РАЗДЕЛ 3. КОМПЬЮТЕРНЫЕ СЕТИ, ИНТЕРНЕТ, КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Тема 3.4. Межсетевые объединения

План:

1. Структуризация локальных сетей
2. Ограничения локальных средств структуризации сети
3. Объединения компьютерных сетей

1. Структуризация локальных сетей

Трафик в сети складывается случайным образом, однако в нем отражены и некоторые закономерности. Как правило, некоторые пользователи, работающие над общей задачей (например, сотрудники одного отдела) чаще всего обращаются с запросами либо друг к другу, либо к общему серверу, и только иногда они испытывают необходимость доступа к ресурсам компьютеров другого отдела.

Желательно, чтобы структура сети соответствовала структуре информационных потоков. В зависимости от сетевого трафика компьютеры в сети могут быть разделены на группы (сегменты сети). Компьютеры объединяются в группу, если большая часть порождаемых ими сообщений адресована компьютерам этой же группы.

Для разделения сети на сегменты используются мосты и коммутаторы. Они экранируют локальный трафик внутри сегмента, не передавая за его пределы никаких кадров, кроме тех, которые адресованы компьютерам, находящимся в других сегментах. Тем самым сеть распадается на отдельные "фрагменты". Это позволяет более рационально выбирать пропускную способность имеющихся линий связи, учитывая интенсивность трафика внутри каждого сегмента, а также активность обмена данными между сегментами.

Мост - представляет собой программно-аппаратный комплекс, который соединяет между собой отдельные сегменты одной сети. В локальных сетях в качестве моста используется компьютер, на котором установлены два (и более) сетевых адаптера, каждый из которых соединяется со своим сегментом сети.

Различают мосты внутренние/внешние, выделенные/совмещенные, локальные/удаленные.

Внутренний мост -располагается на файловом сервере.

Внешний мост – располагается на рабочей станции. Внешние мосты и их программное обеспечение устанавливаются в рабочей станции, которая не загружена функциями файлового сервера. Поэтому внешний мост может передавать данные более эффективно, чем внутренний.

Выделенный мост - это ПК, который используется только как мост и не может функционировать как рабочая станция.

Совмещенный мост - может функционировать и как мост, и как рабочая станция одновременно. Преимущество совмещенных мостов - ограничиваются издержки на пок3пку дополнительного компьютера, недостаток - ограничение возможностей рабочей станции, совмещенной с мостом (если какая-либо программа, запущенная на таком ПК, "зависает", прерывается также и работа моста - разделение данных между сетями и сеансы работы машин, которые связаны через мост с файловым сервером).

Локальный мост - передает данные между сегментами локальной сети, которые расположены в пределах ограничений кабеля по расстоянию.

Удаленный мост - применяется, когда расстояние не позволяет соединять сети посредством кабеля, если ограничение по длине кабеля для локального моста будет превышено. Удаленный мост использует промежуточную среду передачи (телефонные линии) для соединения с удаленной сетью или удаленными ПК. При связи сети с удаленной сетью необходимо установить мост на каждом конце соединения, а при связи сети с удаленным ПК требуется только мост, установленный в сети.

Коммутатор **-** центральное устройство сети (многопортовый концентратор), пересылающий пакеты конкретным портам, вместо широковещательной рассылки, выполняемой обычными концентраторами, каждого пакета в каждый порт. Таким путем соединения между портами достигают максимально возможной пропускной способности.

Коммутатор позволяет делить сеть на сегменты и предотвращать ненужный поток данных из одного сегмента в другой. Либо в случае, если идет обращение клиента из одного сегмента в другой, направлять кадры только по тем сегментам, в которых присутствуют адреса отправителя и получателя. В обычных некоммутируемых сетях каждый раз, когда какое-либо устройство начинает передавать данные, т.е. обращается к сети, другие устройства уже не могут этого сделать. Это позволяет избежать коллизий в сети. И хотя данный метод сохраняет целостность передаваемых данных, он не улучшает общую производительность сети. Коммутаторы же позволяют обращаться к сети нескольким подключенным к нему устройствам. Таким образом, увеличивается скорость работы и уменьшаются задержки.

Вообще, главное отличие коммутаторов от концентраторов заключается в том, что коммутатор при подключении к нему других устройств динамически создает таблицу из пар их аппаратных адресов и соответствующих им своих портов. Таким образом, когда коммутатор принимает кадр, он просматривает, кому этот кадр предназначается, находит в своей коммутационной таблице соответствующий аппаратный адрес и порт, к которому подключено устройство с таким адресом, и отправляет этот кадр через обнаруженный порт.

Использование коммутатора в сети позволяет сократить задержку реагирования сети, ускорить передачу файлов, уменьшить количество коллизий и других ошибок при передаче данных, существенно упростить процесс управления большой сетью. Современные коммутаторы поддерживают такие средства, как назначение приоритетов трафика (что особенно важно при передаче в сети речи или видео), функции управления сетью и управление многоадресной рассылкой.

2. Ограничения локальных средств структуризации сети

Локализация трафика средствами мостов и коммутаторов имеет существенные ограничения. С одной стороны, логические сегменты сети, расположенные между мостами, недостаточно изолированы друг от друга, а именно, они не защищены от так называемых *широковещательных штормов*. В случае, если какая-либо станция посылает широковещательное сообщение, то это сообщение передается всем станциям всех логических сегментов сети. Защита от широковещательных штормов в сетях, построенных на основе мостов, имеет количественный, а не качественный характер: администратор просто ограничивает количество широковещательных пакетов, которое разрешается генерировать некоторому узлу.

С другой стороны, использование *механизма виртуальных сегментов*, реализованного в коммутаторах локальных сетей, приводит к полной локализации трафика - такие сегменты полностью изолированы друг от друга, даже в отношении широковещательных кадров. Поэтому в сетях, построенных только на мостах и коммутаторах, компьютеры, принадлежащие разным виртуальным сегментам, не образуют единой сети. Приведенные недостатки мостов и коммутаторов связаны с тем, что они работают по протоколам канального уровня, в которых в явном виде не определяется понятие части сети (подсети), которое можно было бы использовать при структуризации большой сети.

Среди протоколов канального уровня некоторые обеспечивают доставку данных в сетях с произвольной топологией, но только между парой соседних узлов (например, протокол PPP), а некоторые - между любыми узлами (например,Ethernet), но при этом сеть должна иметь топологию определенного и весьма простого типа, например, древовидную.

При объединении в сеть нескольких сегментов с помощью мостов или коммутаторов продолжают действовать ограничения на ее топологию: в получившейся сети должны отсутствовать петли. Действительно, мост или его функциональный аналог - коммутатор - могут решать задачу доставки пакета адресату только тогда, когда между отправителем и получателем существует единственный путь. Между тем наличие избыточных связей, которые и образуют

петли, часто необходимо для лучшей балансировки нагрузки, а также для повышения надежности сети за счет существования альтернативного маршрута в дополнение к основному.

3. Объединение компьютерных сетей

Принципы объединения сетей

Современные вычислительные сети часто строятся с использованием нескольких различных базовых технологий - Ethernet, Token Ring или FDDI. Такая неоднородность возникает либо при объединении уже существовавших ранее сетей, использующих в своих транспортных подсистемах различные протоколы канального уровня, либо при переходе к новым технологиям.Когда две или более сетей организуют совместную транспортную службу, то такой режим взаимодействия обычно называют *межсетевым взаимодействием* (internetworking). Для обозначения составной сети в англоязычной литературе часто также используется термин *интерсеть* (internetwork или internet).

Для образования единой транспортной системы, объединяющей несколько сетей с различными принципами передачи информации между конечными узлами, служит сетевой уровень. Сетевой уровень позволяет передавать данные между любыми, произвольно связанными узлами сети. Таким образом, объединение различных компьютерных сетей основано на использовании протоколов сетевого уровня.

Протоколы канального уровня не позволяют строить сети с развитой структурой, например, сети, объединяющие несколько сетей предприятия в единую сеть, или высоконадежные сети, в которых существуют избыточные связи между узлами. Сетевой уровень вводится для того, чтобы, с одной стороны, сохранить простоту процедур передачи пакетов для типовых топологий, а с другой стороны, допустить использования произвольных топологий. Основная идея введения сетевого уровня состоит в том, чтобы оставить технологии, используемые в объединяемых сетях, в неизменном виде, но добавить в кадры канального уровня дополнительную информацию - заголовок сетевого уровня, на основании которого можно было бы находить адресата в сети с любой базовой технологией. Заголовок пакета сетевого уровня имеет унифицированный формат, не зависящий от форматов кадров канального уровня тех сетей, которые могут входить в объединенную сеть.

Заголовок сетевого уровня должен содержать адрес назначения и другую информацию, необходимую для успешного перехода пакета из одной сети в другую сеть. К такой информации может относиться, например:

- номер фрагмента пакета, нужный для успешного проведения операций сборки-разборки фрагментов при соединении сетей с разными максимальными размерами кадров канального уровня;
- время жизни пакета, указывающее, как долго от путешествует по интерсети, это время может использоваться для уничтожения "заблудившихся" пакетов;
- информация о наличии и о состоянии связей между сетями, помогающая узлам сети и маршрутизаторам рационально выбирать межсетевые маршруты;
- информация о загруженности сетей, также помогающая согласовать темп посылки пакетов в сеть конечными узлами с реальными возможностями линий связи на пути следования пакетов;
- качество сервиса - критерий выбора маршрута при межсетевых передачах - например, узел-отправитель может потребовать передать пакет с максимальной надежностью, возможно, в ущерб времени доставки.

В качестве адресов отправителя и получателя в составной сети используется не MAC-адрес, а IP-адрес, содержащий информацию о номере сети и номере компьютера в данной сети. В канальных протоколах поле "номер сети" отсутствует - предполагается, что все узлы принадлежат одной сети. Явная нумерация сетей позволяет протоколам сетевого уровня составлять точную карту межсетевых связей и выбирать рациональные маршруты при любой их топологии, используя альтернативные маршруты, если они имеются, что не умеют делать мосты. Таким образом, внутри сети доставка сообщений регулируется канальным уровнем. А доставкой пакетов между сетями занимается сетевой уровень.