абонентом сети, а также осуществлять мониторинг и управление сетью. Управляемость сети обеспечивается интеллектуальностью коммутаторов и конечных узлов сети, поддерживающих стек протоколов, в том числе и специальных протоколов управления.

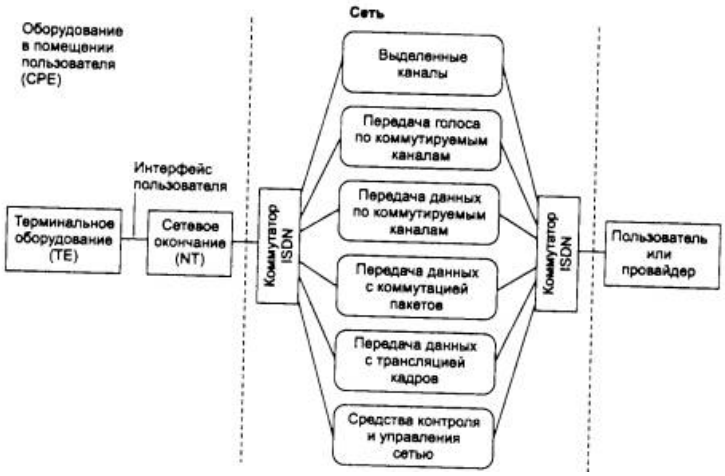


Рис. 6.16. Службы ISDN

Использование служб ISDN в корпоративных сетях

Несмотря на большие отличия от аналоговых телефонных сетей, сети ISDN сегодня используются в основном так же, как аналоговые телеф. сети, то есть как сети с коммутацией каналов, но только более скоростные: интерфейс BRI дает возможность установить дуплексный режим обмена со скоростью 128 Кбит/с (логическое объединение двух каналов типа B), а интерфейс PRI - 2,048 Мбит/с. Кроме того, качество цифровых каналов гораздо выше, чем аналоговых, а это значит, что процент искаженных кадров будет гораздо ниже и полезная скорость обмена данными существенно выше.

Пользовательский интерфейс основан на каналах трех типов:

- B-со скоростью передачи данных 64 Кбит/с;
- D - со скоростью передачи данных 16 или 64 Кбит/с;
- H - со скоростью передачи данных 384 Кбит/с (HO), 1536 Кбит/с (HИ) или 1920 Кбит/с (H12).

Выводы к билету №24 (альтернативный ответ)

- Сети с коммутацией каналов используются в корпоративных сетях в основном для удаленного доступа многочисленных домашних пользователей и гораздо реже - для соединения локальных сетей.
- Отличительными особенностями всех сетей с коммутацией каналов являются: работа в режиме установления соединений, возможность блокировки вызова конечным абонентом или промежуточным коммутатором, необходимость использования на обоих концах сети устройств, поддерживающих одну и ту же скорость передачи данных, так как этот вид сетей не выполняет промежуточную буферизацию данных.
- Сети с коммутацией каналов делятся на аналоговые и цифровые. Аналоговые сети могут использовать аналоговую (FDM) и цифровую (TDM) коммутацию, но в них всегда абонент подключен по аналоговому 2-проводному окончанию. В цифровых сетях мультиплексирование и коммутация всегда выполняются по способу коммутации TDM, а абоненты всегда подключаются по цифровому абонентскому окончанию (DSL).
- Аналоговые сети обеспечивают вызов посредством импульсного или тонового набора номера с частотой 10 Гц, причем тоновый набор примерно в 5 раз быстрее импульсного.
- Аналоговые сети используют электромеханические коммутаторы, создающие большие помехи, и электронные программно-управляемые коммутаторы. При работе электронного коммутатора в режиме частотного уплотнения (FDM) создаются дополнительные помехи при демультиплексировании и мультиплексировании абонентских каналов.
- Модемы для работы по коммутируемым аналоговым телефонным каналам должны поддерживать функцию автовызова удаленного абонента. При асинхронном интерфейсе модем использует для этого команды Hayes-совместимых модемов, а при синхронном интерфейсе - стандарт V.25 или V.25 bis.
- Основные стандарты модемов для коммутируемых каналов тональной частоты - это стандарты V.34+, V.90, V.42 и V.42 bis. Стандарт V.34+ является общим стандартом для работы по выделенным и коммутируемым каналам при 2-проводном окончании. Стандарт V.42 определяет протокол коррекции ошибок LAP-M из семейства HDLC, а стандарт VC.42 bis - метод компрессии данных при асинхронном интерфейсе. В синхронном интерфейсе для коррекции ошибок используется протокол HDLC, а для компрессии - фирменный протокол SDC компании Motorola.
- Стандарт V.90 полезен в том случае, когда между модемом пользователя и сервером удаленного доступа поставщика услуг все АТС обеспечивают цифровые методы коммутации, а сервер подключен по цифровому абонентскому окончанию. В этом случае скорость передачи данных от сервера к пользователю повышается до 56 Кбит/с за счет отсутствия аналогово-цифрового преобразования на этом направлении.
- Цифровые сети с коммутацией каналов представлены двумя технологиями:Switched 56 и ISDN.
- Switched 56 - это переходная технология, которая основана на предоставлении пользователю 4-проводного цифрового абонентского окончания T1/E1, но со скоростью 56 Кбит/с. Коммутаторы такой сети работают с использованием цифровой коммутации. Технология Switched 56 обеспечивает соединение компьютеров и локальных сетей со скоростью 56 Кбит/с.
- Цифровые сети с интегрированными услугами - ISDN - разработаны для объединения в одной сети различных транспортных и прикладных служб. ISDN предоставляет своим абонентам услуги выделенных каналов, коммутируемых каналов, а также коммутации пакетов и кадров (frame relay).
- Интерфейс UNI предоставляется пользователям ISDN в двух видах - BRI и PRI. Интерфейс BRI предназначен для массового пользователя и построен по схеме 2B+D. Интерфейс PRI имеет две разновидности - североамериканскую 23B+D и европейскую 30B+D.
- Каналы типа D образуют сеть с коммутацией пакетов, выполняющую двоякую роль в сети ISDN: во-первых, передачу запроса на установление коммутируемого канала типа B с другим абонентом сети, во-вторых, обмен пакетами X.25 с абонентами сети ISDN или внешней сети X.25, соединенной с сетью ISDN.
- Цифровое абонентское окончание DSL сети ISDN для интерфейса BRI представляет собой 2-проводной кабель с максимальной длиной 5,5 км.
- Построение глобальных связей на основе сетей ISDN в корпоративной сети ограничено в основном организацией удаленного доступа и объединением небольших локальных сетей на основании службы коммутации каналов. Служба коммутации пакетов по каналу типа D реализуется редко - это связано с его невысокой скоростью, которая обычно составляет не более 9600 бит/с. Поэтому сети ISDN используются так же, как и аналоговые телефонные сети, но только как более скоростные и надежные.

25. Сети X.25. Особенности и применение сетей X.25 в современном мире.

Коротко

X.25 первая крупномасштабная реализация сетей с коммутацией пакетов PSN. X.25 имели невысокие скорости передачи данных, кот. компенсируясь службами контроля ошибок на уровне сети и восстановл-ия. X.25 состоит из 4 компонентов: терминальн. оборудование (DTE) - устройство, кот. посылает и получает сетевые данные по сети пакетной коммутации, сборка/разборка пакетов (PAD), оконечное оборудование канала передачи данных (DCE) и пакетные коммутаторы (PSE).

Функции PAD:

- сборка символов, получаемых от асинхронных терминалов, в пакеты.
- разборка полей данных в пакетах и вывод данных на асинхр-е терминалы.
- управление процедурами установления соединения и разъединения по сети с нужным компом.
- передача символов, включающих старт-стопные сигналы и биты проверки на четность.
- продвижение пакетов при наличии соответст-х условий.

PAD используется для подключения кассовых аппаратов и банкоматов.

Технология X.25 имеет трехуровневый стек протоколов (физич., канальн., сетевой)

Протокол физ. уровня не оговорен, что дает возможность использовать каналы разных стандартов.

На канальном уровне используется протокол LAP-B (оба узла уч. в соединении равноправны).

Сетевой протокол X.25/3 выполняет функции маршрутизации пакетов, управления потоком пакетов.

Сеть состоит из коммутаторов соединенных высокоскоростными выделенными каналами.

***

Сети X.25 являются на сегодняшний день самыми распространенными сетями с коммутацией пакетов, используемыми для построения корпоративных сетей. Основная причина такой ситуации состоит в том, что долгое время сети X.25 были единственными доступными сетями с коммутацией пакетов коммерческого типа, в которых давались гарантии коэффициента готовности сети. Сеть Internet также имеет долгую историю существования, но как коммерческая сеть она начала эксплуатироваться совсем недавно, поэтому для корпоративных пользователей выбора не было. Кроме того, сети X.25 хорошо работают на ненадежных линиях благодаря протоколам с установлением соединения и коррекцией ошибок на двух уровнях - канальном и сетевом.

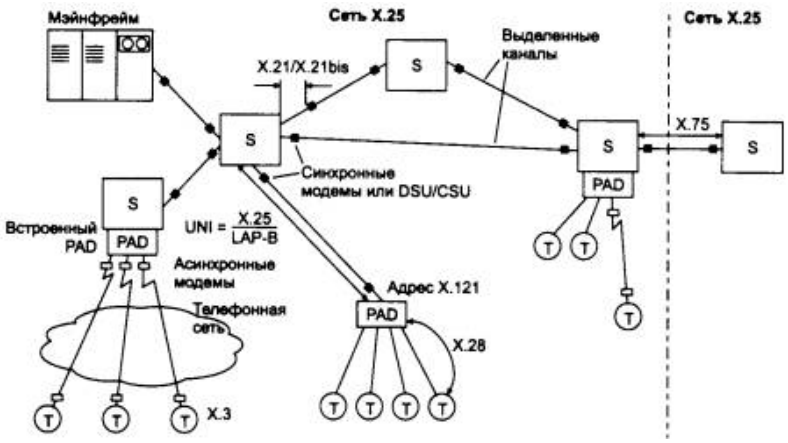


Рис. 6.22. Структура сети X.25

Технология сетей X.25 имеет несколько существенных признаков, отличающих ее от других технологий.

- Наличие в структуре сети специального устройства - PAD (Packet Assembler Disassembler), предназначенного для выполнения операции сборки нескольких низкоскоростных потоков байт от алфавитно-цифровых терминалов в пакеты, передаваемые по сети и направляемые компьютерам для обработки. Эти устройства имеют также русскоязычное название «Сборщик-разборщик пакетов», СРП.
- Наличие трехуровневого стека протоколов с использованием на канальном и сетевом уровнях протоколов с установлением соединения, управляющих потоками данных и исправляющих ошибки.
- Ориентация на однородные стеки транспортных протоколов во всех узлах сети - сетевой уровень рассчитан на работу только с одним протоколом канального уровня и не может подобно протоколу IP объединять разнородные сети. Сеть X.25 состоит из коммутаторов (Switches, S), называемых также центрами коммутации пакетов (ЦКП), расположенных в различных географических точках и соединенных высокоскоростными выделенными каналами (рис. 6.22). Выделенные каналы могут быть как цифровыми, так и аналоговыми.

Выводы к билету №25 (альтернативный ответ)

- Сети X.25 относятся к одной из наиболее старых и отработанных технологий глобальных сетей. Трехуровневый стек протоколов сетей X.25 хорошо работает на ненадежных зашумленных каналах связи, исправляя ошибки и управляя потоком данных на канальном и пакетном уровнях.
- Сети X.25 поддерживают групповое подключение к сети простых алфавитно-цифровых терминалов за счет включения в сеть специальных устройств PAD, каждое из которых представляет собой особый вид терминального сервера.
- На надежных волоконно-оптических каналах технология X.25 становится избыточной и неэффективной, так как значительная часть работы ее протоколов ведется «вхолостую».

Выводы

- К технологиям глобальных сетей с коммутацией пакетов относятся сети X.25, frame relay, SMDS, ATM и TCP/IP. Все эти сети, кроме сетей TCP/IP, используют маршрутизацию пакетов, основанную на виртуальных каналах между конечными узлами сети.
- Сети TCP/IP занимают особое положение среди технологий глобальных сетей, так как они выполняют роль технологии объединения сетей любых типов, в том числе и сетей всех остальных глобальных технологий. Таким образом, сети TCP/ IP относятся к более высокоуровневым технологиям, чем технологии собственно глобальных сетей.
- Техника виртуальных каналов заключается в разделении операций маршрутизации и коммутации пакетов. Первый пакет таких сетей содержит адрес вызываемого абонента и прокладывает виртуальный путь в сети, настраивая промежуточные коммутаторы. Остальные пакеты проходят по виртуальному каналу в режиме коммутации на основании номера виртуального канала, который является локальным адресом для каждого порта каждого коммутатора.
- Техника виртуальных каналов имеет преимущества и недостатки по сравнению с техникой маршрутизации каждого пакета, характерной для сетей IP или IPX. Преимуществами являются: ускоренная коммутация пакетов по номеру виртуального канала, а также сокращение адресной части пакета, а значит, и избыточности заголовка. К недостаткам следует отнести невозможность распараллеливания потока данных между двумя абонентами по параллельным путям, а также неэффективность установления виртуального пути для кратковременных потоков данных.
-
- Технология ATM является дальнейшим развитием идей предварительного резервирования пропускной способности виртуального канала, реализованных в технологии frame relay.
- Технология ATM поддерживает основные типы трафика, существующие у абонентов разного типа: трафик с постоянной битовой скоростью CBR, характерный для телефонных сетей и сетей передачи изображения, трафик с переменной битовой скоростью VBR, характерный для компьютерных сетей, а также для передачи компрессированного голоса и изображения.
- Для каждого типа трафика пользователь может заказать у сети значения нескольких параметров качества обслуживания - максимальной битовой скорости PCR, средней битовой скорости SCR, максимальной пульсации MBS, а также контроля временных соотношений между передатчиком и приемником, важных для трафика, чувствительного к задержкам.
- Технология ATM сама не определяет новые стандарты для физического уровня, а пользуется существующими. Основным стандартом для ATM является физический уровень каналов технологий SONET/SDH и PDH.
- Ввиду того что ATM поддерживает все основные существующие типы трафика, она выбрана в качестве транспортной основы широкополосных цифровых сетей с интеграцией услуг - сетей B-ISDN, которые должны заменить сети ISDN.

26. Уровневые иерархические модели объединения сетей, основы и идеология. Модель взаимодействия открытых систем (OSI) как пример уровневой модели. Характеристики уровней и их реализация в существующих сетях.

В компьютерных сетях идеологической основой стандартизации является многоуровневый подход к разработке средств сетевого взаимодействия. Именно на основе этого подхода была разработана стандартная семиуровневая модель взаимодействия открытых систем, ставшая своего рода универсальным языком сетевых специалистов.

. Как известно, для решения сложных задач используется универсальный прием - декомпозиция, то есть разбиение одной сложной задачи на несколько более простых задач-модулей. При декомпозиции часто используют многоуровневый подход. Он заключается в следующем. Все множество модулей разбивают на уровни. Уровни образуют иерархию, то есть имеются вышележащие и нижележащие уровни. Множество модулей, составляющих каждый уровень, сформировано таким образом, что для выполнения своих задач они обращаются с запросами только к модулям непосредственно примыкающего нижележащего уровня.

Средства сетевого взаимодействия, конечно, тоже могут быть представлены в виде иерархически организованного множества модулей.

Многоуровневый подход к описанию и реализации функций системы применяется не только в отношении сетевых средств. Такая модель функционирования используется, например, в локальных файловых системах, когда поступивший запрос на доступ к файлу последовательно обрабатывается несколькими программными уровнями.

Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется **стеком коммуникационных протоколов**.

В начале 80-х годов ряд международных организаций по стандартизации - ISO, ITU-T и некоторые другие - разработали модель, которая сыграла значительную роль в развитии сетей. Эта модель называется **моделью взаимодействия открытых систем** (*Open System Interconnection, OSI*) или **моделью OSI**. Модель OSI определяет различные уровни взаимодействия систем, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень.

В модели OSI (рис. 1.25) средства взаимодействия делятся на семь уровней:

- прикладной,
- представительный,
- сеансовый,
- транспортный,
- сетевой,
- канальный
- и физический.

Каждый уровень имеет дело с одним определенным аспектом взаимодействия сетевых устройств.

Физический уровень (Physical layer) имеет дело с передачей битов по физическим каналам связи, (коаксиальный кабель, витая пара, оптоволоконный кабель или цифровой территориальный канал). К этому уровню имеют отношение характеристики физических сред передачи данных, такие как полоса пропускания, помехозащищенность, волновое сопротивление и другие. На этом же уровне определяются характеристики электрических сигналов, передающих дискретную информацию, (крутизна фронтов импульсов, уровни напряжения или тока передаваемого сигнала, тип кодирования, скорость передачи сигналов). Кроме этого, здесь стандартизуются типы разъемов и назначение каждого контакта.

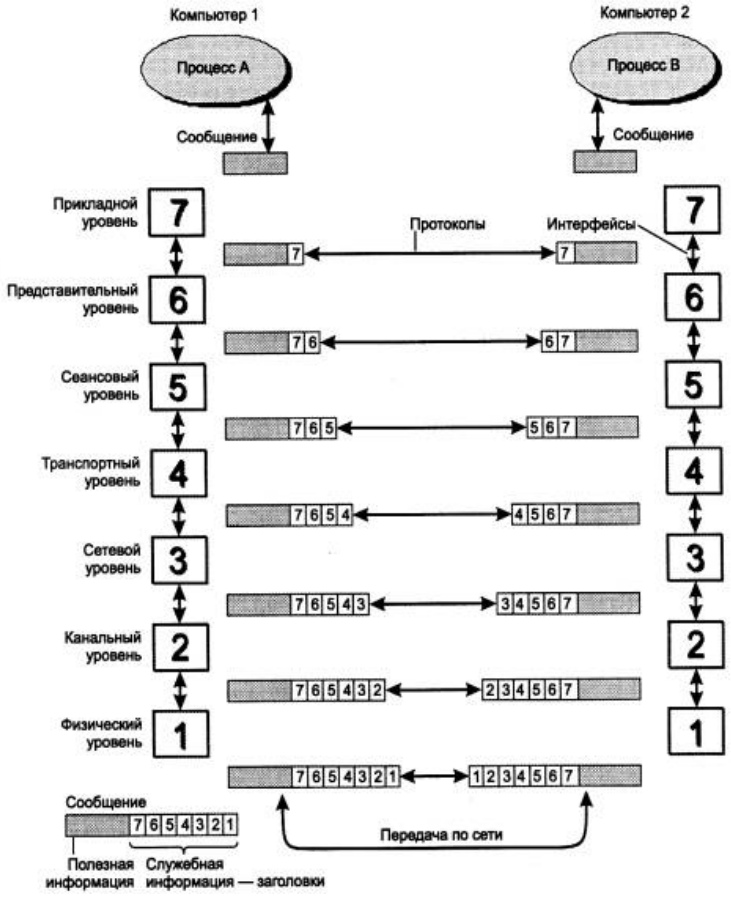


Рис. 1.25. Модель взаимодействия открытых систем ISO/OSI

Функции физического уровня реализуются во всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом.

Примером протокола **физического уровня** может служить спецификация **l0-Base-T технологии Ethernet**, которая определяет в качестве используемого кабеля неэкранированную витую пару категории 3 с волновым сопротивлением 100 Ом, разъем RJ-45, максимальную длину физического сегмента 100 метров, манчестерский код для представления данных в кабеле, а также некоторые другие характеристики среды и электрических сигналов.

Канальный уровень (Data Link layer)

На физическом уровне при пересылке битов не учитывается, что физическая среда передачи может быть занята.

Задачи канального уровня:

- проверка доступности среды передачи.
- реализация механизмов обнаружения и коррекции ошибок**.**

Для этого на канальном уровне биты группируются в наборы, называемые **кадрами** (frames). Канальный уровень обеспечивает корректность передачи каждого кадра, помещая специальную последовательность бит в начало и конец каждого кадра, для его выделения, а также вычисляет контрольную сумму, обрабатывая все байты кадра определенным способом и добавляя контрольную сумму к кадру. Когда кадр приходит по сети, получатель снова вычисляет контрольную сумму полученных данных и сравнивает результат с контрольной суммой из кадра. Если они совпадают, кадр считается правильным и принимается. Если же контрольные суммы не совпадают, то фиксируется ошибка. Канальный уровень может не только обнаруживать ошибки, но и исправлять их за счет повторной передачи поврежденных кадров. Необходимо отметить, что функция исправления ошибок не является обязательной для канального уровня, поэтому в некоторых протоколах этого уровня она отсутствует, например, в Ethernet и frame relay.

В протоколах канального уровня, используемых в локальных сетях, заложена определенная структура связей между компьютерами и способы их адресации. Хотя канальный уровень и обеспечивает доставку кадра между любыми двумя узлами локальной сети, он это делает только в сети с совершенно определенной топологией связей, именно той топологией, для которой он был разработан. К таким типовым топологиям, поддерживаемым протоколами канального уровня локальных сетей, относятся общая шина, кольцо и звезда, а также структуры, полученные из них с помощью мостов и коммутаторов. Примерами протоколов канального уровня являются протоколы Ethernet, Token Ring, FDDI, l00VG-AnyLAN.

В локальных сетях протоколы канального уровня используются компьютерами, мостами, коммутаторами и маршрутизаторами. В компьютерах функции канального уровня реализуются совместными усилиями сетевых адаптеров и их драйверов.

В целом канальный уровень представляет собой весьма мощный и законченный набор функций по пересылке сообщений между узлами сети. В некоторых случаях протоколы канального уровня оказываются самодостаточными транспортными средствами и могут допускать работу поверх них непосредственно протоколов прикладного уровня или приложений, без привлечения средств сетевого и транспортного уровней.

Сетевой уровень (Network layer) служит для образования единой транспортной системы, объединяющей несколько сетей, причем эти сети могут использовать совершенно различные принципы передачи сообщений между конечными узлами и обладать произвольной структурой связей.

Протоколы канального уровня локальных сетей обеспечивают доставку данных между любыми узлами только в сети с соответствующей типовой топологией На сетевом уровне сам термин **сеть** наделяют специфическим значением. В данном случае под сетью понимается совокупность компьютеров, соединенных между собой в соответствии с одной из стандартных типовых топологий и использующих для передачи данных один из протоколов канального уровня, определенный для этой топологии.

Внутри сети доставка данных обеспечивается соответствующим канальным уровнем, а вот доставкой данных между сетями занимается сетевой уровень, который и поддерживает возможность правильного выбора маршрута передачи сообщения даже в том случае, когда структура связей между составляющими сетями имеет характер, отличный от принятого в протоколах канального уровня. Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами. **Маршрутизатор** - это устройство, которое собирает информацию о топологии межсетевых соединений и на ее основании пересылает пакеты сетевого уровня в сеть назначения. Чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество **транзитных передач между сетями, илихопов** (от hop - прыжок), каждый раз выбирая подходящий маршрут. Таким образом, маршрут представляет собой последовательность маршрутизаторов, через которые проходит пакет.

Сообщения сетевого уровня принято называть **пакетами** (packets). При организации доставки пакетов на сетевом уровне используется понятие «номер сети». В этом случае адрес получателя состоит из старшей части - номера сети и младшей - номера узла в этой сети. Все узлы одной сети должны иметь одну и ту же старшую часть адреса, поэтому термину «сеть» на сетевом уровне

можно дать и другое, более формальное определение: сеть - это совокупность узлов, сетевой адрес которых содержит один и тот же номер сети.

На сетевом уровне определяются два вида протоколов. Первый вид - **сетевые протоколы** (routed protocols) - реализуют продвижение пакетов через сеть. Именно эти протоколы обычно имеют в виду, когда говорят о протоколах сетевого уровня. Однако часто к сетевому уровню относят и другой вид протоколов, называемых протоколами обмена маршрутной информацией или просто **протоколами маршрутизации** (routing protocols). С помощью этих протоколов маршрутизаторы собирают информацию о топологии межсетевых соединений. Протоколы сетевого уровня реализуются программными модулями операционной системы, а также программными и аппаратными средствами маршрутизаторов.

На сетевом уровне работают протоколы еще одного типа, которые отвечают за отображение адреса узла, используемого на сетевом уровне, в локальный адрес сети. Такие протоколы часто называют **протоколами разрешения адресов** - *Address Resolution Protocol, ARP*. Иногда их относят не к сетевому уровню, а к канальному, хотя тонкости классификации не изменяют их сути.

Примерами протоколов сетевого уровня являются протокол межсетевого взаимодействия IP стека TCP/IP и протокол межсетевого обмена пакетами IPX стека Novell.

Транспортный уровень

На пути от отправителя к получателю пакеты могут быть искажены или утеряны. Хотя некоторые приложения имеют собственные средства обработки ошибок, существуют и такие, которые предпочитают сразу иметь дело с надежным соединением. **Транспортный уровень** (*Transport layer*) обеспечивает приложениям или верхним уровням стека - прикладному и сеансовому - передачу данных с той степенью надежности, которая им требуется. Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервиса отличаются качеством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное - способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

Как правило, все протоколы, начиная с транспортного уровня и выше, реализуются программными средствами конечных узлов сети - компонентами их сетевых операционных систем. В качестве примера транспортных протоколов можно привести протоколы TCP и UDP стека TCP/IP и протокол SPX стека Novell.

Протоколы нижних четырех уровней обобщенно называют сетевым транспортом или транспортной подсистемой, так как они полностью решают задачу транспортировки сообщений с заданным уровнем качества в составных сетях с произвольной топологией и различными технологиями. Остальные три верхних уровня решают задачи предоставления прикладных сервисов на основании имеющейся транспортной подсистемы.

Сеансовый уровень (*Session layer*) обеспечивает управление диалогом: фиксирует, какая из сторон является активной в настоящий момент, предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, а не начинать все с начала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется в виде отдельных протоколов, хотя функции этого уровня часто объединяют с функциями прикладного уровня и реализуют в одном протоколе.

Представительный уровень (*Presentation layer*) имеет дело с формой представления передаваемой по сети информации, не меняя при этом ее содержания. За счет уровня представления информация, передаваемая прикладным уровнем одной системы, всегда понятна прикладному уровню другой системы. С помощью средств данного уровня протоколы прикладных уровней могут преодолеть синтаксические различия в представлении данных или же различия в кодах символов, например кодов ASCII и EBCDIC. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которому секретность обмена данными обеспечивается сразу для всех прикладных служб. Примером такого протокола является протокол **Secure Socket Layer** (SSL), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

Прикладной уровень (*Application layer*) - это в действительности просто набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые Web-страницы, а также организуют свою совместную работу, например, с помощью протокола электронной почты. Единица данных, которой оперирует прикладной уровень, обычно называется **сообщением** (message).

Существует очень большое разнообразие служб прикладного уровня. Несколько наиболее распространенных реализации файловых служб: NCP в операционной системе Novell NetWare, SMB в Microsoft Windows NT, NFS, FTP и TFTP, входящие в стек TCP/IP.

ВОПРОСЫ

1. Исторические аспекты развития коммуникаций. Эволюция телекоммуникационных систем от древнего мира до наших дней. Примеры наиболее значимых исторических коммуникационных систем. Развитие коммуникаций в XX веке.
2. Основы теории передачи данных по линиям связи. Спектральная теория и ее применение к линиям связи. АЧХ.
3. Характеристики линий связи. Полоса пропускания, затухание, мощность сигнала. Примеры линий связи. Помехоустойчивость, NEXT, BER.
4. Линейное кодирование. Пропускная способность линий связяи. Связь меду полосой пропускания и пропускной способностью (теорема Шеннона, критерий Найквиста).
5. Методы передачи дискретных данных по линиям связи. Аналоговая модуляция, цифровое кодирование и их особенности.
6. Аналоговая модуляция. Модемы. Способы модуляции и их спектральные характеристики.
7. Цифровое кодирование. Особенности и проблемы цифрового кодирования, характеристики цифровых кодов. Основные типы кодирования и их спектральные характеристики.
8. Логическое кодирование. Необходимость и особенности логического кодирования. Наиболее популярные методы логического кодирования.
9. Передача аналоговых сигналов по цифровым линиям связи. Дискретная модуляция. Теорема Найквиста-Котельникова и ее применение к кодированию человеческой речи. Способы улучшения дискретной модуляции для разных типов сигналов.
10. Кабели связи. Характеристики кабелей связи, стандарты кабельной продукции.
11. Структурированные кабельные сети (системы).
12. Проблемы совместного использования линий связи. Мультиплексирование и демультиплексирование. TDM и цифровая телефония.
13. Сети с коммутацией каналов и сети с коммутацией пакетов. Основные отличия и характеристики. Применения и примеры сетей с различными способами коммутации.
14. Методы доступа к среде передачи и их применение в локальных сетях ЭВМ.
15. Сетевые топологии физического уровня и их связь с методами доступа к среде.
16. Локальные и глобальные сети. Основные характеристики и отличия. Структура крупных локальных и глобальных сетей.
17. Локальные сети на основе технологии Ethernet. Физический и канальный уровни. Основные характеристики и отличия. Различные реализации и их особенности.
18. Коммутируемые сети Ethernet. Концепции коммутации и бриджинга, различные типы коммутаторов и мостов.
19. Технологии MetroEthernet, специфика адаптации технологии Ethernet к сетям доступа.
20. Локальные сети на основе технологии FDDI. Физический и канальный уровни. Основные характеристики и отличия. Различные реализации и их особенности.
21. Локальные сети на основе технологии Token Ring. Физический и канальный уровни. Основные характеристики и отличия. Различные реализации и их особенности.
22. Глобальные сети связи. Различные типы глобальных сетей, особенности и характеристики.
23. Сети на основе Frame Relay. Особенности технологии и ее расширения.
24. Сети ISDN. Концепция сети с интеграцией услуг. Характеристики, применение к передаче голоса и данных.
25. Сети X.25. Особенности и применение сетей X.25 в современном мире,
26. Уровневые иерархические модели объединения сетей, основы и идеология. Модель взаимодействия открытых систем (OSI) как пример уровневой модели. Характеристики уровней и их реализация в существующих сетях.

Часть 2
(весна 2010 г.)

Источники указаны в квадратных скобках […] :

1. Олифер (Книга) Олифер глава 5+.doc
2. Шпоргалки nets.pottee.doc
3. Википедия http://ru.wikipedia.org/wiki/
4. Семенов Ю.А. (ГНЦ ИТЭФ) http://book.itep.ru/
   в т.ч. 4.1.1.3 Интернет в Ethernet_CIDR+VLSM.doc
5. Материал из презентации
   в т.ч. it_net_04.ppt
6. В.Г. Олифер, Н.А. Олифер, Сетевые операционные системы , 2-е изд. (книга)

Принятые сокращения:

Сокращение	Полное название
ПО	программное обеспечение
ОС	операционная система
м-р	маршрутизатор
м-ция	маршрутизация
м/у	между
AS	Автономные системы
ЛВС	Локальная вычислительная сеть
SA	Ассоциация безопасности
Олиферы	В.Г. Олифер, Н.А. Олифер, Сетевые операционные системы , 2-е изд.

Перед подготовкой прочитать:

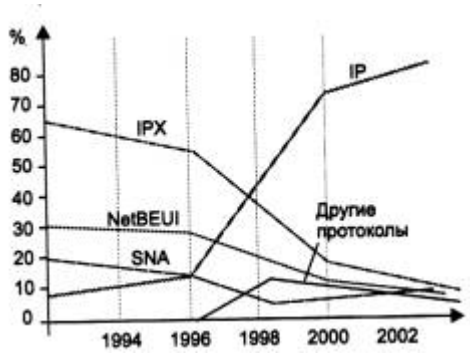
1) **Олиферы [6]]** Из гл.9 Осн. фундаментальные понятия и определения (стр. 408– 424) особо обратить внимание, где помечено карандашом.
2) **4.1.1.3 Интернет в Ethernet_CIDR+VLSM.doc**
3) **it_net_04.ppt**
4) it_net_05_Маршрутизация.ppt
5) **Олиферы [6]** Гл.9 Сеть как трансп. система -всю (стр. 429– 480) хотя бы просмотреть
6) **Олиферы [6]** Из гл.12 (Безопасность) стр.603 внизу, 617– 619 (технология защищённого канала)
6) **Виртуальные частные сети VPN** (до следующего билета)

27. Сети на основе стека протоколов TCP/IP. История возникновения, структура стека протоколов и назначение различных элементов стека. Протоколы, порты, сокеты.

Стек используется для связи компов по Internet, а также в корп.сетях. Стек TCP/IP на нижнем уровне поддерживает все популярные стандарты физического и канального уровней: для локальных сетей — это Ethernet, Token Ring, FDDI, для глобальных — протоколы работы на аналоговых коммутируемых и выделенных линиях SLIP, PPP, протоколы территориальных сетей X.25 и ISDN. Основными протоколами стека, давшими ему название, являются протоколы IP и TCP. Эти протоколы в модели OSI относятся к сетевому и трансп. уровням соотв-но. IP обеспечивает продвижение пакета по составной сети, а TCP гарантирует надежность его доставки. [2]

История возникновения

В настоящее время стек TCP/IP является самым популярным средством организации составных сетей. На рис.1 показана доля, которую составляет тот или иной стек протоколов в общемировой инсталляционной сетевой базе. До 1996 года бесспорным лидером был стек IPX/SPX компании Novell, но затем картина резко изменилась - стек TCP/IP по темпам роста числа установок намного стал опережать другие стеки, а с 1998 года вышел в лидеры и в абсолютном выражении. Именно поэтому дальнейшее изучение функций сетевого уровня будет проводиться на примере стека TCP/IP. [1]



Многоуровневая структура стека TCP/IP

В стеке TCP/IP определены 4 уровня (рис. 2). Каждый из этих уровней несет на себе некоторую нагрузку по решению основной задачи - организации надежной и производительной работы составной сети, части которой построены на основе разных сетевых технологий.

Уровень I	Прикладной уровень
Уровень II	Основной (транспортный) уровень
Уровень III	Уровень межсетевого взаимодействия
Уровень IV	Уровень сетевых интерфейсов

Уровень межсетевого взаимодействия — является стержнем всей архитектуры, и реализует концепцию передачи пакетов в режиме без установления соединений, то есть дейтаграммным способом. Именно этот уровень обеспечивает возможность перемещения пакетов по сети, используя тот маршрут, который в данный момент является наиболее рациональным. Этот уровень также называют уровнем internet, указывая тем самым на основную его функцию - передачу данных через составную сеть.

Основным протоколом сетевого уровня (в терминах модели OSI) в стеке является **протокол IP** (Internet Protocol). Этот протокол изначально проектировался как протокол передачи пакетов в составных сетях, состоящих из большого количества локальных сетей, объединенных как локальными, так и глобальными связями. Поэтому протокол IP хорошо работает в сетях со сложной топологией, рационально используя наличие в них подсистем и экономно расходуя пропускную способность низкоскоростных линий связи. Так как протокол IP является дейтаграммным протоколом, он не гарантирует доставку пакетов до узла назначения, но старается это сделать.

К уровню межсетевого взаимодействия относятся и все протоколы, связанные с составлением и модификацией таблиц маршрутизации, такие как протоколы сбора маршрутной информации RIP (Routing Internet Protocol) и OSPF (Open Shortest Path First), а также протокол межсетевых управляющих сообщений ICMP (Internet Control Message Protocol). Последний протокол предназначен для обмена информацией об ошибках между маршрутизаторами сети и узлом-источником пакета. С помощью специальных пакетов ICMP сообщает о невозможности доставки пакета, о превышении времени жизни или продолжительности сборки пакета из фрагментов, об аномальных величинах параметров, об изменении маршрута пересылки и типа обслуживания, о состоянии системы и т. п.

Основной уровень

Поскольку на сетевом уровне не устанавливаются соединения, то нет никаких гарантий, что все пакеты будут доставлены в место назначения целыми и невредимыми или придут в том же порядке, в котором они были отправлены. Эту задачу -обеспечение надежной информационной связи между двумя конечными узлами -решает основной уровень стека TCP/IP, называемый также транспортным.

На этом уровне функционируют **протокол управления передачей TCP** (Transmission Control Protocol) и протокол дейтаграмм пользователя UDP (User Datagram Protocol). Протокол TCP обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования логических соединений. Этот протокол позволяет равноранговым объектам на компьютере-отправителе и компьютере-получателе поддерживать обмен данными в дуплексном режиме. TCP позволяет без ошибок доставить сформированный на одном из компьютеров поток

байт в любой другой компьютер, входящий в составную сеть. TCP делит поток байт на части - сегменты, и передает их ниже лежащему уровню межсетевого взаимодействия. После того как эти сегменты будут доставлены средствами уровня межсетевого взаимодействия в пункт назначения, протокол TCP снова соберет их в непрерывный поток байт.

Протокол UDP обеспечивает передачу прикладных пакетов дейтаграммным способом, как и главный протокол уровня межсетевого взаимодействия IP, и выполняет только функции связующего звена (мультиплексора) между сетевым протоколом и многочисленными службами прикладного уровня или пользовательскими процессами.

Прикладной уровень и Уровень сетевых интерфейсов см. ниже в разделе КОРОТКО(выводы)

Порты и сокеты (сокеты — см.[6])

Протокол TCP взаимодействует через межуровневые интерфейсы с ниже лежащим протоколом IP и с выше лежащими протоколами прикладного уровня или приложениями.

В то время как задачей сетевого уровня, к которому относится протокол IP, является передача данных между произвольными узлами сети, задача транспортного уровня, которую решает протокол TCP, заключается в передаче данных между любыми **прикладными процессами**, выполняющимися на любых узлах сети. Действительно, после того как пакет средствами протокола IP доставлен в компьютер-получатель, данные необходимо направить конкретному процессу-получателю. Каждый компьютер может выполнять несколько процессов, более того, прикладной процесс тоже может иметь несколько точек входа, выступающих в качестве адреса назначения для пакетов данных.

Пакеты, поступающие на транспортный уровень, организуются операционной системой в виде множества очередей к точкам входа различных прикладных процессов. В терминологии TCP/IP такие системные очереди называются **портами**. Таким образом, адресом назначения, который используется протоколом TCP, является идентификатор (номер) порта прикладной службы. Номер порта в совокупности с номером сети и номером конечного узла однозначно определяют прикладной процесс в сети. Этот набор идентифицирующих параметров имеет название **сокет** (socket).).

Протоколы – Вспомогательные и сопутствующие стеку TCP/IP протоколы и сервисы: DNS, ARP/RARP, ICMP, DHCP, WINS.

<table>
<tr><td>7
6</td><td>www,
Gopher,
WAIS</td><td>SNMP</td><td>FTP</td><td>telnet</td><td>SMTP</td><td>TFTP</td><td>I</td></tr>
<tr><td>5
4</td><td colspan="5">TCP</td><td>UDP</td><td>II</td></tr>
<tr><td>3</td><td>IP</td><td>ICMP</td><td>RIP</td><td>OSPF</td><td colspan="2">ARP</td><td>III</td></tr>
<tr><td>2
1</td><td colspan="6">Не регламентируется
Ethernet, Toking Ring, FDDI, X.25, SLIP, PPP</td><td>IV</td></tr>
</table>

Уровни модели OSI

Уровни стека TCP/IP

КОРОТКО(выводы):

- Наибольшее распространение для построения составных сетей в последнее время получил стек TCP/IP. Стек TCP/IP имеет 4 уровня: прикладной, основной, уровень межсетевого взаимодействия и уровень сетевых интерфейсов. Соответствие уровней стека TCP/IP уровням модели OSI достаточно условно.

- **Прикладной уровень** объединяет все службы, предоставляемые системой пользовательским приложениям: традиционные сетевые службы типа telnet, FTP, TFTP, DNS, SNMP, а также сравнительно новые, такие, например, как протокол передачи гипертекстовой информации HTTP.

- На **основном уровне** стека TCP/IP, называемом также транспортным, функционируют протоколы TCP и UDP. Протокол управления передачей TCP решает задачу обеспечения надежной информационной связи между двумя конечными узлами. Дейтаграммный протокол UDP используется как экономичное средство связи уровня межсетевого взаимодействия с прикладным уровнем.

- **Уровень межсетевого взаимодействия** реализует концепцию коммутации пакетов в режиме без установления соединений. Основными протоколами этого уровня являются дейтаграммный протокол IP и протоколы маршрутизации (RIP, OSPF, BGP и др.). Вспомогательную роль выполняют протокол межсетевых управляющих сообщений ICMP, протокол группового управления IGMP и протокол разрешения адресов ARP.

- **Протоколы уровня сетевых интерфейсов** обеспечивают интеграцию в составную сеть других сетей. Этот уровень не регламентируется, но поддерживает все популярные стандарты физического и канального уровней: для локальных сетей - Ethernet, Token Ring, FDDI и т. д., для глобальных сетей - X.25, frame relay, PPP, ISDN и т. д.

- В стеке TCP/IP для именования единиц передаваемых данных на разных уровнях используют разные названия: поток, сегмент, дейтаграмма, пакет, кадр.

27. из презентации [5] (см.слайды 2 — 7 из it_net_04.ppt)

Уровень MAC (it_net_03.ppt)

- Основными функциями уровня MAC являются:
  - обеспечение доступа к разделяемой среде;
  - передача кадров между конечными узлами, используя функции и устройства физического уровня.

Адресация

- Физические адреса (например, MAC-адресы в сетях Ethernet) используются на канальном уровне для взаимодействия к устройств, находящихся в том же сегменте сети.
- Для описания взаимодействия хостов между отдельными сегментами сети используется адресация на более высоком - **сетевом** - уровне.
- Поиск место размещения хостов и передача данных выполняется специальными устройствами – маршрутизаторами.

Примеры протоколов сетевого уровня

- Наиболее популярным протоколом сетевого уровня, используемым в Интернет, является протокол IP (Internet Protocol).
- Другим протоколом, используемым в локальных сетях, является протокол IPX (Internetwork Packet Exchange) фирмы Novell.
- Протокол NetBEUI является примером немаршрутизируемого протокола сетевого уровня.

Предистория из [4] 4.4.0.0 Интернет-Оглавление.doc

В середине 60-годов в самый разгар холодной войны министерство обороны США планировало создать сеть для управления, которая бы помогла выжить в условиях ядерной войны. Стандартные телефонные сети считались недостаточно надежными, так как выход из строя одного из центральных коммутаторов может парализовать целый регион (телефонная сеть имеет древовидную топологию). *Далее см. [4] 4.4.0.0 Интернет-Оглавление.doc стр.4*

... В 1991 году конгресс США принял закон о создании сети NREN (National Research and Education Network - национальная сеть для науки и образования) с каналами, рассчитанными на скорость передачи в диапазоне гигабит/с. Таким образом, можно считать, что Интернету более 30 лет, а первому официальному документу Интернет (RFC) - более 35.

Со́кеты / *из википедии* / (англ. socket — углубление, гнездо, разъём) — название программного интерфейса для обеспечения обмена данными между процессами. Процессы при таком обмене могут исполняться как на одной ЭВМ, так и на различных ЭВМ, связанных между собой сетью. **Сокет** — абстрактный объект, представляющий конечную точку соединения.

Следует различать клиентские и серверные сокеты. Клиентские сокеты грубо можно сравнить с оконечными аппаратами телефонной сети, а серверные — с коммутаторами. Клиентское приложение (например, браузер) использует только клиентские сокеты, а серверное (например, веб-сервер, которому браузер посылает запросы) — как клиентские, так и серверные сокеты.

Интерфейс сокетов впервые появился в BSD Unix. Программный интерфейс сокетов описан в стандарте POSIX.1 и в той или иной мере поддерживается всеми современными операционными системами.

Сокет на сленге системных администраторов означает комбинацию IP-адреса и номера порта, например 10.10.10.10:80.

Каждый процесс может создать слушающий сокет (серверный сокет) и привязать его к какому-нибудь порту операционной системы (тем не менее, в UNIX непривилегированные процессы не могут использовать порты меньше 1024). Слушающий процесс обычно находится в цикле ожидания, то есть просыпается при появлении нового соединения. При этом сохраняется возможность просто проверить наличие соединений на данный момент, установить тайм-аут для операции и так далее.

Каждый сокет имеет свой адрес. ОС семейства UNIX могут поддерживать много типов адресов, но обязательными являются INET-адрес и UNIX-адрес. Если привязать сокет к UNIX-адресу, то просто будет создан специальный файл (файл сокета) по заданному пути, через который смогут сообщаться любые локальные процессы путём простого чтения/записи из него. Сокеты типа INET доступны из сети и требуют выделения номера порта.

Обычно клиент явно подсоединяется к слушателю, после чего любое чтение или запись через его файловый дескриптор будут на самом деле передавать данные между ним и сервером.

Сокет (программный интерфейс) — программный интерфейс для обеспечения информационного обмена между процессами.

28. Структура адресного пространства в сетях TCP/IP для IPv4. Деление сетей на подсети. CIDR, VLSM.

В стеке TCP/IP используются **три типа адресов**: локальные (называемые также аппаратными), IP-адреса и символьные доменные имена.

В терминологии TCP/IP под **локальным адресом** понимается такой тип адреса, который используется средствами базовой технологии для доставки данных в пределах подсети, являющейся элементом составной интерсети.

IP-адреса представляют собой основной тип адресов, на основании которых сетевой уровень передает пакеты между сетями.

Символьные доменные имена. Символьные имена в IP-сетях называются доменными и строятся по иерархическому признаку. Составляющие полного символьного имени в IP-сетях разделяются точкой и перечисляются в следующем порядке: сначала простое имя конечного узла, затем имя группы узлов, затем имя более крупной группы и так до имени домена самого высокого уровня

IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме и разделенных точками, например, 128.10.2.30 . Адрес состоит из двух логических частей - номера сети и номера узла в сети. Какая часть адреса относится к номеру сети, а какая - к номеру узла, определяется значениями первых бит адреса. Значения этих бит являются также признаками того, к какому классу относится тот или иной IP-адрес.

Рис. 5.9. Структура IP-адреса

Если адрес нач. с 0, то сеть относят к классу A и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети кл. A имеют номера в диапазоне от 1 до 126. Сетей класса A немного, зато кол-во узлов в них может достигать 2^{24}, то есть 16 777 216 узлов.

Если первые два бита адреса = 10, то сеть относится к классу B. В сетях класса B под номер сети и под номер узла отводится по 16 бит, то есть по 2 байта. Таким образом, сеть класса B является сетью средних размеров с макс. числом узлов 2^{16}, что составляет 65 536 узлов.

Если адрес начинается с последовательности 110, то это сеть класса C. В этом случае под номер сети отводится 24 бита, а под номер узла - 8 бит. Сети этого класса наиболее распространены, число узлов в них ограничено 2^8, то есть 256 узлами.

Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес - multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес. Основное назначение multicast-адресов - распространение информации по схеме «один-ко-многим»

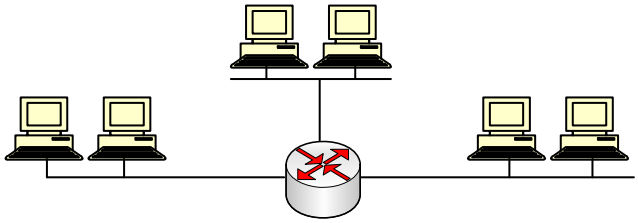
Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Максимальное число узлов в сети
A	0	1.0.0.0	126.0.0.0	2^{24}
B	10	128.0.0.0	191.255.0.0	2^{16}
C	110	192.0.1.0	223.255.255.0	2^8
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.255.255	Зарезервирован

Если адрес начинается с последовательности 11110, то это значит, что данный адрес относится к классу E, Адреса этого класса зарезервированы для будущих применений.

Версия IPv4 (текущая) поддерживает некоторые технологии, направленные на более экономное расходование IP-адресов. Одной из таких технологий является технология **масок** и ее развитие - технология бесклассовой междоменной маршрутизации (Classless Inker-Domain Routing, **CIDR**).

Деление сетей на подсети (коротко из [5])

Для нужд организации выделенная сеть может быть разбита на отдельные части – **подсети**.



Использование подсети не влияет на внешних пользователей, но в пределах организации подсеть рассматривается как структурная единица

Подсети скрыты от внешнего мира с помощью **масок**, называемых масками подсети. С их помощью устройствам сообщается какая часть является адресом подсети, а какая – адресом хоста. . [5] (см.слайды 11 — 13 из it_net_04.ppt)

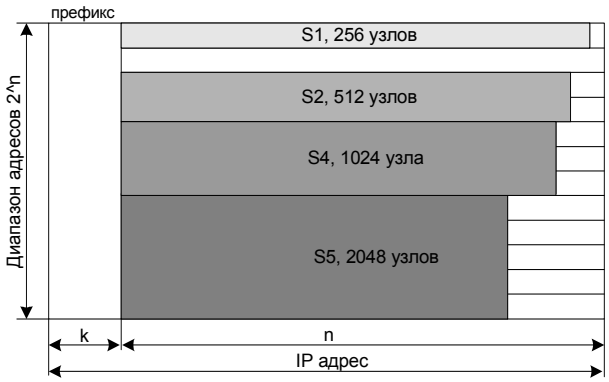
Технология масок позволяет более гибко устанавливать границу между номером сети и номером узла. Снабжая каждый IP-адрес маской, можно отказаться от понятий классов адресов и сделать более гибкой систему адресации. Например, если рассмотренный выше адрес 185.23.44.206 ассоциировать с маской 255.255.255.0, то номером сети будет 185.23.44.0, а не 185.23.0.0, как это определено системой классов. **Маска** - это число, которое используется в паре с IP-адресом; двоичная запись маски содержит единицы в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети. Поскольку номер сети является цельной частью адреса, единицы в маске также должны представлять непрерывную последовательность.

Для стандартных классов сетей маски имеют следующие значения:

- класс A - 11111111. 00000000. 00000000. 00000000 (255.0.0.0);
- класс B - 11111111. 11111111. 00000000. 00000000 (255.255.0.0);
- класс C-11111111.11111111.11111111.00000000 (255.255.255.0).

Технология бесклассовой междоменной маршрутизации CIDR (см. [1] стр.70-74)

Технология CIDR отказывается от традиционной концепции разделения адресов протокола IP на классы, что позволяет получать в пользование столько адресов, сколько реально необходимо. [1]



Значительная роль в будущем IP-сетей отводится технологии бесклассовой междоменной маршрутизации (CIDR), которая решает **две основные задачи**. Первая задача состоит в более экономном расходовании адресного пространства. Благодаря CIDR поставщики услуг получают возможность «нарезать» блоки разных размеров из выделенного им адресного пространства в точном соответствии с требованиями каждого клиента при этом у него остается пространство для маневра на случай его будущего роста. Вторая задача заключается в уменьшении числа записей в таблицах маршрутизации за счет объединения маршрутов - одна запись в таблице маршрутизации может представлять большое количество сетей с общим префиксом. [1]

Суть технологии. Каждому поставщику услуг Internet должен назначаться непрерывный диапазон в пространстве IP-адресов. При таком подходе адреса всех сетей каждого поставщика услуг имеют общую старшую часть - префикс, поэтому маршрутизация на магистралях Internet может осуществляться на основе префиксов, а не полных адресов сетей. Агрегирование адресов позволит уменьшить объем таблиц в маршрутизаторах всех уровней, а следовательно, ускорить работу маршрутизаторов и повысить пропускную способность Internet.

Деление IP-адреса на номер сети и номер узла в технологии CIDR происходит не на основе нескольких старших бит, определяющих класс сети (A, B или C), а на основе маски переменной длины, назначаемой поставщиком услуг

Все адреса имеют общую часть в k старших разрядах - префикс. Оставшиеся n разрядов используются для дополнения неизменяемого префикса переменной частью адреса. Диапазон имеющихся адресов в таком случае составляет 2^n. Когда потребитель услуг обращается к поставщику услуг с просьбой о выделении ему некоторого количества адресов, то в имеющемся пуле адресов «вырезается» непрерывная область S1, S2, S3 или S4 соответствующего размера. Причем границы этой области выбираются такими, чтобы для нумерации требуемого числа узлов хватило некоторого числа младших разрядов, а значения всех оставшихся (старших) разрядов было одинаковым у всех адресов данного диапазона. Таким условиям могут удовлетворять только области, размер которых кратен степени двойки, А границы выделяемого участка должны быть кратны требуемому размеру (количеству узлов). [2 = 1]

Технология VLSM

Бесклассовая адресация основывается **на переменной длине маски подсети** (англ. Variable Length Subnet Mask — VLSM) *см. эту гиперссылку, а также [1] стр.66—70*, в то время, как в классовой (традиционной) адресации длина маски строго фиксирована 0, 1, 2 или 3 установленными октетами. [3]

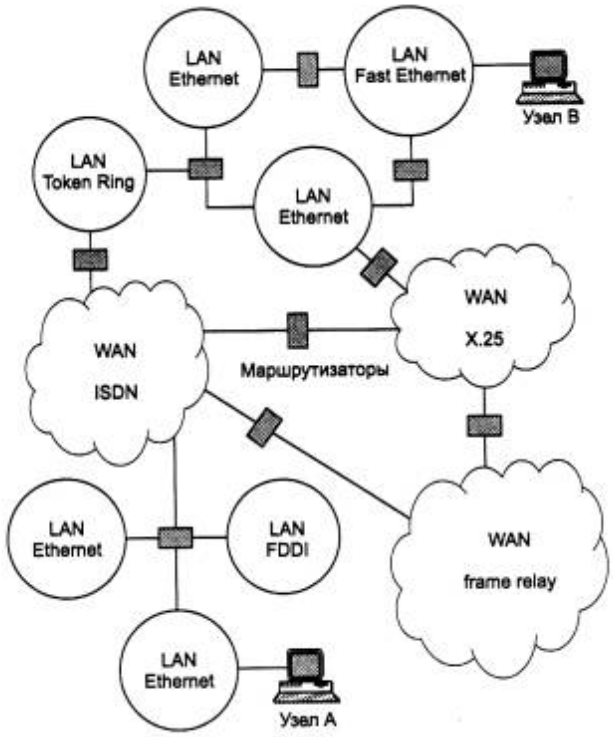
VLSM (из Семёнова [4] См. файлы 4.4.11.5 Бесклассовая интердоменная маршрутизация_CIDR.doc и 4.1.1.3 Интернет в Ethernet_CIDR+VLSM.doc)

При использовании адресов с разделение на классы для разделения на подсети всегда используется одна и та же маска, что не всегда удобно. При использовании масок подсетей переменной длины **VLSM** (Variable Length Subnet Mask) этого ограничения нет. VLSM позволяет разделить диапазон адресов одного класса на подсети с разным числом ЭВМ. Следует лишь учитывать, что это функция маршрутизации, а не адресации. Эта методика

позволяет более эффективно использовать адресное пространство. Разбиения на подсети, выполненные для пространства адресов с классами, могут использоваться и в VLSM. Вычисление адресов в VLSM производится так же как и пасчет адресных диапазонов в CIDR. Практически все провайдеры Интернет используют CIDR и по этой причине выдают адресные блоки с четным числом адресов. При использовании VLSM для сети класса С и подсети 255.255.255.252 могут быть доступны диапазоны адресов X.X.X.5 - X.X.X.6; X.X.X.9 - X.X.X.10; X.X.X.13 - X.X.X.14; X.X.X.21 - X.X.X.22; X.X.X.241 - X.X.X.242 и т.д., а для субсети 255.255.255.240 - X.X.X.33 - X.X.X.46; X.X.X.49 - X.X.X.62; X.X.X.225 - X.X.X.238 и т.д. VLSM поддерживается не всеми протоколами маршрутизации.

Деление сетей на подсети (подробно из [1])

Построение сложных сетей только на основе повторителей, мостов и коммутаторов имеет существенные ограничения и недостатки. Осн. идея введения сетевого уровня состоит в том, что. сеть в общем случае рассматривается как совокупность нескольких сетей и называется составной сетью или интерсетью (internetwork или internet). Сети, входящие в составную сеть, называются **подсетями** (subnet), составляющими сетями или просто сетями (рис. 5.1).



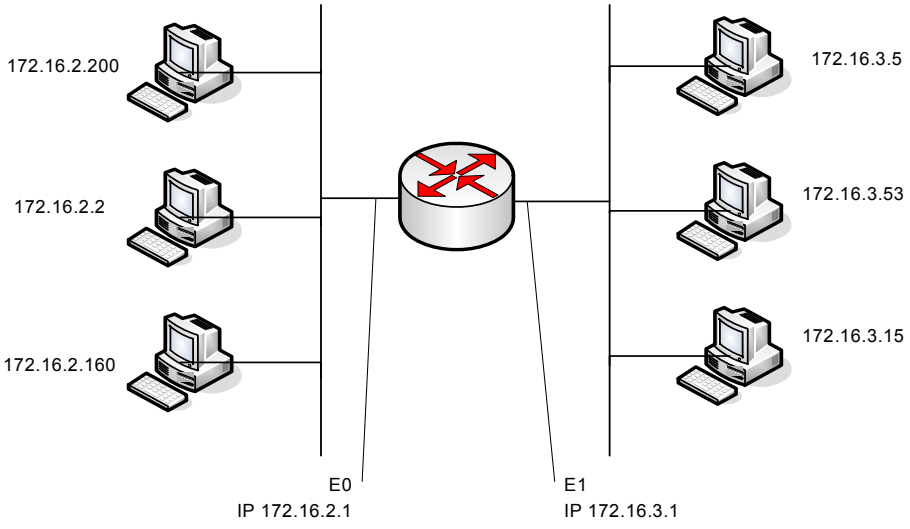
Подсети соединяются между собой маршрутизаторами. Компонентами составной сети могут являться как локальные, так и глобальные сети. Внутренняя структура каждой сети на рисунке не показана, так как она не имеет значения при рассмотрении сетевого протокола. Все узлы в пределах одной подсети взаимодействуют, используя единую для них технологию. Так, в составную сеть, показанную на рисунке, входит несколько сетей разных технологий: локальные сети Ethernet, Fast Ethernet, Token Ring, FDDI и глобальные сети frame relay, X.25, ISDN. Каждая из этих технологий достаточна для того, чтобы организовать взаимодействие всех узлов в своей подсети, но не способна построить информационную связь между произвольно выбранными узлами, принадлежащими разным подсетям, например между узлом А и узлом В на рис. 5.1. Следовательно, для организации взаимодействия между любой произвольной парой узлов этой «большой» составной сети требуются дополнительные средства. Такие средства и предоставляет сетевой уровень.

Сетевой уровень выступает в качестве координатора, организующего работу всех подсетей, лежащих на пути продвижения пакета по составной сети. Для перемещения данных в пределах подсетей сетевой уровень обращается к используемым в этих подсетях технологиям. [1]

Адресация подсетей

- Адреса подсетей, подобно адресам хостов, задаются локально сетевым администратором.
- С точки зрения адресации, подсети являются расширением сетевого номера

[5] (см.слайд 13 из it_net_04.ppt)



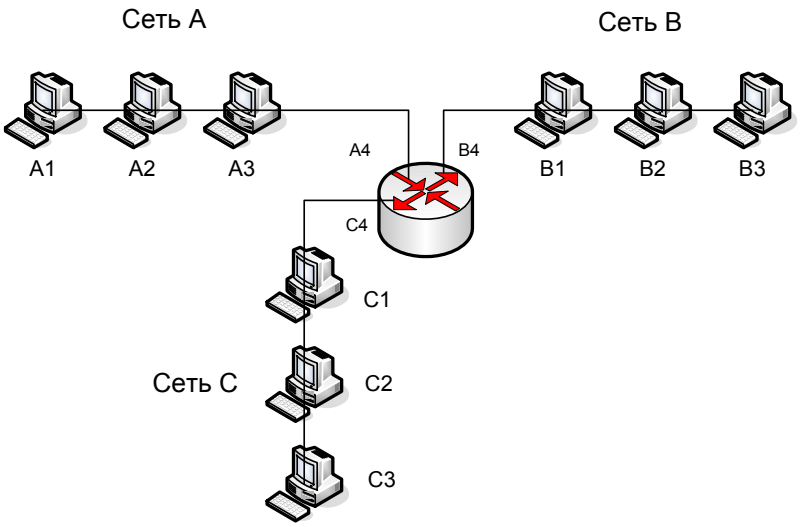
172.016. 002. 160
сеть подсеть хост

Выводы (не все, а только основные):

- Составная сеть (internetwork или internet) - это совокупность нескольких сетей, называемых также **подсетями** (subnet), которые соединяются между собой маршрутизаторами. Организация совместной транспортной службы в составной сети называется межсетевым взаимодействием (internetworking).
- В стеке TCP/IP используются три типа адресов: локальные (называемые также аппаратными), IP-адреса и символьные доменные имена. Все эти типы адресов присваиваются узлам составной сети независимо друг от друга.
- IP-адрес имеет длину 4 байта и состоит из номера сети и номера узла. Для определения границы, отделяющей номер сети от номера узла, реализуются два подхода. Первый основан на понятии класса адреса, второй - на использовании масок.
- Класс адреса определяется значениями нескольких первых бит адреса. В адресах класса A под номер сети отводится один байт, а остальные три байта - под номер узла, поэтому они используются в самых больших сетях. Для небольших сетей больше подходят адреса класса C, в которых номер сети занимает три байта, а для нумерации узлов может быть использован только один байт. Промежуточное положение занимают адреса класса B.
- Другой способ определения, какая часть адреса является номером сети, а какая номером узла, основан на использовании маски. Маска - это число, которое используется в паре с IP-адресом; двоичная запись маски содержит единицы в тех разрядах, которые в IP-адресе должны интерпретироваться как номер сети.

IP-адресация [5] (см.слайд 13 из it_net_04.ppt)

- Для успешной маршрутизации пакетов данных используется иерархическая адресация - каждая сеть (подсеть) имела уникальный номер.
- Эти номера записываются в заголовках пакетов сетевого уровня и анализируются маршрутизаторами для передачи пакетов из сети в сеть.



IP-адресация

- IP-адрес устройства включает в себя **адрес сети**, к которой принадлежит устройство, и адрес устройства в этой сети.
- IP-адрес имеет иерархическую структуру и более удобен для организации адресов компьютеров, чем MAC-адреса.
- IP-адресация позволяет находить пункт назначения в сети Интернет. Для определения адреса используются двоичные значения.
  - Общая длина адреса составляет 32 бита (версия IPv4).
- Для записи IP-адреса как правило применяется десятичная нотация – адрес задается в виде 4 чисел разделенных точками, например, 192.168.160.224.

Протокол IP

- Протокол IP используется для управления рассылкой TCP/IP пакетов по сети Internet.
- Функции, возложенные на уровень IP :
  - определение пакета, который является базовым понятием и единицей передачи данных в сети Internet. Такой IP-пакет называют датаграммой;
  - определение адресной схемы, которая используется в сети Internet;
  - передача данных между канальным уровнем (уровнем доступа к сети) и транспортным уровнем (другими словами мультиплексирование транспортных датаграмм во фреймы канального уровня);
  - маршрутизация пакетов по сети, т.е. передача пакетов от одного шлюза к другому с целью передачи пакета машине-получателю;
  - "нарезка" и сборка из фрагментов пакетов транспортного уровня.

Особенности IP-протокола

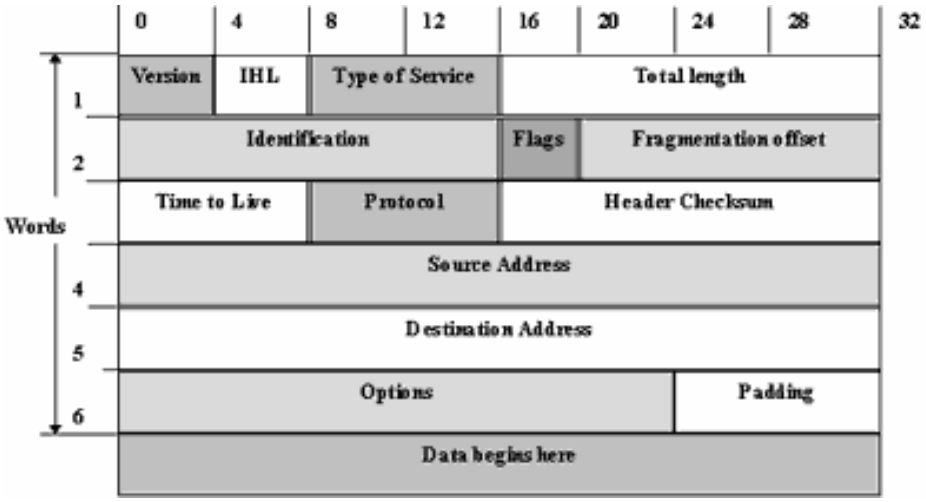
- Главными особенностями протокола IP является отсутствие ориентации на физическое или виртуальное соединение. Это значит, что прежде чем послать пакет в сеть, модуль

операционной системы, реализующий IP, не проверяет возможность установки соединения, т.е. никакой управляющей информации кроме той, что содержится в самом IP-пакете, по сети не передается.

- IP не заботится о проверке целостности информации в поле данных пакета, что заставляет отнести его к протоколам ненадежной доставки. Целостность данных проверяется протоколами транспортного уровня (TCP) или протоколами приложений.
- Вся информация о пути, по которому должен пройти пакет берется из самой сети в момент прохождения пакета.
- Эта процедура и называется маршрутизацией в отличии от коммутации, которая используется для предварительного установления маршрута следования данных, по которому потом эти данные отправляют.

Формат IP пакета

- В заголовке пакета определены:
  - адрес отправителя (4-ое слово заголовка),
  - адрес получателя (5-ое слово заголовка),
  - общая длина пакета (поле Total Lenght)
  - тип пересылаемой датаграммы (поле Protocol).
- Если IP-адрес получателя принадлежит одной из ее сетей, то на интерфейс этой сети пакет и будет отправлен, в противном случае пакет отправят на другой шлюз.



Транспортировка пакетов

- Зная протокол транспортного уровня, IP-модуль производит раскапсулирование информации из своего пакета и ее направление на модуль обслуживания соответствующего транспорта.
- При обычной процедуре инкапсулирования пакет просто помещается в поле данных фрейма, а в случае, когда это не может быть осуществлено, то разбивается на более мелкие фрагменты.
- Размер максимально возможного фрейма, который передается по сети, определяется величиной MTU (Maximum Transsion* Unit), определенной для протокола канального уровня.
- Для того, чтобы потом восстановить пакет IP должен держать информацию о своем разбиении.
  - Для этой цели используется поля "flags" и "fragmentation offset". В этих полях определяется, какая часть пакета получена в данном фрейме, если этот пакет был фрагментирован на более мелкие части.

Transsion* возможно опечатка т.к. ***MTU*** — ***Maximum Transmission Unit*** *(и ещё ссылка на MTU)*

28 из Семёнова [4]

См. файлы 4.4.11.5 Бесклассовая интердоменная маршрутизация_CIDR.doc и 4.1.1.3 Интернет в Ethernet_CIDR+VLSM.doc) – **обязательно прочитать!!!**

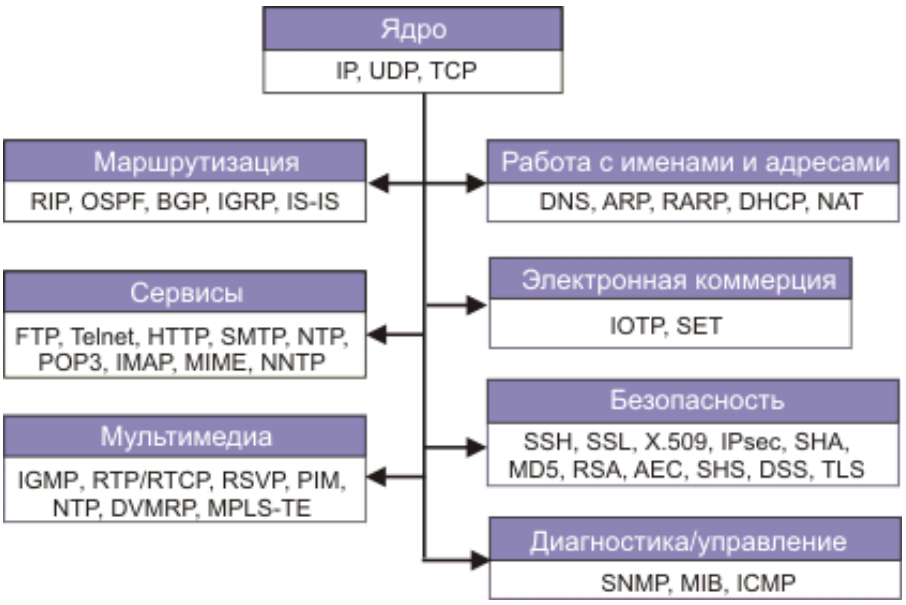
.... Проблема может быть решена, если забыть про разбиение всей совокупности IP-адресов на классы. Такая модель реализуется в рамках **протокола CIDR** (Classless InterDomain Routing). Смотри подробнее "**Интернет в Ethernet**". В этой модели каждой сети ставится в соответствие определенное число смежных блоков по 256 адресов. Далее используется известное географическое зонное распределение IP-адресов (см. RFC-1519). Протокол при просмотре маршрутных таблиц предполагает применение специальных масок и индексных механизмов.

...В связи с дефицитом адресов в сетке **IPv4** в последнее время все шире стала использоваться схема адресации supernet и маршрутизации без классов (**CIDR** -Ckassless Interdomain Routing). Эта технология появилась в 1993 году одновременно с появлением протокола **BGP-4**. Протокол CIDR формирует маршруты на базе непрерывных полей IP-адресов. В варианте без классов группа адресов представляется как единая сеть. Деление адресного пространства на подсети не имеет никакого отношения к протоколу CIDR. Адресное пространство CIDR может содержать любое число адресов с числом 2 в любой степени. Ниже в таблице представленя параметры сетевых адресов без классов (см. 4.1.1.3 Интернет в Ethernet_CIDR+VLSM.doc)

См. также 4.4.1.0_IP-протокол.doc и файлы его подразделов ,

См. также Дерево протоколов стека TCP/IP

Дерево протоколов стека TCP/IP



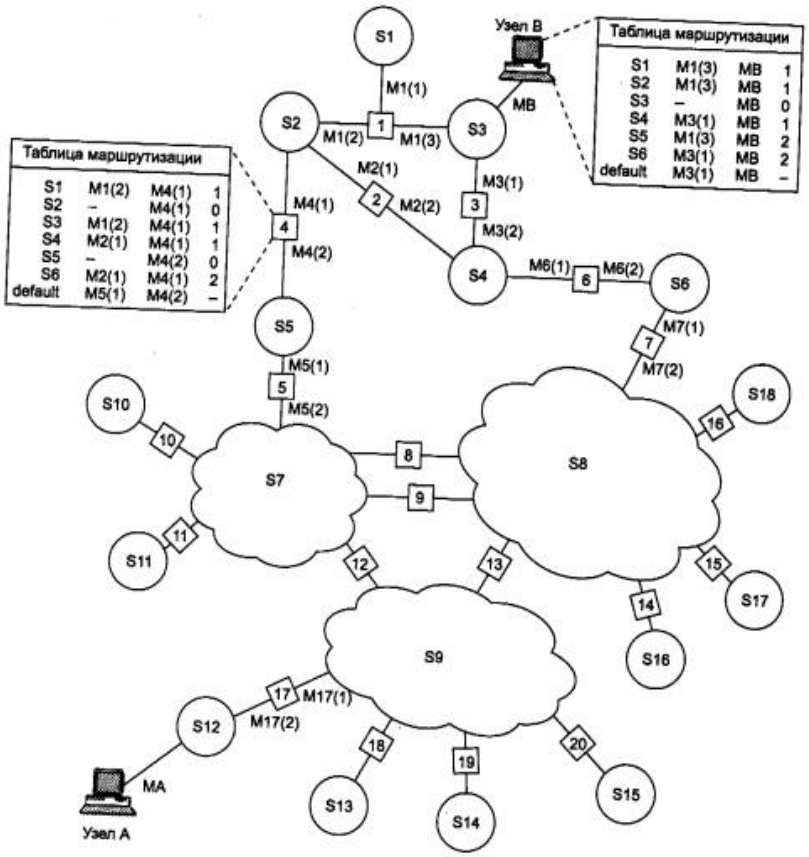
В сущности, современные сети, и Интернет в частности, базируются на достаточно ограниченном списке идей:

1. пакетный принцип передачи данных и управления;
2. адаптация длины пакета к условиям передачи (фрагментация/дефрагментация);
3. инкапсуляция пакетов друг в друга;
4. динамическая маршрутизация.

29. Основные принципы работы маршрутизатора. Таблицы маршрутизации, ~~форвардинг~~, типы маршрутов, фрагментация, MTU (стр. 48, п.5.3.6 стр. 74).

Важнейшей задачей сетевого уровня является маршрутизация - передача пакетов между двумя конечными узлами в составной сети.

Рассмотрим принципы маршрутизации на примере составной сети, изображенной на рис. 5.2. В этой сети 20 маршрутизаторов объединяют 18 сетей в общую сеть; S1, S2, ... , S20 - это номера сетей. Маршрутизаторы имеют по нескольку портов (по крайней мере, по два), к которым присоединяются сети. Каждый порт маршрутизатора можно рассматривать как отдельный узел сети: он имеет собственный сетевой адрес и собственный локальный адрес в той подсети, которая к нему подключена. Например, маршрутизатор под номером 1 имеет три порта, к которым подключены сети S1, S2, S3. На рисунке сетевые адреса этих портов обозначены как M1(1), Ml (2) и M1(3). Порт M1(1) имеет локальный адрес в сети с номером S1, порт Ml (2) - в сети S2, а порт M1(3) - в сети S3. Таким образом, маршрутизатор можно рассматривать как совокупность нескольких узлов, каждый из которых входит в свою сеть. Как единое устройство маршрутизатор не имеет ни отдельного сетевого адреса, ни какого-либо локального адреса.



В сложных составных сетях почти всегда существует несколько альтернативных маршрутов для передачи пакетов между двумя конечными узлами. **Маршрут** - это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до пункта назначения. Так, пакет, отправленный из узла А в узел В, может пройти через маршрутизаторы 17, 12, 5, 4 и 1 или маршрутизаторы 17,13, 7, 6 и 3. Нетрудно найти еще несколько маршрутов между узлами А и В.

Задачу выбора маршрута из нескольких возможных решают маршрутизаторы, а также конечные узлы. Маршрут выбирается на основании имеющейся у этих устройств информации о текущей конфигурации сети, а также на основании указанного критерия выбора маршрута. Обычно в качестве критерия выступает задержка прохождения маршрута отдельным пакетом или средняя пропускная способность маршрута для последовательности пакетов. Часто также используется весьма простой критерий, учитывающий только количество пройденных в маршруте промежуточных маршрутизаторов (**хопов**).

Таблицы маршрутизации

Чтобы по адресу сети назначения можно было бы выбрать рациональный маршрут дальнейшего следования пакета, каждый конечный узел и маршрутизатор анализируют специальную информационную структуру, которая называется **таблицей маршрутизации**. Используя условные обозначения для сетевых адресов маршрутизаторов и номеров сетей в том виде, как они приведены на рис. 5.2, посмотрим, как могла бы выглядеть таблица маршрутизации, например, в маршрутизаторе 4 (табл. 5.1).

Номер сети назначения	Сетевой адрес следующего маршрутизатора	Сетевой адрес выходного порта	Расстояние до сети назначения
S1	M1(2)	M4(1)	1
S2	—	M4(1)	0 (подсоединена)
S3	M1(2)	M4(1)	1
S4	M2(1)	M4(1)	1
S5	—	M4(2)	0 (подсоединена)
S6	M2(1)	M4(1)	2
Default	M5(1)	M4(2)	—

В первом столбце таблицы перечисляются

номера сетей, входящих в интерсеть. В каждой строке таблицы следом за номером сети указывается сетевой адрес следующего маршрутизатора (более точно, сетевой адрес соответствующего порта следующего маршрутизатора), на который надо направить пакет, чтобы тот передвигался по направлению к сети с данным номером по рациональному маршруту.

Когда на маршрутизатор поступает новый пакет, номер сети назначения, извлеченный из поступившего кадра, последовательно сравнивается с номерами сетей из каждой строки таблицы. Строка с совпавшим номером сети указывает, на какой ближайший маршрутизатор следует направить пакет. Например, если на какой-либо порт маршрутизатора 4 поступает пакет, адресованный в сеть S6, то из таблицы маршрутизации следует, что адрес следующего маршрутизатора - M2(1), то есть очередным этапом движения данного пакета будет движение к порту 1 маршрутизатора 2.

Поскольку пакет может быть адресован в любую сеть составной сети, может показаться, что каждая таблица маршрутизации должна иметь записи обо всех сетях, входящих в составную сеть. Но при таком подходе в случае крупной сети объем таблиц маршрутизации может оказаться очень большим, что повлияет на время ее просмотра, потребует много места для хранения и т. п. Поэтому на практике число записей в таблице маршрутизации стараются уменьшить за счет использования специальной записи - «маршрутизатор по умолчанию» (default). Действительно, если принять во внимание топологию составной сети, то в таблицах маршрутизаторов, находящихся на периферии составной сети, достаточно записать номера сетей, непосредственно подсоединенных к данному маршрутизатору или расположенных поблизости, на тупиковых маршрутах. Обо всех же остальных сетях можно сделать в таблице единственную запись, указывающую на маршрутизатор, через который пролегает путь ко всем этим сетям. Такой маршрутизатор называется **маршрутизатором по умолчанию**, а вместо номера сети в соответствующей строке помещается особая запись, например default. В нашем примере таким маршрутизатором по умолчанию для сети S5 является маршрутизатор 5, точнее его порт M5(1). Это означает, что путь из сети S5 почти ко всем сетям большой составной сети пролегает через этот порт маршрутизатора.

Примеры таблиц маршрутизации см. в дополнительном материале или см. [1] п. 5.3.3. стр. 51-57

Функции маршрутизатора

Основная функция маршрутизатора -

- чтение заголовков пакетов сетевых протоколов, принимаемых и буферизуемых по каждому порту (например, IPX, IP, AppleTalk или DECnet),
- и принятие решения о дальнейшем маршруте следования пакета по его сетевому адресу, включающему, как правило, номер сети и номер узла.

Функции маршрутизатора могут быть разбиты на 3 группы в соответствии с уровнями модели OSI (рис. 5.3).

Фрагментация IP-пакетов, MTU (см. [1] п. 5.3.6. стр. 74-78)

Важной особенностью протокола IP, отличающей его от других сетевых протоколов (например, от сетевого протокола IPX), является его способность выполнять динамическую **фрагментацию** пакетов при передаче их между сетями с различными, максимально допустимыми значениями поля данных кадров **MTU**. Свойство **фрагментации** во многом

способствовало тому, что протокол IP смог занять доминирующие позиции в сложных составных сетях.

IP-фрагментация становится необходимой при необходимости передать пакет в следующую сеть, для которой размер пакета является слишком большим. В функции уровня IP входит разбиение слишком длинного для конкретного типа составляющей сети сообщения на более короткие пакеты с созданием соответствующих служебных полей, нужных для последующей сборки фрагментов в исходное сообщение.

В большинстве типов локальных и глобальных сетей значения MTU, то есть максимальный размер поля данных, в которое должен инкапсулировать свой пакет протокол IP, значительно отличается. Сети Ethernet имеют значение MTU, равное 1500 байт, сети FDDI - 4096 байт, а сети X.25 чаще всего работают с MTU в 128 байт.

Процедуры фрагментации и сборки протокола IP рассчитаны на то, чтобы пакет мог быть разбит на практически любое количество частей, которые впоследствии могли бы быть вновь собраны. Получатель фрагмента использует поле идентификации для того, чтобы не перепутать фрагменты различных пакетов. Модуль IP, отправляющий пакет, устанавливает в поле идентификации значение, которое должно быть уникальным для данной пары отправитель - получатель, а также время, в течение которого пакет может быть активным в сети.

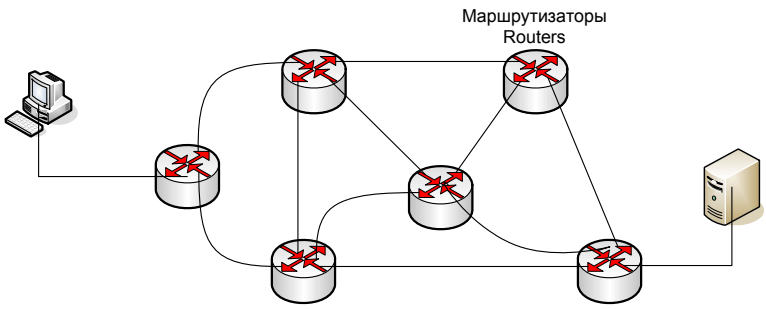
Каждый модуль IP должен быть способен передать пакет из 68 байт без дальнейшей фрагментации. Это связано с тем, что IP-заголовок может включать до 60 байт, а минимальный фрагмент данных - 8 байт. Каждый получатель должен быть в состоянии принять пакет из 576 байт в качестве единого куска либо в виде фрагментов, подлежащих сборке.

Подробнее о **фрагментации** см. здесь (*гиперссылка*)

Maximum Transmission Unit (MTU) *используется для определения максимального размера блока (в байтах), который может быть передан на канальном уровне сетевой модели OSI.» (см. MTU-wiki.doc)*

Маршрутизаторы [5] (см.слайды 4 – 5, 18 из it_net_04.ppt)

- **Маршрутизаторы** – устройства обеспечивающие межсетевое взаимодействия и работающие на сетевом уровне модели OSI.
- Маршрутизатор обеспечивает сквозную маршрутизацию при прохождении пакетов данных перенаправления трафика на основании информации сетевого протокола.
- Маршрутизаторы позволяют решить проблему чрезмерного широковещательного трафика, поскольку они не переадресуют широковещательные кадры, если это не предписано.



Принцип работы маршрутизатора

- Маршрутизатор использует сообщения третьего уровня для определения оптимального маршрута доставки данных в сети. [5]

Маршрутизация и коммутация

- Принцип маршрутизации является одним из тех факторов, который обеспечил гибкость сети Internet.
- Маршрутизация является ресурсоемкой процедурой, так как требует анализа каждого пакета, который проходит через шлюз или маршрутизатор
- При коммутации анализируется только управляющая информация, устанавливается канал, физический или виртуальный, и все пакеты пересылаются по этому каналу без анализа маршрутной информации.
  - При неустойчивой работе сети пакеты могут пересылаться по различным маршрутам и затем собираться в единое сообщение.
  - При коммутации путь придется каждый раз вычислять заново для каждого пакета, а в этом случае коммутация потребует больше накладных затрат, чем маршрутизация. [5]

Маршрутизация [5] (см. it_net_05_Маршрутизация.ppt)

- Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами.
- **Маршрутизатор** — это устройство, которое собирает информацию о топологии межсетевых соединений и пересылает пакеты сетевого уровня в сеть назначения. Чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач между сетями, или **хопов** (от слова hop — прыжок), каждый раз выбирая подходящий маршрут. Таким образом, **маршрут** представляет собой последовательность маршрутизаторов, через которые проходит пакет.
- Сетевой уровень должен обеспечить доставку пакета:
  - между любыми двумя узлами сети с произвольной топологией;
  - между любыми двумя сетями в составной сети;
- **Сеть** — совокупность компьютеров, использующих для обмена данными единую сетевую технологию;
- **Маршрут** — последовательность прохождения пакетом маршрутизаторов в составной сети.]

Задачи маршрутизации

- Проблема выбора наилучшего пути называется маршрутизацией, и ее решение является одной из главных задач **сетевого уровня**.
- Эта проблема осложняется тем, что **самый короткий путь — не всегда самый лучший**.
- Критерием при выборе **маршрута** может служить время передачи данных:
  - Время зависит от пропускной способности каналов связи и интенсивности трафика, которая может с течением времени изменяться.
- Выбор **маршрута** может осуществляться и по другим критериям, таким как **надежность** передачи.
- Функции **сетевого уровня** шире, чем функции передачи сообщений по связям с нестандартной структурой, которые мы рассмотрели на примере объединения нескольких локальных сетей.
- **Сетевой уровень** также решает задачи согласования разных технологий, упрощения **адресации** в крупных сетях и создания надежных и гибких барьеров на пути нежелательного трафика между сетями.

Протоколы маршрутизации

- Протокол маршрутизации – поддерживает маршрутизируемый протокол за счет предоставления механизмов коллективного использования маршрутной информации.
- Сообщения протокола маршрутизации циркулируют между маршрутизаторами для обмена информации и атуализации данных таблиц маршрутизации.
- Примеры протоколов маршрутизации:
  - RIP – протокол маршрутной информации;
  - IGRP – протокол внутренней маршрутизации между шлюзами;
  - EIGR – усовершенствованный протокол внутренней маршрутизации между шлюзами;
  - OSPF – протокол маршрутизации с выбором кратчайшего пути.

Алгоритмы маршрутизации

- Большинство алгоритмов маршрутизации можно свести к трем основным:
  - Маршрутизация на основе вектора расстояния – определяется направление (вектор) и расстояние до каждого канала в сети;
  - Маршрутизация на основе оценки состояния канала (выбор на основе кратчайшего пути), при которой воссоздается точная топология всей сети (по крайней мере, где размещается маршрутизатор);
  - Гибридный подход, объединяющий вышеуказанные алгоритмы.

Протоколы маршрутизации (типы м-ции) [1] (см. билет №32)

Протоколы маршрутизации (например, RIP, OSPF, NLSP) следует отличать от собственно сетевых протоколов (например, IP, IPX). И те и другие выполняют функции сетевого уровня модели OSI - участвуют в доставке пакетов адресату через разнородную составную сеть. Но в то время как первые собирают и передают по сети чисто служебную информацию, вторые предназначены для передачи пользовательских данных, как это делают протоколы канального уровня. Протоколы маршрутизации используют сетевые протоколы как транспортное средство.

С помощью протоколов маршрутизации маршрутизаторы составляют карту связей сети той или иной степени подробности. На основании этой информации для каждого номера сети принимается решение о том, какому следующему маршрутизатору надо передавать пакеты, направляемые в эту сеть, чтобы маршрут оказался рациональным. Результаты этих решений заносятся в таблицу маршрутизации.

Протоколы маршрутизации м.б. построены на основе разных алгоритмов, отличающихся способами построения таблиц маршрутизации, способами выбора наилучшего маршрута и другими особенностями своей работы.

Во всех описанных выше примерах при выборе рационального маршрута определялся только следующий (ближайший) маршрутизатор, а не вся последовательность маршрутизаторов от начального до конечного узла. В соответствии с этим подходом маршрутизация выполняется по распределенной схеме - каждый маршрутизатор ответственен за выбор только одного шага маршрута, а окончательный маршрут складывается в результате работы всех маршрутизаторов, через которые проходит данный пакет. Такие алгоритмы маршрутизации называются **одношаговыми**.

Существует и прямо противоположный, **многошаговый подход - маршрутизация от источника** (Source Routing). В соответствии с ним узел-источник задает в отправляемом в сеть пакете полный маршрут его следования через все промежуточные маршрутизаторы. При использовании многошаговой маршрутизации нет необходимости строить и анализировать таблицы маршрутизации. Это ускоряет прохождение пакета по сети, разгружает маршрутизаторы, но при этом большая нагрузка ложится на конечные узлы. Эта схема в вычислительных сетях применяется сегодня гораздо реже, чем схема распределенной одношаговой маршрутизации. Однако в новой версии протокола IP наряду с классической одношаговой маршрутизацией будет разрешена и маршрутизация от источника.

Одношаговые алгоритмы в зависимости от способа формирования таблиц маршрутизации делятся на три класса:

- алгоритмы фиксированной (или статической) маршрутизации;
- алгоритмы простой маршрутизации;
- алгоритмы адаптивной (или динамической) маршрутизации.

В алгоритмах **фиксированной маршрутизации** все записи в таблице маршрутизации являются статическими. Администратор сети сам решает, на какие маршрутизаторы надо передавать пакеты с теми или иными адресами, и вручную (например, с помощью утилиты route ОС Unix или Windows NT) заносит соответствующие записи в таблицу маршрутизации. Таблица, как правило, создается в процессе загрузки, в дальнейшем она используется без изменений до тех пор, пока ее содержимое не будет отредактировано вручную. Такие исправления могут понадобиться, например, если в сети отказывает какой-либо маршрутизатор и его функции возлагаются на другой маршрутизатор. Различают одномаршрутные таблицы, в которых для каждого адресата задан один путь, и многомаршрутные таблицы, определяющие несколько альтернативных путей для каждого адресата. В многомаршрутных таблицах должно быть задано правило выбора одного из маршрутов. Чаще всего один путь является основным, а остальные - резервными. Понятно, что алгоритм фиксированной маршрутизации с его ручным способом формирования таблиц маршрутизации приемлем только в небольших сетях с простой топологией. Однако этот алгоритм может быть эффективно использован и для работы на магистралях крупных сетей, так как сама магистраль может иметь простую структуру с очевидными наилучшими путями следования пакетов в подсети, присоединенные к магистрали.

В алгоритмах **простой маршрутизации** таблица маршрутизации либо вовсе не используется, либо строится без участия протоколов маршрутизации. **Выделяют три типа простой маршрутизации**:

- случайная маршрутизация, когда прибывший пакет посылается в первом попавшем случайном направлении, кроме исходного;
- лавинная маршрутизация, когда пакет широковещательно посылается по всем возможным направлениям, кроме исходного (аналогично обработке мостами кадров с неизвестным адресом);
- маршрутизация по предыдущему опыту, когда выбор маршрута осуществляется по таблице, но таблица строится по принципу моста путем анализа адресных полей пакетов, появляющихся на входных портах.

Самыми распространенными являются **алгоритмы адаптивной (или динамической) маршрутизации**. Эти алгоритмы обеспечивают автоматическое обновление таблиц маршрутизации после изменения конфигурации сети. Протоколы, построенные на основе адаптивных алгоритмов, позволяют всем маршрутизаторам собирать информацию о топологии связей в сети, оперативно отрабатывая все изменения конфигурации связей. В таблицах маршрутизации при адаптивной маршрутизации обычно имеется информация об интервале

времени, в течение которого данный маршрут будет оставаться действительным. Это время называют временем жизни маршрута (Time To Live, TTL).

Адаптивные алгоритмы обычно имеют распределенный характер, который выражается в том, что в сети отсутствуют какие-либо выделенные маршрутизаторы, которые собирали бы и обобщали топологическую информацию: эта работа распределена между всеми маршрутизаторами.

Адаптивные алгоритмы маршрутизации должны отвечать нескольким важным требованиям.

1. Обеспечивать, если не оптимальность, то хотя бы рациональность маршрута.
2. Должны быть достаточно простыми, чтобы при их реализации не тратилось слишком много сетевых ресурсов, в частности они не должны требовать слишком большого объема вычислений или порождать интенсивный служебный трафик.
3. Должны обладать свойством сходимости, то есть всегда приводить к однозначному результату за приемлемое время.

Адаптивные протоколы обмена маршрутной информацией, применяемые в настоящее время в вычислительных сетях, в свою очередь делятся на две группы, каждая из которых связана с одним из следующих типов алгоритмов:

- дистанционно-векторные алгоритмы (Distance Vector Algorithms, DVA);
- алгоритмы состояния связей (Link State Algorithms, LSA).

В алгоритмах **дистанционно-векторного типа** каждый маршрутизатор периодически и широковещательно рассылает по сети вектор, компонентами которого являются расстояния от данного маршрутизатора до всех известных ему сетей. Под расстоянием обычно понимается число хопов. При получении вектора от соседа маршрутизатор наращивает расстояния до указанных в векторе сетей на расстояние до данного соседа. Получив вектор от соседнего маршрутизатора, каждый маршрутизатор добавляет к нему информацию об известных ему других сетях, о которых он узнал непосредственно (если они подключены к его портам) или из аналогичных объявлений других маршрутизаторов, а затем снова рассылает новое значение вектора по сети. В конце концов, каждый маршрутизатор узнает информацию обо всех имеющихся в интерсети сетях и о расстоянии до них через соседние маршрутизаторы.

Дистанционно-векторные алгоритмы хорошо работают только в небольших сетях, В больших сетях они засоряют линии связи интенсивным широковещательным трафиком, к тому же изменения конфигурации могут отрабатываться по этому алгоритму не всегда корректно, так как маршрутизаторы не имеют точного представления о топологии связей в сети, а располагают только обобщенной информацией - вектором дистанций, к тому же полученной через посредников. Работа маршрутизатора в соответствии с дистанционно-векторным протоколом напоминает работу моста, так как точной топологической картины сети такой маршрутизатор не имеет.

Наиболее распространенным протоколом, основанным на дистанционно-векторном алгоритме, является протокол RIP, который распространен в двух версиях - RIP IP, работающий с протоколом IP, и RIP IPX, работающий с протоколом IPX.

Алгоритмы состояния связей обеспечивают каждый маршрутизатор информацией, достаточной для построения точного графа связей сети. Все маршрутизаторы работают на основании одинаковых графов, что делает процесс маршрутизации более устойчивым к изменениям конфигурации. «Широковещательная» рассылка (то есть передача пакета всем непосредственным соседям маршрутизатора) используется здесь только при изменениях состояния связей, что происходит в надежных сетях не так часто. Вершинами графа являются как маршрутизаторы, так и объединяемые ими сети. Распространяемая по сети информация состоит из описания связей различных типов: маршрутизатор - маршрутизатор, маршрутизатор - сеть,

Чтобы понять, в каком состоянии находятся линии связи, подключенные к его портам, маршрутизатор периодически обменивается короткими пакетами HELLO со своими ближайшими соседями. Этот служебный трафик также засоряет сеть, но не в такой степени как, например, RIP-пакеты, так как пакеты HELLO имеют намного меньший объем.

Протоколами, основанными на алгоритме состояния связей, являются протоколы IS-IS (Intermediate System to Intermediate System) стека OSI, OSPF (Open Shortest Path First) стека TCP/IP и недавно реализованный протокол NLSP стека Novell.

Forwarding - переадресация ????

Выводы (общие)

- **Маршрут** - это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до пункта назначения. Задачу выбора маршрута из нескольких возможных решают **маршрутизаторы** и конечные узлы на основе таблиц маршрутизации. Записи в таблицу могут заноситься вручную администратором и автоматически протоколами маршрутизации.
- Протоколы маршрутизации (например, RIP или OSPF) следует отличать от собственно сетевых протоколов (например, IP или IPX). В то время как первые собирают и передают по сети чисто служебную информацию о возможных маршрутах, вторые предназначены для передачи пользовательских данных.
- Сетевые протоколы и протоколы маршрутизации реализуются в виде программных модулей на конечных узлах-компьютерах и на промежуточных узлах - маршрутизаторах.
- **Маршрутизатор** представляет собой сложное многофункциональное устройство, в задачи которого входит: построение таблицы маршрутизации, определение на ее основе маршрута, буферизация, **фрагментация** и фильтрация поступающих пакетов, поддержка сетевых интерфейсов. Функции маршрутизаторов могут выполнять как специализированные устройства, так и универсальные компьютеры с соответствующим программным обеспечением.
- Для **алгоритмов маршрутизации** характерны одношаговый и многошаговый подходы. **Одношаговые** алгоритмы делятся на алгоритмы фиксированной, простой и адаптивной маршрутизации. Адаптивные протоколы маршрутизации являются наиболее распространенными и в свою очередь могут быть основаны на дистанционно-векторных алгоритмах и алгоритмах состояния связей.
- Важной особенностью протокола IP, отличающей его от других сетевых протоколов, является его способность выполнять динамическую **фрагментацию пакетов** при передаче их между **сетями с различными MTU**. Это свойство во многом способствовало тому, что протокол IP смог занять доминирующие позиции в сложных составных сетях.

Протоколы маршрутизации (Коротко — схемы-тезисы)

1. Подход (алгоритмы)
   - Одношаговый
   - Многошаговый - маршрутизация от источника (Source Routing)

   1.1. Одношаговые алгоритмы делятся на три класса:
   - алгоритмы фиксированной (или статической) маршрутизации;
   - алгоритмы простой маршрутизации;
   - алгоритмы адаптивной (или динамической) маршрутизации.

   1.1.2. Выделяют три типа простой маршрутизации:
   - случайная маршрутизация;
   - лавинная маршрутизация;
   - маршрутизация по предыдущему опыту.

   1.1.3. Самыми распространенными являются алгоритмы адаптивной (или динамической) маршрутизации

   Адаптивные алгоритмы должны отвечать требованиям.
   1) Обеспечивать, оптимальность/рациональность маршрута.
   2) Должны быть достаточно простыми, (чтобы при не тратилось слишком много сетевых ресурсов, небольшой объем вычислений).
   3) Должны обладать свойством сходимости (однозначный результат за приемлемое время).

   Адаптивные протоколы обмена маршрутной информацией делятся на две группы, каждая из которых связана с одним из следующих типов алгоритмов:
   - дистанционно-векторные алгоритмы (Distance Vector Algorithms, DVA);
   - алгоритмы состояния связей (Link State Algorithms, LSA).

Альтернативный ответ к билету№29 (из [2] -20)

20. Проблема и общие алгоритмы маршрутизации.

Проблема выбора наилучшего пути и ее решение является главной задачей сетевого уровня. Эта проблема осложняется тем, что самый короткий путь не всегда самый лучший. Часто критерием при выборе маршрута является время передачи данных по этому маршруту, оно

зависит от пропускной способности каналов связи и интенсивности трафика, которая может изменяться с течением времени.

Протоколы маршр-ии м/б построены на основе разных алгоритмов, отличающихся способами построения таблиц маршр-ии, способами выбора наилучшего маршрута и другими особенностями своей работы. Для алгоритмов маршрутизации характерны одношаговый и многошаговый подходы. Одношаговые алгоритмы (при выборе маршрута определяется только следующий (ближайший) router, а не вся последовательность router'ов от начала до конечного узла). От способа формирования таблиц маршр-ии: алгоритмы фиксированной, простой и адаптивной маршр-ии. Фиксированная маршр-ия - все записи в таблице являются статическими. Админ сети сам решает, на какие router'ы надо передавать пакеты с теми или иными адресами, и вручную заносит соответствующие записи в таблицу маршр-ии. Таблица создается в процессе загрузки, исп-ся без изменений до тех пор, пока ее содержимое не будет отредактировано вручную. Простая маршр-ия - таблица либо вовсе не используется, либо строится без участия протоколов маршр-ии. 3 типа простой маршр-ии: случайная - прибывший пакет посылается в первом попавшем случайном направлении, кроме исходного; лавинная маршрутизация - пакет широковещательно посылается по всем возможным направлениям, кроме исходного; маршрутизация по предыдущему опыту - выбор маршрута осуществляется по таблице, но таблица строится по принципу моста путем анализа адресных полей пакетов, появляющихся на входных портах. Адаптивная маршрутизация - обеспечивает авто обновление таблиц маршр-ии после изменения конфигурации сети. Протоколы, построенные на адаптивных алгоритмах, позволяют всем router'ам собирать инфу о топологии связей в сети, отрабатывая все изменения конфиг-ии связей. В таблицах маршр-ии обычно имеется инфа об интервале времени, в течение кот данный маршрут будет оставаться действительным.

Многошаговый подход — узел-источник задает в пакете полный маршрут его следования ч/з все промежуточные маршрутизаторы. Нет необх-ти строить и анализировать табл марш-ии. Это ускоряет прохождение пакета по сети, разгружает маршрутизаторы, но больше загружает конечные узлы.

Альтернативный ответ к билету №29 (из [2] -21)

21. Маршрутизаторы. Типовые характеристики современных маршрутизаторов.

По областям применения маршрутизаторы делятся на несколько классов.

Магистральные маршрутизаторы (backbone routers) предназначены для построения центральной сети корпорации. Центральная сеть может состоять из большого количества локальных сетей, разбросанных по разным зданиям и использующих самые разнообразные сетевые технологии, типы компьютеров и операционных систем. Магистральные маршрутизаторы - это наиболее мощные устройства, способные обрабатывать несколько сотен тысяч или даже несколько миллионов пакетов в секунду, имеющие большое количество интерфейсов локальных и глобальных сетей. Поддерживаются не только среднескоростные интерфейсы глобальных сетей, такие как T1/E1, но и высокоскоростные, например, ATM или SDH со скоростями 155 Мбит/с или 622 Мбит/с. Чаще всего магистральный маршрутизатор конструктивно выполнен по модульной схеме на основе шасси с большим количеством слотов. Большое внимание уделяется в магистральных моделях надежности и отказоустойчивости маршрутизатора, которая достигается за счет системы терморегуляции, избыточных источников питания, заменяемых «на ходу» (hot swap) модулей, а также симметричного мультипроцессирования.

Маршрутизаторы региональных отделений соединяют региональные отделения между собой и с центральной сетью. Сеть регионального отделения, так же как и центральная сеть, может состоять из нескольких локальных сетей. Такой маршрутизатор обычно представляет собой некоторую упрощенную версию магистрального маршрутизатора. Если он выполнен на основе шасси, то количество слотов его шасси меньше. Возможен также конструктив с фиксированным количеством портов. Поддерживаемые интерфейсы локальных и глобальных сетей менее скоростные. Это наиболее обширный класс выпускаемых маршрутизаторов, характеристики которых могут приближаться к характеристикам магистральных маршрутизаторов, а могут и опускаться до характеристик маршрутизаторов удаленных офисов.

Маршрутизаторы удаленных офисов соединяют, как правило, единственную локальную сеть удаленного офиса с центральной сетью или сетью регионального отделения по глобальной связи. В max варианте такие маршрутизаторы могут поддерживать и два интерфейса локальных сетей. Как правило, интерфейс локальной сети - это Ethernet 10 Мбит/с, а интерфейс глобальной сети - выделенная линия со скоростью 64 Кбит/с, 1,544 или 2 Мбит/с. М.у.о. может поддерживать работу по коммутируемой телефонной линии в качестве резервной связи для выделенного канала. Существует. очень большое кол-во типов м.у.о. Это объясняется как массовостью потенциальных потребителей, так и специализацией такого типа устройств, проявляющейся в поддержке одного конкретного типа глобальной связи.

Маршрутизаторы локальных сетей (коммутаторы 3-го уровня) предназначены для разделения крупных локальных сетей на подсети. Основное требование, предъявляемое к ним, - высокая скорость

маршрутизации, так как в такой конфигурации отсутствуют низкоскоростные порты, такие как модемные порты 33,6 Кбит/с или цифровые порты 64 Кбит/с. Все порты имеют скорость по крайней мере 10 Мбит/с, а многие работают на скорости 100 Мбит/с. В зависимости от области применения маршрутизаторы обладают различными основными и дополнительными техническими характеристиками.

Основные технические характеристики маршрутизатора связаны с тем, как он решает свою главную задачу - маршрутизацию пакетов в составной сети. Именно эти характеристики прежде всего определяют возможности и сферу применения того или иного маршрутизатора. Общая производительность маршрутизатора. Высокая производительность маршрутизации важна для работы с высокоскоростными локальными сетями, а также для поддержки новых высокоскоростных глобальных технологий, таких как frame relay, T3/E3, SDH и ATM.

Общая производительность маршрутизатора зависит от многих факторов, наиболее важными из которых являются: тип используемых процессоров, эффективность программной реализации протоколов, архитектурная организация вычислительных и интерфейсных модулей. Наиболее производительные маршрутизаторы имеют мультипроцессорную архитектуру, сочетающую симметричные и асимметричные свойства - несколько мощных центральных процессоров по симметричной схеме выполняют функции вычисления таблицы маршрутизации, а менее мощные процессоры в интерфейсных модулях занимаются передачей пакетов на подключенные к ним сети и пересылкой пакетов на основании части таблицы маршрутизации, кэшированной в локальной памяти интерфейсного модуля.

Магистральные маршрутизаторы обычно поддерживают максимальный набор протоколов и интерфейсов и обладают высокой общей производительностью в один-два миллиона пакетов в секунду. Маршрутизаторы удаленных офисов поддерживают один-два протокола локальных сетей и низкоскоростные глобальные протоколы, общая производительность таких маршрутизаторов обычно составляет от 5 до 20-30 тысяч пакетов в секунду. Маршрутизаторы региональных отделений занимают промежуточное положение, поэтому их иногда не выделяют в отдельный класс устройств.

Фрагментация и определение MTU пути

(к билету 29 из [4*] *см. файл 4.4.19 Кодирование меток в MPLS.doc***)**

Поскольку возможно получение непомеченной IP-дейтограммы, которая слишком велика, чтобы быть передана в выходной канал, имеется возможность получения помеченного пакета, который также невозможно передать по этой причине на выход.

Возможно также, что полученный пакет (помеченный или нет), который первоначально был достаточно мал для передачи через канал, становится слишком большим, получив одну или более меток. При коммутации меток, пакет может расти в размере, если в его стек заносятся дополнительные метки. Таким образом, если получен помеченный пакет с 1500-байтовым полем данных, и в него записана дополнительная метка, переадресовать нужно будет пакет с размером 1504-байта.

В этом разделе специфицируются правила обработки помеченных пакетов, которые являются "слишком большими". В частности, речь идет о правилах, которые гарантируют, что ЭВМ, использующие определение MTU пути [4], и ЭВМ, работающие с IPv6 [7,8], будут способны формировать IP-дейтограммы, которые не нуждаются в фрагментации, даже если эти дейтограммы получили дополнительные метки при прохождении через сеть.

Вообще, ЭВМ IPv4, которые не используют определение MTU пути [4], посылают IP-дейтограммы, содержащие не более 576 байт. Так как большинство используемых MTU равняются 1500 байт или больше, вероятность того, что такие дейтограммы будут нуждаться в фрагментации, даже если они помечены, весьма мала.

Некоторые ЭВМ, которые не используют определение MTU пути [4], формируют IP-дейтограммы, содержащие 1500 байт. Поскольку IP-адреса отправителя и получателя в одной и той же субсети, эти дейтограммы не проходят через маршрутизаторы, и, следовательно, не будут фрагментироваться

Если же IP-адрес отправителя и получателя находятся в разных автономных системах, это единственный случай, когда имеется риск фрагментации при пометке пакета.

В этом документе специфицированы процедуры, которые позволяют конфигурировать сеть так, что большие дейтограммы от ЭВМ, не использующих определение MTU пути, фрагментируются только раз, когда они впервые помечены. Эти процедуры делают возможным избежать фрагментации пакетов, которые уже помечены.

! *Ссылки [4] в тексте относятся к данной библиографии, а не к источнику в заголовке (номера совпали)*

30. Особенности и отличия IPv6, обеспечение обратной совместимости с IPv4, новая функциональность и проблемы внедрения.

Википедия IPv6-wiki.doc:

IPv6 (англ. Internet Protocol version 6) — новая версия протокола IP, призванная решить проблемы, с которыми столкнулась предыдущая версия (IPv4) при её использовании в Интернете, за счёт использования длины адреса **128 бит вместо 32**. В настоящее время протокол IPv6 уже используется в нескольких сотнях сетей по всему миру (более 1600 сетей на март 2009), но пока ещё не получил столь широкого распространения в Интернете, как IPv4. В России практически не используется. Протокол был разработан IETF.

По прогнозам, после того, как адресное пространство в IPv4 закончится (предположительно 2011—2012 г.), два стека протоколов — IPv6 и IPv4 будут использоваться параллельно (англ. dual stack), с постепенным увеличением доли трафика IPv6 по сравнению с IPv4. Такая ситуация станет возможной из-за наличия огромного количества устройств, в том числе устаревших, не поддерживающих IPv6 и требующих специального преобразования для работы с устройствами, использующими только IPv6.

Сравнение с IPv4

Пропагандисты IPv6 утверждают, что новый протокол обеспечивает 5•1028 адресов на каждого жителя Земли. Это не так — столь огромное адресное пространство сделано ради иерархичности адресов (это упрощает маршрутизацию) и бóльшая его часть в принципе не будет задействована. Тем не менее, увеличенное пространство адресов сделает NAT необязательным.

Из IPv6 убраны вещи, усложняющие работу маршрутизаторов:

- Маршрутизаторы больше не разбивают пакет на части (возможно разбиение пакета с передающей стороны). Соответственно оптимальный MTU придётся искать через Path MTU discovery. Для лучшей работы протоколов, требовательных к потерям, минимальный MTU поднят до 1280 байтов. Информация о разбиении пакетов вынесена из основного заголовка в расширенные;
- Исчезла контрольная сумма. С учётом того, что канальные (Ethernet) и транспортные (TCP) протоколы тоже проверяют корректность пакета, контрольная сумма на уровне IP воспринимается как излишняя. Тем более каждый роутер уменьшает hop limit на единицу, что в IPv4 приводило к пересчёту суммы.

Несмотря на огромный размер адреса IPv6, благодаря этим улучшениям заголовок пакета удлинился всего лишь вдвое: с 20 до 40 байт.

Улучшения IPv6 по сравнению с IPv4:

- На сверхскоростных сетях возможна поддержка огромных пакетов (джамбограмм) — до 4 гигабайт;
- Time to Live переименовано в Hop limit;
- Появились метки потоков и классы трафика;
- Появилось многоадресное вещание;
- Протокол IPSec из желательного превратился в обязательный.

Метки потоков

Введение в протоколе IPv6 поля «Метка потока» позволяет значительно упростить процедуру маршрутизации однородного потока пакетов. Поток — это последовательность пакетов, посылаемых отправителем определённому адресату. При этом предполагается, что все пакеты данного потока должны быть подвергнуты определённой обработке. Характер данной обработки задаётся дополнительными заголовками.

Допускается существование нескольких потоков между отправителем и получателем. Метка потока присваивается узлом-отправителем путём генерации псевдослучайного 20-битного числа. Все пакеты одного потока должны иметь одинаковые заголовки, обрабатываемые маршрутизатором....далее см. IPv6.doc [3]

шпоргалка:

Версии IP. Протокол IPv6 оставляет основные принципы IPv4 неизменными. К ним относятся дейтаграммный метод работы, фрагментация пакетов, разрешение отправителю задавать максимальное число хостов для своих пакетов. Существенное отличие это то, что IPv6 использует **128-битные** адреса. Как и в версии IPv4, адреса в версии **IPv6** делятся на классы, в зависимости от значения нескольких старших бит адреса. Для обеспечения совместимости со схемой адресации версии IPv4, в версии IPv6 имеется класс адресов, имеющих 0000 0000 в старших битах адреса. Младшие 4 байта адреса этого класса должны содержать адрес IPv4. Роутеры, поддерживающие обе версии адресов, должны обеспечивать трансляцию при передаче пакета из сети, поддерживающей адресацию IPv4, в сеть, поддерживающую адресацию IPv6, и наоборот. [2]

Олифер:

С ростом сети задача распределения адресов стала слишком сложной, наблюдается дефицит IP-адресов. дефицит обусловлен не только ростом сетей, но и тем, что имеющееся множество IP-адресов используется нерационально.

Для смягчения проблемы дефицита адресов разработчики стека TCP/IP предлагают разные подходы. Принципиальным решением является переход на новую версию **IPv6**, в которой резко расширяется адресное пространство за счет использования **16-байтных** адресов. Однако и текущая версия IPv4 поддерживает некоторые технологии, направленные на более экономное расходование IP-адресов. Одной из таких технологий является технология масок и ее развитие - технология бесклассовой междоменной маршрутизации (Classless Inker-Domain Routing, **CIDR)** далее см. билет№28 (Технология CIDR)

Другая технология, которая может быть использована для снятия дефицита адресов, это трансляция адресов (Network Address Translator, NAT). Узлам внутренней сети адреса назначаются произвольно (естественно, в соответствии с общими правилами, определенными в стандарте), так, как будто эта сеть работает автономно. Внутренняя сеть соединяется с Internet через некоторое промежуточное устройство (маршрутизатор, межсетевой экран). Это промежуточное устройство получает в свое распоряжение некоторое количество внешних «нормальных» IP-адресов, согласованных с поставщиком услуг или другой организацией, распределяющей IP-адреса. Промежуточное устройство способно преобразовывать внутренние адреса во внешние, используя для этого некие таблицы соответствия. Для внешних пользователей все многочисленные узлы внутренней сети выступают под несколькими внешними IP-адресами. При получении внешнего запроса это устройство анализирует его содержимое и при необходимости пересылает его во внутреннюю сеть, заменяя IP-адрес на внутренний адрес этого узла. Процедура трансляции адресов определена в RFC 1631. *(см [1] стр.33-35)*

Технология CIDR уже успешно используется в текущей версии IPv4 и поддерживается такими протоколами маршрутизации, как OSPF, RIP-2, BGP4. Предполагается, что эти же протоколы будут работать и с новой версией протокола IPv6. Следует отметить, что в настоящее время технология CIDR поддерживается магистральными маршрутизаторами Internet, а не обычными хостами в локальных сетях.

Использование CIDR в сетях IPv4 в общем случае требует перенумерации сетей. Поскольку эта процедура сопряжена с определенными временными и материальными затратами, для ее проведения пользователей нужно каким-либо образом стимулировать. В качестве таких стимулов рассматривается, например, введение оплаты за строку в таблице маршрутизации или же за количество узлов в сети. При использовании классов сетей абонент часто не полностью занимает весь допустимый диапазон адресов узлов - 254 адреса для сети класса С или 65 534 адреса для сети класса В. Часть адресов узлов обычно пропадает. Требование оплаты каждого адреса узла поможет пользователю решиться на перенумерацию, с тем чтобы получить ровно столько адресов, сколько ему нужно. *(см [1] стр.73-74)*

1 Байт=8 бит=2^3

16-байт=$2^4 \cdot 2^3 = 2^{4+3} = 2^7$ (Ipv6)

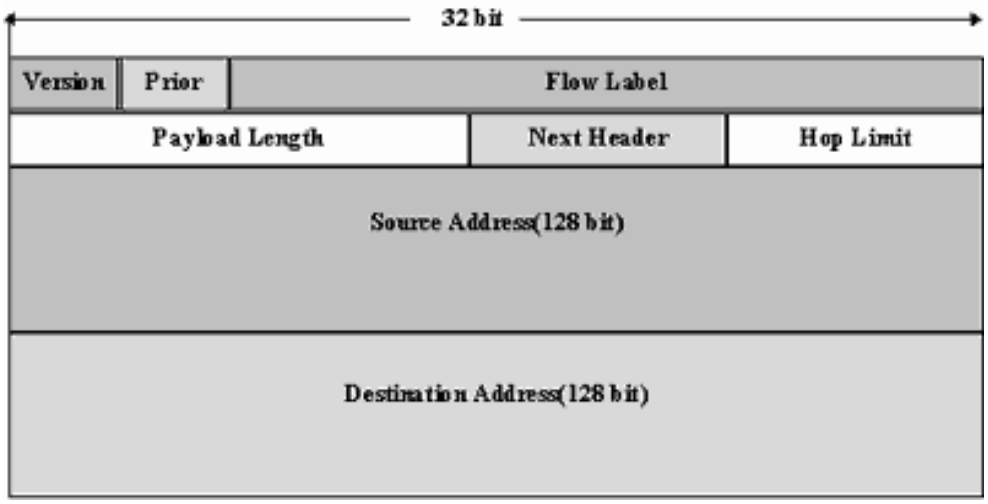
128-бит=2^7 (Ipv6)

32-бит=$2^5 = 2^{2+3} = 2^2 \cdot 2^3$==4 байта (Ipv4)

Стандарт IPv6 [5] (см.слайды 21– 25 из it_net_04.ppt)

- В 1995 года IETF выпустило предложения по новому стандарту протокола IP – IPv6.
- В новом протоколе:
  - используются более длинные поля для адреса хоста,
  - введены новые типы адресов,
  - упрощена структура заголовка пакета,
  - введена идентификация типа информационных потоков для увеличения эффективности обмена данными,
  - введены поля идентификации и конфиденциальности информации.

Формат заголовка IPv6 пакета



- В заголовке поле **Version "версия"** - номер версии IP, равное 6.
- Поле **Prior "приоритет"** может принимать значения от 0 до 15. Первые 8 значений закреплены за пакетами, требующими контроля переполнения, например,
  - 0 - несимвольная информация;
  - 1 - информация заполнения (news),
  - 2 - не критичная ко времени передача данных (e-mail);
  - 4 - передача данных режима on-line (FTP, HTTP, NFS и т.п.);
  - 6 - интерактивный обмен данными (telnet, X);
  - 7 - системные данные или данные управления сетью (SNMP, RIP и т.п.).

Формат заголовка протокола

- Поле **Flow label "метка потока"** предполагается использовать для оптимизации маршрутизации пакетов.
  - В IPv6 вводится понятие потока, который состоит из пакетов. Пакеты потока имеют одинаковый адрес отправителя и одинаковый адрес получателя и ряд других одинаковых опций.
- Поле **Next Header "следующий заголовок"** определяет тип следующего за заголовком IP-заголовка.
- Поле **Hop Limit "ограничение переходов"** определяет число промежуточных шлюзов, которые ретранслируют пакет в сети.
  - При прохождении шлюза это число уменьшается на единицу. При достижении значения "0" пакет уничтожается.
- После первых 8 байтов в заголовке указываются адрес отправителя пакета и адрес получателя пакета. Каждый из этих адресов имеет длину 16 байт.
- Длина заголовка IPv6 составляет 48 байтов.

Адрес в протоколе IPv6

- Шестнадцать байт IP-адреса для IPv6 выглядят достаточными для удовлетворения любых потребностей Internet.
- Не все 2128 адресов можно использовать в качестве адреса сетевого интерфейса в сети.
- Предполагается выделение отдельных групп адресов, согласно специальным префиксам внутри IP-адреса, подобно тому, как это делалось при определении типов сетей в IPv4.
- Двоичный префикс "0000 010" предполагается закрепить за отображением IPX-адресов в IP-адреса.
- В новом стандарте выделяются несколько типов адресов:
  - **unicast addresses** - адреса сетевых интерфейсов,
  - **anycast addresses** - адреса не связанные с конкретным сетевым интерфейсом, но и не связанные с группой интерфейсов
  - **multicast addresses** - групповые адреса.
- Разница между последними двумя группами адресов в том, что anycast address это адрес конкретного получателя, но определяется адрес сетевого интерфейса только в локальной сети, где этот интерфейс подключен, а multicast-сообщение предназначено группе интерфейсов, которые имеют один multicast-адрес.

Маршрутизация и другие возможности

- В стандарт добавлены три новых возможности маршрутизации:
  - **маршрутизация поставщика IP-услуг,**
  - **маршрутизация мобильных узлов**
  - **автоматическая переадресация.**
- Эти функции реализуются путем прямого указания промежуточных адресов шлюзов при маршрутизации пакета. Эти списки помещаются в дополнительных заголовках, которые можно вставлять вслед за заголовком IP-пакета.
- Кроме перечисленных возможностей, новый протокол позволяет улучшить защиту IP-трафика. Для этой цели в протоколе предусмотрены специальные опции.
  - Первая опция предназначена для защиты от подмены IP-адресов машин. При ее использовании нужно кроме адреса подменять и содержимое поля идентификации, что усложняет задачу злоумышленника, который маскируется под другую машину.
  - Вторая опция связана с шифрацией трафика.

30 из Семёнова [4]

См. файлы 4.4.11.5 Бесклассовая интердоменная маршрутизация CIDR.doc и 4.1.1.3 Интернет в Ethernet CIDR+VLSM.doc)

...В связи с дефицитом адресов в сетке **IPv4** в последнее время все шире стала использоваться схема адресации supernet и маршрутизации без классов (**CIDR** -Ckassless Interdomain Routing). Эта технология появилась в 1993 году одновременно с появлением протокола **BGP-4**. Протокол CIDR формирует маршруты на базе непрерывных полей IP-адресов. В варианте без классов группа адресов представляется как единая сеть. Деление адресного пространства на подсети не имеет никакого отношения к протоколу CIDR. Адресное пространство CIDR может содержать любое число адресов с числом 2 в любой степени. Ниже в таблице представленя параметры сетевых адресов без классов.

См. также 4.4.1.1 Адресация IPv6.doc (коротко –см. ниже)

IPv6 представляет собой новую версию протокола Интернет (RFC-1883), являющуюся преемницей версии 4 (IPv4; RFC-791).

Изменения IPv6 по отношению к IPv4 можно поделить на следующие группы:

- **Расширение адресации**

В IPv6 длина адреса расширена до 128 бит (против 32 в IPv4), что позволяет обеспечить больше уровней иерархии адресации, увеличить число адресуемых узлов, упростить авто-конфигурацию. Для расширения возможности мультикастинг-маршрутизации в адресное поле введено субполе "scope" (группа адресов). Определен новый тип адреса "anycast address" (эникастный), который используется для посылки запросов клиента любой группе серверов. Эникаст адресация предназначена для использования с набором взаимодействующих серверов, чьи адреса не известны клиенту заранее.

- **Спецификация формата заголовков**

Некоторые поля заголовка IPv4 отбрасываются или делаются опционными, уменьшая издержки, связанные с обработкой заголовков пакетов с тем, чтобы уменьшить влияние расширения длины адресов в IPv6.

- **Улучшенная поддержка расширений и опций**

Изменение кодирования опций IP-заголовков позволяет облегчить переадресацию пакетов, ослабляет ограничения на длину опций, и делает более доступным введение дополнительных опций в будущем.

- **Возможность пометки потоков данных**

Введена возможность помечать пакеты, принадлежащие определенным транспортным потокам, для которых отправитель запросил определенную процедуру обработки, например, нестандартный тип TOS (вид услуг) или обработка данных в реальном масштабе времени.

- **Идентификация и защита частных обменов**

В IPv6 введена спецификация идентификации сетевых объектов или субъектов, для обеспечения целостности данных и при желании защиты частной информации.

Формат и семантика адресов IPv6 описаны в документе RFC-1884. Версия ICMP IPv6 рассмотрена в RFC-1885.

30 продолжение

Википедия IP_IPv4+IPv6_wiki_A3.doc

Версия 4

В современной сети Интернет используется IP четвёртой версии, также известный как **IPv4**. В протоколе IP этой версии каждому узлу сети ставится в соответствие IP-адрес длиной 4 октета (4 байта). При этом компьютеры в подсетях объединяются общими начальными битами адреса. Количество этих бит, общее для данной подсети, называется маской подсети (ранее использовалось деление пространства адресов по классам — A, B, C; класс сети определялся диапазоном значений старшего октета и определял число адресуемых узлов в данной сети, сейчас используется бесклассовая адресация).

Версия 6

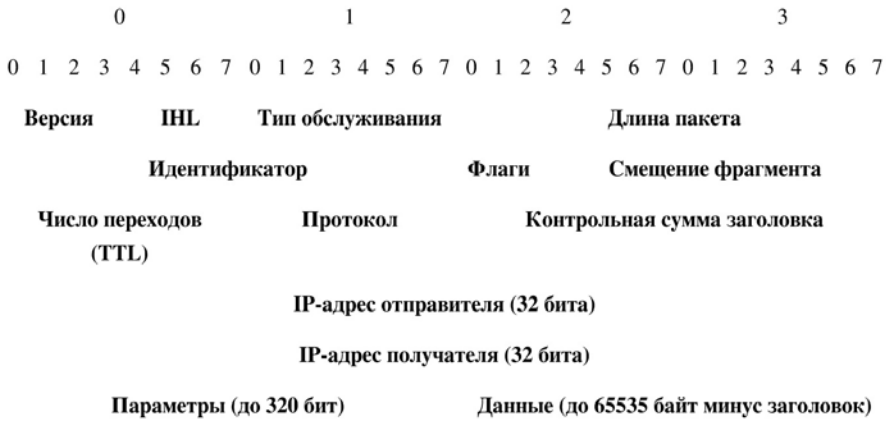
В настоящее время вводится в эксплуатацию шестая версия протокола — IPv6, которая позволяет адресовать значительно большее количество узлов, чем IPv4. Эта версия отличается повышенной разрядностью адреса, встроенной возможностью шифрования и некоторыми другими особенностями. Переход с IPv4 на IPv6 связан с трудоёмкой работой операторов связи и производителей программного обеспечения и не может быть выполнен одномоментно. На начало 2007 года в Интернете присутствовало около 760 сетей, работающих по протоколу IPv6. Для сравнения, на то же время в адресном пространстве IPv4 присутствовало более 203 тысяч сетей, но в IPv6 сети гораздо более крупные, нежели в IPv4.

Пакет (датаграмма)

IP-пакет — форматированный блок информации, передаваемый по вычислительной сети. Соединения вычислительных сетей, которые не поддерживают пакеты, такие как традиционные соединения типа «точка-точка» в телекоммуникациях, просто передают данные в виде последовательности байтов, символов или битов. При использовании пакетного форматирования сеть может передавать длинные сообщения более надежно и эффективно.

Версия 4 (IPv4)

то же, крупно



- Версия — для IPv4 значение поля должно быть равно 4.
- IHL — длина заголовка IP-пакета в 32-битных словах (dword). Именно это поле указывает на начало блока данных в пакете. Минимальное корректное значение для этого поля равно 5.
- Идентификатор — значение, назначаемое отправителем пакета и предназначенное для определения корректной последовательности фрагментов при сборке датаграммы. Для фрагментированного пакета все фрагменты имеют одинаковый идентификатор.
- 3 бита флагов. Первый бит должен быть всегда равен нулю, второй бит DF (don't fragment) определяет возможность фрагментации пакета и третий бит MF (more fragments) показывает, не является ли этот пакет последним в цепочке пакетов.
- Смещение фрагмента — значение, определяющее позицию фрагмента в потоке данных.
- Протокол — идентификатор интернет-протокола следующего уровня (см. IANA protocol numbers и RFC 1700). В IPv6 называется «Next Header».

Версия 6 (IPv6)

Позиция в октетах		0								1								2								3							
	Позиция в битах	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Версия				Класс трафика								Метка потока																			
4	32	Длина полезной нагрузки																След. заголовок								Число переходов							
8	64	IP-адрес отправителя																															
12	96																																
16	128																																
20	160																																
24	192	IP-адрес получателя																															
28	224																																
32	256																																
36	288																																

- Версия — для IPv6 значение поля должно быть равно 6.
- Класс трафика — определяет приоритет трафика (QoS, класс обслуживания).
- Метка потока — уникальное число, одинаковое для однородного потока пакетов.
- Длина полезной нагрузки — длина данных (заголовок IP-пакета не учитывается).
- Следующий заголовок — Определяет следующий инкапсулированный протокол.
- Число переходов — максимальное число маршрутизаторов, которые может пройти пакет. При прохождении маршрутизатора это значение уменьшается на единицу и по достижении нуля пакет отбрасывается.

Диапазоны для локальных сетей

При подключении пользовательского компьютера к Интернету, IP-адреса выбираются из диапазона, предоставленного провайдером. Компьютеры, не имеющие IP-адреса, выданного провайдером, могут (при правильной настройке маршрутизации[1]) работать с другими локальными компьютерами, имея IP-адреса из диапазонов, зарезервированных для локальных сетей (RFC 1918)[2]:

- 10.0.0.0 — 10.255.255.255 (одна подсеть класса A или 16777216 (2^{24}) адресов)
- 172.16.0.0 — 172.31.255.255 (16 подсетей класса B по 65536 (2^{16}) адресов; всего — 1048576)
- 192.168.0.0 — 192.168.255.255 (256 подсетей класса C по 256 адресов; всего — 65536)
- сеть 2001:0DB8::/32 в IPv6 — зарезервировано для примеров и документации

Компьютеры с такими адресами могут получать доступ к Интернету посредством прокси-серверов или NAT. Иногда в компьютерном сленге адреса из указанных диапазонов для локальных сетей называются серыми или плю́шевыми IP.

При построении сетей, составляющих Интернет (например, сетей провайдеров), выбираются строго определённые диапазоны адресов, назначенные организацией IANA (подконтрольна ICANN, «высшей инстанции» в вопросах резервирования диапазонов адресов) и имеет свои представительства по всему миру[4] — например, в Европе распределение адресов координирует RIPE NCC.

30 продолжение

Про IPv6

Надо отметить, что специалисты компании Novell приложили немало усилий, чтобы в новой версии 6 протокол IP приобрел некоторые черты, свойственные протоколу IPX, и тем самым облегчил переход пользователей IPX на **IPv6** (когда это станет практически необходимым). Обычно все три составляющие IPX-адреса, в том числе и номер сети, записываются в шестнадцатеричной форме. [1] *(см [1] стр.105)*

Существуют схемы и временным выделением резервного IP-адреса подвижному пользователю. Международный стандарт для решения проблемы работы с подвижными пользователями пока не разработан.

Одним из радикальных мер решения проблемы может стать географическая маршрутизация, которая станет возможной при массовом внедрении адресации **IPv6**.

При широком внедрении IPv6 с практически неограниченным ресурсом адресов проблемы выделения IP-адреса вообще не будет.
В последнее время конфигурирование сетевого оборудования (маршрутизаторов, DNS и почтовых серверов усложнилось настолько, что это стало составлять заметную часть издержек при формировании коммуникационного узла. Заметного упрощенияи удешевления маршрутизаторов можно ожидать при внедрении IPv6. [4]

Помимо классической схемы маршрутизации по адресу места назначения, часто используется вариант выбора маршрута отправителем (данный вариант получил дальнейшее развитие при введении стандарта **IPv6**). В этом случае IP-пакет содержит соответствующий код опции и список промежуточных адресов узлов, которые он должен посетить по пути к месту назначения.

Существенную проблему составляет необходимость идентифицировать пакеты, принадлежащие определенному процессу. Эта задача легко решается только в рамках протокола **IPv6.** Там в заголовке предусмотрено поле метка потока. Некоторые возможности предоставляет также протокол **MPLS** (4.4.17 Введение в MPLS, TE и QoS.doc)

В протоколе **IPv6** поле приоритет имеет 4 бита (см. IPv6). Биты C, D, T и R характеризуют пожелание относительно способа доставки дейтограммы. В таблице 1 приведены стандартизованные значения поля Type of Service (TOS) IP-пакета.

31. Доменная система имен.

Организация доменов и доменных имен

В стеке TCP/IP используются три типа адресов: локальные (называемые также аппаратными), IP-адреса и символьные доменные имена.

Символьные доменные имена. Символьные имена в IP-сетях называются доменными и строятся по иерархическому признаку. Составляющие полного символьного имени в IP-сетях разделяются точкой и перечисляются в следующем порядке: сначала простое имя конечного узла, затем имя группы узлов (например, имя организации), затем имя более крупной группы (поддомена) и так до имени домена самого высокого уровня (например, домена объединяющего организации по географическому принципу: RU - Россия, UK - Великобритания, SU - США), Примеров доменного имени может служить имя base2.sales.zil.ru. Между доменным именем и IP-адресом узла нет никакого алгоритмического соответствия, поэтому необходимо использовать какие-то дополнительные таблицы или службы, чтобы узел сети однозначно определялся как по доменному имени, так и по IP-адресу. В сетях TCP/IP используется специальная распределенная служба **Domain Name System (DNS)**, которая устанавливает это соответствие на основании создаваемых администраторами сети таблиц соответствия. Поэтому доменные имена называют также DNS-именами, [1, стр.28]

Для идентификации компьютеров аппаратное и программное обеспечение в сетях TCP/IP полагается на IP-адреса. Однако пользователи обычно предпочитают работать с символьными именами компьютеров, и операционные системы локальных сетей приучили их к этому удобному способу. Следовательно, в сетях TCP/IP должны существовать символьные имена хостов и механизм для установления соответствия между символьными именами и IP-адресами.

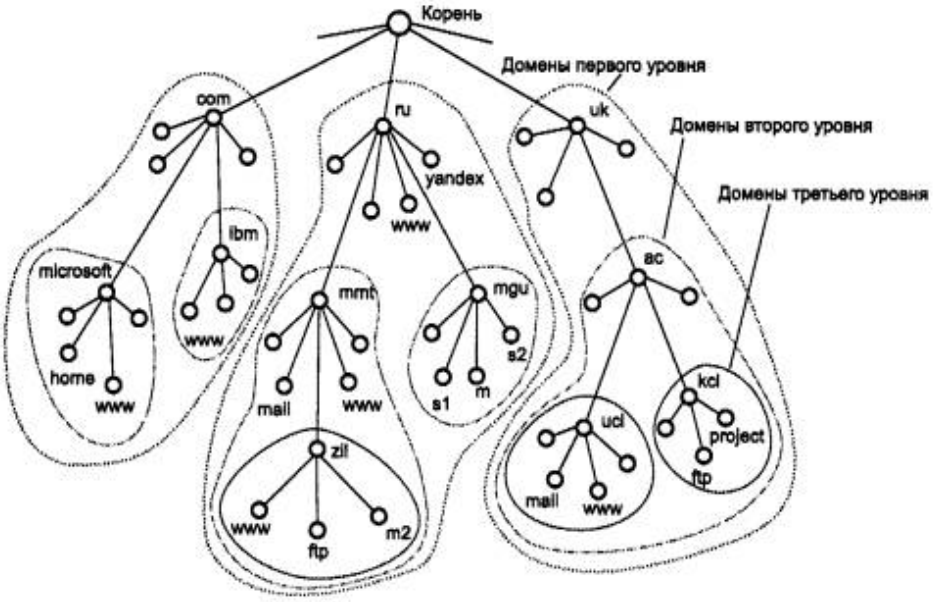
Так как локальные сети состояли из небольшого числа компьютеров, то использовались так называемые плоские имена, состоящие из последовательности символов, не разделенных на части. Примерами таких имен являются: NW1_1, mail2, MOSCOW_SALES_2.

Для стека TCP/IP, рассчитанного в общем случае на работу в больших территориально распределенных сетях, подобный подход оказывается неэффективным по нескольким причинам.

- не дают возможности разработать единый алгоритм обеспечения уникальности имен
- Широковещательный способ хорошо работает только в небольшой локальной сети, не разделенной на подсети. В крупных сетях, где общая широковещательность не поддерживается, нужен другой способ разрешения символьных имен.

Для эффективной организации именования компьютеров в больших сетях естественным является применение иерархических составных имен.

В стеке TCP/IP применяется **доменная система имен**, которая имеет иерархическую древовидную структуру, допускающую использование в имени произвольного количества составных частей (рис. 5.11).



Иерархия доменных имен аналогична иерархии имен файлов, принятой во многих популярных файловых системах. Дерево имен начинается с корня, обозначаемого здесь точкой (.). Затем следует старшая символьная часть имени, вторая по старшинству символьная часть имени и т. д. Младшая часть имени соответствует конечному узлу сети. В отличие от имен файлов, при записи которых сначала указывается самая старшая составляющая, затем составляющая более низкого уровня и т. д., запись доменного имени начинается с самой младшей составляющей, а заканчивается самой старшей. Составные части доменного имени отделяется друг от друга точкой.

Разделение имени на части позволяет **разделить административную ответственность** за назначение уникальных имен между различными людьми или организациями в пределах своего уровня иерархии.

Разделение административной ответственности позволяет решить проблему образования уникальных имен без взаимных консультаций между организациями, отвечающими за имена одного уровня иерархии. Очевидно, что должна существовать одна организация, отвечающая за назначение имен верхнего уровня иерархии.

Совокупность имен, у которых несколько старших составных частей совпадают, образуют **домен имен** (domain). Например, имена wwwl.zil.mmt.ru, ftp.zil.mmt.ru, yandex.ru и sl.mgu.ru входят в домен ru, так как все эти имена имеют одну общую старшую часть - имя ru. Другим примером является домен mgu.ru. Из представленных на рис. 5.11 имен в него входят имена sl.mgu.ru, s2.mgu.ru и rn.mgu.ru. Этот домен образуют имена, у которых две старшие части всегда равны rngu.ru. Имя www.mmt.ru в домен mgu.ru не входит, так как имеет отличающуюся составляющую mmt.

ВНИМАНИЕ *Термин «домен» очень многозначен, поэтому его нужно трактовать в рамках определенного контекста. Кроме доменов имен стека TCP/IP в компьютерной литературе также часто упоминаются домены Windows NT, домены коллизий н некоторые другие. Общим у всех этих терминов является то, что они описывают некоторое множество компьютеров, обладающее каким-либо определенным свойством.*

Если один домен входит в другой домен как его составная часть, то такой домен могут называть **поддоменом (subdomain)**, хотя название домен за ним также остается. Обычно поддомен называют по имени той его старшей составляющей, которая отличает его от других поддоменов. Например, поддомен mmt.ru обычно называют поддоменом (или доменом) mmt. Имя поддомену назначает администратор вышестоящего домена.

По аналогии с файловой системой, в доменной системе имен различают **краткие** имена, **относительные** имена и **полные** доменные имена. **Краткое имя** - это имя конечного узла сети: хоста или порта маршрутизатора. Краткое имя - это лист дерева имен. **Относительное имя** - это составное имя, начинающееся с некоторого уровня иерархии, но не самого верхнего. Например, wwwi.zil - это относительное имя. Полное доменное имя (fully qualified domain name, FQJDN) включает составляющие всех уровней иерархии, начиная от краткого имени и кончая корневой точкой: wwwl.zil.mmt.ru.

Необходимо подчеркнуть, что компьютеры входят в домен в соответствии со своими составными именами, при этом они могут иметь совершенно различные IP-адреса, принадлежащие к различным сетям и подсетям. Например, в домен mgu.ru могут входить хосты с адресами 132.13.34.15, 201.22.100.33,14.0.0.6. Доменная система имен реализована в сети Internet, но она может работать и как автономная система имен в крупной корпоративной сети, использующей стек TCP/IP, но не связанной с Internet.

В Internet корневой домен управляется центром InterNIC. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны следовать международному стандарту ISO 3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций - следующие обозначения:

- corn - коммерческие организации (например, microsoft.com);
- edu - образовательные (например, mitedu);
- gov - правительственные организации (например, nsf.gov);
- org - некоммерческие организации (например, fidonet.org);
- net - организации, поддерживающие сети (например, nsf.net).

Каждый домен администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Чтобы получить доменное имя, необходимо зарегистрироваться в какой-либо организации, которой InterNIC делегировал свои полномочия по распределению имен доменов. В России такой организацией является РосНИИРОС, которая отвечает за делегирование имен поддоменов в домене ru. [1, стр.40-43]

Система доменных имен DNS

Соответствие между доменными именами и IP-адресами может устанавливаться как средствами локального хоста, так и средствами централизованной службы. На раннем этапе развития Internet на каждом хосте вручную создавался текстовый файл с известным именем hosts. Этот файл состоял из некоторого количества строк, каждая из которых содержала одну пару «IP-адрес - доменное имя», например 102.54.94.97 - rhino.acme.com.

По мере роста Internet файлы hosts также росли, и создание масштабируемого решения для разрешения имен стало необходимостью.

Таким решением стала специальная служба **- система доменных имен (Domain Name System, DNS)**. **DNS** - это централизованная служба, основанная на распределенной базе отображений «доменное имя - IP-адрес». Служба DNS использует в своей работе протокол типа «клиент-сервер». В нем определены DNS-серверы и DNS-кли-енты. DNS-серверы поддерживают распределенную базу отображений, а DNS-клиен-ты обращаются к серверам с запросами о разрешении доменного имени в IP-адрес.

Служба DNS использует текстовые файлы почти такого формата, как и файл hosts, и эти файлы администратор также подготавливает вручную. Однако служба DNS опирается на иерархию доменов, и каждый сервер службы DNS хранит только часть имен сети, а не все имена, как это происходит при использовании файлов hosts. При росте количества узлов в сети проблема масштабирования решается созданием новых доменов и поддоменов имен и добавлением в службу DNS новых серверов.

Для каждого домена имен создается свой **DNS-сервер**. Этот сервер может хранить отображения «доменное имя - IP-адрес» для всего домена, включая все его поддомены. Однако при этом решение оказывается плохо масштабируемым, так как при добавлении новых поддоменов нагрузка на этот сервер может превысить его возможности. Чаще сервер домена хранит только имена, которые заканчиваются на следующем ниже уровне иерархии по сравнению с именем домена. (Аналогично каталогу файловой системы, который содержит записи о файлах и подкаталогах, непосредственно в него «входящих».) Именно при такой организации службы DNS нагрузка по разрешению имен распределяется более-менее равномерно между всеми DNS-серверами сети. Например, в первом случае DNS-сервер домена mmtru будет хранить отображения для всех имен, заканчивающихся на mmt.ru: wwwl.zil.mmt.ru, ftp.zil.mmt.ru, mail.mmt.ru и т. д. Во втором случае этот сервер хранит отображения только имен типа mail.mmt.ru, www.mmt.ru, а все остальные отображения должны храниться на DNS-сервере поддомена zil.

Каждый DNS-сервер кроме таблицы отображений имен содержит ссылки на DNS-серверы своих поддоменов. Эти ссылки связывают отдельные DNS-серверы в единую службу DNS. Ссылки представляют собой IP-адреса соответствующих серверов. Для обслуживания корневого домена выделено несколько дублирующих друг друга DNS-серверов, IP-адреса которых являются широко известными (их можно узнать, например, в InterNIC).

Процедура разрешения DNS-имени во многом аналогична процедуре поиска файловой системой адреса файла по его символьному имени. Действительно, в обоих случаях составное имя отражает иерархическую структуру организации соответствующих справочников - каталогов файлов или таблиц DNS. Здесь домен и доменный DNS-сервер являются аналогом каталога файловой системы. Для доменных имен, так же как и для символьных имен файлов, характерна независимость именования от физического местоположения.

Процедура поиска адреса файла по символьному имени заключается в последовательном просмотре каталогов, начиная с корневого. При этом предварительно проверяется кэш и текущий каталог. Для определения IP-адреса по доменному имени также необходимо просмотреть все DNS-серверы, обслуживающие цепочку поддоменов, входящих в имя хоста, начиная с корневого домена. Существенным же отличием является то, что файловая система расположена на одном компьютере, а служба DNS по своей природе является распределенной.

Существуют **две основные схемы разрешения DNS-имен**.

В первом варианте работу по поиску IP-адреса координирует DNS-клиент:

- DNS-клиент обращается к корневому DNS-серверу с указанием полного доменного имени;
- DNS-сервер отвечает, указывая адрес следующего DNS-сервера, обслуживающего домен верхнего уровня, заданный в старшей части запрошенного имени;
- DNS-клиент делает запрос следующего DNS-сервера, который отсылает его к DNS-серверу нужного поддомена, и т. д., пока не будет найден DNS-сервер, в котором хранится соответствие запрошенного имени IP-адресу. Этот сервер дает окончательный ответ клиенту.

Такая схема взаимодействия называется **нерекурсивной** или **итеративной**, когда клиент сам итеративно выполняет последовательность запросов к разным серверам имен. Так как эта схема загружает клиента достаточно сложной работой, то она применяется редко.

Во втором варианте реализуется **рекурсивная процедура**:

- DNS-клиент запрашивает локальный DNS-сервер, то есть тот сервер, который обслуживает поддомен, к которому принадлежит имя клиента;
- если локальный DNS-сервер знает ответ, то он сразу же возвращает его клиенту; это может соответствовать случаю, когда запрошенное имя входит в тот же поддомен, что и имя клиента, а также может соответствовать случаю, когда сервер уже узнавал данное соответствие для другого клиента и сохранил его в своем кэше;
- если же локальный сервер не знает ответ, то он выполняет итеративные запросы к корневому серверу и т. д. точно так же, как это делал клиент в первом варианте; получив ответ, он передает его клиенту, который все это время просто ждал его от своего локального DNS-сервера.

В этой схеме клиент перепоручает работу своему серверу, поэтому схема называется **косвенной** или **рекурсивной**. Практически все DNS-клиенты используют рекурсивную процедуру.

Для ускорения поиска IP-адресов DNS-серверы широко применяют процедуру кэширования проходящих через них ответов. Чтобы служба DNS могла оперативно отрабатывать изменения, происходящие в сети, ответы кэшируются на определенное время - обычно от нескольких часов до нескольких дней.

Выводы

- В стеке TCP/IP применяется **доменная система символьных имен**, которая имеет иерархическую древовидную структуру, допускающую использование в имени произвольного количества составных частей. Совокупность имен, у которых несколько старших составных частей совпадают, образуют **домен имен**. Доменные имена назначаются централизованно, если сеть является частью Internet, в противном случае - локально.
- Соответствие между доменными именами и IP-адресами может устанавливаться

— как средствами локального хоста с использованием файла hosts,

— так и с помощью централизованной службы DNS, основанной на распределенной базе отображений «доменное имя - IP-адрес».

Из Шпоргалки [2]

Domain Name System (DNS) — служба разрешения доменных имен, базовая для Интернета. В традиционной реализации DNS требует указывать статическое соотв м/у именем хоста и его адресом. Т.к. служба DNS не динамична, изменения в базе данных DNS необходимо делать вручную.

DNS-сервер (или сервер имен) - программа (1 или неск), обраб запросы типа: "определить IP-адрес по имени", "определить имя по IP-адресу", "определить имя сервера, на кот должна направлятся эл почта для заданного домена", "определить имя другого сервера имен, ответственного за заданный домен".

DNS (Domain Name System) - распределенная БД, поддерживающая иерархич систему имен для идентификации узлов в сети Internet. DNS-серверы хранят часть распределенной БД о соотв символьных имен и IP-адресов. DNS имеет структуру дерева, наз доменным пространством имен, в кот любой домен (узел дерева) имеет имя и может содержать поддомены. Имя домена идентифицирует его положение в этой БД по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена.

Корень базы данных DNS управляется центром Internet Network Information Center. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе.

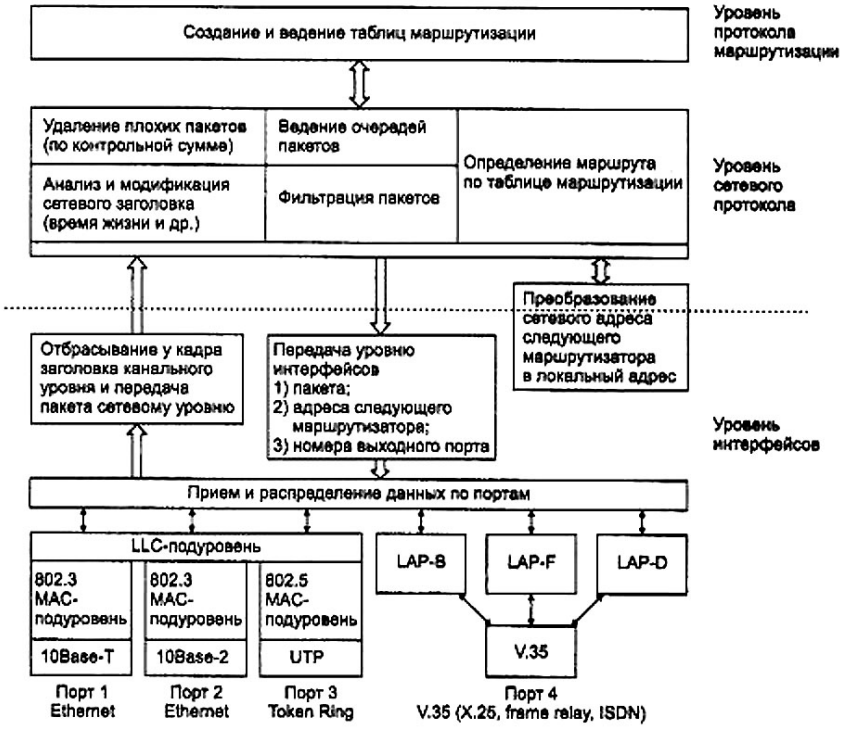
Протокол обмена управляющими сообщениями ICMP (Internet Control Message Protocol) позволяет маршрутизатору сообщить конечному узлу об ошибках, с кот машрутизатор столкнулся при передаче какого-либо IP-пакета от данного конечного узла. Протокол ICMP - протокол сообщения об ошибках, а не протокол коррекции ошибок. Конечный узел может предпринять некот. действия для того, чтобы ошибка больше не возникала, но эти действия протоколом ICMP не регламентируются. Любой сообщение протокола ICMP передается по сети внутри пакета IP. Пакеты IP с сообщениями ICMP маршрутизируются точно так же, как и любые другие пакеты.

ARP/RARP. Назначение IP-адресов узлам сети даже при не очень > размере сети может представлять для админа утомительную процедуру. Для определения локального адреса по IP-адресу используется протокол разрешения адреса (Address Resolution Protocol, **ARP**). Протокол ARP в зависимости от того, какой протокол канальн уровня работает в данной сети - протокол лок. сети с возможностью широковещ доступа одновременно ко всем узлам сети или же протокол глоб. сети (X.25, frame relay), не поддерж широковещ доступ. Существует протокол, решающий обратную задачу - нахождение IP-адреса по известному лок адресу - реверсивный ARP (Reverse Address Resolution Protocol, **RARP**) и используется при старте бездисковых станций, не знающих в нач. момент своего IP-адреса, но знающих адрес своего сетевого адаптера.

Протокол WINS. Разработан компанией MicroSoft для операционной среды Windows и предназначен для расширения возможностей NetBIOS. WINS-запросы обычно транспортируются в UDP-дейтограммах. При этом используется порт отправителя=137. Протокол WINS весьма удобен для сбора данных о MAC-адресах ЭВМ в многоранговой сети, где получить эти данные с помощью ARP-запросов невозможно. Какие-то данные можно извлечь из кэша маршрутизаторов или таблиц сетевых переключателей, если они доступны с помощью SNMP-запросов.

Сервер WINS обрабатывает запросы на регистрацию имен от клиентов WINS, регистрирует их имена и IP-адреса и отвечает на запросы разрешения имен NetBIOS от клиентов, возвращая IP-адрес по имени, если это имя находится в базе данных сервера. Сервер WINS поддерживает базу данных WINS.

32. Маршрутизация. Принципиальные подходы к решению проблемы маршрутизации для сетей различного размера. Distance vector и Link-state алгоритмы (концепция). IGP против EGP. Проблемы роста и подходы к их решению.



Важнейшей задачей сетевого уровня является **маршрутизация** - передача пакетов между двумя конечными узлами в составной сети.

Функции маршрутизатора

- чтение заголовков пакетов сетевых протоколов, принимаемых и буферизуемых по каждому порту (например, IPX, IP, AppleTalk или DECnet),
- и принятие решения о дальнейшем маршруте следования пакета по его сетевому адресу, включающему, как правило, номер сети и номер узла.

Функции маршрутизатора могут быть разбиты на 3 группы в соответствии с уровнями модели OSI (рис. 5.3).

Задачу выбора маршрута из нескольких возможных решают маршрутизаторы, а также конечные узлы. Маршрут выбирается на основании имеющейся у этих устройств информации о текущей конфигурации сети, а также на основании указанного критерия выбора маршрута. Обычно в качестве критерия выступает задержка прохождения маршрута отдельным пакетом или средняя пропускная способность маршрута для последовательности пакетов. Часто также используется весьма простой критерий, учитывающий только количество пройденных в маршруте промежуточных маршрутизаторов (**хопов**). [см. билет №29, Протоколы маршрутизации]

Протоколы маршрутизации (Коротко — схемы-тезисы)

1. Подход (алгоритмы)
   - **Одношаговый**
   - Многошаговый - маршрутизация от источника (Source Routing)

   1.1. Одношаговые алгоритмы делятся на три класса:
   - алгоритмы фиксированной (или статической) маршрутизации;
   - алгоритмы простой маршрутизации;
   - **алгоритмы адаптивной (или динамической) маршрутизации**.

   1.1.2. Выделяют три типа простой маршрутизации:
   - случайная маршрутизация;
   - лавинная маршрутизация;
   - маршрутизация по предыдущему опыту.

   1.1.3. Самыми распространенными являются алгоритмы адаптивной (или динамической) маршрутизации

   Адаптивные алгоритмы должны отвечать требованиям.
   1) Обеспечивать, оптимальность/рациональность маршрута.
   2) Должны быть достаточно простыми, (чтобы при не тратилось слишком много сетевых ресурсов, небольшой объем вычислений).
   3) Должны обладать свойством сходимости (однозначный результат за приемлемое время).

   Адаптивные протоколы обмена маршрутной информацией делятся на две группы, каждая из которых связана с одним из следующих типов алгоритмов:
   - дистанционно-векторные алгоритмы (**Distance Vector Algorithms**, **DVA**);

- алгоритмы состояния связей (**Link State Algorithms**, **LSA**).

В алгоритмах **дистанционно-векторного типа** каждый маршрутизатор периодически и широковещательно рассылает по сети вектор, компонентами которого являются расстояния от данного маршрутизатора до всех известных ему сетей. Под расстоянием обычно понимается число **хопов**. При получении вектора от соседа маршрутизатор наращивает расстояния до указанных в векторе сетей на расстояние до данного соседа. Получив вектор от соседнего маршрутизатора, каждый маршрутизатор добавляет к нему информацию об известных ему других сетях, о которых он узнал непосредственно (если они подключены к его портам) или из аналогичных объявлений других маршрутизаторов, а затем снова рассылает новое значение вектора по сети. В конце концов, каждый маршрутизатор узнает информацию обо всех имеющихся в интерсети сетях и о расстоянии до них через соседние маршрутизаторы.

Дистанционно-векторные алгоритмы хорошо работают только в небольших сетях, В больших сетях они засоряют линии связи интенсивным широковещательным трафиком, к тому же изменения конфигурации могут отрабатываться по этому алгоритму не всегда корректно, так как маршрутизаторы не имеют точного представления о топологии связей в сети, а располагают только обобщенной информацией - вектором дистанций, к тому же полученной через посредников. Работа маршрутизатора в соответствии с дистанционно-векторным протоколом напоминает работу моста, так как точной топологической картины сети такой маршрутизатор не имеет.

Наиболее распространенным протоколом, основанным на дистанционно-векторном алгоритме, является протокол RIP, который распространен в двух версиях - RIP IP, работающий с протоколом IP, и RIP IPX, работающий с протоколом IPX.

Алгоритмы состояния связей обеспечивают каждый маршрутизатор информацией, достаточной для построения точного графа связей сети. Все маршрутизаторы работают на основании одинаковых графов, что делает процесс маршрутизации более устойчивым к изменениям конфигурации. «Широковещательная» рассылка (то есть передача пакета всем непосредственным соседям маршрутизатора) используется здесь только при изменениях состояния связей, что происходит в надежных сетях не так часто. Вершинами графа являются как маршрутизаторы, так и объединяемые ими сети. Распространяемая по сети информация состоит из описания связей различных типов: маршрутизатор - маршрутизатор, маршрутизатор - сеть,

Чтобы понять, в каком состоянии находятся линии связи, подключенные к его портам, маршрутизатор периодически обменивается короткими пакетами HELLO со своими ближайшими соседями. Этот служебный трафик также засоряет сеть, но не в такой степени как, например, RIP-пакеты, так как пакеты HELLO имеют намного меньший объем.

Протоколами, основанными на алгоритме состояния связей, являются протоколы IS-IS (Intermediate System to Intermediate System) стека OSI, OSPF (Open Shortest Path First) стека TCP/IP и недавно реализованный протокол NLSP стека Novell.

5.4.1. Внутренние и внешние протоколы маршрутизации Internet [1, стр.85-88]

Большинство протоколов маршрутизации, применяемых в современных сетях с коммутацией пакетов, ведут свое происхождение от сети Internet и ее предшественницы - сети ARPANET. Для того чтобы понять их назначение и особенности, полезно сначала познакомиться со структурой сети Internet, которая наложила отпечаток на терминологию и типы протоколов.

Internet изначально строилась как сеть, объединяющая большое количество существующих систем. С самого начала в ее структуре выделяли **магистральную сеть** (core backbone network), а сети, присоединенные к магистрали, рассматривались как **автономные системы** (autonomous systems, AS). Магистральная сеть и каждая из автономных систем имели свое собственное административное управление и собственные протоколы маршрутизации. Необходимо подчеркнуть, что автономная система и домен имен Internet - это разные понятия, которые служат разным целям. Автономная система объединяет сети, в которых под общим административным руководством одной организации осуществляется маршрутизация, а домен объединяет компьютеры (возможно, принадлежащие разным сетям), в которых под общим административным руководством одной организации осуществляется назначение уникальных символьных имен. Естественно, области действия автономной системы и домена имен могут в частном случае совпадать, если одна организация выполняет обе указанные функции.

Общая схема архитектуры сети Internet показана на рис. 5.25. Далее **маршрутизаторы** мы будем называть **шлюзами**, чтобы оставаться в русле традиционной терминологии Internet.

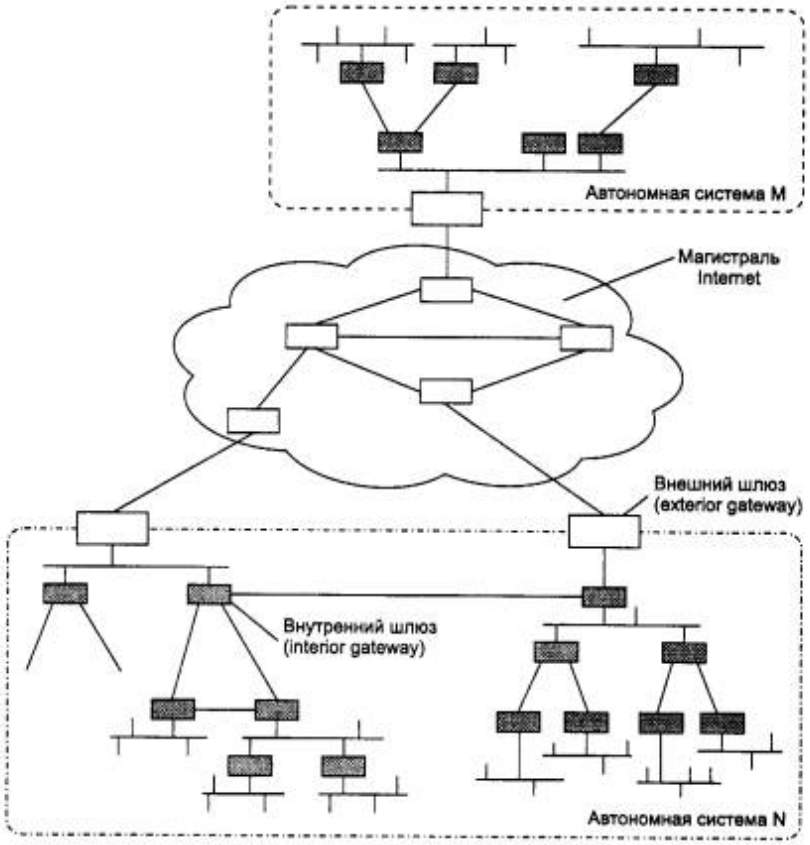


Рис. 5.25. Магистраль и автономные системы Internet

Шлюзы, которые используются для образования сетей и подсетей внутри автономной системы, называются **внутренними шлюзами** (interior gateways), а шлюзы, с помощью которых автономные системы присоединяются к магистрали сети, называются **внешними шлюзами** (exterior gateways). Магистраль сети также является автономной системой. Все автономные системы имеют уникальный 16-разрядный номер, который выделяется организацией, учредившей новую автономную систему, InterNIC.

Соответственно протоколы маршрутизации внутри автономных систем называются **протоколами внутренних шлюзов** (interior gateway protocol, **IGP**), а протоколы, определяющие обмен маршрутной информацией между внешними шлюзами и шлюзами магистральной сети - **протоколами внешних шлюзов** (exterior gateway protocol, **EGP**). Внутри магистральной сети также допустим любой собственный внутренний протокол IGP. [1, стр.87]

Смысл разделения всей сети Internet на автономные системы - в ее многоуровневом модульном представлении, что необходимо для любой крупной системы, способной к расширению в больших масштабах. Изменение протоколов маршрутизации внутри какой-либо автономной системы никак не должно влиять на работу остальных автономных систем. Кроме того, деление Internet на автономные системы должно способствовать агрегированию информации в магистральных и внешних шлюзах. Внутренние шлюзы могут использовать для внутренней маршрутизации достаточно подробные графы связей между собой, чтобы выбрать наиболее рациональный маршрут. Однако если информация такой степени детализации будет храниться во всех маршрутизаторах сети, то топологические базы данных так разрастутся, что потребуют наличия памяти гигантских размеров, а время принятия решений о маршрутизации станет неприемлемо большим.

Поэтому детальная топологическая информация остается внутри автономной системы, а автономную систему как единое целое для остальной части Internet представляют внешние шлюзы, которые сообщают о внутреннем составе автономной системы минимально необходимые сведения - количество IP-сетей, их адреса и внутреннее расстояние до этих сетей от данного внешнего шлюза.

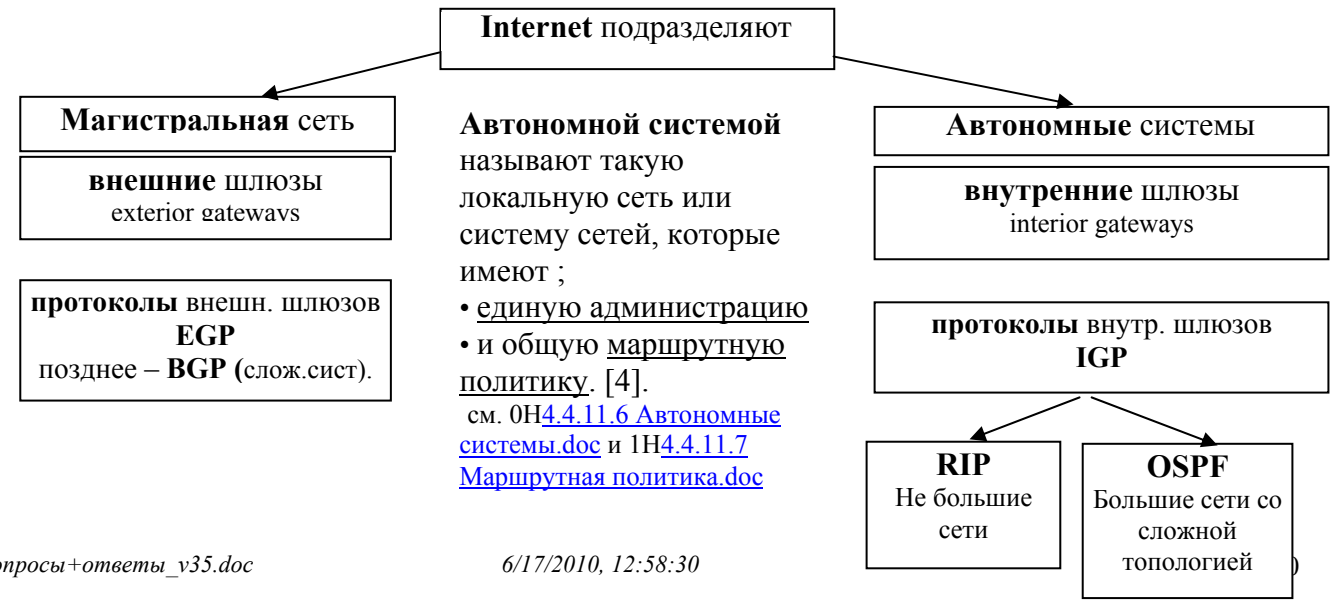
Техника бесклассовой маршрутизации CIDR может значительно сократить объемы маршрутной информации, передаваемой между автономными системами. Так, если все сети внутри некоторой автономной системы начинаются с общего префикса, например 194.27.0.0/16, то внешний шлюз этой автономной системы должен делать объявления только об этом адресе, не сообщая отдельно о существовании внутри данной автономной системы, например, сети 194.27.32.0/19 или 194.27.40.0/21, так как эти адреса агрегируются в адрес 194.27.0.0/16.

Проблемы роста и подходы к их решению.

Приведенная на рис. 5.25 структура Internet с единственной магистралью достаточно долго соответствовала действительности, поэтому специально для нее был разработан протокол обмена маршрутной информации между автономными системами, названный **EGP**. Однако по мере развития сетей поставщиков услуг структура Internet стала гораздо более сложной, с произвольным характером связей между автономными системами. Поэтому протокол EGP уступил место протоколу BGP, который позволяет распознать наличие петель между автономными системами и исключить их из межсистемных маршрутов. Протоколы EGP и BGP используются только во внешних шлюзах автономных систем, которые чаще всего организуются поставщиками услуг Internet. В маршрутизаторах корпоративных сетей работают внутренние протоколы маршрутизации, такие как RIP и OSPF

Выводы

- Крупные сети разбивают на автономные системы, в которых проводится общая политика маршрутизации IP-пакетов. Если сеть подключена к Internet, то идентификатор автономной системы назначается в InterNIC.
- Протоколы маршрутизации делятся на внешние и внутренние. Внешние протоколы (EGP, BGP) переносят маршрутную информацию между автономными системами, а внутренние (RIP, OSPF) применяются только в пределах определенной автономной системы.
- Протокол RIP является наиболее заслуженным и распространенным протоколом маршрутизации сетей TCP/IP. Несмотря на его простоту, определенную использованием дистанционно-векторного алгоритма, RIP успешно работает в .небольших сетях с количеством промежуточных маршрутизаторов не более 15.
- RIP-маршрутизаторы при выборе маршрута обычно используют самую простую метрику - количество промежуточных маршрутизаторов между сетями, то есть хопов.
- Версия RIPvl не распространяет маски подсетей, что вынуждает администраторов использовать маски фиксированной длины во всей составной сети. В версии RIPv2 это ограничение снято.
- В сетях, использующих RIP и имеющих петлевидные маршруты, могут наблюдаться достаточно длительные периоды нестабильной работы, когда пакеты зацикливаются в маршрутных петлях и не доходят до адресатов. Для борьбы с этими явлениями в RIP-маршрутизаторах предусмотрено несколько приемов (Split Horizon, Hold Down, Triggered Updates), которые сокращают в некоторых случаях периоды нестабильности.
- Протокол OSPF был разработан для эффективной маршрутизации IP-пакетов в больших сетях со сложной топологией, включающей петли. Он основан на алгоритме состояния связей, который обладает высокой устойчивостью к изменениям топологии сети.
- При выборе маршрута OSPF-маршрутизаторы используют метрику, учитывающую пропускную способность составных сетей.
- Протокол OSPF является первым протоколом маршрутизации для IP-сетей, который учитывает биты качества обслуживания (пропускная способность, задержка и надежность) в заголовке IP-пакета. Для каждого типа качества обслуживания строится отдельная таблица маршрутизации.
- Протокол OSPF обладает высокой вычислительной сложностью, поэтому чаще всего работает на мощных аппаратных маршрутизаторах.



32. Из презентации

Маршрутизация [5] (см. it_net_05_Маршрутизация.ppt)

- Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами.
- **Маршрутизатор** — это устройство, которое собирает информацию о топологии межсетевых соединений и пересылает пакеты сетевого уровня в сеть назначения. Чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач между сетями, или **хопов** (от слова hop — прыжок), каждый раз выбирая подходящий маршрут. Таким образом, **маршрут** представляет собой последовательность маршрутизаторов, через которые проходит пакет.
- Сетевой уровень должен обеспечить доставку пакета:
  - между любыми двумя узлами сети с произвольной топологией;
  - между любыми двумя сетями в составной сети;
- **Сеть** — совокупность компьютеров, использующих для обмена данными единую сетевую технологию;
- **Маршрут** — последовательность прохождения пакетом маршрутизаторов в составной сети.]

Задачи маршрутизации

- Проблема выбора наилучшего пути называется маршрутизацией, и ее решение является одной из главных задач **сетевого уровня**.
- Эта проблема осложняется тем, что **самый короткий путь — не всегда самый лучший**.
- Критерием при выборе **маршрута** может служить время передачи данных:
  - Время зависит от пропускной способности каналов связи и интенсивности трафика, которая может с течением времени изменяться.
- Выбор **маршрута** может осуществляться и по другим критериям, таким как **надежность** передачи.
- Функции **сетевого уровня** шире, чем функции передачи сообщений по связям с нестандартной структурой, которые мы рассмотрели на примере объединения нескольких локальных сетей.
- **Сетевой уровень** также решает задачи согласования разных технологий, упрощения **адресации** в крупных сетях и создания надежных и гибких барьеров на пути нежелательного трафика между сетями.

Протоколы маршрутизации

- Протокол маршрутизации – поддерживает маршрутизируемый протокол за счет предоставления механизмов коллективного использования маршрутной информации.
- Сообщения протокола маршрутизации циркулируют между маршрутизаторами для обмена информации и атуализации данных таблиц маршрутизации.
- Примеры протоколов маршрутизации:
  - RIP – протокол маршрутной информации;
  - IGRP – протокол внутренней маршрутизации между шлюзами;
  - EIGR – усовершенствованный протокол внутренней маршрутизации между шлюзами;
  - OSPF – протокол маршрутизации с выбором кратчайшего пути.

Алгоритмы маршрутизации

- Большинство алгоритмов маршрутизации можно свести к трем основным:
  - Маршрутизация на основе вектора расстояния – определяется направление (вектор) и расстояние до каждого канала в сети;
  - Маршрутизация на основе оценки состояния канала (выбор на основе кратчайшего пути), при которой воссоздается точная топология всей сети (по крайней мере, где размещается маршрутизатор);
  - Гибридный подход, объединяющий вышеуказанные алгоритмы.

Подробнее см. этуссылку

32 – Маршрутизация из Семёнова

подробнее см. [4] файл 4.4.11.0 Протоколы маршрутизации+.doc

Основная задача сетей – трансп ортировка информации от ЭВМ-отправителя к ЭВМ-получателю. В большинстве случаев для этого нужно совершить несколько пересылок. Проблему выбора пути решают алгоритмы маршрутизации. Если транспортировка данных осуществляется дейтограммами, для каждой из них эта задача решается независимо. При использовании виртуальных каналов выбор пути выполняется на этапе формирования этого канала. В Интернет с его IP-дейтограммами реализуется первый вариант (если не рассматривать виртуальные сети), а в ISDN и ATM - второй. Для решения проблемы маршрутизации используются специальные устройства, называемые **маршрутизаторами**.

Маршрутизация подразумевает два параллельных процесса: подготовку маршрутной таблицы и переадресацию дейтограмм с помощью этой таблицы. Формирование маршрутной таблицы производится посредством протоколов маршрутизации или под воздействием инструкций сетевого администратора.

Алгоритм маршрутизации должен обладать вполне определенными свойствами: надежностью, корректностью, стабильностью, простотой и оптимальностью. Последнее свойство не так прозрачно, как это может показаться на первый взгляд, все зависит от того, по какому или каким параметрам производится оптимизация. ....далее см. [4]

Параметры оптимизации маршрута

Среди параметров оптимизации может быть минимальная задержка доставки, максимальная пропускная способность, минимальная цена, максимальная надежность или минимальная вероятность ошибки.

Главным параметром при маршрутизации пакета в Интернет является IP-адрес его места назначения.

На практике оптимизация осуществляется для ограниченной области сегментов, тогда и объем данных, подлежащих обработке, сокращается на многие порядки. Понятно, что компромиссы здесь неизбежны и результирующий маршрут в этом случае отнюдь не всегда будет оптимальным. Сбор данных о сетевых сегментах и маршрутах выполняется путем обмена этой информацией между маршрутизаторами.

Одним из радикальных мер решения проблемы может стать географическая маршрутизация, которая станет возможной при массовом внедрении адресации **IPv6**.

Метрики маршрутов

Если адресат достижим более чем одним путем, маршрутизатор должен сделать выбор, этот выбор осуществляется на основании оценки маршрутов-кандидатов. Обычно каждому сегменту, составляющему маршрут, присваивается некоторая величина - оценка этого сегмента. Каждый протокол маршрутизации использует свою систему оценки маршрутов. Оценка сегмента маршрута называется **метрикой**. Здесь следует обратить внимание на то, что при выборе маршрута всем сегментам пути должны быть даны сопоставимые значения метрики. Недопустимо, чтобы одни сегменты оценивались числом шагов, а другие - по величине задержки в миллисекундах. В пределах автономной системы это обычно не создает проблем, ведь это зона ответственности одного администратора. Но в региональных сетях, где работает много администраторов, проблема выбора метрики может стать реальной трудностью. Именно по этой причине в таких сетях часто используется вектор расстояния, исключающий субъективность оценок метрики.

Помимо классической схемы маршрутизации по адресу места назначения, часто используется вариант выбора маршрута отправителем (данный вариант получил дальнейшее развитие при введении стандарта **IPv6**). В этом случае IP-пакет содержит соответствующий код опции и список промежуточных адресов узлов, которые он должен посетить по пути к месту назначения.

Широковещательный алгоритм оптимизации маршрута

Существуют и другие схемы, например, использующие широковещательные методы адресации (flooding), где каждый приходящий пакет посылается по всем имеющимся исходящим каналам, за исключением того, по которому он получен. Существует усовершенствованная версия широковещательной маршрутизации, называемая *селективной широковещательной рассылкой*. В этом алгоритме рассылка производится не по всем возможным направлениям, а только по тем, которые предположительно ведут в правильную сторону.

Маршруты по умолчанию

Заметно сокращают размер маршрутной таблицы **маршруты по умолчанию**. В этой схеме сначала ищется маршрут в таблицах, а если он не найден, пакет посылается в узел, специально выбранный для данного случая. Так, когда имеется только один канал за рубеж, неудачный поиск в таблице маршрутов по России означает, что пакет следует послать по этому каналу и пусть там с ним разбираются. Маршруты по умолчанию используются обычно тогда, когда маршрутизатор имеет ограниченный объем памяти или по какой-то иной причине не имеет полной таблицы маршрутизации. Маршрут по умолчанию может помочь реализовать связь даже при ошибках в маршрутной таблице. *Это может не иметь никаких последствий для малых сетей, но для региональных сетей с ограниченной пропускной способностью такое решение может повлечь серьезные последствия. Экономия на памяти для маршрутных таблиц - дурной стиль, который не доведет до добра. Например, из-за такого рода ошибки довольно долго пакеты из Ярославля в Москву шли через США, я уже не говорю о случае, когда машины, размещенные в соседних комнатах Президиума РАН, вели обмен через Амстердам (правда, это было достаточно давно).*

Динамические протоколы (обычно используются именно они, наиболее известным разработчиком является компания CISCO):

В маршрутизаторе с динамическим протоколом (например, **BGP-4**) резидентно загруженная программа-драйвер изменяет таблицы маршрутизации на основе информации, полученной от соседних маршрутизаторов. В ЭВМ, работающей под UNIX и выполняющей функции маршрутизатора, эту задачу часто решает резидентная программа gated или routed (демон). Последняя - поддерживает только внутренние протоколы маршрутизации.

Внешние и внутренние протоколы маршрутизации

...существуют протоколы, базирующиеся на векторе расстояния (RIP), и на состоянии канала (OSPF или IGRP).

Внутренний протокол маршрутизации **IGP** (Interior Gateway Protocol) определяет маршруты внутри автономной системы. Наиболее популярный IGP - RIP (Routing Information Protocol, RFC-1058), *разработан Фордом, Фулкерсоном и Белманом (фирма XEROX) разработан в 1957-62 годах* и использует в качестве метрики вектор расстояния.

Существует более новый протокол **OSPF** (Open Shortest Pass First, RFC-1131, -1245, -1247, -1253, -1584, -1850, -2328, -2740). базирующийся на оценках состояний каналов. Как во всех маршрутных протоколах, использующих состояние канала, многое зависит от того, как вычисляется метрика.

33. Протокол RIP. Особенности и проблемы, способы их решения. Ограничения применения и их анализ.

Протокол RIP. Коротко из Шпрогалки [2]

RIP протокол маршрутизации предназначенный для сравнительно небольших и относительно однородных сетей. Маршрут здесь характеризуется вектором расстояния до места назначения. Предполагается, что каждый маршрутизатор является отправной точкой нескольких маршрутов до сетей, с которыми он связан. Описания этих маршрутов хранится в маршрутной таблице. Она содержит по записи на каждую обслуживаемую машину (на каждый маршрут). Запись должна включать в себя:

- IP-адрес места назначения;
- метрика маршрута (от 1 до 15; число шагов до места назначения);
- IP-адрес ближайшего маршрутизатора по пути к месту назначения;
- таймеры маршрута.

Периодически (раз в 30 сек) каждый маршрутизатор посылает широковещательно копию своей маршрутной таблицы всем соседям-маршрутизаторам, с которыми связан непосредственно. Маршрутизатор-получатель просматривает таблицу. Если в таблице присутствует новый путь или сообщение о более коротком маршруте, или произошли изменения длин пути, эти изменения фиксируются получателем в своей маршрутной таблице. Малая скорость установления маршрутов в RIP (и других протоколах, ориентированных на вектор расстояния) и является причиной их постепенного вытеснения другими протоколами. [2]

Протокол RIP. из [1]

Протокол RIP (Routing Information Protocol) является внутренним протоколом маршрутизации дистанционно-векторного типа, он представляет собой один из наиболее ранних протоколов обмена маршрутной информацией и до сих пор чрезвычайно распространен в вычислительных сетях ввиду простоты реализации.

Для IP имеются две версии протокола RIP: первая и вторая. Протокол RIPvl не поддерживает масок, то есть он распространяет между маршрутизаторами только информацию о номерах сетей и расстояниях до них, а информацию о масках этих сетей не распространяет, считая, что все адреса принадлежат к стандартными классам А, В или С. Протокол RIPv2 передает информацию о масках сетей, поэтому он в большей степени соответствует требованиям сегодняшнего дня. Так как при построении таблиц маршрутизации работа версии 2 принципиально не отличается от версии 1, то в дальнейшем для упрощения записей будет описываться работа первой версии.

В качестве расстояния до сети стандарты протокола RIP допускают различные виды метрик: хопы, метрики, учитывающие пропускную способность, вносимые задержки и надежность сетей (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.

Построение таблицы маршрутизации (подробно – см. эту гиперссылку или [1] стр. 88-98)

Этап 1 - создание минимальных таблиц

В исходном состоянии в каждом м-ре программным обеспечением стека TCP/IP автоматически создается минимальная таблица м-ции, в которой учитываются только непосредственно подсоединенные сети.

Этап 2 - рассылка минимальных таблиц соседям

После инициализации каждого м-ра 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 м-ра.

Соседями являются те м-ры, которым данный м-р непосредственно может передать IP-пакет по какой-либо своей сети, не пользуясь услугами промежуточных м-ров.

Этап 3 - получение RIP-сообщений от соседей и обработка полученной информации

После получения аналогичных сообщений от м-ров М2 и М3(соседей) м-р Ml наращивает каждое полученное поле метрики на единицу и запоминает, через какой порт и от какого м-ра получена новая информация (адрес этого м-ра будет адресом следующего м-ра, если эта запись будет внесена в таблицу маршрутизации). Затем м-р начинает сравнивать новую информацию с той, которая хранится в его таблице маршрутизации

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

Аналогичные операции с новой инф. выполняют и остальные м-ры сети.

Этап 4 - рассылка новой, уже не минимальной, таблицы соседям

Каждый м-р отсылает новое RIP-сообщение всем своим соседям. В этом сообщении он помещает данные о всех известных ему сетях - как. 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 м-ции.

Адаптация RIP-маршрутизаторов к изменениям состояния сети

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-маршрутиза-торы 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 более недействителен:

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

Главная причина нестабильной работы маршрутизаторов, работающих по протоколу RIP, коренится в самом принципе работы дистанционно-векторных протоколов - пользовании информацией, полученной из вторых рук. Искоренить эту причину полностью нельзя, ведь сам способ построения таблиц маршрутизации связан с передачей чужой информации без указания источника ее происхождения.

Не следует думать, что при любых отказах интерфейсов и маршрутизаторов в сетях возникают маршрутные петли. Если бы маршрутизатор Ml успел передать сообщение о недостижимости сети 201.36.14.0 раньше ложной информации маршрутизатора М2, то маршрутная петля не образовалась бы. Так что маршрутные петли даже без дополнительных методов борьбы с ними, описанными в следующем разделе, возникают в среднем не более чем в половине потенциально возможных случаев.

Методы борьбы с ложными маршрутами в протоколе RIP

Несмотря на то что протокол RIP не в состоянии полностью исключить переходные состояния в сети, когда некоторые маршрутизаторы пользуются устаревшей информацией об уже несуществующих маршрутах, имеется несколько методов, которые во многих случаях решают подобные проблемы.

Ситуация с петлей, образующейся между соседними маршрутизаторами, надежно решается с помощью **метода 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).

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.

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. Предполагается, что 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 устаревшие сведения по сети.

Выводы

- Протокол RIP является наиболее заслуженным и распространенным протоколом маршрутизации сетей TCP/IP. Несмотря на его простоту, определенную использованием дистанционно-векторного алгоритма, RIP успешно работает в .небольших сетях с количеством промежуточных маршрутизаторов не более 15.
- RIP-маршрутизаторы при выборе маршрута обычно используют самую простую метрику - количество промежуточных маршрутизаторов между сетями, то есть хопов.
- Версия RIPvl не распространяет маски подсетей, что вынуждает администраторов использовать маски фиксированной длины во всей составной сети. В версии RIPv2 это ограничение снято.
- В сетях, использующих RIP и имеющих петлевидные маршруты, могут наблюдаться достаточно длительные периоды нестабильной работы, когда пакеты зацикливаются в маршрутных петлях и не доходят до адресатов. Для борьбы с этими явлениями в RIP-маршрутизаторах предусмотрено несколько приемов (Split Horizon, Hold Down, Triggered Updates), которые сокращают в некоторых случаях периоды нестабильности.

32 – RIP из Семёнова

RIP (Routing Information Protocol, RFC-1058), разработан Фордом, Фулкерсоном и Белманом (фирма XEROX) разработан в 1957-62 годах и использует в качестве метрики вектор расстояния. *подробнее см.* ***[4]*** *файл* 4.4.11.0 Протоколы маршрутизации+.doc
и 4.4.11.1 Внутренний протокол маршрутизации RIP.doc

Этот протокол (RFC-1388, -1582, -1721, -1722 (std0057), -2453, -1724, -2080, -2082, -2092, -2453) маршрутизации предназначен для сравнительно небольших и относительно однородных сетей (алгоритм Белмана-Форда). *Протокол разработан в университете Калифорнии (Беркли), базируется на разработках фирмы Ксерокс и реализует те же принципы, что и программа маршрутизации routed, используемая в ОС UNIX (4BSD).* **Маршрут** здесь характеризуется вектором расстояния до места назначения. Предполагается, что каждый маршрутизатор является отправной точкой нескольких маршрутов до сетей, с которыми он связан.

Если сеть однородна, то есть все каналы имеют равную пропускную способность и примерно равную загрузку, что типично для небольших локальных сетей, то число шагов до цели является разумной оценкой пути (**метрикой**).

Описания этих маршрутов хранится в специальной таблице, называемой маршрутной. Таблица маршрутизации RIP содержит по записи на каждую обслуживаемую машину (на каждый маршрут). Запись должна включать в себя:

- IP-адрес места назначения.
- Метрика маршрута (от 1 до 15; число шагов до места назначения).
- IP-адрес ближайшего маршрутизатора (gateway) по пути к месту назначения.
- Таймеры маршрута.

Первым двум полям записи мы обязаны появлению термина вектор расстояния (место назначение - направление; метрика - модуль вектора). Периодически (раз в 30 сек) каждый маршрутизатор посылает широковещательно копию своей маршрутной таблицы всем соседям-маршрутизаторам, с которыми связан непосредственно. Маршрутизатор-получатель просматривает таблицу. Если в таблице присутствует новый путь или сообщение о более коротком маршруте, или произошли изменения длин пути, эти изменения фиксируются получателем в своей маршрутной таблице. Протокол RIP должен быть способен обрабатывать три типа ошибок:

1. Циклические маршруты. Так как в протоколе нет механизмов выявления замкнутых маршрутов, необходимо либо слепо верить партнерам, либо принимать меры для блокировки такой возможности.
2. Для подавления нестабильностей RIP должен использовать малое значение максимально возможного числа шагов (<16).
3. Медленное распространение маршрутной информации по сети создает проблемы при динамичном изменении маршрутной ситуации (система не поспевает за изменениями). Малое предельное значение метрики улучшает сходимость, но не устраняет проблему.

Несоответствие маршрутной таблицы реальной ситуации типично не только для RIP, но характерно для всех протоколов, базирующихся на векторе расстояния, где информационные сообщения актуализации несут в себе только пары кодов: адрес места назначение и расстояние до него. Пояснение проблемы дано на рис. 4.4.1.11.1 ниже)см. 4.4.11.1 Внутренний протокол маршрутизации RIP.doc)

34. Протокол OSPF в сетях сложной структуры. Концепция областей и обмена маршрутами. Агрегирование.

Протокол OSPF. Коротко из Шпрогалки [2]

OSPF (Open Shortest Pass First) является альтернативой. OSPF представляет собой протокол состояния маршрута (в качестве метрики используется - коэффициент качества обслуживания). Каждый маршрутизатор обладает полной информацией о состоянии всех интерфейсов всех маршрутизаторов (переключателей) АС (автономной системы).

АС может быть разделена на несколько областей, куда могут входить как отдельные ЭВМ, так и целые сети. В этом случае внутренние маршрутизаторы области могут и не иметь информации о топологии остальной части АС. Обычно имеется выделенный маршрутизатор, который является источником маршрутной информации для остальных маршрутизаторов АС. Каждый маршрутизатор самостоятельно решает задачу оптимизации маршрутов. Если к месту назначения ведут два или более эквивалентных маршрута, информационный поток будет поделен между ними поровну. Переходные процессы в OSPF завершаются быстрее, чем в RIP. В процессе выбора оптимального маршрута анализируется ориентированный граф сети. Для транспортных целей OSPF использует IP непосредственно.

Маршрутная таблица OSPF содержит в себе:

- IP-адрес места назначения и маску;
- тип места назначения (сеть, граничный маршрутизатор и т.д.);
- тип функции;
- область (описывает область, связь с которой ведет к цели, возможно несколько записей данного типа, если области действия граничных маршрутизаторов перекрываются);
- тип пути (характеризует путь как внутренний, межобластной или внешний, ведущий к АС);
- цена маршрута до цели;
- очередной маршрутизатор, куда следует послать дейтограмму;
- объявляющий маршрутизатор (используется для межобластных обменов и для связей автономных систем друг с другом).

Преимущества OSPF

- Для каждого адреса может быть несколько маршрутных таблиц
- Каждому интерфейсу присваивается безразмерная цена, учитывающая пропускную способность, время транспортировки сообщения. Для каждой IP-операции может быть присвоена своя цена (коэффициент качества).
- При существовании эквивалентных маршрутов OSFP распределяет поток равномерно по этим маршрутам.
- Поддерживается адресация субсетей (разные маски для разных маршрутов).
- При связи точка-точка не требуется IP-адрес для каждого из концов. (Экономия адресов!)
- Применение мультикастинга вместо широковещательных сообщений снижает загрузку не вовлеченных сегментов.

Недостатки:

- Трудно получить информацию о предпочтительности каналов для узлов, поддерживающих другие протоколы, или со статической маршрутизацией.
- OSPF является лишь внутренним протоколом.

Протокол OSPF (см. [1] стр. 98—103) подробнее см. гиперссылку

Протокол OSPF (Open Shortest Path First, открытый протокол «кратчайший путь первыми) является достаточно современной реализацией алгоритма состояния связей (он принят в 1991 году) и обладает многими особенностями, ориентированными на применение в больших гетерогенных сетях.

В OSPF процесс построения таблицы маршрутизации разбивается на два крупных этапа. **На первом этапе** каждый маршрутизатор 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 Дийкстры. 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-маршрутиза-торы не используют обмен полной таблицей маршрутизации, как это не очень рационально делают MP-маршрутизаторы. Вместо этого они передают специальные короткие сообщения HELLO. Если состояние сети не меняется, то OSPF-мар-шрутизаторы 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 (подробнее см. гиперссылку и рис. 5.27).

Маршрутизаторы соединены как с локальными сетями, так и непосредственно между собой глобальными каналами типа «точка-точка».

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.

Так как информация о некоторой связи изначально генерируется только тем маршрутизатором, который выяснил фактическое состояние этой связи путем тестирования с помощью сообщений HELLO, а остальные маршрутизаторы только ретранслируют эту информацию без преобразования, то недостоверная информация о достижимости сетей, которая может появляться в RIP-маршрутиэаторах, в OSPF-маршрутизаторах появиться не может, а устаревшая информация быстро заменяется новой, так как при изменении состояния связи новое сообщение генерируется сразу же.

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) (не нужно путать с автономной системой Internet). 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.

Выводы

- Протокол OSPF был разработан для эффективной маршрутизации IP-пакетов в больших сетях со сложной топологией, включающей петли. Он основан на алгоритме состояния связей, который обладает высокой устойчивостью к изменениям топологии сети.
- При выборе маршрута OSPF-маршрутизаторы используют метрику, учитывающую пропускную способность составных сетей.
- Протокол OSPF является первым протоколом маршрутизации для IP-сетей, который учитывает биты качества обслуживания (пропускная способность, задержка и надежность) в заголовке IP-пакета. Для каждого типа качества обслуживания строится отдельная таблица маршрутизации.
- Протокол OSPF обладает высокой вычислительной сложностью, поэтому чаще всего работает на мощных аппаратных маршрутизаторах.

Агрегирование (ссылка1 А в исп. Масок перем длинны, ссылка 2 А в технол. CIDR)

16. Агрегирование каналов. Горячее резервирование каналов. Горячее резервирование. [2]

Суть в том, что один канал функционирует, а остальные находятся в «горячем» резерве для замены отказавшей связи. Проблема резервирования возникает в тех сетях где используются протоколы, которые поддерживают только древовидную топологию связей. Для автоматического перевода в резервное состояние всех альтернативных связей, не вписывающихся в топологию дерева, в локальных сетях исп. алгоритм покрывающего дерева (STA). STA обеспечивает поиск древовидной топологии связей с единственным путем от каждого сегмента до некоторого выделенного коммутатора при минимально возможном расстоянии.

Агрегирование физ. каналов м/у(между) 2 коммуникационными устройствами в один лог. канал (транк) является формой использования избыточных альтернативных связей. При агрегировании все избыточные связи остаются в рабочем состоянии, а существующий трафик распределяется м/у ними для достижения баланса загрузки. При отказе одного из каналов, трафик распределяется м/у оставшимися. Применяется как для связи м/у двумя коммутаторами сети, так и для связи м/у комп. и коммутатором или м/у портами маршрутизатора. Все сетевые адаптеры и порты маршрутизатора, которые входят в транк, разделяют один и тот же сетевой адрес. Агрегирование приводит к повышению производительности и надежности. Однако есть ограничение – работа транков не координируется м/у собой, поэтому агрегирование применяется одновременно с алгоритмом покрывающего дерева. Порт коммутатора для продвижения кадра ч/з транка выбирается динамически либо статически. Динамический способ распределения учитывает текущую загрузку портов, но не всегда приводит к максимальной пропускной способности. Для ряда протоколов производительность существенно уменьшится, пакеты будут приходить не в том порядке в котором они были отправлены. Такая ситуация может возникнуть, если два или более смежных по отношению сеанса кадров передаются ч/з разные порты транка. Статическое распределение подразумевает закрепление за определенным портом транка потока кадров определенного сеанса.

34 – OSPF из Семёнова

...существуют протоколы, базирующиеся на векторе расстояния (RIP), и на состоянии канала (**OSPF** или IGRP).

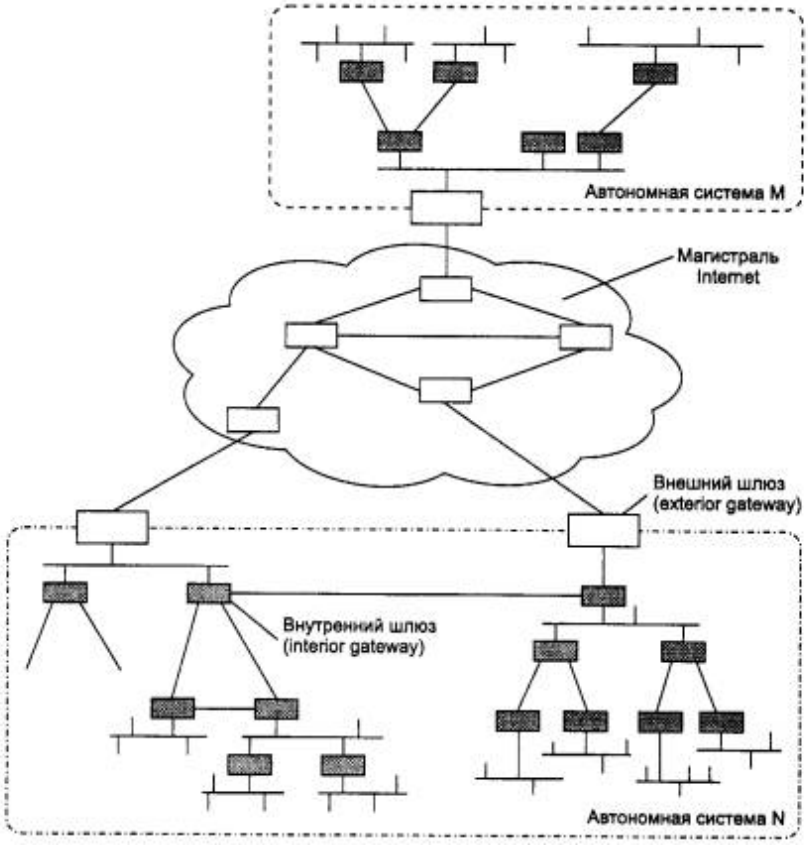
Существует более новый протокол **OSPF** (Open Shortest Pass First, RFC-1131, -1245, -1247, -1253, -1584, -1850, -2328, -2740). базирующийся на оценках состояний каналов. Как во всех маршрутных протоколах, использующих состояние канала, многое зависит от того, как вычисляется метрика.. *подробнее см.* ***[4]*** *файл* 4.4.11.0 Протоколы маршрутизации+.doc *и* 4.4.11.2 Протокол OSPF.doc

Протокол OSPF (Open Shortest Pass First, RFC-1245-48, RFC-1583-1587, std-54, алгоритмы предложены Дикстрой) является альтернативой RIP в качестве внутреннего протокола маршрутизации. OSPF представляет собой протокол состояния маршрута (в качестве метрики используется - коэффициент качества обслуживания). Каждый маршрутизатор обладает полной информацией о состоянии всех интерфейсов всех маршрутизаторов (переключателей) автономной системы. Протокол OSPF реализован в демоне маршрутизации gated, который поддерживает также RIP и внешний протокол маршрутизации BGP.

Базовые особенности учета состояния канала

Определяющими являются три характеристики: задержка, пропускная способность и надежность. Для транспортных целей OSPF использует IP непосредственно, т.е. не привлекает протоколы UDP или TCP. OSPF имеет свой код (89) в протокольном поле IP-заголовка. Код TOS (type of service) в IP-пакетах, содержащих OSPF-сообщения, равен нулю, значение TOS здесь задается в самих пакетах OSPF. Маршрутизация в этом протоколе определяется IP-адресом и типом сервиса. Так как протокол не требует инкапсуляции пакетов, сильно облегчается управление сетями с большим количеством бриджей и сложной топологией (исключается циркуляция пакетов, сокращается транзитный трафик). Автономная система может быть поделена на отдельные области, каждая из которых становится объектом маршрутизации, а внутренняя структура снаружи не видна (узлы на рис. 4.2.11.2.1 могут представлять собой как отдельные ЭВМ или маршрутизаторы, так и целые сети). Этот прием позволяет значительно сократить необходимый объем маршрутной базы данных. В OSPF используется термин опорной сети (backbone) для коммуникаций между выделенными областями. Протокол работает лишь в пределах автономной системы. В пределах выделенной области может работать свой протокол маршрутизации.

35. Маршрутизация в рамках EGP. Протоколы BGP-3 и BGP-4. Атрибуты и их характеристики. Особенности и проблемы, присущие протоколам глобальной маршрутизации. Агрегирование, CIDR, VLSM.



Далее маршрутизаторы мы будем называть шлюзами.

Протоколы, определяющие обмен маршрутной информацией между внешними шлюзами и шлюзами магистральной сети - **протоколами внешних шлюзов** (exterior gateway protocol, **EGP**). *см. схему*

Протокол обмена маршрутной информации между автономными системами, названный **EGP** был разработан специально для структура Internet с единственной магистралью (рис. 5.25). Однако по мере развития сетей поставщиков услуг структура Internet стала гораздо более сложной, с произвольным характером связей между автономными системами. Поэтому протокол EGP уступил место протоколу BGP, который позволяет распознать наличие петель между автономными системами и исключить их из межсистемных маршрутов. Протоколы EGP и BGP используются только во внешних шлюзах автономных систем, которые чаще всего организуются поставщиками услуг Internet. В маршрутизаторах корпоративных сетей работают внутренние протоколы маршрутизации, такие как RIP и OSPF.

Техника бесклассовой маршрутизации CIDR может значительно сократить объемы маршрутной информации, передаваемой между автономными системами. Так, если все сети внутри некоторой автономной системы начинаются с общего префикса, например 194.27.0.0/16, то внешний шлюз этой автономной системы должен делать объявления только об этом адресе, не сообщая отдельно о существовании внутри данной автономной системы, например, сети 194.27.32.0/19 или 194.27.40.0/21, так как эти адреса агрегируются в адрес 194.27.0.0/16.

Технология CIDR уже успешно используется в текущей версии IPv4 и поддерживается такими протоколами маршрутизации, как OSPF, RIP-2, **BGP4**. Предполагается, что эти же протоколы будут работать и с новой версией протокола IPv6. Следует отметить, что в настоящее время технология CIDR поддерживается магистральными маршрутизаторами Internet, а не обычными хостами в локальных сетях.

35 из Семёнова [4]

BGP

Для взаимодействия маршрутизаторов используются внешние протоколы (EGP - Exterior Gateway Protocols).

Одной из разновидностей EGP является протокол **BGP** (Border Gateway Protocol, RFC-1268 [BGP-3], RFC-1467 [BGP-4]).

IP делит все ЭВМ на маршрутизаторы и обычные *ЭВМ (host*), последние, как правило, не рассылают свои маршрутные таблицы. Предполагается, что маршрутизатор владеет исчерпывающей информацией о правильных маршрутах (хотя это и не совсем так). Обычная ЭВМ имеет минимальную маршрутную информацию (например, адрес маршрутизатора локальной сети и сервера имен). Автономная система может содержать множество маршрутизаторов, но взаимодействие с другими AS она осуществляет только через один маршрутизатор, называемый пограничным (border gateway, именно он дал название протоколу **BGP**). Пограничный маршрутизатор нужен лишь тогда, когда автономная система имеет более одного внешнего канала, в противном случае его функции выполняет порт внешнего

подключения (gateway; поддержка внешнего протокола маршрутизации в этом случае не требуется). *Далее(подробнее) см.* ***[4]*** *файл* 4.4.11.0 Протоколы маршрутизации+.doc *стр.4 и далее*

Протокол BGP разработан компаниями IBM и CISCO. Главная цель BGP - сократить транзитный трафик. Местный трафик либо начинается, либо завершается в автономной системе (AS); в противном случае - это транзитный трафик. Системы без транзитного трафика не нуждаются в BGP (им достаточно EGP для общения с транзитными узлами). Но не всякая ЭВМ, использующая протокол BGP, является маршрутизатором, даже если она обменивается маршрутной информацией с пограничным маршрутизатором соседней автономной системы. AS передает информацию только о маршрутах, которыми она сама пользуется. BGP-маршрутизаторы обмениваются сообщениями об изменении маршрутов (UPDATE-сообщения, рис. 4.4.11.4.1). *Далее(подробнее) см.* ***[4]*** *файл* *4.4.11.4 Внешний протокол BGP.doc*

На сегодня используется версия BGP-4

Протокол BGP позволяет реализовать маршрутную политику, определяемую администратором AS (см. 4.4.11.6 Автономные системы.doc и 4.4.11.7 Маршрутная политика.doc). Политика отражается в конфигурационных файлах BGP. Маршрутная политика это не часть протокола, она определяет решения, когда место назначения достижимо несколькими путями, политика отражает соображения безопасности, экономические интересы и пр. Количество сетей в пределах одной AS не лимитировано. Один маршрутизатор на много сетей позволяет минимизировать таблицу маршрутов.

BGP отличается от RIP и OSPF тем, что использует TCP в качестве транспортного протокола. Две системы, использующие BGP, связываются друг с другом и пересылают посредством TCP полные таблицы маршрутизации. В дальнейшем обмен идет только в случае каких-то изменений. ЭВМ, использующая BGP, не обязательно является маршрутизатором. Сообщения обрабатываются только после того, как они полностью получены.

BGP является протоколом, ориентирующимся на вектор расстояния. Вектор описывается списком AS по 16 бит на AS. BGP регулярно (каждые 30сек) посылает соседям TCP-сообщения, подтверждающие, что узел жив (это не тоже самое что "Keepalive" функция в TCP). Если два BGP-маршрутизатора попытаются установить связь друг с другом одновременно, такие две связи могут быть установлены. Такая ситуация называется столкновением, одна из связей должна быть ликвидирована. При установлении связи маршрутизаторов сначала делается попытка реализовать высший из протоколов (например, BGP-4), если один из них не поддерживает эту версию, номер версии понижается

Протоколы ~~BGP-3~~ и BGP-4

Протокол BGP-4 является усовершенствованной версией (по сравнению с BGP-3). Эта версия позволяет пересылать информацию о маршруте в рамках одного IP-пакета. Концепция классов сетей и субсети находятся вне рамок этой версии.). *Далее(подробнее) см.* ***[4]*** *файл* *4.4.11.4 Внешний протокол BGP.doc* *стр.9* Для того чтобы приспособиться к этому, изменена семантика и кодирование атрибута AS_PASS. Введен новый атрибут **LOCAL_PREF** (степень предпочтительности маршрута для собственной AS), который упрощает процедуру выбора маршрута. Атрибут INTER_AS_METRICSпереименован в MULTI_EXIT_DISC (4 октета; служит для выбора пути к одному из соседей). Введены новые атрибуты **ATOMIC_AGGREGATE** и **AGGREGATOR**, которые позволяют группировать маршруты. Структура данных отражается и на схеме принятия решения, которая имеет три фазы:

1. Вычисление степени предпочтения для каждого маршрута, полученного от соседней AS, и передача информации другим узлам местной AS.
2. Выбор лучшего маршрута из наличного числа для каждой точки назначения и укладка результата в LOC-RIB.
3. Рассылка информации из loc_rib всем соседним AS согласно политике, заложенной в RIB. Группировка маршрутов и редактирование маршрутной информации.

Бесклассовая интердоменная маршрутизация (**CIDR**- classless interdomain routing) - способ избежать того, чтобы каждая С-сеть требовала свою таблицу маршрутизации. Основополагающий *принцип CIDR* заключается в группировке (агрегатировании) IP-адресов таким образом, чтобы сократить число входов в таблицах маршрутизации

Основу протокола CIDR составляет идея бесклассовых адресов, где нет деления между полем сети и полем ЭВМ.

Важным свойством протокола является возможность декларации резервного (backup) маршрута. Так, если основной маршрут автономной системы стал недоступен, маршрутизатор переключит поток на этот резервный канал. При этом пользователи сети не должны ожидать момента, когда администратор сети вернется из отпуска, проснется или вернется из кафетерия и сам внесет необходимые коррективы.

Протоколы BGP-3 и BGP-4. Атрибуты и их характеристики ??? *см.* ***[4]*** *файлы* *4.4.11.4 Внешний протокол BGP.doc* *???* *4.4.11.9 Мультипротокольные расширения для BGP-4.doc*

BGP-4. Атрибуты и их характеристики

Из *4.4.11.9 Мультипротокольные расширения для BGP-4.doc*

BGP-4 транспортирует три типа данных, которые ориентированы на IPv4:

a. атрибут NEXT_HOP (представляет собой адрес IPv4),
b. AGGREGATOR (содержит адрес IPv4) и
c. NLRI (представляет собой префикс IPv4).

Чтобы BGP-4 мог поддерживать несколько протоколов сетевого уровня, необходимо добавить две вещи:

a. возможность ассоциирования конкретного протокола сетевого уровня с данными о следующем шаге и
b. возможность для заданного протокола сетевого уровня работать с NLRI (Network Layer Reachibility Information).

Чтобы идентифицировать протокол сетевого уровня в данной статье используется понятие семьи адресов (Address Family),

В качестве транспорта BGP-4 использует протокол TCP с портом 179. Можно также заметить, что данные о следующем шаге (информация, предоставляемая атрибутом NEXT_HOP) имеет смысл (и необходима) только в сочетании с анонсированием достижимости адресатов, в сочетании с оповещением о недостижимости адресатов (ликвидация маршрута) данные о следующем шаге бессмысленны. Это предполагает, что анонсирование о достижимых адресатах следует группировать с анонсированием следующего шага, а оповещения о достижимых адресатах должны быть отделены от объявлений о недостижимых.

Чтобы обеспечить обратную совместимость, а также упростить введение мультипротокольных возможностей в BGP-4, в данном документе используются **новые атрибуты**:

- многопротокольная NLRI достижимости (MP_REACH_NLRI),
- и многопротокольная NLRI недостижимости (MP_UNREACH_NLRI).

Первый из них (MP_REACH_NLRI) используется для хранения набора достижимых адресатов и данных о следующем шаге, который следует использовать для достижения этих мест назначения. Второй атрибут (MP_UNREACH_NLRI) используется для хранения набора недостижимых адресатов. Таким способом партнер BGP, который не поддерживает мультипротокольные возможности, будет просто игнорировать информацию, содержащуюся в этих атрибутах, и не передаст эти данные другим BGP партнерам.

Атрибуты:

Многопротокольная NLRI достижимости - MP_REACH_NLRI

Это опционный не транзитивный атрибут, который может использоваться для следующих целей:

(a) Чтобы оповестить о возможном пути до партнера
(b) Чтобы позволить маршрутизатору сообщать об адресе сетевого уровня маршрутизатора, который следует использовать в качестве следующего шага на пути к месту назначения, указанному в поле информации достижимости сетевого уровня атрибута MP_NLRI.
(c) Чтобы позволить данному маршрутизатору уведомить некоторую или все точки подключения к субсети SNPA (Subnetwork Points of Attachment), которые имеются в локальной системе

Далее см. 4.4.11.9 Мультипротокольные расширения для BGP-4.doc стр.2

Мультипротокольное NLRI недостижимости - MP_UNREACH_NLRI

Это опционный не транзитивный атрибут, который может использоваться для целей аннулирования недоступных маршрутов. Атрибут имеет следующий формат:

Идентификатор семейства адресов (2 октета)
Идентификатор последующего семейства адресов (1 октет)
Ликвидируемые маршруты (переменная длина)

Далее см. 4.4.11.9 Мультипротокольные расширения для BGP-4.doc стр.4

Кодирование NLRI

Информация достижимости сетевого уровня кодируется в виде одного или более 2-полуоктетов в форме <длина, префикс>, представленной ниже:

Длина (1 октет)
Префикс (переменная длина)

Далее см. 4.4.11.9 Мультипротокольные расширения для BGP-4.doc стр.5

Динамические протоколы (обычно используются именно они, наиболее известным разработчиком является компания CISCO):

В маршрутизаторе с динамическим протоколом (например, **BGP-4**) резидентно загруженная программа-драйвер изменяет таблицы маршрутизации на основе информации, полученной от соседних маршрутизаторов.

Агрегирование каналов. . *см* *билет№34* [2]

Суть в том, что один канал функционирует, а остальные находятся в «горячем» резерве для замены отказавшей связи.

BGP-4 и CIDR

См. файлы 4.4.11.5 Бесклассовая интердоменная маршрутизация_CIDR.doc
и 4.1.1.3 Интернет в Ethernet_CIDR+VLSM.doc

...В связи с дефицитом адресов в сетке **IPv4** в последнее время все шире стала использоваться схема адресации supernet и маршрутизации без классов (**CIDR** -Ckassless Interdomain Routing). Эта технология появилась в 1993 году одновременно с появлением протокола **BGP-4**. Протокол CIDR формирует маршруты на базе непрерывных полей IP-адресов. В варианте без классов группа адресов представляется как единая сеть. Деление адресного пространства на подсети не имеет никакого отношения к протоколу CIDR. Адресное пространство CIDR может содержать любое число адресов с числом 2 в любой степени. Ниже в таблице представленя параметры сетевых адресов без классов

Агрегирование,
CIDR,
VLSM.

36. Технологии MPLS/IP и EoMPLS, концепция Label Switching, применение MPLS для построения виртуальных частных сетей (MPLS/VPN), пересекающиеся адресные пространства.

Материал из Википедии [3] см. также VPN и Классификация VPN

MPLS (англ. Multiprotocol Label Switching — мультипротокольная коммутация по меткам) — механизм передачи данных, который эмулирует различные свойства сетей с коммутацией каналов поверх сетей с коммутацией пакетов.

MPLS работает на уровне, который можно было бы расположить между вторым (канальным) и третьим (сетевым) уровнями модели OSI, и поэтому его обычно называют протоколом второго с половиной уровня (2.5-уровень). Он был разработан с целью обеспечения универсальной службы передачи данных как для клиентов сетей с коммутацией каналов, так и сетей с коммутацией пакетов. С помощью MPLS можно передавать трафик самой разной природы, такой как IP-пакеты, ATM, Frame Relay, SONET и кадры Ethernet.

В традиционной IP сети пакеты передаются от одного маршрутизатора другому и каждый маршрутизатор читая заголовок пакета (адрес назначения) принимает решение о том, по какому маршруту отправить пакет дальше.

В протоколе MPLS никакого последующего анализа заголовков в маршрутизаторах по пути следования не производится, а переадресация управляется исключительно на основе меток. *[3]*

Из. 4.4.17 Введение в MPLS, TE и QoS.doc ***(очень сложно)*** подробнее см. **MPLS**

Именно идея сохранения в маршрутной таблице только реально используемых виртуальных путей и легла в основу разработки протокола MPLS

Технология виртуальных сетей L2 позволяет сформировать в локальной сети соединение точка-точка. В таком соединении можно гарантировать пропускную способность на уровне 10/100Мбит/с.

Протокол MPLS хорошо приспособлен для формирования виртуальных сетей (VPN) ***повышенного быстродействия*** (метки коммутируются быстрее, чем маршрутизируются пакеты). Принципиальной основой MPLS являются IP-туннели. Для его работы нужна поддержка протокола маршрутизации MP-BGP (RFC-2858 [23]). Протокол MPLS может работать практически для любого маршрутизируемого транспортного протокола (не только IP). После того как сеть сконфигурирована (для этого используются специальные, поставляемые производителем скрипты), сеть существует, даже если в данный момент через нее не осуществляется ни одна сессия. При появлении пакета в виртуальной сети ему присваивается метка, которая не позволяет ему покинуть пределы данной виртуальной сети. Никаких других ограничений протокол MPLS не накладывает. Протокол MPLS предоставляет возможность обеспечения значения QoS, гарантирующего более высокую безопасность. Не следует переоценивать уровня безопасности, гарантируемого MPLS, атаки типа “человек посередине” могут быть достаточно разрушительны. При этом для одного и того же набора узлов можно сформировать несколько разных виртуальных сетей (используя разные метки), например, для разных видов QoS.

Для обеспечения структурирования потоков в пакете создается стек меток, каждая из которых имеет свою зону действия.

Управление трафиком MPLS основано на следующих механизмах IOS:

- **Туннелях LSP** (Label-switched path), которые формируются посредством RSVP, с расширениями системы управления трафиком. Туннели LSP представляют собой туннельные двунаправленные интерфейсы IOS с известным местом назначения.
- **Протоколах маршрутизации IGP**, базирующиеся на состоянии канала (такие как IS-IS) с расширениями для глобальной рассылки ресурсной информации, и расширениях для автоматической маршрутизации трафика по LSP туннелям.
- **Модуле вычисления пути MPLS**, который определяет пути для LSP туннелей.
- **Модуле управления трафиком MPLS**, который обеспечивает доступ и запись ресурсной информации, подлежащей рассылке.
- **Переадресации согласно меткам**, которая предоставляет маршрутизаторам возможности, сходные с уровнем L2, перенаправлять трафик через большое число узлов согласно алгоритму маршрутизации отправителя.

Выводы

- Протокол MPLS является удобным средством формирования корпоративных сетей (VPN), которые позволяют поднять их безопасность.
- Протокол MPLS предоставляет гибкие средства мониторинга трафика в пределах VPN.
- **Переход на IPv6** существенно расширяет возможности управления трафиком за счет использования меток потоков (пока не ясно насколько эта возможность поддерживается

программно). Данное свойство особенно важно для передачи мультимедийных данных, например, программ цифрового телевидения. Последнее предполагает значительное расширение интегральной полосы каналов опорной сети (хотя бы до 155Мбит/с).

Частные виртуальные сети 4.4.21 BGP_MPLS VPN.doc **см. также** Классификация VPN

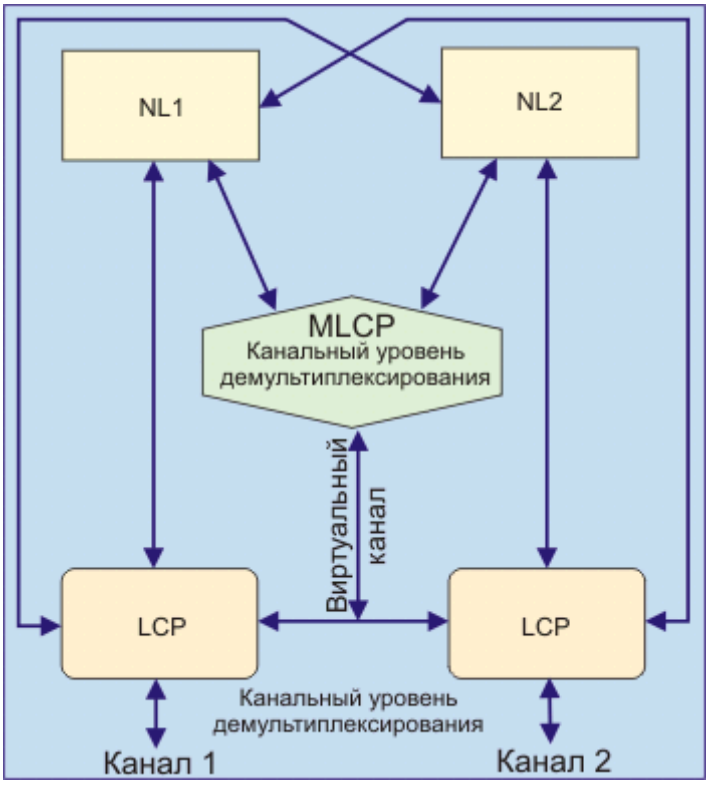
Рассмотрим набор сайтов, которые подсоединены к общей сети, называемой опорной. Определим некоторую политику при создании субнаборов этого набора, и введем следующее правило: два сайта могут взаимодействовать друг с другом через опорную сеть, только если, по крайней мере, один из этих субнаборов содержит оба эти сайта.

Субнаборы, которые создаются, являются "Частными виртуальными сетями" (VPN). Два сайта имеют IP коннективность через опорную сеть, только если существует VPN, которая содержит в себе оба эти сайта. Два сайта, которые не имеют общих VPN, не имеют связи через опорную сеть. ????

Всё описано у Семёнова[4] (п. 4.4.17– 4.4.23) но очень сложно

Рис. 3.5.6. Пример Multilink-конфигурации

3.5 Протокол PP.doc



37. Механизмы обеспечения качества обслуживания (QoS) в IPv4, различные подходы к обеспечению QoS в зависимости от задачи, алгоритмы обслуживания и предотвращения перегрузки сети.

Из шпоргалки [2] п. 17

Поддержка QoS

В условиях экономного отношения пропускной способности канала в глобальных сетях требуется применение методов обеспечения качества обслуживания (**Quality of Service**).

Типы служб QoS в зависимости от строгости соблюдения гарантий:

- сервис с максимальными усилиями (отсутствие QoS)
- сервис с предпочтением. Некоторые типы трафика обслуживаются лучше чем остальные. Это статистическое предпочтение.
- гарантированный сервис. Дает статистические численные гарантии (близкие к 1) различным потокам трафика.

Базовая архитектура QoS включает:

- средства QoS узла, выполняющие обработку поступающего в узел трафика.
- протоколы QoS-сигнализации для координации работы сетевых элементов по поддержке качества обслуживания
- централизованные функции политики, управления и учета QoS

Средства QoS узла состоят из механизмов обслуживания очередей и механизмов кондиционирования трафика. Механизм кондиционирования трафика обычно включает классификацию, профилирования и формирования трафика.

Протоколы сигнализации QoS нужны механизмам QoS в отдельных узлах для обмена служебной информацией [2]

См. также файл 4.4.3.2 Качество обслуживание (QoS) в локальных сетях и не только.doc

Из [4] см. файл 4.4.11.2 Протокол OSPF.doc

Качество сервиса (QoS) может характеризоваться следующими параметрами:

- пропускной способностью канала;
- задержкой (время распространения пакета);
- числом дейтограмм, стоящих в очереди для передачи;
- загрузкой канала;
- требованиями безопасности;
- типом трафика;
- числом шагов до цели;
- возможностями промежуточных связей (например, многовариантность достижения адресата).

Из [3] (wiki) см. QoS_wiki.doc

QoS (англ. Quality of Service — качество обслуживания) — этим термином в области компьютерных сетей называют вероятность того, что сеть связи соответствует заданному соглашению о трафике, или же, в ряде случаев, неформальное обозначение вероятности прохождения пакета между двумя точками сети

Механизм работы

Для большинства случаев качество связи определяется четырьмя параметрами:

- Полоса пропускания (Bandwidth), описывает номинальную пропускную способность среды передачи информации, определяет ширину канала. Измеряется в bit/s (bps), kbit/s (kbps), Mbit/s (Mbps), Gbit/s (Gbps).
- Задержка при передаче пакета (Delay), измеряется в миллисекундах.
- Колебания (дрожание) задержки при передаче пакетов — джиттер (Jitter).
- Потеря пакетов (Packet loss). Определяет количество пакетов, потерянных в сети во время передачи.

Протоколы, которые предоставляют услугу QoS

- IP Differentiated services (DiffServ)

- IP Integrated services (IntServ)
- Resource reSerVation Protocol (RSVP)
- Multiprotocol Label Switching (**MPLS**)
- RSVP-TE
- Frame relay
- X.25
- Некоторые ADSL-модемы
- Asynchronous Transfer Mode (ATM)
- IEEE 802.1p
- IEEE 802.1Q
- IEEE 802.11e
- IEEE 802.11p
- HomePNA

[3]

Из Олифера [1]

...В связи с дефицитом адресов в сетке **IPv4** в последнее время все шире стала использоваться схема адресации supernet и маршрутизации без классов (**CIDR** -Ckassless Interdomain Routing). Эта технология появилась в 1993 году одновременно с появлением протокола **BGP-4**. Протокол CIDR формирует маршруты на базе непрерывных полей IP-адресов. В варианте без классов группа адресов представляется как единая сеть. Деление адресного пространства на подсети не имеет никакого отношения к протоколу CIDR. Адресное пространство CIDR может содержать любое число адресов с числом 2 в любой степени. Ниже в таблице представленя параметры сетевых адресов без классов (см. 4.1.1.3 Интернет в Ethernet_CIDR+VLSM.doc)

Из. 4.4.17 Введение в MPLS, TE и QoS.doc

Качество обслуживания QoS *(может быть тоько для MPLS ???)*

QoS связана с возможностью сети предоставить клиенту необходимый ему уровень услуг в условиях работы поверх сетей с самыми разнообразными технологиями, включая Frame Relay, ATM, Ethernet, сети 802.1, SONET, и маршрутизуемые IP-сети.

QoS представляет собой собрание технологий, которые позволяют приложениям запрашивать и получать предсказуемый уровень услуг с точки зрения

- пропускной способности,
- временного разброса задержки отклика,
- а также общей задержки доставки данных.

В частности, QoS подразумевает улучшение параметров или достижение большей предсказуемости предоставляемых услуг. Это достигается следующими методами:

- Поддержкой определенной полосы пропускания.
- Сокращением вероятности потери кадров.
- Исключением или управляемостью сетевых перегрузок.
- Возможностью конфигурирования сетевого трафика.
- Установкой количественных характеристик трафика по пути через сеть.

IEFT определяет для QoS следующие две архитектуры:

- Интегрированные услуги (IntServ)
- Дифференцированные услуги (DiffServ)

IntServ для явного задания уровня услуги (QoS) использует протокол RSVP. Это делается путем уведомления об этом требовании всех узлов вдоль пути обмена. Если все сетевые устройства вдоль пути могут предоставить запрошенную полосу, резервирование завершается успешно (смотри документ RFC-1633 [2]).

DiffServ, вместо того чтобы уведомлять о требованиях приложения, использует в IP-заголовке DiffServ Code Point (DSCP), чтобы указать требуемые уровни QoS. Cisco IOS® Software Release 12.1(5)T вводит совместимость маршрутизаторов Cisco с DiffServ (см. [15-16]). DSCP размещается в поле TOS IP-пакета

L2 QoS предполагает: см. эту ссылку

38. Виртуальные частные сети как механизм туннелирования траффика, технологии PPTP и L2TP, особенности применения и отличительные особенности.

Из шпоргалки [2] п. 39 см. также Классификация VPN и Билет №39

Основы технологий виртуальных частных сетей VPN. Сети VPN создаются для организации взаимодействия индивидуальных пользователей с удаленной сетью через Internet и для связи нескольких ЛВС. Также с помощью VPN может быть реализовано и такое приложение как Extranet, позволяющее через Internet связывать с сетью компании сети ее заказчиков, поставщиков и партнеров. Главное преимущество виртуальных частных сетей - невысокая стоимость их создания и эксплуатации.

Структура виртуальной сети состоит из каналов глобальной сети, защищенных протоколов и маршрутизатороов. Для объединения удаленных ЛВС в виртуальную сеть используются так называемые виртуальные выделенные каналы. Для организации подобных соединений применяется **механизм туннелирования**. (см. [4] 4.4.1.2 IP-туннели.doc и 4.4.1.3 Протокол туннелей на сетевом уровне L2 (L2TP).doc в разделе 4.4.1.0 IP-протокол.doc) Инициатор туннеля инкапсулирует пакеты локальной сети в IP-пакеты, содержащие в заголовке адреса инициатора и терминатора туннеля. Терминатор туннеля извлекает исходный пакет. Конфиденциальность передаваемой корпоративной информации достигается шифрованием.

Основная проблема сетей VPN - отсутствие устоявшихся стандартов аутентификации и обмена шифрованной информацией. Эти стандарты все еще находятся в процессе разработки и не всегда реализуются в продуктах различных изготовителей. Возможность построения VPN на оборудовании и ПО различных производителей достигается внедрением некоторого стандартного механизма.

Таким механизмом выступает протокол **Internet Protocol Security (IPSec)**, он описывает все стандартные методы VPN. Этот протокол определяет методы идентификации при инициализации туннеля, методы шифрования в конечных точках туннеля и механизмы обмена и управления ключами шифрования между этими точками. В числе других механизмов построения VPN можно назвать: протокол **PPTP (Point-to-Point Tunneling Protocol)**, разработанный компаниями Ascend Communications и 3Com, протокол L2F (Layer-2 Forwarding) компании Cisco Systems, протокол **L2TP (Layer-2 Tunneling Protocol)**, объединивший оба вышеназванных протокола.

Вариант «Intranet VPN», который позволяет объединить в единую защищенную сеть несколько распределенных филиалов одной организации, взаимодействующих по открытым каналам связи. Именно этот вариант получил широкое распространение во всем мире, и именно его в первую очередь реализуют компании-разработчики. Вариант «Remote Access VPN», позволяющий реализовать защищенное взаимодействие между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который подключается к корпоративным ресурсам из дома (домашний пользователь) или через notebook (мобильный пользователь). Данный вариант отличается от первого тем, что удаленный пользователь, как правило, не имеет «статического» адреса и подключается к защищаемому ресурсу не через выделенное устройство VPN, а напрямую с собственного компьютера, где и устанавливается программное обеспечение, реализующее функции VPN. Вариант «Client/Server VPN», который обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например между рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда необходимо создать в одной физической несколько логических сетей. Например, когда требуется разделить трафик между финансовым департаментом и отделом кадров, которые обращаются к серверам, находящимся в одном физическом сегменте. Этот вариант похож на технологию VLAN, которая действует на уровне выше канального. Вариант «Extranet VPN» предназначен для тех сетей, куда подключаются так называемые пользователи со стороны, уровень доверия к которым намного ниже, чем к своим сотрудникам. [2]

Материал из Википедии [3] L2TP-wiki.doc

L2TP (англ. Layer 2 Tunneling Protocol) — сетевой протокол туннелирования канального уровня, сочетающий в себе протокол L2F (Layer 2 Forwarding Protocol), разработанный компанией Cisco, и протокол PPTP корпорации Microsoft. Стандарт IETF. Позволяет организовывать VPN с заданными приоритетами доступа, однако не содержит в себе средств шифрования и механизмов аутентификации (для создания защищённой VPN его используют совместно с IPSec)

L2TP	
Название:	Layer 2 Tunneling Protocol
Уровень (по модели OSI):	Канальный
Семейство:	TCP/IP
Создан в:	1999 г.
Порт/ID:	1701/TCP, 1701/UDP
Спецификация:	RFC 2661

Материал из Википедии [3] PPTP-wiki.doc

PPTP (англ. Point-to-point tunneling protocol) — туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной, незащищённой сети. PPTP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например Интернет. PPTP может также использоваться для организации туннеля между двумя локальными сетями. PPTP использует дополнительное TCP-соединение для обслуживания туннеля.

Спецификация

Спецификация протокола была опубликована как «информационная» RFC 2637 в 1999 году. Она не была ратифицирована IETF. Протокол считается менее безопасным, чем IPSec. PPTP работает, устанавливая обычную PPP сессию с противоположной стороной с помощью протокола Generic Routing Encapsulation. Второе соединение на TCP-порту 1723 используется для инициации и управления GRE-соединением. PPTP сложно перенаправлять за сетевой экран, так как он требует одновременного установления двух сетевых сессий. *[3]*

Протокол PPP служит и для создания межсетевых туннелей (протокол PPTP - Point to Point Tunneling Protocol). Протокол PPTP использует MTU=1532, номер порта 5678 и номер версии 0x0100, пакеты данных здесь транспортируются с использованием протокола инкапсуляции GRE V2 (см. сноску в начале раздела). 3.5 Протокол PP.doc

*Семёнов**(очень сложно)** [4]* 4.4.1.3 Протокол туннелей на сетевом уровне L2 (L2TP).doc

Протокол PPP [RFC1661] определяет механизм инкапсуляции для транс пировки мультипротокольных пакетов для соединений точка-точка сетевого уровня L2.

Протокол L2TP расширяет модель PPP, позволяя размещение терминальных точек L2 и PPP в различных физических устройствах, подключенных к сети с коммутацией пакетов. В L2TP, пользователь имеет соединение L2 с концентратором доступа (например, модемным пулом, ADSL DSLAM, и т.д.), а концентратор в свою очередь туннелирует индивидуальные PPP-кадры в NAS.

На диаграмме (рис. 1.) показана схема работы протокола L2TP. Целью здесь является туннелирование кадров PPP между удаленной системой или клиентом LAC и LNS, размещенной в LAN.

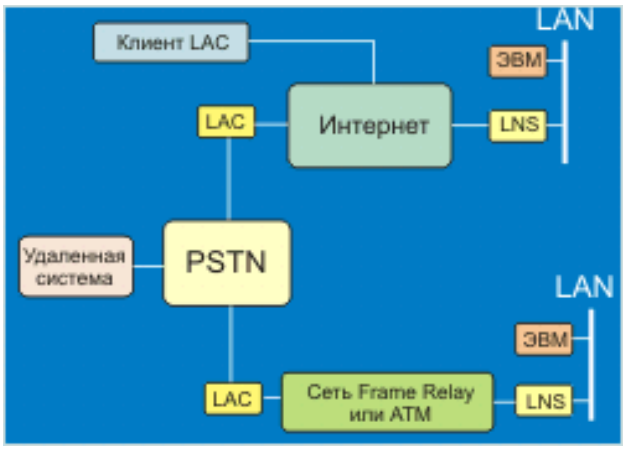


Рис. 1. Схема работы протокола L2TP

Удаленная система инициирует PPP-соединение с LAC через коммутируемую телефонную сеть PSTN. LAC затем прокладывает туннель для PPP-соединения через Интернет, Frame Relay или ATM к LNS, посредством чего осуществляется доступ к исходной LAN (Home LAN). Адреса удаленной системе предоставляются исходной LAN через согласование с PPP NCP. Аутентификация, авторизация и аккоунтинг могут быть предоставлены областью управления LAN, как если бы пользователь был непосредственно соединен с сервером сетевого доступа NAS

L2TP использует два вида пакетов,

- управляющие
- и информационные сообщения.

Управляющие сообщения используются при установлении, поддержании и аннулировании туннелей и вызовов. Информационные сообщения используются для инкапсуляции PPP-кадров пересылаемых по туннелю. Управляющие сообщения используют надежный контрольный канал в пределах L2TP, чтобы гарантировать

PPP кадры		
L2TP Информационные сообщения		L2TP Управляющие сообщения
L2TP Информационный канал (ненадежный)		L2TP Канал управления (надежный)
Транспортировка пакетов (UDP, FR, ATM, etc.)		

Рис. 2.0. Структура протокола L2TP

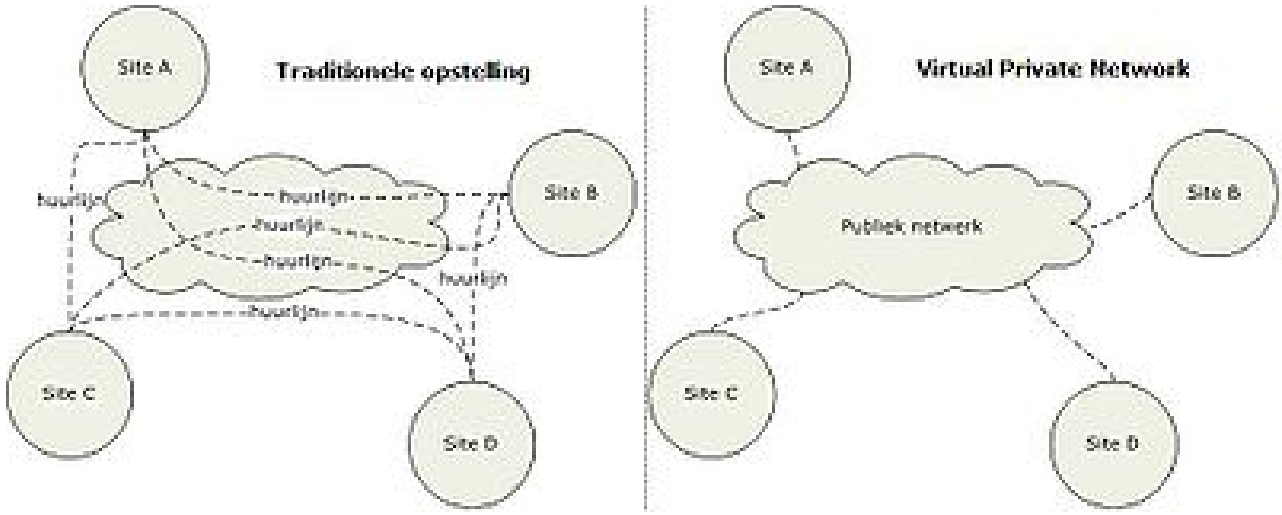
???? *Всё описано у Семёнова[4] но очень сложно*

38. *Продолжение* - Виртуальные частные сети VPN

Совокупность защищённых каналов, созданных предприятиемв публичной сети для объединения своих филиалов, часто называют **виртуальной частной сетью** (Virtual Private Network, **VPN**) [6] гл.12 стр.617

Материал из Википедии [3] VPN-wiki.doc

VPN (англ. Virtual Private Network — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрованию, аутентификация, инфраструктуры публичных ключей, средствам для защиты от повторов и изменения передаваемых по логической сети сообщений).



Traditional ***Virtual Private Network***

В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть.

Уровни реализации

Обычно VPN развёртывают на уровнях не выше сетевого, так как применение криптографии на этих уровнях позволяет использовать в неизменном виде транспортные протоколы (такие как TCP, UDP).

Пользователи Microsoft Windows обозначают термином VPN одну из реализаций виртуальной сети — **PPTP**, причём используемую зачастую не для создания частных сетей.

Чаще всего для создания виртуальной сети используется инкапсуляция протокола PPP в какой-нибудь другой протокол — IP (такой способ использует реализация **PPTP** — Point-to-Point Tunneling Protocol). Технология VPN в последнее время используется не только для создания собственно частных сетей, но и некоторыми провайдерами «последней мили» для предоставления выхода в Интернет.

При должном уровне реализации и использовании специального программного обеспечения сеть VPN может обеспечить высокий уровень шифрования передаваемой информации. При правильной настройке всех компонентов технология VPN обеспечивает анонимность в Сети.

Структура VPN

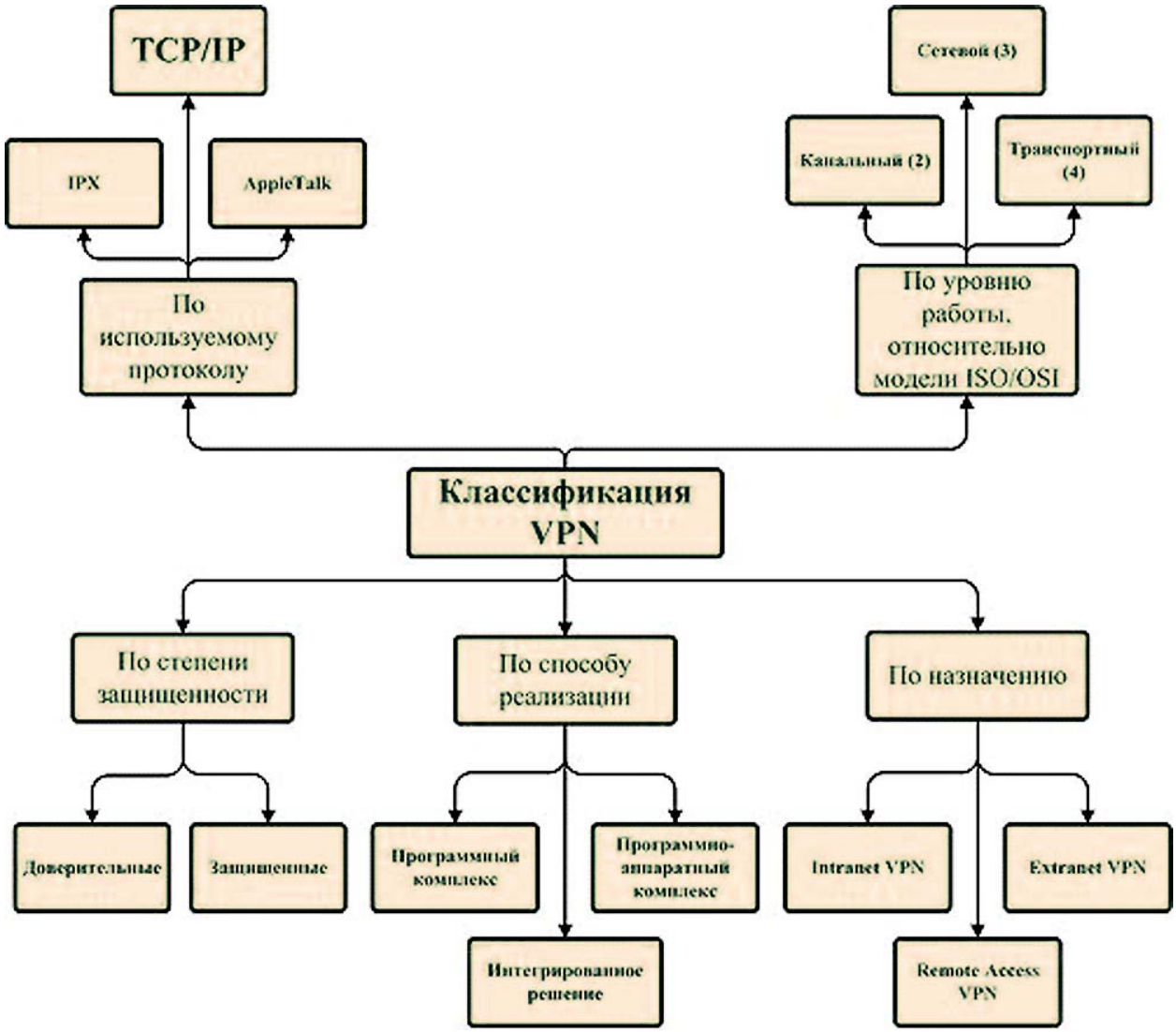
VPN состоит из двух частей:

- «внутренняя» (подконтрольная) сеть, которых может быть несколько,
- и «внешняя» сеть, по которой проходит инкапсулированное соединение (обычно используется Интернет).

Возможно также подключение к виртуальной сети отдельного компьютера. Подключение удалённого пользователя к VPN производится посредством сервера доступа, который подключён как к внутренней, так и к внешней (общедоступной) сети. При подключении удалённого пользователя (либо при установке соединения с другой защищённой сетью) сервер доступа требует прохождения процесса идентификации, а затем процесса аутентификации.

После успешного прохождения обоих процессов, удалённый пользователь (удаленная сеть) наделяется полномочиями для работы в сети, то есть происходит процесс авторизации.

Классификация VPN



Классификация VPN

Классифицировать VPN решения можно по нескольким основным параметрам:

По степени защищенности используемой среды

Защищённые

Наиболее распространённый вариант виртуальных частных сетей. С его помощью возможно создать надежную и защищенную подсеть на основе ненадёжной сети, как правило, Интернета. Примером защищённых VPN являются: **IPSec**, OpenVPN и **PPTP**.

Доверительные

Используются в случаях, когда передающую среду можно считать надёжной и необходимо решить лишь задачу создания виртуальной подсети в рамках большей сети. Вопросы обеспечения безопасности становятся неактуальными. Примерами подобных VPN решений являются: Multi-protocol label switching (**MPLS**) и **L2TP** (Layer 2 Tunnelling Protocol). (точнее сказать, что эти протоколы перекладывают задачу обеспечения безопасности на другие, например L2TP, как правило, используется в паре с IPSec).

По способу реализации

- **В виде специального программно-аппаратного обеспечения**

Реализация VPN сети осуществляется при помощи специального комплекса программно-аппаратных средств. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищённости.

- **В виде программного решения**

Используют персональный компьютер со специальным программным обеспечением, обеспечивающим функциональность VPN.

- **Интегрированное решение**

Функциональность VPN обеспечивает комплекс, решающий также задачи фильтрации сетевого трафика, организации сетевого экрана и обеспечения качества обслуживания.

По назначению

- **Intranet VPN**

Используют для объединения в единую защищённую сеть нескольких распределённых филиалов одной организации, обменивающихся данными по открытым каналам связи.

- **Remote Access VPN**

Используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам с домашнего компьютера, корпоративного ноутбука, смартфона или интернет-киоска.

- **Extranet VPN**

Используют для сетей, к которым подключаются «внешние» пользователи (например, заказчики или клиенты). Уровень доверия к ним намного ниже, чем к сотрудникам компании, поэтому требуется обеспечение специальных «рубежей» защиты, предотвращающих или ограничивающих доступ последних к особо ценной, конфиденциальной информации.

- **Internet VPN**

Используется для предоставления доступа к интернету провайдерами, обычно в случае если по одному физическому каналу подключаются несколько пользователей.

- **Client/Server VPN**

Он обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда в одной физической сети необходимо создать несколько логических сетей. Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, обращающихся к серверам, находящимся в одном физическом сегменте. Этот вариант похож на технологию VLAN, но вместо разделения трафика, используется его шифрование.

По типу протокола

Существуют реализации виртуальных частных сетей под TCP/IP, IPX и AppleTalk. Но на сегодняшний день наблюдается тенденция к всеобщему переходу на протокол TCP/IP, и абсолютное большинство VPN решений поддерживает именно его. Адресация в нём чаще всего выбирается в соответствии со стандартом RFC5735, из диапазона Приватных сетей TCP/IP

По уровню сетевого протокола

По уровню сетевого протокола на основе сопоставления с уровнями эталонной сетевой модели ISO/OSI.

Примеры VPN

- IPSec (IP security) — часто используется поверх IPv4.
- PPTP (point-to-point tunneling protocol) — разрабатывался совместными усилиями нескольких компаний, включая Microsoft.
- PPPoE (PPP (Point-to-Point Protocol) over Ethernet
- L2TP (Layer 2 Tunnelling Protocol) — используется в продуктах компаний Microsoft и Cisco.
- L2TPv3 (Layer 2 Tunnelling Protocol version 3).
- OpenVPN SSL VPN с открытым исходным кодом, поддерживает режимы PPP, bridge, point-to-point, multi-client server

39. Построение защищенных каналов связи поверх IP с использованием технологии IPSEC, интеграция IPSEC в IPv6, использование IPSEC в IPv4. Протоколы IKE, ISAKMP, AH, ESP.

Из шпоргалки [2] п. 39 см. билет №38 см. также VPN и Классификация VPN

Основы технологий виртуальных частных сетей VPN. Сети VPN создаются для организации взаимодействия индивидуальных пользователей с удаленной сетью через Internet и для связи нескольких ЛВС. Также с помощью VPN может быть реализовано и такое приложение как Extranet, позволяющее через Internet связывать с сетью компании сети ее заказчиков, поставщиков и партнеров. Главное преимущество виртуальных частных сетей - невысокая стоимость их создания и эксплуатации.

Структура виртуальной сети состоит из каналов глобальной сети, защищенных протоколов и маршрутизатороов. Для объединения удаленных ЛВС в виртуальную сеть используются так называемые виртуальные выделенные каналы. Для организации подобных соединений применяется **механизм туннелирования**. Инициатор туннеля инкапсулирует пакеты локальной сети в IP-пакеты, содержащие в заголовке адреса инициатора и терминатора туннеля. Терминатор туннеля извлекает исходный пакет. Конфиденциальность передаваемой корпоративной информации достигается шифрованием.

Основная проблема сетей VPN - отсутствие устоявшихся стандартов аутентификации и обмена шифрованной информацией. Эти стандарты все еще находятся в процессе разработки и не всегда реализуются в продуктах различных изготовителей. Возможность построения VPN на оборудовании и ПО различных производителей достигается внедрением некоторого стандартного механизма.

Таким механизмом выступает протокол **Internet Protocol Security (IPSec)**, он описывает все стандартные методы VPN. Этот протокол определяет методы идентификации при инициализации туннеля, методы шифрования в конечных точках туннеля и механизмы обмена и управления ключами шифрования между этими точками. В числе других механизмов построения VPN можно назвать: протокол **PPTP (Point-to-Point Tunneling Protocol)**, разработанный компаниями Ascend Communications и 3Com, протокол L2F (Layer-2 Forwarding) компании Cisco Systems, протокол **L2TP (Layer-2 Tunneling Protocol)**, объединивший оба вышеназванных протокола.

Материал из Семёнова [4] см. 6.14 Технология IpSec.doc, безопасность

Технология IPsec

IPsec представляет собой набор протоколов для обеспечения безопасности сетевого соединения. Протоколы IPsec разработаны IETF (Internet Engineering Task Force). Под безопасностью здесь подразумевается: контроль доступа, обеспечение сохранности данных, идентификация отправителя, защита от атак воспроизведения и секретность обмена. Первые документы, регламентирующие IPsec, были приняты в 1998-99 годах (RFC-2401-02, -2406, -2408 и -2709). Существуют версии IPsec для IPv4 и IPv6. Важной особенностью этой технологии является то, что пользователь может даже не знать, что он пользуется IPsec и, как правило, нет необходимости адаптировать для работы с IPsec уже существующие приложения. И, тем не менее, дебаты и обсуждения области и способов применения этой технологии продолжаются. Связано это с тем, что если, например комбинация WEB-сервера/клиента поддерживает эту функцию, разработчик должен гарантировать, что данная услуга будет доступна на всех платформах, где данное приложение может работать.

В IPsec используются две базы данных: SPD (Security Policy Database, куда записываются правила обеспечения безопасности) и SADB (Security Association Database, где хранятся данные об активных ассоциациях безопасности).

Система IPsec предлагает многовариантный механизм реализации безопасности для обоих концов соединения. Эта техника пригодна для отдельного пользователя, особенно если он работает на выезде, и для виртуальных субсетей организаций, работающих с данными, которые требуют секретности.

При использовании совместно с Firewall IPsec предоставляет высокий уровень безопасности. При этом нужно иметь в виду, что для реализации IPsec оба партнера должны иметь оборудование и/или программы, которые поддерживают эти протоколы.

IPsec предусматривает процедуры аутентификации и шифрования. Формирование и удаления заголовка IPsec может осуществляться в машине клиента или в сетевом шлюзе (маршрутизаторе).

Протокол IPsec предоставляет три вида услуг: аутентификацию (**AH**), шифрование (**ESP**) и безопасную пересылку ключей. Обычно желательны обе первые услуги, так как неавторизованный клиент не сможет проникнуть в **VPN** (Virtual Private Network - виртуальная

частная сеть), а шифрование не позволит злоумышленникам прочитать, исказить или подменить сообщения. По этой причине протокол ESP предпочтительнее, так как он позволяет совместить обе эти услуги. Схема транспортировки данных в рамках IPsec показана на рис. 1. Это типичный пример IPsec-туннеля.

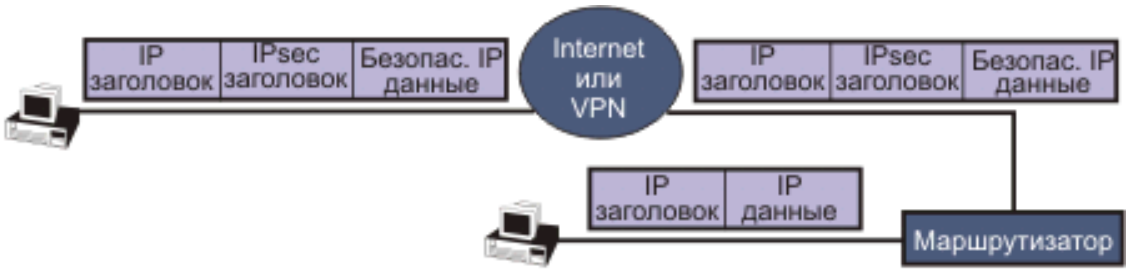


Рис. 1. Общая схема преобразования данных в IPsec

AH и ESP

Заголовок аутентификации (**AH**) и Encapsulating Security Payload (**ESP**) являются двумя протоколами нижнего уровня, используемыми IPsec, именно они осуществляют аутентификацию и шифрование+аутентификацию данных, передаваемых через соединение. Эти механизмы обычно используются независимо, хотя возможно (но не типично) их совместное применение.

Режим туннеля и транспортный режим

Транспортный режим обеспечивает безопасное соединение двух терминалов путем инкапсуляции содержимого IP-данных, в то время как туннельный режим инкапсулирует весь IP-пакет на участке между шлюзами. Последний вариант используется для формирования традиционной VPN, где туннель создает безопасный путь через полный опасностей Интернет.

Установление IPsec-соединения подразумевает любые варианты крипто-алгоритмов, но ситуация существенно упрощается благодаря тому, что обычно допустимо использование двух, максимум трех вариантов.

На фазе аутентификации вычисляется контрольная сумма ICV (Integrity Check Value) пакета с привлечением алгоритмов MD5 или SHA-1. При этом предполагается, что оба партнера знают секретный ключ, который позволяет получателю вычислить ICV и сравнить с результатом, присланным отправителем. Если сравнение ICV прошло успешно, считается, что отправитель пакета аутентифицирован. Протокол AH всегда осуществляет аутентификацию, а ESP выполняет ее опционно.

Шифрование использует секретный ключ для кодирования данных перед их транспортировкой, что исключает доступ к содержимому со стороны злоумышленников. В системе IPsec могут использоваться следующие алгоритмы: DES, 3DES, Blowfish, CAST, IDEA, RC5 и AES. Но, в принципе, разрешены и другие алгоритмы. Так как обе стороны диалога должны знать секретный ключ, используемый при хэшировании или шифровании, существует проблема транспортировки этих ключей. Возможен ввод ключей вручную, когда эти коды вводятся при конфигурации системы с помощью клавиатуры обоими партнерами. При этом предполагается, что доставка этих кодов осуществлена каким-то достаточно безопасным методом, алгоритм же **IKE** (Internet Key Exchange – обмен ключами по Интернет) является безопасным механизмом пересылки ключей в реальном масштабе времени, например, через Интернет.

Протокол AH

Протокол AH используется для аутентификации, но не для шифрования IP трафика, и служит для подтверждения того, что мы связаны именно с тем, с кем предполагаем, что полученные данные не искажены и не подменены при транспортировке.

Аутентификация выполняется путем вычисления зашифрованного аутентификационного хэш-кода сообщения. Хэширование охватывает практически все поля IP пакета (исключая только те, которые могут модифицироваться при транспортировке, например, TTL или контрольная сумма заголовка). Этот код записывается в AH заголовке и пересылается получателю. *Далее см. см. 6.14 Технология IpSec.doc, безопасность*

Построение VPN

При полном перекрытии аутентификационного заголовка и инкапсулированного поля данных можно построить настоящую VPN (Virtual Private Network). Конечной целью VPN является объединение двух безопасных сетей через небезопасные каналы (например, сети двух

отделений компании через Internet). Схема построения VPN показана на рис. 8. Предполагается, что обработка пакетов VPN на входе/выходе локальных сетей осуществляется в сетевых шлюзах (GW). Функции GW могут выполнять и сетевые экраны (Firewall).

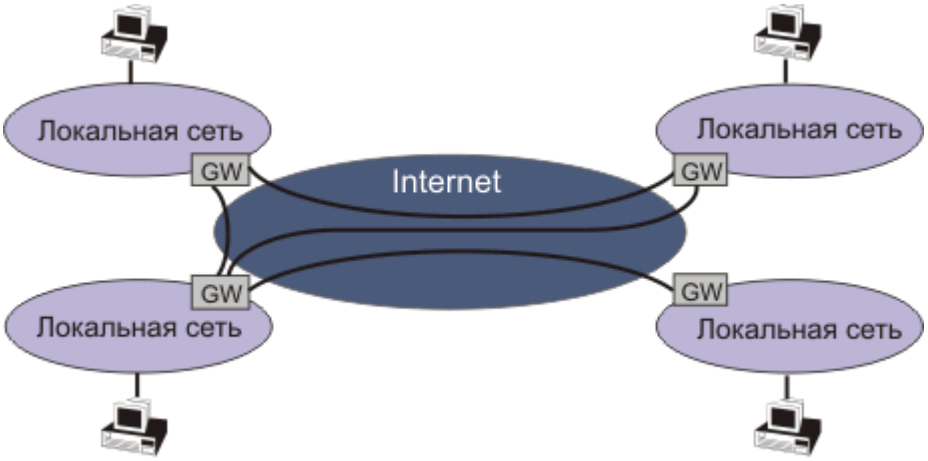


Рис. 8. Схема построения VPN

Понятно, что безопасные VPN требуют применения, как аутентификации, так и шифрования. Известно, что ESP является лишь средством обеспечения шифрования, но ESP и AH могут осуществлять аутентификацию.

Ассоциации безопасности и SPI

Кажется самоочевидным, что если два партнера или шлюза намереваются установить безопасное соединение, необходим некоторый объем общих секретных данных для реализации аутентификации и/или алгоритмов шифрования. Существует, конечно, проблема безопасной транспортировки этих секретных данных.

Когда IPsec-дейтограмма, AH или ESP попадает в интерфейс, как интерфейс узнает, какой набор параметров (ключ, алгоритм и политика) использовать? Любая машина может вести много диалогов, каждый со своим набором параметров безопасности и нужен механизм управления этим процессом.

Параметры безопасности задаются SA (Security Association), которая определяет параметры и процедуры, специфические для конкретного соединения. Каждый партнер может иметь один или более SA. Когда дейтограмма приходит, для нахождения правильного SA в базе данных SADB (Security Associations Database – база данных ассоциаций безопасности) используются три значения:

- IP адрес места назначения.
- IPsec протокол (ESP или AH, содержится в заголовке).
- Индекс параметров безопасности (SPI).

Во многих отношениях эта тройка может быть уподоблена IP сокету, который однозначно определяется IP адресом удаленного партнера (IPv4 или IPv6), протоколом и номером порта. В перечень компонентов SA входят:

- Номер по порядку. 32-битовый код, используемый для формирования поля порядковый номер в заголовках AH и ESP.
- Переполнение счетчика порядкового номера. Флаг, индицирующий переполнение счетчика порядкового номера. При его установке дальнейшая посылка пакетов для заданной SA должна быть прекращена.
- Окно для подавления попыток атак воспроизведения. Используется для определения того, является ли входящий AH- или ESP-пакет воспроизведением. Задача решается путем контроля того, попадает ли номер пакета в скользящее окно номеров.
- Информация AH. алгоритм аутентификации, ключи, время жизни ключей и другие параметры.
- Информация ESP: алгоритмы шифрования и аутентификации, ключи, параметры инициализации (IV), времена жизни ключей и другие параметры.
- Окно для подавления попыток атак воспроизведения. Используется для определения того, является ли входящий AH- или ESP-пакет воспроизведением. Задача решается путем контроля того, попадает ли номер пакета в скользящее окно номеров.
- Информация AH. алгоритм аутентификации, ключи, время жизни ключей и другие параметры.
- Информация ESP: алгоритмы шифрования и аутентификации, ключи, параметры инициализации (IV), времена жизни ключей и другие параметры.

- Режим работы IPsec. Туннельный, транспортный или любой.
- MTU пути. Максимальный размер пакета, который может быть передан через виртуальный канал без фрагментации.

При создании новой SA в счетчик номера по порядку заносится нуль, далее он инкрементируется при посылке каждого пакета. Когда содержимое счетчика достигает значения 232-1, текущая SA аннулируется и должна быть согласована новая ассоциация безопасности и новый ключ.

В базе данных SADB содержится:
- AH: алгоритм аутентификации.
- AH: аутентификационный секретный ключ (authentication secret).
- ESP: алгоритм шифрования.
- ESP: секретный ключ шифрования.
- ESP: разрешение аутентификации (yes/no).
- Параметры обмена ключами.
- Ограничения маршрутизации.
- **IP политика фильтрации**.

Некоторые реализации поддерживают SPD (Security Policy Database) со средствами работы из командной строки, другие с GUI, в то время как прочие предоставляют WEB-интерфейс для работы через сеть. Каждая запись в SPD определяется набором значений полей IP и протокола верхнего уровня, называемых селекторами. Эти селекторы используются для фильтрации исходящего трафика, для того чтобы поставить его в соответствие с определенной SA. Обработка исходящих IP-пакетов производится в следующей последовательности.
- сравниваются значения соответствующих полей в пакете (селекторные поля) с SPD и находится нуль или более SA.
- Определяется SA (если таковая имеется) для пакета и сопряженный с ней SPI.
- Выполняются необходимые операции IPsec (AH или ESP).

SPD запись определяется следующими селекторами:
- IP-адрес места назначения. Это может быть один IP-адрес (обязательно уникастный!), нумерованный список адресов или адресная маска (префикс). Последние два варианта нужны для работы группами адресов, имеющими идентичную SA (например, за firewall).
- IP-адрес отправителя. Это может быть один IP-адрес, нумерованный список адресов или адресная маска (префикс). Последние два варианта нужны для поддержки нескольких отправителей, имеющих идентичную SA, (например, за firewall).
- UserID. Идентификатор пользователя служит для идентификации политики, соответствующей имени пользователя или системы.
- Уровень чувствительности данных. Уровень чувствительности данных используется для определения характера данных (например, “Секретно” или “Unclassified”).
- Протокол транспортного уровня. Это значение извлекается из поля следующий заголовок пакета IPv4 или IPv6. Это может быть индивидуальный код протокола, список кодов протокола или диапазон таких кодов.
- Протокол IPsec (AH, ESP или AH/ESP). Извлекается (если присутствует) из поля следующий заголовок пакета IPv4 или IPv6.
- Порты отправителя и получателя. Это могут быть индивидуальные номера портов TCP или UDP, список портов или произвольный порт.
- **Класс IPv6**. Значение класса получается из заголовка IPv6. Это может быть специфическое значение и код произвольного класса.
- **Метка потока IPv6**. Значение метки потока получается из заголовка IPv6. Это может быть специфическое значение метки потока или код произвольной метки.
- **Тип сервиса IPv4**. Значение ToS получается из заголовка IPv4. Это может быть специфическое значение ToS или указатель произвольного значения.

Управление ключами

Для управления ключами используется несколько протоколов. IPsec был бы бесполезным без шифрования и аутентификации, которые в свою очередь невозможны без секретных ключей, известных партнерам обмена и неизвестных больше никому.

Наиболее простым способом задания этих секретных ключей является ручная конфигурация: один партер генерирует набор ключей и передает ключи другим партерам.

Но такая схема плохо масштабируется, кроме того, кто-то из партнеров может пренебречь мерами безопасности и в результате вся сеть будет скомпрометирована. В больших системах с большим числом узлов такая схема обычно не приемлема.

Система **IKE** (Internet Key Exchange) позволяет двум партнерам динамически аутентифицировать друг друга, согласовать использование ассоциации безопасности (Security Association), включая секретные ключи, и генерировать сами ключи. Система IKE использует

ISAKMP (Internet Security Association Key Management Protocol – протокол управления ключами ассоциации безопасности Интернет, разработан Национальным агентством безопасности США - NSA). Протокол ISAKMP сам по себе не регламентирует какой-либо конкретный алгоритм обмена ключами, он содержит в себе описание ряда сообщений, которые позволяют согласовать использование алгоритмов обмена ключами. Согласование осуществляется в два этапа:

- Узлы ISAKMP согласуют механизмы защиты дальнейшего обмена данными, путем установления SA. Эта ассоциация служит для защиты последующих операций и отличается от прочих SA.
- Протокол ISAKMP устанавливает SA для других протоколов, например, из семейства IPsec.

Механизм обмена ключами в IKE берется из протокола Oakley (RFC-2412). Основой протокола обмен ключами Oakley является алгоритм Диффи-Хелмана (см. http://book.itep.ru/6/difi_646.htm), дополненный некоторыми усовершенствованиями. В частности в каноническом алгоритме Диффи-Хелмана отсутствует аутентификация партнеров, что допускает возможность атаки с подменом ключей. В IPsec версии алгоритма, аутентификация партнеров является обязательной процедурой.

Заметим, что IPsec осуществляет пересылку ключей через порт 500/udp. В IPsec при обмене ключами предусмотрено использование сертификатов. Для получения сертификата посылается запрос в сертификационный центр CA (Certificate Authority). Сертификация включает в себя следующие операции:

- Клиент генерирует пару ключей (общедоступный и секретный). Далее он готовит неподписанный сертификат, который содержит идентификатор клиента и его общедоступный ключ. После этого клиент посылает этот сертификат в CA, шифруя его открытым ключом CA.
- CA формирует хэш для присланного неподписанного сертификата и шифрует его своим секретным ключом. CA добавляет сформированную так электронную подпись к неподписанному сертификату и посылает уже подписанный сертификат клиенту.
- Клиент теперь может послать свой подписанный сертификат любому другому пользователю. Получатель сертификата может легко его проверить, если располагает общедоступным ключом CA.

Клиенты могут пользоваться одним и тем же CA или быть клиентами разных CA. На практике обычно реализуется иерархическая структура CA.

Материал из Википедии [3] - IKE-wiki.doc

IKE (IKE+ISAKMP+AH+ESP-ipsec)

AH, сокращение. Может означать: ... Authentication Header (идентификационный заголовок), один из заголовоков IPsec -протокола. Application ...

ESP - Encapsulating Security Payload (англ.) — протокол шифрования сетевого трафика, часть IPSEC

IKE (Internet Key Exchange) — стандартный протокол IPsec, используемый для обеспечения безопасности взаимодействия в виртуальных частных сетях. Предназначение IKE — защищенное согласование и доставка идентифицированного материала для ассоциации безопасности (SA).

Архитектура

Протокол передает сообщения через UDP порты 500 и/или 4500. Установленная SA включает в себя разделяемый секретный ключ и набор криптографических алгоритмов. Также IKE может использовать компрессию IP.

Обмен информацией осуществляется парными сообщениями «запрос — ответ». Такие пары называются «обмен» («exchange»).

Обмен данными в IKE происходит в 2 фазы. В первой фазе устанавливается SA IKE. Во второй SA IKE используется для согласования протокола (обычно **IPSec**).

Определения

SKEYID — строка, получаемая из секретного ключа, известного только участникам обмена.

SKEYID_e — материал ключей, используемый SA **ISAKMP** для защиты конфиденциальности своих сообщений.

SKEYID_a — материал ключей, используемый SA **ISAKMP** для идентификации своих сообщений.

SKEYID_d — материал ключей используемый при получении ключей для SA, не относящихся к **ISAKMP**

Nx — данные текущего времени (x может быть i или r в случае инициатора или получателя соответственно)

prf(key, msg) — псевдослучайная функция с ключом (pseudo-random function). Часто используется хэш-функция.

g^xy — разделяемый секретный код Диффи-Хеллмана.

CKY_x — cookies инициатора (если x == I) или получателя (если x == R) из заголовка **ISAKMP**

HDR — заголовок **ISAKMP**. Его поле типа обмена определяет режим. Если пишется HDR*, то данные зашифрованы.

SA — данные согласования, содержащие одно или несколько предложений. Инициатор может отправить несколько предложений, но ответчик обязан ответить только одним предложением.

IDx — данные идентификации для x. В случае, если x == ii, то это данные инициатора в первой фазе, если x == ir, то это данные ответчика в первой фазе, если x == ui, то это данные инициатора во второй фазе, если x == ur, то это данные ответчика во второй фазе.

CERT — данные сертификации.

SIG_X — данные подписи инициатора или ответчика в случае X == I или X == R соответственно.

KE — данные обмена ключами, которые содержат открытую информацию, передаваемую в процессе обмена Диффи-Хеллмана.

HASH(X) — данные хэш-кода.

<X>_b — тело данных X.

<x>y — x зашифрован ключом y.

X | Y — конкатенация X и Y.

[править] Фаза 1

Для первой фазы возможны 2 режима: основной и агрессивный.

В основном режиме происходят 3 обмена: в первом узлы договариваются о правилах, во втором обмениваются открытыми значениями Диффи-Хеллмана и вспомогательными данными, в третьем происходит подтверждение обмена Диффи-Хеллмана.

В агрессивном режиме в первом обмене устанавливаются правила, передаются открытые значения Диффи-Хеллмана и вспомогательная информация. Причем во втором сообщении первого обмена происходит идентификация отвечающей стороны (responder). Третье сообщение идентифицирует инициатора и подтверждает участие в обмене. Последнее (четвертое) сообщение может быть не послано.

Для обоих этих методов возможны четыре типа различных методов идентификации: цифровой подписью, два типа шифрования открытым ключом и разделяемый ключ (pre-shared key).

В зависимости от типа идентификации в начале генерируется SKEYID.

SKEYID = prf(Ni_b | Nr_b, g^xy) в случае идентификации цифровой подписью.

SKEYID = prf(hash(Ni_b | Nr_b), CKY-I | CKY-R) в случае шифрования открытым ключом.

SKEYID = prf(pre-shared-key, Ni_b | Nr_b) в случае разделяемого ключа.

После этого стороны вычисляют материалы ключей SKEYID_d, SKEYID_a, SKEYID_e.

SKEYID_d = prf(SKEYID, g^xy | CKY-I | CKY-R | 0)

SKEYID_a = prf(SKEYID, SKEYID_d | g^xy | CKY-I | CKY-R | 1)

SKEYID_e = prf(SKEYID, SKEYID_a | g^xy | CKY-I | CKY-R | 2)

Далее подробнее см. IKE-wiki.doc

40. Передача голосового трафика поверх IP, протоколы SIP, RTP. Особенности алгоритмов компрессии голоса и проблемы транспортной инфраструктуры.

Из шпоргалки [2] п. 40 (см. ссылку - реальное голосовое общение)

См.также из *Семёнова* [4] – 4.4.9.0 Протокол IGMP и передача мультимедиа по Интернет.doc 4.4.9.2 Протокол реального времени RTP.doc и 4.4.9.8 Протокол запуска сессий SIP.doc

См. билет №41

Протокол RTP 4.4.9.2 Протокол реального времени RTP.doc

В начале 90-х годов были сделаны первые попытки использовать Интернет для передачи голоса в реальном масштабе времени (VocalTek). В настоящее время IP-телефония стала обычным видом услуг. Более того, она сыграла определяющую роль в снижении телефонных тарифов. Появились регулярные музыкальные программы. На подходе подключение к этому виду сервиса всех мобильных коммуникаций и цифрового телевидения. Этому способствовала разработка алгоритмов MPEG-1 ÷ -4 и прикладных программ, реализующих эти алгоритмы.

Специфическим для мультимедиа является использование для транспортировки протокола UDP (без установления соединения и без гарантии доставки). В случае передачи голоса или изображения повторная передача дейтограммы становится бессмысленной.

В Интернет, также как и в некоторых других сетях, возможна потеря пакетов изменение их порядка в процессе транспортировки, а также вариация времени доставки в достаточно широких пределах. Мультимедийные приложения накладывают достаточно жесткие требования на транспортную среду. Для согласования таких требований с возможностями Интернет был разработан протокол **RTP**. **Протокол RTP** (См. RFC-2205, -2209, -2210, -1990, -1889,-3550, -3551, -3989, -3952; "RTP: A Transport Protocol for Real-Time Applications" H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson) базируется на идеях, предложенных Кларком и Тенненхаузом [1], и предназначен для доставки данных в реальном масштабе времени (например, аудио- или видео). При этом определяется тип поля данных, производится нумерация посылок, присвоение временных меток и мониторирование доставки. Приложения обычно используют RTP поверх протокола UDP для того, чтобы использовать его возможности мультиплексирования и контрольного суммирования. **Но RTP может использоваться и поверх любой другой сетевой транспортной среды.** RTP поддерживает одновременную доставку по многим адресам, если мультикастинг поддерживается нижележащим сетевым уровнем.

Следует иметь в виду, что сам по себе RTP не обеспечивает своевременной доставки и не предоставляет каких-либо гарантий уровня сервиса (QoS. Этот протокол не может гарантировать также корректного порядка доставки данных.

Правильный порядок выкладки информации может быть обеспечен принимающей стороной с помощью порядковых номеров пакетов. Такая возможность крайне важна практически всегда, но особое внимание этому уделяется при восстановлении передаваемого изображения.

На практике протокол RTP не отделим от протокола RTCP (RTP control protocol). Последний служит для мониторинга qos и для передачи информации об участниках обмена в ходе сессии.

RTP гибкий протокол, который может доставить приложению нужную информацию, его функциональные модули не образуют отдельный слой, а чаще встраиваются в прикладную программу. Протокол RTP не является жестко регламентирующим.

При организации аудио-конференции каждый участник должен иметь адрес и два порта, один для звуковых данных, другой для управляющих RTCP-пакетов. Эти параметры должны быть известны всем участникам конференции. При необходимости соблюдения конфиденциальности информация и пакеты управления могут быть зашифрованы. При аудио конференциях каждый из участников пересылает небольшие закодированные звуковые фрагменты длительностью порядка 20 мсек. Каждый из таких фрагментов помещается в поле данных RTP-пакета, который в свою очередь вкладывается в UDP-дейтограмму.

Заголовок пакета RTP определяет, какой вид кодирования звука применен (PCM, ADPCM или LPC), что позволяет отправителю при необходимости сменить метод кодирования, если к конференции подключился новый потребитель с определенными ограничениями или сеть требует снижения скорости передачи.

Так как участники конференции могут появляться и исчезать по своему усмотрению, полезно знать, кто из них присутствует в сети в данный момент, и как до них доходят передаваемые данные. Для этой цели периодически каждый из участников транслирует через порт RTCP мультикастинг-сообщение, содержащее имя участника и диагностические данные. Узел-участник конференции шлет пакет BUY (RTCP), если он покидает сессию.

Если в ходе конференции передается не только звук но и изображение, они передаются как два независимых потока с использованием двух пар UDP-портов. RTCP-пакеты посылаются независимо для каждой из этих двух сессий.

На уровне RTP не существует какой-либо взаимосвязи между аудио- и видео сессиями. Только RTCP-пакеты несут в себе одни и те же канонические имена участников.

В некоторых случаях можно столкнуться с ситуацией, когда один из участников конференции подключен к сети через узкополосный канал. Было бы не слишком хорошо требовать от всех участников перехода на кодировку, соответствующую этой малой полосе. Для того чтобы этого избежать, можно установить преобразователь, называемый смесителем, в непосредственной близости от узкополосной области.

Смеситель преобразует поток аудио-пакетов в следовательность пакетов, которая соответствует возможностям узкополосного канала. Эти пакеты могут быть уникастными (адресованными одному получателю) или мультикастными. Заголовок RTP включает в себя средства, которые позволяют мультиплексорам идентифицировать источники, внесшие вклад. Так что получатель может правильно идентифицировать источник звукового сигнала.

Недостаточно использовать в качестве идентификатора локальный сетевой адрес (такой как IPv4), так как может быть не уникальным. Так как RTP трансляторы и смесители допускают работу с сетями, использующими различные адресные пространства, это допускает их случайное совпадение с большей вероятностью, чем в случае использования случайных чисел.

Протокол SIP 4.4.9.8 Протокол запуска сессий SIP.doc

Протокол SIP (Session Initiation Protocol) описан в документе RFC 3261, и служит для запуска, модификации и завершения сессий реального времени **между партнерами IP-сети**. SIP может поддерживать как моно так и мультимедийные приложения, включая видеоконференции.

Протокол SIP является лишь одним из протоколов, которые обеспечивают мультимедийный обмен через Интернет. SIP представляет собой сигнальный протокол, который позволяет одному партнеру послать запрос другому и согласовать параметры мультимедиа сессии.

Собственно транспортировка мультимедиа данных обычно осуществляется с помощью протокола **RTP** (Real-Time Transport Protocol).

Базовым стимулом создания протокола SIP являлась необходимость реализации работы с VoIP (Voice **over IP**). Протокол поддерживает пять аспектов, сопряженных с установлением и завершением мультимедийных коммуникаций:

Положение пользователя: Пользователи могут менять свое положение и сохранять доступ к телефонии и другим приложениям дистанционно.

Доступность пользователя: Предполагается проверка готовности парнера-адресата участвовать в коммуникациях.

Возможности пользователя: Определяются параметры среды, которые должны быть использованы.

Формирование сессии: Создается соединение точка-точка или сессия с несколькими партнерами при заданных коммуникационных параметрах.

Управление сессией: Предполагается создание и завершение сессий, модификация параметров сессии и сервисов.

SIP базируется на модели транзакций, сходных с запросами/откликами в протоколе HTTP. Каждая транзакция состоит из запроса клиента, который включает в себя определенный метод, или функцию, для сервера и, по крайней мере, один отклик. SIP использует большинство полей заголовков, правил кодирования и коды статуса протокола HTTP. Это позволяет работать с данными легко читаемого и отображаемого формата. SIP использует протокол SDP (Session Description Protocol), который с помощью набора типов данных, используемых в MIME (Multipurpose Internet Mail Extensions), определяет содержимое сессии.

41. Технологии IP multicast для IPv4: взаимодействие с unicast-маршрутизацией, IGMP, PIM, RP.

Из шпоргалки [2] п. 40 (см. ссылку - реальное голосовое общение)

См.также из *Семёнова* [4] – 4.4.9.0 Протокол IGMP и передача мультимедиа по Интернет.doc 4.4.9.5 Протокол PIM.doc, 4.4.9.2 Протокол реального времени RTP.doc

IGMP

Передача мультимедийных данных по сетям Интернет является одним из наиболее важных направлений. Этот вид информации передается обычно в режиме без установления соединения (протокол UDP-RTP). Наиболее типичной схемой в этом случае является наличие одного передатчика и большого числа приемников. Эта схема реализуется с использованием мультикастинг-адресации. Мультикастинг-адресация может осуществляться на IP- и MAC-уровнях. В Ethernet для этих целей зарезервирован блок адресов в диапазоне от 01:00:5E:00:00:00 до 01:00:5E:7F:FF:FF. Первый байт адреса, равный 01, указывает на то, что адрес является мультикастным. Данная схема резервирования адресного пространства позволяет использовать 23 бита Ethernet-адреса для идентификации группы рассылки при IP-мультикастинге (см. рис. 4.4.9.1.).

Рис. 4.4.9.1. Соотношение мультикастинговых MAC- и IP-адресов

Область из 5 бит в IP-адресе, отмеченная *****, не используется при формировании Ethernet-адреса. Так как соотношение IP и MAC-адресов не является однозначным, драйверы должны обеспечивать обработку адресов с тем, чтобы интерфейсы получали только те кадры, которые действительно им предназначены. Для того чтобы информировать маршрутизатор о наличии участников мультикастинг-обмена в субсети, связанной с тем или иным интерфейсом, используется протокол IGMP.

Протокол IGMP (internet group management protocol, RFC-1112) используется для видеоконференций, передачи звуковых сообщений, а также группового исполнения команд различными ЭВМ. Этот протокол использует групповую адресацию (мультикастинг).

Групповая форма адресации нужна тогда, когда какое-то сообщение или последовательность сообщений необходимо послать нескольким (но не всем) адресатам одновременно. При этой форме адресации ЭВМ имеет возможность выбрать, хочет ли она участвовать в этой процедуре. Когда группа ЭВМ хочет взаимодействовать друг с другом, используется один групповой (мультикастинг) адрес. Групповая адресация может рассматриваться как обобщение обычной системы адресов, а традиционный IP-адрес - частный случай группового обращения при числе ЭВМ, равном 1.

При групповой адресации один и тот же пакет может быть доставлен заданной группе ЭВМ. Членство в этой группе может динамично меняться со временем. Любая ЭВМ может войти в группу и выйти из группы в любое время по своей инициативе. В то же время ЭВМ может быть членом большого числа таких групп. ЭВМ может посылать пакеты членам группы, не являясь им сама. Каждая группа имеет свой адрес класса D (рис. 4.4.9.2, см. также рис. 4.4.9.1).

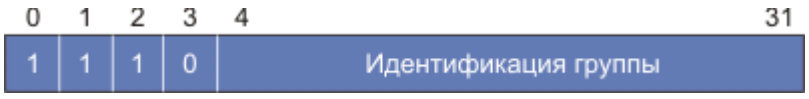


Рис. 4.4.9.2. Формат группового адреса

Для того чтобы участвовать в коллективных обменах в локальной сети ЭВМ должна быть снабжена программой, которая поддерживает этот режим. При этом сервер локальной сети (gateway) информируется о намерении использовать мультикастинг. Сервер передает эту информацию другим внешним серверам IP-сети. Следует иметь в виду, что мультикастинг также как и широковещательный режим, заметно загружает сеть. IGMP для передачи своих сообщений использует IP-дейтограммы (IGMP-пакеты инкапсулируются в них). Для

подключения к группе сначала посылается IGMP-сообщение "всем ЭВМ" о включении в группу, при этом локальный мультикаст-сервер подготавливает маршрут. Локальный мультикаст-сервер время от времени проверяет ЭВМ и определяет, не покинули ли они группу (ЭВМ не подтверждает свое членство в группе). Все обмены между ЭВМ и мультикаст-сервером производятся в режиме ip-мультикастинга, те есть, любое сообщение адресуется всем ЭВМ группы. ЭВМ, не принадлежащая группе, IGMP-сообщений не получает, что сокращает загрузку сети.

4.4.9.1 Мультикастинг и MBONE.doc

MBONE - это виртуальная сеть, базирующаяся на мультикастинг-протоколах. Данный режим работы поддерживается не всеми маршрутизаторами. Сеть представляет собой систему Ethernet-сетей, объединенных друг с другом соединениями точка-точка, которые называются "туннелями". Конечными точками таких туннелей обычно являются машины класса рабочих станций, снабженные соответствующим программным обеспечением.

IP-мультикастинг-пакеты инкапсулируются при передаче через туннели так, что они выглядят как обычные IP-уникаст-пакеты.

Мультикастинг-маршрутизатор при посылке пакета через туннель подготавливает IP-пакет с заголовком, который содержит адрес маршрутизатора-партнера на другом конце туннеля, при этом поле IP-протокола содержит код 4 (IP). Маршрутизатор-приемник извлекает вложенный мультикастинг-пакет и направляет далее, если это требуется.

Протокол PIM и узел RP 4.4.9.5 Протокол PIM.doc

Протокол PIM (Protocol Independent Multicast) призван решить проблемы маршрутизации для произвольного числа и расположения членов группы и для произвольного числа отправителей информации.

Главным преимуществом данного протокола является эффективная поддержка работы "рассеянных" мультикастинг-групп.

PIM базируется на традиционных маршрутных протоколах, конкретно не связан ни с каким из них, им используются сформированные этими протоколами маршрутные таблицы.
Существует два режима работы протокола –

DM (для компактных групп)
и **SM** (Protocol Independent Multicast-Sparse Mode (PIM-SM)).

В режиме SM маршрутизаторы, имеющие членов мультикастинг-группы, посылают сообщения о присоединении к дереву рассылки в узлы, которые называются точками встречи (**RP**). Отправители используют RP для объявления о своем существовании, а получатели, чтобы узнать о новых отправителях. В качестве RP может использоваться любой маршрутизатор, поддерживающий протокол PIM.

Когда какой-то клиент хочет подключиться к некоторой группе, ближайший к нему маршрутизатор посылает специальное сообщение о включении в группу (PIM-joint) узлу, объявленному для данной группы точкой встречи (**RP**). Число **RP** в сети может быть произвольным. Узел **RP** пересылает сообщение о включении узлу-отправителю (или отправителям). Если маршрутизатор не имеет информации о **RP**, включается схема, работающая для компактных групп. При обработке сообщения о включении в группу промежуточные маршрутизаторы формируют часть дерева мультикастинг-маршрутов между **RP** и получателем. При отправке мультикастинг-пакета соответствующий маршрутизатор посылает узлу **RP** регистрационное сообщение (PIM-register), куда вкладывается информационный пакет. Если используется несколько RP, отправитель должен посылать пакеты всем RP. Получатель же должен быть подключен лишь к одному из RP. В случае, когда сообщение о включении достигнет отправителя раньше, чем RP, подключение осуществляется, минуя RP. Если необходимо оптимизировать дерево доставки пакетов, маршрутизаторы-получатели должны послать сообщение о включении самому отправителю. После этого дерево соединений видоизменяется, некоторыми узлами, если требуется, посылается сообщение об отключении.

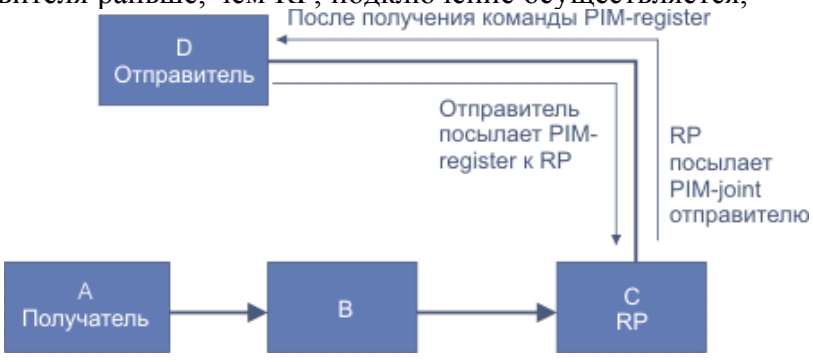


Рис. 4.4.9.5.1. Иллюстрация реализации протокола мультикастинг маршрутизации PIM

Получатель посылает PIM-joint пакет в RP, устанавливая канал от RP до получателя. Из рисунка видно, что исходный маршрут d-c-b-a длиннее оптимального d-b-a. Последний может быть реализован после посылки PIM-joint команды от a к d.

Следует заметить, что большинство протоколов для маршрутизации мультимедийной информации формируют маршрут не от отправителя к получателю, а в обратном направлении. Это имеет под собой веские причины. Дерево рассылки должно быть построено так, чтобы поток отправителя как можно дольше и меньше разветвлялся. Желательно, чтобы разветвления происходили как можно ближе к получателю. Это соображение проиллюстрировано на рис. 4.4.9.5.2. На рисунке условно, в виде сетки маршрутизаторов (желтые кружочки) показан фрагмент сети Интернет. Зеленым прямоугольником отмечен передатчик, а голубыми кружочками приемники - члены группы. Маршруты от передатчика к приемникам можно проложить индивидуально (выделены зеленым цветом), а можно и "коллективно" (синий цвет). От передатчика до маршрутизатора отмеченного красным цветом следует один поток для всех приемников. Такое решение приводит к минимизации сетевой загрузки, ведь всем приемникам посылаются одни и те же пакеты. Чем позже их пути разойдутся, тем лучше. Именно этот алгоритм и реализует протокол PIM. Точки разветвления потоков на рис. 4.4.9.5.2 отмечены крестами (RP).

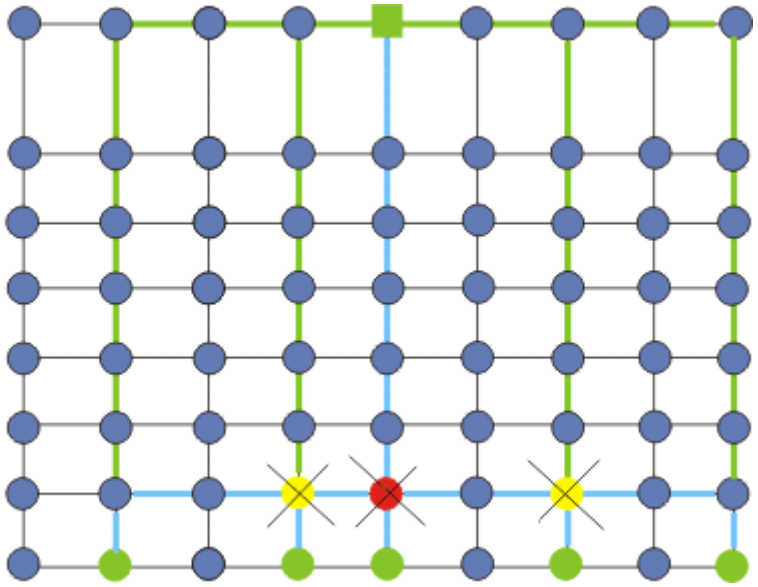


Рис. 4.4.9.5.2.

42. Функционирование почтовой системы на основе SMTP/ESMTP, envelope и header адреса, различные технологии защиты от спама.

Семёнов [4] – 4.5.10 Электронная почта.doc и 4.4.14 Протокол электронной почты SMTP.doc 4.4.14.6 SPAM.doc

Электронная почта - наиболее популярный и быстро развивающийся вид общения. Широко используются протоколы электронной почты UUCP (unix-to-unix copy protocol, RFC-976) и **SMTP** (simple mail transfer protocol; RFC-821, -822, -1351, -1352). Один из протоколов (RFC-822) определяет формат почтовых сообщений, второй (RFC-821) управляет их пересылкой. Имея механизмы промежуточного хранения почты (spooling) и механизмы повышения надежности доставки, протокол SMTP базируется на TCP-протоколе в качестве транспортного и допускает использование различных транспортных сред. Он может доставлять сообщения даже в сети, не поддерживающие протоколы TCP/IP. Протокол SMTP обеспечивает как транспортировку сообщений одному получателю, так и размножение нескольких копий сообщения для передачи по разным адресам. Обычно в любом узле Интернет имеется почтовый сервер (MX), который принимает все сообщения и устанавливает их в очередь. Далее производится раскладка сообщений по почтовым ящикам ЭВМ пользователей. Если какая-то ЭВМ не включена, сервер попытается доставить почту позднее (например, через 30 мин). После заданного числа неудачных попыток или по истечении определенного времени (> 4-5 дней) сообщение может быть утрачено. При этом отправитель должен получить уведомление об этом. Над SMTP располагается почтовая служба конкретных вычислительных систем (например, POP3(RFC-1460), IMAP (RFC-2060), sendmail (UNIX), pine, elm (надстройка над sendmail), mush, mh и т.д.).

Существует множество реализаций электронной почты. Имеются версии практически для всех ЭВМ, операционных систем и сред.

Адреса электронной почты уникальны и однозначно определяют адресата, обладая иногда даже некоторой избыточностью. Символьные адреса электронной почты вполне соответствуют IP-нотации. Электронный почтовый адрес содержит две части, местную и доменную, например, vanja.ivanov@itep.ru (vanya.ivanov - местная). Доменная часть обычно совпадает с символьным IP-именем домена.

Главной целью протокола Simple Mail Transfer Protocol (**SMTP**, RFC-821, -822) служит надежная и эффективная доставка электронных почтовых сообщений. SMTP является довольно независимой субсистемой и требует только надежного канала связи. Средой для SMTP может служить отдельная локальная сеть, система сетей или весь Интернет.

SMTP базируется на следующей модели коммуникаций: в ответ на запрос пользователя почтовая программа-отправитель устанавливает двухстороннюю связь с программой-приемником (TCP, порт 25). Получателем может быть оконечный или промежуточный адресат. SMTP-команды генерируются отправителем и посылаются получателю. На каждую команду должен быть отправлен и получен отклик.

Когда канал организован, отправитель посылает команду MAIL, идентифицирую себя. Если получатель готов к приему сообщения, он посылает положительное подтверждение. Далее отправитель посылает команду RCPT, идентифицируя получателя почтового сообщения. Если получатель может принять сообщение для оконечного адресата, он выдает снова положительное подтверждение (схема формирования откликов помещена в приложении 10.14). В противном случае он отвергает получение сообщения для данного адресата, но не вообще почтовой посылки.

SMTP-отправитель и SMTP-получатель могут вести диалог с несколькими оконечными пользователями (рис. 4.4.14.1). Любое почтовое сообщение завершается специальной последовательностью символов. Если получатель успешно завершил прием и обработку почтового сообщения, он посылает положительное подтверждение.

SMTP обеспечивает передачу почтового сообщения непосредственно конечному получателю, когда они соединены непосредственно. В противном случае пересылка может выполняться через одного или более промежуточных "почтовых станций".

Рис. 4.4.14.1 Схема взаимодействия различных частей почтовой системы

СПАМ –. Методы борьбы 4.4.14.6 SPAM.doc *(интересную инфу о спаме см. в этом файле)*

Фильтрация, стат. анализ, "черные" списки, блокировка доменов, аппаратные ср-ва, юридические меры

Профессионалы могут попытаться с помощью специального запроса проверить, какой тип операционной системы установлен на машине-отправителе. Если это, например, Windows-XP, вероятно, эта мошина входит в состав botnet и участвует в рассылке спам.

Можно попытаться создать отправителю почтовых сообщений нештатную ситуацию, например, послв отклик 451 (временная недоступность) Please try again later. Нормальный почтовый сервер прервется и обязательно повторит попытку позднее. Сервер рассылки SPAM обычно этого не делает.

Вообще тщательный контроль следованию SMTP-протоколу может быть указанием на добротность почтового сервера. Например, при установлении соединения получатель должен послать отклик 200 mail.example.com **ESMTP** Service ready. Машина-отправитель должна подождать этого отклика и не должна ничего посылать до этого. Если **SPAM-фильтр** задержит этот отклик, а отправитель начнет посылку сообщения, не дожидаясь отклика, получатель может решить, перед ним типичный спамер.

Распознать спам-сообщение можно и после его получения. Например, если для большого числа клиентов сети с одного и того же адреса пришли идентичные или почти идентичные сообщения, это может считаться признаком SPAM. Кроме того, отправитель спам-сообщения должен предоставит адресату какую-то контактную информацию (номер телефона, почтовый адрес или URL). Нужно свериться с репутационной базой данных и проверить, нет ли там этих координат. Иногда спамеры оформляют свои сообщения как ответ на запрос клиента локальной сети. Можно проверить, был ли такой запрос и, если такого запроса не было, пометить такое сообщение как SPAM.

Часто спамеры вводят в текст сообщений некоторые символы или слова, чтобы сообщения, направленные разным адресатам отличались. Таким образом они надеются обойти входной спам-фильтр. Но так как эти символы/слова вводит программа, они повторяются и сами могут стать признаками SPAM, которые сможет использовать фильтр.

Продвинутые фильтры используют **статистический анализ сообщений** (частота использования определенных слов и т.д.). Конечно, это не может дать 100%-ного распознавания, но в сочетании с другими критериями и методами может поднять эффективность фильтрации.

Спамеры используют множество разнообразных приемов, чтобы SPAM-фильтры их не распознали. Это и замена обычного или HTML-текста рисунком, размещение SPAM-сообщения внутри произвольного изменяемого текста, напечатанного супермелкими буквами и т.д. и т.д.

Некоторые методы фильтрации SPAM используют специальные **"черные" списки** машин, вовлеченных в такую рассылку. В такой список может попасть и машина, владелец которой об этом может и не подозревать (просто его ЭВМ была взломана ранее). Хозяин такой машины может столкнуться с проблемой недоставки своих сообщений (некоторые почтовые серверы будут считать их спамом). Если такая машина была ранее использована хакером для попыток взлома других машин, ее IP-адрес может быть включен в ACL или репутационный список. В этом случае **доставка может блокироваться маршрутизатором или сетевым шлюзом**. Так что пользователям имеет смысл следить за состоянием своей машины (например, использовать встроенный Firewall, который может детектировать попытки несанкционированного выхода машины в Интернет), иначе не избежать побочных неприятных эффектов. Обычно SPAM-фильтры производят **оценку вероятности** того, что конкретное сообщение является спамом по совокупности параметров.

В последнее время **фильтрацией SPAM начали заниматься сервис-провайдеры**, предоставляя этот вид услуг как SaaS.

Следует, впрочем, понимать, что спамеры внимательно изучают принципы построения SPAM-фильтров и предпринимают контрмеры. Botnet с числом машин 600.000 позволяет рассылать до 40 миллиардов SPAM-сообщений в сутки. **Пока наиболее эффективным средством борьбы со SPAM является блокировка доменов, участвующих в рассылке таких сообщений**. 80% всего объема SPAM приходится на эти десять botnet. Эти сети посылают до 135 миллиардов SPAM-сообщений в день.

В последнее время появилось достаточное число коммерческих и общедоступных программ фильтрации SPAM. Разработаны и поступили в продажу и **аппаратные средства** противодействия, которые среди прочего существенно снижают загрузку локального DNS.

Учитывая доходность рассылки SPAM, вряд ли удастся победить это явление число аппаратно-программными способами. Здесь нужны **юридические меры**, которые сделают этот бизнес более рискованным. Рискованность должна перекрывать возможность получения дохода от нелегальной рассылки.

43. Обеспечение безопасности в сетях на основе IPv4 и IPv6. Проблемы и способы их решения.

Из шпоргалки [2] п. 32 Механизмы защиты данных в сетях

Основной механизм защиты данных в сетях - шифрование информации. При помощи процедуры шифрования отправитель сообщения преобразует его из простого текста в набор символов, не поддающийся прочтению без применения специального ключа, известного получателю. Получатель сообщения, используя ключ, преобразует переданный ему набор символов обратно в текст. Т.о., если информация в зашифрованном виде попадет к злоумышленнику, он просто не сможет ей воспользоваться. [2]

Существенную проблему составляет необходимость идентифицировать пакеты, принадлежащие определенному процессу. Эта задача легко решается только в рамках протокола **IPv6.** Там в заголовке предусмотрено поле метка потока. Некоторые возможности предоставляет также протокол **MPLS** (4.4.17 Введение в MPLS, TE и QoS.doc)

В протоколе **IPv6** поле приоритет имеет 4 бита (см. IPv6). Биты C, D, T и R характеризуют пожелание относительно способа доставки дейтограммы. В таблице 1 приведены стандартизованные значения поля Type of Service (TOS) IP-пакета.

См. также ссылки IPsec и безопасность , см. билет№39 и 6.14 Технология IpSec.doc

Из билета №39 (материал Семёнова -6.14 Технология IpSec.doc)

Ассоциации безопасности и SPI

Кажется самоочевидным, что если два партнера или шлюза намереваются установить безопасное соединение, необходим некоторый объем общих секретных данных для реализации аутентификации и/или алгоритмов шифрования. Существует, конечно, проблема безопасной транспортировки этих секретных данных.

Когда IPsec-дейтограмма, AH или ESP попадает в интерфейс, как интерфейс узнает, какой набор параметров (ключ, алгоритм и политика) использовать? Любая машина может вести много диалогов, каждый со своим набором параметров безопасности и нужен механизм управления этим процессом.

Параметры безопасности задаются SA (Security Association), которая определяет параметры и процедуры, специфические для конкретного соединения. Каждый партнер может иметь один или более SA. Когда дейтограмма приходит, для нахождения правильного SA в базе данных SADB (Security Associations Database – база данных ассоциаций безопасности) используются три значения:

- IP адрес места назначения.
- IPsec протокол (ESP или AH, содержится в заголовке).
- Индекс параметров безопасности (SPI).

Во многих отношениях эта тройка может быть уподоблена IP сокету, который однозначно определяется IP адресом удаленного партнера (IPv4 или IPv6), протоколом и номером порта. В перечень компонентов SA входят:

- Номер по порядку. 32-битовый код, используемый для формирования поля порядковый номер в заголовках AH и ESP.
- Переполнение счетчика порядкового номера. Флаг, индицирующий переполнение счетчика порядкового номера. При его установке дальнейшая посылка пакетов для заданной SA должна быть прекращена.
- Окно для подавления попыток атак воспроизведения. Используется для определения того, является ли входящий AH- или ESP-пакет воспроизведением. Задача решается путем контроля того, попадает ли номер пакета в скользящее окно номеров.
- Информация AH. алгоритм аутентификации, ключи, время жизни ключей и другие параметры.
- Информация ESP: алгоритмы шифрования и аутентификации, ключи, параметры инициализации (IV), времена жизни ключей и другие параметры.
- Окно для подавления попыток атак воспроизведения. Используется для определения того, является ли входящий AH- или ESP-пакет воспроизведением. Задача решается путем контроля того, попадает ли номер пакета в скользящее окно номеров.
- Информация AH. алгоритм аутентификации, ключи, время жизни ключей и другие параметры.

- Информация ESP: алгоритмы шифрования и аутентификации, ключи, параметры инициализации (IV), времена жизни ключей и другие параметры.
- Режим работы IPsec. Туннельный, транспортный или любой.
- MTU пути. Максимальный размер пакета, который может быть передан через виртуальный канал без фрагментации.

При создании новой SA в счетчик номера по порядку заносится нуль, далее он инкрементируется при посылке каждого пакета. Когда содержимое счетчика достигает значения 232-1, текущая SA аннулируется и должна быть согласована новая ассоциация безопасности и новый ключ.

В базе данных SADB содержится:

- AH: алгоритм аутентификации.
- AH: аутентификационный секретный ключ (authentication secret).
- ESP: алгоритм шифрования.
- ESP: секретный ключ шифрования.
- ESP: разрешение аутентификации (yes/no).
- Параметры обмена ключами.
- Ограничения маршрутизации.
- **IP политика фильтрации**.

Некоторые реализации поддерживают SPD (Security Policy Database) со средствами работы из командной строки, другие с GUI, в то время как прочие предоставляют WEB-интерфейс для работы через сеть. Каждая запись в SPD определяется набором значений полей IP и протокола верхнего уровня, называемых селекторами. Эти селекторы используются для фильтрации исходящего трафика, для того чтобы поставить его в соответствие с определенной SA. Обработка исходящих IP-пакетов производится в следующей последовательности.

- сравниваются значения соответствующих полей в пакете (селекторные поля) с SPD и находится нуль или более SA.
- Определяется SA (если таковая имеется) для пакета и сопряженный с ней SPI.
- Выполняются необходимые операции IPsec (AH или ESP).

SPD запись определяется следующими селекторами:

- IP-адрес места назначения. Это может быть один IP-адрес (обязательно уникастный!), нумерованный список адресов или адресная маска (префикс). Последние два варианта нужны для работы группами адресов, имеющими идентичную SA (например, за firewall).
- IP-адрес отправителя. Это может быть один IP-адрес, нумерованный список адресов или адресная маска (префикс). Последние два варианта нужны для поддержки нескольких отправителей, имеющих идентичную SA, (например, за firewall).
- UserID. Идентификатор пользователя служит для идентификации политики, соответствующей имени пользователя или системы.
- Уровень чувствительности данных. Уровень чувствительности данных используется для определения характера данных (например, “Секретно” или “Unclassified”).
- Протокол транспортного уровня. Это значение извлекается из поля следующий заголовок пакета IPv4 или IPv6. Это может быть индивидуальный код протокола, список кодов протокола или диапазон таких кодов.
- Протокол IPsec (AH, ESP или AH/ESP). Извлекается (если присутствует) из поля следующий заголовок пакета IPv4 или IPv6.
- Порты отправителя и получателя. Это могут быть индивидуальные номера портов TCP или UDP, список портов или произвольный порт.
- **Класс IPv6**. Значение класса получается из заголовка IPv6. Это может быть специфическое значение и код произвольного класса.
- **Метка потока IPv6**. Значение метки потока получается из заголовка IPv6. Это может быть специфическое значение метки потока или код произвольной метки.
- **Тип сервиса IPv4**. Значение ToS получается из заголовка IPv4. Это может быть специфическое значение ToS или указатель произвольного значения.

ДОПОЛНИТЕЛЬНЫЙ МАТЕРИАЛ К ЧАСТИ 2

Введение. Основные фундаментальные понятия и определения из [6]

Современные компьютерные сетиработают на основе техники **комутационных пакетов.** Эта техника была специально разработана для передачи компьютерного трафика.

Телефонные сети используют текнику **коммутации каналов**, с фиксированной пропусконой способностью 64Кбит/с

При коммутации пакетов все передаваемые данные разбиваются в исходном узле на сравнительно небольшие части, называемые **пакетами, кадрами** или **ячейками**.

Иерархически организованный набро протоколов, достаточный для организации взаимодействия узлов в сети наз. **стеком протоколов**.

International Organization for Standartization (**ISO**) разработали стандартную модель **взаимодействия открытых систем** (Open System Interconnection, **OSI**) В модели OSI взаимодействия делятся на семь уровней.

Интерфейс прикладного программирования (иногда интерфейс программирования приложений) (англ. Application Programming Interface, API [эй-пи-ай])[1] — набор готовых классов, функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) для использования во внешних программных продуктах. Используется программистами для написания всевозможных приложений.

ДОПОЛНИТЕЛЬНЫЙ МАТЕРИАЛ К ЧАСТИ 2 (ОЛИФЕР – ГЛАВА 5 – тема - Маршрутизация)

Протоколы маршрутизации (часть1) (см. билет №32)

Протоколы маршрутизации (например, RIP, OSPF, NLSP) следует отличать от собственно сетевых протоколов (например, IP, IPX). И те и другие выполняют функции сетевого уровня модели OSI - участвуют в доставке пакетов адресату через разнородную составную сеть. Но в то время как первые собирают и передают по сети чисто служебную информацию, вторые предназначены для передачи пользовательских данных, как это делают протоколы канального уровня. Протоколы маршрутизации используют сетевые протоколы как транспортное средство.

С помощью протоколов маршрутизации маршрутизаторы составляют карту связей сети той или иной степени подробности. На основании этой информации для каждого номера сети принимается решение о том, какому следующему маршрутизатору надо передавать пакеты, направляемые в эту сеть, чтобы маршрут оказался рациональным. Результаты этих решений заносятся в таблицу маршрутизации.

Протоколы маршрутизации м.б. построены на основе разных алгоритмов, отличающихся способами построения таблиц маршрутизации, способами выбора наилучшего маршрута и другими особенностями своей работы.

Во всех описанных выше примерах при выборе рационального маршрута определялся только следующий (ближайший) маршрутизатор, а не вся последовательность маршрутизаторов от начального до конечного узла. В соответствии с этим подходом маршрутизация выполняется по распределенной схеме - каждый маршрутизатор ответственен за выбор только одного шага маршрута, а окончательный маршрут складывается в результате работы всех маршрутизаторов, через которые проходит данный пакет. Такие алгоритмы маршрутизации называются **одношаговыми**.

Существует и прямо противоположный, **многошаговый подход - маршрутизация от источника** (Source Routing). В соответствии с ним узел-источник задает в отправляемом в сеть пакете полный маршрут его следования через все промежуточные маршрутизаторы. При использовании многошаговой маршрутизации нет необходимости строить и анализировать таблицы маршрутизации. Это ускоряет прохождение пакета по сети, разгружает маршрутизаторы, но при этом большая нагрузка ложится на конечные узлы. Эта схема в вычислительных сетях применяется сегодня гораздо реже, чем схема распределенной одношаговой маршрутизации. Однако в новой версии протокола IP наряду с классической одношаговой маршрутизацией будет разрешена и маршрутизация от источника.

Одношаговые алгоритмы в зависимости от способа формирования таблиц маршрутизации делятся на три класса:

- алгоритмы фиксированной (или статической) маршрутизации;
- алгоритмы простой маршрутизации;
- алгоритмы адаптивной (или динамической) маршрутизации.

В алгоритмах **фиксированной маршрутизации** все записи в таблице маршрутизации являются статическими. Администратор сети сам решает, на какие маршрутизаторы надо передавать пакеты с теми или иными адресами, и вручную (например, с помощью утилиты route ОС Unix или Windows NT) заносит соответствующие записи в таблицу маршрутизации. Таблица, как правило, создается в процессе загрузки, в дальнейшем она используется без изменений до тех пор, пока ее содержимое не будет отредактировано вручную. Такие исправления могут понадобиться, например, если в сети отказывает какой-либо маршрутизатор и его функции возлагаются на другой маршрутизатор. Различают одномаршрутные таблицы, в которых для каждого адресата задан один путь, и многомаршрутные таблицы, определяющие несколько альтернативных путей для каждого адресата. В многомаршрутных таблицах должно быть задано правило выбора одного из маршрутов. Чаще всего один путь является основным, а остальные - резервными. Понятно, что алгоритм фиксированной маршрутизации с его ручным способом формирования таблиц маршрутизации приемлем только в небольших сетях с простой топологией. Однако этот алгоритм может быть эффективно использован и для работы на магистралях крупных сетей, так как сама магистраль может иметь простую структуру с очевидными наилучшими путями следования пакетов в подсети, присоединенные к магистрали.

В алгоритмах **простой маршрутизации** таблица маршрутизации либо вовсе не используется, либо строится без участия протоколов маршрутизации. **Выделяют три типа простой маршрутизации**:

- случайная маршрутизация, когда прибывший пакет посылается в первом попавшем случайном направлении, кроме исходного;
- лавинная маршрутизация, когда пакет широковещательно посылается по всем возможным направлениям, кроме исходного (аналогично обработке мостами кадров с неизвестным адресом);
- маршрутизация по предыдущему опыту, когда выбор маршрута осуществляется по таблице, но таблица строится по принципу моста путем анализа адресных полей пакетов, появляющихся на входных портах.

Самыми распространенными являются **алгоритмы адаптивной (или динамической) маршрутизации**. Эти алгоритмы обеспечивают автоматическое обновление таблиц маршрутизации после изменения конфигурации сети. Протоколы, построенные на основе адаптивных алгоритмов, позволяют всем маршрутизаторам собирать информацию о топологии связей в сети, оперативно отрабатывая все изменения конфигурации связей. В таблицах маршрутизации при адаптивной маршрутизации обычно имеется информация об интервале времени, в течение которого данный маршрут будет оставаться действительным. Это время называют временем жизни маршрута (Time To Live, TTL).

Адаптивные алгоритмы обычно имеют распределенный характер, который выражается в том, что в сети отсутствуют какие-либо выделенные маршрутизаторы, которые собирали бы и обобщали топологическую информацию: эта работа распределена между всеми маршрутизаторами.

Адаптивные алгоритмы маршрутизации должны отвечать нескольким важным требованиям.

1. Обеспечивать, если не оптимальность, то хотя бы рациональность маршрута.
2. Должны быть достаточно простыми, чтобы при их реализации не тратилось слишком много сетевых ресурсов, в частности они не должны требовать слишком большого объема вычислений или порождать интенсивный служебный трафик.
3. Должны обладать свойством сходимости, то есть всегда приводить к однозначному результату за приемлемое время.

Адаптивные протоколы обмена маршрутной информацией, применяемые в настоящее время в вычислительных сетях, в свою очередь делятся на две группы, каждая из которых связана с одним из следующих типов алгоритмов:

- дистанционно-векторные алгоритмы (Distance Vector Algorithms, DVA);
- алгоритмы состояния связей (Link State Algorithms, LSA).

В алгоритмах **дистанционно-векторного типа** каждый маршрутизатор периодически и широковещательно рассылает по сети вектор, компонентами которого являются расстояния от данного маршрутизатора до всех известных ему сетей. Под расстоянием обычно понимается число хопов. При получении вектора от соседа маршрутизатор наращивает расстояния до указанных в векторе сетей на расстояние до данного соседа. Получив вектор от соседнего маршрутизатора, каждый маршрутизатор добавляет к нему информацию об известных ему других сетях, о которых он узнал непосредственно (если они подключены к его портам) или из аналогичных объявлений других маршрутизаторов, а затем снова рассылает новое значение вектора по сети. В конце концов, каждый маршрутизатор узнает информацию обо всех имеющихся в интерсети сетях и о расстоянии до них через соседние маршрутизаторы.

Дистанционно-векторные алгоритмы хорошо работают только в небольших сетях, В больших сетях они засоряют линии связи интенсивным широковещательным трафиком, к тому же изменения конфигурации могут отрабатываться по этому алгоритму не всегда корректно, так как маршрутизаторы не имеют точного представления о топологии связей в сети, а располагают только обобщенной информацией - вектором дистанций, к тому же полученной через посредников. Работа маршрутизатора в соответствии с дистанционно-векторным протоколом напоминает работу моста, так как точной топологической картины сети такой маршрутизатор не имеет.

Наиболее распространенным протоколом, основанным на дистанционно-векторном алгоритме, является протокол RIP, который распространен в двух версиях - RIP IP, работающий с протоколом IP, и RIP IPX, работающий с протоколом IPX.

Алгоритмы состояния связей обеспечивают каждый маршрутизатор информацией, достаточной для построения точного графа связей сети. Все маршрутизаторы работают на основании одинаковых графов, что делает процесс маршрутизации более устойчивым к изменениям конфигурации. «Широковещательная» рассылка (то есть передача пакета всем непосредственным соседям маршрутизатора) используется здесь только при изменениях состояния связей, что происходит в надежных сетях не так часто. Вершинами графа являются как маршрутизаторы, так и объединяемые ими сети. Распространяемая по сети информация

состоит из описания связей различных типов: маршрутизатор - маршрутизатор, маршрутизатор - сеть,

Чтобы понять, в каком состоянии находятся линии связи, подключенные к его портам, маршрутизатор периодически обменивается короткими пакетами HELLO со своими ближайшими соседями. Этот служебный трафик также засоряет сеть, но не в такой степени как, например, RIP-пакеты, так как пакеты HELLO имеют намного меньший объем.

Протоколами, основанными на алгоритме состояния связей, являются протоколы IS-IS (Intermediate System to Intermediate System) стека OSI, OSPF (Open Shortest Path First) стека TCP/IP и недавно реализованный протокол NLSP стека Novell.

Функции маршрутизатора

Основная функция маршрутизатора -

- чтение заголовков пакетов сетевых протоколов, принимаемых и буферизуемых по каждому порту (например, IPX, IP, AppleTalk или DECnet),
- и принятие решения о дальнейшем маршруте следования пакета по его сетевому адресу, включающему, как правило, номер сети и номер узла.

Функции маршрутизатора могут быть разбиты на 3 группы в соответствии с уровнями модели OSI (рис. 5.3).

Важной особенностью протокола IP, отличающей его от других сетевых протоколов (например, от сетевого протокола IPX), является его способность выполнять динамическую **фрагментацию** пакетов при передаче их между сетями с различными, максимально допустимыми значениями поля данных кадров **MTU**. Свойство **фрагментации** во многом способствовало тому, что протокол IP смог занять доминирующие позиции в сложных составных сетях.

…мостами и коммутаторами не поддерживается функция **фрагментации** кадров. (стр.2 [1])

Выводы

- **Маршрут** - это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до пункта назначения. Задачу выбора маршрута из нескольких возможных решают **маршрутизаторы** и конечные узлы на основе таблиц маршрутизации. Записи в таблицу могут заноситься вручную администратором и автоматически протоколами маршрутизации.
- Протоколы маршрутизации (например, RIP или OSPF) следует отличать от собственно сетевых протоколов (например, IP или IPX). В то время как первые собирают и передают по сети чисто служебную информацию о возможных маршрутах, вторые предназначены для передачи пользовательских данных.
- Сетевые протоколы и протоколы маршрутизации реализуются в виде программных модулей на конечных узлах-компьютерах и на промежуточных узлах - маршрутизаторах.
- **Маршрутизатор** представляет собой сложное многофункциональное устройство, в задачи которого входит: построение таблицы маршрутизации, определение на ее основе маршрута, буферизация, **фрагментация** и фильтрация поступающих пакетов, поддержка сетевых интерфейсов. Функции маршрутизаторов могут выполнять как специализированные устройства, так и универсальные компьютеры с соответствующим программным обеспечением.
- Для **алгоритмов маршрутизации** характерны одношаговый и многошаговый подходы. **Одношаговые** алгоритмы делятся на алгоритмы фиксированной, простой и адаптивной маршрутизации. Адаптивные протоколы маршрутизации являются наиболее распространенными и в свою очередь могут быть основаны на дистанционно-векторных алгоритмах и алгоритмах состояния связей.

Протоколы маршрутизации (Коротко — схемы-тезисы)

1. Подход (алгоритмы)
   - Одношаговый
   - Многошаговый - маршрутизация от источника (Source Routing)

1.1. Одношаговые алгоритмы делятся на три класса:
- алгоритмы фиксированной (или статической) маршрутизации;
- алгоритмы простой маршрутизации;
- алгоритмы адаптивной (или динамической) маршрутизации.

1.1.2. Выделяют три типа простой маршрутизации:
- случайная маршрутизация;
- лавинная маршрутизация;
- маршрутизация по предыдущему опыту.

1.1.3. Самыми распространенными являются алгоритмы адаптивной (или динамической) маршрутизации

Адаптивные алгоритмы должны отвечать требованиям.
1) Обеспечивать, оптимальность/рациональность маршрута.
2) Должны быть достаточно простыми, (чтобы при не тратилось слишком много сетевых ресурсов, небольшой объем вычислений).
3) Должны обладать свойством сходимости (однозначный результат за приемлемое время).

Адаптивные протоколы обмена маршрутной информацией делятся на две группы, каждая из которых связана с одним из следующих типов алгоритмов:
- дистанционно-векторные алгоритмы (Distance Vector Algorithms, DVA);
- алгоритмы состояния связей (Link State Algorithms, LSA).

5.6.1. Маршрутизаторы (стр. 112-117)

Основная задача маршрутизатора - выбор наилучшего маршрута в сети - часто является достаточно сложной с математической точки зрения. Особенно интенсивных вычислений требуют протоколы, основанные на алгоритме состояния связей, вычисляющие оптимальный путь на графе, - OSPF, NLSP, IS-IS. Кроме этой основной функции в круг ответственности маршрутизатора входят и другие задачи, такие как буферизация, фильтрация и фрагментация перемещаемых пакетов. При этом очень важна производительность, с которой маршрутизатор выполняет эти задачи.

Поэтому типичный маршрутизатор является мощным вычислительным устройством с одним или даже несколькими процессорами, часто специализированными или построенными на RISC-архитектуре, со сложным программным обеспечением. То есть сегодняшний маршрутизатор - это специализированный компьютер, имеющий скоростную внутреннюю шину или шины (с пропускной способностью 600-2000 Мбит/с), часто использующий симметричное или асимметричное мультипроцессирование и работающий под управлением специализированной операционной системы, относящейся к классу систем реального времени. Многие разработчики маршрутизаторов построили в свое время такие операционные системы на базе операционной системы Unix, естественно, значительно ее переработав.

Маршрутизаторы могут поддерживать как один протокол сетевого уровня (например, IP, IPX или DECnet), так и множество таких протоколов. В последнем случае они называются многопротокольными маршрутизаторами. Чем больше протоколов сетевого уровня поддерживает маршрутизатор, тем лучше он подходит для корпоративной сети.

Большая вычислительная мощность позволяет маршрутизаторам наряду с основной работой по выбору оптимального маршрута выполнять и ряд вспомогательных высокоуровневых функций.

Классификация маршрутизаторов по областям применения

По областям применения маршрутизаторы делятся на несколько классов.

Магистральные маршрутизаторы (backbone routers) предназначены для построения центральной сети корпорации. Центральная сеть может состоять из большого количества локальных сетей, разбросанных по разным зданиям и использующих самые разнообразные сетевые технологии, типы компьютеров и операционных систем. Магистральные маршрутизаторы - это наиболее мощные устройства, способные обрабатывать несколько сотен тысяч или даже несколько миллионов пакетов в секунду, имеющие большое количество интерфейсов локальных и глобальных сетей. Поддерживаются не только среднескоростные интерфейсы глобальных сетей, такие как T1/E1, но и высокоскоростные, например, ATM или

SDH со скоростями 155 Мбит/с или 622 Мбит/с. Чаще всего магистральный маршрутизатор конструктивно выполнен по модульной схеме на основе шасси с большим количеством слотов - до 12-14. Большое внимание уделяется в магистральных моделях надежности и отказоустойчивости маршрутизатора, которая достигается за счет системы терморегуляции, избыточных источников питания, заменяемых «на ходу» (hot swap) модулей, а также симметричного муль-типроцессирования. Примерами магистральных маршрутизаторов могут служить маршрутизаторы Backbone Concentrator Node (BCN) компании Nortel Networks (ранее Bay Networks), Cisco 7500, Cisco 12000.

Маршрутизаторы региональных отделений соединяют региональные отделения между собой и с центральной сетью. Сеть регионального отделения, так же как и центральная сеть, может состоять из нескольких локальных сетей. Такой маршрутизатор обычно представляет собой некоторую упрощенную версию магистрального маршрутизатора. Если он выполнен на основе шасси, то количество слотов его шасси меньше: 4-5. Возможен также конструктив с фиксированным количеством портов. Поддерживаемые интерфейсы локальных и глобальных сетей менее скоростные. Примерами маршрутизаторов региональных отделений могут служить маршрутизаторы BLN, ASN компании Nortel Networks, Cisco 3600, Cisco 2500, NetBuilder II компании 3Com. Это наиболее обширный класс выпускаемых маршрутизаторов, характеристики которых могут приближаться к характеристикам магистральных маршрутизаторов, а могут и опускаться до характеристик маршрутизаторов удаленных офисов.

Маршрутизаторы удаленных офисов соединяют, как правило, единственную локальную сеть удаленного офиса с центральной сетью или сетью регионального отделения по глобальной связи. В максимальном варианте такие маршрутизаторы могут поддерживать и два интерфейса локальных сетей. Как правило, интерфейс локальной сети - это Ethernet 10 Мбит/с, а интерфейс глобальной сети - выделенная линия со скоростью 64 Кбит/с, 1,544 или 2 Мбит/с. Маршрутизатор удаленного офиса может поддерживать работу по коммутируемой телефонной линии в качестве резервной связи для выделенного канала. Существует очень большое количество типов маршрутизаторов удаленных офисов. Это объясняется как массовостью потенциальных потребителей, так и специализацией такого типа устройств, проявляющейся в поддержке одного конкретного типа глобальной связи. Например, существуют маршрутизаторы, работающие только по сети ISDN, существуют модели только для аналоговых выделенных линий и т. п. Типичными представителями этого класса являются маршрутизаторы Nautika компании Nortel Networks, Cisco 1600, Office Connect компании 3Com, семейство Pipeline компании Ascend.

Маршрутизаторы локальных сетей (коммутаторы 3-го уровня) предназначены для разделения крупных локальных сетей на подсети. Основное требование, предъявляемое к ним, - высокая скорость маршрутизации, так как в такой конфигурации отсутствуют низкоскоростные порты, такие как модемные порты 33,6 Кбит/с или цифровые порты 64 Кбит/с. Все порты имеют скорость по крайней мере 10 Мбит/с, а многие работают на скорости 100 Мбит/с. Примерами коммутаторов 3-го уровня служат коммутаторы CoreBuilder 3500 компании 3Com, Accelar 1200 компании Nortel Networks, Waveswitch 9000 компании Plaintree, Turboiron Switching Router компании Foudry Networks.

В зависимости от области применения маршрутизаторы обладают различными основными и дополнительными техническими характеристиками.

Основные технические характеристики маршрутизатора

Основные технические характеристики маршрутизатора связаны с тем, как он решает свою главную задачу - маршрутизацию пакетов в составной сети. Именно эти характеристики прежде всего определяют возможности и сферу применения того или иного маршрутизатора.

Перечень поддерживаемых сетевых протоколов. Магистральный маршрутизатор должен поддерживать большое количество сетевых протоколов и протоколов маршрутизации, чтобы обеспечивать трафик всех существующих на предприятии вычислительных систем (в том числе и устаревших, но все еще успешно эксплуатирующихся, так называемых унаследованных - legacy), а также систем, которые могут появиться на предприятии в ближайшем будущем. Если центральная сеть образует отдельную автономную систему Internet, то потребуется поддержка и специфических протоколов маршрутизации этой сети, таких как EGP и BGP. Программное обеспечение магистральных маршрутизаторов обычно строится по модульному принципу, поэтому при возникновении потребности можно докупать и добавлять программные модули, реализующие недостающие протоколы.

Перечень поддерживаемых сетевых протоколов обычно включает протоколы IP, CONS и CLNS OSI, IPX, AppleTalk, DECnet, Banyan VINES, Xerox XNS.

Перечень протоколов маршрутизации составляют протоколы IP RIP, IPX RIP, NLSP, OSPF, IS-IS OSI, EGP, BGP, VINES RTP, AppleTalk RTMP.

Перечень поддерживаемых интерфейсов локальных и глобальных сетей. Для локальных сетей - это интерфейсы, реализующие физические и канальные протоколы сетей Ethernet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet, 100VG-AnyLAN иATM.

Для глобальных связей - это интерфейсы физического уровня для связи с аппаратурой передачи данных, а также протоколы канального и сетевого уровней, необходимые для подключения к глобальным сетям с коммутацией каналов и пакетов.

Поддерживаются интерфейсы последовательных линий (serial lines) RS-232, RS-449/422, V.35 (для передачи данных со скоростями до 2-6 Мбит/с), высокоскоростной интерфейс HSSI, обеспечивающий скорость до 52 Мбит/с, а также интерфейсы с цифровыми каналами T1/E1, T3/E3 и интерфейсами BRI и PRI цифровой сети ISDN. Некоторые маршрутизаторы имеют аппаратуру связи с цифровыми глобальными каналами, что исключает необходимость использования внешних устройств сопряжения с этими каналами.

В набор поддерживаемых глобальных технологий обычно входят технологии X.25, frame relay, ISDN и коммутируемых аналоговых телефонных сетей, сетей ATM, а также поддержка протокола канального уровня PPP.

Общая производительность маршрутизатора. Высокая производительность маршрутизации важна для работы с высокоскоростными локальными сетями, а также для поддержки новых высокоскоростных глобальных технологий, таких как frame relay, T3/E3, SDH и ATM. Общая производительность маршрутизатора зависит от многих факторов, наиболее важными из которых являются: тип используемых процессоров, эффективность программной реализации протоколов, архитектурная организация вычислительных и интерфейсных модулей. Общая производительность маршрутизаторов колеблется от нескольких десятков тысяч пакетов в секунду до нескольких миллионов пакетов в секунду. Наиболее производительные маршрутизаторы имеют мультипроцессорную архитектуру, сочетающую симметричные и асимметричные свойства - несколько мощных центральных процессоров по симметричной схеме выполняют функции вычисления таблицы маршрутизации, а менее мощные процессоры в интерфейсных модулях занимаются передачей пакетов на подключенные к ним сети и пересылкой пакетов на основании части таблицы маршрутизации, кэшированной в локальной памяти интерфейсного модуля.

Магистральные маршрутизаторы обычно поддерживают максимальный набор протоколов и интерфейсов и обладают высокой общей производительностью в один-два миллиона пакетов в секунду. Маршрутизаторы удаленных офисов поддерживают один-два протокола локальных сетей и низкоскоростные глобальные протоколы, общая производительность таких маршрутизаторов обычно составляет от 5 до 20-30 тысяч пакетов в секунду.

Маршрутизаторы региональных отделений занимают промежуточное положение, поэтому их иногда не выделяют в отдельный класс устройств.

Наиболее высокой производительностью обладают коммутаторы 3-го уровня, особенности которых рассмотрены ниже.

Дополнительные функциональные возможности маршрутизаторов

Наряду с функцией маршрутизации многие маршрутизаторы обладают следующими важными дополнительными функциональными возможностями, которые значительно расширяют сферу применения этих устройств.

Поддержка одновременно нескольких протоколов маршрутизации. В протоколах маршрутизации обычно предполагается, что маршрутизатор строит свою таблицу на основе работы только этого одного протокола. Деление Internet на автономные системы также направлено на исключение использования в одной автономной системе нескольких протоколов маршрутизации. Тем не менее иногда в большой корпоративной сети приходится поддерживать одновременно несколько таких протоколов, чаще всего это складывается исторически. При этом таблица маршрутизации может получаться противоречивой - разные протоколы маршрутизации могут выбрать разные следующие маршрутизаторы для какой-либо сети назначения. Большинство маршрутизаторов решает эту проблему за счет придания приоритетов решениям разных протоколов маршрутизации. Высший приоритет отдается статическим маршрутам (администратор всегда прав), следующий приоритет имеют маршруты, выбранные протоколами состояния связей, такими как OSPF или NLSP, а низшим приоритетов обладают маршруты дистанционно-векторных протоколов, как самых несовершенных.

Приоритеты сетевых протоколов. Можно установить приоритет одного протокола сетевого уровня над другими. На выбор маршрутов эти приоритеты не оказывают никакого влияния, они влияют только на порядок, в котором многопротокольный маршрутизатор обслуживает пакеты разных сетевых протоколов. Это свойство бывает полезно в случае недостаточной полосы пропускания кабельной системы и существования трафика, чувствительного к временным задержкам, напримертрафика SNA или голосового трафика, передаваемого одним из сетевых протоколов.

Поддержка политики маршрутных объявлений. В большинстве протоколов обмена маршрутной информации (RIP, OSPF, NLSP) предполагается, что маршрутизатор объявляет в своих сообщениях обо всех сетях, которые ему известны. Аналогично предполагается, что маршрутизатор при построении своей таблицы учитывает все адреса сетей, которые поступают ему от других маршрутизаторов сети. Однако существуют ситуации, когда администратор хотел бы скрыть существование некоторых сетей в определенной части своей сети от других администраторов, например, по соображениям безопасности. Или же администратор хотел бы запретить некоторые маршруты, которые могли бы существовать в сети. При статическом построении таблиц маршрутизации решение таких проблем не составляет труда. Динамические же протоколы маршрутизации не позволяют стандартным способом реализовывать подобные ограничения. Существует только один широко используемый протокол динамической маршрутизации, в котором описана возможность существования правил (policy), ограничивающих распространение некоторых адресов в объявлениях, - это протокол BGP. Необходимость поддержки таких правил в протоколе BGP понятна, так как это протокол обмена маршрутной информацией между автономными системами, где велика потребность в административном регулировании маршрутов (например, некоторый поставщик услуг Internet может не захотеть, чтобы через него транзитом проходил трафик другого поставщика услуг). Разработчики маршрутизаторов исправляют этот недостаток стандартов протоколов, вводя в маршрутизаторы поддержку правил передачи и использования маршрутной информации, подобных тем, которые рекомендует BGP.

Защита от широковещательных штормов (broadcast storm). Одна из характерных неисправностей сетевого программного обеспечения - самопроизвольная генерация с высокой интенсивностью широковещательных пакетов. Широковещательным штормом считается ситуация, в которой процент широковещательных пакетов превышает 20 % от общего количества пакетов в сети. Обычный коммутатор или мост слепо передает такие пакеты на все свои порты, как того требует его логика работы, засоряя, таким образом, сеть. Борьба с широковещательным штормом в сети, соединенной коммутаторами, требует от администратора отключения портов, генерирующих широковещательные пакеты. Маршрутизатор не распространяет такие поврежденные пакеты, поскольку в круг его задач не входит копирование широковещательных пакетов во все объединяемые им сети. Поэтому маршрутизатор является прекрасным средством борьбы с широковещательным штормом, правда, если сеть разделена на достаточное количество подсетей.

Поддержка немаршрутизируемых протоколов, таких как NetBIOS, NetBEUI или DEC LAT, которые не оперируют с таким понятием, как сеть. Маршрутизаторы могут обрабатывать пакеты таких протоколов двумя способами.

- В первом случае они могут работать с пакетами этих протоколов как мосты, то есть передавать их на основании изучения MAC - адресов. Маршрутизатор необходимо сконфигурировать особым способом, чтобы по отношению к некоторым немаршрутизируемым протоколам на некоторых портах он выполнял функции моста, а по отношению к маршрутизируемым протоколам - функции маршрутизатора. Такой мост/маршрутизатор иногда называют brouter (bridge плюс router).
- Другим способом передачи пакетов немаршрутизируемых протоколов является инкапсуляция этих пакетов в пакеты какого-либо сетевого протокола. Некоторые производители маршрутизаторов разработали собственные протоколы, специально предназначенные для инкапсуляции немаршрутизируемых пакетов. Кроме того, существуют стандарты для инкапсуляции некоторых протоколов в другие, в основном в IP. Примером такого стандарта является протокол DLSw, определяющий методы инкапсуляции пакетов SDLC и NetBIOS в IP-пакеты, а также протоколы PPTP и L2TP, инкапсулирующие кадры протокола PPP в IP-пакеты. Более подробно технология инкапсуляции рассматривается в главе, посвященной межсетевому взаимодействию.

Разделение функций построения и использования таблицы маршрутизации. Основная вычислительная работа проводится маршрутизатором при составлении таблицы маршрутизации с маршрутами ко всем известным ему сетям. Эта работа состоит в обмене пакетами протоколов маршрутизации, такими как RIP или OSPF, и вычислении оптимального пути к каждой целевой сети по некоторому критерию. Для вычисления оптимального пути на графе, как того требуют протоколы состояния связей, необходимы значительные вычислительные мощности. После того как таблица маршрутизации составлена, функция продвижения пакетов происходит весьма просто - осуществляется просмотр таблицы и поиск совпадения полученного адреса с адресом целевой сети. Если совпадение есть, то пакет передается на соответствующий порт маршрутизатора. Некоторые маршрутизаторы поддерживают только функции продвижения пакетов по готовой таблице маршрутизации. Такие маршрутизаторы являются усеченными маршрутизаторами, так как для их полноценной работы требуется наличие полнофункционального маршрутизатора, у которого можно взять

готовую таблицу маршрутизации. Этот маршрутизатор часто называется сервером маршрутов. Отказ от самостоятельного выполнения функций построения таблицы маршрутизации резко удешевляет маршрутизатор и повышает его производительность. Примерами такого подхода являются маршрутизаторы NetBuilder компании 3Com, поддерживающие фирменную технологию Boundary Routing, маршрутизирующие коммутаторы Catalyst 5000 компании Cisco Systems.

Альтернативный ответ к билетам №№29 и 32 (из [2])

21. Маршрутизаторы. Типовые характеристики современных маршрутизаторов.

По областям применения маршрутизаторы делятся на несколько классов.

Магистральные маршрутизаторы (backbone routers) предназначены для построения центральной сети корпорации. Центральная сеть может состоять из большого количества локальных сетей, разбросанных по разным зданиям и использующих самые разнообразные сетевые технологии, типы компьютеров и операционных систем. Магистральные маршрутизаторы - это наиболее мощные устройства, способные обрабатывать несколько сотен тысяч или даже несколько миллионов пакетов в секунду, имеющие большое количество интерфейсов локальных и глобальных сетей. Поддерживаются не только среднескоростные интерфейсы глобальных сетей, такие как T1/E1, но и высокоскоростные, например, ATM или SDH со скоростями 155 Мбит/с или 622 Мбит/с. Чаще всего магистральный маршрутизатор конструктивно выполнен по модульной схеме на основе шасси с большим количеством слотов. Большое внимание уделяется в магистральных моделях надежности и отказоустойчивости маршрутизатора, которая достигается за счет системы терморегуляции, избыточных источников питания, заменяемых «на ходу» (hot swap) модулей, а также симметричного мультипроцессирования.

Маршрутизаторы региональных отделений соединяют региональные отделения между собой и с центральной сетью. Сеть регионального отделения, так же как и центральная сеть, может состоять из нескольких локальных сетей. Такой маршрутизатор обычно представляет собой некоторую упрощенную версию магистрального маршрутизатора. Если он выполнен на основе шасси, то количество слотов его шасси меньше. Возможен также конструктив с фиксированным количеством портов. Поддерживаемые интерфейсы локальных и глобальных сетей менее скоростные. Это наиболее обширный класс выпускаемых маршрутизаторов, характеристики которых могут приближаться к характеристикам магистральных маршрутизаторов, а могут и опускаться до характеристик маршрутизаторов удаленных офисов.

Маршрутизаторы удаленных офисов соединяют, как правило, единственную локальную сеть удаленного офиса с центральной сетью или сетью регионального отделения по глобальной связи. В max варианте такие маршрутизаторы могут поддерживать и два интерфейса локальных сетей. Как правило, интерфейс локальной сети - это Ethernet 10 Мбит/с, а интерфейс глобальной сети - выделенная линия со скоростью 64 Кбит/с, 1,544 или 2 Мбит/с. М.у.о. может поддерживать работу по коммутируемой телефонной линии в качестве резервной связи для выделенного канала. Существует. очень большое кол-во типов м.у.о. Это объясняется как массовостью потенциальных потребителей, так и специализацией такого типа устройств, проявляющейся в поддержке одного конкретного типа глобальной связи.

Маршрутизаторы локальных сетей (коммутаторы 3-го уровня) предназначены для разделения крупных локальных сетей на подсети. Основное требование, предъявляемое к ним, - высокая скорость маршрутизации, так как в такой конфигурации отсутствуют низкоскоростные порты, такие как модемные порты 33,6 Кбит/с или цифровые порты 64 Кбит/с. Все порты имеют скорость по крайней мере 10 Мбит/с, а многие работают на скорости 100 Мбит/с. В зависимости от области применения маршрутизаторы обладают различными основными и дополнительными техническими характеристиками.

Основные технические характеристики маршрутизатора связаны с тем, как он решает свою главную задачу - маршрутизацию пакетов в составной сети. Именно эти характеристики прежде всего определяют возможности и сферу применения того или иного маршрутизатора. Общая производительность маршрутизатора. Высокая производительность маршрутизации важна для работы с высокоскоростными локальными сетями, а также для поддержки новых высокоскоростных глобальных технологий, таких как frame relay, T3/E3, SDH и ATM.

Общая производительность маршрутизатора зависит от многих факторов, наиболее важными из которых являются: тип используемых процессоров, эффективность программной реализации протоколов, архитектурная организация вычислительных и интерфейсных модулей. Наиболее производительные маршрутизаторы имеют мультипроцессорную архитектуру, сочетающую симметричные и асимметричные свойства - несколько мощных центральных процессоров по симметричной схеме выполняют функции вычисления таблицы маршрутизации, а менее мощные процессоры в интерфейсных модулях занимаются передачей пакетов на подключенные к ним сети и пересылкой пакетов на основании части таблицы маршрутизации, кэшированной в локальной памяти интерфейсного модуля.

Магистральные маршрутизаторы обычно поддерживают максимальный набор протоколов и интерфейсов и обладают высокой общей производительностью в один-два миллиона пакетов в секунду. Маршрутизаторы удаленных офисов поддерживают один-два протокола локальных сетей и низкоскоростные глобальные протоколы, общая производительность таких маршрутизаторов обычно составляет от 5 до 20-30 тысяч пакетов в секунду. Маршрутизаторы региональных отделений занимают промежуточное положение, поэтому их иногда не выделяют в отдельный класс устройств.

ДОПОЛНИТЕЛЬНЫЙ МАТЕРИАЛ К ЧАСТИ 2 (ОЛИФЕР – ГЛАВА 5 тема - Протокол IP)

5.3. Протокол IP.

5.3.1. Основные функции протокола IP (стр.47).

Основу транспортных средств стека протоколов TCP/IP составляет протокол межсетевого взаимодействия (**Internet Protocol, IP**). Он обеспечивает передачу дейтаграмм от отправителя к получателям через объединенную систему компьютерных сетей.

Название данного протокола - Intrenet Protocol - отражает его суть: он должен передавать пакеты между сетями. В каждой очередной сети, лежащей на пути перемещения пакета, протокол IP вызывает средства транспортировки, принятые в этой сети, чтобы с их помощью передать этот пакет на маршрутизатор, ведущий к следующей сети, или непосредственно на узел-получатель.

Протокол IP относится к протоколам без установления соединений. Перед IP не ставится задача надежной доставки сообщений от отправителя к получателю. Протокол IP обрабатывает каждый IP-пакет как независимую единицу, не имеющую связи ни с какими другими IP-пакетами. В протоколе IP нет механизмов, обычно применяемых для увеличения достоверности конечных данных. Все вопросы обеспечения надежности доставки данных по составной сети в стеке TCP/IP решает протокол TCP, работающий непосредственно над протоколом IP. Именно TCP организует повторную передачу пакетов, когда в этом возникает необходимость.

Важной особенностью протокола IP, отличающей его от других сетевых протоколов (например, от сетевого протокола IPX), является его способность выполнять динамическую фрагментацию пакетов при передаче их между сетями с различными, максимально допустимыми значениями поля данных кадров MTU. Свойство фрагментации во многом способствовало тому, что протокол IP смог занять доминирующие позиции в сложных составных сетях.

Структура IP-пакета

IP-пакет состоит из заголовка и поля данных. Заголовок, как правило, имеющий длину 20 байт, имеет следующую структуру (рис. 5.12).

Поле **Номер версии** (Version), занимающее 4 бит, указывает версию протокола IP. Сейчас повсеместно используется версия 4 (IPv4), и готовится переход на версию 6 (IPv6).

Поле **Длина заголовка** (IHL) IP-пакета занимает 4 бит и указывает значение длины заголовка, измеренное в 32-битовых словах. Обычно заголовок имеет длину в 20 байт (пять 32-битовых слов), но при увеличении объема служебной информации эта длина может быть увеличена за счет использования дополнительных байт в поле Опции (IP Options). Наибольший заголовок занимает 60 октетов.

Поле **Тип сервиса** (Type of Service) занимает один байт и задает приоритетность пакета и вид критерия выбора маршрута. Первые три бита этого поля образуют подполе приоритета пакета (Precedence), Приоритет может иметь значения от самого низкого - 0 (нормальный пакет) до самого высокого - 7 (пакет управляющей информации). Маршрутизаторы и компьютеры могут принимать во внимание приоритет пакета и обрабатывать более важные пакеты в первую очередь. Поле Тип сервиса содержит также три бита, определяющие критерий выбора маршрута. Реально выбор осуществляется между тремя альтернативами: малой задержкой, высокой достоверностью и высокой пропускной способностью. Установленный бит D (delay) говорит о том, что маршрут должен выбираться для минимизации задержки доставки данного пакета, бит T - для максимизации пропускной способности, а бит R - для максимизации надежности доставки. Во многих сетях улучшение одного из этих параметров

связано с ухудшением другого, кроме того, обработка каждого из них требует дополнительных вычислительных затрат. Поэтому редко, когда имеет смысл устанавливать одновременно хотя бы два из этих трех критериев выбора маршрута. Зарезервированные биты имеют нулевое значение.

Поле **Общая длина** (Total Length) занимает 2 байта и означает общую длину пакета с учетом заголовка и поля данных. Максимальная длина пакета ограничена разрядностью поля, определяющего эту величину, и составляет 65 535 байт, однако в большинстве хост-компьютеров и сетей столь большие пакеты не используются. При передаче по сетям различного типа длина пакета выбирается с учетом максимальной длины пакета протокола нижнего уровня, несущего IP-пакеты. Если это кадры Ethernet, то выбираются пакеты с максимальной длиной в 1500 байт, умещающиеся в поле данных кадра Ethernet. В стандарте предусматривается, что все хосты должны быть готовы принимать пакеты вплоть до 576 байт длиной (приходят ли они целиком или по фрагментам). Хостам рекомендуется отправлять пакеты размером более чем 576 байт, только если они уверены, что принимающий хост или промежуточная сеть готовы обслуживать пакеты такого размера.

Поле **Идентификатор пакета** (Identification) занимает 2 байта и используется для распознавания пакетов, образовавшихся путем фрагментации исходного пакета. Все фрагменты должны иметь одинаковое значение этого поля.

Поле **Флаги** (Flags) занимает 3 бита и содержит признаки, связанные с фрагментацией. Установленный бит DF (Do not Fragment) запрещает маршрутизатору фрагментировать данный пакет, а установленный бит MF (More Fragments) говорит о том, что данный пакет является промежуточным (не последним) фрагментом. Оставшийся бит зарезервирован.

Поле **Смещение фрагмента** (Fragment Offset) занимает 13 бит и задает смещение в байтах поля данных этого пакета от начала общего поля данных исходного пакета, подвергнутого фрагментации. Используется при сборке/разборке фрагментов пакетов при передачах их между сетями с различными величинами **MTU**. Смещение должно быть кратно 8 байт.

Поле **Время жизни** (Time to Live) занимает один байт и означает предельный срок, в течение которого пакет может перемещаться по сети. Время жизни данного пакета измеряется в секундах и задается источником передачи. На маршрутизаторах и в других узлах сети по истечении каждой секунды из текущего времени жизни вычитается единица; единица вычитается и в том случае, когда время задержки меньше секунды. Поскольку современные маршрутизаторы редко обрабатывают пакет дольше, чем за одну секунду, то время жизни можно считать равным максимальному числу узлов, которые разрешено пройти данному пакету до того, как он достигнет места назначения. Если параметр времени жизни станет нулевым до того, как пакет достигнет получателя, этот пакет будет уничтожен. Время жизни можно рассматривать как часовой механизм самоуничтожения. Значение этого поля изменяется при обработке заголовка IP-пакета.

Идентификатор **Протокол верхнего уровня** (Protocol) занимает один байт и указывает, какому протоколу верхнего уровня принадлежит информация, размещенная в поле данных пакета (например, это могут быть сегменты протокола TCP, дейтаграммы UDP, пакеты ICMP или OSPF). Значения идентификаторов для различных протоколов приводятся в документе RFC «Assigned Numbers».

Контрольная сумма (Header Checksum) занимает 2 байта и рассчитывается только по заголовку. Поскольку некоторые поля заголовка меняют свое значение в процессе передачи пакета по сети (например, время жизни), контрольная сумма проверяется и повторно рассчитывается при каждой обработке IP-заголовка. Контрольная сумма - 16 бит - подсчитывается как дополнение к сумме всех 16-битовых слов заголовка. При вычислении контрольной суммы значение самого поля «контрольная сумма» устанавливается в нуль. Если контрольная сумма неверна, то пакет будет отброшен, как только ошибка будет обнаружена.

Поля **IP-адрес источника** (Source IP Address) и IP-адрес назначения (Destination IP Address) имеют одинаковую длину - 32 бита - и одинаковую структуру.

Поле **Опции** (IP Options) является необязательным и используется обычно только при отладке сети. Механизм опций предоставляет функции управления, которые необходимы или просто полезны при определенных ситуациях, однако он не нужен при обычных коммуникациях. Это поле состоит из нескольких подполей, каждое из которых может быть одного из восьми предопределенных типов. В этих подполях можно указывать точный маршрут прохождения маршрутизаторов, регистрировать проходимые пакетом маршрутизаторы, помещать данные системы безопасности, а также временные отметки. Так как число подполей может быть произвольным, то в конце поля Опции должно быть добавлено несколько байт для выравнивания заголовка пакета по 32-битной границе.

Поле **Выравнивание** (Padding) используется для того, чтобы убедиться в том, что IP-заголовок заканчивается на 32-битной границе. Выравнивание осуществляется нулями.

Ниже приведена распечатка значений полей заголовка одного из реальных IP-пакетов, захваченных в сети Ethernet средствами анализатора протоколов Microsoft Network Monitor.

IP Version = 4 (0x4)

IP Header Length = 20 (0x14)

IP Service Type = 0 (0x0)

IP Precedence = Routine

IP ...0.... = Normal Delay

IP ....0... = Normal Throughput

IP .....0.. = Normal Reliability

IP Total Length = 54 (0x36)

IP Identification = 31746 (0x7C02)

IP Flags Summary ° 2 (0x2)

IP ..... 0 = Last fragment in datagram

IP ..... 1. = Cannot fragment datagram

IP Fragment Offset = 0 (0x0) bytes

IP Time to Live = 128 (0x80)

IP Protocol = TCP - Transmission Control

IP Checksum =0xEB86

IP Source Address = 194.85.135.75

IP Destination Address = 194.85.135.66

IP Data: Number of data bytes remaining = 34 (0x0022)

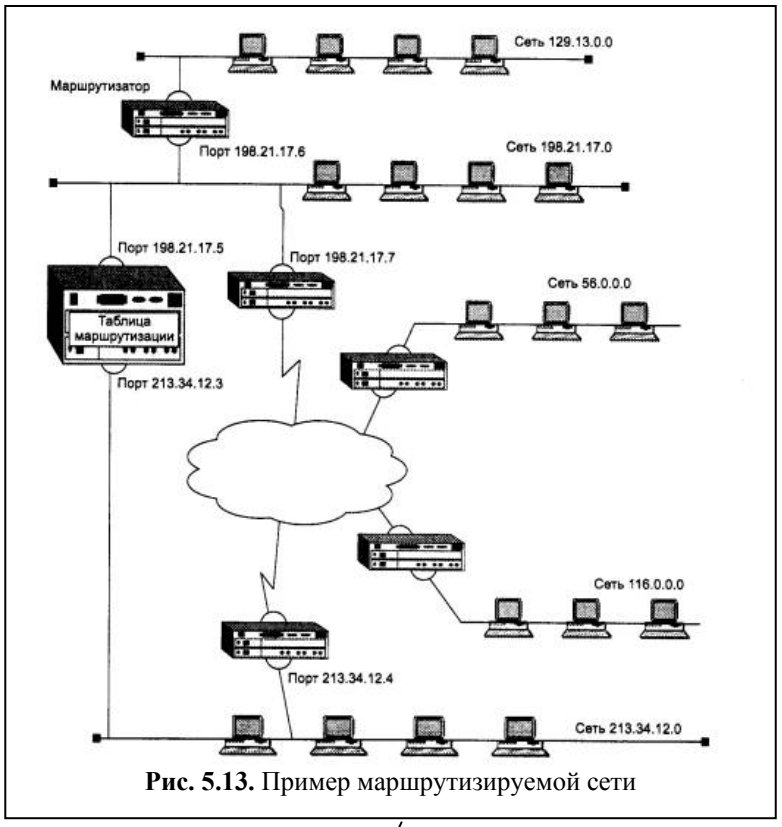


Рис. 5.13. Пример маршрутизируемой сети

5.3.3. Таблицы маршрутизации в IP-сетях

Программные модули протокола IP устанавливаются на всех конечных станциях и маршрутизаторах сети. Для продвижения пакетов они используют таблицы маршрутизации.

Если представить, что в качестве маршрутизатора Ml в данной сети работает штатный программный маршрутизатор MPR операционной системы Microsoft Windows NT, то его таблица маршрутизации могла бы иметь следующий вид (табл. 5.9).

Таблица 5.9. Таблица программного маршрутизатора MPR Windows NT

Network Address	Netmask	Gateway Address	Interface	Metric
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0	1
0.0.0.0	0.0.0.0	198.21.17.7	198.21.17.5	1
56.0.0.0	255.0.0.0	213.34.12.4	213.34.12.3	15
116.0.0.0	255.0.0.0	213.34.12.4	213.34.12.3	13
129.13.0.0	255.255.0.0	198.21.17.6	198.21.17.5	2
198.21.17.0	255.255.255.0	198.21.17.5	198.21.17.5	1
198.21.17.5	255.255.255.255	127.0.0.1	127.0.0.1	1
198.21.17.255	255.255.255.255	198.21.17.5	198.21.17.5	1
213.34.12.0	255.255.255.0	213.34.12.3	213.34.12.3	1
213.34.12.3	255.255.255.255	127.0.0.1	127.0.0.1	1
213.34.12.255	255.255.255.255	213.34.12.3	213.34.12.3	1
224.0.0.0	224.0.0.0	198.21.17.6	198.21.17.6	1
224.0.0.0	224.0.0.0	213.34.12.3	213.34.12.3	1
255.255.255.255	255.255.255.255	198.21.17.6	198.21.17.6	1

Если на месте маршрутизатора M1 установить аппаратный маршрутизатор NetBuilder II компании 3 Com, то его таблица маршрутизации для этой же сети может выглядеть так, как показано в табл. 5.10.

Таблица 5.10. Таблица маршрутизации аппаратного маршрутизатора NetBuilder II компании 3 Com

NetBuilder# Show — IP AllRoutes

Total Routes = 5 Total Direct Networks = 2

Destination	Mask	Gateway	Metric	Status	TTL	Source
198.21.17.0	255.255.255.0	198.21.17.5	0	Up	—	Connected
213.34.12.0	255.255.255.0	213.34.12.3	0	Up	—	Connected
56.0.0.0	255.0.0.0	213.34.12.4	14	Up	—	Static
116.0.0.0	255.0.0.0	213.34.12.4	12	Up	—	Static
129.13.0.0	255.255.0.0	198.21.17.6	1	Up	160	RIP

Таблица 5.11 представляет собой таблицу маршрутизации для маршрутизатора Ml, реализованного в виде программного маршрутизатора одной из версий операционной системы Unix.

Таблица 5.11. Таблица маршрутизации Unix-маршрутизатора

Destination	Gateway	Flags	Refcnt	Use	Interface
127.0.0.0	127.0.01	UH	1	154	lo0
Default	198.21.17.7	UG	5	43270	le0
198.21.17.0	198.21.17.5	U	35	246876	le0
213.34.12.0	213.34.12.3	U	44	132435	le1
129.13.0.0	198.21.1.7.6	UG	6	16450	le0
56.0.0.0	213.34.12.4	UG	12	5764	le1
116.0.0.0	213.34.12.4	UG	21	23544	le1

Назначение полей таблицы маршрутизации

Несмотря на достаточно заметные внешние различия, во всех трех таблицах есть все те ключевые параметры (три параметра), необходимые для работы маршрутизатора :

- **адрес сети назначения** (столбцы «Destination» в маршрутизаторах NetBuilder и Unix или «Network Address» в маршрутизаторе MPR) и
- **адрес следующего маршрутизатора** (столбцы «Gateway» в маршрутизаторах NetBuilder и Unix или «Gateway Address» в маршрутизаторе MPR).
- **адрес порта, на который нужно направить пакет**, в некоторых таблицах указывается прямо (поле «Interface» в таблице Windows NT), а в некоторых - косвенно. Так, в таблице Unix-маршрутизатора вместо адреса порта задается его условное наименование - 1e0 для порта с адресом 198.21.17.5, lei для порта с адресом 213.34.12.3 и 1o0 для внутреннего порта с адресом 127.0.0.1.

В маршрутизаторе NetBuilder II поле, обозначающее выходной порт в какой-либо форме, вообще отсутствует. Это объясняется тем, что адрес выходного порта всегда можно косвенно определить по адресу следующего маршрутизатора.

Остальные параметры, которые можно найти в представленных версиях таблицы маршрутизации, являются необязательными для принятия решения о пути следования пакета.

Наличие или отсутствие поля маски в таблице говорит о том, насколько современен данный маршрутизатор. Стандартным решением сегодня является использование поля маски в каждой записи таблицы, как это сделано в таблицах маршрутизаторов MPR Windows NT (поле «Netmask») и NetBuilder (поле «Mask»). Отсутствие поля маски говорит о том, что либо маршрутизатор рассчитан на работу только с тремя стандартными классами адресов, либо он использует для всех записей одну и ту же маску, что снижает гибкость маршрутизации.

Метрика, как видно из примера таблицы Unix-маршрутизатора, является необязательным параметром. В остальных двух таблицах это поле имеется, однако оно используется только в качестве признака непосредственно подключенной сети.

Источники и типы записей в таблице маршрутизации (подробнее – см. [1] стр. 56—58)**:**

1-ый — ПО стека TCP/IP. При инициализации маршрутизатора это ПО автоматически заносит в таблицу несколько записей, в результате чего создается так называемая минимальная таблица маршрутизации.

- Это, во-первых, записи о непосредственно подключенных сетях и маршрутизаторах по умолчанию (default)
- Во-вторых, ПО автоматически заносит в таблицу м-ции записи об адресах особого назначения.
  - Особый адрес 127.0.0.0 (loopback), который используется для локального тестирования стека TCP/IP. Пакеты, направленные в сеть с номером 127.0.0.0, не передаются протоколом IP на канальный уровень для последующей передачи в сеть, а возвращаются в источник - локальный модуль IP.
  - Записи с адресом 224.0.0.0 требуются для обработки групповых адресов (multicast address).
  - Кроме того, в таблицу могут быть занесены адреса, предназначенные для обработки широковещательных рассылок

2-ой — администратор, непосредственно формирующий запись с пом. некоторой сист. утилиты, например программы route, имеющейся в ОС Unix и Windows NT. В аппаратных м-рах также всегда имеется команда для ручного задания записей таблицы м-ции. Заданные вручную записи всегда являются статическими, то есть не имеют срока истечения жизни. Эти записи могут быть как постоянными, то есть сохраняющимися при перезагрузке маршрутизатора, так и временными, хранящимися в таблице только до выключения устройства. Часто администратор вручную заносит запись default о м-ре по умолчанию. Таким же образом в таблицу м-ции может быть внесена запись о специфичном для узла маршруте. Специфичный для узла маршрут содержит вместо номера сети полный IP-адрес, то есть адрес, имеющий ненулевую информацию не только в поле номера сети, но и в поле номера узла. Предполагается, что для такого конечного узла маршрут должен выбираться не так, как для всех остальных узлов сети, к которой он относится. В случае когда в таблице есть разные записи о продвижении пакетов для всей сети и ее отдельного узла, при поступлении пакета, адресованного узлу, маршрутизатор отдаст предпочтение записи с полным адресом узла.

3-ий — протоколы м-ции, такие как RIP или OSPF. Такие записи всегда являются динамическими, то есть имеют ограниченный срок жизни. Программные м-ры Windows NT и Unix не показывают источник появления той или иной записи в таблице, а м-р NetBuilder использует для этой цели поле «Source». В приведенном в табл. 5.10 примере первые две записи созданы программным обеспечением стека на основании данных о конфигурации портов маршрутизатора - это показывает признак «Connected». Следующие две записи обозначены как «Static», что указывает на то, что их ввел вручную администратор. Последняя запись является следствием работы протокола RIP, поэтому в ее поле «TTL» имеется значение 160.

Маршрутизация с использованием масок [1] стр. 61 – 70

Использование масок для структуризации сети (Маршрутизация с использованием масок одинаковой длины *[1] стр. 61 – 65***)**

Рассмотрим, как изменяется работа модуля IP, когда становится необходимым учитывать наличие масок. Во-первых, в каждой записи таблицы маршрутизации появляется новое поле - поле маски.

Во-вторых, меняется алгоритм определения маршрута по таблице маршрутизации. После того как IP-адрес извлекается из очередного полученного IP-пакета, необходимо определить адрес следующего маршрутизатора, на который надо передать пакет с этим адресом. Модуль IP последовательно просматривает все записи таблицы маршрутизации. С каждой записью производятся следующие действия.

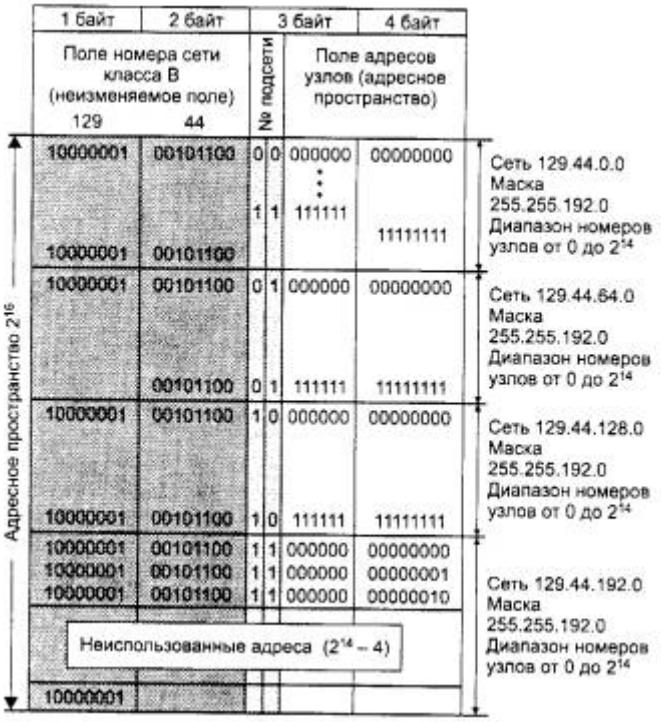


Рис. 5.15. Разделение адресного пространства сети класса B 129.44.0.0 на четыре равные части путем использования масок одинаковой длины 255.255.192.0

- Маска M, содержащаяся в данной записи, накладывается на IP-адрес узла назначения, извлеченный из пакета.
- Полученное в результате число является номером сети назначения обрабатываемого пакета. Оно сравнивается с номером сети, который помещен в данной записи таблицы маршрутизации.
- Если номера сетей совпадают, то пакет передается маршрутизатору, адрес которого помещен в соответствующем поле данной записи. [1] стр. 65

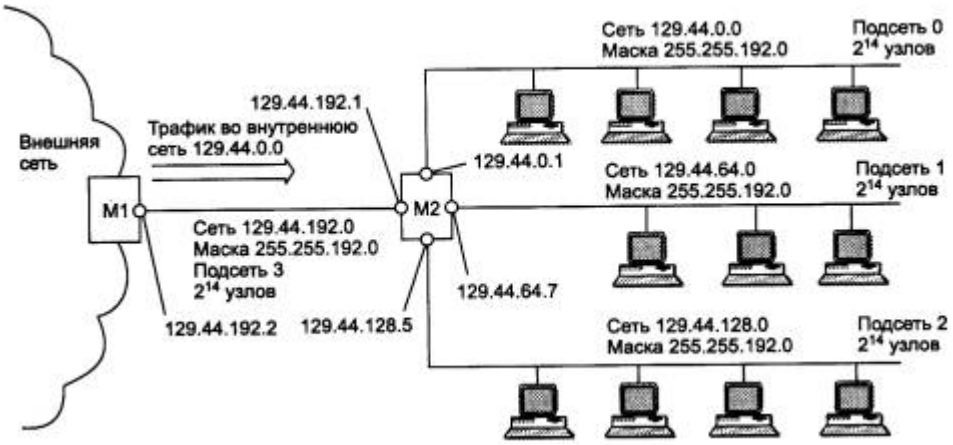


Рис. 5.16. Маршрутизация с использованием масок одинаковой длины

Таблица 5.12. Таблица маршрутизатора M2 в сети с масками одинаковой длины

Номер сети	Маска	Адрес следующего маршрутизатора	Адрес порта	Расстояние
129.44.0.0	255.255.192.0	129.44.0.1	129.44.192.2	Подключена
129.44.64.0	255.255.192.0	129.44.64.7	129.44.64.7	Подключена
129.44.128.0	255.255.192.0	129.44.128.5	129.44.128.5	Подключена
129.44.192.0	255.255.192.0	129.44.192.1	129.44.192.1	Подключена
0.0.0.0	0.0.0.0	129.44.192.2	129.44.192.1	—

Использование масок переменной длины (Технология VLSM. *Variable Length Subnet Mask***)**

В предыдущем примере использования масок (см. рис. 5.15 и 5.16) все подсети имеют одинаковую длину поля номера сети - 18 двоичных разрядов, и, следовательно, для нумерации узлов в каждой из них отводится по 14 разрядов. То есть все сети являются очень большими и имеют одинаковый размер. Однако в этом случае, как и во многих других, более эффективным явилось бы разбиение сети на подсети разного размера. В частности, большое число узлов, вполне желательное для пользовательской подсети, явно является избыточным для подсети, которая связывает два маршрутизатора по схеме «точка-точка». В этом случае требуются всего два адреса для адресации двух портов соседних маршрутизаторов. В предыдущем же примере для этой вспомогательной сети Ml - M2 был использован номер, позволяющий адресовать 214 узлов, что делает такое решение неприемлемо избыточным. Администратор может более рационально распределить имеющееся в его распоряжении адресное пространство с помощью масок переменной длины.

На рис. 5.17 приведен пример распределения адресного пространства, при котором **избыточность имеющегося множества IP-адресов может быть сведена к минимуму**. Половина из имеющихся адресов (215) была отведена для создания сети с адресом 129.44.0.0 и маской 255.255.128.0. Следующая порция адресов, составляющая четверть всего адресного пространства (214), была назначена для сети 129.44.128.0 с маской 255.255.192.0. Далее в пространстве адресов был «вырезан» небольшой фрагмент для создания сети, предназначенной для связывания внутреннего маршрутизатора M2 с внешним маршрутизатором Ml.

В IP-адресе такой вырожденной сети для поля номера узла как минимум должны быть отведены два двоичных разряда. Из четырех возможных комбинаций номеров узлов: 00, 01,10 и 11 два номера имеют специальное назначение и не могут быть присвоены узлам, но оставшиеся два 10 и 01 позволяет адресовать порты маршрутизаторов. В нашем примере сеть

была выбрана с некоторым запасом - на 8 узлов. Поле номера узла в таком случае имеет 3 двоичных разряда, маска в десятичной нотации имеет вид 255.255.255.248, а номер сети, как видно из рис. 5.17, равен в данном конкретном случае 129.44.192.0. Если эта сеть является локальной, то на ней могут быть расположены четыре узла помимо двух портов маршуртизаторов.

ПРИМЕЧАНИЕ Заметим, что глобальным связям между маршрутизаторами типа «точка-точка» не обязательно давать IP-адреса, так как к такой сети не могут подключаться никакие другие узлы, кроме двух портов маршрутизаторов. Однако чаще всего такой вырожденной сети все же дают IP-адрес. Это делается, например, для того, чтобы скрыть внутреннюю структуру сети и обращаться к ней по одному адресу входного порта маршрутизатора, в данном примере по адресу 129.44.192.1. Кроме того, этот адрес может понадобиться при туннелировании немаршрутизируемых протоколов в IP-пакеты, что будет рассмотрено ниже.

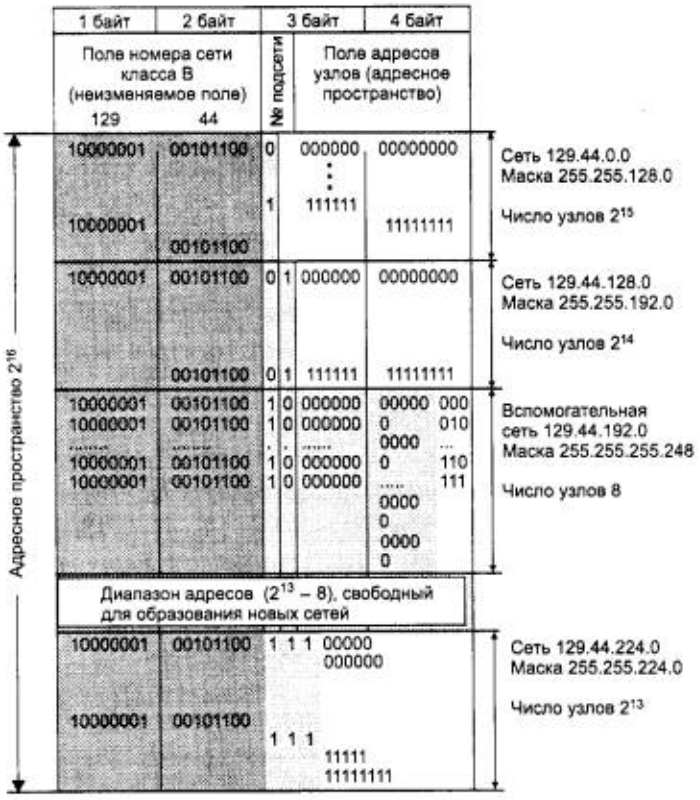


Рис. 5.17. Разделение адресного пространства сети класса B 129.44.0.0 на сети разного размера путем использования масок переменной длины

Оставшееся адресное пространство администратор может «нарезать» на разное количество сетей разного объема в зависимости от своих потребностей. Из оставшегося пула (214 - 4) адресов администратор может образовать еще одну достаточно большую сеть с числом узлов 213. При этом свободными останутся почти столько же адресов (213 - 4), которые также могут быть использованы для создания новых сетей. К примеру, из этого «остатка» можно образовать 31 сеть, каждая из которых равна размеру стандартной сети класса C, и к тому же еще несколько сетей меньшего размера. Ясно, что разбиение может быть другим, но в любом случае **с помощью масок переменного размера администратор всегда имеет возможность гораздо рациональнее использовать все имеющиеся у него адреса**.

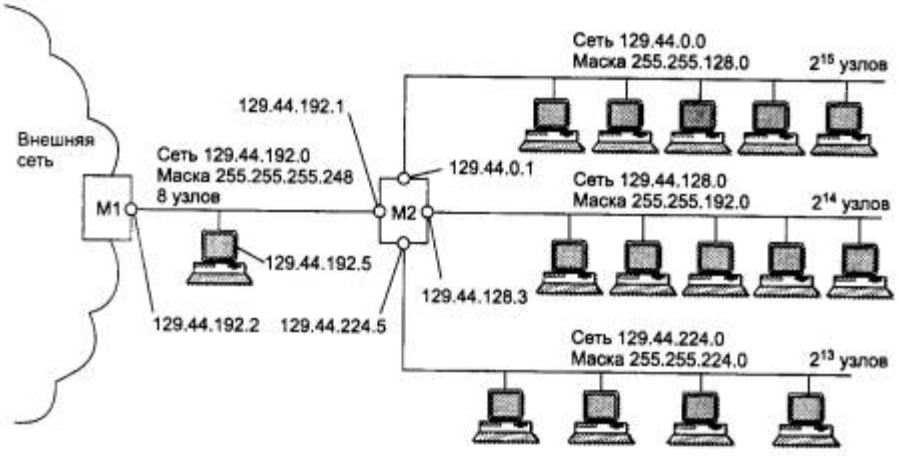


Рис. 5.18. Сеть, структурированная с использованием масок переменной длины

Таблица маршрутизации M2, соответствующая структуре сети, показанной на рис. 5.18, содержит записи о четырех непосредственно подключенных сетях и запись о маршрутизаторе по умолчанию (табл. 5.13). Процедура поиска маршрута при использовании масок переменной

длины ничем не отличается от подобной процедуры, описанной ранее для масок одинаковой длины.

Таблица 5.13. Таблица маршрутизатора М2 в сети с масками переменной длины

Номер сети	Маска	Адрес следующего маршрутизатора	Адрес порта	Расстояние
129.44.0.0	255.255.128.0	129.44.0.1	129.44.0.1	Подключена
129.44.128.0	255.255.192.0	129.44.128.3	129.44.128.3	Подключена
129.44.192.0	255.255.255.248	129.44.192.1	129.44.191.1	Подключена
129.44.224.0	255.255.224.0	129.44.224.5	129.44.224.5	Подключена
0.0.0.0	0.0.0.0	129.44.192.2	129.44.192.1	—

Некоторые особенности масок переменной длины проявляются при наличии так называемых «перекрытий». Под перекрытием понимается наличие нескольких маршрутов к одной и той же сети или одному и тому же узлу. В этом случае адрес сети в пришедшем пакете может совпасть с адресами сетей, содержащихся сразу в нескольких записях таблицы маршрутизации.

Рассмотрим пример. Пусть пакет, поступивший из внешней сети на маршрутизатор Ml, имеет адрес назначения 129.44.192.5. Ниже приведен фрагмент таблицы маршрутизации маршрутизатора Ml. Первая из приведенных двух записей говорит о том, что все пакеты, адреса которых начинаются на 129.44, должны быть переданы на маршрутизатор М2. Эта запись выполняет **агрегирование** адресов всех подсетей, созданных на базе одной сети 129.44.0.0. Вторая строка говорит о том, что среди всех возможных подсетей сети 129.44.0.0 есть одна, 129.44.192.0, для которой пакеты можно направлять непосредственно, а не через м-р М2.

Номер сети	Маска	Адрес следующего маршрутизатора	Адрес порта	Расстояние
.....	.....	.....	.....	.....
129.44.0.0	255.255.0.0	129.44.192.1	129.44.191.2	2
129.44.192.0	255.255.255.248	129.44.192.2	129.44.192.2	Подключена
.....	.....	.....	.....	.....

Если следовать стандартному алгоритму поиска маршрута по таблице, то сначала на адрес назначения 129.44.192.5 накладывается маска из первой строки 255.255.0.0 и получается результат 129.44.0.0, который совпадает с номером сети в этой строке. Но и при наложении на адрес 129.44.192.5 маски из второй строки 255.255.255.248 полученный результат 129.44.192.0 также совпадает с номером сети во второй строке. В таких случаях должно быть применено следующее правило: «Если адрес принадлежит нескольким подсетям в базе данных маршрутов, то продвигающий пакет маршрутизатор использует наиболее специфический маршрут, то есть выбирается адрес подсети, дающий большее совпадение разрядов».

В данном примере будет выбран второй маршрут, то есть пакет будет передан в непосредственно подключенную сеть, а не пойдет кружным путем через маршрутизатор М2.

Механизм выбора самого специфического маршрута является обобщением понятия «маршрут по умолчанию». Поскольку в традиционной записи для маршрута по умолчанию 0.0.0.0 маска 0.0.0.0 имеет нулевую длину, то этот маршрут считается самым неспецифическим и используется только при отсутствии совпадений со всеми остальными записями из таблицы маршрутизации.

ПРИМЕЧАНИЕ В IP-пакетах при использовании механизма масок по-прежнему передается только IP-адрес назначения, а маска сети назначения не передается. Поэтому из IP-адреса пришедшего пакета невозможно выяснить, какая часть адреса относится к номеру сети, а какая - к номеру узла. Если маски во всех подсетях имеют один размер, то это не создает проблем. Если же для образования подсетей применяют маски переменной длины, то маршрутизатор должен каким-то образом узнавать, каким адресам сетей какие маски соответствуют. Для этого используются протоколы маршрутизации, переносящие между маршрутизаторами не только служебную информацию об адресах сетей, но и о масках, соответствующих этим номерам. К таким протоколам относятся протоколы RIPv2 и OSPF, а вот, например, протокол RIP маски не распространяет и для использования масок переменной длины не подходит.

Технология бесклассовой междоменной маршрутизации CIDR

За последние несколько лет в сети Internet многое изменилось: резко возросло число узлов и сетей, повысилась интенсивность трафика, изменился характер передаваемых данных. Из-за несовершенства протоколов маршрутизации обмен сообщениями об обновлении таблиц стал иногда приводить к сбоям магистральных маршрутизаторов из-за перегрузки при обработке большого объема служебной информации. Так, в 1994 году таблицы магистральных маршрутизаторов в Internet содержали до 70 000 маршрутов.

На решение этой проблемы была направлена, в частности, и технология бес-классовой междоменной маршрутизации (Classless Inter-Domain Routing, CIDR), впервые о которой было официально объявлено в 1993 году, когда были опубликованы RFC 1517, RFC 1518, RFC 1519 и RFC 1520.

Суть технологии CIDR заключается в следующем. Каждому поставщику услуг Internet должен назначаться непрерывный диапазон в пространстве IP-адресов. При таком подходе адреса всех сетей каждого поставщика услуг имеют общую старшую часть - префикс, поэтому маршрутизация на магистралях Internet может осуществляться на основе префиксов, а не полных адресов сетей. Агрегирование адресов позволит уменьшить объем таблиц в маршрутизаторах всех уровней, а следовательно, ускорить работу маршрутизаторов и повысить пропускную способность Internet.

Деление IP-адреса на номер сети и номер узла в технологии CIDR происходит не на основе нескольких старших бит, определяющих класс сети (A, B или C), а на основе маски переменной длины, назначаемой поставщиком услуг. На рис. 5.19 показан пример некоторого пространства IP-адресов, которое имеется в распоряжении гипотетического поставщика услуг. Все адреса имеют общую часть в k старших разрядах - префикс. Оставшиеся n разрядов используются для дополнения неизменяемого префикса переменной частью адреса. Диапазон имеющихся адресов в таком случае составляет 2n. Когда потребитель услуг обращается к поставщику услуг с просьбой о выделении ему некоторого количества адресов, то в имеющемся пуле адресов «вырезается» непрерывная область S1, S2, S3 или S4 соответствующего размера. Причем границы этой области выбираются такими, чтобы для нумерации требуемого числа узлов хватило некоторого числа младших разрядов, а значения всех оставшихся (старших) разрядов было одинаковым у всех адресов данного диапазона. Таким условиям могут удовлетворять только области, размер которых кратен степени двойки, А границы выделяемого участка должны быть кратны требуемому размеру.

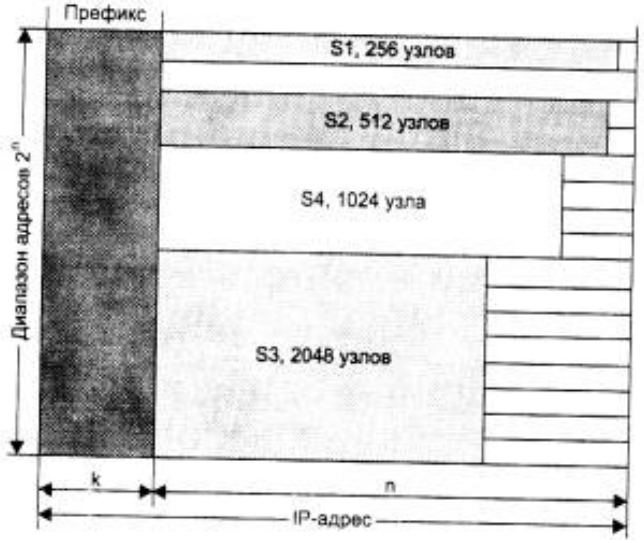


Рис. 5.19. Технологии CIDR

Рассмотрим пример. Пусть поставщик услуг Internet располагает пулом адресов в диапазоне 193.20.0.0-193.23.255.255 (1100 0001.0001 0100.0000 0000.0000 0000-11000001.0001 0111.11111111.11111111) с общим префиксом 193.20(11000001.0001 01) и маской, соответствующей этому префиксу 255.252.0.0.

Если абоненту этого поставщика услуг требуется совсем немного адресов, например 13, то поставщик мог бы предложить ему различные варианты: сеть 193.20.30.0, сеть 193.20.30.16 или сеть 193.21.204.48, все с одним и тем же значением маски 255.255.255.240. Во всех случаях в распоряжении абонента для нумерации узлов имеются 4 младших бита.

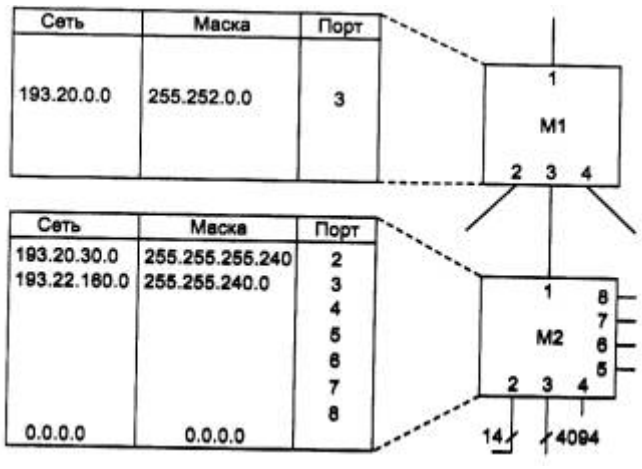


Рис. 5.20. Выигрыш в количестве записей в маршрутизаторе при использовании технологии CIDR

Рассмотрим другой вариант, когда к

поставщику услуг обратился крупный заказчик, сам, возможно собирающийся оказывать услуги по доступу в Internet. Ему требуется блок адресов в 4000 узлов. В этом случае поставщик услуг мог бы предложить ему, например, диапазон адресов 193,22.160.0-193.22.175.255 с маской 255.255.240.0. Агрегированный номер сети (префикс) в этом случае будет равен 193.22.160.0.

Администратор маршрутизатора М2 (рис. 5.20) поместит в таблицу маршрутизации только по одной записи на каждого клиента, которому был выделен пул адресов, независимо от количества подсетей, организованных клиентом. Если клиент, получивший сеть 193.22.160.0, через некоторое время разделит ее адресное пространство в 4096 адресов на 8 подсетей, то в маршрутизаторе М2 первоначальная информация о выделенной ему сети не изменится.

Для поставщика услуг верхнего уровня, поддерживающего клиентов через маршрутизатор Ml, усилия поставщика услуг нижнего уровня по разделению его адресного пространства также не будут заметны. Запись 193.20.0,0 с маской 255.252.0,0 полностью описывает сети поставщика услуг нижнего уровня в маршрутизаторе Ml.

Итак, внедрение технологии CIDR позволяет решить две основные задачи.

- **Более экономное расходование адресного пространства**. Действительно, получая в свое распоряжение адрес сети, например, класса С, некоторые организации не используют весь возможный диапазон адресов просто потому, что в их сети имеется гораздо меньше 255 узлов. Технология CIDR отказывается от традиционной концепции разделения адресов протокола IP на классы, что позволяет получать в пользование столько адресов, сколько реально необходимо. Благодаря технологии CIDR поставщики услуг получают возможность «нарезать» блоки из выделенного им адресного пространства в точном соответствии с требованиями каждого клиента, при этом у клиента остается пространство для маневра на случай его будущего роста.
- **Уменьшение числа записей в таблицах маршрутизаторов за счет объединения маршрутов** - одна запись в таблице маршрутизации может представлять большое количество сетей. Действительно, для всех сетей, номера которых начинаются с одинаковой последовательности цифр, в таблице маршрутизации может быть предусмотрена одна запись (см. рис. 5.20). Так, маршрутизатор М2 установленный в организации, которая использует технику CIDR для выделения адресов своим клиентам, должен поддерживать в своей таблице маршрутизации все 8 записей о сетях клиентов. А маршрутизатору Ml достаточно иметь одну запись о всех этих сетях, на основании которой он передает пакеты с префиксом 193.20 маршрутизатору М2, который их и распределяет по нужным портам.

Если все поставщики услуг Internet будут придерживаться стратегии CIDR, то особенно заметный выигрыш будет достигаться в магистральных маршрутизаторах.

Технология CIDR уже успешно используется в текущей версии IPv4 и поддерживается такими протоколами маршрутизации, как OSPF, RIP-2, **BGP4**. Предполагается, что эти же протоколы будут работать и с новой версией протокола IPv6. Следует отметить, что в настоящее время технология CIDR поддерживается магистральными маршрутизаторами Internet, а не обычными хостами в локальных сетях.

Использование CIDR в сетях IPv4 в общем случае требует перенумерации сетей. Поскольку эта процедура сопряжена с определенными временными и материальными затратами, для ее проведения пользователей нужно каким-либо образом стимулировать. В качестве таких стимулов рассматривается, например, введение оплаты за строку в таблице маршрутизации или же за количество узлов в сети. При использовании классов сетей абонент часто не полностью занимает весь допустимый диапазон адресов узлов - 254 адреса для сети класса С или 65 534 адреса для сети класса В. Часть адресов узлов обычно пропадает. Требование оплаты каждого адреса узла поможет пользователю решиться на перенумерацию, с тем чтобы получить ровно столько адресов, сколько ему нужно.

5.3.6. Фрагментация IP-пакетов

Протокол IP позволяет выполнять фрагментацию пакетов, поступающих на входные порты маршрутизаторов.

Следует различать фрагментацию сообщений в узле-отправителе и динамическую фрагментацию сообщений в транзитных узлах сети - маршрутизаторах. Практически во всех стеках протоколов есть протоколы, которые отвечают за фрагментацию сообщений прикладного уровня на такие части, которые укладываются в кадры канального уровня. В стеке TCP/IP эту задачу решает протокол TCP, который разбивает поток байтов, передаваемый ему с прикладного уровня на сообщения нужного размера (например, на 1460 байт для протокола Ethernet). Поэтому протокол IP в узле-отправителе не использует свои возможности по фрагментации пакетов.

А вот при необходимости передать пакет в следующую сеть, для которой размер пакета является слишком большим, IP-фрагментация становится необходимой. В функции уровня IP входит разбиение слишком длинного для конкретного типа составляющей сети сообщения на более короткие пакеты с созданием соответствующих служебных полей, нужных для последующей сборки фрагментов в исходное сообщение.

В большинстве типов локальных и глобальных сетей значения MTU, то есть максимальный размер поля данных, в которое должен инкапсулировать свой пакет протокол IP, значительно отличается. Сети Ethernet имеют значение MTU, равное 1500 байт, сети FDDI - 4096 байт, а сети X.25 чаще всего работают с MTU в 128 байт.

IP-пакет может быть помечен как не фрагментируемый. Любой пакет, помеченный таким образом, не может быть фрагментирован модулем IP ни при каких условиях. Если же пакет, помеченный как не фрагментируемый, не может достигнуть получателя без фрагментации, то этот пакет просто уничтожается, а узлу-отправителю посылается соответствующее ICMP-сообщение.

Протокол IP допускает возможность использования в пределах отдельной подсети ее собственных средств фрагментирования, невидимых для протокола IP. Например, технология ATM делит поступающие IP-пакеты на ячейки с полем данных в 48 байт с помощью своего уровня сегментирования, а затем собирает ячейки в исходные пакеты на выходе из сети. Но такие технологии, как ATM, являются скорее исключением, чем правилом.

Процедуры фрагментации и сборки протокола IP рассчитаны на то, чтобы пакет мог быть разбит на практически любое количество частей, которые впоследствии могли бы быть вновь собраны. Получатель фрагмента использует поле идентификации для того, чтобы не перепутать фрагменты различных пакетов. Модуль IP, отправляющий пакет, устанавливает в поле идентификации значение, которое должно быть уникальным для данной пары отправитель - получатель, а также время, в течение которого пакет может быть активным в сети.

Поле смещения фрагмента сообщает получателю положение фрагмента в исходном пакете. Смещение фрагмента и длина определяют часть исходного пакета, принесенную этим фрагментом. Флаг «more fragments» показывает появление последнего фрагмента. Модуль протокола IP, отправляющий неразбитый на фрагменты пакет, устанавливает в нуль флаг «more fragments» и смещение во фрагменте.

Эти поля дают достаточное количество информации для сборки пакета.

Чтобы разделить на фрагменты большой пакет, модуль протокола IP, установленный, например, на маршрутизаторе, создает несколько новых пакетов и копирует содержимое полей IP-заголовка из большого пакета в IP-заголовки всех новых пакетов. Данные из старого пакета делятся на соответствующее число частей, размер каждой из которых, кроме самой последней, обязательно должен быть кратным 8 байт. Размер последней части данных равен полученному остатку.

Каждая из полученных частей данных помещается в новый пакет. Когда происходит фрагментация, то некоторые параметры IP-заголовка копируются в заголовки всех фрагментов, а другие остаются лишь в заголовке первого фрагмента. Процесс фрагментации может изменить значения данных, расположенных в поле параметров, и значение контрольной суммы заголовка, изменить значение флага «more fragments» и смещение фрагмента, изменить длину IP-заголовка и общую длину пакета, В заголовок каждого пакета заносятся соответствующие значения в поле смещения «fragment offset», а в поле общей длины пакета помещается длина каждого пакета. Первый фрагмент будет иметь в поле «fragment offset» нулевое значение. Во всех пакетах, кроме последнего, флаг «more fragments» устанавливается в единицу, а в последнем фрагменте - в нуль.

Чтобы собрать фрагменты пакета, модуль протокола IP (например, модуль на хост - компьютере) объединяет IP-пакеты, имеющие одинаковые значения в полях идентификатора, отправителя, получателя и протокола. Таким образом, отправитель должен выбрать идентификатор таким образом, чтобы он был уникален для данной пары отправитель-получатель, для данного протокола и в течение того времени, пока данный пакет (или любой его фрагмент) может существовать в составной IP-сети.

Очевидно, что модуль протокола IP, отправляющий пакеты, должен иметь таблицу идентификаторов, где каждая запись соотносится с каждым отдельным получателем, с которым осуществлялась связь, и указывает последнее значение максимального времени жизни пакета в IP-сети. Однако, поскольку поле идентификатора допускает 65 536 различных значений, некоторые хосты могут использовать просто уникальные идентификаторы, не зависящие от адреса получателя.

В некоторых случаях целесообразно, чтобы идентификаторы IP-пакетов выбирались протоколами более высокого, чем IP, уровня. Например, в протоколе TCP предусмотрена повторная передача TCP - сегментов, по каким-либо причинам не дошедшим до адресата.

Вероятность правильного приема увеличивалась бы, если бы при повторной передаче идентификатор для IP-пакета был бы тем же, что и в исходном IP-пакете, поскольку его фрагменты могли бы использоваться для сборки правильного TCP - сегмента.

Процедура объединения заключается в помещении данных из каждого фрагмента в позицию, указанную в заголовке пакета в поле «fragment offset».

Каждый модуль IP должен быть способен передать пакет из 68 байт без дальнейшей фрагментации. Это связано с тем, что IP-заголовок может включать до 60 байт, а минимальный фрагмент данных - 8 байт. Каждый получатель должен быть в состоянии принять пакет из 576 байт в качестве единого куска либо в виде фрагментов, подлежащих сборке.

Если бит флага запрета фрагментации (Don't Fragment, DF) установлен, то фрагментация данного пакета запрещена, даже если в этом случае он будет потерян. Данное средство может использоваться для предотвращения фрагментации в тех случаях, когда хост - получатель не имеет достаточных ресурсов для сборки фрагментов.

Работа протокола IP по фрагментации пакетов в хостах и маршрутизаторах иллюстрируется на рис. 5.21.

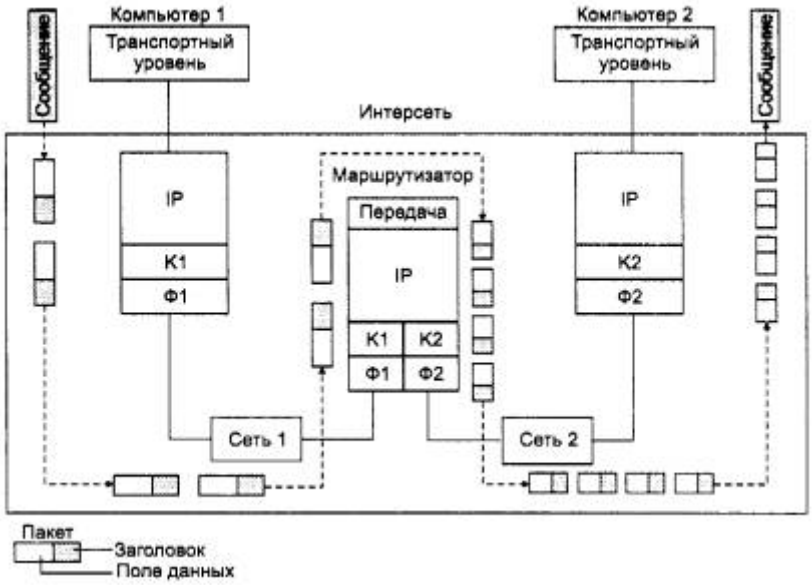


Рис.5.21. Фрагментация IP-пакетов при передаче между сетями с разным максимальным размером пакетов: К1 и 01 - канальный и физический уровень сети 1; К2 и Ф2 - канальный и физический уровень сети 2

Пусть компьютер 1 связан с сетью, имеющей значение MTU в 4096 байт, например с сетью FDDI, При поступлении на IP-уровень компьютера 1 сообщения от транспортного уровня размером в 5600 байт протокол IP делит его на два IP-пакета, устанавливая в первом пакете признак фрагментации и присваивая пакету уникальный идентификатор, например 486, В первом пакете величина поля смещения равна 0, а во втором - 2800. Признак фрагментации во втором пакете равен нулю, что показывает, что это последний фрагмент пакета. Общая величина IP-пакета составляет 2800 плюс 20 (размер IP-заголовка), то есть 2820 байт, что умещается в поле данных кадра FDDI. Далее модуль IP компьютера 1 передает эти пакеты своему сетевому интерфейсу (образуемому протоколами канального уровня К 1 и физического уровня Ф1), Сетевой интерфейс отправляет кадры следующему маршрутизатору.

После того, как кадры пройдут уровень сетевого интерфейса маршрутизатора (К1 и Ф1) и освободятся от заголовков FDDI, модуль IP по сетевому адресу определяет, что прибывшие два пакета нужно передать в сеть 2, которая является сетью Ethernet и имеет значение MTU, равное 1500. Следовательно, прибывшие IP-пакеты необходимо фрагментировать. Маршрутизатор извлекает поле данных из каждого пакета и делит его еще пополам, чтобы каждая часть уместилась в поле данных кадра Ethernet. Затем он формирует новые IP-пакеты, каждый из которых имеет длину 1400 + 20 - 1420 байт, что меньше 1500 байт, поэтому они нормально помещаются в поле данных кадров Ethernet.

В результате в компьютер 2 по сети Ethernet приходят четыре IP-пакета с общим идентификатором 486, что позволяет протоколу IP, работающему в компьютере 2, правильно собрать исходное сообщение. Если пакеты пришли не в том порядке, в котором были посланы, то смещение укажет правильный порядок их объединения.

Отметим, что IP-маршрутизаторы не собирают фрагменты пакетов в более крупные пакеты, даже если на пути встречается сеть, допускающая такое укрупнение. Это связано с тем, что отдельные фрагменты сообщения могут перемещаться по интерсети по различным маршрутам,

поэтому нет гарантии, что все фрагменты проходят через какой-либо промежуточный маршрутизатор на их пути.

При приходе первого фрагмента пакета узел назначения запускает таймер, который определяет максимально допустимое время ожидания прихода остальных фрагментов этого пакета. Таймер устанавливается на максимальное из двух значений: первоначальное установочное время ожидания и время жизни, указанное в принятом фрагменте. Таким образом, первоначальная установка таймера является нижней границей для времени ожидания при сборі. Если таймер истекает раньше прибытия последнего фрагмента, то все ресурсы сборки, связанные с данным пакетом, освобождаются, все полученные к этому моменту фрагменты пакета отбрасываются, а в узел, пославший исходный пакет, направляется сообщение об ошибке с помощью протокола ICMP.

Технология CIDR и VLSM из Семёнова [4]

5.3.7. Протокол надежной доставки TCP-сообщений

Протокол IP является дейтаграммным протоколом и поэтому по своей природе не может гарантировать надежность передачи данных. Эту задачу - обеспечение надежного канала обмена данными между прикладными процессами в составной сети -решает **протокол TCP** (Transmission Control Protocol), относящийся к транспортному уровню.

Протокол TCP работает непосредственно над протоколом IP и использует для транспортировки своих блоков данных потенциально ненадежный протокол IP. Надежность передачи данных протоколом TCP достигается за счет того, что он основан на установлении логических соединений между взаимодействующими процессами. До тех пор пока программы протокола TCP продолжают функционировать корректно, а составная сеть не распалась на несвязные части, ошибки в передаче данных на уровне протокола IP не будут влиять на правильное получение данных.

Протокол IP используется протоколом TCP в качестве транспортного средства. Перед отправкой своих блоков данных протокол TCP помещает их в оболочку IP-пакета. При необходимости протокол IP осуществляет любую фрагментацию и сборку блоков данных TCP, требующуюся для осуществления передачи и доставки через множество сетей и промежуточных шлюзов.

На рис. 5.22 показано, как процессы, выполняющиеся на двух конечных узлах, устанавливают с помощью протокола TCP надежную связь через составную сеть, все узлы которой используют для передачи сообщений дейтаграммный протокол IP.

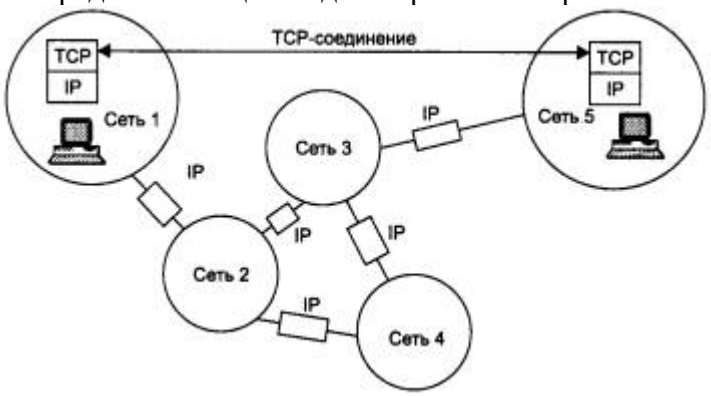


Рис. 5.22. TCP-соединение создает надежный канал связи между конечными узлами

Порты

Протокол TCP взаимодействует через межуровневые интерфейсы с ниже лежащим протоколом IP и с выше лежащими протоколами прикладного уровня или приложениями.

В то время как задачей сетевого уровня, к которому относится протокол IP, является передача данных между произвольными узлами сети, задача транспортного уровня, которую решает протокол TCP, заключается в передаче данных между любыми **прикладными процессами**, выполняющимися на любых узлах сети. Действительно, после того как пакет средствами протокола IP доставлен в компьютер-получатель, данные необходимо направить конкретному процессу-получателю. Каждый компьютер может выполнять несколько процессов, более того, прикладной процесс тоже может иметь несколько точек входа, выступающих в качестве адреса назначения для пакетов данных.

Пакеты, поступающие на транспортный уровень, организуются операционной системой в виде множества очередей к точкам входа различных прикладных процессов. В терминологии TCP/IP такие системные очереди называются **портами**. Таким образом, адресом назначения, который используется протоколом TCP, является идентификатор (номер) порта прикладной службы. Номер порта в совокупности с номером сети и номером конечного узла однозначно определяют прикладной процесс в сети. Этот набор идентифицирующих параметров имеет название **сокет** (socket).

Назначение номеров портов прикладным процессам осуществляется либо **централизованно,** если эти процессы представляют собой популярные общедоступные службы (например, номер 21 закреплен за службой удаленного доступа к файлам FTP, а 23 - за службой удаленного управления telnet), либо локально для тех служб, которые еще не стали столь распространенными, чтобы закреплять за ними стандартные (зарезервированные) номера. Централизованное присвоение службам номеров портов выполняется организацией Internet Assigned Numbers Authority (IANA). Эти номера затем закрепляются и опубликовываются в стандартах Internet (RFC 1700).

Локальное присвоение номера порта заключается в том, что разработчик некоторого приложения просто связывает с ним любой доступный, произвольно выбранный числовой идентификатор, обращая внимание на то, чтобы он не входил в число зарезервированных номеров портов. В дальнейшем все удаленные запросы к данному приложению от других приложений должны адресоваться с указанием назначенного ему номера порта.

Протокол TCP ведет для каждого порта две очереди: очередь пакетов, поступающих в данный порт из сети, и очередь пакетов, отправляемых данным портом в сеть. Процедура обслуживания протоколом TCP запросов, поступающих от нескольких различных прикладных служб, называется **мультиплексированием**. Обратная процедура распределения протоколом TCP поступающих от сетевого уровня пакетов между набором высокоуровневых служб, идентифицированных номерами портов, называется **демультиплексированием** (рис. 5.23).

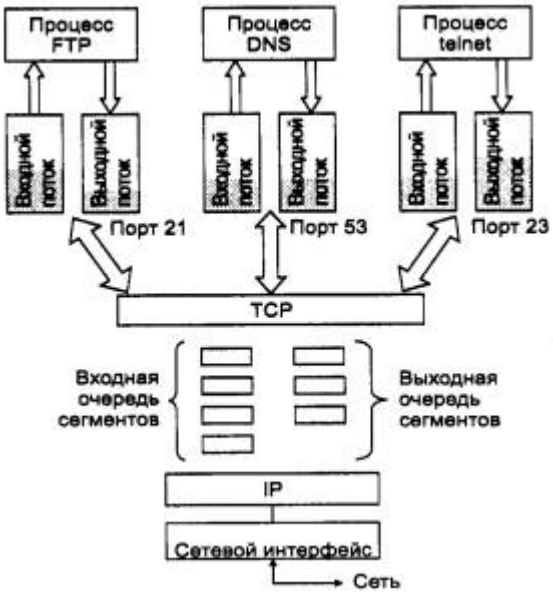


Рис. 5.23. Функции протокола TCP по мультиплексированию и демультиплексированию потоков

Сегменты и потоки

Единицей данных протокола TCP является **сегмент**. Информация, поступающая к протоколу TCP в рамках логического соединения от протоколов более высокого уровня, рассматривается протоколом TCP как неструктурированный поток байтов. Поступающие данные буферизуются средствами TCP. Для передачи на сетевой уровень из буфера «вырезается» некоторая непрерывная часть данных, которая и называется сегментом (см. рис. 5.23). В отличие от многих других протоколов, протокол TCP подтверждает получение не пакетов, а байтов потока.

Не все сегменты, посланные через соединение, будут одного и того же размера, однако оба участника соединения должны договориться о максимальном размере сегмента, который они будут использовать. Этот размер выбирается таким образом, чтобы при упаковке сегмента в IP-пакет он помещался туда целиком, то есть максимальный размер сегмента не должен превосходить максимального размера поля данных IP-пакета, В противном случае пришлось бы выполнять фрагментацию, то есть делить сегмент на несколько частей, чтобы разместить его в IP-пакете,

Соединения

Для организации надежной передачи данных предусматривается установление логического **соединения** между двумя прикладными процессами. Поскольку соединения устанавливаются через ненадежную коммуникационную систему, основанную на протоколе IP, то во избежание ошибочной инициализации соединений используется специальная многошаговая процедура подтверждения связи.

Соединение в протоколе TCP идентифицируется парой полных адресов обоих взаимодействующих процессов - **сокетов**. Каждый из взаимодействующих процессов может участвовать в нескольких соединениях.

Формально соединение можно определить как набор параметров, характеризующий процедуру обмена данными между двумя процессами. Помимо полных адресов процессов этот набор включат и параметры, значения которых определяются в результате переговорного

процесса модулей TCP двух сторон соединения. К таким параметрам относятся, в частности, согласованные размеры сегментов, которые может посылать каждая из сторон, объемы данных, которые разрешено передавать без получения на них подтверждения, начальные и текущие номера передаваемых байтов. Некоторые из этих параметров остаются постоянными в течение всего сеанса связи, а некоторые адаптивно изменяются.

В рамках соединения осуществляется обязательное подтверждение правильности приема для всех переданных сообщений и при необходимости выполняется повторная передача. Соединение в TCP позволяет вести передачу данных одновременно в обе Стороны, то есть полнодуплексную передачу.

Реализация скользящего окна в протоколе TCP

В рамках установленного соединения правильность передачи каждого сегмента должна подтверждаться квитанцией получателя. **Квитирование** - это один из традиционных методов обеспечения надежной связи. В протоколе TCP используется **частный случай квитирования - алгоритм скользящего окна**. Идея этого алгоритма была изложена в главе 2, «Основы передачи дискретных данных».

Особенность использования алгоритма скользящего окна в протоколе TCP состоит в том, что, хотя единицей передаваемых данных является сегмент, окно определено на множестве нумерованных байтов неструктурированного потока данных, поступающих с верхнего уровня и буферизуемых протоколом TCP. Получающий модуль TCP отправляет «окно» посылающему модулю TCP. Данное окно задает количество байтов (начиная с номера байта, о котором уже была выслана квитанция), которое принимающий модуль TCP готов в настоящий момент принять.

Квитанция (подтверждение) посылается только в случае правильного приема данных, отрицательные квитанции не посылаются. Таким образом, отсутствие квитанции означает либо прием искаженного сегмента, либо потерю сегмента, либо потерю квитанции. В качестве квитанции получатель сегмента отсылает ответное сообщение (сегмент), в которое помещает число, на единицу превышающее максимальный номер байта в полученном сегменте. Это число часто называют номером очереди.

На рис. 5.24 показан поток байтов, поступающий на вход протокола TCP. Из потока байтов модуль TCP нарезает последовательность сегментов. Для определенности на рисунке принято направление перемещения данных справа налево. В этом потоке можно указать несколько логических границ. Первая граница отделяет сегменты, которые уже были отправлены и на которые уже пришли квитанции. Следующую часть потока составляют сегменты, которые также уже отправлены, так как входят в границы, определенные окном, но квитанции на них пока не получены. Третья часть потока - это сегменты, которые пока не отправлены, но могут быть отправлены, так как входят в пределы окна. И наконец, последняя граница указывает на начало последовательности сегментов, ни один из которых не может быть отправлен до тех пор, пока не придет очередная квитанция и окно не будет сдвинуто вправо.

Рис. 5.24. Особенности реализации алгоритма скользящего окна в протоколе TCP

Если размер окна равен W, а последняя по времени квитанция содержала значение N, то отправитель может посылать новые сегменты до тех пор, пока в очередной сегмент не попадет байт с номером N+W. Этот сегмент выходит за рамки окна, и передачу в таком случае необходимо приостановить до прихода следующей квитанции.

Надежность передачи достигается благодаря подтверждениям и номерам очереди. Концептуально каждому байту данных присваивается номер очереди. Номер очереди для первого байта данных в сегменте передается вместе с этим сегментом и называется номером очереди для сегмента. Сегменты также несут номер подтверждения, который является номером для следующего ожидаемого байта данных, передаваемого в обратном направлении. Когда протокол TCP передает сегмент с данными, он помещает его копию в очередь повторной передачи и запускает таймер. Когда приходит подтверждение для этих данных, соответствующий сегмент удаляется из очереди. Если подтверждение не приходит до истечения срока, то сегмент посылается повторно.

Выбор времени ожидания (тайм-аута) очередной квитанции является важной задачей, результат решения которой влияет на производительность протокола TCP. Тайм-аут не должен быть слишком коротким, чтобы по возможности исключить избыточные повторные передачи, которые снижают полезную пропускную способность системы. Но он не должен быть и слишком большим, чтобы избежать длительных простоев, связанных с ожиданием несуществующей или «заблудившейся» квитанции.

При выборе величины тайм-аута должны учитываться скорость и надежность физических линий связи, их протяженность и многие другие подобные факторы. В протоколе TCP тайм-аут определяется с помощью достаточно сложного адаптивного алгоритма, идея которого состоит в следующем. При каждой передаче засекается время от момента отправки сегмента до прихода квитанции о его приеме (время оборота). Получаемые значения времени оборота усредняются с весовыми коэффициентами, возрастающими от предыдущего замера к последующему. Это делается с тем, чтобы усилить влияние последних замеров. В качестве тайм-аута выбирается среднее время оборота, умноженное на некоторый коэффициент. Практика показывает, что значение этого коэффициента должно превышать 2. В сетях с большим разбросом времени оборота при выборе тайм-аута учитывается и дисперсия этой величины.

Поскольку каждый байт пронумерован, то каждый из них может быть опознан. Приемлемый механизм опознавания является накопительным, поэтому опознавание номера X означает, что все байты с предыдущими номерами уже получены. Этот механизм позволяет регистрировать появление дубликатов в условиях повторной передачи. Нумерация байтов в пределах сегмента осуществляется так, чтобы первый байт данных сразу вслед за заголовком имел наименьший номер, а следующие за ним байты имели номера по возрастающей.

Окно, посылаемое с каждым сегментом, определяет диапазон номеров очереди, которые отправитель окна (он же получатель данных) готов принять в настоящее время. Предполагается, что такой механизм связан с наличием в данный момент места в буфере данных.

Варьируя величину окна, можно влиять на загрузку сети. Чем больше окно, тем большую порцию неподтвержденных данных можно послать в сеть. Но если пришло большее количество данных, чем может быть принято программой TCP, данные будут отброшены. Это приведет к излишним пересылкам информации и ненужному увеличению нагрузки на сеть и программу TCP.

С другой стороны, указание окна малого размера может ограничить передачу данных скоростью, которая определяется временем путешествия по сети каждого посылаемого сегмента. Чтобы избежать применения малых окон, получателю данных предлагается откладывать изменение окна до тех пор, пока свободное место не составит 20-40 % от максимально возможного объема памяти для этого соединения. Но и отправителю не стоит спешить с посылкой данных, пока окно не станет достаточно большим. Учитывая эти соображения, разработчики протокола TCP предложили схему, согласно которой при установлении соединения заявляется большое окно, но впоследствии его размер существенно уменьшается.

Если сеть не справляется с нагрузкой, то возникают очереди в промежуточных узлах - маршрутизаторах и в конечных узлах-компьютерах.

При переполнении приемного буфера конечного узла «перегруженный» протокол TCP, отправляя квитанцию, помещает в нее новый, уменьшенный размер окна. Если он совсем отказывается от приема, то в квитанции указывается окно нулевого размера. Однако даже после этого приложение может послать сообщение на отказавшийся от приема порт. Для этого сообщение должно сопровождаться пометкой «срочно». В такой ситуации порт обязан принять сегмент, даже если для этого придется вытеснить из буфера уже находящиеся там данные. После приема квитанции с нулевым значением окна протокол-отправитель время от времени делает контрольные попытки продолжить обмен данными. Если протокол-приемник уже готов принимать информацию, то в ответ на контрольный 'запрос он посылает квитанцию с указанием ненулевого размера окна.

Другим проявлением перегрузки сети является переполнение буферов в маршрутизаторах. В таких случаях они могут централизованно изменить размер окна, посылая управляющие сообщения некоторым конечным узлам, что позволяет им дифференцированно управлять интенсивностью потока данных в разных частях сети.

Дистанционно-векторный протокол RIP

Построение таблицы маршрутизации

Рассмотрим процесс построения таблицы маршрутизации с помощью протокола RIP на примере составной сети, изображенной на рис. 5.26.

Этап 1 - создание минимальных таблиц

В этой сети имеется восемь IP-сетей, связанных четырьмя маршрутизаторами с идентификаторами: Ml, М2, М3 и М4. Маршрутизаторы, работающие по протоколу RIP, могут иметь идентификаторы, однако для работы протокола они не являются необходимыми. В RIP-сообщениях эти идентификаторы не передаются.

В исходном состоянии в каждом маршрутизаторе программным обеспечением стека TCP/IP автоматически создается минимальная таблица маршрутизации, в которой учитываются только непосредственно подсоединенные сети. На рисунке адреса портов маршрутизаторов в отличие от адресов сетей помещены в овалы.

Таблица 5.14 позволяет оценить примерный вид минимальной таблицы маршрутизации маршрутизатора Ml.

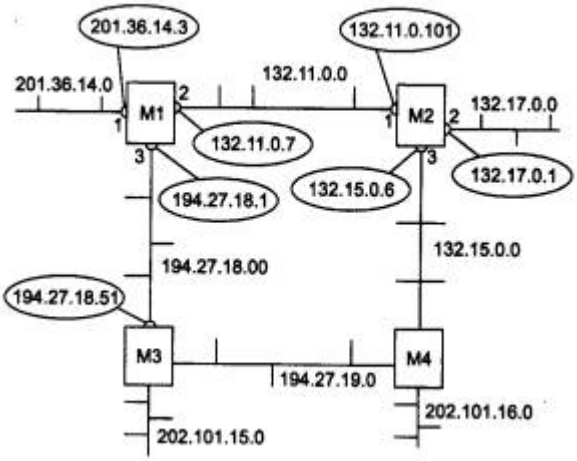


Рис. 5.26. Сеть, объединенная RIP-маршрутизаторами

Таблица 5.14. Минимальная таблица маршрутизации маршрутизатора 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

Минимальные таблицы маршрутизации в других маршрутизаторах будут выглядеть соответственно, например, таблица маршрутизатора М2 будет состоять из трех записей (табл. 5.15).

Таблица 5.15. Минимальная таблица маршрутизации маршрутизатора М2

Номер сети	Адрес следующего маршрутизатора	Порт	Расстояние
132.11.0.0	132.11.0.101	1	1
132.17.0.0	132.17.0.1	2	1
132.15.0.0	132.15.0.6	3	1

Этап 2 - рассылка минимальных таблиц соседям

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 и 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). Затем маршрутизатор начинает сравнивать новую информацию с той, которая хранится в его таблице маршрутизации (табл. 5.16).

Таблица 5.16. Таблица маршрутизации маршрутизатора 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
132.15.0.0	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~~	~~2~~
~~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, уже не минимальной, 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.

Посмотрим, как это делает маршрутизатор Ml (табл. 5.17).

Таблица 5.17. Таблица маршрутизации маршрутизатора 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
132.15.0.0	132.11.0.101	2	2
~~132.15.0.0~~	~~194.27.18.51~~	~~3~~	~~3~~
194.27.19.0	194.27.18.51	3	2
~~194.27.19.0~~	~~132.11.0.101~~	~~2~~	~~3~~
~~202.101.15.0~~	~~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~~

На этом этапе маршрутизатор Ml получил от маршрутизатора M3 информацию о сети 132.15.0.0, которую тот в свою очередь на предыдущем цикле работы получил от маршрутизатора M4. Маршрутизатор уже знает о сети 132.15.0.0, причем старая информация имеет лучшую метрику, чем новая, поэтому 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 M3 и M4. Поскольку метрики в этих сообщениях указаны одинаковые, то в таблицу попадают данные, которые пришли первыми. 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 маршругизации. 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, подобных той, которая образуется на рис. 5.26, маршрутизаторами М1-М2-М3-М4.

Очевидно, если в сети все маршрутизаторы, их интерфейсы и соединяющие их каналы связи постоянно работоспособны, то объявления по протоколу RIP можно делать достаточно редко, например, один раз в день. Однако в сетях постоянно происходят изменения - изменяется как работоспособность маршрутизаторов и каналов, так и сами маршрутизаторы и каналы могут добавляться в существующую сеть или же выводиться из ее состава.

Для адаптации к изменениям в сети протокол RIP использует ряд механизмов.

Адаптация RIP-маршрутизаторов к изменениям состояния сети

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-маршрутиза-торы 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 более 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, которые станут понятны из дальнейшего изложения. 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.

Как видно из объяснения, сведения о недоступных через отказавший маршрутизатор сетях распространяются по сети не очень быстро, время распространения кратно времени жизни записи, а коэффициент кратности равен количеству хопов между самыми дальними маршрутизаторами сети. В этом заключается одна из причин выбора в качестве периода рассылки небольшой величины в 30 секунд.

Если отказывает не маршрутизатор, а интерфейс или сеть, связывающие его с каким-либо соседом, то ситуация сводится к только что описанной - снова начинает работать механизм тайм-аута и ставшие недействительными маршруты постепенно будут вычеркнуты из таблиц всех маршрутизаторов сети.

Тайм-аут работает в тех случаях, когда маршрутизатор не может послать соседям сообщение об отказавшем маршруте, так как либо он сам неработоспособен, либо неработоспособна линия связи, по которой можно было бы передать сообщение.

Когда же сообщение послать можно, RIP-маршрутизаторы не используют специальный признак в сообщении, а указывают бесконечное расстояние до сети, причем в протоколе RIP оно выбрано равным 16 хопам (при другой метрике необходимо указать маршрутизатору ее значение, считающееся бесконечностью). Получив сообщение, в котором некоторая сеть сопровождается расстоянием 16 (или 15, что приводит к тому же результату, так как

маршрутизатор наращивает полученное значение на 1), маршрутизатор должен проверить, исходит ли эта «плохая» информация о сети от того же маршрутизатора, сообщение которого послужило в свое время основанием для записи о данной сети в таблице маршрутизации. Если это тот же маршрутизатор, то информация считается достоверной и маршрут помечается как недоступный.

Такое небольшое значение «бесконечного» расстояния вызвано тем, что в некоторых случаях отказы связей в сети вызывают длительные периоды некорректной работы RIP-маршрутизаторов, выражающейся в зацикливании пакетов в петлях сети. И чем меньше расстояние, используемое в качестве «бесконечного», тем такие периоды становятся короче.

Рассмотрим случай зацикливания пакетов на примере сети, изображенной на рис. 5.26.

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. 5.18).

Таблица 5.18. 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. 5.19).

Таблица 5.19. 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 (вернее, пока не была бы исчерпана разрядная сетка поля расстояния и не было бы зафиксировано переполнения при очередном наращивании расстояния).

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, например OSPF, 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. Искоренить эту причину полностью нельзя, ведь сам способ построения таблиц маршрутизации связан с передачей чужой информации без указания источника ее происхождения.

Не следует думать, что при любых отказах интерфейсов и маршрутизаторов в сетях возникают маршрутные петли. Если бы маршрутизатор Ml успел передать сообщение о недостижимости сети 201.36.14.0 раньше ложной информации маршрутизатора М2, то маршрутная петля не образовалась бы. Так что маршрутные петли даже без дополнительных методов борьбы с ними, описанными в следующем разделе, возникают в среднем не более чем в половине потенциально возможных случаев.

Методы борьбы с ложными маршрутами в протоколе RIP

Несмотря на то что протокол RIP не в состоянии полностью исключить переходные состояния в сети, когда некоторые маршрутизаторы пользуются устаревшей информацией об уже несуществующих маршрутах, 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. 5.26, 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. Предполагается, что 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 устаревшие сведения по сети.

5.4.3. Протокол «состояния связей» OSPF

Протокол OSPF (Open Shortest Path First, открытый протокол «кратчайший путь первыми) является достаточно современной реализацией алгоритма состояния связей (он принят в 1991 году) и обладает многими особенностями, ориентированными на применение в больших гетерогенных сетях.

В OSPF процесс построения таблицы маршрутизации разбивается на два крупных этапа. **На первом этапе** каждый маршрутизатор 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 Дийкстры. 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-маршрутиза-торы не используют обмен полной таблицей маршрутизации, как это не очень рационально делают MP-маршрутизаторы. Вместо этого они передают специальные короткие сообщения HELLO. Если состояние сети не меняется, то OSPF-мар-шрутизаторы 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. 5.27).

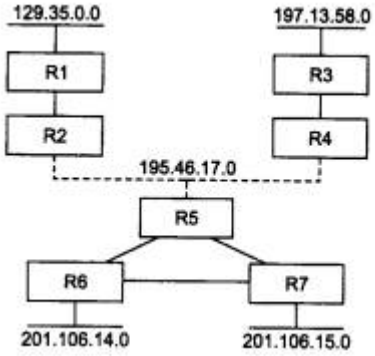


Рис. 5.27. Построение таблицы маршрутизации по протоколу OSPF

Маршрутизаторы соединены как с локальными сетями, так и непосредственно между собой глобальными каналами типа «точка-точка».

Данной сети соответствует граф, приведенный на рис. 5.28.

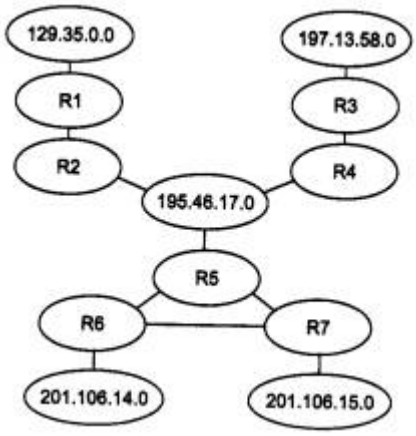


Рис. 5.28. Граф сети, построенный протоколом OSPF

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. При использовании хопов был бы выбран маршрут через R6, что не было бы оптимальным.

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.

Так как информация о некоторой связи изначально генерируется только тем маршрутизатором, который выяснил фактическое состояние этой связи путем тестирования с помощью сообщений HELLO, а остальные маршрутизаторы только ретранслируют эту информацию без преобразования, то недостоверная информация о достижимости сетей, которая может появляться в RIP-маршрутиэаторах, в OSPF-маршрутизаторах появиться не может, а устаревшая информация быстро заменяется новой, так как при изменении состояния связи новое сообщение генерируется сразу же.

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) (не нужно путать с автономной системой Internet). 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.

Дейтаграмма (У Семёнова - Дейтограмма) *см. файл Дейтаграмма-wiki.doc*

Материал из Википедии — свободной энциклопедии

Дейтаграмма (англ. datagram), также **датаграмма** — блок информации, посланный как **пакет сетевого уровня** через передающую среду без предварительного установления соединения и создания виртуального канала. Датаграмма представляет собой единицу информации в протоколе (protocol data unit, PDU) для обмена информацией на сетевом (в случае протокола IP, IP-датаграммы) и транспортном (в случае протокола UDP, UDP-датаграммы) уровнях эталонной модели OSI. Название «датаграмма» было выбрано по аналогии со словом телеграмма.

IP-датаграммы, IP-пакеты и IP-фрагменты

В современной практике термин «IP-пакет» обычно используется в качестве синонима к термину «IP-датаграмма». Вместе с тем в ряде документов IETF (RFC 1812, RFC 1547, RFC 1661 и др.) между ними проводится определенное различие. Как известно, модули данных верхних уровней сетевой модели последовательно инкапсулируются в модули данных нижележащих уровней (см. Инкапсуляция). При передаче на канальный уровень IP-датаграмма может не помещаться в модуль данных канального уровня. В таком случае для инкапсуляции требуется предварительная фрагментация датаграммы для удовлетворения требований конкретной технологии уровня среды передачи данных. Таким образом, возникает ещё один термин — IP-**фрагмент**. Термин IP-пакет обобщает понятия IP-датаграммы и IP-фрагмента, с тем существенным условием, что он обозначает модуль данных, передаваемый канальному уровню для инкапсуляции в кадр. Можно сказать, что на сетевом уровне IP-датаграмма является инкапсулирующим модулем данных, а IP-пакет — инкапсулируемым. В частном случае они могут совпадать, в общем случае — нет, так как IP-датаграмма может дробиться на фрагменты. Не всякая датаграмма, и даже не всякий фрагмент без дополнительной фрагментации может стать IP-пакетом.

Разведение понятий IP-датаграммы, IP-фрагмента и IP-пакета удобно для понимания процессов, происходящих на сетевом уровне. Вместе с тем следует иметь в виду, что общая структура сообщения с его заголовками и телом во всех трёх случаях одна и та же. Полные датаграммы и фрагменты датаграмм различаются только определенной информацией в заголовках. Пакет просто идентичен датаграмме или фрагменту, если они помещаются в кадр. Таким образом, необходимо помнить, что датаграммы, фрагменты и пакеты представляют собой разные единицы сетевого уровня не в структурном, а в функциональном плане.

Источник — «http://ru.wikipedia.org/wiki/%D0%94%D0%B5%D0%B9%D1%82%D0%B0%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0»

Материал из презентации

Уровень MAC (it_net_03.ppt)

- Основными функциями уровня MAC являются:
  - обеспечение доступа к разделяемой среде;
  - передача кадров между конечными узлами, используя функции и устройства физического уровня.

Адресация

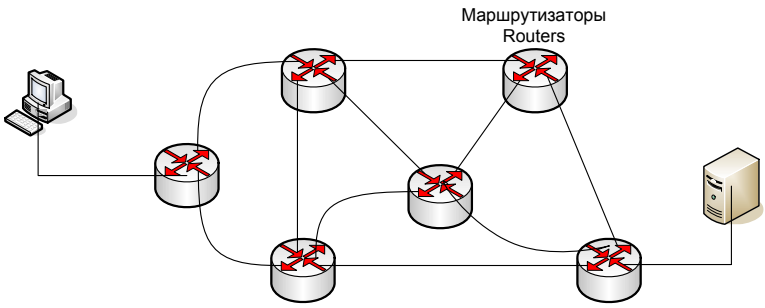
- Физические адреса (например, MAC-адресы в сетях Ethernet) используются на канальном уровне для взаимодействия к устройств, находящихся в том же сегменте сети.
- Для описания взаимодействия хостов между отдельными сегментами сети используется адресация на более высоком - **сетевом** - уровне.
- Поиск место размещения хостов и передача данных выполняется специальными устройствами – маршрутизаторами.

Примеры протоколов сетевого уровня

- Наиболее популярным протоколом сетевого уровня, используемым в Интернет, является протокол IP (Internet Protocol).
- Другим протоколом, используемым в локальных сетях, является протокол IPX (Internetwork Packet Exchange) фирмы Novell.
- Протокол NetBEUI является примером немаршрутизируемого протокола сетевого уровня.

Маршрутизаторы

- **Маршрутизаторы** – устройства обеспечивающие межсетевое взаимодействия и работающие на сетевом уровне модели OSI.
- Маршрутизатор обеспечивает сквозную маршрутизацию при прохождении пакетов данных перенаправления трафика на основании информации сетевого протокола.
- Маршрутизаторы позволяют решить проблему чрезмерного широковещательного трафика, поскольку они не переадресуют широковещательные кадры, если это не предписано.



Принцип работы маршрутизатора

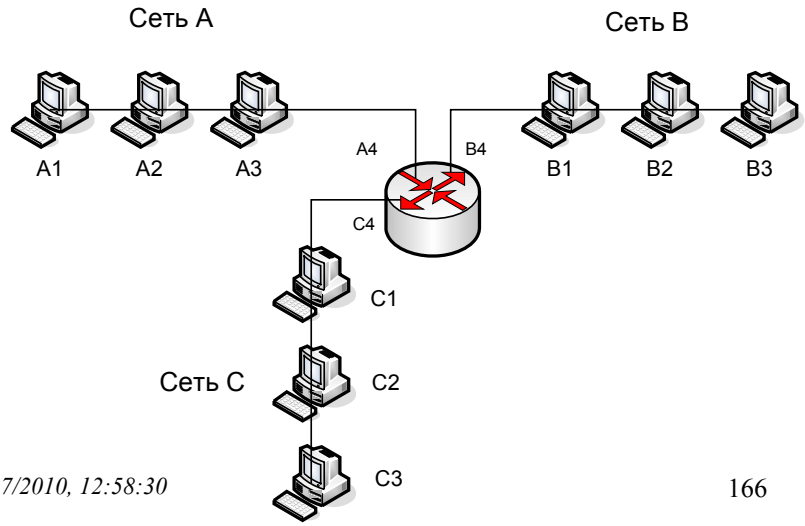
- Маршрутизатор использует сообщения третьего уровня для определения оптимального маршрута доставки данных в сети.

IP-адресация

- Для успешной маршрутизации пакетов данных используется иерархическая адресация - каждая сеть (подсеть) имела уникальный номер.
- Эти номера записываются в заголовках пакетов сетевого уровня и анализируются маршрутизаторами для передачи пакетов из сети в сеть.

IP-адресация

- IP-адрес устройства включает в себя **адрес сети**, к которой принадлежит устройство, и адрес устройства в этой сети.
- IP-адрес имеет иерархическую структуру и более удобен для организации адресов компьютеров, чем MAC-адреса.
- IP-адресация позволяет находить пункт назначения в сети Интернет. Для определения адреса используются двоичные значения.
  - Общая длина адреса составляет 32 бита (версия IPv4).



- Для записи IP-адреса как правило применяется десятичная нотация – адрес задается в виде 4 чисел разделенных точками, например, 192.168.160.224.

Протокол IP

- Протокол IP используется для управления рассылкой TCP/IP пакетов по сети Internet.
- Функции, возложенные на уровень IP :
  - определение пакета, который является базовым понятием и единицей передачи данных в сети Internet. Такой IP-пакет называют датаграммой;
  - определение адресной схемы, которая используется в сети Internet;
  - передача данных между канальным уровнем (уровнем доступа к сети) и транспортным уровнем (другими словами мультиплексирование транспортных датаграмм во фреймы канального уровня);
  - маршрутизация пакетов по сети, т.е. передача пакетов от одного шлюза к другому с целью передачи пакета машине-получателю;
  - "нарезка" и сборка из фрагментов пакетов транспортного уровня.

Особенности IP-протокола

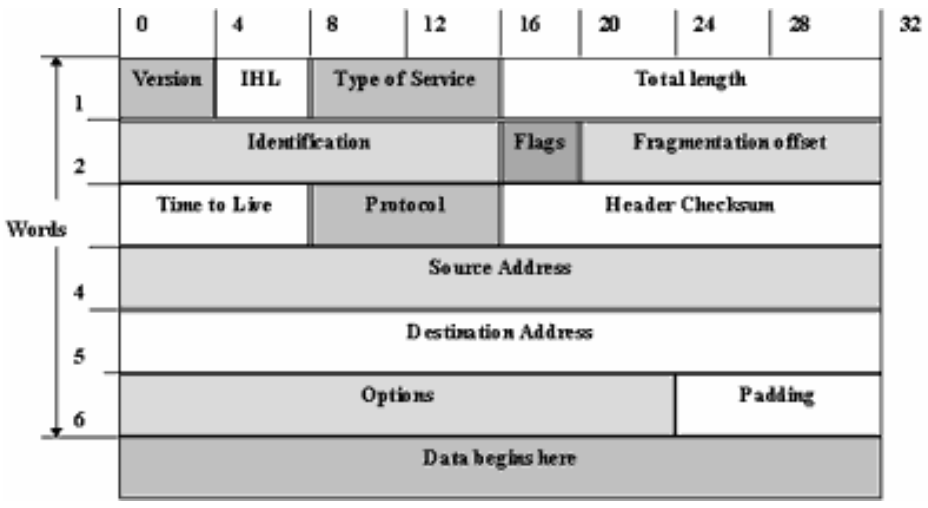
- Главными особенностями протокола IP является отсутствие ориентации на физическое или виртуальное соединение. Это значит, что прежде чем послать пакет в сеть, модуль операционной системы, реализующий IP, не проверяет возможность установки соединения, т.е. никакой управляющей информации кроме той, что содержится в самом IP-пакете, по сети не передается.
- IP не заботится о проверке целостности информации в поле данных пакета, что заставляет отнести его к протоколам ненадежной доставки. Целостность данных проверяется протоколами транспортного уровня (TCP) или протоколами приложений.
- Вся информация о пути, по которому должен пройти пакет берется из самой сети в момент прохождения пакета.
- Эта процедура и называется маршрутизацией в отличии от коммутации, которая используется для предварительного установления маршрута следования данных, по которому потом эти данные отправляют.

Маршрутизация и коммутация

- Принцип маршрутизации является одним из тех факторов, который обеспечил гибкость сети Internet.
- Маршрутизация является ресурсоемкой процедурой, так как требует анализа каждого пакета, который проходит через шлюз или маршрутизатор
- При коммутации анализируется только управляющая информация, устанавливается канал, физический или виртуальный, и все пакеты пересылаются по этому каналу без анализа маршрутной информации.
  - При неустойчивой работе сети пакеты могут пересылаться по различным маршрутам и затем собираться в единое сообщение.
  - При коммутации путь придется каждый раз вычислять заново для каждого пакета, а в этом случае коммутация потребует больше накладных затрат, чем маршрутизация.

Формат IP пакета

- В заголовке пакета определены:
  - адрес отправителя (4-ое слово заголовка),
  - адрес получателя (5-ое слово заголовка),
  - общая длина пакета (поле Total Lenght)
  - тип пересылаемой датаграммы (поле Protocol).
- Если IP-адрес получателя принадлежит одной из ее сетей, то на интерфейс этой сети пакет и будет отправлен, в противном случае пакет отправят на другой шлюз.



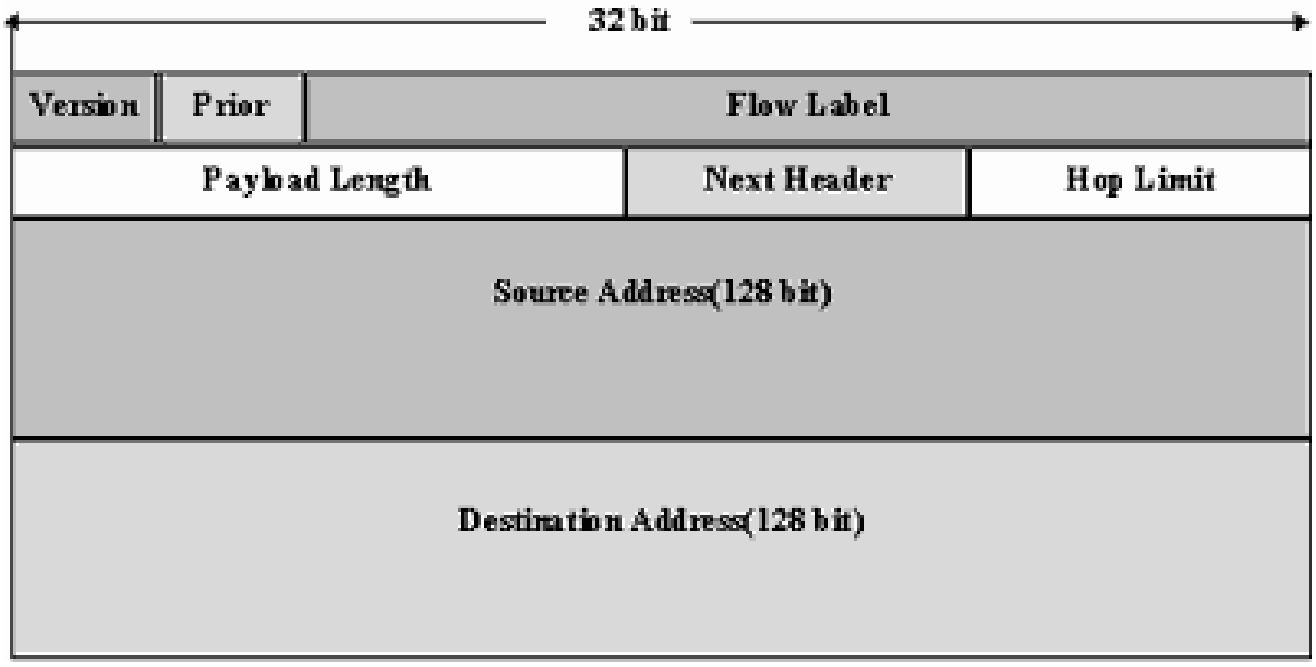
Транспортировка пакетов

- Зная протокол транспортного уровня, IP-модуль производит раскапсулирование информации из своего пакета и ее направление на модуль обслуживания соответствующего транспорта.
- При обычной процедуре инкапсулирования пакет просто помещается в поле данных фрейма, а в случае, когда это не может быть осуществлено, то разбивается на более мелкие фрагменты.
- Размер максимально возможного фрейма, который передается по сети, определяется величиной MTU (Maximum Transsion Unit), определенной для протокола канального уровня.
- Для того, чтобы потом восстановить пакет IP должен держать информацию о своем разбиении.
  - Для этой цели используется поля "flags" и "fragmentation offset". В этих полях определяется, какая часть пакета получена в данном фрейме, если этот пакет был фрагментирован на более мелкие части.

Стандарт IPv6

- В 1995 года IETF выпустило предложения по новому стандарту протокола IP – IPv6.
- В новом протоколе:
  - используются более длинные поля для адреса хоста,
  - введены новые типы адресов,
  - упрощена структура заголовка пакета,
  - введена идентификация типа информационных потоков для увеличения эффективности обмена данными,
  - введены поля идентификации и конфиденциальности информации.

Формат заголовка IPv6 пакета



- В заголовке поле **Version "версия"** - номер версии IP, равное 6.
- Поле **Prior "приоритет"** может принимать значения от 0 до 15. Первые 8 значений закреплены за пакетами, требующими контроля переполнения, например,
  - 0 - несимвольная информация;
  - 1 - информация заполнения (news),
  - 2 - не критичная ко времени передача данных (e-mail);
  - 4 - передача данных режима on-line (FTP, HTTP, NFS и т.п.);
  - 6 - интерактивный обмен данными (telnet, X);
  - 7 - системные данные или данные управления сетью (SNMP, RIP и т.п.).

Формат заголовка протокола

- Поле **Flow label "метка потока"** предполагается использовать для оптимизации маршрутизации пакетов.
  - В IPv6 вводится понятие потока, который состоит из пакетов. Пакеты потока имеют одинаковый адрес отправителя и одинаковый адрес получателя и ряд других одинаковых опций.
- Поле **Next Header "следующий заголовок"** определяет тип следующего за заголовком IP-заголовка.
- Поле **Hop Limit "ограничение переходов"** определяет число промежуточных шлюзов, которые ретранслируют пакет в сети.
  - При прохождении шлюза это число уменьшается на единицу. При достижении значения "0" пакет уничтожается.
- После первых 8 байтов в заголовке указываются адрес отправителя пакета и адрес получателя пакета. Каждый из этих адресов имеет длину 16 байт.
- Длина заголовка IPv6 составляет 48 байтов.

Адрес в протоколе IPv6

- Шестнадцать байт IP-адреса для IPv6 выглядят достаточными для удовлетворения любых потребностей Internet.
- Не все 2128 адресов можно использовать в качестве адреса сетевого интерфейса в сети.
- Предполагается выделение отдельных групп адресов, согласно специальным префиксам внутри IP-адреса, подобно тому, как это делалось при определении типов сетей в IPv4.
- Двоичный префикс "0000 010" предполагается закрепить за отображением IPX-адресов в IP-адреса.
- В новом стандарте выделяются несколько типов адресов:
  - **unicast addresses** - адреса сетевых интерфейсов,
  - **anycast addresses** - адреса не связанные с конкретным сетевым интерфейсом, но и не связанные с группой интерфейсов
  - **multicast addresses** - групповые адреса.
- Разница между последними двумя группами адресов в том, что anycast address это адрес конкретного получателя, но определяется адрес сетевого интерфейса только в локальной сети, где этот интерфейс подключен, а multicast-сообщение предназначено группе интерфейсов, которые имеют один multicast-адрес.

Маршрутизация и другие возможности

- В стандарт добавлены три новых возможности маршрутизации:
  - **маршрутизация поставщика IP-услуг,**
  - **маршрутизация мобильных узлов**
  - **автоматическая переадресация.**
- Эти функции реализуются путем прямого указания промежуточных адресов шлюзов при маршрутизации пакета. Эти списки помещаются в дополнительных заголовках, которые можно вставлять вслед за заголовком IP-пакета.
- Кроме перечисленных возможностей, новый протокол позволяет улучшить защиту IP-трафика. Для этой цели в протоколе предусмотрены специальные опции.
  - Первая опция предназначена для защиты от подмены IP-адресов машин. При ее использовании нужно кроме адреса подменять и содержимое поля идентификации, что усложняет задачу злоумышленника, который маскируется под другую машину.
- Вторая опция связана с шифрацией трафика.

Маршрутизация [5] (см. it_net_05_Маршрутизация.ppt)

- Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами.
- **Маршрутизатор** — это устройство, которое собирает информацию о топологии межсетевых соединений и пересылает пакеты сетевого уровня в сеть назначения. Чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач между сетями, или **хопов** (от слова hop — прыжок), каждый раз выбирая подходящий маршрут. Таким образом, **маршрут** представляет собой последовательность маршрутизаторов, через которые проходит пакет.
- Сетевой уровень должен обеспечить доставку пакета:
  - между любыми двумя узлами сети с произвольной топологией;
  - между любыми двумя сетями в составной сети;

- **Сеть** — совокупность компьютеров, использующих для обмена данными единую сетевую технологию;
- **Маршрут** — последовательность прохождения пакетом маршрутизаторов в составной сети.]

Задачи маршрутизации

- Проблема выбора наилучшего пути называется маршрутизацией, и ее решение является одной из главных задач **сетевого уровня**.
- Эта проблема осложняется тем, что **самый короткий путь — не всегда самый лучший**.
- Критерием при выборе **маршрута** может служить время передачи данных:
  - Время зависит от пропускной способности каналов связи и интенсивности трафика, которая может с течением времени изменяться.
- Выбор **маршрута** может осуществляться и по другим критериям, таким как **надежность** передачи.
- Функции **сетевого уровня** шире, чем функции передачи сообщений по связям с нестандартной структурой, которые мы рассмотрели на примере объединения нескольких локальных сетей.
- **Сетевой уровень** также решает задачи согласования разных технологий, упрощения **адресации** в крупных сетях и создания надежных и гибких барьеров на пути нежелательного трафика между сетями.

Протоколы маршрутизации

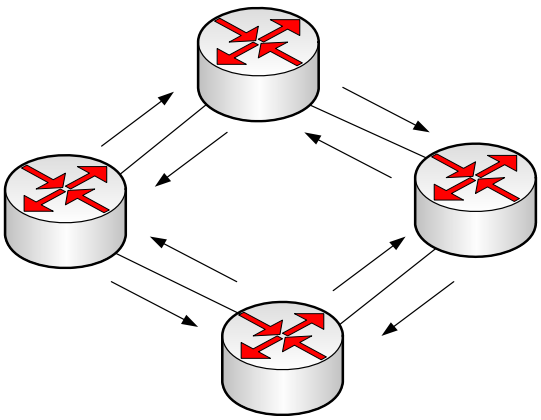
- Протокол маршрутизации – поддерживает маршрутизируемый протокол за счет предоставления механизмов коллективного использования маршрутной информации.
- Сообщения протокола маршрутизации циркулируют между маршрутизаторами для обмена информации и атуализации данных таблиц маршрутизации.
- Примеры протоколов маршрутизации:
  - RIP – протокол маршрутной информации;
  - IGRP – протокол внутренней маршрутизации между шлюзами;
  - EIGR – усовершенствованный протокол внутренней маршрутизации между шлюзами;
  - OSPF – протокол маршрутизации с выбором кратчайшего пути.

Алгоритмы маршрутизации

- Большинство алгоритмов маршрутизации можно свести к трем основным:
  - Маршрутизация на основе вектора расстояния – определяется направление (вектор) и расстояние до каждого канала в сети;
  - Маршрутизация на основе оценки состояния канала (выбор на основе кратчайшего пути), при которой воссоздается точная топология всей сети (по крайней мере, где размещается маршрутизатор);
  - Гибридный подход, объединяющий вышеуказанные алгоритмы.

Алгоритмы маршрутизации по вектору расстояния

- Алгоритмы маршрутизации на основе вектора расстояния (алгоритмы Беллмана-Форда) предусматривают периодическую передачу копий таблицы маршрутизации от одного маршрутизатора другому.
  - Такие передачи позволяют актуализировать изменения в топологии сети.
- Каждый маршрутизатор получает информацию от соседнего маршрутизатора.
- При добавлении информации в таблицу маршрутизации добавляется величина, отражающая вектор расстояния (например, число переходов) и далее информация передается следующему маршрутизатору.



Алгоритм маршрутизации по вектору расстояния и исследованию сети

- В данных алгоритмах каждый маршрутизатор начинает с идентификации или исследования своих соседей.
  - Порт к каждой непосредственно подключенной сети имеет нулевое расстояние.

- Продолжая процесс исследования векторов расстояния в сети, маршрутизаторы открывают наилучший путь до сети пункта назначения на основе информации от каждого соседа.
- Каждая запись в талице маршрутизации имеет коммулятивное значение вектора расстояния, показывающая насколько далеко данная сеть находится в этом направлении.

Алгоритм маршрутизации по вектору расстояния и изменение топологии

- При изменении топологии сети, использующей протокол на основе вектора расстояния, таблицы маршрутизации должны быть обновлены.
- Обновление содержания таблиц маршрутизации выполняется шаг за шагом от одного маршрутизатора к другому.
- Алгоритмы с вектором расстояния заставляют каждый маршрутизатор отсылать всю таблицу маршрутизации каждому своему непосредственному соседу.
- Таблицы маршрутизации, генерируемые в рамках метода вектора расстояния, содержат информацию об общей стоимости пути (метрика) и логический адрес маршрутизатора, стоящего на пути к каждой известной ему сети.

Маршрутизация с учетом состояния канала связи

- Алгоритмы маршрутизации с учетом канала связи также называются **алгоритмы выбора первого кратчайшего пути (shortest path first, SPF)**.
  - Алгоритмы направлены на поддержку базы данных о топологии информационных потоков.
- Для выполнения маршрутизации по данному алгоритму используются специальные сообщения объявлений о состоянии канала (link state advertisements, LSA), база данных топологии, SPF-алгоритм, результирующее SPS-дерево и таблица маршрутизации, содержащая пути и порты к каждой сети.

Режим исследования сети

- В режиме исследования сети при маршрутизации с учетом состояния канала связи используется следующий подход:
  - Маршрутизаторы обмениваются LSA-сообщениями, начиная с непосредственно подключенных маршрутизаторов;
  - Маршрутизаторы параллельно друг с другом топологическую базу данных, содержащую все LSA-сообщения;
  - SPF-алгоритм вычисляет достижимость сетей, определяя кратчайший путь до каждой сети комплекса. Маршрутизатор создает эту логическую топологию кратчайших путей в виде SPF-дерева, помещая себя в корень. Это дерево отображает пути от маршрутизатора до всех пунктов назначения.
  - Наилучшие пути и порты, имеющие выход на эти сети назначения, сводятся в таблицы маршрутизации. Также формируется базы данных с топологическими элементами и подробностями о статусе.

Обработка изменений топологии в протоколах маршрутизации

- Алгоритмы учета состояния канала связи полагаются на маршрутизаторы, имеющие общее представление о сети.
- Для достижения сходимости каждый маршрутизатор выполняет:
  - Отслеживает своих соседей: имя, рабочее состояние и стоимость линии связи;
  - Создает LSA-пакетов, в котором приводится перечень имен соседних маршрутизаторов и стоимость линий связи, а также данные о новых соседях и об изменениях в стоимости линий;
  - Посылает LSA-пакет на другие маршрутизаторы;
  - Получая LSA-пакет, записывает его в базу данных;
  - Используя накопленные данные LSA-пакетов для создания полной карты топологии сети, маршрутизатор запускает на исполнение SPF-алгоритм и рассчитывает оптимальные маршруты до каждой сети.

Сравнение методов маршрутизации

- Процесс маршрутизации по вектору расстояния получает топологические данные из таблиц маршрутизации соседних маршрутизаторов.
  - Процесс маршрутизации SPF позволяет получить широкое представление обо всей топологии сетевого комплекса, собирая данные из всех LSA-пакетов;

- Процесс маршрутизации по вектору расстояния определяет лучший путь с помощью сложения метрик по мере того как таблица движется от одного маршрутизатора к другому.
  - При использовании маршрутизации SPF каждый маршрутизатор работает отдельно, вычисляя свой собственный оптимальный путь;
- В большинстве протоколов маршрутизации по вектору расстояния пакеты актуализации, содержащие сведения об изменениях топологии, - периодически посылаемые пакеты актуализации таблиц.
  - Эти таблицы передаются от одного маршрутизатора к другому, что приводит к медленной сходимости;
- В протоколах маршрутизации SPF пакеты актуализации генерируются и рассылаются по факту возникновения изменения топологии.
  - Относительно небольшие LSA-пакеты передаются всем маршрутизаторам, что приводит к более быстрой сходимости при любом изменении топологии сети.

Поддержка параметров QoS (it_net_03.ppt)

Для каждого виртуального соединения определяется несколько параметров, связанных со скоростью передачи данных и влияющих на качество обслуживания.

- **Согласованная скорость передачи данных** (Committed Information Rate, CIR) — скорость, с которой сеть будет передавать данные пользователя.
- **Согласованная величина пульсации** (Committed Burst Size, Bc) — максимальное количество байтов, которое сеть будет передавать от данного пользователя за интервал времени T, называемый временем пульсации, соблюдая согласованную скорость CIR.
- **Дополнительная величина пульсации** (Excess Burst Size, Be) — максимальное количество байтов, которое сеть будет пытаться передать сверх установленного значения Bc за интервал времени T.

Техника виртуальных каналов (it_net_03.ppt. см. it_net_03_Техника виртуальных каналов.ppt)

MPLS

Из. 4.4.17 Введение в MPLS, TE и QoS.doc

Именно идея сохранения в маршрутной таблице только реально используемых виртуальных путей и легла в основу разработки протокола MPLS и сопряженных с ним протоколов маршрутизации. См. 4.4.17 Введение в MPLS, TE и QoS.doc стр. 1

Если рассмотреть ситуацию на уровне L2, здесь имеется сильная зависимость от физического уровня (L1). В сетях с маркерным доступом (Token Ring или FDDI, см. book.itep.ru) существуют механизмы управления приоритетом и способы контроля доступа, гарантирующие определенное значение задержек сетевого отклика. В сетях ISDN и в особенности в ATM предусмотрен целый арсенал средств управления, работающих на фазе установления виртуального канала (процедура SETUP). Для Ethernet до последнего времени ситуация была много хуже. Здесь только некоторые переключатели поддерживают VLAN. Технология виртуальных сетей L2 позволяет сформировать в локальной сети соединение точка-точка. В таком соединении можно гарантировать пропускную способность на уровне 10/100Мбит/с. К сожалению VLAN L2 создаются и модифицируются, как правило администратором, но можно эту проблему перепоручить сценарию, например, на PERL, работающему с демоном SNMP сетевого прибора. В такой сети можно также гарантировать низкий уровень разброса времени реакции сети. Если сформировать VLAN с числом узлов (N) больше двух, можно гарантировать полосу лишь не ниже (10/100)/N. Для произвольной сети Ethernet никаких гарантий на уровне L2 предоставить нельзя. Здесь можно рассчитывать только на вышележащие уровни (IP/TCP/UDP).

Управление трафиком

В настоящее время используется несколько методов управления трафиком:

1. Динамическая маршрутизация (RIP, OSPF, IGRP, BGP) и т.д.). Здесь нет средства резервирования полосы, но имеется механизм изменения маршрута при изменении значений метрики или из-за выхода из строя узла или обрыва канала. Некоторые из таких протоколов (OSPF, IGRP) могут строить отдельные таблицы маршрутизации для каждого уровня TOS/QOS [1], но метрики для каждого уровня задаются сетевым администратором. Здесь имеется возможность запараллеливания потоков с целью увеличения пропускной способности. Эти протоколы работают только в пределах одной автономной системы (AS). Протокол же BGP, используемый для прокладки путей между автономными системами не способен как-либо учитывать уровень TOS/QOS (использует алгоритм вектора расстояния, что связано с трудностью согласования значений метрик состояния канала администраторами разных AS). Новая версия многопротокольного расширения MP-BGP специально создана для совместной работы с MPLS при формировании виртуальных сетей, но и он безразличен к TOS/QOS.
2. Формирование виртуальных сетей на уровнях L2 и L3. Протоколы VLAN обеспечивают повышенный уровень безопасности, но не способны резервировать полосу. К этому типу относится и протокол MPLS.
3. Резервирование полосы в имеющемся виртуальном канале (протокол RSVP). RSVP может работать с протоколами IPv4 и IPv6. Протокол достаточно сложен для параметризации, по этой причине для решения этой задачи был разработан протокол COPS, который существенно облегчает параметризацию. Функция COPS сходна с задачей языка RPSL для маршрутизации.
4. Автоматическое резервирование полосы при формировании виртуального канала процедурой SETUP в сетях ATM, ISDN, DQDB, Frame Relay и т.д. Управление очередями осуществляется аппаратно, но базовые параметры могут задаваться программно. Программы управления трафиком MPLS позволяют расширяют возможности L2 сетей ATM и Frame Relay.
5. Использование приоритетов в рамках протокола IPv6. Возможность присвоения потокам меток облегчает, например, разделение аудио- и видеоданных.
6. Управление перегрузкой (окно перегрузки в TCP, ICMP(4) для UDP-потоков (ICMP L2 и т.д.).

Качество обслуживания QoS

QoS связана с возможностью сети предоставить клиенту необходимый ему уровень услуг в условиях работы поверх сетей с самыми разнообразными технологиями, включая Frame Relay, ATM, Ethernet, сети 802.1, SONET, и маршрутизуемые IP-сети.

QoS представляет собой собрание технологий, которые позволяют приложениям запрашивать и получать предсказуемый уровень услуг с точки зрения

- пропускной способности,

- временного разброса задержки отклика,
- а также общей задержки доставки данных.

В частности, QoS подразумевает улучшение параметров или достижение большей предсказуемости предоставляемых услуг. Это достигается следующими методами:

- Поддержкой определенной полосы пропускания.
- Сокращением вероятности потери кадров.
- Исключением или управляемостью сетевых перегрузок.
- Возможностью конфигурирования сетевого трафика.
- Установкой количественных характеристик трафика по пути через сеть.

IEFT определяет для QoS следующие две архитектуры:

- Интегрированные услуги (IntServ)
- Дифференцированные услуги (DiffServ)

IntServ для явного задания уровня услуги (QoS) использует протокол RSVP. Это делается путем уведомления об этом требовании всех узлов вдоль пути обмена. Если все сетевые устройства вдоль пути могут предоставить запрошенную полосу, резервирование завершается успешно (смотри документ RFC-1633 [2]).

DiffServ, вместо того чтобы уведомлять о требованиях приложения, использует в IP-заголовке DiffServ Code Point (DSCP), чтобы указать требуемые уровни QoS. Cisco IOS® Software Release 12.1(5)T вводит совместимость маршрутизаторов Cisco с DiffServ (см. [15-16]). DSCP размещается в поле TOS IP-пакета.

L2 QoS предполагает следующее:

1. **Управление входными очередями**: когда кадр приходит на вход порта, он может быть отнесен к одной из нескольких очередей, ассоциированных с портом, прежде чем он будет направлен на один из выходных портов. Обычно, несколько очередей используются тогда, когда различные информационные потоки требуют различных уровней услуг или минимизации задержки. Например, IP мультимедиа требует минимизации задержки, в отличие от передачи данных в FTP, WWW, email, Telnet, и т.д. **Классификация:** процесс классификации включает просмотр различных полей в заголовке Ethernet L2, а также полей IP-заголовка (уровень 3 - L3) и заголовков TCP/UDP (уровень 4 - L4), чтобы обеспечить определенный уровень услуг при коммутации пакетов.
2. **Политика:** осуществление политики является процессом анализа кадра Ethernet, чтобы определить, не будет ли превышен заданный уровень трафика за определенный интервал времени (обычно, это время является внутренним параметром переключателя). Если кадр создает ситуацию, при которой трафик превысит заданный уровень, он будет отброшен. Или значение CoS (Class of Service) может быть понижено.
3. **Перезапись:** процесс перезаписи предоставляет возможность переключателю модифицировать CoS в заголовке или ToS (Type of Service) в IPv4-заголовке. Следует учесть, что заголовок Ethernet 802.3 поля CoS не имеет (именно эта версия стандарта наиболее распространена в РФ).
4. **Управление выходными очередями:** после процесса перезаписи переключатель поместит кадр Ethernet, в выходную очередь для последующей коммутации. Переключатель выполнит управление буфером так, чтобы не произошло переполнение. Это обычно осуществляется с помощью алгоритма RED (Random Early Discard), когда некоторые кадры случайным образом удаляются из очереди. Weighted RE (WRED) является директивой RED (используемой некоторыми модулями семейства Catalyst 6000), где значения CoS анализируются с целью определения того, какие кадры следует отбросить. Когда буферы окажутся заполнены до определенного уровня, кадры с низким уровнем приоритета отбрасываются, в очереди сохраняются только высокоприоритетные кадры.

Протокол MPLS хорошо приспособлен для формирования виртуальных сетей (VPN) ***повышенного быстродействия*** (метки коммутируются быстрее, чем маршрутизируются пакеты). Принципиальной основой MPLS являются IP-туннели. Для его работы нужна поддержка протокола маршрутизации MP-BGP (RFC-2858 [23]). Протокол MPLS может работать практически для любого маршрутизируемого транспортного протокола (не только IP). После того как сеть сконфигурирована (для этого используются специальные, поставляемые производителем скрипты), сеть существует, даже если в данный момент через нее не осуществляется ни одна сессия. При появлении пакета в виртуальной сети ему присваивается метка, которая не позволяет ему покинуть пределы данной виртуальной сети. Никаких других ограничений протокол MPLS не накладывает. Протокол MPLS предоставляет возможность обеспечения значения QoS, гарантирующего более высокую безопасность. Не следует переоценивать уровня безопасности, гарантируемого MPLS, атаки типа “человек посередине” могут быть достаточно разрушительны. При этом для одного и того же набора узлов можно

сформировать несколько разных виртуальных сетей (используя разные метки), например, для разных видов QoS.

Для обеспечения структурирования потоков в пакете создается стек меток, каждая из которых имеет свою зону действия. Формат стека меток представлен на рис. 3 (смотри RFC-3032). В норме стек меток размещается между заголовками сетевого и канального уровней (соответственно L2 и L3). Каждая запись в стеке занимает 4 октета.

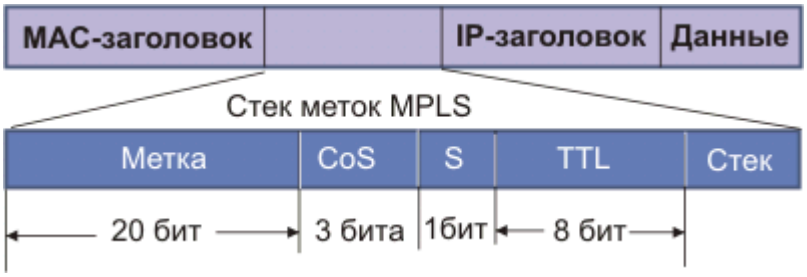
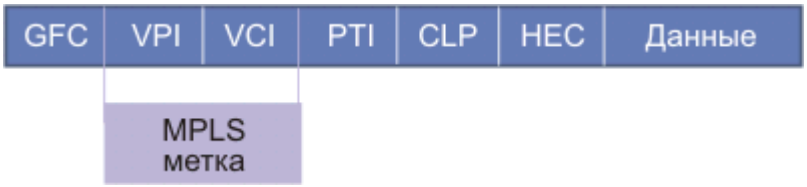


Рис. 3. Формат стека меток

Рис. 3а. Размещение меток в стеке

Место заголовка MAC может занимать заголовок PPP. В случае работы с сетями ATM метка может занимать поля VPI и VCI. Смотри рис 4. Глубина стека в данном случае не может превышать 1.



Управление коммутацией по меткам основывается на базе данных LIB (Label Information Base). Пограничный маршрутизатор MPLS LER (Label Edge Router) удаляет метки из пакетов, когда пакет покидает облако MPLS, и вводит их во входящие пакеты. Схема работы с помеченными и обычными IP-пакетами показана на рис. 5.

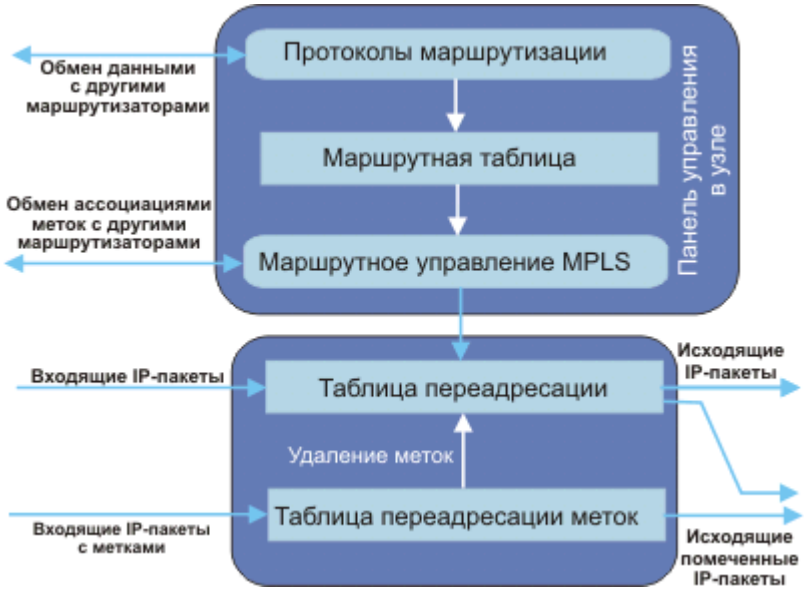


Рис. 5. Обработка помеченных и обычных IP-пакетов

Управление трафиком MPLS автоматически устанавливает и поддерживает туннель через опорную сеть, используя возможности RSVP. Путь, используемый данным туннелем в любой момент времени определяется на основе ресурсных требований и сетевых возможностей, таких как полоса пропускания. В самом ближайшем будущем MPLS сможет решать проблему обеспечения требуемого уровня QoS и самостоятельно.

Информация об имеющихся ресурсах доводится до сведения заинтересованных субъектов с помощью протокола IPG (Interior Protocol Gateway), алгоритм которого базируется на состоянии канала.

Путь туннеля вычисляется, основываясь на сформулированных требованиях и имеющихся ресурсах (constraint-based routing). IGP автоматически маршрутизирует трафик через эти туннели. Обычно, пакет, проходящий через опорную сеть MPLS движется по одному туннелю от его входной точки к выходной.

Управление **трафиком MPLS основано на следующих механизмах IOS:**

- **Туннелях** LSP (Label-switched path), которые формируются посредством RSVP, с расширениями системы управления трафиком. Туннели LSP представляют собой туннельные двунаправленные интерфейсы IOS с известным местом назначения.
- **Протоколах маршрутизации IGP,** базирующиеся на состоянии канала (такие как IS-IS) с расширениями для глобальной рассылки ресурсной информации, и расширениях для автоматической маршрутизации трафика по LSP туннелям.
- **Модуле вычисления пути MPLS**, который определяет пути для LSP туннелей.
- **Модуле управления трафиком MPLS**, который обеспечивает доступ и запись ресурсной информации, подлежащей рассылке.
- **Переадресации согласно меткам**, которая предоставляет маршрутизаторам возможности, сходные с уровнем L2, перенаправлять трафик через большое число узлов согласно алгоритму маршрутизации отправителя.

Выводы

1. Для сетей TCP/IP основным инструментом управления QoS пока является протокол RSVP (это касается и MPLS).
2. Протокол MPLS является удобным средством формирования корпоративных сетей (VPN), которые позволяют поднять их безопасность.
3. Для обеспечения работы MPLS необходима поддержка протоколов IS-IS и MP-BGP всеми маршрутизаторами VPN.
4. Протокол MPLS предоставляет гибкие средства мониторинга трафика в пределах VPN.
5. Технология управления трафиком TE предполагает совмещение возможностей протоколов уровней L2 и L3.
6. Протокольных средств управления очередями в Ethernet или в TCP/IP не существует. Такие средства имеются вATM-коммутаторах, ограниченные возможности имеются в некоторых маршрутизаторах CISCO и в коммутаторах L2 (например, выбор между режимами store-and-forward и cutthrough и т.д.). В любом случае такие режимы конфигурируются администратором индивидуально для каждого сетевого устройства. Разумеется, что-то можно сделать с помощью протокола SNMP дистанционно, если имеется пароль доступа (community).
7. **Переход на IPv6** существенно расширяет возможности управления трафиком за счет использования меток потоков (пока не ясно насколько эта возможность поддерживается программно). Данное свойство особенно важно для передачи мультимедийных данных, например, программ цифрового телевидения. Последнее предполагает значительное расширение интегральной полосы каналов опорной сети (хотя бы до 155Мбит/с).
8. Все выше сказанное отражает ситуацию сегодняшнего дня, когда не стандартизовано дополнительных средств управления трафиком и QoS. Положение может измениться, если будут, например, стандартизованы какие-то дополнительные атрибуты потоков (как это было сделано при введении меток для VPN). Такие работы уже ведутся (см. [3])
9. Возможности, заложенные в протоколе MPLS, предполагают определенный уровень сотрудничества между администраторами узлов, образующих VPN.

IP-туннели см. 4.4.1.2 IP-туннели.doc.

Особенность IP-протокола (опция принудительной маршрутизации) позволяет переадресовывать IP-дейтограммы определенным узлам сети. На первый взгляд эта возможность может показаться совершенно бесполезной, ведь существуют механизмы динамической маршрутизации, которые несравненно эффективнее и надежней обеспечивают обмен данными. Но тем не менее существуют приложения, где принудительная маршрутизация на IP-уровне представляет возможности недоступные для традиционных решений. Это прежде всего сети, работающие с использованием протоколов IPX/SPX (Novell), где традиционная маршрутизация не предусмотрена. Для подключений удаленных серверов, находящихся вне локальной сети, здесь используется технология так называемых IP-туннелей. При реализации этой технологии IPX-пакеты инкапсулируются в IP-дейтограммы и доставляются в соответствие с протоколами TCP/IP. Процедура инкапсуляции осуществляется специальным драйвером (IPtunnel; использует протокол IPxodi), который работает так, как если бы он был драйвером аппаратного сетевого интерфейса. При этом необходимо модифицировать конфигурационный файл net.cfg.

Протокол PPP Олифер гл.6 п. 6.2.3.

протокол «точка-точкам», Point-to-Point Protocol, PPP.

Этот протокол разработан группой IETF (Internet Engineering Task Force) как часть стека TCP/IP для передачи кадров информации по последовательным глобальным каналам связи взамен устаревшего протокола SLIP (Serial Line IP). Протокол PPP стал фактическим стандартом для глобальных линий связи при соединении удаленных клиентов с серверами и для образования соединений между маршрутизаторами в корпоративной сети. При разработке протокола PPP за основу был взят формат кадров HDLC и дополнен собственными полями. Поля протокола PPP вложены в поле данных кадра HDLC. Позже были разработаны стандарты, использующие вложение кадра PPP в кадры frame relay и других протоколов глобальных сетей.

Основное отличие PPP от других протоколов канального уровня состоит в том, что он добивается согласованной работы различных устройств с помощью переговорной процедуры, во время которой передаются различные параметры, такие как качество линии, протокол аутентификации и инкапсулируемые протоколы сетевого уровня. Переговорная процедура происходит во время установления соединения.

Протокол PPP основан на четырех принципах:

- переговорное принятие параметров соединения,
- многопротокольная поддержка,
- расширяемость протокола,
- независимость от глобальных служб.

Переговорное принятие параметров соединения. В корпоративной сети конечные системы часто отличаются размерами буферов для временного хранения пакетов, ограничениями на размер пакета, списком поддерживаемых протоколов сетевого уровня. Физическая линия, связывающая конечные устройства, может варьироваться от низкоскоростной аналоговой линии до высокоскоростной цифровой линии с различными уровнями качества обслуживания.

Чтобы справиться со всеми возможными ситуациями, в протоколе PPP имеется набор стандартных установок, действующих по умолчанию и учитывающих все стандартные конфигурации. При установлении соединения два взаимодействующих устройства для нахождения взаимопонимания пытаются сначала использовать эти установки. Каждый конечный узел описывает свои возможности и требования. Затем на основании этой информации принимаются параметры соединения, устраивающие обе стороны, в которые входят форматы инкапсуляции данных, размеры пакетов, качество линии и процедура аутентификации.

Протокол, в соответствии с которым принимаются параметры соединения, называется **протоколом управления связью (Link Control Protocol, LCP**). Протокол, который позволяет конечным узлам договориться о том, какие сетевые протоколы будут передаваться в установленном соединении, называется **протоколом управления сетевым уровнем (Network Control Protocol, NCP)**. Внутри одного PPP - соединения могут передаваться потоки данных различных сетевых протоколов.

Одним из важных параметров PPP - соединения является режим аутентификации. Для целей аутентификации PPP предлагает по умолчанию протокол PAP (Password Authentication Protocol), передающий пароль по линии связи в открытом виде, или протокол CHAP (Challenge Handshake Authentication Protocol), не передающий пароль по линии связи и поэтому обеспечивающий большую безопасность сети. Пользователям также разрешается добавлять и новые алгоритмы аутентификации. Дисциплина выбора алгоритмов компрессии заголовка и данных аналогична.

Многопротокольная поддержка - способность протокола PPP поддерживать несколько протоколов сетевого уровня - обусловила распространение PPP как стандарта де-факто. В отличие от протокола SLIP, который может переносить только IP-пакеты, или LAP-B, который может переносить только пакеты X.25, PPP работает со многими протоколами сетевого уровня, включая IP, Novell IPX, AppleTalk, DECnet, XNS, Banyan VINES и OSI, а также протоколами канального уровня локальной сети. Каждый протокол сетевого уровня конфигурируется отдельно с помощью соответствующего протокола NCP. Под конфигурированием понимается, во-первых, констатация того факта, что данный протокол будет использоваться в текущей сессии PPP, а во-вторых, переговорное утверждение некоторых параметров протокола. Больше всего параметров устанавливается для протокола IP - IP-адрес узла, IP-адрес серверов DNS, использование компрессии заголовка IP-пакета и т. д. Протоколы конфигурирования параметров соответствующего протокола верхнего уровня называются по имени этого протокола с добавлением аббревиатуры CP (Control Protocol), например протокол IPCP, IPXCP и т. п.

Расширяемость протокола. Под расширяемостью понимается как возможность включения новых протоколов в стек PPP, так и возможность использования собственных протоколов

пользователей вместо рекомендуемых в PPP по умолчанию. Это позволяет наилучшим образом настроить PPP для каждой конкретной ситуации.

Независимость от глобальных служб. Начальная версия PPP работала только с кадрами HDLC. Теперь в стек PPP добавлены спецификации, позволяющие использовать PPP в любой технологии глобальных сетей, например ISDN, frame relay, X.25, Sonet и HDLC.

Переговорная процедура протоколов LCP и NCP может и не завершиться соглашением о каком-нибудь параметре. Если, например, один узел предлагает в качестве MTU значение 1000 байт, а другой отвергает это предложение и в свою очередь предлагает значение 1500 байт, которое отвергается первым узлом, то по истечении тайм-аута переговорная процедура может закончиться безрезультатно.

Возникает вопрос - каким образом два устройства, ведущих переговоры по протоколу PPP, узнают о тех параметрах, которые они предлагают своему партнеру? Обычно у реализации протокола PPP есть некоторый набор параметров по умолчанию, которые и используются в переговорах. Тем не менее каждое устройство (и программа, реализующая протокол PPP в операционной системе компьютера) позволяет администратору изменить параметры по умолчанию, а также задать параметры, которые не входят в стандартный набор. Например, IP-адрес для удаленного узла отсутствует в параметрах по умолчанию, но администратор может задать его для сервера удаленного доступа, после чего сервер будет предлагать его удаленному узлу.

Хотя протокол PPP и работает с кадром HDLC, но в нем отсутствуют процедуры контроля кадров и управления потоком протокола HDLC. Поэтому в PPP используется только один тип кадра HDLC - ненумерованный информационный. В поле управления такого кадра всегда содержится величина 03. Для исправления очень редких ошибок, возникающих в канале, необходимы протоколы верхних уровней - TCP, SPX, NetBUEl, NCP и т. п.

Одной из возможностей протокола PPP является использование нескольких физических линий для образования одного логического канала, так называемый транкинг каналов. Эту возможность реализует дополнительный протокол, который носит название MLPPP (Multi Link PPP). Многие производители поддерживают такое свойство в своих маршрутизаторах и серверах удаленного доступа фирменным способом. Использование стандартного способа всегда лучше, так как он гарантирует совместимость оборудования разных производителей.

Общий логический канал может состоять из каналов разной физической природы. Например, один канал может быть образован в телефонной сети, а другой может являться виртуальным коммутируемым каналов сети frame relay.

Протокол PPP служит и для создания межсетевых туннелей (протокол PPTP - Point to Point Tunneling Protocol). Протокол PPTP использует MTU=1532, номер порта 5678 и номер версии 0x0100, пакеты данных здесь транспортируются с использованием протокола инкапсуляции GRE V2 (см. сноску в начале раздела). 3.5 Протокол PP.doc

Протоколы файлового обмена, электронной почты, дистанционного управления. Конференц-связь. Web-технологии

Наиболее подходящим для классификации сервисов Интернет является деление на сервисы интерактивные, прямые и отложенного чтения. Эти группы объединяют сервисы по большому числу признаков.

Сервисы, относящиеся к классу **отложенного чтения**, наиболее распространены, наиболее универсальны и наименее требовательны к ресурсам компьютеров и линиям связи. Основным признаком этой группы является та особенность, что запрос и получение информации могут быть достаточно сильно (что, вообще говоря, ограничивается только актуальностью информации на момент получения) разделены по времени. Сюда относится, например, электронная почта.

Сервисы прямого обращения характерны тем, что информация по запросу возвращается немедленно. Однако от получателя информации не требуется немедленной реакции. Сервисы, где требуется немедленная реакция на полученную информацию, т.е. получаемая информация является, по сути дела, запросом, относятся к интерактивным сервисам. Электронная почта (e-mail) - первый из сервисов Интернет, наиболее распространенный и эффективный из них. Электронная почта - типичный сервис отложенного чтения (off-line). Вы посылаете Ваше сообщение, как правило в виде обычного текста, адресат получает его на свой компьютер через какой-то, возможно достаточно длительный промежуток времени, и читает Ваше сообщение тогда, когда ему будет удобно. Сетевые новости Usenet, или, как их принято называть в российских сетях, телеконференции - это, пожалуй, второй по распространенности сервис Интернет. Если электронная почта передает сообщения по принципу "от одного - одному", то сетевые новости передают сообщения "от одного - многим". Механизм передачи каждого сообщения похож на передачу слухов: каждый узел сети, узнавший что-то новое (т.е. получивший новое сообщение), передает новость всем знакомым узлам, т.е. всем тем узлам, с кем он обменивается новостями. Таким образом, посланное Вами сообщение распространяется, многократно дублируясь, по сети, достигая за довольно короткие сроки всех участников телеконференций Usenet во всем мире. При этом в обсуждении интересующей Вас темы может участвовать множество людей, независимо от того, где они находятся физически, и Вы можете найти собеседников для обсуждения самых необычных тем.

Еще один широко распространенный сервис Интернет - FTP. Расшифровывается эта аббревиатура как протокол передачи файлов, но при рассмотрении FTP как сервиса Интернет имеется в виду не просто протокол, но именно сервис - доступ к файлам в файловых архивах. Вообще говоря, FTP - стандартная программа, работающая по протоколу TCP, обычно поставляющаяся с операционной системой. Ее исходное предназначение - передача файлов между разными компьютерами, работающими в сетях TCP/IP: на одном из компьютеров

работает программа-сервер, на втором пользователь запускает программу-клиента, которая соединяется с сервером и передает или получает по протоколу FTP файлы.

Широко распространены сервисы Интернет, обеспечивающие общение между пользователями в реальном времени через набор своих слов на клавиатуре, это, например, службы ICQ и IRC. В последнее время на каналах связи с большой пропускной способностью стали возможными **реальное голосовое общение и даже видеосвязь**. Помимо перечисленных существует ряд сервисов и протоколов для исполнения программ на удаленной машине, удаленного управления файлами и дисками, работы с распределенными базами данных и т.п. Гипертекстовая система Gopher - это распределенная система экспорта структурированной информации. При работе с gopher Вы находитесь в системе вложенных меню, из которых доступны файлы различных типов - как правило, простые тексты, но это может быть и графика, и звук и любые другие виды файлов. Gopher - сервис прямого доступа и требует, чтобы и сервер, и клиент были полноценно подключены к Интернет. WWW (World Wide Web - всемирная паутина) - самый популярный и интересный сервис Интернет сегодня, самое популярное и удобное средство работы с информацией. WWW работает по принципу клиент-сервер, точнее, клиент-серверы: существует множество серверов, которые по запросу клиента возвращают ему гипермедийный документ - документ, состоящий из частей с разнообразным представлением информации (текст, звук, графика, трехмерные объекты и т.д.), в котором каждый элемент может являться ссылкой на другой документ или его часть. Ссылки эти в документах WWW организованы таким образом, что каждый информационный ресурс в глобальной сети Интернет однозначно адресуется, и документ, который Вы читаете в данный момент, способен ссылаться как на другие документы на этом же сервере, так и на документы (и вообще на ресурсы Интернет) на других компьютерах Интернет. Причем пользователь не замечает этого, и работает со всем информационным пространством Интернет как с единым целым. Ссылки WWW указывают не только на документы, специфичные для самой WWW, но

и на прочие сервисы и информационные ресурсы Интернет. Более того, большинство программ-клиентов WWW (browsers, навигаторы) не просто понимают такие ссылки, но и являются программами-клиентами соответствующих сервисов: FTP, gopher, сетевых новостей Usenet, электронной почты и т.д. Таким образом, программные средства WWW являются универсальными для различных сервисов Интернет, а сама информационная система WWW играет интегрирующую роль.

Основные протоколы TCP/IP по уровням (список портов)

AODV • BGP • HTTP • DHCP • IRC • SNMP • DNS • NNTP • XMPP • SIP • BitTorrent • IPP • NTP • SNTP • RDP

Прикладной	***Электронная почта***	SMTP • POP3 • IMAP4
	Передача файлов	FTP • TFTP • SFTP
	Удалённый доступ	rlogin • Telnet
Представления	XDR • SSL	
Сеансовый	ADSP • H.245 • iSNS • L2F • **L2TP** • NetBIOS • PAP • RPC • PPTP • RTCP • SMPP • SCP • SSH • ZIP • SDP	
Транспортный	TCP • UDP • SCTP • DCCP • RTP • RUDP	
Сетевой	IPv4 • IPv6 • ICMP • IGMP • ARP • RARP • RIP2 • OSPF	
Канальный	Ethernet • 802.11 Wi-Fi • 802.16 WiMax • Token ring • ARCNET • FDDI • PPP • HDLC • SLIP • ATM • DTM • X.25 • Frame relay • SMDS	
Физический	Ethernet • RS-232 • EIA-422 • RS-449 • RS-485	

Библиография

[1] Rosen, E., Viswanathan, A., и R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[3] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, September 1981.

[4] Mogul, J. и S. Deering, "Path MTU Discovery", RFC 1191, November 1990.

[5] Katz, D., "IP Router Alert Option", RFC 2113, February 1997.

[6] Simpson, W., Editor, "The Point-to-Point Protocol (PPP)", STD 51, RFC1661, July 1994.

[7] Conta, A. и S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 1885, December 1995.

[8] McCann, J., Deering, S. и J. Mogul, "Path MTU Discovery for IP version 6", RFC 1981, August 1996.

[9] Davie, B., Lawrence, J., McCloghrie, K., Rekhter, Y., Rosen, E. и G. Swallow, "MPLS Using LDP и ATM VC Switching", RFC 3035, January 2001

ВОПРОСЫ 5 КУРСА

27. Сети на основе стека протоколов TCP/IP. История возникновения, структура стека протоколов и назначение различных элементов стека. Протоколы, порты, сокеты.
28. Структура адресного пространства в сетях TCP/IP для IPv4. Деление сетей на подсети. CIDR, VLSM.
29. Основные принципы работы маршрутизатора. Таблицы маршрутизации, форвардинг, типы маршрутов, фрагментация, MTU.
30. Особенности и отличия IPv6, обеспечение обратной совместимости с IPv4, новая функциональность и проблемы внедрения.
31. Доменная система имен.
32. Маршрутизация. Принципиальные подходы к решению проблемы маршрутизации для сетей различного размера. Distance vector и Link-state алгоритмы (концепция). IGP против EGP. Проблемы роста и подходы к их решению.
33. Протокол RIP. Особенности и проблемы, способы их решения. Ограничения применения и их анализ.
34. Протокол OSPF в сетях сложной структуры. Концепция областей и обмена маршрутами. Агрегирование.
35. Маршрутизация в рамках EGP. Протоколы BGP-3 и BGP-4. Атрибуты и их характеристики. Особенности и проблемы, присущие протоколам глобальной маршрутизации. Агрегирование, CIDR, VLSM.
36. Технологии MPLS/IP и EoMPLS, концепция Label Switching, применение MPLS для построения виртуальных частных сетей (MPLS/VPN), пересекающиеся адресные пространства.
37. Механизмы обеспечения качества обслуживания (QoS) в IPv4, различные подходы к обеспечению QoS в зависимости от задачи, алгоритмы обслуживания и предотвращения перегрузки сети.
38. Виртуальные частные сети как механизм туннелирования траффика, технологии PPTP и L2TP, особенности применения и отличительные особенности.
39. Построение защищенных каналов связи поверх IP с использованием технологии IPSEC, интеграция IPSEC в IPv6, использование IPSEC в IPv4. Протоколы IKE, ISAKMP, AH, ESP.
40. Передача голосового трафика поверх IP, протоколы SIP, RTP. Особенности алгоритмов компрессии голоса и проблемы транспортной инфраструктуры.
41. Технологии IP multicast для IPv4: взаимодействие с unicast-маршрутизацией, IGMP, PIM, RP.
42. Функционирование почтовой системы на основе SMTP/ESMTP, envelope и header адреса, различные технологии защиты от спама.
43. Обеспечение безопасности в сетях на основе IPv4 и IPv6. Проблемы и способы их решения.