Лекция 3. КОММУНИКАЦИОННОЕ ОБОРУДОВАНИЕ. КОММУТУТОРЫ

Основные положения

1. **Общие характеристики коммуникационного оборудования проводной связи в локальных сетях**

Рассмотрим основные характеристики коммуникационного оборудования проводных сетей. В этом разделе рассмотрим некоторые виды коммутационного оборудования локальных сетей и особенности их работы.

Концентратор (анг. hub)

Назначение: объединение устройств в сеть.

Принцип работы: объединяет узлы на физическом уровне, усиливает сигнал, некоторые концентраторы могут согласовывать параметры сигнала. Поступающие сообщения концентратор копирует во все порты, предоставляя подключенным устройствам фильтровать трафик по назначению. Концентратор фактически предоставляет узлам общую среду передачи данных.

Особенности передачи трафика: никакого анализа трафика или его обработки не производится. Производит усиление сигнала.

Обработка широковещательных сообщений: рассылаются без ограничений.

Коммутаторы 2-го уровня (анг. L2 switch)

Назначение: объединение устройств в сеть.

Принцип работы: объединяет узлы на канальном уровне. Проходящие кадры фильтруются и продвигаются согласно адресной информации (MAC-адресам), содержащейся в их заголовках. Упрощенно принцип работы коммутатора 2-го уровня сводится к составлению и поддержанию в актуальном состоянии таблицы принадлежности адресов устройств к портам коммутатора и последующей фильтрации проходящего трафика согласно таблице.

Особенности передачи трафика: поступающий на порт коммутатора кадр записывается только в тот порт, к которому подключено устройство с адресом назначения. Остальные порты коммутатора свободны и могут участвовать в обмене данными между друг другом. В случае, если в таблице нет данных об адресе назначения, кадр записывается во все порты устройства. Адресная информация в заголовке кадра канального уровня не изменяется.

Обработка широковещательных сообщений: рассылаются без ограничений.

Маршрутизатор (анг. router)

Назначение: объединение устройств в сети, работа в качестве узловых точек сети, объединение сегментов сетей в составную сеть.

Принцип работы: объединяет устройства на сетевом уровне. Входящий кадр при поступлении на принимающий порт маршрутизатора подвергается деинкапсуляции на канальном уровне. Адресная информация, содержащаяся в заголовке сетевого пакета, используется для выбора маршрута передачи (порта маршрутизатора через который и шлюза, на который необходимо передать сетевой пакет). Решение принимается на основе записей таблицы маршрутизации, которые могут заноситься в нее вручную или с использованием специальных протоколов маршрутизации. Пакет инкапсулируется в новый кадр канального уровня.

Особенности передачи трафика: единицей передачи данных выступает сетевой пакет. Он передается в порт, определенный по таблице маршрутизации и подвергается инкапсуляции в кадр канального уровня. В качестве адреса назначения канального уровня выступает MAC адрес шлюза.

Обработка широковещательных сообщений: широковещательный трафик канального уровня не передается.

Коммутатор 3-го уровня (анг. L3 switch)

Назначение: объединение устройств в сети, работа в качестве узловых точек сети, объединение сегментов сетей в составную сеть.

Принцип работы: может работать в режиме коммутатора 2-го уровня. В режиме коммутатора 3-го уровня осуществляет коммутацию на основе таблиц коммутации, составленных относительно адресов сетевого уровня. Эти таблицы могут составляться автоматически, путем наблюдения трафика, вручную или с использованием протоколов маршрутизации. За счет аппаратной реализации большинства операций и отсутствие необходимости деинкапсуляции-инкапсуляции сетевых сообщений, в большинстве случаев работает быстрее маршрутизатора.

Особенности передачи трафика: кадр может передаваться без изменения адресной информации.

Обработка широковещательных сообщений: сообщения могут передаваться или фильтроваться в зависимости от настроек.

2. Топологические ограничения сети, построенной на неуправляемых коммутаторах L2

Локальная сеть может строиться путем соединения нескольких коммутаторов через сетевые порты. При построении сети на неуправляемых коммутаторах L2 следует выполнять следующее топологическое правило: топология такой сети должна из себя представлять односвязный граф. Это требование обусловлено особенностями передачи кадров и алгоритмом работы коммутаторов.

Рассмотрим ключевые моменты.

a. Передача одноадресной рассылки. Когда осуществляется передача от узла к узлу, кадр проходит по сети до конечного узла. После доставки кадр не транслируется. Если в сети есть топологическая петля, то кадр одноадресной рассылки будет ретранслироваться (ходить по петле). Коммутатор на входе петли будет перестраивать таблицу коммутации, так как кадр от узла источника будет приходить с порта, к которому подключен узел и с порта, который учувствует в петле. Перестройка таблицы отрицательно сказывается на производительности коммутатора и на надежности доставки кадров.
b. Передача широковещательного трафика. Коммутаторы должны передавать широковещательный (broadcast) и ограничено широковещательный (multicast) трафик без ограничений, по всем портам. Кадры такого трафика принимаются узлами и не ретранслируются. Если в топологии присутствует петля, то такие кадры будут постоянно ходить по сети. Постепенно такой широковещательный трафик накапливается и полностью занимает пропускную способность сети, не оставляя «места» для полезного трафика. Если петель несколько – то кадры множатся. Ситуация заполнения сети ошибочным широковещательным трафиком называется широковещательным штормом.

Эти обстоятельства диктуют топологическое правило. Отметим, что существуют технологии (STP, RSPT), которые позволяют безопасно строить сети с топологическими петлями.

3. Основные технологии коммутаторов

Функции коммутаторов 2 уровня

a. Spanning Tree Protocol (приблизительный перевод - связующее дерево) – описывается стандартами IEEE 802.1d (STP), IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), IEEE 802.1s Multiple Spanning Tree Protocol (MSTP). Технология позволяет использовать сложносвязанные топологии сетей основанных на коммутаторах. STP

снимет ограничение на использование только древовидных топологий в таких сетях. Принцип работы заключается в выделении логического древовидного графа в сложносвязанном графе реальной сети. Технология применяется для повышения отказоустойчивости ЛВС или для реализации резервных каналов связи между несколькими ЛВС.

b. Автоопределение типа кабеля MDI/MDI-X – позволяет автоматически определить тип соединения в подключенном кабеле витая пара (прямой или кроссовый).
c. Автосогласование между режимами Full-duplex или Half-duplex – автоматическое определение возможного режима передачи данных по линии. В режиме Full-duplex данные передаются в двух направлениях одновременно по разным парам. При режиме Half-duplex данные могут передаваться только в одну сторону одновременно. Функция автосогласования между режимами позволяет избежать проблем с использованием разных режимов на разных устройствах.
d. Агрегация каналов (анг. Link aggregation for parallel links или pool) – описывается стандартом IEEE 802.3ad и предназначена для повышения пропускной способности канала за счет объединения нескольких портов в один высокоскоростной порт с суммарной скоростью объединенных портов.
e. Виртуальные локальные сети (анг. VLAN) – описывается стандартом IEEE 802.1q и позволяет внутри одной физической локальной сети построить несколько отдельных логических сетей (виртуальных сетей), узлы которых изолированы от остальных участков сети.
f. Возможность установки в стойку (анг. rackmount) – возможность установки коммутатора в стойку или в коммутационный шкаф. Наибольшее распространение получили 19 дюймовые шкафы и стойки, которые стали для современного сетевого оборудования стандартом де-факто.
g. Возможность установки дополнительных модулей – эта возможность подразумевать наличие слотов расширения или портов подключения внешних модулей, позволяющие разместить дополнительные интерфейсы. В качестве дополнительных интерфейсов выступают гигабитные модули, использующие витую пару, и оптические интерфейсы, способные передавать данные по оптоволоконному кабелю.
h. Диагностика кабеля – технология, позволяющая контролировать состояние подключенных кабелей на основе медной витой пары или оптических линий. При помощи этой функции может быть определено местонахождение коротких замыканий, разрывов, несовпадений волнового сопротивления.
i. Зеркалирование портов (анг. Port Mirroring)- технология, позволяющая перенаправлять весь трафик с одного (One-to-One) или с нескольких (Many-to-One) портов на единственный порт коммутатора. Технология применяется для содержательного анализа сетевого трафика, проходящего через коммутатор.
j. Объединение в стек – технология, позволяющее объединять через специальные физические интерфейсы нескольких коммутаторов в одно логическое устройство. Стекирование целесообразно производить, когда в итоге требуется получить коммутатор с большим количеством портов (больше 48 портов). Различные производители коммутаторов используют свои фирменные технологии стекирования, к примеру, Cisco использует технологию стекирования StackWise (шина между коммутаторами 32 Гбит/сек) и StackWise Plus (шина между коммутаторами 64 Гбит/сек).
k. Приоритетизация трафика по тегам (анг. Priority tags) – описывается стандартом IEEE 802.1p и позволяет отсортировать кадры по степени важности, выставив

приоритеты. Более приоритетные кадры будут отправляться в первую очередь, например, высокий приоритет выставляется пакетам VoIP и низкий — пакетам FTP.

l. Сбор статистики – одна из основных функций сетевого оборудования, дающая возможность анализировать трафик, тем самым выявлять уязвимые места инфраструктуры и в кратчайшие сроки ликвидировать их. Существую стандарты на данные статистики, например NetFlow от компании CISCO.
m. Удаленное управление – возможность конфигурирования устройства через сетевое соединение, например средствами протокола SNMP (Simple Network Management Protocol), через встроенный в устройство Web-сервер или через консольный доступ, осуществляемый через ssh или telnet. Консольный доступ может осуществляться через локальные интерфейсы, такие как RS232 (COM-порт).
n. Управление потоком (анг. Flow Control) – описывается стандартов IEEE 802.3x и обеспечивает защиту от потерь пакетов при их передаче по сети. Принцип действия упрощенно заключается в согласовании работы взаимодействующих устройств, когда передающее и принимающее устройство согласуют интенсивность потока кадров в случае переполнения буфера приемника.
o. Управляемое питание по витой паре (Power over Ethernet/PSE) – описывается стандартом IEEE 802.af. Функция позволяет обеспечить питание (до 15,4 Ватт на порт) подключенных к коммутатору устройств таких, как IP-камеры, Wi-Fi точки доступа, IP-телефоны или многофункциональные терминалы.
p. Фильтрация многоадресных рассылок – технология, позволяющая фильтровать широковещательные рассылки канального уровня, которые обычно передаются без ограничений по всем портам коммутатора. Применяется для оптимизации трафика в крупных сетях.
q. Фильтрация трафика по MAC адресам – технология, позволяющая составлять ACL (списки контроля доступа) по отношения к адресам канального уровня. Используется для привязки подключенных устройств к порту коммутатора или для разрешения передачи трафика от определенных устройств на выбранный порт.

Функции коммутаторов 3-го уровня

r. L3 коммутация – упрощенно, возможность коммутатора проводить продвижение пакетов не на основе MAC адресов, а на основе IP адресов.
s. Поддержка протоколов маршрутизации – составление таблиц коммутации с помощью протоколов маршрутизации.
t. Фильтрация по параметрам IP и TCP\UDP – осуществление фильтрации трафика по алгоритмам формального межсетевого экрана, т.е. основываясь на значении IP адресов или портов TCP \ UDP.

4. Типовая архитектура корпоративной сети

Современные корпоративные сети строятся по иерархическому принципу.

Согласно этому подходу, сеть делится на три основных уровня:

- Уровень доступа (Access Layer).
- Уровень распределения (Distribution Layer).
- Уровень ядра/базовый уровень (Core Layer).

Эти три уровня предоставляют различные функции и возможности. В зависимости от необходимости могут применяться один, два или все три уровня. Например для офиса с количеством пользователей менее 10 имеет смысл внедрять только уровень доступа. Для большой организации, занимающей несколько этажей или целое здание, будет разумным применение как уровня доступа, так и уровня распределения. Для огромных сетей, объединяющих

несколько зданий необходимы все три уровня: уровень доступа, уровень распределения и уровень ядра.

Уровень доступа (Access Layer) - предоставляет пользователям или устройствам (принтер, сканер, ip-телефон) доступ к сети. В качестве коммутаторов могут применяться даже не управляемые коммутаторы L2, однако целесообразнее применять управляемые устройства, так как можно реализовывать механизмы VLAN и QoS.
Уровень распределения (Distribution Layer) - агрегирует/объединяет уровни доступа и предоставляет доступ к различным сервисам организации. Применяются управляемые коммутаторы L3. Для дублирования линий связи применяется STP или агрегация каналов. Решаются вопросы безопасности (ACL на основе MAC или IP) и защиты от основных атак.
Уровень ядра/базовый уровень (Core Layer) - агрегирует/объединяет уровни распределения в больших сетях. Применяются коммутаторы L3 большой производительности. Основная задача слоя – быстрая и надёжная связь крупных участков сети. Обязательно используется дублирование линий связи через STP, RSPT или протоколы маршрутизации сетевого уровня.

Основные термины

1. Hub – то же что и концентратор.
2. MAC адрес – аппаратный адрес сетевого интерфейса на канальном уровне.
3. Switch - то же что и коммутатор.
4. Кадр – сообщение канального уровня.

Дополнительная литература

1. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Юбилейное издание. СПб.: Питер, 2020 г.
2. Коммутаторы D-Link http://dlink.ru/ru/products/1/
3. Design Zone for Campus Wired and Wireless LAN https://www.cisco.com/c/en/us/solutions/design-zone/networking-design-guides/campus-wired-wireless.html