Оглавление

1.Протокол LCC 802.2....2
2.Структура кадров LCC....3
3.Подуровень MAC....4
4.CSMA/CD....5
5.Распознавание коллизий....6
6.Производительности сети Ethernet....7
7.4 типа кадров канального уровня....9
8.Согласование различных типов кадров в сетях Ethernet....12
9.Стандарты Ethernet....13
Технология Fast Ethernet....13
100BASE — FX....13
100BASE — TX....13
100BASE — T4....13
10.Правила построения сегментов Fast Ethernet в случае использования повторителей....14
11.Коммутаторы локальной сети....16
12.Full-duplex. Протоколы локальной сети (коммутация кадров)....17
13.Оценка необходимой общей производительности коммутатора....18
14.Адресная таблица коммутатора....21
15.Объем буфера....23
16.Дополнительные возможности коммутатора....23
17.Структуризация локальной сети на базе коммутатора и основные определения....24
Технология Spanning-Tree....24
Основные поля пакета BPDU....25
18.Способы управления потоком кадров....27
19.Возможности коммутатора по фильтрации трафика....29
20.Использование различных классов сервисов....30
21.Поддержка виртуальных сетей....31
22.Технология Gigabit Ethernet....32
23.Технология 10 Gigabit Ethernet....33
24.Виртуальные сети....34
25.Создание виртуальных сетей....34
26.Управление коммутируемыми сетями....34
27.Управление виртуальными сетями....34
28.Сетевые адаптеры....34
29.Этапы приема из кабеля в компьютер....35
30.Классификация адаптеров....36
1-ое поколение....36
2-ое поколение....36
3-е поколение....36
4-ое поколение....36
31.Протокол 3-его уровня IPX....37
32.Формат пакета протокола IPX....38
33.Маршрутизация протокола IPX....39
34.Характеристика RIP и IPX (не закончил)....40
35.Методы управления и анализа локальных сетей....41
36.Архитектура систем управления локальных сетей....44
37.Системы управления системой....47

1. Протокол LCC 802.2

Logical Link Control (LCC) — подуровень управления логической связью — по стандарту IEEE 802 — верхний подуровень канального уровня модели OSI, осуществляет: управление передачей данных и обеспечивает проверку и правильность передачи информации по соединению. В основу протокола LCC положен протокол HDLC.

В соответствии со стандартом 802.2 уровень управления логическим каналом LCC предоставляет верхним уровням три типа процедур:

- LCC1 — сервис без установления соединения и без подтверждения
- LCC2 — сервис с установлением соединения и подтверждения
- LCC3 — сервис без установления соединения, но с подтверждением

LCC1 — дает пользователю средства для передачи данных с минимум издержек. Обычно, этот вид сервиса используется тогда, когда такие функции как восстановление данных после ошибок и упорядочивание данных выполняются протоколами вышележащих уровней, поэтому нет нужды дублировать их на уровне LCC.

LCC2 дает пользователю возможность установить логическое соединение перед началом передачи любого блока данных и, если это требуется, выполнить процедуры восстановления после ошибок и упорядочивание потока этих блоков в рамках установленного соединения. Протокол LCC2 во многом аналогичен протоколам семейства HDLC, которые применяются в глобальных сетях для обеспечения надежной передачи кадров на зашумленных линиях.

В некоторых случаях, когда временные издержки установления логического соединения перед отправкой данных неприемлемы, а подтверждение корректности приема переданных данных необходимо, базовый сервис без установления соединения и без подтверждения не подходит. Для таких случаев предусмотрен дополнительный сервис, сервис LCC3.

2. Структура кадров LCC

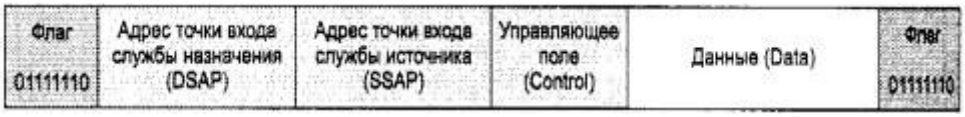
По своему назначению все кадры уровня LLC (называемые в стандарте 802.2 блоками данных — Protocol Data Unit, PDU) подразделяются на три типа — информационные, управляющие и ненумерованные.

Информационные кадры предназначены для передачи информации в процедурах с установлением логического соединения LCC2 и должны обязательно содержать поле информации. В процессе передачи информационных блоков осуществляется их нумерация в режиме скользящего окна.

Управляющие кадры предназначены для передачи команд и ответов в процедурах с установлением логического соединения LCC2, в том числе запросов на повторную передачу искаженных информационных блоков.

Ненумерованные кадры предназначены для передачи ненумерованных команд и ответов, выполняющих в процедурах без установления логического соединения передачу информации, идентификацию и тестирование LCC - уровня, а в процедурах с установлением логического соединения LCC2 — установление и разъединение логического соединения, а также информирование об ошибках.

Все типы кадров уровня LCC имеют единый формат:



Кадр LCC обрамляется двумя однобайтовыми полями «Флаг», имеющим значение 01111110. Флаги используются на уровне MAC для определения границ кадра LCC.

Кадр LCC содержит поле данных (46-1497 байт) и заголовок из трех полей: адрес точки входа службы назначения (DSAP), адрес точки входа службы источника (SSAP) и управляющее поле (Control). DSAP и SSAP занимают по 1 байту. Они позволяют указать, какая служба верхнего уровня пересылает данные с помощью этого кадра. Поле управления (1 или 2 байта) имеет сложную структуру при работе в режиме LLC2 и достаточно простую структуру при работе в режиме LCC1:

3. Подуровень MAC

Канальный уровень разделен на 2 подуровня: верхний подуровень логической передачи данных LLC (Logical Link Control), являющийся общим для всех технологий, и нижний подуровень управления доступом к среде MAC (Media Access Control).

Подуровень MAC определяет особенности доступа к физической среде при использовании различных технологий локальных сетей. Протоколы MAC-уровня ориентированы на совместное использование физической среды абонентами. Разделяемая среда (shared media) применяется в таких широко распространенных в локальных сетях технологиях, как Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI. Использование разделяемой между пользователями среды улучшает загрузку канала связи, удешевляет сеть, но ограничивает скорость передачи данных между двумя узлами.

Каждой технологии MAC - уровня соответствует несколько вариантов (спецификаций) протоколов физического уровня. Спецификация технологии MAC - уровня определяет среду физического уровня и основные параметры передачи данных (скорость передачи, вид среды, узкополосная или широкополосная).

Так, протоколу 802.3, описывающему наиболее известную технологию Ethernet, соответствуют спецификации физического уровня: 10Base-T, 10Base-FB, 10Base-FL. Число 10 показывает, что скорость передачи данных составляет 10 Мбит/с, Base – система узкополосная. Спецификация 10Base-T предусматривает построение локальной сети на основе использования неэкранированной витой пары UTP не ниже 3-й категории и концентратора. Спецификации 10Base-FB, 10Base-FL используют волоконно-оптические кабели. Более ранние спецификации 10Base-5 и 10Base-2 предусматривали использование "толстого" или "тонкого" коаксиального кабеля.

Протоколу Fast Ethernet (802.3u) соответствуют следующие спецификации физического уровня:

- 100Base-T4, где используется четыре витых пары кабеля UTP не ниже 3-й категории;
- 100Base-TX – применяется две пары кабеля UTP не ниже 5-й категории;
- 100Base-FX – используется два волокна многомодового оптического кабеля.

Помимо Ethernet и Fast Ethernet на MAC-уровне используется еще ряд технологий: Gigabit Ethernet со скоростью передачи 1000 Мбит/с – стандарты 802.3z и 802.3ab; 10Gigabit Ethernet со скоростью передачи 10 000 Мбит/с – стандарт 802.3ae, а также ряд других. Например, протокол 802.5 описывает технологию сетей Token Ring, где в качестве физической среды используется экранированная витая пара STP, с помощью которой все станции сети соединяются в кольцевую структуру. В отличие от технологии Ethernet, в сетях с передачей маркера (Token Ring) реализуется не случайный, а детерминированный доступ к среде с помощью кадра специального формата – маркера (token). Сети Token Ring позволяют передавать данные по кольцу со скоростями либо 4 Мбит/с, либо 16 Мбит/с. По сравнению с Ethernet технология Token Ring более сложная и надежная, однако Token Ring несовместима с новыми технологиями Fast Ethernet, Gigabit Ethernet, 10Gigabit Ethernet. Технологии Ethernet и совместимые с ними как раз и рассматриваются в настоящем курсе лекций.

4. CSMA/CD

CSMA/CD (множественный доступ с контролем несущей и обнаружения коллизий) — технология множественного доступа к общей передающей среде в локальной компьютерной сети с контролем коллизий. В сетях Ethernet используется метод доступа к среде передачи данных, называемый методом коллективного доступа с опознаванием несущей и обнаружением коллизий.

Этот метод применяется исключительно в сетях с логической общей шиной. 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. Простота схемы подключения — это один из факторов, определивших успех стандарта Ethernet. Кабель к которому подключены все станции, работает в режиме коллективного доступа.

5. Распознавание коллизий

При описанном подходе (CSMA/CD — все компьютеры имеют непосредственный доступ к общей шины) возможна ситуация, когда две станции одновременно пытаются передать кадр данных по общей среде. Механизм прослушивания среды и пауза между кадрами не гарантирует от возникновения такой ситуации, когда две или более станции одновременно решают, что среда свободная, и начинают передавать свои кадры. При этом происходит коллизия, так как содержимое обоих кадров сталкивается на общем кабеле и происходит искажение информации.

Коллизия — это нормальная ситуация в работе сетей Ethernet. Для возникновения коллизии не обязательно, чтобы несколько станций начали передачу абсолютно одновременно, такая ситуация маловероятна. Гораздо вероятней, что коллизия возникает из-за того, что один узел начинает передачу раньше другого, но до второго узла сигналы первого просто не успевают дойти к тому времени, когда второй узел решает начать передачу своего кадра. То есть коллизия — это следствие распределенного характера сети.

Чтобы корректно обработать коллизию, все станции одновременно наблюдают за возникающими на кабеле сигналами. Если передаваемые и наблюдаемые сигналы отличаются, то фиксируется *обнаружение коллизии* (CD — collision detection). Для увеличения вероятности скорейшего обнаружения коллизии всеми станциями сети станция, которая обнаружила коллизию, прерывает передачу своего кадра и усиливает ситуацию коллизии посылкой в сеть специальной последовательностью из 32-бит, называемой последовательностью. После этого обнаружившая коллизию передающая станция обязана прекратить передачу и сделать паузу в течении короткого случайного интервала времени. Затем она может снова предпринять попытку захвата среды и передачи кадра. Если 16 последовательных попыток передачи кадра вызывают коллизию, то передатчик должен прекратить попытки и отбросить этот кадр.

6. Производительности сети Ethernet

Количество обрабатываемых кадров Ethernet в секунду часто указывается производителями мостов/коммутаторов и маршрутизаторов как основная характеристика производительности этих устройств. В свою очередь, интересно знать чистую максимальную пропускную способность сегмента Ethernet в кадрах в секунду в идеальном случае, когда в сети нет коллизий и нет дополнительных задержек, вносимых мостами и маршрутизаторами. Такой показатель помогает оценить требования к производительности коммуникационных устройств, так как в каждый порт устройства не может поступать больше кадров в единицу времени, чем позволяет это сделать соответствующий протокол.

Для коммуникационного оборудования наиболее тяжелым режимом является обработка кадров минимальной длины. Это объясняется тем, что на обработку каждого кадра мост, коммутатор или маршрутизатор тратит примерно одно и то же время, связанное с просмотром таблицы продвижения пакета, формированием нового кадра (для маршрутизатора) и т. п. А количество кадров минимальной длины, поступающих на устройство в единицу времени, естественно больше, чем кадров любой другой длины. Другая характеристика производительности коммуникационного оборудования - бит в секунду - используется реже, так как она не говорит о том, какого размера кадры при этом обрабатывало устройство, а на кадрах максимального размера достичь высокой производительности, измеряемой в битах в секунду гораздо легче.

Для расчета максимального количества кадров минимальной длины, проходящих по сегменту Ethernet, заметим, что размер кадра минимальной длины вместе с преамбулой составляет 72 байт или 576 бит, поэтому на его передачу затрачивается 57,5 мкс. Прибавив межкадровый интервал в 9,6 мкс, получаем, что период следования кадров минимальной длины составляет 67,1 мкс. Отсюда максимально возможная пропускная способность сегмента Ethernet составляет 14 880 кадр/с.

Естественно, что наличие в сегменте нескольких узлов снижает эту величину за счет ожидания доступа к среде, а также за счет коллизий, приводящих к необходимости повторной передачи кадров.

Кадры максимальной длины технологии Ethernet имеют поле длины 1500 байт, что вместе со служебной информацией дает 1518 байт, а с преамбулой составляет 1526 байт или 12 208 бит. Максимально возможная пропускная способность сегмента Ethernet для кадров максимальной длины составляет 813 кадр/с. Очевидно, что при работе с большими кадрами нагрузка на мосты, коммутаторы и маршрутизаторы довольно ощутимо снижается.

Теперь рассчитаем, какой максимальной полезной пропускной способностью в бит в секунду обладают сегменты Ethernet при использовании кадров разного размера.

Под полезной пропускной способностью протокола понимается скорость передачи пользовательских данных, которые переносятся полем данных кадра. Эта пропускная способность всегда меньше номинальной битовой скорости протокола Ethernet за счет нескольких факторов:

- служебной информации кадра
- межкадровых интервалов (IPG)

- ожидания доступа к среде

Для кадров минимальной длины полезная пропускная способность равна:

$V_п$= 14880 * 46 * 8 = 5,48 Мбит/с.

Это намного меньше 10 Мбит/с, но следует учесть, что кадры минимальной длины используются в основном для передачи квитанций, так что к передаче собственно данных файлов эта скорость отношения не имеет.

Для кадров максимальной длины полезная пропускная способность равна:

$V_п$ = 813 *1500 * 8 =9,76 Мбит/с, что весьма близко к номинальной скорости протокола.

Еще раз подчеркнем, что такой скорости можно достигнуть только в том случае, когда двум взаимодействующим узлам в сети Ethernet другие узлы не мешают, что бывает крайне редко.

При использовании кадров среднего размера с полем данных в 512 байт пропускная способность сети составит 9,29 Мбит/с, что тоже достаточно близко к предельной пропускной способности в 10 Мбит/с.

- $V_{эф.} = V_{н.} * k_1 * k_2 * k_3$ – эффективная скорость [бит/сек.]
- $k_{1(64)}$ = 46*8 / 72*8 + 96 = 5,48 Мбит/с.
- $k_{1(1500)}$ = 1500*8 / 1500*8+96 = 9,76 Мбит/с
- k_2 – учитывает переспрос из-за ошибок. $k_2 = (1 – p)^l$, p – вероятность ошибки, l – длина защищаемой части кабеля Ethernet в битах
- k_3 – определяет снижение эффективной скорости в сети за счет коллизий

7. 4 типа кадров канального уровня

Стандарт на технологию Ethernet, описанный в документе 802.3, дает описание единственного формата кадра MAC - уровня. Так как в кадр MAC - уровня должен вкладываться кадр уровня LLC, описанный в документе 802.2, то по стандартам IEEE в сети Ethernet может использоваться только единственный вариант кадра канального уровня, образованный комбинацией заголовков MAC и LLC подуровней.

Тем не менее, на практике в сетях Ethernet на канальном уровне используются заголовки 4-х типов. Это связано с длительной историей развития технологии Ethernet до принятия стандартов IEEE 802, когда подуровень LLC не выделялся из общего протокола и, соответственно, заголовок LLC не применялся.

Консорциум трех фирм Digital, Intel и Xerox в 1980 году представил на рассмотрение комитету 802.3 свою фирменную версию стандарта Ethernet, но комитет 802.3 принял стандарт, отличающийся в некоторых деталях от предложения DIX. Отличия касались и формата кадра, что породило существование двух различных типов кадров в сети Ethernet.

Еще один формат кадра появился в результате усилий компании Novell по ускорению работы своего стека протоколов в сетях Ethernet.

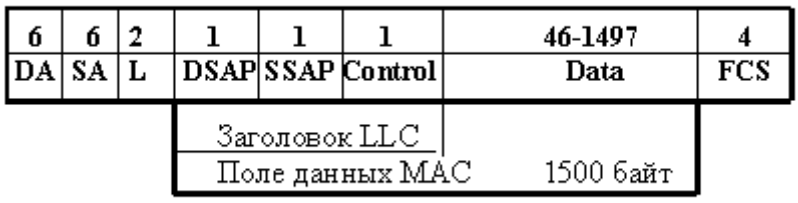
И, наконец, четвертый формат кадра стал результатом деятельности комитета 802.2 по приведению предыдущих форматов кадров к некоторому общему стандарту.

Сегодня практически все сетевые адаптеры, драйверы сетевых адаптеров, мосты/коммутаторы и маршрутизаторы умеют работать со всеми используемыми на практике форматами кадров технологии Ethernet, причем распознавание типа кадра выполняется автоматически.

Ниже приводится описание всех четырех модификаций заголовков кадров Ethernet (здесь под кадром понимается весь набор полей, которые относятся к канальному уровню, то есть поля MAC и LLC уровней):

- *Кадр 802.3/LLC (кадр 802.3/802.2 или кадр Novell 802.2)*

Кадр 802.3/LLC



Адрес назначения (Destination Address, DA) - 6 байт. Первый бит старшего байта адреса назначения является признаком того, является адрес индивидуальным или групповым. Если 0, то адрес является индивидуальным (unicast), а если 1, то это групповой адрес (multicast). Групповой адрес сети может предназначаться всем узлам сети или же определенной группе узлов сети. Если адрес состоит из всех единиц, то есть имеет шестнадцатеричное представление 0*FFFFFFFFFFF, то он предназначен всем узлам сети и называется широковещательным адресом (broadcast). В остальных случаях групповой адрес связан только с теми узлами, которые сконфигурированы

(например, вручную) как члены группы, номер которой указан в групповом адресе. Второй бит старшего байта адреса определяет способ назначения адреса - централизованный или локальный. Если этот бит равен0(что бывает почти всегда в стандартной аппаратуре Ethernet), то адрес назначен централизованно, с помощью комитета IEEE. Комитет IEEE распределяет между производителями оборудования так называемые организационно уникальные идентификаторы (Organizationally Unique Identifier, OUI). Этот идентификатор помещается в 3 старших байта адреса (например, идентификатор 000081 определяет компанию Bay Networks). За уникальность младших 3-х байт адреса отвечает производитель оборудования. Двадцать четыре бита, отводимые производителю для адресации интерфейсов его продукции, позволяют выпустить16 миллионов интерфейсов под одним идентификатором организации. Уникальность централизованно распределяемых адресов распространяется на все основные технологии локальных сетей -Ethernet, TokenRing, FDDI и т.д.

Адрес источника (Source Address, SA) - 6-ти байтовое поле, содержащее адрес станции - отправителя кадра. Первый бит - всегда имеет значение 0.

Длина (Length, L). Двухбайтовое поле длины определяет длину поля данных в кадре.

DSAP адрес доступа к службе получателя (Destination Service Access Point) -1 байт.

SSAP адрес доступа службы отпрвителя (Source Service Access Point) - 1 байт.

Control поле управления– 1 байт в режиме LLC1 и 2 байта в режиме LLC2.

Поле данных (Data) может содержать от 0 до 1500 байт. Но если длина поля меньше 46 байт, то используется поле заполнения (Padding), чтобы дополнить кадр до минимально допустимого значения в 46 байт. Так как кадр LLC имеет заголовок длиной 3 (в режиме LLC1) или 4 байт (в режиме LLC2), то максимальный размер поля данных уменьшается до 1497 (1796) байт.

Поле контрольной суммы (frame Check Sequence, FCS) - 4 байта, содержащие значение, которое вычисляется по определенному алгоритму CRC-32.

- *Кадр Raw 802.3 (или кадр Novell 802.3)*

Кадр Raw 802.3/Novell 802.3

6	6	2	46-1500	4
DA	SA	L	Data	FCS

Как видно из рисунка-это кадр уровня MAC без вложенного заголовка LLC. Дело в том,что Novell долгое время не использовала поля кадра LLC из-за отсутствия необходимости идентифицировать тип вышележащего протокола-всегда использовался IPX. Теперь ,когда NetWare поддерживает и другие протоколы, Novell стала вкладывать в MAC - кадр заголовок LLC, т.е. использовать обычный кадр 802.3/LLC.

- *Кадр Ethernet DIX (или кадр Ethernet II)*

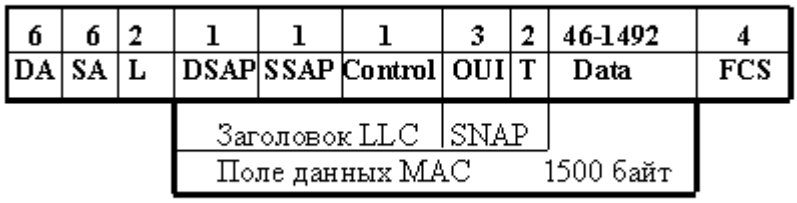
Кадр Ethernet DIX

6	6	2	46-1500	4
DA	SA	T	Data	FCS

Появление этого формата связано с тем ,что после подачи заявки в IEEE консорциумом Digital, Intel и Xerox результирующий стандарт IEEE 802.3 в деталях отличался от Ethernet DIX,ставшего к тому времени промышленным стандартом де-факто. Кадр Ethernet DIX практически совпадает с Raw 802.3,за исключением того,что вместо поля L используется также двухбайтовое поле T (Type), предназначенное для тех же целей, что и SAP кадра уровня LLC - указания типа вышележащего протокола.

- *Кадр Ethernet SNAP*

Кадр Ethernet SNAP



Для устранения различий в форматах кадров комитетом IEEE 802 была проведена работа по стандартизации кадров Ethernet - появился кадр Ethernet SNAP (SNAP-Sub Network Access Protocol,протокол доступа к подсетям).Кадр Ethernet SNAP представляет собой расширение кадра 802.3/LLC за счет введения дополнительного заголовка SNAP из двух полей:OUI и Type. Поле Type полностью повторяет аналогичное поле кадра Ethernet DIX,а поле OUI определяет организацию,контролирующую коды протоколов в поле Type (для IEEE OUI=000000). При этом в полях DSAP и SSAP записываются коды 0xAA,а для идентификации вышележащего протокола используются поля заголовка SNAP. Так как SNAP является дополнением к заголовку LLC и не зависит от MAC - уровня,то он допустим не только в кадрах Ethernet,но и других технологий,например FDDI.

8. Согласование различных типов кадров в сетях Ethernet

Различия в формате кадров могут приводить к не совместимости в работе сетевого оборудования и программного обеспечения,рассчитанного на работу только с определенным форматом кадра,однако на сегодняшний день практически все сетевое оборудование поддерживает все 4 формата кадров,причем распознавание производится автоматически. Распознавание формата происходит следующим образом. Для кодирования типа протокола в поле Type кадра Ethernet DIX всегда используются коды более 1500 (макс. значение L),поэтому по значению поля L/T легко отличить кадры Ethernet DIX. Далее анализируется наличие или отсутствие заголовка LLC. Поля заголовка LLC могут отсутствовать только в кадрах Raw 802.3 ,значит следом идет пакет IPX,первые 2 байта которого всегда заполняются единицами;поля же DSAP и SSAP не могут иметь значение 0xFF, поэтому это однозначно кадр Raw802.3. Отличить кадры 802.3/LLC и Ethernet SNAP можно по значениям SAP — полей в кадрах Ethernet SNAP DSAP=SSAP=0xAA.

9. Стандарты Ethernet

- *Технология Fast Ethernet*

  Общее название для набора стандартов передачи данных в компьютерных сетях по технологии Ethernet со скоростью до 100 Мбит/с, в отличие от исходных 10 Мбит/с.

- *100BASE — FX*

  Две жилы, волоконно-оптического кабеля. Передача также осуществляется в соответствии со стандартом передачи данных в волоконно-оптической среде, которой разработан ANSI. Использует алгоритм кодирования данных 4B/5B и метод физического кодирования NRZI.

- *100BASE — TX*

  Две витые пары проводов. Передача осуществляется в соответствии со стандартом передачи данных в витой физической среде, разработанным ANSI (American National Standards Institute — Американский национальный институт стандартов). Витой кабель для передачи данных может быть экранированным, либо неэкранированным. Использует алгоритм кодирования данных 4B/5B и метод физического кодирования MLT-3.

- *100BASE — T4*

  Это особая спецификация, разработанная комитетом IEEE 802.3u . Согласно этой спецификации, передача данных осуществляется по четырем витым парам телефонного кабеля, который называют кабелем UTP категории 3. Использует алгоритм кодирования данных 8B/6T и метод физического кодирования NRZI.

Физические интерфейсы стандарта Fast Ethernet IEEE 802.3u и их основные характеристики

Физический интерфейс	100Base-FX	100Base-TX	100Base-T4***
Порт устройства	Duplex SC	RJ-45	RJ-45
Среда передачи	Оптическое волокно	Витая пара UTP Cat.5 (5e)	Витая пара UTP Cat. 3,4,5
Сигнальная схема	4B/5B	4B/5B	8B/6T
Битовое кодирование	NRZI	MLT-3	
Число витых пар/волокон	2 волокна	2 витых пары	4 витых пары
Протяженность сегмента*	До 412 м (ММВ), до 2 км, дуплекс (ММВ)**, до 100 км (ОМВ)***	До 100 м	До 100 м

1.ОМВ -- одномодовое оптоволокно, ММВ -- многомодовое оптоволокно.

2.Расстояние может быть достигнуто только при дуплексном режиме связи.

3.В нашей стране распространения не получил ввиду принципиальной невозможности поддержки дуплексного режима передачи.

10. Правила построения сегментов Fast Ethernet в случае использования повторителей

Технология Fast Ethernet, как и все некоаксиальные варианты Ethernet'а рассчитана на подключение конечных узлов - компьютеров с соответствующими сетевыми адаптерами - к многопортовым концентраторам-повторителям или коммутаторам.

Правила корректного построения сегментов сетей Fast Ethernet включают:

- ограничения на максимальные длины сегментов, соединяющих DTE с DTE;
- ограничения на максимальные длины сегментов, соединяющих DTE с портом повторителя;
- ограничения на максимальный диаметр сети;
- ограничения на максимальное число повторителей и максимальную длину сегмента, соединяющего повторители.

Рассмотрим вначале влияние ограничений длин сегментов DTE-DTE.

В качестве DTE (Data Terminal Equipment) может выступать любой источник кадров данных для сети: сетевой адаптер, порт моста, порт маршрутизатора, модуль управления сетью и другие подобные устройства. Порт повторителя не является DTE. В типичной конфигурации сети Fast Ethernet несколько DTE подключается к портам повторителя, образуя сеть звездообразной топологии.

Спецификация IEEE 802.3u определяет следующие максимальные значения сегментов DTE-DTE:

Стандарт	Тип кабеля	Максимальная длина сегмента
100Base-TX	Category 5 UTP	100 метров
100Base-FX	Многомодовое оптоволокно 62.5/125 мкм	412 метров (полудуплекс) 2 км (полнодуплекс)
100Base-T4	Category 3, 4 или 5 UTP	100 метров

Остановимся подробнее на ограничениях, связанных с соединениями с повторителями.

Повторители Fast Ethernet делятся на два класса.

Повторители класса I поддерживают все типы систем кодирования физического уровня: 100Base-TX/FX и 100Base-T4. Повторители класса II поддерживают только один тип системы кодирования физического уровня - 100Base-TX/FX или 100Base-T4.

В одном домене коллизий допускается наличие только одного повторителя класса I. Это связано с тем, что такой повторитель вносит большую задержку при распространении сигналов из-за необходимости трансляции различных систем сигнализации.

Максимальное число повторителей класса II в домене коллизий - 2, причем они должны быть соединены между собой кабелем не длиннее 5 метров.

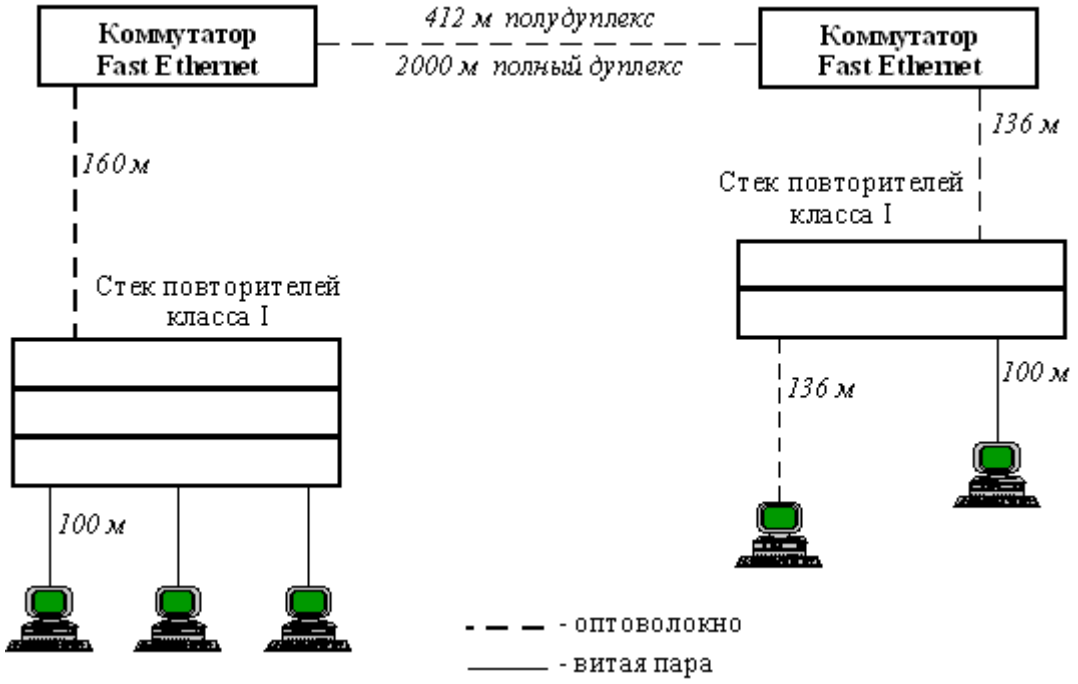
Небольшое количество повторителей Fast Ethernet не является серьезным препятствием при построении сетей. Во-первых, наличие стековых повторителей снимает проблемы ограниченного числа портов - все каскадируемые повторители представляют собой один повторитель с достаточным числом портов - до нескольких сотен. Во-вторых, применение

коммутаторов и маршрутизаторов делит сеть на несколько доменов коллизий, в каждом из которых обычно имеется не очень большое число станций.

В следующей таблице сведены правила построения сети на основе повторителе класса I.

Тип кабелей	Максимальный диаметр сети	Максимальная длина сегмента
Только витая пара (TX)	200 м	100 м
Только оптоволокно (FX)	272 м	136 м
Несколько сегментов на витой паре и один на оптоволокне 260 м	100 м (TX)	160 м (FX)
Несколько сегментов на витой паре и несколько сегментов на оптоволокне 272 м	100 м (TX)	136 м (FX)

Эти ограничения проиллюстрированы типовыми конфигурациями сетей:



11. Коммутаторы локальной сети

Сетевой коммутатор или свитч, свич (от англ. switch — переключатель) — устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного сегмента. В отличие от концентратора, который распространяет трафик от одного подключенного устройства ко всем остальным, коммутатор передает данные только непосредственно получателю. Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

Свич работает на канальном уровне модели OSI, и потому в общем случае может только объединять узлы одной сети по их MAC-адресам. Для соединения нескольких сетей на основе сетевого уровня служат маршрутизаторы.

Принцип работы коммутатора. Коммутатор хранит в памяти специальную таблицу (MAC-таблицу), в которой указывается соответствие MAC-адреса узла порту коммутатора. При включении switch эта таблица пуста, и он работает в режиме обучения. В этом режиме поступающие на какой-либо порт данные передаются на все остальные порты коммутатора. При этом свитч анализирует пакеты данных, определяя MAC-адрес компьютера-отправителя, и заносит его в таблицу. Впоследствии, если на один из портов коммутатора поступит пакет, предназначенный для этого компьютера, этот пакет будет отправлен только на соответствующий порт. Если MAC-адрес компьютера-получателя еще не известен, то пакет будет продублирован на все интерфейсы. Со временем коммутатор строит полную таблицу для всех своих портов, и в результате трафик локализуется.

Возможности и разновидности коммутаторов. Свичи подразделяются на управляемые и неуправляемые (наиболее простые). Более сложные свичи позволяют управлять коммутацией на канальном (втором) и сетевом (третьем) уровне модели OSI. Обычно их именуют соответственно, например Layer 2 Switch или просто, сокращенно L2. Управление свичем может осуществляться посредством протокола Web-интерфейса, SNMP, RMON и т.п. Многие управляемые свичи позволяют выполнять дополнительные функции: VLAN, QoS, агрегирование, зеркалирование. Сложные коммутаторы можно объединять в одно логическое устройство - стек, с целью увеличения числа портов (например, можно объединить 4 коммутатора с 24 портами и получить логический коммутатор с 96 портами).

12. Full-duplex. Протоколы локальной сети (коммутация кадров)

Режим передачи определяет способ коммуникации между двумя узлами. Полнодуплексный (full duplex) режим позволяет одновременно передавать информацию в двух направлениях. В самом простом случае для дуплексной связи используется две линии связи (прям и обратная), но существуют решения, которые позволяют поддерживать дуплексный режим на единственной линии (например, оба узла могут одновременно передавать данные, а из принятого сигнала вычитать собственные данные).

Полнодуплексный режим может быть симметричным (полоса пропускания канала одинакова в обоих направлениях) или асимметричным.

Существует три способа коммутации. Каждый из них — это комбинация таких параметров, как время ожидания и надёжность передачи.

С промежуточным хранением (Store and Forward). Коммутатор читает всю информацию в кадре, проверяет его на отсутствие ошибок, выбирает порт коммутации и после этого посылает в него кадр.

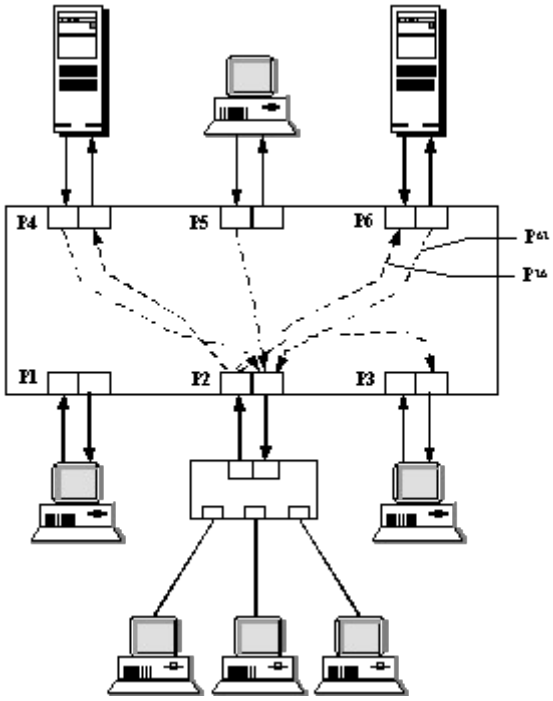
Сквозной (cut-through). Коммутатор считывает в кадре только адрес назначения и после выполняет коммутацию. Этот режим уменьшает задержки при передаче, но в нём нет метода обнаружения ошибок.

Бесфрагментный (fragment-free) или гибридный. Этот режим является модификацией сквозного режима. Передача осуществляется после фильтрации фрагментов коллизий (первые 64 байта кадра анализируются на наличие ошибки и при её отсутствии кадр обрабатывается в сквозном режиме).

Задержка, связанная с «принятием коммутатором решения», добавляется к времени, которое требуется кадру для входа на порт коммутатора и выхода с него, и вместе с ним определяет общую задержку коммутатора.

13. Оценка необходимой общей производительности коммутатора

В идеальном случае коммутатор, установленный в сети, передает кадры между узлами, подключенными к его портам, с той скоростью, с которой узлы генерируют эти кадры, не внося дополнительных задержек и не теряя ни одного кадра. В реальной практике коммутатор всегда вносит некоторые задержки при передаче кадров, а также может некоторые кадры терять, то есть не доставлять их адресатам. Из-за различий во внутренней организации разных моделей коммутаторов, трудно предвидеть, как тот или иной коммутатор будет передавать кадры какого-то конкретного образца трафика. Лучшим критерием по-прежнему остается практика, когда коммутатор ставится в реальную сеть и измеряются вносимые им задержки и количество потерянных кадров. Однако, существуют несложные расчеты, которые могут дать представление о том, как коммутатор будет вести себя в реальной ситуации.



Основой для оценки того, как будет справляться коммутатор со связью узлов или сегментов, подключенных к его портам, являются данные о средней интенсивности трафика между узлами сети. Для приведенного примера это означает, что нужно каким-то образом оценить, сколько в среднем кадров в секунду узел, подключенный к порту P2, генерирует узлу, подключенному к порту P4 (трафик P24), узлу, подключенному к порту P3 (трафик P23), и так далее, до узла, подключенного к порту P6. Затем эту процедуру нужно повторить для трафика, генерируемого узами, подключенными к портам 3, 4, 5 и 6. В общем случае, интенсивность трафика, генерируемого одним узлом другому, не совпадает с интенсивностью трафика, генерируемого в обратном направлении.

Результатом исследования трафика будет построение матрицы трафика, приведенной на рисунке ниже. Трафик можно измерять как в кадрах в секунду, так и в битах в секунду. Так как затем требуемые значения трафика будут сравниваться с показателями производительности коммутатора, то нужно их иметь в одних и тех же единицах. Для определенности будем считать, что в рассматриваемом примере трафик и производительность коммутатора измеряются в битах в секунду.

	1	2	3	4	5	6
1	0	P_{12}	P_{13}	P_{14}	P_{15}	P_{16}
2	P_{21}	0	P_{23}	P_{24}	P_{25}	P_{26}
3	P_{31}	P_{32}	0	P_{34}	P_{35}	P_{36}
4	P_{41}	P_{42}	P_{43}	0	P_{45}	P_{46}
5	P_{51}	P_{52}	P_{53}	P_{54}	0	P_{56}
6	P_{61}	P_{62}	P_{63}	P_{64}	P_{65}	0

Подобную матрицу строят агенты RMON MIB (переменная Traffic Matrix), встроенные в сетевые адаптеры или другое коммуникационное оборудование.

Для того, чтобы коммутатор справился с поддержкой требуемой матрицы трафика, необходимо выполнение нескольких условий.

1. Общая производительность коммутатора должна быть больше или равна суммарной интенсивности передаваемого трафика:

$$B = \sum \eta_{ij} P_{ij}$$

где B - общая производительность коммутатора, P_{ij} - суммарная интенсивность трафика от i-го порта к j - му; сумма берется по всем портам коммутатора.

2. Номинальная максимальная производительность протокола каждого порта коммутатора должна быть не меньше средней интенсивности суммарного трафика, проходящего через порт:

$$C_k = \sum \eta_j P_{kj} + \eta_i P_{ik}$$

где C_k - номинальная максимальная производительность протокола k - го порта (например, если k -ый порт поддерживает Ethernet, то C_k равно 10 Мб/с), первая сумма равна интенсивности выходящего из порта трафика, а вторая – входящего. Эта формула полагает, что порт коммутатора работает в стандартном полудуплексном режиме, для полудуплексного режима величину C_k нужно удвоить.

3. Производительность процессора каждого порта должна быть не меньше средней интенсивности суммарного трафика, проходящего через порт. Условие аналогично предыдущему, но вместо номинальной производительности поддерживаемого протокола в ней должна использоваться производительность процессора порта.

4. Производительность внутренней шины коммутатора должна быть не меньше средней интенсивности суммарного трафика, передаваемого между портами, принадлежащими

разными модулям коммутатора:

$$B_{bus} = \sum \eta_{ij} P_{ij},$$

где B_{bus} производительность общей шины коммутатора, а сумма $n_{ij}P_{ij}$ берется только по тем i и j, которые принадлежат разным модулям.

14. Адресная таблица коммутатора

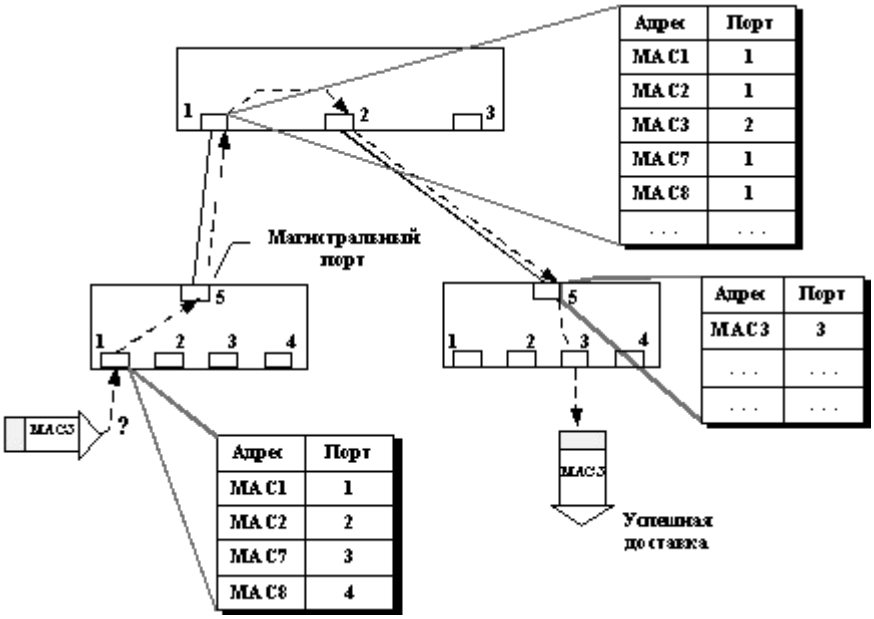
Максимальная емкость адресной таблицы определяет максимальное количество MAC-адресов, с которыми может одновременно оперировать коммутатор. Так как коммутаторы чаще всего используют для выполнения операций каждого порта выделенный процессорный блок со своей памятью для хранения экземпляра адресной таблицы, то размер адресной таблицы для коммутаторов обычно приводится в расчете на один порт. Экземпляры адресной таблицы разных процессорных модулей не обязательно содержат одну и ту же адресную информацию - скорее всего повторяющихся адресов будет не так много, если только распределение трафика каждого порта не полностью равновероятное между остальными портами. Каждый порт хранит только те наборы адресов, которыми он пользуется в последнее время.

Значение максимального числа MAC-адресов, которое может запомнить процессор порта, зависит от области применения коммутатора. Коммутаторы рабочих групп обычно поддерживают всего несколько адресов на порт, так как они предназначены для образования микросегментов. Коммутаторы отделов должны поддерживать несколько сотен адресов, а коммутаторы магистралей сетей - до нескольких тысяч, обычно 4К - 8К адресов.

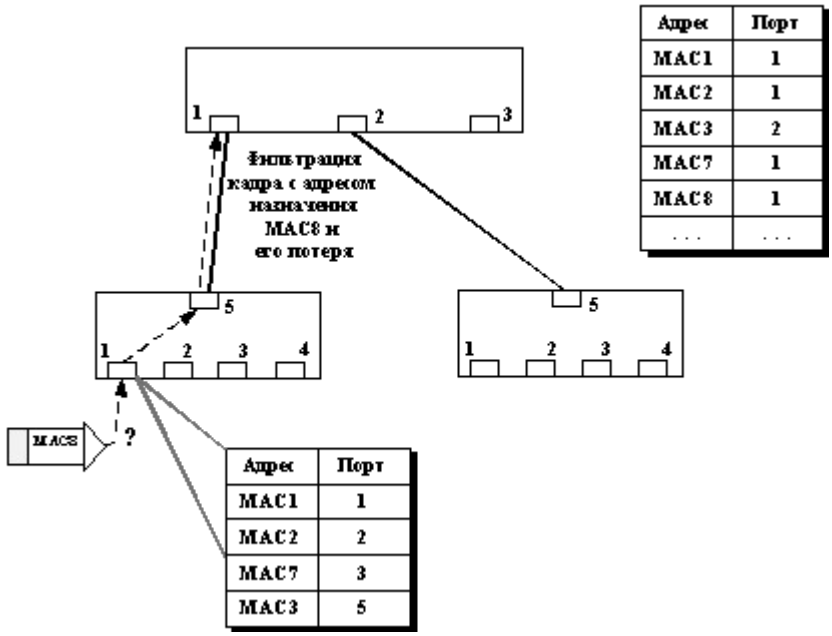
Недостаточная емкость адресной таблицы может служить причиной замедления работы коммутатора и засорения сети избыточным трафиком. Если адресная таблица процессора порта полностью заполнена, а он встречает новый адрес источника в поступившем пакете, то он должен вытеснить из таблицы какой-либо старый адрес и поместить на его место новый. Эта операция сама по себе отнимет у процессора часть времени, но главные потери производительности будут наблюдаться при поступлении кадра с адресом назначения, который пришлось удалить из адресной таблицы. Так как адрес назначения кадра неизвестен, то коммутатор должен передать этот кадр на все остальные порты. Эта операция будет создавать лишнюю работу для многих процессоров портов, кроме того, копии этого кадра будут попадать и на те сегменты сети, где они совсем необязательны.

Некоторые производители коммутаторов решают эту проблему за счет изменения алгоритма обработки кадров с неизвестным адресом назначения. Один из портов коммутатора конфигурируется как магистральный порт, на который по умолчанию передаются все кадры с неизвестным адресом. В маршрутизаторах такой прием применяется давно, позволяя сократить размеры адресных таблиц в сетях, организованных по иерархическому принципу.

Передача кадра на магистральный порт производится в расчете на то, что этот порт подключен к вышестоящему коммутатору, который имеет достаточную емкость адресной таблицы и знает, куда нужно передать любой кадр. Пример успешной передачи кадра при использовании магистрального порта приведен на рисунке ниже. Коммутатор верхнего уровня имеет информацию о всех узлах сети, поэтому кадр с адресом назначения MAC3, переданный ему через магистральный порт, он передает через порт 2 коммутатору, к которому подключен узел с адресом MAC3.



Хотя метод магистрального порта и будет работать эффективно во многих случаях, но можно представить такие ситуации, когда кадры будут просто теряться. Одна из таких ситуаций изображена на рисунке ниже. Коммутатор нижнего уровня удалил из своей адресной таблицы адрес MAC8, который подключен к его порту 4, для того, чтобы освободить место для нового адреса MAC3. При поступлении кадра с адресом назначения MAC8, коммутатор передает его на магистральный порт 5, через который кадр попадает в коммутатор верхнего уровня. Этот коммутатор видит по своей адресной таблице, что адрес MAC8 принадлежит его порту 1, через который он и поступил в коммутатор. Поэтому кадр далее не обрабатывается и просто отфильтровывается, а, следовательно, не доходит до адресата. Поэтому более надежным является использование коммутаторов с достаточным количеством адресной таблицы для каждого порта, а также с поддержкой общей адресной таблицы модулем управления коммутатором.



15. Объем буфера

Внутренняя буферная память коммутатора нужна для временного хранения кадров данных в тех случаях, когда их невозможно немедленно передать на выходной порт. Буфер предназначен для сглаживания кратковременных пульсаций трафика. Ведь даже если трафик хорошо сбалансирован и производительность процессоров портов, а также других обрабатывающих элементов коммутатора достаточна для передачи средних значений трафика, то это не гарантирует, что их производительности хватит при очень больших пиковых значениях нагрузок. Например, трафик может в течение нескольких десятков миллисекунд поступать одновременно на все входы коммутатора, не давая ему возможности передавать принимаемые кадры на выходные порты.

Для предотвращения потерь кадров при кратковременном многократном превышении среднего значения интенсивности трафика (а для локальных сетей часто встречаются значения коэффициента пульсации трафика в диапазоне 50 - 100) единственным средством служит буфер большого объема. Как и в случае адресных таблиц, каждый процессорный модуль порта обычно имеет свою буферную память для хранения кадров. Чем больше объем этой памяти, тем менее вероятны потери кадров при перегрузках, хотя при несбалансированности средних значений трафика буфер все равно рано или поздно переполниться.

Обычно коммутаторы, предназначенные для работы в ответственных частях сети, имеют буферную память в несколько десятков или сотен килобайт на порт. Хорошо, когда эту буферную память можно перераспределять между несколькими портами, так как одновременные перегрузки по нескольким портам маловероятны. Дополнительным средством защиты может служить общий для всех портов буфер в модуле управления коммутатором. Такой буфер обычно имеет объем в несколько мегабайт.

16. Дополнительные возможности коммутатора

Так как коммутатор представляет собой сложное вычислительное устройство, имеющее несколько процессорных модулей, то естественно нагрузить его помимо выполнения основной функции передачи кадров с порта на порт по алгоритму моста и некоторыми дополнительными функциями, полезными при построении надежных и гибких сетей. Ниже описываются наиболее распространенные дополнительные функции коммутаторов, которые поддерживаются большинством производителей коммуникационного оборудования:

- Поддержка алгоритма Spanning Tree (подробней в 17)
- Фильтрация трафика (подробней в 19)
- Коммутация "на лету" или с буферизацией
- Использование различных классов сервиса (подробней в 20)
- Поддержка виртуальных сетей (подробней в 21)

17. Структуризация локальной сети на базе коммутатора и основные определения

- *Технология Spanning-Tree*

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

Поддерживающие алгоритм STA коммутаторы автоматически создают активную древовидную конфигурацию связей (то есть связную конфигурацию без петель) на множестве всех связей сети. Такая конфигурация называется покрывающим деревом - Spanning Tree (иногда ее называют остовным или основным деревом), и ее название дало имя всему алгоритму. Коммутаторы находят покрывающее дерево адаптивно с помощью обмена служебными пакетами. Реализация в коммутаторе алгоритма STA очень важна для работы в больших сетях - если коммутатор не поддерживает этот алгоритм, то администратор должен самостоятельно определить, какие порты нужно перевести в заблокированное состояние, чтобы исключить петли. К тому же при отказе какой-либо связи, порта или коммутатора администратор должен, во-первых, обнаружить факт отказа, а, во-вторых, ликвидировать последствия отказа, переведя резервную связь в рабочий режим путем активизации некоторых портов.

Основные определения.

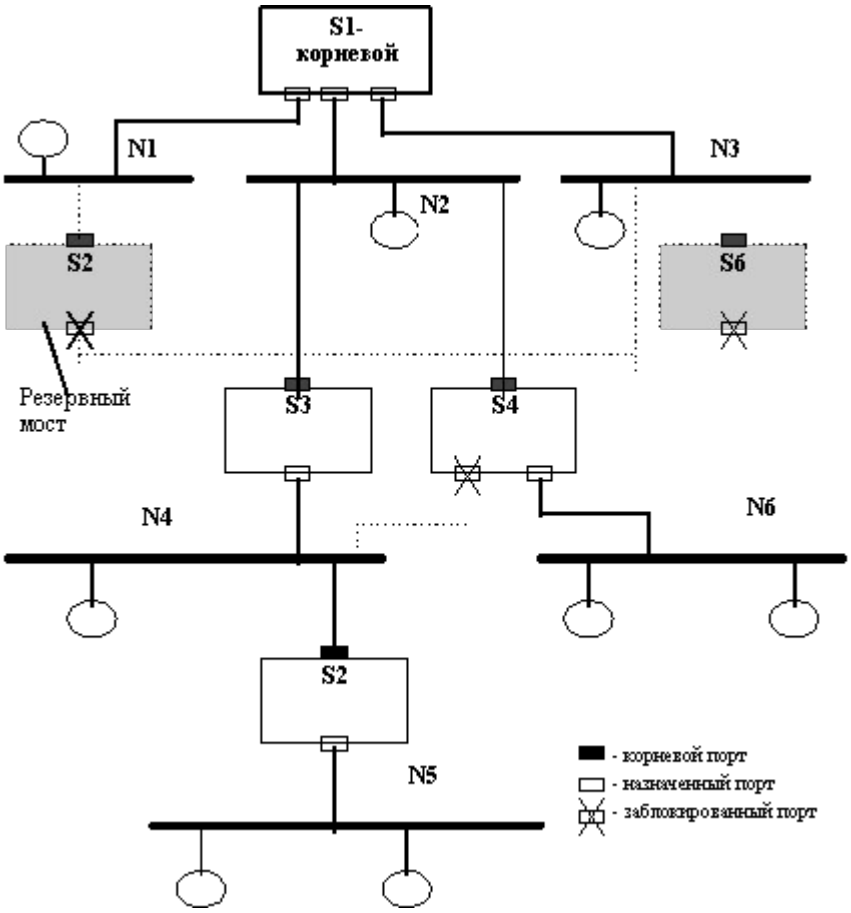
В сети определяется корневой коммутатор (root switch), от которого строится дерево. Корневой коммутатор может быть выбран автоматически или назначен администратором. При автоматическом выборе корневым становится коммутатор с меньшим значением MAC-адреса его блока управления.

Для каждого коммутатора определяется корневой порт (root port) - это порт, который имеет по сети кратчайшее расстояние до корневого коммутатора (точнее, до любого из портов корневого коммутатора). Затем для каждого сегмента сети выбирается так называемый назначенный порт (designated port) - это порт, который имеет кратчайшее расстояние от данного сегмента до корневого коммутатора.

Понятие расстояния играет важную роль в построении покрывающего дерева. Именно по этому критерию выбирается единственный порт, соединяющий каждый коммутатор с корневым коммутатором, и единственный порт, соединяющий каждый сегмент сети с корневым коммутатором. Все остальные порты переводятся в резервное состояние, то есть такое, при котором они не передают обычные кадры данных. Можно доказать, что при таком выборе активных портов в сети исключаются петли и оставшиеся связи образуют покрывающее дерево.

На рисунке ниже показан пример построения конфигурации покрывающего дерева для сети, состоящей из 6 сегментов (N1 - N6) и 6 коммутаторов (S1 - S6). Корневые порты закрашены черным цветом, назначенные не закрашены, а заблокированные порты перечеркнуты. В активной конфигурации коммутаторы S2 и S6 не имеют портов, передающих кадры данных,

поэтому они закрашены как резервные.



Расстояние до корня определяется как суммарное условное время на передачу данных от порта данного коммутатора до порта корневого коммутатора. При этом считается, что время внутренних передач данных (с порта на порт) коммутатором пренебрежимо мало, а учитывается только время на передачу данных по сегментам сети, соединяющим коммутаторы. Условное время сегмента рассчитывается как время, затрачиваемое на передачу одного бита информации в 10-наносекундных единицах между непосредственно связанными по сегменту сети портами. Так, для сегмента Ethernet это время равно 10 условным единицам, а для сегмента Token Ring 16 Мб/с - 6.25. (Алгоритм STA не связан с каким-либо определенным стандартом канального уровня, он может применяться к коммутаторам, соединяющим сети различных технологий.)

В приведенном примере предполагается, что все сегменты имеют одинаковое условное расстояние, поэтому оно не показано на рисунке.

- *Основные поля пакета BPDU*

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

Пакеты BPDU помещаются в поле данных кадров канального уровня, например, кадров Ethernet или FDDI. Желательно, чтобы все коммутаторы поддерживали общий групповой адрес, с помощью которого кадры, содержащие пакеты BPDU, могли одновременно

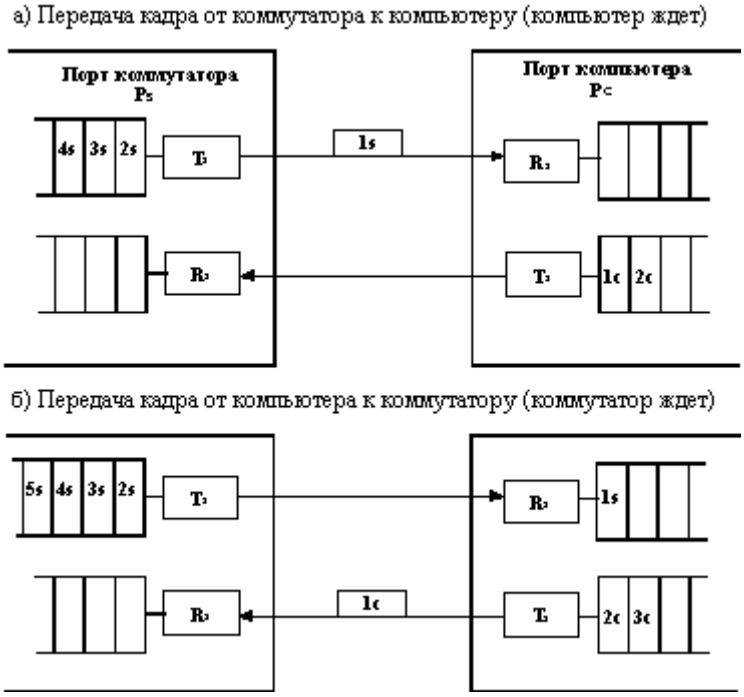
передаваться всем коммутаторам сети. Иначе пакеты BPDU рассылаются широковещательно.

Пакет BPDU имеет следующие поля:

- Идентификатор версии протокола STA - 2 байта. Коммутаторы должны поддерживать одну и ту же версию протокола STA, иначе может установиться активная конфигурация с петлями.
- Тип BPDU - 1 байт. Существует два типа BPDU - конфигурационный BPDU, то есть заявка на возможность стать корневым коммутатором, на основании которой происходит определение активной конфигурации, и BPDU уведомления о реконфигурации, которое посылается коммутатором, обнаружившим событие, требующее проведения реконфигурации - отказ линии связи, отказ порта, изменение приоритетов коммутатора или портов.
- Флаги - 1 байт. Один бит содержит флаг изменения конфигурации, второй бит - флаг подтверждения изменения конфигурации.
- Идентификатор корневого коммутатора - 8 байтов.
- Расстояние до корня - 2 байта.
- Идентификатор коммутатора - 8 байтов.
- Идентификатор порта - 2 байта.
- Время жизни сообщения - 2 байта. Измеряется в единицах по 0.5 с, служит для выявления устаревших сообщений. Когда пакет BPDU проходит через коммутатор, тот добавляет ко времени жизни пакета время его задержки данным коммутатором.
- Максимальное время жизни сообщения - 2 байта. Если пакет BPDU имеет время жизни, превышающее максимальное, то он игнорируется коммутаторами.
- Интервал hello, через который посылаются пакеты BPDU.
- Задержка смены состояний - 2 байта. Минимальное время перехода портов коммутатора в активное состояние. Такая задержка необходима, чтобы исключить возможность временного возникновения альтернативных маршрутов при неодновременной смене состояний портов во время реконфигурации.

18. Способы управления потоком кадров

Некоторые производители применяют в своих коммутаторах приемы управления потоком кадров, отсутствующие в стандартах протоколов локальных сетей, для предотвращения потерь кадров при перегрузках.



На рисунке выше приведен пример обмена кадрами между коммутатором и портом сетевого адаптера компьютера в режиме пиковой загрузки коммутатора. Коммутатор не успевает передавать кадры из буфера передатчика Tx, так как при нормальном полудуплексном режиме работы передатчик должен часть времени простаивать, ожидая, пока приемник не примет очередной кадр от компьютера.

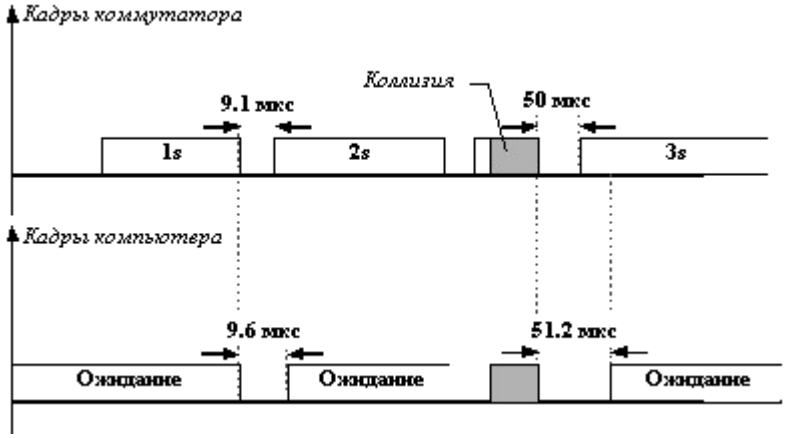
Так как потери, даже небольшой доли кадров, обычно намного снижают полезную производительность сети, то при перегрузке коммутатора рационально было бы замедлить интенсивность поступления кадров от конечных узлов в приемники коммутатора, чтобы дать возможность передатчикам разгрузить свои буфера с более высокой скоростью. Алгоритм чередования передаваемых и принимаемых кадров (frame interleave) должен быть гибким и позволять компьютеру в критических ситуациях на каждый принимаемый кадр передавать несколько своих, причем не обязательно снижая при этом интенсивность приема до нуля, а просто уменьшая ее до необходимого уровня.

Для реализации такого алгоритма в распоряжении коммутатора должен быть механизм снижения интенсивности трафика подключенных к его портам узлов. У некоторых протоколов локальных сетей, таких как FDDI, Token Ring или 100VG-AnyLAN имеется возможность изменять приоритет порта и тем самым давать порту коммутатора преимущество перед портом компьютера. У протоколов Ethernet и Fast Ethernet такой возможности нет, поэтому производители коммутаторов для этих очень популярных технологий используют два приема воздействия на конечные узлы.

Эти приемы основаны на том, что конечные узлы строго соблюдают все параметры

алгоритма доступа к среде, а порты коммутатора - нет.

Первый способ "торможения" конечного узла основан на так называемом агрессивном поведении порта коммутатора при захвате среды после окончания передачи очередного пакета или после коллизии. Эти два случая иллюстрируются рисунком ниже.



В первом случае коммутатор окончил передачу очередного кадра и вместо технологической паузы в 9.6 мкс сделал паузу в 9.1 мкс и начал передачу нового кадра. Компьютер не смог захватить среду, так как он выдержал стандартную паузу в 9.6 мкс и обнаружил после этого, что среда уже занята.

Во втором случае кадры коммутатора и компьютера столкнулись и была зафиксирована коллизия. Так как компьютер сделал паузу после коллизии в 51.2 мкс, как это положено по стандарту (интервал отсрочки равен 512 битовых интервалов), а коммутатор - 50 мкс, то и в этом случае компьютеру не удалось передать свой кадр.

Коммутатор может пользоваться этим механизмом адаптивно, увеличивая степень своей агрессивности по мере необходимости.

Второй прием, которым пользуются разработчики коммутаторов - это передача фиктивных кадров компьютеру в том случае, когда у коммутатора нет в буфере кадров для передачи по данному порту. В этом случае коммутатор может и не нарушать параметры алгоритма доступа, честно соревнуясь с конечным узлом за право передать свой кадр. Так как среда при этом равновероятно будет доставаться в распоряжение то коммутатору, то конечному узлу, то интенсивность передачи кадров в коммутатор в среднем уменьшится вдвое. Такой метод называется методом обратного давления (backpressure). Он может комбинироваться с методом агрессивного захвата среды для большего подавления активности конечного узла.

Метод обратного давления используется не для того, чтобы разгрузить буфер процессора порта, непосредственно связанного с подавляемым узлом, а разгрузить либо общий буфер коммутатора (если используется архитектура с разделяемой общей памятью), либо разгрузить буфер процессора другого порта, в который передает свои кадры данный порт. Кроме того, метод обратного давления может применяться в тех случаях, когда процессор порта не рассчитан на поддержку максимально возможного для протокола трафика. Один из первых примеров применения метода обратного давления как раз связан с таким случаем - метод был применен компанией LANNET в модулях LSE-1 и LSE-2, рассчитанных на коммутацию трафика Ethernet с максимальной интенсивностью соответственно 1 Мб/с и 2.

19. Возможности коммутатора по фильтрации трафика

Многие коммутаторы позволяют администраторам задавать дополнительные условия фильтрации кадров наряду со стандартными условиями их фильтрации в соответствии с информацией адресной таблицы. Пользовательские фильтры предназначены для создания дополнительных барьеров на пути кадров, которые ограничивают доступ определенных групп пользователей к определенным сервисам сети.

Если коммутатор не поддерживает протоколы сетевого и транспортного уровней, в которых имеются поля, указывающие к какому сервису относятся передаваемые пакеты, то администратору приходится для задания условий интеллектуальной фильтрации определять поле, по значению которого нужно осуществлять фильтрацию, в виде пары "смещение-размер" относительно начала поля данных кадра канального уровня. Поэтому, например, для того, чтобы запретить некоторому пользователю печатать свои документы на определенном принт-сервере NetWare, администратору нужно знать положение поля "номер сокета" в пакете IPX и значение этого поля для принт-сервиса, а также знать MAC-адреса компьютера пользователя и принт-сервера.

Обычно условия фильтрации записываются в виде булевских выражений, формируемых с помощью логических операций AND и OR.

Наложение дополнительных условий фильтрации может снизить производительность коммутатора, так как вычисление булевских выражений требует проведения дополнительных вычислений процессорами портов.

Кроме условий общего вида коммутаторы могут поддерживать специальные условия фильтрации. Одним из очень популярных видов специальных фильтров являются фильтры, создающие виртуальные сегменты.

Специальным является и фильтр, используемый многими производителями для защиты сети, построенной на основе коммутаторов.

20. Использование различных классов сервисов

Эта функция позволяет администратору назначить различным типам кадров различные приоритеты их обработки. При этом коммутатор поддерживает несколько очередей необработанных кадров и может быть сконфигурирован, например, так, что он передает один низкоприоритетный пакет на каждые 10 высокоприоритетных пакетов. Это свойство может особенно пригодиться на низкоскоростных линиях и при наличии приложений, предъявляющих различные требования к допустимым задержкам.

Так как не все протоколы канального уровня поддерживают поле приоритета кадра, например, у кадров Ethernet оно отсутствует, то коммутатор должен использовать какой-либо дополнительный механизм для связывания кадра с его приоритетом. Наиболее распространенный способ - приписывание приоритета портам коммутатора. При этом способе коммутатор помещает кадр в очередь кадров соответствующего приоритета в зависимости от того, через какой порт поступил кадр в коммутатор. Способ несложный, но недостаточно гибкий - если к порту коммутатора подключен не отдельный узел, а сегмент, то все узлы сегмента получают одинаковый приоритет. Примером подхода к назначению классов обслуживания на основе портов является технология PACE компании 3Com.

Более гибким является назначение приоритетов MAC-адресам узлов, но этот способ требует выполнения большого объема ручной работы администратором.

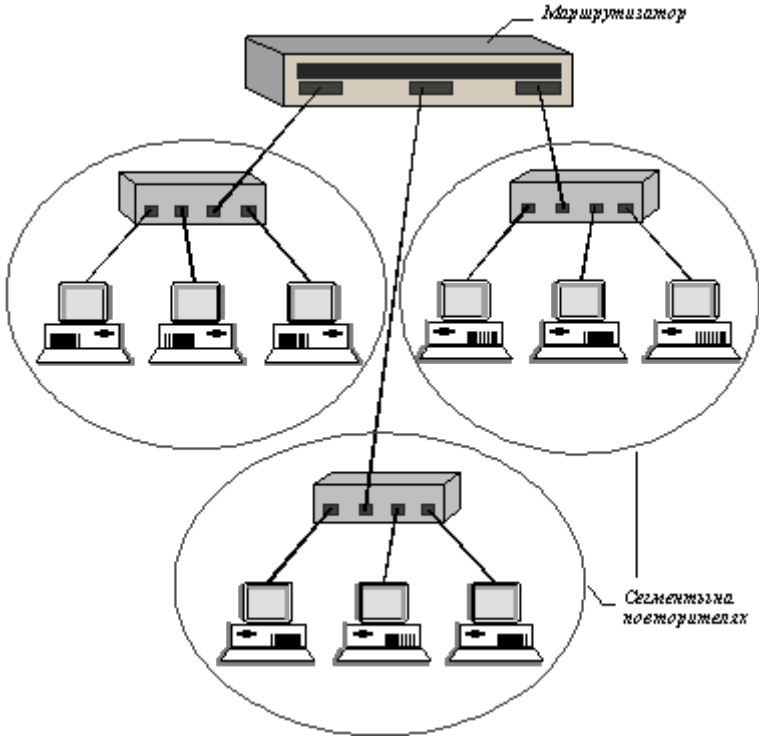
21. Поддержка виртуальных сетей

Кроме своего основного назначения - повышения пропускной способности связей в сети - коммутатор позволяет локализовывать потоки информации в сети, а также контролировать эти потоки и управлять ими, используя пользовательские фильтры. Однако, пользовательский фильтр может запретить передачи кадров только по конкретным адресам, а широковещательный трафик он передает всем сегментам сети. Так требует алгоритм работы моста, который реализован в коммутаторе, поэтому сети, созданные на основе мостов и коммутаторов иногда называют плоскими - из-за отсутствия барьеров на пути широковещательного трафика.

Технология виртуальных сетей (Virtual LAN, VLAN) позволяет преодолеть указанное ограничение. Виртуальной сетью называется группа узлов сети, трафик которой, в том числе и широковещательный, на канальном уровне полностью изолирован от других узлов сети. Это означает, что передача кадров между разными виртуальными сегментами на основании адреса канального уровня невозможна, независимо от типа адреса - уникального, группового или широковещательного. В то же время внутри виртуальной сети кадры передаются по технологии коммутации, то есть только на тот порт, который связан с адресом назначения кадра.

Говорят, что виртуальная сеть образует домен широковещательного трафика (broadcast domain), по аналогии с доменом коллизий, который образуется повторителями сетей Ethernet.

Назначение технологии виртуальных сетей состоит в облегчении процесса создания независимых сетей, которые затем должны связываться с помощью протоколов сетевого уровня. Для решения этой задачи до появления технологии виртуальных сетей использовались отдельные повторители, каждый из которых образовывал независимую сеть. Затем эти сети связывались маршрутизаторами в единую интерсеть



22. Технология Gigabit Ethernet

Внедрение услуг передачи голоса, данных и видеоинформации по единой мультисервисной сети привело к необходимости повышения пропускной способности линий связи. Поэтому была разработана технология *Gigabit Ethernet,* предусматривающая передачу данных со скоростью 1 Гбит/с. В данной технологии, так же как в Fast Ethernet, была сохранена преемственность с технологией Ethernet: практически не изменились форматы кадров, сохранился метод доступа CSMA/CD в полудуплексном режиме. На логическом уровне используется кодирование 8B/10B.

Поскольку скрость передачи увеличилось в 10 раз по сравнению с Fast Ethernet, то было необходимо либо уменьшить диаметр сети до 20-25м, либо увеличить минимальную длину кадра. В технологии GbE пошли по второму пути, увеличив минимальную длину кадра на 512 байт, вместо 64 байт в технологии Ethernet и FE. Диаметр сети остался равным 200м, так же как в FE. Поскольку на практике часто передаются короткие кадры, для снижения непроизводительной загрузки сети разрешается передавать несколько коротких кадров с общей длиной до 8192 байт.

Современные сети Gigabit Ethernet, как правило, строятся на основе коммутаторов и работают в полнодуплексном режиме. В этом случае говорят не о диаметре сети, а о длине сегмента, которая определяется физической средой передачи данных. GbE предусматривает использование:

- одномодового оптоволоконного кабеля (802.3z)
- многомодового оптоволоконного кабеля (802.3z)
- симметричного кабеля UTP категории 5 (802.3ab)
- коаксиального кабеля

Сравнительные характеристики спецификаций Gigabit Ethernet:

Спецификация	Среда	Расстояние
1000Base-LX	Волокно 10 мкм	5000м
	Волокно 50 мкм	500м
	Волокно 62.5 мкм	500м
1000Base-SX	Волокно 50 мкм	500м
	Волокно 62.5 мкм	300м
1000Base-T	Витая пара UTP, 5e	100м
1000Base-CX	Коаксиальный кабель	25м

23. Технология 10 Gigabit Ethernet

Технология 10GbE описывается стандартом IEEE802.3ae, которая определяет полнодуплексную передачу данных со скоростью 10 Гбит/с по волоконно-оптическому кадру. Максимальное расстояние передачи зависят от типа применяемого волокна. Используя одномодовое волокно как среду передачи, максимальное расстояние передачи - 40км.

Стандарт 10GbE на физическом уровне позволяет увеличить расстояние связи до 40км по одномодовому волокну и обеспечить совместимость с сетями синхронной цифровой иерархии и фотонными сетями, использующими уплотнение по длине волны DWDM. Функционирование на 40км, скорость передачи до 10Gbps и совместимость с системами SDH делает технологию 10GbE не только технологией локальных сетей, но и технологией глобальных сетей. Таким образом, стандарт развивается не только для LAN, но так же для MAN и WAN. Поскольку в технологии 10GbE задействована только полнодуплексная связь, в режиме CSMA/CD нет необходимости. Следовательно, в сетях исключается использование концентраторов hub.

Стандарт 802.3ae управляет семейством 10GbE, которое включает следующие новые технологии:

- 10GBASE-SR — для коротких расстояний по уже установленному многомодовому волокну, поддерживает связь на расстоянии от 26м до 82м
- 10GBASE-LX4 — использует технологию уплотнения по длине волны (WDM), поддерживает связь на расстоянии от 240м до 300м по уже установленному многомодовому волокну и до 10км по одномодовому волокну
- 10GBASE-LR и 10GBASE-ER — обеспечивает связь от 10км до 40км по одномодовому волокну
- 10GBASE-SW, 10GBASE-LW и 10GBASE-EW — технологии с общим названием 10GBASE-W, предназначены, чтобы обеспечить работу оборудования глобальных сетей с модулями SONET/SDH

Сравнительные характеристики спецификаций Gigabit Ethernet:

Спецификация	Длина волны	Волокно	Расстояние
10GBASE-LX4	1310 нм	62.5 мкм	2 - 300м
		50 мкм	2 - 300м
		10 мкм	2 - 10км
		62.5 мкм	2 - 33м
		50 мкм	2 - 300м
10GBASE-L	1310 нм	10 мкм	2 - 10км
10GBASE-E	1550 нм	10 мкм	2 - 40км

24. Виртуальные сети

VLAN (Virtual Local Area Network) — группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам. И наоборот, устройства, находящиеся в разных VLAN'ах, невидимы друг для друга на канальном уровне, даже если они подключены к одному коммутатору, и связь между этими устройствами возможна толька на сетевом или более высоком уровне.

В современных сетях VLAN — главный механизм для создания логической топологии сети, не зависящей от физической топологии. VLAN'ы используются для сокращения широковещательного трафика в сети. Имеют большое значение с точки зрения безопасности.

Виртуальная частная сеть (VPN) представляет собой подключение типа «точка-точка» в частной или общедоступной сети, например в интернете. VPN - клиенты используют специальные TCP/IP — протоколы, называемые туннельными протоколами, обеспечивающие установление защищенного канала обмена данными между двумя компьютерами. С точки зрения взаимодействующих компьютеров между ними организуется выделенный канал типа «точка-точка», хотя в действительности соответствующие данные передаются через Интернет, как и любые другие пакеты. При обычной реализации VPN клиент инициирует виртуальное подключение типа «точка-точка» к серверу удаленного доступа через Интернет. Сервер удаленного доступа отвечает на вызов, выполняет проверку подлинности вызывающей стороны и передает данные между VPN - клиентом и частной сетью организации.

Для эмуляции канала типа «точка-точка» к данным добавляется заголовок (выполняется инкапсуляция). Этот заголовок содержит сведения о маршрутизации, которое обеспечивает прохождение данных по общей или публичной сети до конечной точки. Для эмуляции частного канала и сохранения конфиденциальности передаваемые данные шифруются.

25. Создание виртуальных сетей

26. Управление коммутируемыми сетями

27. Управление виртуальными сетями

28. Сетевые адаптеры

Сетевой адаптер (Network Interface Card, NIC) - это периферийное устройство компьютера, непосредственно взаимодействующее со средой передачи данных, которая прямо или через другое коммуникационное оборудование связывает его с другими компьютерами. Это устройство решает задачи надежного обмена двоичными данными, представленными соответствующими электромагнитными сигналами, по внешним линиям связи. Как и любой контроллер компьютера, сетевой адаптер работает под управлением драйвера операционной системы и распределение функций между сетевым адаптером и драйвером может изменяться от реализации к реализации.

29. Этапы приема из кабеля в компьютер

Сетевой адаптер совместно с драйвером выполняют две операции: передачу и прием кадра. Передача кадра из компьютера в кабель состоит из перечисленных ниже этапов (некоторые могут отсутствовать, в зависимости от принятых методов кодирования):

- Прием кадра данных LLC через межуровневый интерфейс вместе с адресной информацией MAC-уровня. Обычно взаимодействие между протоколами внутри компьютера происходит через буферы, расположенные в оперативной памяти. Данные для передачи в сеть помещаются в эти буферы протоколами верхних уровней, которые извлекают их из дисковой памяти либо из файлового кэша с помощью подсистемы ввода-вывода операционной системы.
- Оформление кадра данных MAC-уровня, в который инкапсулируется кадр LLC (с отброшенными флагами 01111110). Заполнение адресов назначения и источника, вычисление контрольной суммы.
- Формирование символов кодов при использовании избыточных кодов типа 4B/5B. Скремблирование кодов для получения более равномерного спектра сигналов. Этот этап используется не во всех протоколах — например, технология Ethernet 10 Мбит/с обходится без него.
- Выдача сигналов в кабель в соответствии с принятым линейным кодом — манчестерским, NRZI, MLT-3 и т. п.

Прием кадра из кабеля в компьютер включает следующие действия:

- Прием из кабеля сигналов, кодирующих битовый поток.
- Выделение сигналов на фоне шума. Эту операцию могут выполнять различные специализированные микросхемы или сигнальные процессоры DSP. В результате в приемнике адаптера образуется некоторая битовая последовательность, с большой степенью вероятности совпадающая с той, которая была послана передатчиком.
- Если данные перед отправкой в кабель подвергались скремблированию, то они пропускаются через дескремблер, после чего в адаптере восстанавливаются символы кода, посланные передатчиком.
- Проверка контрольной суммы кадра. Если она неверна, то кадр отбрасывается, а через межуровневый интерфейс наверх, протоколу LLC передается соответствующий код ошибки. Если контрольная сумма верна, то из MAC-кадра извлекается кадр LLC и передается через межуровневый интерфейс наверх, протоколу LLC. Кадр LLC помещается в буфер оперативной памяти.

30. Классификация адаптеров

В качестве примера классификации адаптеров используем подход фирмы 3Com.

- *1-ое поколение*
  Адаптеры первого поколения были выполнены на дискретных логических микросхемах, в результате чего обладали низкой надежностью. Они имели буферную память только на один кадр, что приводило к низкой производительности адаптера, так как все кадры передавались из компьютера в сеть или из сети в компьютер последовательно. Кроме этого, задание конфигурации адаптера первого поколения происходило вручную, с помощью перемычек. Для каждого типа адаптеров использовался свой драйвер, причем интерфейс между драйвером и сетевой операционной системой не был стандартизирован.
- *2-ое поколение*
  В сетевых адаптерах второго поколения для повышения производительности стали применять метод многокадровой буферизации. При этом следующий кадр загружается из памяти компьютера в буфер адаптера одновременно с передачей предыдущего кадра в сеть. В режиме приема, после того как адаптер полностью принял один кадр, он может начать передавать этот кадр из буфера в память компьютера одновременно с приемом другого кадра из сети.
- *3-е поколение*
  В сетевых адаптерах третьего поколения осуществляется конвейерная схема обработки кадров. Она заключается в том, что процессы приема кадра из оперативной памяти компьютера и передачи его в сеть совмещаются во времени. Таким образом, после приема нескольких первых байт кадра начинается их передача. Это существенно (на 25—55 %) повышает производительность цепочки «оперативная память — адаптер — физический канал — адаптер — оперативная память». Такая схема очень чувствительна к порогу начала передачи, то есть к количеству байт кадра, которое загружается в буфер адаптера перед началом передачи в сеть. Сетевой адаптер третьего поколения осуществляет самонастройку этого параметра путем анализа рабочей среды, а также методом расчета, без участия администратора сети. Самонастройка обеспечивает максимально возможную производительность для конкретного сочетания производительности внутренней шины компьютера, его системы прерываний и системы прямого доступа к памяти.
- *4-ое поколение*
  Выпускаемые сегодня сетевые адаптеры можно отнести к четвертому поколению. В эти адаптеры обязательно входит ASIC, выполняющая функции MAC-уровня, скорость развита до 1 Гбит/сек, а также есть большое количество высокоуровневых функций. В набор таких функций может входить поддержка агента удаленного мониторинга RMON, схема приоритизации кадров, функции дистанционного управления компьютером и т. п. В серверных вариантах адаптеров почти обязательно наличие мощного процессора, разгружающего центральный процессор.

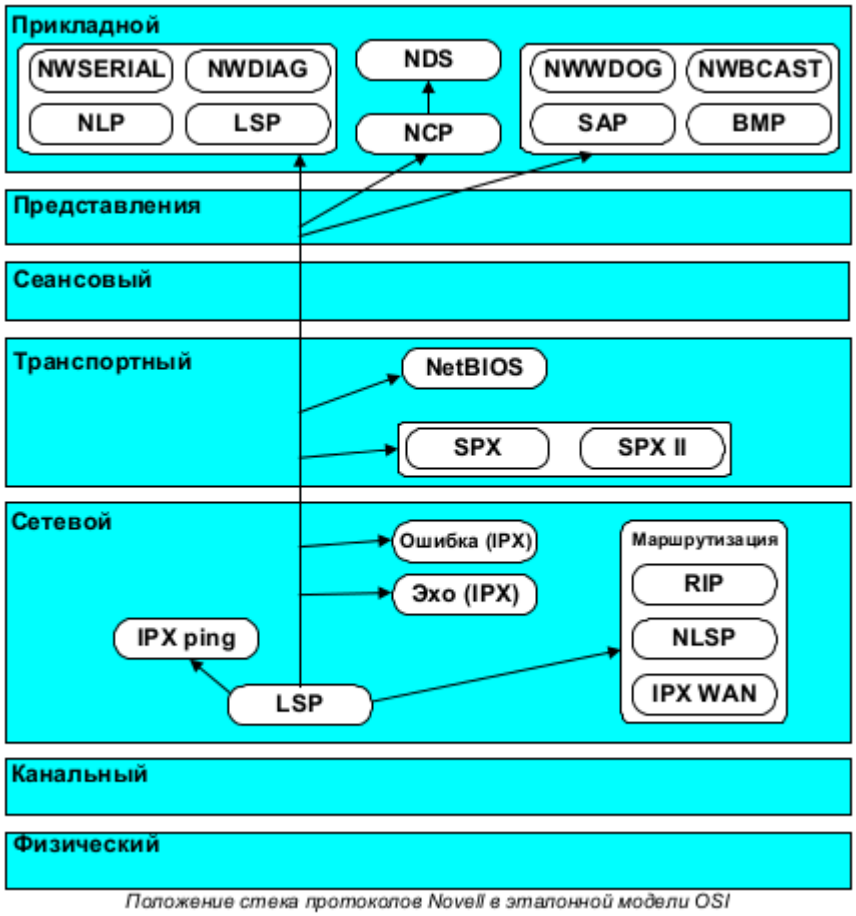
31. Протокол 3-его уровня IPX

IPX/SPX (Internetwork Packet eXchange/Sequenced Packet eXchange - межсетевой обмен пакетами/последовательный обмен пакетами) стек протоколов, используемый в сетях Novell NetWare. Протокол IPX обеспечивает сетевой уровень (доставку пакетов, аналог IP), SPX — транспортный и сеансовый уровни (аналог TCP).

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

Стек протоколов IPX/SPX был разработан Novell для ее проприетарной сетевой операционной системы NetWare. За основу IPX был взят протокол IDP из стека протоколов Xerox Network Services.

С конца 1980-х и до середины 1990-х годов сети на основе IPX были широко распространены из-за большой популярности NetWare. Однако в дальнейшем с развитием Интернета и стека TCP/IP оригинальный транспортный протокол SPX от Novell не способствовал успеху IPX-сетей. Из-за стремительного роста популярности сетей на основе TCP/IP, IPX в настоящее время имеют шансы исчезнуть.



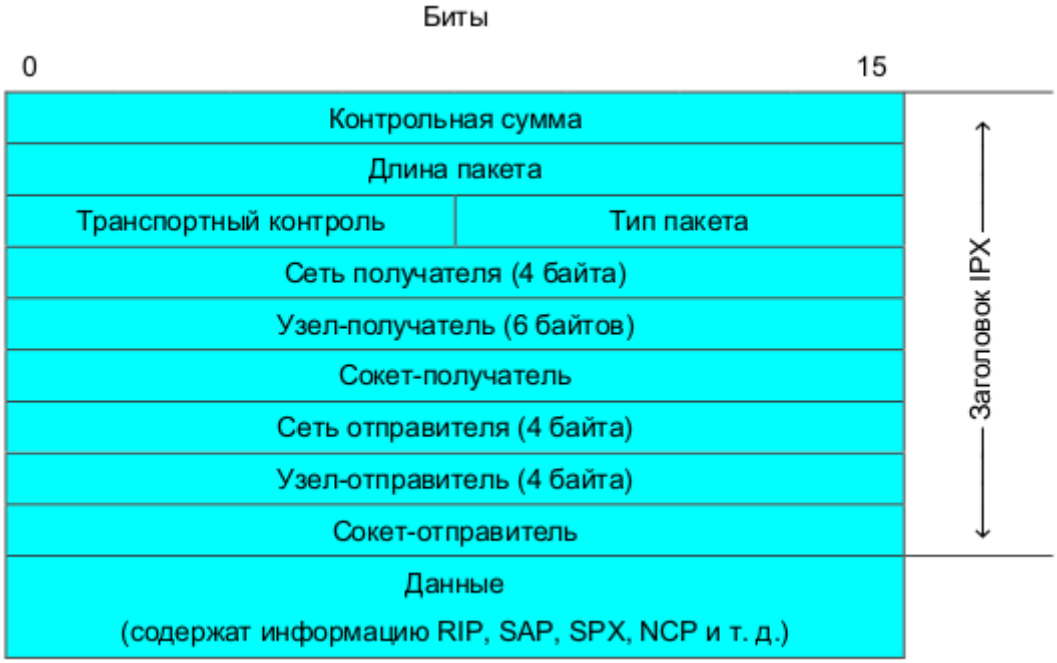
Положение стека протоколов Novell в эталонной модели OSI

SPX (Sequenced Packet eXchange) - протокол последовательного обмена пакетами. Это протокол транспортного уровня с соединением. Работает поверх сетевого протокола IPX. Предполагается, что перед отправкой сообщения между рабочими станциями устанавливается соединение. На уровне протокола SPX достоверность (надёжность) передачи информации резко возрастает. При неверной передаче пакета выполняется повторная его передача.

Протокол SPX используется для гарантированной доставки пакетов, в той последовательности, в которой они передавались передатчиком.

На рисунке справа показано расположение стека протоколов Novell в эталонной модели OSI.

32. Формат пакета протокола IPX



Контрольная сумма — содержит значение FFFFH.

Длина пакета — размер дейтаграммы IPX в откетах.

Транспортный контроль — данное поле используется маршрутизаторами, работающими с протоколом IPX. Перед передачей пакета протокол IPX устанавливает для этого поля нулевое значение.

Тип пакета — указывает тип информации, содержащейся в пакете:

- 0 — Hello или SAP
- 1 — RIP
- 2 — эхо-пакет
- 3 — пакет, содержащий информацию об ошибке
- 4 — NetWare 386 или SAP
- 5 — протокол SPX
- 16 - 31 — экспериментальные протоколы
- NetWare 286

Номер сети — это 32-битовое число, которое задает сетевой администратор. При локальном использовании сети (отсутствуют соединения с другими сетями IPX) для этого поля можно задать нулевое значение.

Номер узла — является 48-битовое число, идентичное аппаратному адресу сетевого адаптера. Для широковещательных сообщений используется номер узла FFFF FFFF FFFF. Адрес 0000 0000 0000 в NetWare версий 3.x и 4.x используется для сервера.

Номер сокета — 16-битовое поле, служащее для идентификации пакетов вышележащих уровне:

- 0451H - NCP.
- 0452H - SAP.

- 0453H - RIP.
- 0455H - NetBIOS.
- 0456H - Диагностика.
- 0x457 - Пакет проверки серийных номеров (SER).
- 4000-6000H - Номера сокетов, используемые для файл-серверов и сетевых соединений.

33. Маршрутизация протокола IPX

В целом маршрутизация протокола IPX выполняется аналогично маршрутизации протокола IP. Каждый IPX - маршрутизатор поддерживает таблицу маршрутизации, на основании которой принимается решение о продвижении пакета. IPX - маршрутизаторы поддерживает одношаговую маршрутизацию, при которой каждый маршрутизатор принимает решение только о выборе следующего на пути маршрутизатора. Возможности маршрутизации от источника в протоколе IPX отсутствуют.

Протокол IPX поддерживает использование двух различных протоколов маршрутизации дистанционно–векторный протокол RIP(Routing Information Protocol)и протокол состояния связей NLSP (NetWare Link Services Protocol).

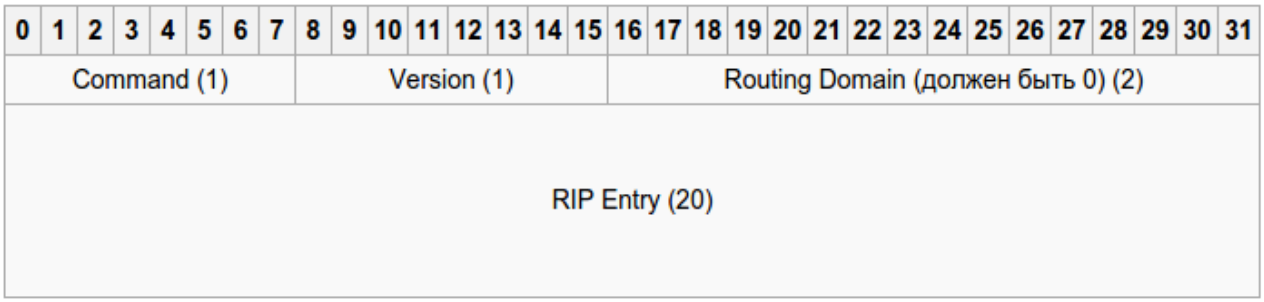
34. Характеристика RIP и IPX (не закончил)

Протокол маршрутной информации (Routing Information Protocol) — один из самых простых протоколов маршрутизации. Применяется в небольших компьютерных сетях, позволяет маршрутизаторам динамически обновлять маршрутную информацию (направление и дальность в хопах), получая ее от соседних маршрутизаторов.

RIP — так называемый протокол дистанционно-векторной маршрутизации, который оперирует транзитными участками в качестве метрики маршрутизации. Максимальное количество хопов, разрешенное в RIP — 15 (метрика 16 означает «бесконечно большую метрику»). Каждый RIP-маршрутизатор по умолчанию вещает в сеть свою полную таблицу маршрутизации раз в 30 секунд, довольно сильно нагружая низкоскоростные линии связи. RIP работает на 3 уровне (сетевой) стека TCP/IP, используя UDP порт 520.

В современных сетевых средах RIP — не самое лучшее решение для выбора в качестве протокола маршрутизации, так как его возможности уступают более современным протоколам, таким как EIGRP, OSPF. Ограничение на 15 хопов не дает применять его в больших сетях. Преимущество этого протокола — простота конфигурирования.

Формат:



- Command — команда, определяет назначение датаграммы (1 — request; 2 — response)
- Version — номер версии, в зависимости от версии, определяется формат пакета
- Routing Domain — идентификатор RIP-системы, к которой принадлежит данное сообщение; часто — номер автономной системы. Используется, когда к одному физическому каналу подключены маршрутизаторы из нескольких автономных систем, в каждой автономной системе поддерживается своя таблица маршрутов. Поскольку сообщения RIP рассылаются всем маршрутизаторам, подключенным к сети, требуется различать сообщения, относящиеся к «своей» и «чужой» автономным системам. Поле использовалось короткое время в версии протокола RIP-2. В протоколе RIP-1 и в текущей версии RIP-2 не используется.
- RIP Entry (RTE) — запись маршрутной информации RIP. RIP пакет может содержать от 1 до 25 записей RIP Entry.

35. Методы управления и анализа локальных сетей

Независимо от объекта *управления*, желательно, чтобы система управления выполняла ряд функций, которые определены международными стандартами, обобщающими опыт применения систем управления в различных областях. Существуют рекомендации ITU-T X.700 и близкий к ним стандарт ISO 7498-4, которые делят задачи системы управления на пять функциональных групп:

- *Управление конфигурацией сети и именованием (Configuration Management)*. Эти задачи заключаются в конфигурировании параметров как элементов сети (Network Element, NE), так и сети в целом. Для элементов сети, таких как маршрутизаторы, мультиплексоры и т. п., с помощью этой группы задач определяются сетевые адреса, идентификаторы (имена), географическое положение и пр.
  Для сети в целом управление конфигурацией обычно начинается с построения карты сети, то есть отображении реальных связей между элементами сети и изменении связей между элементами сети - образование новых физических или логических каналов, изменение таблиц коммутации и маршрутизации.
  Управление конфигурацией (как и другие задачи системы управления) могут выполняться в автоматическом, ручном или полуавтоматическом режимах. Чаще всего применяются полуавтоматические методы, когда автоматически полученную карту оператор подправляет вручную. Методы автоматического построения топологической карты, как правило, являются фирменными разработками.
- *Обработка ошибок (Fault Management)*. Эта группа задач включает выявление, определение и устранение последствий сбоев и отказов в работе сети. На этом уровне выполняется не только регистрация сообщений об ошибках, но и их фильтрация, маршрутизация и анализ на основе некоторой корреляционной модели, Фильтрация позволяет выделить из весьма интенсивного потока сообщений об ошибках, который обычно наблюдается в большой сети, только важные сообщения, маршрутизация обеспечивает их доставку нужному элементу системы управления, а корреляционный анализ позволяет найти причину, породившую поток взаимосвязанных сообщений (например, обрыв кабеля может быть причиной большого количества сообщений о недоступности сетей и серверов).
  Устранение ошибок может быть как автоматическим, так и полуавтоматическим. В первом случае система непосредственно управляет оборудованием или программными комплексами и обходит отказавший элемент за счет резервных каналов и т. п. В полуавтоматическом режиме основные решения и действия по устранению неисправности выполняют люди, а система управления только помогает в организации этого процесса - оформляет квитанции на выполнение работ и отслеживает их поэтапное выполнение (подобно системам групповой работы).
- *Анализ производительности и надежности (Performance Management).* Задачи этой группы связаны с оценкой на основе накопленной статистической информации таких параметров, как время реакции системы, пропускная способность реального или виртуального канала связи между двумя конечными абонентами сети, интенсивность трафика в отдельных сегментах и каналах сети, вероятность искажения данных при их передаче через сеть, а также коэффициент готовности сети или ее определенной

транспортной службы. Функции анализа производительности и надежности сети нужны как для оперативного управления сетью, так и для планирования развития сети.

- *Управление безопасностью (Security Management).* Задачи этой группы включают в себя контроль доступа к ресурсам сети (данным и оборудованию) и сохранение целостности данных при их хранении и передаче через сеть. Базовыми элементами управления безопасностью являются процедуры аутентификации пользователей, назначение и проверка прав доступа к ресурсам сети, распределение и поддержка ключей шифрования, управления полномочиями и т. п. Часто функции этой группы не включаются в системы управления сетями, а реализуются либо в виде специальных продуктов (например, системы аутентификации и авторизации Kerberos, различных защитных экранов, систем шифрования данных), либо входят в состав операционных систем и системных приложений.
- *Учет работы сети (Accounting Management).* Задачи этой группы занимаются регистрацией времени использования различных ресурсов сети - устройств, каналов и транспортных служб. Эти задачи имеют дело с такими понятиями, как время использования службы и плата за ресурсы - billing. Ввиду специфического характера оплаты услуг у различных поставщиков и различными формами соглашения об уровне услуг, эта группа функций обычно не включается в коммерческие системы и платформы управления типа HP Open View, а реализуется в заказных системах, разрабатываемых для конкретного заказчика.

Все многообразие средств, применяемых для *анализа* и диагностики вычислительных сетей, можно разделить на несколько крупных классов.

- Агенты систем управления, поддерживающие функции одной из стандартных MIB и поставляющие информацию по протоколу SNMP или CMIP. Для получения данных от агентов обычно требуется наличие системы управления, собирающей данные от агентов в автоматическом режиме.
- Встроенные системы диагностики и управления (Embedded systems). Эти системы выполняются в виде программно-аппаратных модулей, устанавливаемых в коммуникационное оборудование, а также в виде программных модулей, встроенных в операционные системы. Они выполняют функции диагностики и управления только одним устройством, и в этом их основное отличие от ценрализованных систем управления.
- Анализаторы протоколов (Protocol analyzers). Представляют собой програмные или аппаратно-программные системы, которые ограничиваются в отличие от систем управления лишь функциями мониторинга и анализа трафика в сетях. Хороший анализатор протоколов может захватывать и декодировать пакеты большого количества протоколов, применяемых в сетях, - обычно несколько десятков. Анализаторы протоколов позволяют установить некоторые логические условия для захвата отдельных пакетов и выполняют полное декодирование захваченных пакетов, то есть показывают в удобной для специалиста форме вложенность пакетов протоколов разных уровней друг в друга с расшифровкой содержания отдельных полей каждого пакета.

- Экспертные системы. Этот вид систем аккумулирует знания технических специалистов о выявлении причин аномальной работы сетей и возможных способах приведения сети в работоспособное состояние. Экспертные системы часто реализуются в виде отдельных подсистем различных средств мониторинга и анализа сетей: систем управления сетями, анализаторов протоколов, сетевых анализаторов.
- Оборудование для диагностики и сертификации кабельных систем. Условно это оборудование можно поделить на четыре основные группы: сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.
- Сетевые мониторы (называемые также сетевыми анализаторами) предназначены для тестирование кабелей различных категорий. Сетевые мониторы собирают также данные о статистических показателях трафика - средней интенсивности общего трафика сети, средней интенсивности потока пакетов с определенным типом ошибки и т. п. Эти устройства являются наиболее интеллектуальными устройствами из всех четырех групп устройств данного класса, так как работают не только на физическом, но и на канальном, а иногда и на сетевом уровнях.
- Устройства для сертификации кабельных систем выполняют сертификацию в соответствии с требованиями одного из международных стандартов на кабельные системы.
- Кабельные сканеры используются для диагностики медных кабельных систем.
- Тестеры предназначены для проверки кабелей на отсутствие физического разрыва.
- Многофункциональные портативные устройства анализа и диагностики. В связи с развитием технологии больших интегральных схем появилась возможность производства портативных приборов, которые совмещали бы функции нескольких устройств: кабельных сканеров, сетевых мониторов и анализаторов протоколов.

36. Архитектура систем управления локальных сетей

Основным элементом любой системы управления сетью является схема взаимодействия «менеджер — агент — управляемый объект». На основе этой схемы могут быть построены системы практически любой сложности с большим количеством агентов, менеджеров и ресурсов разного типа.

Чтобы можно было автоматизировать управление объектами сети, создается некоторая модель управляемого объекта, называемая базой данных управляющей информации (Management Information Base, MIB). MIB отражает только те характеристики объекта, которые нужны для его контроля. Например, модель маршрутизатора обычно включает такие характеристики, как количество портов, их тип, таблицу маршрутизации, количество кадров и пакетов протоколов канального, сетевого и транспортного уровней, прошедших через эти порты.

Менеджер и агент работают с одной и той же моделью управляемого объекта, однако в использовании этой модели агентом и менеджером имеются существенные различия.

Агент наполняет MIB управляемого объекта текущими значениями его характеристик, а менеджер извлекает из MIB данные, на основании которых он узнает, какие характеристики он может запросить у агента и какими параметрами объекта можно управлять. Таким образом, агент является посредником между управляемым объектом и менеджером. Агент поставляет менеджеру только те данные, которые предусматриваются MIB.

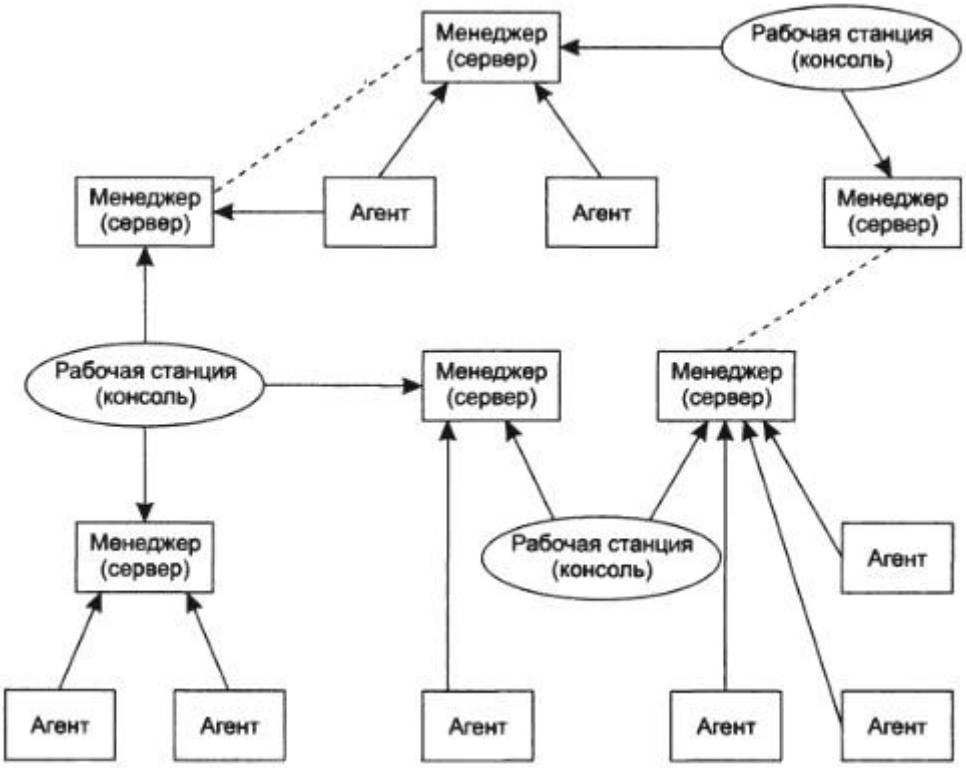
Менеджер и агент взаимодействуют по стандартному протоколу. Этот протокол позволяет менеджеру запрашивать значения параметров, хранящихся в MIB, а также передавать агенту информацию, на основе которой тот должен управлять объектом. Обычно менеджер работает на отдельном компьютере, взаимодействуя с несколькими агентами.

Агенты могут встраиваться в управляемое оборудование или работать на отдельном компьютере, связанном с управляемым оборудованием. Для получения требуемых данных об объекте, а также для выдачи на него управляющих воздействий агент должен иметь возможность взаимодействовать с ним. Однако многообразие типов управляемых объектов не позволяет стандартизовать способ взаимодействия агента с объектом. Эта задача решается разработчиками при встраивании агентов в коммуникационное оборудование или в операционную систему. Агент может снабжаться специальными датчиками для получения информации, например датчиками релейных контактов или датчиками температуры. Агенты могут отличаться разным уровнем интеллекта: обладать как самым минимальным

интеллектом, необходимым для подсчета проходящих через оборудование кадров и пакетов, так и весьма высоким, достаточным для самостоятельных действий по выполнению последовательности управляющих команд в аварийных ситуациях, построению временных зависимостей, фильтрации аварийных сообщений и т.п..

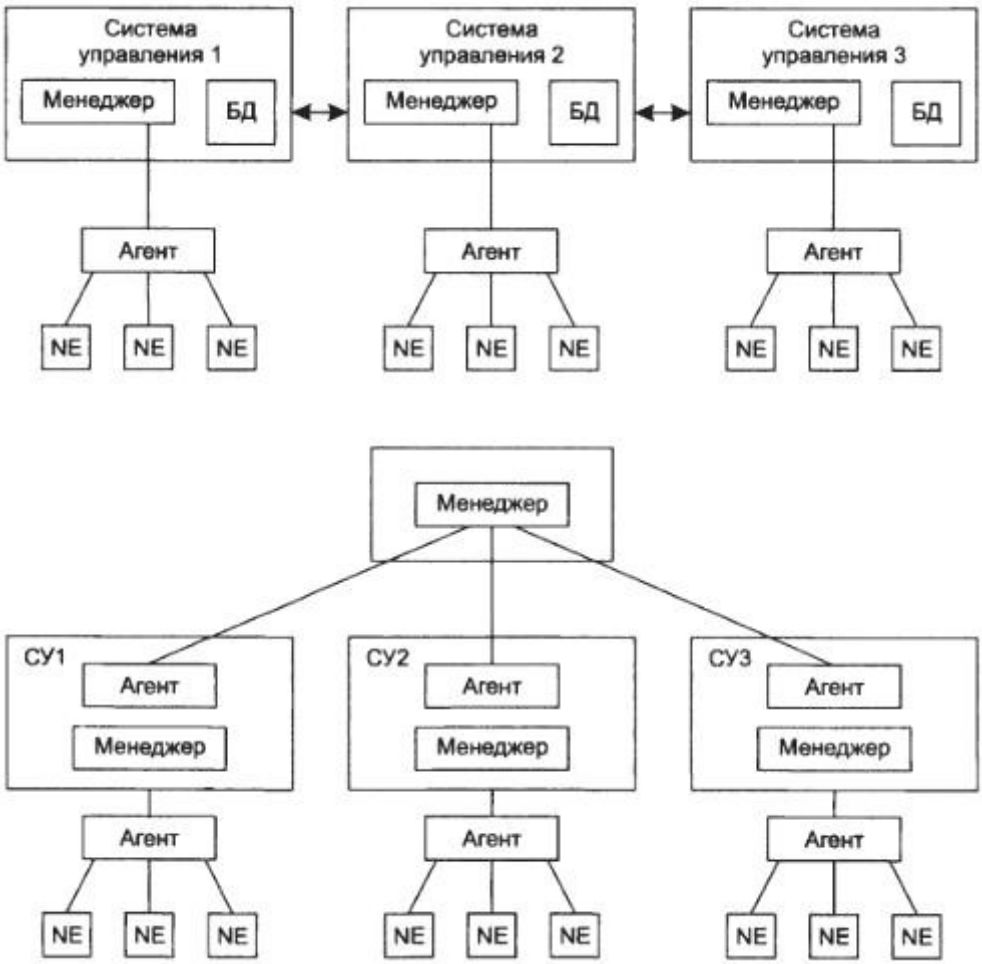
Различают внутриполосное управление, когда управляющие сигналы идут по тому же каналу, по которому передаются пользовательские данные, и внеполосное управление, то есть осуществляемое вне канала, по которому передаются пользовательские данные. Внутриполосное управление более экономично, так как не требует создания отдельной инфраструктуры передачи управляющих данных. Однако внеполосное управление на дежнее, так как соответствующее оборудование может выполнять свои функции даже тогда, когда те или иные сетевые элементы выходят из строя, и основные каналы передачи данных оказываются недоступными.

Схема «менеджер — агент — управляемый объект» позволяет строить достаточно сложные в структурном отношении распределенные системы управления:



Каждый агент, показанный на рисунке, управляет одним или несколькими элементами сети, параметры которых он помещает в соответствующую базу MIB. Менеджеры извлекают данные из баз MIB своих агентов, обрабатывают их и хранят в собственных базах данных. Операторы, работающие за рабочими станциями, могут соединиться с любым из менеджеров и с помощью графического интерфейса просмотреть данные об управляемой сети, а также выдать менеджеру некоторые директивы по управлению сетью или ее элементами.

Наличие нескольких менеджеров позволяет распределить между ними нагрузку по обработке данных управления, обеспечивая масштабируемость системы. Как правило, используются два типа связей между менеджерами, одноранговая и иерархическая.



В случае одноранговых связей каждый менеджер управляет своей частью сети на осно информации, получаемой от нижележащих агентов. Центральный менеджер отсутствуй Координация работы менеджеров достигается за счет обмена информацией между базан данных менеджеров. Одноранговое построение системы управления сегодня считает неэффективным и устаревшим.

Значительно более гибким является иерархическое построение связей между менеджер ми. Каждый менеджер нижнего уровня выполняет также функции агента для менедже верхнего уровня. Такой агент работает уже с укрупненной моделью MIB своей части сет В такой базе MIB собирается именно та информация, которая нужна менеджеру верхнє уровня для управления сетью в целом.

Модель «менеджер — агент — управляемый объект» лежит в основе таких популярні стандартов управления, как стандарты Интернета на основе протокола SNMP и станда ты управления ISO/OSI на основе протокола CMIP (Common Management Informarte Protocol — протокол общей управляющей информации).

37. Системы управления системой

Управление системами — это администрирование распределенных компьютерных систем масштаба предприятия. Выполнение множества функций необходимых для контроля, планирования, выделения, внедрения, координации и мониторинга ресурсов компьютерной сети. Включает в себя выполнение таких функций как начальное сетевое планирование, распределение частот, предопределение маршрутов трафика, управление конфигурацией, отказоустойчивостью, безопасностью, производительностью и учетной информацией. К наиболее известным системам управления системами относятся LANDesk, IBM Tivoli, Microsoft Systems Management Server, HP OpenView, Novell ZENworks и CA Unicenter.

Функциональные группы управления сетями:

- Управление конфигурации сети и именование (конфигурирование параметров, построение карты сети. Выполняется как автоматически так и вручную, но чаще используют полуавтоматические методы. Настройка коммутаторов и маршрутизаторов);
- Обработка ошибок (выполняется на корреляционной модели, устранение ошибок, этапы ремонта, тестирование работы);
- Анализ производительности и надежности (скорость, время отклика, LAN Analizer);
- Управление безопасностью (мониторинг сети, управление устройствами, обеспечение безопасности данных и защита ресурсы сети. Средства управления безопасностью осуществляют: шифрование и управление ключами расшифровки; регистрацию паролей; идентификацию пользователей; обслуживание и анализ файлов безопасности; защиту от компьютерных вирусов);
- Учет работы сети (включает регистрацию и управление используемыми ресурсами и устройствами).