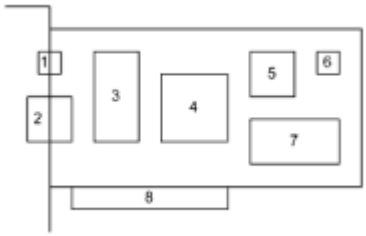
1 Назначение и структура сетевых адаптеров

Сетевые адаптеры -- Network Interface Cards (NICs) предназначены для подключения пользовательских станций, то есть клиентских и серверных компьютеров, к КС.

Где показано примерное расположение следующих компонентов:



1. Блок индикации (обычно выражен в: link LED, speed LED и act LED; первые два часто совмещают; единых правил индикации нет).

2. Разъем для подключения к СрПД.

3. Блок «развязки » для подключения к определенной СрПД, то есть приемопередатчик (transceiver).

4. Собственно сетевой контроллер (микросхема большой степени интеграции).

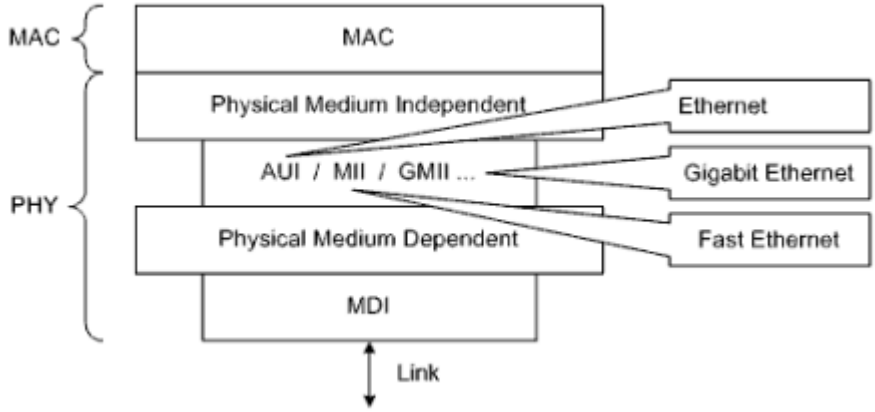
5. Блок перемычек (можно устанавливать: номер прерывания, адреса портов ввода - вывода и памяти; если адаптер PNP, то отсутствует).

6. ПЗУ для хранения настроек по умолчанию (обычно подключается по шине I2C).

7. Гнездо для boot ROM либо boot ROM.

8. Разъем для подключения к шине расширения компьютера (PCI либо другая).

2 Соответствие компонентов сетевых адаптеров модели OSI



Где: AUI -- Attachment Unit Interface, MII -- Medium Independent Interface, MDI -- Medium Dependent Interface, GMII -- Gigabit MII.

Блок PHY (PHYsical), он же трансивер, не обязательно интегрирован в кристалл контроллера -- он может быть изготовлен на основе отдельной микросхем.

В случае с Ethernet структура PHY постепенно претерпевала изменения и, в результате, собственно внешний трансивер (как и внутренний) может подключаться по-разному.

На практике, при подключении внешних трансиверов, интерфейсы AUI и MII соответствуют физическим разъемам (DA-15 плюс кабель, и сорокаконтактные разъемы D Miniature соответственно).

Ситуация с интерфейсом GMII и его модификациями иная. После появления Gigabit Ethernet широкое применение нашли трансиверы: сначала GBIC (GigaBit Interface Converter), затем SFP (Small Form-factor Pluggable), и затем SFP+ (уже 10 Gigabit Ethernet). При этом физическое подключение происходит через интерфейс SGMII (Serial GMII), а преобразования данных между GMII и SGMII (serialization/deserialization) выполняет блок PMA (Physical Medium Attachment). Внешние трансиверы обычно подключают к коммутаторам. Сам контроллер также может быть интегрирован, например, в IOCH. Контроллер может располагаться как на плате сетевого адаптера, так и на материнской плате -- LOM (LAN On Motherboard).

3 Характеристики и критерии выбора сетевых адаптеров

1. СрПД.
2. Область применения: desktop, server, mobile.
3. Степень интеграции: add-on, on-board.
4. Управляемость: management, unmanagement.
5. Режим работы: half duplex, full duplex.
6. Технические характеристики: размеры буферов и так далее.
7. Количество предоставляемых сетевых интерфейсов: single, dual, quad.
8. Дополнительные возможности: аппаратная поддержка шифрования, сбор статистики и другое.
9. Возможности энергосбережения: ACPI, WOL и другие.
10. Вариант поставки: OEM, Retail.

4 Поколения сетевых адаптеров

1. Шина XT; 8 битов; дискретная элементная база; управление перемычками; подключение к толстому коаксиальному кабелю; внешние приемопередатчики; NE1000-compatible и другие

2. Шина ISA; 16 битов; дискретная элементная база; управление перемычками; подключение к тонкому коаксиальному кабелю; NE2000- compatible и другие.

3. Шина ISA, либо EISA, либо MCA, либо PCI, либо другая; 16 либо 32 бита; индикация; появившиеся контроллеры большой степени интеграции; управление как перемычками, так и с помощью PNP; подключение как к тонкому коаксиальному кабелю, так и к витой паре; UMC UM9006, 3COM 3C509, Realtek RTL8029 и многие другие.

4. Шина PCI; 32 бита; подключение к витой паре; Fast Ethernet; Intel 82559, 3COM 3C905, Realtek RTL8139 и многие другие.

5. Шина PCI, либо PCI-X, либо PCI Express; 32 либо 64 бита; подключение к витой паре либо к оптоволокну; Gigabit Ethernet; Intel 82574, Broadcom BCM5751, Realtek RTL8169 и многие другие.

5 Назначение и классификация пассивного сетевого оборудования

Сетевое оборудование, предназначенное не для анализа передаваемой информации, а, в первую очередь, для обеспечения требующихся технических характеристик, называют пассивным (passive).

1. Оконечные концентраторы (hubs) -- работают с сигналами на физическом уровне модели OSI и тем самым осуществляют передачу принимаемых пакетов во всех направлениях (уже давно не производят).

2. Повторители (repeaters) -- осуществляют усиление принимаемых сигналов (не обязательно работают с пакетами).

3. Приемопередатчики (transceivers) -- подключают к коммутаторам и маршрутизаторам посредством стандартных разъемов (AUI, MII, GBIC, SFP), осуществляют передачу пакетов в определенные СрПД и прием пакетов из них.

4. Модули (modules) -- оригинальные (как правило) модули маршрутизаторов и коммутаторов (некоторые модули можно рассматривать как активное сетевое оборудование).

5. Медиаконвертеры (mediaconverters) -- осуществляют преобразование СрПД (например, BALUN -- BALance-UNbalance -- двунаправленный преобразователь из коаксиального кабеля в витую пару и наоборот).

6. Фильтры, сплиттеры и сумматоры -- осуществляют выделение, подавление, разделение и объединение диапазонов частот.

6 Назначение и классификация активного сетевого оборудования

Сетевое оборудование, способное анализировать передаваемую информацию называют активным (active).

1. Коммутаторы (switches) -- работают на втором уровне модели OSI и осуществляют целевую передачу принятых пакетов (кадров) в единственных правильных направлениях (в пределах сегментов).

2. Маршрутизаторы (routers) -- работают на третьем уровне модели OSI и осуществляют передачу принятых пакетов в соответствии с маршрутной информацией.

Этот список можно смело дополнить еще одним типом оборудования:

+3. Шлюзы (gateways) -- не то же самое, что IP-шлюзы -- осуществляют «перенаправление» сетевых сервисов прикладного уровня.

7 Структура коммутатора и методы коммутации

С точки зрения крупноблочного проектирования все современные коммутаторы можно свести к трем базовым структурным схемам (и их комбинациям):

1. На основе коммутационной матрицы (crossbar fabric) -- пакеты между портами проходят по выделенным путям, проложенным через коммутационную матрицу.

2. На основе разделяемой шины (bus backplane) -- пакеты проходят через связывающую все порты общую высокоскоростную шину.

3. На основе разделяемой памяти (shared memory) -- пакеты перемещаются между портами посредством размещения в общей для всех портов памяти.

Следует различать программную и аппаратную буферизацию. Следует учитывать и тот факт, что современные сетевые контроллеры (выполняющие роль сетевых интерфейсов) по сути являются интеллектуальными сопроцессорами.

Основные методы коммутации:

1. Store&Forward -- с промежуточной буферизацией -- коммутатор получает пакет полностью перед его ретрансляцией; анализируется адрес назначения и проверяется контрольная сумма.

2. Cut Through -- без промежуточной буферизации -- коммутатор не ожидает получения пакета целиком; анализируется лишь адрес назначения.

3. Fragment Free -- модифицированный метод с промежуточной буферизацией -- перед тем как осуществить коммутацию, коммутатор ожидает получение первых 64 байтов пакета; таким образом, если в пакете присутствует ошибка, то она почти всегда обнаруживается путем анализа этих байтов.

4. Hybrid -- гибридный -- поочередное адаптивное применение перечисленных методов.

8 Структура таблицы коммутатора Ethernet и ее использование

В основу работы классического коммутатора второго уровня положена таблица MAC-адресов, по -другому называемая CAM-таблицей (Content Addressable Memory).

По сути, в таблице хранится соответствие MAC-адресов и портов.

При приеме юникаст -кадра некоторым портом, коммутатор связывает MAC-адрес источника с номером этого порта и заносит в таблицу (этот процесс называют изучением). При ретрансляции кадра порт для передачи определяется исходя из MAC-адреса назначения по таблице.

Широковещательный кадр и кадр с еще незнакомым юникаст-MAC-адресом назначения ретранслируются всеми портами.

Для передачи мультикаст -кадров в правильных направлениях нужна особая поддержка (IPv4 IGMP и IPv6 MLD).

При ретрансляции пакетов (Smart-коммутаторами) учитываются виланы

MAC-адреса в CAM-таблице коммутатора могут быть двух видов:

1. Динамические (dynamic) -- изучаются коммутатором автоматически.
2. Статические (static) -- администратор «вручную» привязывает их к портам по одному или по несколько.

9 Гибридные технологии L2 -- L3

Традиционно выделяют три основных типа коммутаторов третьего уровня («гибриды » коммутаторов и маршрутизаторов):

1. Маршрутизирующие коммутаторы (routing switches) -- направление ретрансляции определяется на основе анализа информации, относящейся к третьему уровню в заголовке пакета; от маршрутизаторов отличаются виртуальностью сетевых интерфейсов.

2. Коммутаторы потоков (flow switches) -- выполняются попытки обнаружить продолжительные потоки пакетов между двумя станциями; после того, как факт наличия потока установлен на третьем уровне, дальнейшая коммутация осуществляется традиционным способом.

3. Коммутирующие маршрутизаторы (switching routers) -- выполняются попытки снизить расчетную нагрузку с маршрутизатора и возложить часть функций на уровень коммутации.

10 Характеристики и критерии выбора активного сетевого оборудования

Характеристики и критерии выбора активного сетевого оборудования:

1. Область применения: workgroup -- для рабочих групп, backbone (core) -- магистральные.
2. Тип и число физических портов: 4 (+1), 8, 12, 16, 24, 48 (другие редко).
3. Уровень модели OSI: L2, L2+, L3, L3+.
4. Набор поддерживаемых протоколов маршрутизации (для L3-устройств).
5. Управляемость: unmanaged -- неуправляемые, managed -- управляемые (свой IP адрес, выделенная консоль RS-232C, web-интерфейс, SNMP).
6. Структура: fixed -- фиксированная, modular -- модульная.
7. Возможность масштабирования: unstackable -- нестекируемые, stackable -- стекируемые.
8. Наличие разъемов расширений: стандартных и оригинальных.
9. Технические характеристики: размеры таблиц, времена задержек и другие.
10. Суммарная пропускная способность (стоит выделить отдельно).
11. Возможность автоматическ ого определения скорости и режима (физического соединения): auto-negotiation и auto-MDI/MDIX.
12. Поддержка виртуальных ЛКС: VLANs.
13. Поддержка резервирования: spanning tree, link aggregation, clusters.
14. Поддержка дополнительных возможностей по обеспечению безопасности: port security и access control lists.
15. Поддержка качества обслуживания: QoS.

11 Производители сетевого оборудования различных категорий

High-end:

Intel (в готовом виде уже давно не производит) (Shiva, Express, NetStructure),

HP (3COM) (OfficeConnect, Baseline, SuperStack), HPE (ProCurve), Aruba (HPE),

Cisco (множество серий коммутаторов Catalyst и маршрутизаторов), Avaya (Nortel) (Passport, Baystack, Netgear, много серий), Alcatel-Lucent (Nokia) (много серий),

Juniper (много серий),

Allied Telesis (много серий), Commscope

Commscope (Ruckus), Zyxel (Omni LAN, Dimension),

Broadcom (Persona), Marvell (Prestera) и некоторые другие.

Low-end:

Huawei, D-Link, Compex, CeLAN, Realtek, Surecom и другие.

12 Коммутаторы Cisco

По состоянию на сентябрь 2022 г. пять категорий (Access, Core and distribution, Data center and cloud, Industrial Ethernet, Small business and LAN compact).

Некоторые серии поддерживают модули.

Модули разрабатывают целенаправленно -- только для конкретной серии (либо нескольких «родственных » серий)

Некоторые серии поддерживают стекирование.

Интересно, что для наращивания портов коммутаторов Nexus вместо стекирования используют внешние устройства -расширители (fabric extenders).

Выделяют:

2960-S, 2960+, 2960-X, 2960-L

серию 1000 (Smart, немодульные, обычно нестекируемые).

А также серии (L3 или, как официально называли раньше, многоуровневые): 3560, 3560v2, 3560-X, другие «вариации» 3560 (немодульные и модульные, нестекируемые),

плюс заменившую 3560 серию 3650 (немодульные, стекируемые),

плюс заменяющую 3650 серию 9200 (немодульные и модульные, стекируемые);

В 3750 (во всех моделях кроме самых ранних), как и в 3560, как и в 2960 (2960+), установлен процессор Cisco Yeti-2 (изготавливаемый под заказ вариант IBM -- AMCC PowerPC 405 с архитектурой Power, одноядерный, SoC);

в 3750-X, как и в 3560-X -- Cisco Yeti-3 (еще более усовершенствованный вариант Yeti, по-прежнему одноядерный)

3850, как и в 3650 -- Cavium Octeon II CN6230 (с архитектурой MIPS64, четырехядерный, SoC) либо CN6335 (в моделях с поддержкой Multigigabit Ethernet, шестиядерный);

в 9300 -- Intel Xeon D-1526 (с архитектурой Intel 64, четырехядерный, SoC),

в 9200 -- ARM Cortex-A53 (с архитектурой ARM64, четырехядерный, SoC - - не отдельно, а на одном кристалле с ASIC).

Cisco все больше берет за основу перепрограммируемые ASICs (не совсем то же самое что FPGA) и другие аппаратные программируемые структуры (в том числе FPGA).

Заметно, что AUX-порты в коммутаторы Cisco не устанавливают. У относительно дешевых коммутаторов нет тумблеров питания. Отдельно взятый порт отдельно взятого коммутатора Cisco имеет традиционно совмещенный двуцветный (зеленый и оранжевый) индикатор. Для переключения режима индикации (состояние и другое) используют кнопку Mode, расположенную так же на лицевой панели (эту кнопку используют и в других целях). Некоторые индикационные коды (например, коды скорости) на коммутаторах не такие как на маршрутизаторах.

Коммутаторы серии 2960 поставляли со встроенным web-интерфейсом -- адаптированным вариантом SDM (2960+ поставляют с CP for Catalyst). Исключением, в смысле администрирования, являются не Catalystкоммутаторы. Они вовсе не имеют CLI («младшие» серии) либо имеют упрощенный CLI, называемый Textview («старшие» серии), зато имеют полноценный встроенный web-интерфейс (поэтому и не Catalyst).

13 Cisco IOS и коммутаторы

Основы IOS, которые относятся к коммутаторам, а также те, которые уместнее изучать на примерах с коммутаторами.

В настоящее время наиболее актуальны следующие версии IOS для коммутаторов:

12.2 -- для 2960, 3560, 3750 и других «современников» (по-прежнему),

15.X -- для 2960, 2960-S, 3560-X, 3750-X, 2960-L, 1000 и других.

И IOS XE для коммутаторов: 16.X -- для 3650, 3850, 9200, 9300 и других.

По понятным причинам, ОС IOS XE более громоздка в сравнении с IOS.

IOS XE может быть установлена на коммутатор -- режим install. Процесс установки сильно упрощен в сравнении с процессом установки Linux.

Альтернативно, IOS XE может быть загружена традиционно с использованием бинарного образа -- режим bundle. Необходимое файловое окружение воссоздается (на накопителе все равно будет достаточно много файлов).

Режим install позволяет ускорить загрузку и более эффективно использовать память (программные пакеты не распаковываются в память, а хранятся на накопителе в виде файлов .cfg).

Коммутаторы соответствующих серий поставляют с IOS XE в режиме install.

На маршрутизаторах режим install не доступен (по крайней мере пока).

Шаги для установки IOS:

1) подключаемся через консольный кабель к комутатору
2) настраиваем сеть, добавляем пк и маршрутизатор в общую подсеть
3) подключаем пк по ethernet к маршрутизатору
4) на пк запускаем tftp сервер
5) делаем резервную копию прошивки
6) удаляем рабочую прошивку
7) копируем новую прошивку с компьютера
8) указываем, что новая прошивка будет использоваться при загрузке
9) сохраняем конфиг
10) перезагружаем коммутатор.

14 Конфигурирование порта Ethernet коммутатора Cisco

Примеры конфигурирования физических параметров портов коммутаторов Cisco:

```
Switch(config)#interface range gi0/1,gi0/11-12
Switch(config-if-range)#speed 1000
Switch(config-if-range)#duplex full
Switch(config-if-range)#no mdix auto
Switch(config-if-range)#exit
```

Feature	Default Setting
Operating mode	Layer 2 or switching mode (**switchport** command).
Port enable state	All ports are enabled.
Port description	None defined.
Speed	Autonegotiate.
Duplex mode	Autonegotiate.
Flow control	Flow control is set to **receive: off**. It is always off for sent packets.
Port blocking (unknown multicast and unknown unicast traffic)	Disabled (not blocked)
Broadcast, multicast, and unicast storm control	Disabled.
Protected port	Disabled.
Port security	Disabled.
Port Fast	Disabled.
Auto-MDIX	Enabled.
Power over Ethernet (PoE)	Enabled (auto).
Keepalive messages	Disabled on SFP module ports; enabled on all other ports.

Конфигурация порта (Ethernet) коммутатора Cisco по умолчанию [Cisco]

15 Таблица коммутатора Cisco 2960

```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports !С учетом виланов
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU !Должен обработать сам коммутатор
 All    0100.0ccc.cccd    STATIC      CPU !(входит в мультикаст-группы служебных
 All    0180.c200.0000    STATIC      CPU !протоколов второго уровня)
...
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU !Также должен обработать сам
                                        !коммутатор (управляемый) (свои L3-
                                        !интерфейсы не отображены)
 500    0019.d102.ce0a    DYNAMIC     Gi0/4
 500    001c.c06e.f7cb    DYNAMIC     Gi0/11
 500    0022.4d80.e641    DYNAMIC     Gi0/10 !Порт соединен с портом другого
 500    0027.0e1f.af88    DYNAMIC     Gi0/10 !коммутатора (либо портом
 500    bcf6.8503.3c6a    DYNAMIC     Gi0/10 !«продвинутого» устройства)
 502    001b.2122.8e77    DYNAMIC     Gi0/2
 502    009e.1e8e.edcf    DYNAMIC     Po1 !EtherChannel (агрегированный канал)
...
 508    0025.906c.ea64    DYNAMIC     Gi0/8
Total Mac Addresses for this criterion: 51
```

16 Понятие виланов, их достоинства и недостатки

Виртуальные ЛКС -- Virtual LANs (VLANs), называемые также виланами, представляют собой множество реализаций находящей все большее применение концепции виртуальных машин.

Виланы позволяют строить на базе одной физической сети некоторое количество логических, причем логические сети будут существовать независимо друг от друга, то есть переданный в одной сети пакет никогда не будет принят в другой (если дополнительно об этом не позаботиться).

Применительно к подавляющему числу практических случаев, встречающееся в предыдущем предложении слово «сеть» следует заменить словом «сегмент».

Основные достоинства виланов:

1. Использование виланов помогает контролировать трафик, в первую очередь широковещательный.
2. С помощью виланов обеспечивают дополнительную защиту информации.
3. Виланы лучше адаптированы к изменениям в составе сетевого оборудования.

Основные недостатки виланов:

1. Необходимость наличия значительно более дорогостоящего сетевого оборудования (например, сетевые адаптеры типа server и коммутаторы не ниже уровня L2+).
2. Применение виланов приводит к увеличению вычислительной нагрузки по причине вносимых количественных и качественных дополнений.

17 Классификации и реализации виланов

Критерии классификации виланов:

1. Порт-, интерфейс - либо канал -ориентированность: port-based, interfacebased, link-based.
2. Наличие тегировки пакетов: tagged, untagged.
3. Наличие протокол -ориентированности (адрес -ориентированности): protocol-based.
4. Уровень модели OSI: L2, L3 и другие.
5. Наличие аутентификации: authentication-based.
6. Постоянство членства: static, dynamic.

Здесь уместна еще одна классификация виланов на основе тегов для 802.1Q:

1. Data VLAN -- «рабочий » вилан -- предназначен для передачи пользовательского трафика (может быть назначен любой незарезервированный VID).
2. Default VLAN -- вилан по умолчанию -- в данный вилан включаются все порты коммутатора по умолчанию (не может быть ни изменен, ни удален; зарезервирован VID = 1).
3. Management VLAN -- административный вилан -- предназначен для администрирования (выделяют исходя из соображений безопасности; от пользовательских виланов отличается только назначением).
4. Native VLAN -- вилан для оригинального трафика -- предназначен для передачи нетегированного трафика (по умолчанию это вилан с VID = 1; может быть назначен любой незарезервированный VID).
5. Private VLAN -- приватный вилан -- предназначен для частичного запрета трафика в рамках вилана (позволяет масштабировать виланы).
6. Reserved VLAN -- зарезервированный вилан -- предназначен для передачи специфического трафика (например, голосового; VID может быть как из зарезервированного, так и с незарезервированного диапазона; в Cisco IOS зарезервированы VIDs: 0, 1, 1002 -- 1005, 1006 -- 1024, 4095).

Реализации:

1. Собственно Port-based -- членство в вилане определяется в соответствии с портами активного сетевого оборудования.
2. 802.1Q. - - в кадр Ethernet вставляется специальный тег.
3. Cisco ISL (Inter-Switch Link) -- проприетарный протокол, аналогичный 802.1Q.
4. 3Com VLT (Virtual LAN Trunk) -- еще один проприетарный протокол, аналогичный 802.1Q.
5. Cisco VTP (VLAN Trunking Protocol) -- проприетарный протокол, позволяющий частично автоматизировать настройку виланов.

Так же:

802.1v -> 802.1Q (protocol-based),

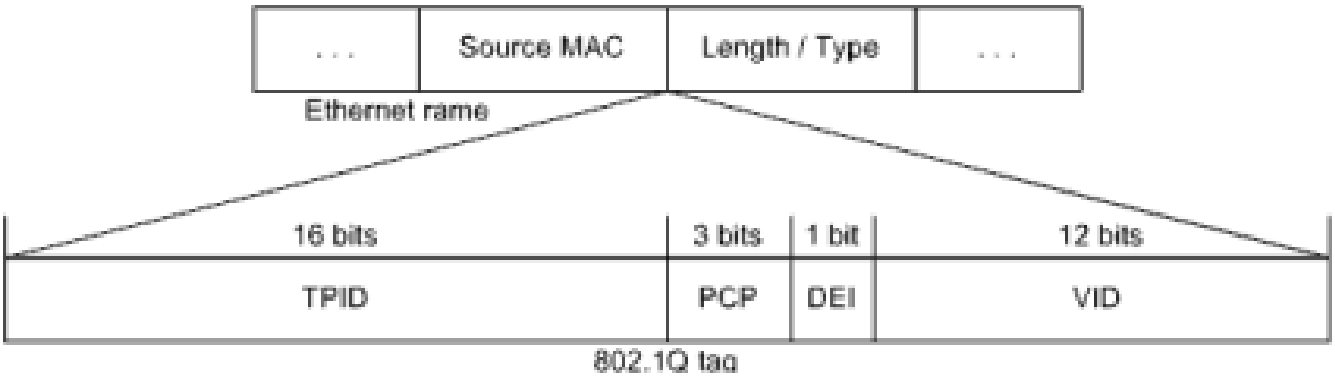
Cisco VQP (VLAN Query Protocol) (аналог 802.1X),

D-Link ISM (IGMP Snooping Multicast) VLAN,

GVRP (GARP VLAN Registration Protocol) (открытый аналог VTP),

MAC-based VLANs от различных производителей, auto voice VLAN (связь с QoS), auto surveillance VLAN.

18 802.1Q



Поля:

1. TPID (Tag Protocol IDentifier) -- идентификатор протокола тегировки (является и признаком наличия тега, для 802.1Q равно 8100h).

2. PCP (Priority Code Point) либо (до 802.1Q-2005) User_Priority -- код приоритета либо приоритет пользователя.

3. Drop Eligible Indicator (DEI) либо (до 802.1Q-2011) CFI (Canonical Format Indicator) -- индикатор разрешения отброса кадра либо индикатор канонического формата MAC-адреса (в обычном кадре Ethernet равно нулю).

4. VID (VLAN IDentifier) -- идентификатор вилана (собственно значение тега).

Отдельно взятый вилан представляет собой определенную независимую сущность на коммутаторе. Поэтому для использования вилан нужно привязать к портам.

Все виланы пронумерованы. Номера не только позволяют коммутаторам разграничивать трафик, а и позволяют связать воедино виланы на соседних коммутаторах.

В рядовом случае, полученный от оконечной пользовательской станции кадр тегируется ближайшим коммутатором с поддержкой 802.1Q.

При этом физические порты, обращенные к оконечным пользовательским станциям (в общем случае, к домену, «не заботящемуся» о виланах) принято называть портами доступа (access ports) (согласно терминологии некоторых компаний, в первую очередь Cisco) или, по-другому, нетегирующими портами (untagged ports).

Один и тот же физический канал может быть связан с передачей тегированных кадров, относящихся к различным виланам.

В рядовом случае, таковыми являются физические каналы между коммутаторами. Эти каналы называют транками (trunks) (согласно терминологии Cisco), а примыкающие к ним порты (в общем случае обращенные к домену, «заботящемуся» о виланах) называют транковыми портами (trunk ports) или, по -другому, тегирующими портами (tagged ports).

Транковый порт привязан ко всем имеющимся виланам либо к списку разрешенных.

PVIDs при этом не нужны и не используются.

Транковый порт по своей сути предназначен для работы с тегированными кадрами, но, с учетом широко распространенной практики использования, должен «понимать» и нетегированные.

Согласно общеиндустриальному представлению проблему сосуществования нетегированного и тегированного трафика решают просто -- один и тот же соответствующий порт рассматривают как тегирующий, так и нетегирующий одновременно (часто в реализациях каждый порт в отношении каждого вилана является тегирующим, либо нетегирующим, либо вообще не относящимся к данному вилану).

Понятие native VLAN применимо только к транковому порту. Это вилан, в который коммутатор помещает все принимаемые через данный транковый порт нетегированные кадры, и, попутно, вилан, все кадры из которого передаются через данный транковый порт нетегированными. По умолчанию native VLAN является вилан с VID = 1, в результате весь трафик по умолчанию передается нетегированным.

Cisco решает проблему с помощью вилана для оригинального трафика. Таким образом, на коммутаторе с поддержкой 802.1Q отдельно взятый порт может быть либо портом доступа, либо транковым, либо, если предусмотрено, сочетать эти два режима (поддержка 802.1Q не отключается).

Замечание о вилане по умолчанию. Вилан по умолчанию отличается от других виланов лишь тем, что к нему привязываются все порты по умолчанию («отвязывают» -- по мере надобности) и он на коммутаторе существует всегда. Виланом по умолчанию является вилан с VID = 1

Конечно, теги может вносить и сама станция, например, серверная, но для этого требуется поддержка 802.1Q со стороны сетевого адаптера. Возлагать задачу внесения тегов на рядовую клиентскую станцию некорректно.

Концепция 802.1Q допускает многократную тегировку кадров (QinQ), но нужно помнить что каждый тег увеличивает кадр, а значит длина кадра может превысить значение MTU.

19 Маршрутизация между виланами

Маршрутизация выполняется:

1. L3-коммутатором с виртуальными сетевыми интерфейсами в разных IP-подсетях.

2. Маршрутизатором с относящимися к разным IP-подсетям виртуальными подинтерфейсами одного реального сетевого интерфейса (иногда называют router-on-stick).

3. Маршрутизатором с относящимися к разным IP-подсетям сетевыми интерфейсами (иногда называют классической маршрутизацией между виланами).

“Router-on-a-stick” при маршрутизации между VLAN имеет недостаток – использование пропускной способности только одного физического интерфейса для передачи трафика нескольких виртуальных локальных сетей, т.к. виртуальные сети делят пропускную способность одного канала.

При использовании нескольких физических интерфейсов маршрутизатор должен иметь столько портов, сколько в сети применяется VLAN. Порты коммутатора, к которому подключается маршрутизатор в такой сети, должны работать в режиме доступа, и соответственно находится в разных VLAN. Порты маршрутизатора должны иметь настроенные статические адреса в IP-сетях, применяемых в виртуальных локальных сетях, и эти адреса должны использоваться узлами каждой сети как шлюз по умолчанию.

20 Поддержка виланов в Windows и Linux

В Windows, исключая Server 2012 -- Server 2019, виланы поддерживаются только на уровне драйверов сетевых адаптеров (например, Intel).

При этом необходимо конфигурационное ПО (например, утилиты) от производителей.

Подинтерфейсы как таковые не поддерживаются.

Виланы представлены виртуальными мультиплексируемыми сетевыми интерфейсами (тегированный и нетегированный трафик).

В Linux поддержка виланов выражена в подинтерфейсах.

На примере eth0 -- это eth0.1, eth0.2, eth0.3 и так далее.

Номер подинтерфейса соответствует VID в кадре (тегированный трафик), eth0 соответствует native VLAN (нетегированный трафик).

Подинтерфейсы eth0 могут сосуществовать с eth0.

/etc/sysconfig/network-scripts/ifcfg-eth1.10 (ветви Red Hat и SUSE):

```
DEVICE=eth1.10
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.10.1
NETMASK=255.255.255.0
```

/etc/network/interfaces (ветвь Debian):

```
auto eth1.10 iface eth1.10 inet static
        address 192.168.10.1
        netmask 255.255.255.0
        vlan_raw_device eth1
```

21 Конфигурирование виланов в IOS

Для сохранения информации о виланах создается специальная база данных vlan.dat -- традиционный файл в корневом каталоге подсистемы памяти Flash.

Создание VLAN:

```
Switch#vlan database
Switch(vlan)#vlan 10 name STUDENTS
Switch(vlan)#exit
Switch#
```

Установка access mode

```
Switch(config)#interface fa0/11
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
```

Установка trunk mode:

```
Switch(config)#interface fa0/12
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport trunk allowed vlan 10,20,30,40
Switch(config-if)#switchport trunk native vlan 40
Switch(config-if)#exit
```

Конфигурирование ассоциированного с виланом виртуального сетевого интерфейса (SVI):

```
Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.11.11 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

22 Конфигурирование маршрутизации между виланами в IOS

Поскольку L2 коммутатор Cisco по умолчанию является устройством второго уровня, IP-маршрутизация на нем по умолчанию выключена (в отличии от маршрутизатора -- устройства третьего уровня).

```
Switch(config)#ip default-gateway 192.168.11.1
Switch(config)#ip routing
...
Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.11.1
```

Пример создания и конфигурирования подинтерфейсов на маршрутизаторе (нумерацию можно начинать с нуля). При этом IP-адрес можно назначить только после включения инкапсуляции и IP-адрес подинтерфейса совместим с IP-адресом интерфейса.

```
Router(config)#interface gi0/0. 1
Router(config-subif)#encapsulation dot1q 40 native
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface gi0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
```

23 Протокол VTP и его использование

Основное назначение протокола второго уровня VTP (VLAN Trunking Protocol) заключается в автоматизации процесса настройки транков.

VTP-домен (VTP domain) представляет собой единую зону ответственности, работающую по правилам протокола VTP и состоящую из некоторого количества соединенных между собой коммутаторов. Тем не менее, в рамках СПД может существовать несколько VTP-доменов. Каждый VTP-домен уникальным образом именуют. Коммутатор может входить в состав только одного VTP-домена. Разработаны три версии протокола VTP: 1, 2 и 3. В границах VTP-домена допускается применение только одной версии.

В отношении VTP коммутатор может функционировать в одном из трех режимов (VTP mode):

1. VTP-сервер (VTP server).
2. VTP-клиент (VTP client).
3. Прозрачный режим (VTP transparent).

VTP-сервер предназначен для создания, модификации или удаления виланов, а также задания конфигурационных параметров применительно ко всему VTP-домену. Все заданные параметры в последствии «распространяются» в пределах VTP-домена. В VTP-домене может быть только один VTP-сервер.

VTP-клиент не предназначен для внесения информации о виланах. VTPклиент работает на основе сведений, получаемых от VTP-сервера. Все коммутаторы в VTP-домене, кроме одного, должны быть VTP-клиентами. Тем самым гарантируется слаженность работы VTP-домена.

В прозрачном режиме коммутатор не участвует в работе VTP-домена, с которым связан.

Для обеспечения синхронизации VTP-конфигураций на коммутаторах вводятся ревизионные номера (VTP revision numbers), которые после включения коммутатора в домен инкрементируются начиная с нуля при каждом изменении в базе данных виланов (создание, удаление, приостановка работы, активация, переименование, изменение MTU вилана).

Единственный способ «сбросить » ревизионный номер -- это изменить название домена.

Обмен по протоколу VTP осуществляется посредством VTP-сообщений (VTP advertisements), передаваемых по зарезервированному мультикастMAC-адресу 01-00-0C-CC-CC-CC.

VTP-сообщения бывают трех видов:

1. Summary -- содержат обобщенную информацию, порождаются сервером и распространяются по всему домену, посылаются незамедлительно при любых изменениях и затем периодически с интервалом равным 5 min (интервал изменить нельзя), также посылаются по запросу.

2. Subset -- содержат информацию о виланах, порождаются сервером и распространяются по всему домену, посылаются при любых изменениях или по запросу, при необходимости фрагментируются.

3. Request (+Join) -- запросы от клиентов к серверу о конфигурации, посылаются при подключении клиентов к домену, также посылаются если текущий ревизионный номер меньше полученного посредством summary или произошла потеря subset, в ответ сервер посылает summary плюс одно либо несколько subset.

Если по каким-либо причинам в домен попал VTP-клиент с ревизионным номером больше чем у сервера, то возникает исключительная ситуация, и, благодаря скрытым механизмам, клиент на время становится сервером. В результате, его конфигурация «разносится» по домену, что обычно неправильно.

Опционально VTP поддерживает шифрование сообщений (MD5).

Если VTP-пароли задаются, то в пределах домена они должны быть идентичными.

VTP поддерживает только так называемые normal-range VLANs (VIDs от 1 до 1005).

Extended-range VLANs (VIDs больше 1005) игнорируются

TP, с одной стороны, избавляет от рутинной ручной работы, но, с другой стороны, порождает избыточность.

Усовершенствование под названием VTP-сдерживание (VTP pruning) препятствует распространению по транкам относящегося к определенным виланам трафика в ненужных направлениях, тем самым увеличивая эффективность СПД.

24 Конфигурирование VTP

Задание сервера/клиента:

```
Switch(config)#vtp mode server
Switch(config)#vtp domain EVMDEPT
Switch(config)#vtp password mypassword

Switch(config)#vtp mode client
Switch(config)#vtp domain EVMDEPT
Switch(config)#vtp password mypassword

Switch(config)#vtp mode transparent
```

Выбор версии VTP:

```
Switch(config)#vtp version 2
```

Пример включения VTP-сдерживания:

```
Switch(config)#vtp pruning

Switch(config)#interface fa0/12
Switch(config-if)#switchport trunk pruning vlan except 20
Switch(config-if)#exit
```

Основная команда для определения состояния подсистемы VTP -- это show vtp status.

На коммутаторах, находящихся в клиентском режиме, информация о виланах в энергонезависимой памяти не сохраняется, а в серверном и прозрачном режимах -- сохраняется.

VTP-конфигурация сохраняется в базе данных виланов.

25 Назначение и терминология протокола STP

Пакеты второго уровня (фреймы) не имеют поля TTL, что приводит к возможности возникновения бесконечных циклов при их ретрансляции.

Группа протоколов второго уровня под общим названием Spanning Tree призвана бороться с зацикливанием в СПД при резервировании физических каналов.

Собственно STP (Spanning Tree Protocol) (802.1D с дополнением 802.1t) -- это, по сути, один из алгоритмов построения из группы произвольно соединенных между собой L2-устройств виртуального дерева, то есть графа, не содержащего логических петель. Заложенный в STP алгоритм позволяет находить один из лучших вариантов среди множества возможных.

Некоторые модификации STP совместимы с виланами.

STP-домен (STP domain) может находиться в одном из трех состояний:

1. Первоначальная STP-конвергенция (STP convergence) -- первоначальное построение дерева.
2. Устоявшееся состояние -- полезная работоспособность.
3. Повторная STP-конвергенция -- перестроение дерева по причине топологических изменений с последующим возвращением в устоявшееся состояние.

По протоколу STP коммутаторы обмениваются сообщениями BPDUs (Bridge Protocol Data Units).

Для STP BPDUs зарезервировано 17 мультикаст-MAC-адресов: 01-80- C2-00-00-00 -- 01-80-C2-00-00-10.

Обмен BPDUs происходит во всех состояниях STP-домена, но поразному.

BPDUs коммутаторами передаются и принимаются, но не ретранслируются.

В устоявшемся STP-домене корнем дерева является коммутатор, называемый корневым мостом (root bridge).

В результате работы алгоритма каждому отдельно взятому порту каждого из коммутаторов назначается одна из следующих STP-ролей (порты доступа в контексте STP рассматривать не принято):

1. Корневой (root) -- разрешено передавать кадры, ближайший обращенный к корневому мосту.
2. Назначенный (designated) -- разрешено передавать кадры, обращенный в сторону от корневого моста.
3. Альтернативный (alternate) или, иначе, резервный (backup) -- запрещено передавать кадры.

В каждый момент времени каждый порт коммутатора находится в одном из следующих STP-состояний:

1. Блокировка (blocking) -- не участвует в пересылке кадров.
2. Прослушивание (listening) -- принимается решение о возможности участия в пересылке кадров.
3. Изучение (learning) -- готовится к участию в пересылке кадров.
4. Ретрансляция (forwarding) -- участвует в пересылке кадров.
5. Запрет (disabled) -- вообще не участвует в работе, то есть не подключен к СрПД, административно выключен, или не поддерживает STP.

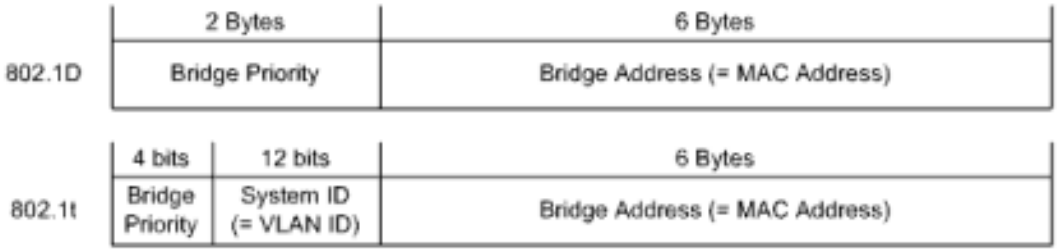
26 STP-конвергенция

STP-конвергенция протекает в три фазы:

1. Выбор корневого моста.
2. Выбор корневых портов.
3. Выбор назначенных и альтернативных портов

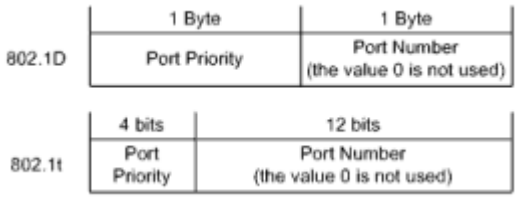
В процессе упомянутых выборов анализируются следующие параметры:

1. Идентификатор моста (bridge Identifier) -- ассоциирован с каждым мостом, должен быть уникален



2. Стоимость пути (path cost) -- ассоциирована с каждым портом, оценивается в рамках STP-домена (2 байта либо, в соответствии с 802.1t, 4 байта).

3. Идентификатор порта (port identifier) -- ассоциирован с каждым портом, оценивается в рамках коммутатора.



В реализациях STP перечисленные параметры можно конфигурировать, то есть параметрам можно присваивать значения, отличные от значений по умолчанию.

Изначально каждый коммутатор считает себя корневым мостом, но после обмена BPDUs корневым становится мост с наивысшим приоритетом, то есть с наименьшим цифровым значением идентификатора моста.

Получается, что при совпадении приоритетов мостов учитывается MAC-адрес.

В дальнейшем корневой мост используется как точка отсчета.

Корневые порты выбираются исходя из стоимости пути к корневому мосту, то есть из суммы условных стоимостей физических каналов, ведущих к корневому мосту. Выбирается путь с минимальной стоимостью.

В случае полного совпадения стоимостей учитываются идентификаторы портов. Выбирается порт с наименьшим цифровым значением идентификатора.

При совпадении приоритетов портов учитываются номера портов.

Если из оставшихся портов два связанных порта входят в образовавшуюся петлю, то решается, какой из них активировать, а какой зарезервировать и блокировать (то есть каждый из физических каналов заканчивается только одним активным портом).

Назначенный порт выбирается исходя из наименьшей стоимости пути к корневому мосту.

При совпадении стоимости учитывается идентификатор моста. Выбирается порт с наименьшим идентификатором.

Роль порта в процессе STP-конвергенции может изменяться неоднократно.

В последствии, если какая -либо часть STP-домена претерпела изменение, то оно обнаруживается (регулярный обмен BPDUs) и специальное BPDU (Topology Change Notification) отсылается в сторону корневого моста. Затем корневой мост информирует об изменении топологии все коммутаторы. В результате топология перерассчитывается и резервные пути активируются.

27 Модификации протокола STP

Протокол STP имеет следующие основные модификации:

1. RSTP (Rapid STP) (802.1w -> 802.1D) -- алгоритм предоставляет возможность ускоренной STP-конвергенции.

2. PVST (Per-VLAN Spanning Tree) -- проприетарный протокол Cisco, в отличие от 802.1D в каждом из виланов коммутатор рассматривается как независимая сущность (при этом native VLAN на обоих концах транка должен быть одним и тем же), поддерживает ISL-транки, ряд расширений от Cisco (например, PortFast).

3. PVST+ -- проприетарный протокол Cisco, поддерживает ISL- и 802.1Qтранки, новые расширения (например, BPDU Guard).

4. RPVST+ (Rapid PVST+) -- от PVST+ отличается только тем, что базируется на 802.1w.

5. MSTP (Multiple STP) (802.1s -> 802.1Q) -- коммутатор как независимую сущность можно отобразить в несколько виланов.

В качестве альтернативы Spanning Tree применимы другие технологии, например, Cisco Flex Links (порту назначают дублирующий порт).

Некоторые реализации собственно Ethernet (в том числе от Cisco) поддерживают механизм Ethernet keep-alive, также позволяющий обнаружить зацикливание (через порт периодически передается специальный «нулевой» кадр типа 9000h с MAC-адресом источника и MAC-адресом назначения, равными MAC-адресу, относящемуся к порту).

28 Конфигурирование STP в IOS

В отличие от многих других протоколов, работа STP почти не требует вмешательства.

Командой no spanning-tree vlan можно отключить STP -- глобально в соответствующих виланах.

Совместимость с 802.1D либо 802.1t контролируют командами spanning-tree extend system-id (на большинстве современных платформ «инверсный » вариант команды недоступен) и spanning-tree pathcost method.

Пример назначения коммутатора корневым мостом.

Switch(config)#spanning-tree vlan 40 root primary diameter 3

Пример задания стоимости пути.

Switch(config)#interface fa0/1

Switch(config-if)#spanning-tree vlan 40 cost 50

Switch(config-if)#exit

С функционированием STP на коммутаторах Cisco связаны следующие таймеры:

1. Hello timer -- позволяет задать частоту обмена периодическими BPDUs с соседними коммутаторами (по умолчанию 2 s).

2. Forward-delay timer -- позволяет задать паузу при переходе порта из состояния изучения в состояние ретрансляции (по умолчанию 15 s).

3. Maximum-age timer -- позволяет задать интервал времени, в течении которого принятые интерфейсом BPDUs считаются валидными (по умолчанию 20 s).

+4. Transmit hold count -- позволяет задать количество BPDUs, которые могут быть переданы перед паузой в 1 секунду (по умолчанию 6).

Пример задания таймера

Switch(config)#spanning-tree vlan 40 hello-time 10

PortFast -- это технология Cisco, которая заключается в незамедлительном переводе порта доступа из состояния блокировки в состояние ретрансляции.

BPDU Guard -- заключается в незамедлительном административном выключении находящегося в режиме PortFast порта доступа после приема им BPDU.

Включение PortFast и BPDU Guard.

Switch(config)#interface fa0/2

Switch(config-if)#spanning-tree portfast

...

Switch(config-if)#spanning-tree bpduguard enable

Switch(config-if)#exit

Основная команда для просмотра состояния подсистемы STP -- это show spanning-tree.

29 Понятие агрегации каналов

Часто с целями повышения производительности (load balancing) и попутного обеспечения надежности (fault tolerance) применяют технологии под общим названием Link Aggregation или Port Trunking, то есть технологии агрегирования каналов или портов.

Применительно к сетевым адаптерам их обычно называют NIC Teaming или NIC Bonding.

Суть заключается в формировании из нескольких «параллельных » физических каналов одного логического аппаратного канала -- транка (trunk не в терминологии Cisco), что открывает возможности более гибкого распределении ресурсов задействованных каналов.

С точки зрения STP, транк рассматривается как единая сущность.

Часто при резервировании выделяется так называемый связующий канал (primary link). Переход к резервным каналам происходит при стопроцентной загрузке или сбое связующего.

Максимальное количество членов транка часто ограничено двумя либо восемью.

30 Технологии агрегации каналов

Основные реализации транков:

1. Intel Adaptive Load Balancing (ALB) -- per-interface, L3, NIC -- switch, static.

Несколько (до восьми) сетевых адаптеров серверной (или клиентской) пользовательской станции подключают к одному коммутатору, поддержка со стороны коммутатора не требуется, все адаптеры разделяют передаваемый трафик, прием осуществляет только связующий порт, отказ одного из адаптеров чреват только исключением его из группы.

Вариант с Receive Load Balancing (RLB) обеспечивает разделение трафика в обоих направлениях.

2. Broadcom SLB (Smart Load Balancing) -- аналог Intel ALB плюс RLB.

Два варианта. Вариант Auto-fallback disable отличается от варианта Failover тем, что в случае восстановления после сбоя связующего адаптера эта функция (связующего адаптера) ему не возвращается.

3. HP NFT (Network Fault Tolerance) TLB (Transmit Load Balancing) -- еще один аналог Intel ALB.

Два варианта. Вариант Fault Tolerance отличается от варианта Fault Tolerance and Preference Order тем, что входящим в состав транка адаптерам можно задать приоритеты, в соответствии с которыми они будут становиться связующими.

4. Nortel & Avaya MLT (Multi-Link Trunking) -- группа проприетарных технологий (и протоколов) -- per-link плюс per-interface, L2 плюс L3, switch -- switch, static плюс dynamic.

Несколько вариантов, адаптированных для различных применений: собственно MLT, DMLT (Distributed SMLT), SMLT (Split MLT), SLT равно SSMLT (Single port SMLT), RSMLT (Routed SMLT).

5. 802.3ad (позже 802.1AX) SLA (Static Link Aggregation) -- ставший стандартом вариант технологии Cisco FEC (Fast EtherChannels) и GEC (Gigabit EtherChannels) -- per-link, L2, switch -- switch либо NIC -- switch, static.

Все «вручную» объединяемые в транк пары связанных портов должны быть идентичными (скорость, режим, виланы, состояние и другое), обеспечивается разделение трафика, сбойный канал исключается из группы.

6. 802.3ad (позже 802.1AX) LACP (Link Aggregation Control Protocol) -- в отличие от SLA, dynamic.

Позволяет автоматизировать формирование транков из пар портов на которых включена поддержка этого протокола, используются специальные сообщения LACPDUs (LACP Data Units) и мультикаст-MAC-адрес 01-80-C2- 00-00-02.

Современные EtherChannels поддерживают LACP.

7. Cisco Port Aggregation Protocol (PAgP) -- проприетарный протокол в рамках EtherChannels, аналог LACP.

Как и в случае с VTP, сообщения инкапсулируются в SNAP-пакеты и передаются по мультикаст-MAC-адресу 01-00-0C-CC-CC-CC.

8. Cabletron SmartTrunking & DEC Hunt Groups -- нынче редко применяемые проприетарные технологии -- per-link, L2, switch -- switch либо NIC -- switch, static плюс dynamic.

Кроме всего прочего, позволяют отслеживать и устранять зацикливания, если транки образуют петли (альтернатива STP). Базируются на двух протоколах: LLAP (Logical Link Aging Protocol) и PLAP (Physical Link Affinity Protocol).

31 Поддержка агрегации каналов в Windows и Linux

1. Microsoft NLB (Network Load Balancing) -- поддерживается в серверных редакциях Windows -- per-node, L2 плюс L3 плюс L4, NIC -- switch, static.

Содержащие по одному -- двум сетевым адаптерам серверные станции подключают к коммутаторам произвольным образом, поддержка со стороны коммутаторов не требуется.

Несколько режимов, возможно распределение трафика между станциями с учетом программных портов и приоритетов станций.

2. Microsoft NIC Teaming -- поддерживается в Windows Server 2012 -- Server 2019 -- per-link плюс per-interface, L2 плюс L3, NIC -- switch, static плюс dynamic.

Три режима: Switch Independent, Static Teaming, LACP.

3. Linux NIC Bonding -- per-link плюс per-interface, L2 плюс L3, NIC -- switch, static плюс dynamic.

Семь разных режимов, в том числе с поддержкой некоторых вышеперечисленных L2-технологий.

Конфигурирование NIC Bounding Linux

ifcfg-bond0:

DEVICE=bond0
ONBOOT=yes
BOOTPROTO=none
IPADDR=192.168.11.15
NETMASK=255.255.255.224

USERCTL=no ifcfg-eth0 (eth1 и так далее):
DEVICE=eth0 ONBOOT=yes
BOOTPROTO=non
SLAVE=yes
MASTER=bond0

USERCTL=no modprobe.conf: alias bond0 bonding options bond0 mode=balance-alb miimon=100 !Режим и интервал проверки в ms

32 Конфигурирование EtherChannels

EtherChannels (современная реализация) поддерживают SLA, LACP и PAgP в следующих режимах:

1. on -- SLA.
2. passive -- пассивный LACP.
3. active -- активный LACP.
4. auto -- пассивный PAgP.
5. desirable -- активный PAgP.

Интерфейс включают в группу (channel-group) с выбранным номером с помощью команды channel-group, при этом необходимо указать режим.

Группа создается автоматически при первом «обращении » к ней. Важно, что параметры интерфейсов в группе должны быть идентичными (даже текущие скорости).

Если параметры интерфейса при включении в группу отличны, либо, если параметры хотя бы одного из интерфейсов в составе группы по какой -либо причине стали отличны, то этот интерфейс, равно как и интерфейс, соединенный с этим интерфейсом, переводится в особое состояние -- down (suspended) и индикатор порта начинает гореть оранжевым цветом.

При создании группы автоматически создается и соответствующий виртуальный сетевой интерфейс port-channel. Channel-groups и port-channels связываются по номерам.

EtherChannels могут быть организованы как на втором, так и на третьем уровне.

```
Switch(config)#interface range gi0/1-2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#channel-group 1 mode on
Switch(config-if-range)#exit Switch(config)#interface port-channel 1
Switch(config-if)#spanning-tree portfast
Switch(config-if)#exit

Switch(config)#interface range gi0/3-4
Switch(config-if-range)#no switchport
Switch(config-if-range)#no ip address
Switch(config-if-range)#channel-group 2 mode active
Switch(config-if-range)#exit
Switch(config)#interface port-channel 2
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.168.0.11 255.255.255.0
Switch(config-if)#exit
```

Предусмотрены шесть вариантов балансировки нагрузки на основе анализа MAC- и IP-адресов источника и назначения.

```
Switch(config)#port-channel load-balance dst-mac
```

Основная команда для просмотра состояния EtherChannels -- это show etherchannel.

33 Понятие кластеризации активного сетевого оборудования

Существуют технологии, позволяющие формировать кластеры и из коммутаторов (switch clusters).

Увы, создавать кластеры проводного оборудования уровня доступа неуместно (отдельно взятый ПК не расчитан на одновременное подключение к нескольким коммутаторам), правда и неисправности на уровне доступа обнаруживать относительно легко.

Критерии классификации кластеров активного сетевого оборудования совпадают с критериями классификации транков.

Практически все технологии агрегирования каналов в то же время обеспечивают резервирование. Здесь упор сделан именно на резервирование устройств.

В настоящее время наблюдается все больший уклон в виртуализацию.

Взаимодействие маршрутизаторов в составе кластера, в том числе назначение активных (active, master) и резервных (standby, backup, slave) маршрутизаторов, а также балансировка нагрузки, осуществляется посредством группы протоколов третьего уровня под общим названием FHRPs (First Hop Redundancy Protocols).

Основные протоколы:

1. IRDP (ICMP Router Discovery Protocol) (RFC 1256) -- устаревший протокол для обнаружения маршрутизаторов посредством ICMP.

2. VRRP (Virtual Router Redundancy Protocol) (RFC 5798) -- протокол резервирования маршрутизаторов путем объединения их в виртуальный маршрутизатор. VRRPv3 отличается от VRRPv2 поддержкой не только IPv4, а и IPv6.

3. Cisco HSRP (Hot Standby Router Protocol) -- протокол «горячей» замены маршрутизатора. Поддерживаются IPv4 и IPv6.

4. Cisco GLBP (Gateway Load Balancing Protocol) -- протокол балансировки нагрузки между шлюзами. HSRP + балансировка нагрузки. Поддерживаются IPv4 и IPv6.

34 Технологии кластеризации активного сетевого оборудования

Основные технологии, связанные с коммутаторами:

1. Intel Adapter Fault Tolerance (AFT).

Несколько сетевых адаптеров станции подключают к одному коммутатору, поддержка со стороны коммутатора не требуется, в случае отказа текущего связующего адаптера активируется очередной резервный.

2. Intel Switch Fault Tolerance (SFT).

Два сетевых адаптера станции подключают к разным коммутаторам, поддержка со стороны коммутаторов не требуется, в случае отказа связующего канала активируется резервный.

3. HP NFT Only -- аналог Intel AFT.

Два варианта. Вариант Preference Order отличается тем, что адаптерам можно задать приоритеты, в соответствии с которыми они будут становиться связующими.

4. Cisco & IBM Link-State Tracking.

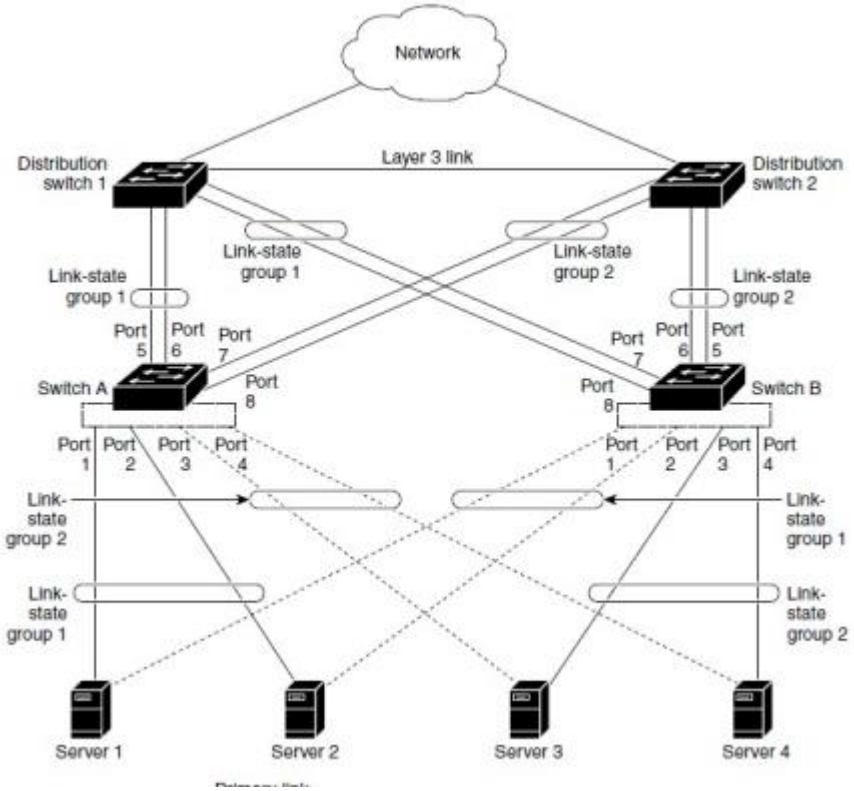
Состояние downstream-портов (обращенных в сторону ООД) ставят в зависимость от состояния upstream-портов (обращенных в сторону СПД), что позволяет более правильно распределять нагрузку в некоторых типовых топологиях с резервированием.

5. Cisco Virtual Switching System (VSS).

Предоставлена возможность формировать на базе высокопроизводительных платформ, таких как 6500, мощные коммутационные кластеры, используются расширения PAgP.

6. Alcatel-Lucent Multi-Chassis Link Aggregation (MC-LAG) & PseudoWire (PW) redundancy -- аналог Cisco VSS, ориентированный на собственное оборудование.

7. Juniper Virtual Chassis -- еще один аналог Cisco VSS.



35 Конфигурирование маршрутизирующих кластеров в IOS

Активный маршрутизатор выбирается исходя из приоритета. Приоритет задают числом от 0 до 255. Чем больше число, тем выше приоритет. При равенстве чисел сравниваются IP-адреса. Чем больше IP-адрес, тем выше приоритет.

После восстановления маршрутизатора с наивысшим приоритетом после сбоя он опционально снова может гарантированно стать активным (preemption).

Возможна аутентификация (символьная строка).

```
R1(config)#interface gi0/1
R1(config-if)#standby 1 ip 192.168.11.1
R1(config-if)#standby 1 priority 150
R1(config-if)#standby 1 preempt
R1(config-if)#exit

R2(config)#interface gi0/1
R2(config-if)#standby 1 ip 192.168.11.1
R2(config-if)#exit

R1(config)#interface gi0/1
R1(config-if)#glbp 1 ip 192.168.11.1
R1(config-if)#glbp 1 priority 150
R1(config-if)#glbp 1 preempt
R1(config-if)#glbp 1 load-balancing round-robin
R1(config-if)#exit

R2(config)#interface gi0/1
R2(config-if)#glbp 1 ip 192.168.11.1
R2(config-if)#glbp 1 load-balancing round-robin
R2(config-if)#exit
```

Основные команды для просмотра состояния кластера -- это show standby и show glbp.

MHSRP (Multiple HSRP) -- расширение, позволяющее включить маршрутизатор в несколько HSRP-групп, что используют для обеспечения балансировки нагрузки между группами.

36 Назначение, использование и альтернативы Cisco Port Security 2

Комплекс мероприятий для обеспечения защиты физических портов коммутатора от несанкционированного доступа известен как Port Security.

В отличие от упомянутых выше технологий, Port Security почти не регламентируют едиными промышленными стандартами. Серьезное исключение составляет стандарт 802.1X.

Port Security конфигурируют в отношении индивидуального L2-порта или группы L2-портов, что применимо только к портам доступа и транкам -- с учетом виланов (с L3-портами, DTP, EtherChannels и некоторыми другими возможностями совместимости нет).

После включения Port Security, со ставшим таким образом защищенным портом (secure port) могут ассоциироваться статические и динамические доверительные MAC-адреса (secure MAC addresses), но их суммарное количество не должно превышать установленного максимума.

В рамках лимита, доверительными адресами автоматически становятся изученные первыми динамические адреса (в том числе изученные до включения Port Security) и явно указываемые статические адреса (в данном случае приоритета не имеют).

Все остальные динамические адреса считаются недоверительными, недоверительные статические адреса в отношении защищенного порта не поддерживаются.

Понятно, что отдельно взятый адрес может быть доверительным либо недоверительным.

После включения опционального более «серьезного » изучения (sticky address learning) динамические доверительные адреса (в том числе изученные до включения этой возможности) считаются «липкими» (sticky) и, в результате, сохраняются не только в CAM-таблице, аив рабочей конфигурации.

В добавок, можно явно указать какие адреса считать «липкими».

«Липкие » адреса не теряются при выключении -включении порта (физическая перекоммутация, административное выключение -включение и так далее).

Можно задать время валидности доверительных адресов (port security aging).

Если MAC-адрес источника из принятого портом кадра не содержится в окончательно сформированном списке доверительных адресов или содержится в списке доверительных адресов, привязанных к другому порту, то это рассматривается как попытка несанкционированного доступа (security violation). Можно выбрать один из нескольких режимов реагирования на таковую ситуацию (violation mode).

Срабатывание Port Security в режиме shutdown переключает порт в особое состояние -- down (err-disabled) (не up, не просто down и не administratively down).

Следует отметить, что в таковое состояние порт может перейти и по другим причинам (BPDU Guard, поздняя коллизия, цикл Ethernet keep-alive и так далее).

Для возврата порта в нормальное состояние необходимо административно выключить и затем снова включить порт (shutdown и no shutdown), либо предварительно настроить автоматическое восстановление командой errdisable recovery.

Кроме собственно Port Security, есть еще две технологии Cisco для защиты портов: Port Blocking (запрет передачи портом незнакомого юникаст- и мультикаст-трафика) и Protected Ports (трафик между protected-портами запрещен)

37 Конфигурирование Cisco Port Security

```
Switch(config)# interface fa0/7
Switch(config-if)#switchport mode access !Либо trunk
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 3 vlan access !Опциональный
                                                                  !учет виланов
Switch(config-if)#switchport port-security violation protect
Switch(config-if)#switchport port-security mac-address 6045.cba7.f876
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security mac-address sticky 7054.d2bf.5b81
                !Таким же образом вносится в рабочую конфигурацию
                !автоматически (после предыдущей команды)
Switch(config-if)#switchport port-security aging time 1440 !Минуты
Switch(config-if)#switchport port-security aging type inactivity
Switch(config-if)#switchport port-security aging static
Switch(config-if)#exit
```

Основная команда для определения состояния Port Security -- это show port-security (без аргументов, с аргументом address, с аргументом interface).

Пример настройки автовосстановления.

```
Switch(config)#errdisable recovery cause psecure-violation
Switch(config)#errdisable recovery interval 86400
```

38 Назначение и классификация Cisco ACLs

ACLs (Access Control Lists) -- это универсальный механизм описания правил фильтрации пакетов, который может быть задействован различными подсистемами маршрутизаторов и коммутаторов.

ACLs не регламентируют едиными промышленными стандартами.

Фундаментально ACLs делят на три типа:

1. Port ACLs -- применимы к L2-интерфейсам (физическим портам).
2. Router ACLs -- применимы к L3-интерфейсам (обычным сетевым интерфейсам, SVIs и L3-EtherChannels).
3. VLAN ACLs (VLAN maps) -- применимы к виланам.

С точки зрения направленности потока пакетов ACLs могут быть:

1. Входными (inbound) -- предназначены для фильтрации входящего трафика, проверка происходит еще до маршрутизации.
2. Выходными (outbound) -- предназначены для фильтрации исходящего трафика, проверка происходит после маршрутизации.

Поэтому порядок ACEs критически важен.

ACL всегда заканчивается неявным запретом. Следовательно, при «непопадании » пакет отбрасывается (при отсутствии ACL, по умолчанию, пакет продвигается без ограничений).

С точки зрения синтаксиса ACLs могут быть:

1. Нумерованными (numbered) -- идентифицируются уникальными номерами. «Рядовые». Особенны тем, что не подлежат редактированию.
2. Именованными (named) -- идентифицируются уникальными названиями. Совместимы не со всеми командами. В качестве названий можно присваивать и номера, но согласно правилам для нумерованных ACLs. Особенны тем, что их можно редактировать (в соответствующих режимах конфигурирования добавлять или удалять ACEs).

39 Структура Cisco ACLs

Table *Access List Numbers*

Access List Number	Type
1–99	IP standard access list
100–199	IP extended access list
200–299	Protocol type-code access list
300–399	DECnet access list
400–499	XNS standard access list
500–599	XNS extended access list
600–699	AppleTalk access list
700–799	48-bit MAC address access list
800–899	IPX standard access list
900–999	IPX extended access list
1000–1099	IPX SAP access list
1100–1199	Extended 48-bit MAC address access list
1200–1299	IPX summary address access list
1300–1999	IP standard access list (expanded range)
2000–2699	IP extended access list (expanded range)

40 Правила фильтрации в Cisco ACLs и их обработка

Правило может быть разрешающим (permit) либо запрещающим (deny).

ACL создается после ввода первого его правила. Затем, по мере ввода дополнительных правил, ACEs автоматически дописываются в конец списка.

При этом ACEs автоматически последовательно нумеруются начиная с 10 с шагом 10, что открывает возможность вставлять дополнительные ACEs в «нужные места», но редактировать список произвольным образом возможности нет.

Номера в рабочей конфигурации не сохраняются, поэтому таковая автоматическая перенумерация происходит и после перезагрузки.

Команда ip access-list resequence позволяет автоматически перенумеровать ACEs когда угодно.

С одним интерфейсом одного уровня в одном направлении по одному протоколу может быть связан только один ACL.

При повторном связывании, предыдущий ACL вытесняется новым.

Аналогично, с одним виланом может быть связана только одна карта VLAN map. Применительно к VLAN map направление трафика не учитывается.

Port ACL проверяется перед router ACL и VLAN map.

С одним интерфейсом одного уровня в одном направлении по одному протоколу может быть связан только один ACL.

Поступивший пакет последовательно, в направлении от начала к концу ACL, сопоставляется с ACEs -- вплоть до первого выполнения условия фильтрации.

При обнаружении «попадания » пакет дальше не подвергается анализу, то есть либо пропускается, либо отбрасывается.

Поэтому порядок ACEs критически важен.

ACL всегда заканчивается неявным запретом. Следовательно, при «непопадании » пакет отбрасывается (при отсутствии ACL, по умолчанию, пакет продвигается без ограничений).

Какая часть IP-адреса должна учитываться при фильтрации, задают с помощью так называемой wildcard-маски: нули соответствуют учитываемым битам, единицы -- неучитываемым.

Ключевые слова any и host позволяют сослаться на любой и конкретный хост соответственно.

Более сложные технологии фильтрации являются дальнейшим развитием идеи автоматизации создания и активации правил.

Для облегчения работы с ACLs, если не обойтись без очень большого числа правил фильтрации, Cisco предлагает так называемые группы объектов (object groups).

Cisco FPM (Flexible Packet Matching) позволяет осуществлять фильтрацию пакетов по специальным шаблонам с точностью до бита.

Правило для фильтрации TCP-трафика может содержать флаг established -- говорит о том, что правило будет применяться только к TCPсоединениям находящимся в таковом состоянии. Если флаг ACK в TCPсегменте не установлен, то считается, что соединение устанавливается (например, извне) и сегмент отбрасывается.

41 Нумерованные стандартные IP ACLs и их примеры

Пример создания нумерованного стандартного IP ACL (запрет IP-трафика только от одной станции).

```
Router(config)#access-list 99 deny host 192.168.11.100
Router(config)#access-list 99 permit any
```

42 Именованные стандартные IP ACLs и их примеры

Router(config)#ip access-list standard WEB
Router(config-ext-nacl)#access-list 99 deny host 192.168.11.100
Router(config-ext-nacl)#access-list 99 permit any

43 Нумерованные расширенные IP ACLs и их примеры

Пример создания нумерованного расширенного IP ACL (запрет обращения станциям из подсети к серверу по протоколу HTTP).

Router(config)#access-list 199 deny tcp 192.168.11.128 0.0.0.31 host 192.168.11.11 eq www

Router(config)#access-list 199 permit tcp any any

44 Именованные расширенные IP ACLs и их примеры

Пример создания именованного расширенного IP ACL (аналогичный запрет обращения станциям из подсети к серверу по протоколу HTTP).

Применительно к названиям ACLs, как и к другим названиям, Cisco рекомендует использовать прописные буквы. При этом прописные и строчные буквы различаются.

```
Router(config)#ip access-list extended WEB
Router(config-ext-nacl)#deny tcp 192.168.11.128 0.0.0.31 host 192.168.11.11 eq www
Router(config-ext-nacl)#permit tcp any any
Router(config-ext-nacl)#exit
```

45 Правила и примеры привязки классических ACLs

ACL обязательно нужно привязать к чему-либо, иначе ACL не имеет смысла.
Примеры привязки ACLs к интерфейсам.

```
Router(config)#interface gi0/0
Router(config-if)#ip access-group 99 in
Router(config-if)#exit

Router(config)#interface gi0/1
 Router(config-if)#ip access-group WEB out
Router(config-if)#exit
```

Привязка ACL к линии возможна, но имеет особенности.

```
Router(config)#access-list 23 permit host 192.168.11.11
Router(config)#access-list 23 deny any

Router(config)#line vty 0 4
Router(config-if)#ip access-class 23 in
Router(config-if)#exit
```

46 VLAN maps и их примеры

Mapping VLAN - функция на коммутаторах позволяющая заменить текущий идентификатор (номер VID) VLAN на другой. С помощью этой функции можно перенаправлять траффик приходящий на коммутатор в определенной vlan в нужную нам vlan.

Карта VLAN map предназначена для отображения одного либо нескольких ACLs в один либо несколько виланов.

Карта указывает действие (forward -- по умолчанию, либо drop), которое нужно совершить с пакетом при попадании, то есть «срабатывании» одного из списков ACL (под «срабатыванием» ACL здесь понимают «срабатывание» именно одного из разрешающих правил; следовательно явные запрещающие правила практически не имеют смысла, разве что ускоряют обработку ACL при большом числе специфических разрешающих правил).

Если ни один из списков ACL «не сработал» то пакет неявно отбрасывается.

Карту идентифицируют названием и номером. Номер позволяет объединять отдельно взятые карты с одинаковыми названиями -- по аналогии с ACEs в ACL (если номер не указан, то присваивается автоматически с шагом 10). Название используют при привязке карты к виланам.

```
Switch(config)#vlan access-map MAP1 10
Switch(config-access-map)#match ip address ACL1
Switch(config-access-map)#action forward
Switch(config-access-map)#exit

Switch(config)#vlan access-map MAP1 20
Switch(config-access-map)#match ip address 190 191
Switch(config-access-map)#action drop
Switch(config-access-map)#exit

Switch(config)#vlan filter MAP1 vlan-list 2
```

В учебниках от Cisco безапелляционно сформулированы два базовых правила размещения ACLs:

1. Расширенные ACLs нужно располагать как можно ближе к источнику нежелательного трафика.
2. Стандартные ACLs нужно располагать как можно ближе к защищаемым станциям

47 IPv6 ACLs и их примеры

IPv6 ACL в настоящее время находятся в состоянии разработки и имеют ограничения.

Отличия IPv6 ACL от IPv4 ACL:

1. Только именованные, причем только расширенные.

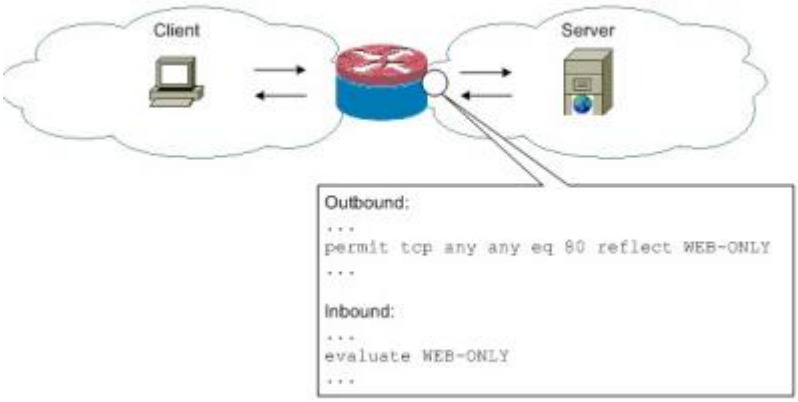
2. Привязывают к интерфейсу командой ipv6 traffic-filter.

3. Используют не wildcard-маски, а IPv6-префиксы.

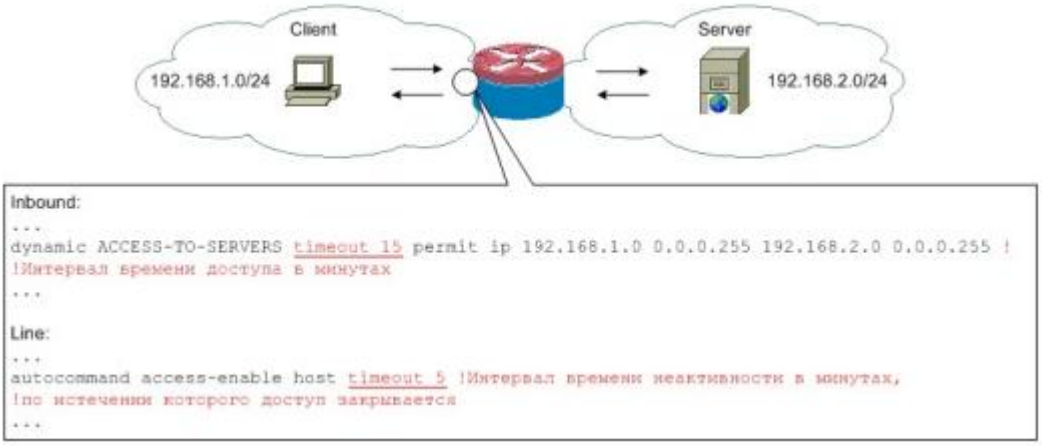
4. Перед неявным запретом в самом конце, есть еще два неявных разрешающими правила: permit icmp any any nd-na и permit icmp any any nd-ns.

48 Комплексные ACLs и их примеры

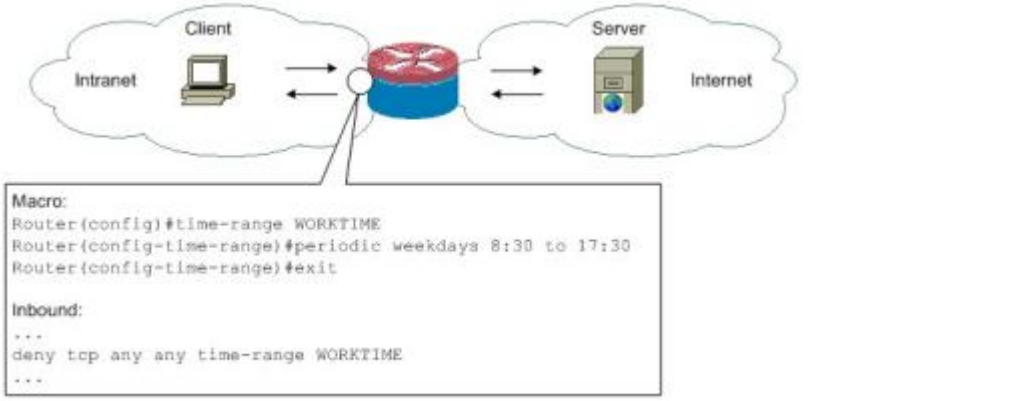
Идея рефлексивных ACLs заключается в том, чтобы для некоторого правила некоторого ACL автоматически активировать его особым образом описанное «обратное» правило другого ACL, «открывающее дверь» для ответного трафика.



Идея динамических ACLs (по-другому, Lock-and-key) заключается в том, чтобы автоматически активировать на некоторое время подготовленное правило (placeholder) (только одно) некоторого ACL по условию. Условием является успешность аутентификации посредством Telnet либо SSH.



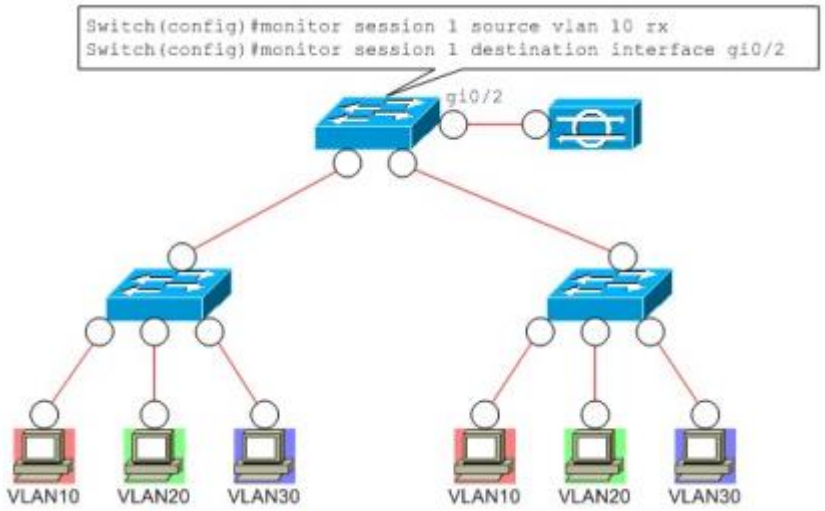
Временны'е ACLs, в отличие от динамических, срабатывают по расписанию. В правило включается предварительно подготовленное макро time-range.



49 Port Mirroring и Storm Control, их примеры

Типичные реализации одного из подходов для анализа трафика известны как Port Mirroring -- дублирование входящих или исходящих кадров определенного физического порта на другом порте.

Применительно к оборудованию Cisco, аналогичную технологию называют SPAN (Switched Port Analyzer). Плюс RSPAN (Remote SPAN).



Существуют технологии сдерживания штормов кадров под обобщенным названием Storm Control.

storm-control {broadcast | multicast | unicast}
level {level [level-low] | bps bps [bps-low] | pps pps [pps-low]

SW1(config-if)#storm-control multicast level bps 10m

50 Протоколы для активного сетевого оборудования одного производителя и стекирование коммутаторов, их примеры

Разработаны протоколы, позволяющие активному сетевому оборудованию одного производителя определять наличие друг друга

Применительно к оборудованию D-link, соответствующий протокол называют DDP (D-Link Discovery Protocol).

Применительно к оборудованию Cisco, соответствующий протокол называют CDP (Cisco Discovery Protocol).

Устройство посылает мультикаст-анонс (advertisement) на MAC-адрес 01-00-0c-cc-cc-cc. В конфигурации по умолчанию анонсы рассылаются каждые 60 секунд на порты Ethernet, Frame Relay и ATM. Каждое устройство, понимающее анонсы, сохраняет полученную информацию в CDP-таблице и позволяет посмотреть её по команде show cdp neighbors, и более детально по команде show cdp entry устройство. Если устройство трижды не прислало анонс (при значениях по умолчанию — 3 минуты (180 секунд)), оно удаляется из таблицы.

Указание с какого интерфейса будет взят IP-адрес, который передается в CDP пакетах:

dyn1(config)# cdp source-interface lo 0

Изменение частоты отправки пакетов CDP (в секундах):

dyn1(config)# cdp timer 10

Стекирование позволяет объединить несколько коммутаторов (обычно одинаковых) в единую сущность -- с целью наращивания количества портов.

Наряду с традиционным стекированием посредством специальных разъемов как правило расположенных на задней панели), все большее распространение получает стекирование посредством Ethernet-портов с высокой пропускной способностью (расположенных на передней панели) (distributed, horizontal, front panel stacking). А так же «чисто » виртуальное стекирование.

Обычное физическое стекирование осуществляют с помощью стековых портов (stack ports).

По сути, стековые порты -- это разъемы для соединения ASICs разных коммутаторов.

Стековые порты устанавливают парами.

Использование обоих стековых портов позволяет обеспечить полноценную пропускную способность и, заодно, резервирование.

Согласно правилам хорошего тона, стековые порты следует соединять кольцом.

Взаимодействие через стековые порты осуществляется по специальному протоколу (stack protocol).

Протокол имеет ряд версий (например, для 3750G с IOS 12.2(46) версия равна 1.40).

Версии с различными мажорными частями номеров (обычно при различных мажорных частях номеров версий IOS) несовместимы, с различными минорными частями -- совместимы частично.

51 Конфигурирование стека коммутаторов в IOS

Каждый коммутатор в составе стека должен иметь уникальный номер (stack member number).

Учет номера позволяет обратиться к определенному порту определенного коммутатора.

Если коммутатор является стекируемым, то номер включен в систему нумерации портов изначально (даже если по факту коммутатор не является членом стека).

По умолчанию номер равен единице, может быть изменен командой switch ... renumber.

Номер хранится в переменной окружения SWITCH_NUMBER (можно присвоить значение напрямую -- в режиме ПЗУ -монитора).

Номер может быть изменен как до, так и после начала членства коммутатора в стеке.

Если номер не назначен вручную, то назначается автоматически: выбирается минимальный доступный.

Если обнаружен конфликт номеров, то так же выбирается минимальный доступный.

Изменение номера учитывается только после перезагрузки.

Центром администрирования и управления стеком является один из коммутаторов -- стек -мастер.

Системные настройки стек -мастера относятся ко всему стеку.

Стек-мастер выбирается автоматически исходя из приоритета (stack member priority).

По умолчанию приоритет равен единице, может быть изменен switch ... priority.

Приоритет задают числом от 1 до 15.

Приоритет хранится в переменной окружения SWITCH_PRIORITY.

Изменение приоритета учитывается только при следующем выборе (перевыборе).

Рекомендуемый вариант назначения предпочтительного коммутатора стек-мастером -- это увеличение приоритета

Стек-мастером становится коммутатор с наибольшим цифровым значением приоритета.

При равенстве приоритетов учитываются конфигурации портов.

Выбирается коммутатор с конфигурацией портов, отличной от конфигурации портов по умолчанию.

При наличии нескольких таковых коммутаторов учитываются лицензии.

Выбирается коммутатор с самой «старшей» лицензией. 4.9.4.12a

Ну и в последнюю очередь, учитываются MAC-адреса.

Выбирается коммутатор с наименьшим MAC-адресом.

Идентификатор моста (включая MAC-адрес) всего стека равен идентификатору моста стек-мастера.

Командой stack-mac persistent timer текущий MAC-адрес стека можно сделать персистентным на некоторое время (чтобы удерживался после сбоя стек-мастера).

```
3750g(config)#switch 1 renumber 2
3750g(config)#switch 1 priority 15
3750g(config)#stack-mac persistent timer 0 !В минутах (0 -- бесконечность)
3750g(config)#interface gi2/0/1 !Номер коммутатора в стеке
```

Для просмотра состояния стека используют команду show platform stack-manager all (show platform stack manager all), того или иного коммутатора в отношении стека -- show switch.

StackPower позволяет оптимизировать распределение питания при объединении коммутаторов в стек (так же посредством дополнительных разъемов и соответствующих кабелей).

Горизонтальное стекирование или, по -другому, Single IP Management осуществляют и конфигурируют аналогично, только порты назначают.

Стекирование StackWise Virtual осуществляют с помощью виртуальных физических каналов (StackWise virtual links).

На дочерних устройствах-расширителях Nexus, для подключения к родительским коммутаторам Nexus устанавливают специальные uplink-порты.

52 Семейство стандартов Wi-Fi

Wi-Fi	Каналы	Модуляция и кодирование	Скорости	Ориентировочная дальность
802.11b (1999, вместо 802.11)	2,4 GHz: до 4 x 20 MHz (до 7 x 20 MHz – с учетом перекрытий)	802.11 (DSSS: DBPSK, DQPSK); DSSS: CCK, PBCC	802.11 (1, 2 Mbit/s); 5,5, 11 Mbit/s	до 30 m (типовые условия)
802.11a (1999)	5 GHz: до 19 x 20 MHz	OFDM: BPSK, QPSK, 16-QAM, 64-QAM и BCC	6, 12, 24 Mbit/s (обязательные), 9, 18, 36, 48, 54 Mbit/s	меньше 802.11b
802.11g (2003)	2,4 GHz: 802.11b (при OFDM до 3 x 20 MHz)	802.11b; OFDM, PBCC, DSSS-OFDM	802.11b; 6, 12 и 24 Mbit/s (обязательные), 9, 18, 36, 48, 54 Mbit/s	примерно равно 802.11b
802.11n (2009)	2,4 GHz: 802.11b (либо 2 x 40 MHz – с учетом перекрытия); 5 GHz: 802.11a + 4 x 20 MHz либо до 11 x 40 MHz	802.11a; 802.11g; MIMO (SU, до 4x4:4) OFDM: BPSK, QPSK, 16-QAM, 64-QAM и BCC, LDPC	до 600 Mbit/s (на практике меньше)	больше 802.11b
802.11ad (WiGig) (2012)	2,4 GHz: 802.11n; 5 GHz: 802.11n; 60 GHz (основная область): 4 x 2,16 GHz	DMG Control:, SC:, OFDM: DBPSK, SQPSK, QPSK, 16-QAM, 64-QAM, π/2-BPSK, π/2-QPSK, π/2-16QAM и LDPC, блочные коды	до 6,8 Gbit/s	до 10 m
802.11ac (2013)	5 GHz: 802.11n + 1 x 20 MHz либо 802.11n +1 x 40 MHz либо до 6 x 80 MHz либо до 2 x 160 MHz либо несмежные 80+80 MHz	802.11n (без 802.11g); SU-MIMO (до 8x8:8), MU-MIMO (только downlink, до 4 пользователей, до 4 потоков на пользователя, всего до 8 потоков) OFDM: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM и BCC, LDPC	до 1,3 Gbit/s (Wave 1); до 5,2 Gbit/s (Wave 2); до 6,9 Gbit/s (в теории)	примерно равно 802.11n
802.11ax (Wi-Fi 6) (черновик)	2,4 GHz: 802.11n; 5 GHz: 802.11ac; 6 GHz: до 59 x 20 MHz либо до 29 x 40 MHz либо до 14 x 80 MHz либо до 7 x 160 MHz либо несмежные 80+80 MHz	802.11g; 802.11ac; SU-MIMO (до 8x8:8), MU-MIMO (downlink и uplink, аналогично 802.11c) OFDM:, OFDMA: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM и BCC, LDPC	до 9,6 Gbit/s (в теории)	больше 802.11ac

53 Физический уровень Wi-Fi

Очевидно, физический уровень Wi-Fi устроен сложно.

В отличие от Ethernet, переход от канального уровня к физическому предполагает дополнительную инкапсуляцию и заключается в том, что CSMA/CA (равно DCF) задействует PLCP (Physical Layer Convergence Protocol).

При этом MPDUs (собственно кадры Wi-Fi, рассмотренные ранее) вкладываются в PPDUs (PLCP Protocol Data Units) -- вкладываются как PSDUs (PLCP Service Data Units).

Таким образом, используют четыре частотные области (bands): 2,4, 5, 6 и 60 GHz.

Области 2,4 и 5 GHz известны как ISM (Industrial, Scientific and Medical) и U-NII (Unlicensed National Information Infrastructure) соответственно (законодательство США) и освоены в первую очередь.

В области 5 GHz четко выражены три поддиапазона (sub-bands).

Базовый алгоритм Wi-Fi предполагает использование в качестве канала (здесь термин channel) одной более или менее узкой полосы частот.

Каналы могут быть шириной примерно 20 (как в 802.11b), 40, 80 и 160 MHz (в WiGig еще 2,16 GHz). Так же допустимы каналы, сформированные из пар несмежных каналов шириной 80 MHz.

Заметно, что «распараллеливание» реализуют не одновременным использованием нескольких каналов (с канальным перемежением и фрагментацией), а «слиянием» (своеобразной агрегацией) каналов.

Обобщенно, один канал представлен одной несущей (carrier).

Однако, по правилам модуляции OFDM, несущую делят на множество поднесущих (subcarriers) -- от 64 в каналах шириной 20 MHz до 512 в каналах шириной 160 MHz.

Увеличение ширины канала позволяет увеличить количество поднесущих и, следовательно, скорость.

Часть поднесущих используют для служебных целей: нулевые (null) позволяют лучше изолировать каналы, а так называемые пилотные (pilot) позволяют лучше детектировать каналы (например, 48 информационных плюс 12 нулевых плюс 4 пилотных).

Наличие поднесущих, на следующем шаге развития, позволяет по-своему повысить гибкость.

Так, по правилам модуляции OFDMA из поднесущих разрешено формировать так называемые блоки ресурсов (resource units) -- чтобы ресурсы канала можно было динамически распределять для обеспечения «параллельного» взаимодействия более чем двух устройств (от 26 до 996 фиксированных информационных поднесущих в одном блоке).

Вопрос №54. Каналы WI-FI

Базовый алгоритм Wi-Fi предполагает использование в качестве канала (здесь термин channel) одной более или менее узкой полосы частот. Каналы могут быть шириной примерно 20 (как в 802.11b), 40, 80 и 160 MHz (в WiGig еще 2,16 GHz). Так же допустимы каналы, сформированные из пар несмежных каналов шириной 80 MHz. Заметно, что «распараллеливание» реализуют не одновременным использованием нескольких каналов (с канальным перемежением и фрагментацией), а «слиянием» (своеобразной агрегацией) каналов.

Обобщенно, один канал представлен одной несущей (carrier). Однако, по правилам модуляции OFDM, несущую делят на множество поднесущих (subcarriers) -- от 64 в каналах шириной 20 MHz до 512 в каналах шириной 160 MHz. Увеличение ширины канала позволяет увеличить количество поднесущих и, следовательно, скорость. Часть поднесущих используют для служебных целей: нулевые (null) позволяют лучше изолировать каналы, а так называемые пилотные (pilot) позволяют лучше детектировать каналы (например, 48 информационных плюс 12 нулевых плюс 4 пилотных)

Наличие поднесущих, на следующем шаге развития, позволяет по-своему повысить гибкость. Так, по правилам модуляции OFDMA из поднесущих разрешено формировать так называемые блоки ресурсов (resource units) -- чтобы ресурсы канала можно было динамически распределять для обеспечения «параллельного» взаимодействия более чем двух устройств (от 26 до 996 фиксированных информационных поднесущих в одном блоке)

В стандартах Wi-Fi приведена одна из систем нумерации каналов. Существует и ряд альтернативных систем нумерации (в том числе не связанных с Wi-Fi). Наборы каналов вариативны, так как на использование тех или иных каналов в разных странах наложены свои ограничения. В таблице указано максимальное количество одновременно доступных для выбора каналов. Допустимо перекрытие (overlap) каналов, что актуально в отношении сложно организованных и конфликтующих беспроводных сегментов. Но на практике перекрытие каналов порождает проблемы, поэтому его следует избегать. В этом смысле показательна область 2,4 GHz с каналами 802.11b

Вопрос №55. Модуляция и кодирование в рамках Wi-Fi

В стандартах 802.11 описан ряд способов модуляции и кодирования: 1. PPM (Pulse Position Modulation) -- модуляция позициями импульсов (изначально в 802.11, для IR). 2. FHSS (Frequency Hopping Spread Spectrum) -- широкополосная модуляция со скачкообразным изменением частоты (изначально в 802.11, для 2,4 GHz). 3. DSSS (Direct Sequence Spread Spectrum) -- широкополосная модуляция с прямым расширением спектра. 4. BPSK (Binary Phase Shift Keying) и QPSK (Quadrature Phase Shift Keying) -- соответственно двоичное и квадратичное манипулирование фазовыми сдвигами. +5. DBPSK (Differential BPSK) и DQPSK (Differential QPSK) -- дифференциальные варианты BPSK и QPSK. +6 SQPSK (Spread QPSK) -- раздвоенный вариант QPSK. 7. CCK (Complementary Code Keying) -- манипулирование дополнительными кодами. 8. BCC (Binary Convolutional Coding) -- двоичное сверточное кодирование. +9. PBCC (Packet Binary Convolutional Coding) -- пакетный вариант BCC

10. OFDM (Orthogonal Frequency Division Multiplexing) -- мультиплексирование с ортогональным частотным разделением. +11. OFDMA (Orthogonal Frequency Division Multiple Access) -- множественный доступ с ортогональным частотным разделением. 12. QAM (Quadrature Amplitude Modulation) -- квадратурная амплитудная модуляция. 13. MIMO (Multiple Input, Multiple Output) -- множественный ввод -вывод (с использованием нескольких антенн). +14. SU-MIMO (Single-User MIMO) -- однопользовательский вариант MIMO. +15. MU-MIMO (Multi-User MIMO) -- многопользовательский вариант MIMO. 16. LDPC (Low-Density Parity Check) -- низкоплотная проверка паритета. 17. DMG Control -- контроль DMG (контроль в особом режиме называемом DMG). 18. SC (Single Carrier) -- использование одной несущей. И некоторые другие

Физическая модуляция сильно переплетена с канальным кодированием в отношении PPDU. Канальное кодирование может быть как проявлением модуляции, так и дополнительным преобразованием данных. Модуляция может быть многоуровневой (например, в связке с OFDM, к отдельно взятой поднесущей может применяться QAM). И канальное кодирование может быть многоуровневым (например, LDPC всегда предшествует простейшее «перемешивание» -- scrambling -- с целью равномерного распределения нулей и единиц). Поддержка той или иной модуляции (кодирования) может быть как обязательной, так и опциональной. С учетом совместимости, модуляция (кодирование) автоматически подбирается в зависимости от требующейся скорости. В рамках одного стандарта, одни и те же каналы могут использоваться по -разному

Вопрос №56. Стандарты беспроводной связи, кроме Wi-Fi

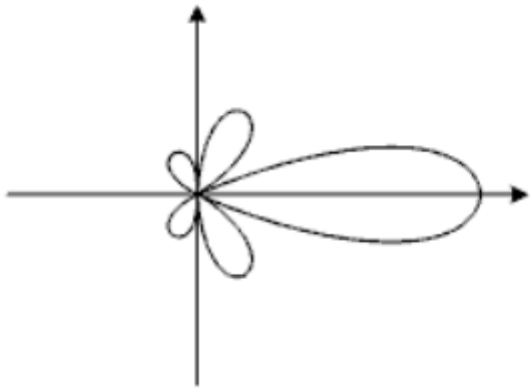
Беспроводное пользовательское устройство информирует станцию - координатор о переходе в режим (выходе из режима) энергосбережения с помощью флага в поле контроля кадра. Предназначенные «спящему » устройству информационные кадры должна буферизировать станция - координатор. «Спящее » устройство может только принимать кадры-«маяки » и передавать специальные контролирующие (не управляющие) кадры (power save poll). Если анализ информационного элемента TIM (Traffic Indication Map) в кадре-«маяке » говорит о наличии буферизованных информационных кадров, то передается соответствующий запрос. «Пробуждение » происходит при необходимости принимать или передавать информационные кадры. Начиная с 802.11ax (точнее, 802.11ah), поддерживается TWT (Target Wake Time), что позволяет согласовать время «пробуждения » беспроводного пользовательского устройства (группы устройств).

Теперь стандарты: 1. Satellite broadband -- спутниковая связь; LMDS и MMDS; скорость ориентировочно до 10 Mbit/s. 2. Cellular broadband -- мобильная связь; поддержка доступна начиная со второго поколения мобильных телефонов (2G); 2G: GSM, CDMA и TDMA; 3G: EDGE, CDMA2000, HSPA+, UMTS; 4G: WiMAX и LTE; 5G (пока много вопросов). 3. WiMAX (Worldwide Interoperability for Microwave Access) -- для городских и глобальных сетей; 802.16; расстояние до 50 km; скорость до 1 Gbit/s. 4. Bluetooth -- для персональных сетей; 802.15; три версии; расстояние (v3) до 100 m (long range), до 10 m (ordinary range), до 10 cm (short range); скорость (v3) до 24 Mbit/s. 5. NFC (Near-Field Communication) -- для широкого применения на очень коротких расстояниях; до 10 cm; скорость до 0,5 Mbit/s. И другие: HomeRF, Wireless 1394, xG, ..

Вопрос №57 Антенны для беспроводного сетевого оборудования и сопутствующие расчеты

Практически используют внутренние и внешние антенны самых разных конструкций вплоть до ФАР (фазированных антенных решеток). Например, применительно к SOHO, очень часто используют антенны Single Detachable Reverse SMA.

Антенна излучает энергию во всех направлениях, но неравномерно. Основным параметром, определяющим эффективность антенны в определенном направлении является диаграмма направленности -- зависимость мощности излучения от пространственных координат. Примером может служить диаграмма направленности параболической антенны



Направленная параболическая антенна обеспечивает усиление сигнала: G = 4 πA / λ 2 , dB, где A -- площадь; λ -- длина волны несущей.

Основой устойчивой связи является прямая видимость между передающей и принимающей антеннами. При передаче в эфир, ключевую роль в поглощении волн в атмосфере играет вода в том или ином виде. Дождь, снег или туман могут существенно ухудшить качество связи. В добавок, на более низких частотах влияют в основном грозовые разряды, а на более высоких -- космическое излучение. Затухание радиоволн в беспрепятственной воздушной среде рассчитывают по упрощенной формуле: L = 32,44 + 20lg (F) + 20lg (D) , dB, где F -- частота в GHz; D -- расстояние (в метрах)

Точки доступа Aironet могут использовать внешние антенны трех типов: 1. Omnidirectional -- всенаправленные (для применения на открытых пространствах). 2. Dipole -- дипольные (позволяют корректировать направленность). 3. Directional -- направленные (для применения в ограниченных пространствах), включая: -- patch -- патч-антенны или, по-другому, полосковые (для применения при небольшой дальности). -- yagi -- так называемые «яги» или, по-другому, «волновой канал» (для применения при повышенной дальности) весьма действенным способом борьбы с интерференцией является использование направленных антенн (beamforming)

Вопрос №58 Назначение и классификация беспроводного сетевого оборудования

Беспроводное сетевое оборудование делят на три типа: 1. Для домашних и офисных КС. 2. Для распределенных и городских КС. 3. Для беспроводных каналов связи. Кроме того, в отличие от проводного сетевого оборудования, оно может быть не только indoor, а и outdoor

Первым шагом в истории беспроводной компьютерной связи стали радиомодемы В дальнейшем, специфика беспроводных сетей привела к возникновению нового типа активного сетевого оборудования -- точек доступа (access points). Точки доступа предназначены для интеграции беспроводных и традиционных проводных сегментов

Классические точки доступа выполняют функции мостов. Все современные точки доступа, по сути, являются беспроводными маршрутизаторами, то есть маршрутизаторами, в которых кроме проводных сетевых интерфейсов имеются беспроводные. А вот под беспроводными мостами часто понимают беспроводные сегменты, связывающие проводные

Производители беспроводного сетевого оборудования совпадают с производителями проводного

Вопрос №59 Структура беспроводной сети

Топологически, в основу беспроводных сетей (не только Wi-Fi) положена так называемая сотовая структура. В общем случае предполагают наличие точек доступа -- режим инфраструктуры (infrastructure). СПД может состоять из одной либо нескольких сот (cells). Каждая сота управляется персональной точкой доступа. Точка доступа и ассоциированные с ней беспроводные пользовательские устройства образуют базовую зону обслуживания -- BSS (Basic Service Set). Точки доступа многосотовой сети взаимодействуют между собой посредством распределенной системы -- DS (Distribution System). DS -- это обычная проводная инфраструктура второго уровня (наполнение стандартами не регламентировано). Совокупность BSSes и DS образует расширенную зону обслуживания -- ESS (Extended Service Set). Из данной структуры закономерно «вытекает» что и находящиеся в одной соте беспроводные пользовательские устройства взаимодействуют посредством точки доступа

Для обеспечения возможности перемещения мобильных беспроводных пользовательских устройств из одних сот в другие предусмотрен роуминг (roaming, mobility -- в терминологии Cisco). Таким образом, ESS -- представляет собой отдельную сущность беспроводного сегмента (в общем случае, устроенного сложно)

Если же два беспроводных пользовательских устройства взаимодействуют не посредством точки доступа, а напрямую -- режим ad hoc, то образуется независимая базовая зона обслуживания -- IBSS (Independent BSS).

WiGig допускает использование еще одной (третьей) структуры -- режим DMG (Directional Multi-Gigabit). При этом образуется персональная базовая зона обслуживания -- PBSS (Personal BSS), в которой одну из станций назначают точкой контроля -- PCP (PBSS Control Point). Беспроводные пользовательские устройства взаимодействуют друг с другом напрямую, но под управлением точки контроля (предполагают наличие в каждом из устройств нескольких направленных антенн).

Вопрос №60 Идентификация и виланы в беспроводных сетях

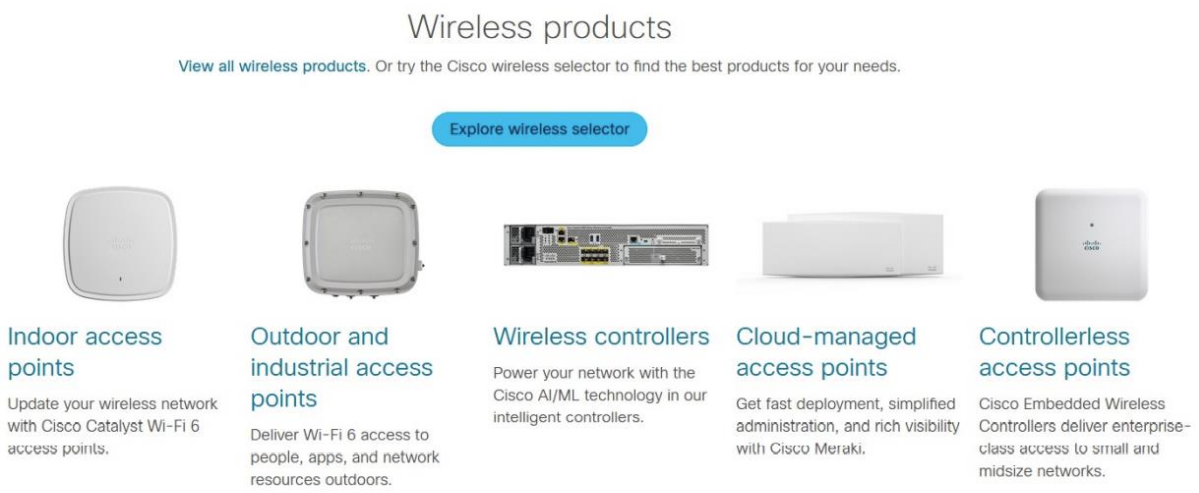
Концепция виланов вполне совместима с WLANs, правда с учетом особенностей. Беспроводные виланы представлены различными SSIDs, сосуществующими в рамках одной ESS (иногда приравнивают к multiple SSIDs). При рассмотрении классического порта доступа подразумевают, что стационарная пользовательская станция имеет доступ только к одному физическому порту, однако «спрятать » от мобильной пользовательской станции доступные SSIDs невозможно. Точка доступа должна ставить в соответствие беспроводные виланы (SSIDs) проводным (VIDs), следовательно, должна работать в режиме моста. Для управления самой точкой доступа создают административный вилан. Вне административного вилана может быть создан отдельный вилан, посредством которого легковесная точка доступа взаимодействует с WLC. Расширения виланов 802.1X также применимы, в том числе для динамического включения пользователей в виланы

Вопрос №61 Развертывание беспроводной сети

Рекомендации по развертыванию WLAN: 1. На основании имеющихся предпосылок выбрать беспроводную технологию. 2. Определить наличие ранее установленных WLANs в непосредственной близости, определить зоны их покрытия и частоты. 3. Экспериментальным или другим способом определить необходимое количество точек доступа (лучше, чтобы каждая точка доступа обслуживала менее десяти мобильных или стационарных беспроводных пользовательских станций). 4. Окончательно определиться с беспроводной технологией 5. Установить точки доступа с учетом наилучшего покрытия и интерференции, подключить их к проводным сегментам (лучше обеспечить некоторое перекрытие BSSes). 6. Выполнить базовую настройку точек доступа (задать IP-адреса, частоты, идентификаторы зон обслуживания и так далее). 7. Настроить права доступа на точках доступа (если требуется, шифрование -- WPA2, аутентификацию -- локальную или RADIUS/TACACS, списки MAC-адресов и другое). 8. Настроить дополнительные сетевые сервисы на точках доступа (обычно DHCP или NAT). 9. Наконец, настроить пользовательские станции (в соответствии с предыдущими пунктами)

Вопрос №62 Беспроводное сетевое оборудование Cisco

По состоянию на октябрь 2021 года беспроводное оборудование Cisco делят на пять основных целевые категорий



Вопрос №63 Беспроводные технологии Cisco

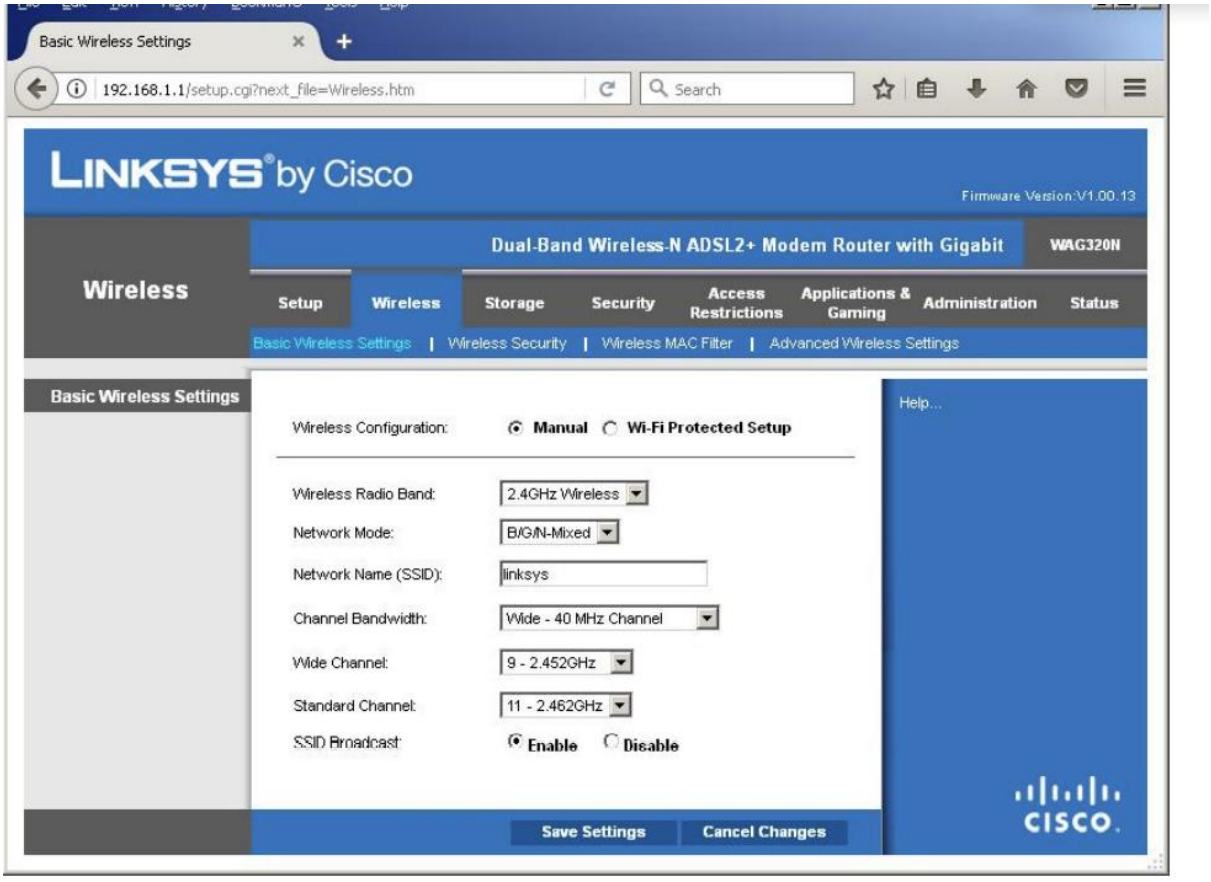
Технология Cisco CleanAir позволяет обеспечить интеллектуальное сосуществование точки доступа с другими точками доступа в «агрессивном» окружении, решая проблему интерференции

Технология Cisco OfficeExtend позволяет защищенным образом связать WLAN удаленного офиса и основную корпоративную WLAN

Несколько особняком стоит оригинальная технология Cisco Wireless Mesh, позволяющая без усилий строить на базе расставленных в outdoorокружении специальных точек доступа полнофункциональную сеть с произвольной физической топологией, динамически формировать каналы, находить ближайший WLC, оптимизировать трафик (своеобразная динамическая маршрутизация). Для этих целей разработан новый протокол -- AWPP (Adaptive Wireless Path Protocol)

Вопрос №64 Конфигурирование беспроводного маршрутизатора Linksys

Приблизительно в 2000 году, в результате приобретения компании Aironet, Cisco начала производство точек доступа enterprise/industrial -- под торговой маркой Aironet, и постепенно нарастила номенклатуру изделий. С 2003 по 2013 год Cisco владела компанией Linksys (торговая марка Linksys by Cisco), которой была отведена «львиная доля» направления SOHO/SMB. С 2010 года Cisco представлена своими моделями этого направления. С 2005 года Cisco выпускает легковесные точки доступа и WLCs



Linksys web interface

Вопрос №65 Интеграция компьютерных сетей в системы связи (не уверен в инфе)

Рассматриваемые КС переплетаются с традиционной связной инфраструктурой, при этом выделяют два направления интеграции: 1. КС интегрируют в системы связи. 2. Системы связи интегрируют в КС

Для передачи обычных голосовых сообщений, а так же компьютерной информации, используют стандартный так называемый канал тональной частоты (ТЧ -канал, voice channel). В свое время, для передачи речи была установлена полоса частот 300 -- 3400 Hz (4 kHz), что соответствует девяностопроцентному уровню разборчивости. В системах аналоговой связи применяют мультиплексирование с частотным разделением каналов -- Frequency Division Multiplexing (FDM). Каждый телефонный сигнал в результирующем объединенном сигнале занимает полосу частот 4 kHz. На базе ТЧ -каналов формируют так называемые групповые тракты (voice groups): первичный К-12 (12 ТЧ -каналов, 60 -- 180 kHz), вторичный К-60 (60 ТЧ -каналов, 312 -- 552 kHz), третичный К-300

Вопрос №66 Структура и синхронизация цифровых сетевых интерфейсов

Возможны два принципиально разных типа TDMs: 1. Синхронные (synchronous) -- время формирования тайм -слотов четко связано с тактированием и предопределено. 2. Асинхронные (asynchronous) -- тайм -слоты формируются по мере надобности. С пользовательской точки зрения, мультиплексируемые цифровые каналы как правило «нагружены » по -разному. При статистическом (statistical) мультиплексировании соотношение количеств тайм -слотов цифровых каналов в смешанном потоке соответствует востребованности этих цифровых каналов. Наконец, еще одним аспектом является согласованность работы связанных мультиплексоров. В нормативных документах предусмотрена комплексная схема создания и распространения синхросигналов, плюс описан ряд типовых моделей. Нужно учитывать два обстоятельства: -- источники синхронизации могут быть локальными и глобальными, причем в отношении как отдельных мультиплексоров, так и выделенных (из всех мультиплексоров в СПД) групп; -- элементы синхронизации включаются и в передаваемые кадры.

При классификации систем цифровой связи с точки зрения организации их синхронизации есть некоторая особенность. В первую очередь оценивают качество синхронизации. При этом регламентируют и количество сбоев, приводящих к так называемым проскальзываниям (slips).

В стандартах описаны 4 режима синхронизации передатчиков и приемников мультиплексоров в составе СПД: 1. Асинхронный (asynchronous) -- источники синхронизации не связаны друг с другом и относительно нестабильны (не более одного проскальзывания за 7 секунд). 2. Плезиохронный (plesiochronous) -- большинство источников синхронизации не связаны друг с другом, но они относительно стабильны (не более одного проскальзывания за 17 часов). 3. Псевдосинхронный (pseudo-synchronous) -- все источники синхронизации высокостабильны и многие из них привязаны к одному эталонному глобальному источнику (не более одного проскальзывания за 70 суток). 4. Синхронный (synchronous) -- все источники синхронизации привязаны к одному эталонному глобальному источнику (проскальзываний фактически нет)

Вопрос №67 Плезиохронная и псевдосинхронная цифровая иерархия

В стандартах описаны 4 режима синхронизации передатчиков и приемников мультиплексоров в составе СПД:

1. Асинхронный (asynchronous) -- источники синхронизации не связаны друг с другом и относительно нестабильны (не болееодного проскальзывания за 7 секунд).

2. **Плезиохронный** (plesiochronous) – большинство источников синхронизации не связаны друг с другом, но они относительно стабильны (не более одного проскальзывания за 17 часов).

3. **Псевдосинхронный** (pseudo-synchronous) – все источники синхронизации высокостабильны и многие из них привязаны к одному эталонному глобальному источнику (не более одного проскальзывания за 70 суток).

4. Синхронный (synchronous) -- все источники синхронизации привязаны к одному эталонному глобальному источнику (проскальзываний фактически нет).

Для реализаций **плезиохронного** режима характерно наличие независимых источников синхронизации, что приводит к необходимости «выравнивать» цифровые потоки. При накоплении погрешности задействуются прозрачные методы вставки или удаления битов (stuffing). «Выравнивание» на более высоких уровнях иерархии еще больше «запутывает» данные и делает невозможным их прямое извлечение.

Для реализаций **псевдосинхронного** режима характерно наличие централизованной синхронизации с больши'м числом резервных источников, а также включение в цифровые потоки метаданных об этих потоках, что не только обеспечивает дополнительную синхронизацию, а и позволяет напрямую извлекать данные.

Первыми нашли широкое применение реализации **плезиохронного** режима. Их постепенно вытесняют более совершенные реализации **псевдосинхронного** режима.

Плезиохронная цифровая иерархия -- PDH (Plesiochronous Digital Hierarchy) -- уже описана выше (G.704).

PDH базируется на электрических средах (G.703).

Воплощениями **псевдосинхронной** цифровой иерархии стали SONET (Synchronous Optical NETwork) (Telcordia GR-253-CORE, ATIS 0900105.06) в Северной Америке и SDH (Synchronous Digital Hierarchy) (G.783) в Европе.

Как SONET, так и SDH могут базироваться на электрических -- Electrical Signaling (ES) и оптических -- Optical Signaling (OS) средах (SONET: те же стандарты Telcordia и ATIS, SDH: G.703 и G.957).

В качестве первичных цифровых каналов приняты Optical Carrier level 1 (OC-1), Synchronous Transport Signal level 1 (STS-1) и Synchronous Transport Module level 1 (STM-1).

Применение коэффициентов кратности дает соответствующий ряд скоростей

Вопрос №68 Абонентское и провайдерское оборудование

Цифровое и аналоговое RAS-, WAN- и связное оборудование, прежде всего, делят на:

1. **Абонентское** -- CPE (Customer Premises Equipment) -- устанавливают у потребителя услуг.

2. **Провайдерское** -- SPE (Service Provider Equipment) -- устанавливают у поставщика услуг и интегрируют в инфраструктуру определенного уровня (например, городского).

Зоны ответственности абонента и провайдера разграничивает **демаркационная линия** (demarcation point). Где проходит демаркационная линия зависит от законодательства той или иной страны.

Физический канал между граничащими CPE и SPE принято называть **«последней милей»** («last mile») или **«локальной петлей»** («local loop»).

К **абонентскому** оборудованию относят, в первую очередь, различные модемы, различные телефонные аппараты и офисные АТС. Хотя на стороне абонента может быть и достаточно сложная инфраструктура.

К высокоспециализированному **провайдерскому** оборудованию относят, в первую очередь, различные коммутаторы и модули, устанавливаемые в маршрутизаторы и АТС.

Вопрос №69 Последовательные сетевые интерфейсы

Отличительной особенностью RASes и WANs является широкое применение последовательных сетевых интерфейсов различной пропускной способности -- вплоть до около 50 Mbit/s.

Большинство стандартов в области последовательных интерфейсов разработаны тремя организациями: ANSI/TIA/EIA (американские), ITU-T (международные) и ISO/IEC (международные).

Основные моменты, связанные с последовательными интерфейсами:

-- в стандартах четко разделены роли DCE и DTE;

-- при непосредственном соединении двух последовательных сетевых интерфейсов (третьего или более высоких уровней) имеют смысл только подключения DTE -- DCE и DTE -- DTE, при этом в первом случае применяют «прямые» кабели, а во втором -- кросс-кабели;

-- DTE и DCE отличаются формой контактов: M и F соответственно;

-- практически ни один из протоколов нельзя ассоциировать только с одним видом разъемов;

-- список цепей для взаимодействия DCE и DTE унифицирован и функционально полон;

-- цепи могут быть как несбалансированными (unbalanced, single-ended), так и сбалансированными (balanced, differential);

-- благодаря более эффективному заполнению полосы пропускания, в СПД значительно чаще применяют именно синхронный, а не асинхронный режим;

-- в синхронном режиме синхронизация, как правило, осуществляется не путем вставки в информационные цепи синхробайтов, а путем тактирования через отдельные цепи;

-- в нормальной ситуации источником тактирования является DCE, но иногда эту роль возлагают на DTE (например, при подключениях DTE--DTE);

-- тактовый генератор обычно один, но для тактирования предусмотрены несколько независимых цепей: при передаче от DCE, при приеме от DCE, при передаче от DTE, при приеме от DTE; как альтернативу, допускают внешнее тактирование; возможно побитное и побайтное тактирование;

-- последовательные интерфейсы образуют не только point-to-point-топологии, но и различные point-to-multipoint-топологии;

– как и положено, компьютерная информация передается по последовательным интерфейсам в виде пакетов (кадров), при этом возможны канальное кодирование, канальное сжатие и канальное фрагментирование;

-- отличительной особенностью последовательных интерфейсов является отсутствие MAC-адресов.

Ключевые стандарты: TIA-232, TIA-422, TIA-423, TIA-449, TIA-530, V.35, X.21 и HSSI (High Speed Serial Interface).

Основные разъемы: DE-9, DA-15, DB-25, DC-37, LFH60, ISO 2593 и SS26

Вопрос №70 Протокол PPP и смежные протоколы

При применении топологий point-to-point в RASes и WANs значительное место отведено протоколу **PPP** (Point-to-Point Protocol) (RFC 1661).

Протокол **PPP** пришел на смену протоколу **SLIP** (Serial Line IP).

PPP -- это очень гибкий протокол второго уровня, который позволяет устанавливать канальное point-to-point-соединение. Затем это соединение может использоваться практически любыми протоколами третьего уровня, причем «одновременно» (SLIP поддерживает только IP).

Над PPP концентрируется очень большое количество протоколов. Из четырех групп можно выделить две основные:

1. **LCPs** (Link-layer Control Protocols).

2. **NCPs** (Network Control Protocols).

Собственно **LCP** (Link Control Protocol) обеспечивает создание, конфигурирование, опциональное тестирование, контроль состояния и закрытие соединения.

Под конфигурированием понимают согласование опций инкапсуляции, то есть согласование максимальной длины пакетов, способа аутентификации, способа сжатия и другое. Тем самым происходит адаптация к конкретной СрПД.

Работа **LCP** базируется на механизме запросов-подтверждений.

Набор NCPs позволяет адаптировать подготовленное соединение к нуждам протоколов третьего уровня и включает: **IPCP** (IP Control Protocol), **IPv6CP**, **IPXCP**, **CCP** (Compression CP) и так далее.

Например, **IPCP** позволяет согласовать возможность сжатия заголовков пакетов и правило назначения IP-адреса.

PPP поддерживает два алгоритма аутентификации на канальном уровне:

1. **PAP** (Password Authentication Protocol) -- «двойное рукопожатие», разовый обмен незашифрованными PAP-сообщениями.

2. **CHAP** (Challenge Handshake Authentication Protocol) -- «тройное рукопожатие», периодический обмен зашифрованными CHAP-сообщениями.

Еще две серьезные возможности PPP:

1. **Multilink** -- задействование соединением ресурсов нескольких параллельных физических каналов (фрагментация, перемежение, балансировка нагрузки и другое).

2. **Bridging** -- поддержка мостов

Вопрос №71 Конфигурирование последовательных сетевых интерфейсов в IOS

Пример настройки последовательного сетевого интерфейса маршрутизатора Cisco (по умолчанию считается DTE).

```
Router(config)#interface se0/0/0
Router(config-if)#clock rate 64000
Router(config-if)#encapsulation ppp
Router(config-if)#ppp multilink
Router(config-if)#exit
```

Примеры настройки PAP- и CHAP-аутентификации между двумя маршрутизаторами.

```
R1(config)#username router2 password cisco
R1(config)#interface se0/0/1
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication pap
R1(config-if)#exit

R2(config)#interface se0/0/0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp pap sent-username router2 password cisco
R2(config-if)#exit

R1(config)#username R2 password cisco
R1(config)#interface se0/1/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication chap
R1(config-if)#exit

R2(config)#username R1 password cisco
R2(config)#interface se0/1/1
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication chap
R2(config-if)#exit
```

Вопрос №72 Обзор технологии Dial-up и структура Dial-up RAS

Первой широко распространенной технологией подключения удаленных пользователей стала технология Dial-up.

Традиционные модемы используют сложившуюся телефонную инфраструктуру и соответственно ту же полосу частот, что и телефоны (0 -- 4 kHz).

На абонентской стороне устанавливают внутренний либо внешний Dialup-модем, на провайдерской -- внутренний либо внешний, аналоговый либо цифровой модемный пул.

Посредником является то, что в настоящее время принято называть традиционной телефонной сетью общего пользования -- **PSTN** (Public Switched Telephone Network) или, по-другому, **POTS** (Plain Old Telephone Service). PSTN охватывает сеть возможно разных **АТС** (лучше telephone exchanges).

В настоящее время почти все **АТС** цифровые и применяют основном цифровые модемные пулы.

Офисные АТС -- PBX (Private Branch Exchanges) относят к CPE.

На RAS-сервере (которым может быть и маршрутизатор) происходит так называемое терминирование (termination) абонентских сессий.

Вершиной развития стал стандарт V.92, утвердивший скорость 56 kbit/s.

Вопрос №73 Обзор технологии ISDN и структура ISDN-домена

Первой достаточно широко распространенной полностью цифровой технологией, пришедшей на смену Dial-up и как Dial-up уже устаревшей, стала **ISDN** (Integrated Services Digital Network).

ISDN предназначена для передачи разнородного трафика и эту технологию условно относят к технологиям коммутации цепей.

В архитектуре и структуре ISDN-домена выделяют **четыре плана** (control, management, transport, user), для каждого из которых предусмотрены набор интерфейсов и набор устройств: ISDN-модемы, ISDN-коммутаторы и другие (в том числе ISDN-терминал-адаптеры для подключения к ISDN аналоговых оконечных устройств).

Сетевые интерфейсы ISDN состоят из каналов следующих видов:

1. **D-канал** (Delta channel) -- используется для сигнализации и контроля (но в исключительных случаях и для пересылки данных) -- обычно packet-switched 16 kbit/s.

2. **B-канал** (Bearer channel) -- используется для пересылки электронных данных, голоса и видео -- circuit- либо packet-switched DS0.

3. **H-канал** (Hybrid channel) -- транк из некоторого количества B-каналов.

Стандартизированы два вида сетевых интерфейсов ISDN:

1. **BRI** (Basic Rate Interface) -- базовый -- типичная схема: 2B (128 kbit/s) + 1D (I.430).

2. **PRI** (Primary Rate Interface) -- первичный -- схема: 23B (1,472 Mbit/s) + 1D либо 30B (1,92 Mbit/s) + 1D (I.431).

BRI и PRI были определены в ISDN изначально и известны как **N-ISDN** (Narrow-band ISDN).

В **B-ISDN** (Broadband ISDN) определены скорости до 622 Mbit/s (I.432).

Недостаточно сильная стандартизация процесса сигнализации привела к несовместимости оборудования и возникновению трех основных типов ISDN-коммутаторов: Lucent (AT&T), Nortel и Siemens.

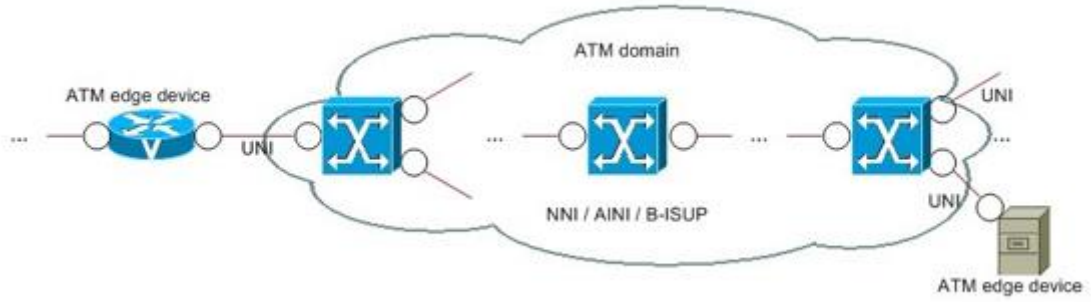
Проблема несовместимости в США была решена внедрением стандарта **National ISDN.**

Вопрос №74 Обзор технологии ATM и структура ATM-домена

Технология **ATM** (Asynchronous Transfer Mode) уходит корнями в B-ISDN и связана с NBMA-топологиями.

ATM условно относят к технологиям коммутации пакетов.

Серьезными достоинствами ATM являются заложенные поддержка качества обслуживания разнородного трафика и ориентированность на соединение.



ATM-домен (ATM domain) состоит из некоторого количества объединенных ATM-коммутаторов (ATM switches) и подключенных к ним граничных ATM-устройств (ATM edge devices).

Граничными ATM-устройствами могут быть маршрутизаторы, пользовательские станции, коммутаторы с поддержкой ATM и так далее.

Согласно идее ATM, информация передается посредством фиксированной длины кадров, называемых **ячейками** (cells) (53 байта, 5 байтов заголовок и 48 байтов наполнение.

Немного абстрактный термин **виртуальная цепь** (VC -- Virtual Circuit) в приложении к ATM считают синонимом термина **виртуальный канал** (так же VC -- Virtual Channel) и раскрывают как связывающую два абонентских граничных ATM-устройства цепочку под названием **VCC** (Virtual Channel Connection), состоящую из ограниченных физическими каналами между ATM-портами звеньев под названием **VCLs** (Virtual Channel Links).

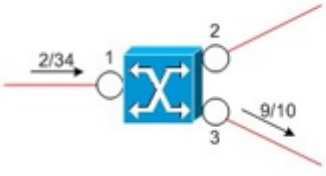
VCs объединяют в группы, называемые **VPs** (Virtual Paths).

В пределах физического канала может существовать множество VCLs. Каждый VCL, а следовательно и VC со стороны абонента, идентифицируют парой:

1. **VPI** (Virtual Path Identifier).

2. **VCI** (Virtual Channel Identifier).

Принцип работы ATM-коммутатора.



Switching table

Ingress		Egress	
Port	VPI/VCI	Port	VPI/VCI
1	2/33	2	3/44
1	2/34	3	9/10
2	3/44	1	2/33
3	9/10	1	2/34

Таким образом, коммутация выполняется исходя из значения **VPI/VCI** в заголовке ячейки.

Пара VPI/VCI значима только в пределах физического канала и поэтому может меняться в процессе пересылки ячейки по ATM-домену.

Значения VCI от **0 до 31 зарезервированы**.

Ячейки с нулевыми значениями VPI и VCI считаются пустыми.

Виртуальные цепи ATM бывают трех видов:

1. **PVCs** (Permanent Virtual Circuits) -- и на граничных ATM-устройствах, и на ATM-коммутаторах, пары VPI/VCI администраторы задают статически.

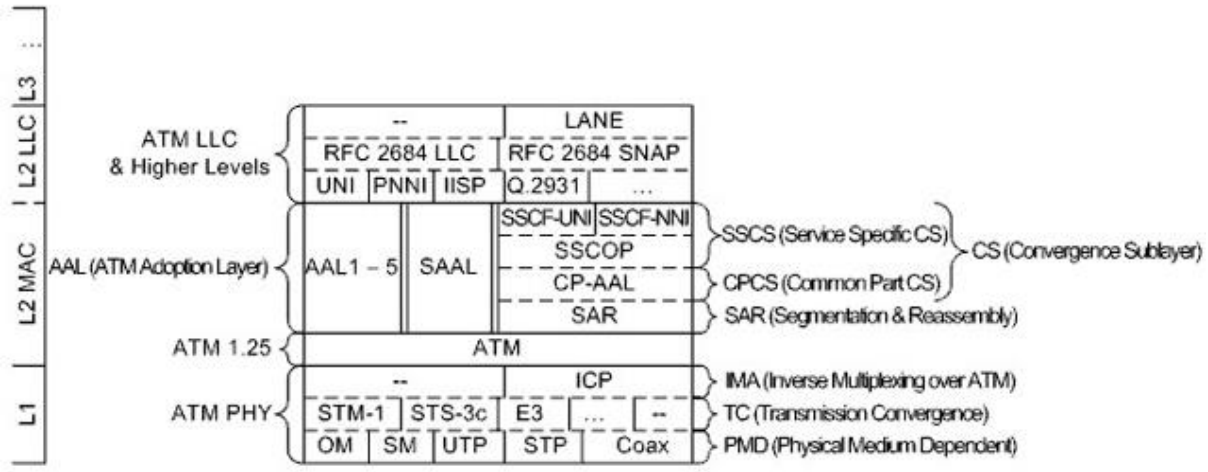
2. **SVCs** (Switched Virtual Circuits) -- пары VPI/VCI и таблицы коммутации формируются ATM-коммутаторами динамически и автоматически.

3. **Soft PVCs** -- гибриды PVCs и SVCs, связь между граничными ATM-устройствами и ATM-коммутаторами организована по PVC-правилам, а между ATM-коммутаторами -- по SVC-правилам.

Для обеспечения возможности создания SVCs со стороны граничных ATM-устройств используется специальный механизм -- **сигнализация**.

Вопрос №75 Примеры инкапсуляции в ATM-системе

Сопоставить **ATM** с моделью **OSI** весьма сложно, так как ATM представляет собой целый «мир», внутри которого смело можно выделить семь уровней в соответствии с той же моделью OSI.



На физическом уровне выделяются два основных подуровня.

На подуровне PMD осуществляется: генерация и восстановление битов, модуляция и демодуляция, соединение с физической средой.

На подуровне TC осуществляется: адаптация к СрПД, возможная упаковка ячеек в другие кадры с подсчетом и проверкой контрольных сумм, разграничение ячеек, обеспечение заданной (decoupling) скорости потока. В зависимости от вида конкретной СрПД, ячейки могут вставляться и изыматься напрямую. Типичные реализации ATM ориентированы на потоки T3/E3.

Иногда, например для обеспечения нестандартной скорости потока, делают распараллеливание путем наращивания числа физических каналов и вводят еще один соответствующий подуровень-надстройку -- IMA, на котором с помощью протокола ICP (IMA Control Protocol) осуществляется управление мультиплексированием потока ячеек.

Применительно к ATM, канальный уровень имеет очень сложную структуру.

На подуровне собственно ATM осуществляется: генерация и распознавание ячеек, проверка заголовков ячеек, коммутация виртуальных цепей, управление потоком ячеек. (В синхронных средах пустые ячейки распознаются по нулевым значениям VPI/VCI).

На подуровне SAR осуществляется фрагментация на ячейки подготовленного (converged) кадра с более высоких подуровней (передающая сторона) и сборка (принимающая сторона).

На подуровне CS осуществляется преобразование поступившего с более высоких подуровней кадра в ATM-совместимую форму. При этом SSCS обеспечивает требующиеся характеристики трафика, а CPCS -- адаптацию и проверку.

Для решения задач AAL задействуются следующие протоколы: SSCF-UNI (Service Specific Coordination Function - UNI), SSCF-NNI, SSCOP (Service Specific Connection Oriented Protocol), CP-AAL (Common Part AAL Peer-to-Peer Protocol).

Различные варианты AAL (AAL1 -- AAL5) можно считать различными вариантами качества обслуживания. Способ инкапсуляции AALx определяет форматы пакетов SSCS, CPCS, SAR и то, как они вкладываются друг в друга. Наиболее часто применяется инкапсуляция AAL5.

При сигнализации вызывается функционал SAAL (Signaling AAL), который задействует все подуровни AAL.

За UNI-сигнализацию отвечает протокол Q.2931.

При NNI-сигнализации, при назначении SVCs, правильное направление определяется за счет так называемой ATM-маршрутизации.

Есть два типа ATM-маршрутизации:

1. IISP (Interim Interswitch Signaling Protocol) -- статическое задание ATM-маршрутов.

2. PNNI (Private Network-to-Network Interface) -- поиск и динамическое задание ATM-маршрутов.

Услугами ATM могут пользоваться самые разные приложения, взаимодействующие по разным семействам протоколов.

На граничном ATM-устройстве, поступающие с третьего уровня пакеты могут использовать ATM не только напрямую (native), а и посредством эмуляции MAC-уровня LAN -- LANE (LAN Emulation).

В любом случае, используется многопротокольная инкапсуляция по правилам RFC 2684 (усовершенствование RFC 1483), которая бывает двух видов: LLC (Logical Link Control) и SNAP (Subnetwork Access Protocol). В результате, пакеты разных L3-протоколов могут пересылаться по одной виртуальной цепи.

Вопрос №76 Семейство стандартов xDSL

Одними из наиболее широко применяемых в настоящее время RAS-технологий являются технологии под общим названием xDSL (Digital Subscriber Loop).

Семейство xDSL представляет собой «облегченный» вариант ATM, пришедший, после некоторой паузы, на смену ISDN.

Технологии DSL соответствуют физическому уровню модели OSI и, как и следует из названия, их относят к локальной петле.

Задействуется полоса частот выше 4 kHz, поскольку ресурсы медной пары этим не ограничиваются.

Стандарты xDSL разрабатывают не только ITU-T (серия G) и ADSL Forum, но и другие организации и компании.

В настоящее время семейство стандартов xDSL включает:

1. HDSL (High bit rate DSL) (G.991.1).

+2. SDSL (Symmetric DSL).

+3. SHDSL (Single-pair HDSL) (G991.2 = G.shdsl). +4. SHDL.bis (G991.2 Annex F).

5. ADSL (Asymmetric DSL) (G.992.1 = G.dmt, G.992.2 = G.lite -- без сплиттеров).

+6. ADSL2 (G.992.3, G.992.4 -- без сплиттеров). +7. ADSL2+ (G.992.5).

+8. ADSL2++.

9. VDSL (Very high bit rate DSL) (G.993.1). +10. VDSL2 (G.993.2).

Вопрос №77 Каналы и модуляция в рамках xDSL

Стандарты различают по: способам модуляции, способам кодирования, способам подавления шумов, частотным диапазонам, скорости и дальности передачи.

Модуляции:

1. **CAP** (Carrierless Amplitude and Phase Modulation) -- нетребующая наличия несущей амплитудно-фазовая.

2. **TCPAM** (Trellis Coded Pulse Amplitude Modulation) -- амплитудная с кодированием импульсов решетчатым кодом.

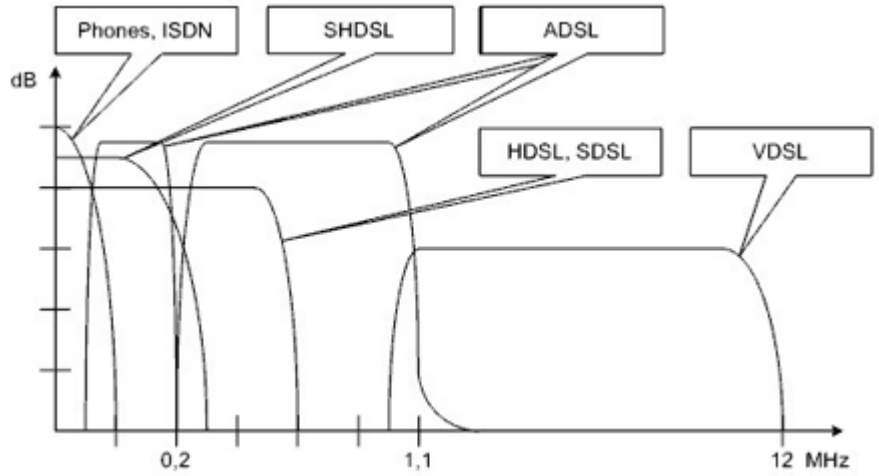
3. **DMT** (Discrete Multi Tone) -- дискретная многотональность.

4. **QAM** (Quadratic Amplitude Modulation) -- квадратурная амплитудная (просто квадратурная).

С точки зрения организации каналов, нужно разделять:

1. **Направление** передачи **upstream** и **downstream** -- соответственно от абонента к провайдеру и наоборот.

2. **Симметричность** (symmetric) и **несимметричность** (asymmetric) каналов -- исходя из двух взаимосвязанных характеристик: частоты канала и возможности задействовать канал в определенном направлении).



Таким образом, можно говорить о трех устоявшихся группах технологий: **ADSL** (асимметричные), **SHDSL** (симметричные) и **VDSL** (гибридные). Но явно доминируют именно ADSL.

В случае с ADSL, по правилам модуляции DMT, данные передаются одновременно по большому количеству (до 256 -- ADSL и ADSL2, до 512 --ADSL2+) параллельных каналов (по 4 kHz шириной).

Часть каналов, расположенных в нижней области рабочей полосы частот, используется как upstream, оставшиеся -- как downstream.

В зависимости от отношения сигнал-шум для каждого из каналов выбираются соответствующие уровни квадратурной модуляции.

При подключении по xDSL, и на стороне абонента, и на стороне провайдера, необходимо использование сплиттеров -- для исключения взаимовлияния частот PSTN и xDSL.

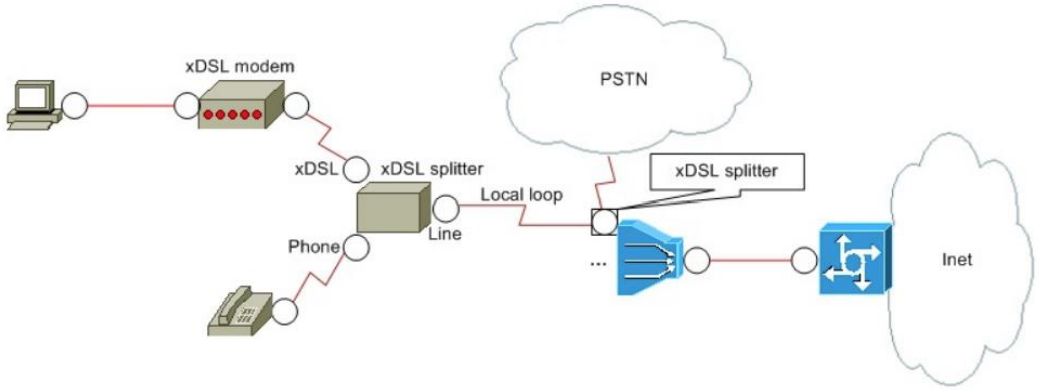
При использовании xDSL не обойтись без особого типа активного провайдерского сетевого оборудования -- без DSLAM (DSL Access Multiplexor), предназначенного для агрегирования xDSL-линий.

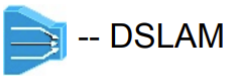
Часто DSLAM мультиплексирует множество xDSL-линий в один Ethernet-канал, при этом упаковывая поступающие от абонентов пакеты в отдельные виланы.

На стороне провайдера сплиттеры обычно встроены в DSLAM

Вопрос №78 Структура xDSL RAS

Одними из наиболее широко применяемых в настоящее время RASтехнологий являются технологии под общим названием xDSL (Digital Subscriber Loop). Семейство xDSL представляет собой «облегченный » вариант ATM, пришедший, после некоторой паузы, на смену ISDN. Технологии DSL соответствуют физическому уровню модели OSI и, как и следует из названия, их относят к локальной петле. Задействуется полоса частот выше 4 kHz, поскольку ресурсы медной пары этим не ограничиваются



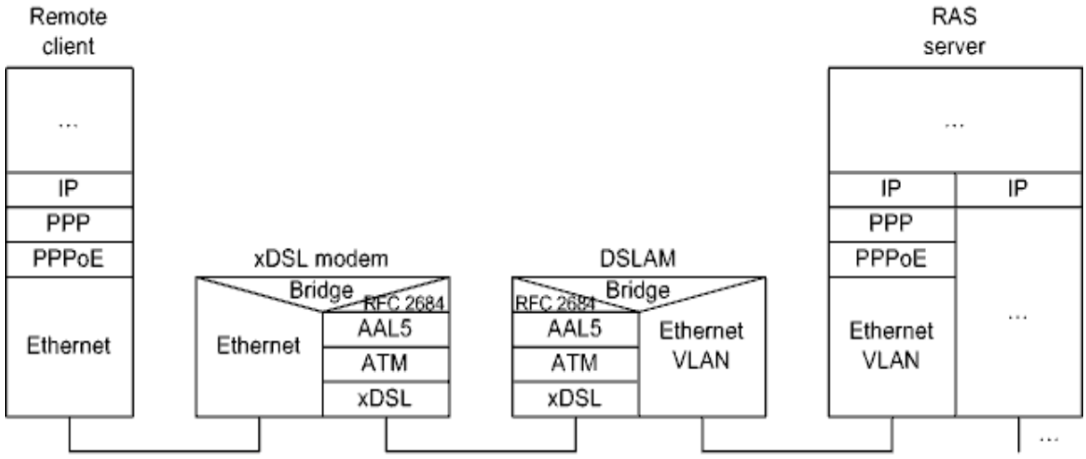


Инфраструктура (второго и третьего уровней) между DSLAM и RASсервером может быть достаточно сложной и состоять из множества разных устройств. Может применяться даже L2-туннелирование через L3-СПД с помощью протокола L2TP (Layer 2 Tunneling Protocol)

Вопрос №79 Примеры инкапсуляции в xDSL-системе(не уверен)

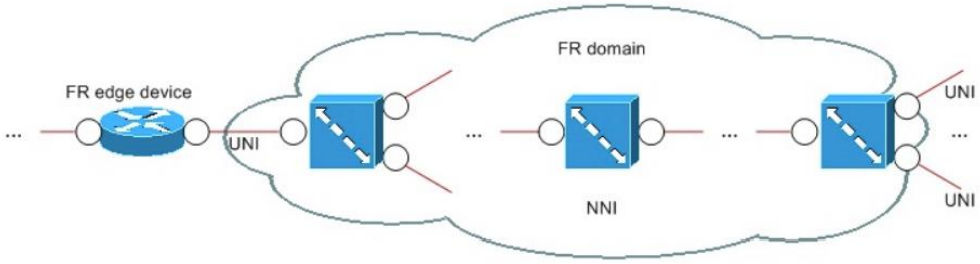
Надстройкой над xDSL является архитектура ATM. Как правило, протоколы третьего уровня задействуют ATM через PPPпрослойку. При этом возможны два варианта, выраженные в соответствующих протоколах: 1. PPPoA (PPP over ATM) (RFC 2364) -- напрямую (но в связке с многопротокольной инкапсуляцией). 2. PPPoE (PPP over Ethernet) (RFC 2516) -- посредством эмуляции Ethernet (так же в связке с многопротокольной инкапсуляцией).

В общем случае, возможно множество вариантов организации xDSLсистемы. Одним примером может служить xDSL-система, в которой используется PPPoE, PPPoE-клиент установлен на удаленной пользовательской станции, DSLAM работает с виланами



Вопрос №80 Обзор технологии FR и структура FR-домена

Структура и архитектура FR-домена напоминает структуру и архитектуру доменов X.25, ISDN и ATM



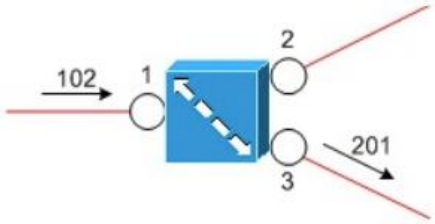
Технология FR (Frame Relay) произошла от X.25 и Narrowband ISDN. Как и ATM, связана с NBMA-топологиями, но устанавливать соединение не позволяет. FR условно относят к технологиям коммутации пакетов.

Вопрос №81 Виртуальные цепи ATM, FR и подобных технологий

По аналогии с ATM, поддерживается два вида подинтерфейсов FR (по умолчанию multipoint), при конфигурировании которых следует придерживаться аналогичных правил. И при использовании подинтерфейсов FR-инкапсуляцию включают на уровне интерфейса. При статическом связывании PVCs создаются автоматически. В IOS оригинальной особенностью поддержки использующих виртуальные цепи технологий (FR, ATM и прочих), в сравнении с другими технологиями, является то, что для обеспечения достижимости собственного сетевого интерфейса необходимо связать свой IP-адрес с одной из имеющихся PVC

Вопрос №82 Принцип работы ATM- и FR-коммутаторов

Принцип работы FR-коммутфтора



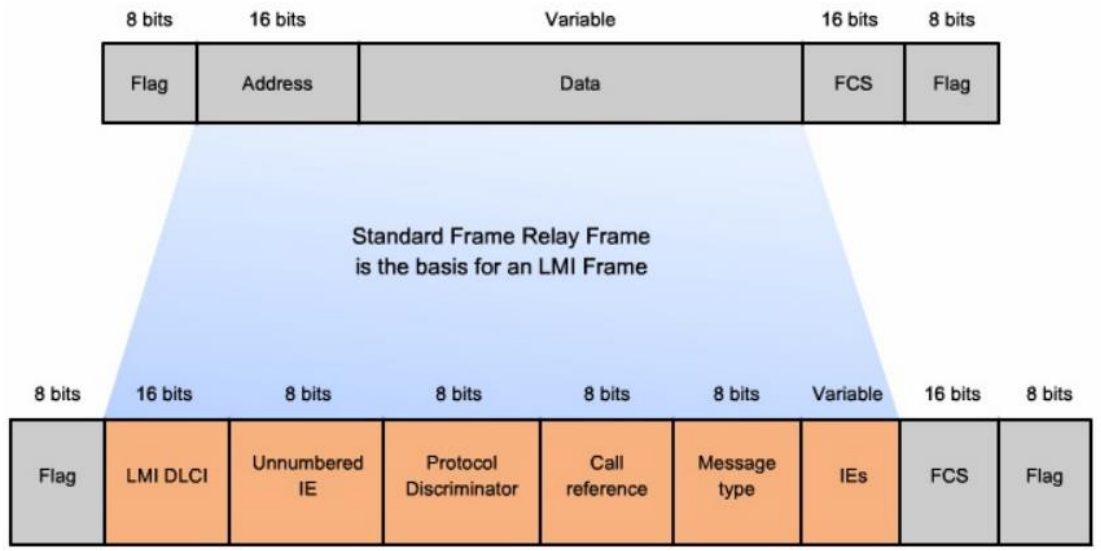
Switching table

Ingress		Egress	
Port	DLCI	Port	DLCI
1	102	3	201
1	103	2	103
2	103	1	103
3	201	1	102

Маршрутизатор Cisco может выполнять роль FR-коммутатора. Непосредственное соединение маршрутизаторов Cisco по FR (без коммутатора) возможно, но смысла не имеет (в отличие от ATM). При этом одна из сторон должна быть в роли DTE (что по умолчанию), а вторая -- DCE (можно назначить только после ввода команды frame-relay switching), причем FR-роли DTE и DCE могут не совпадать с ролями DTE и DCE последовательных сетевых интерфейсов (накладывают «поверх»)

Вопрос №83 Протоколы ILMI и ELMI

В FR, так же как и в ATM, имеется LMI, точнее ELMI (Enhanced LMI). Так же происходит периодический обмен (по умолчанию 10 s). За достаточно длительную историю FR были разработаны три стандарта LMI: 1. ITU-T Q.933 Annex A -- общепромышленный стандарт, задействуется DLCI = 0. 2. ANSI T1.617 Annex D -- альтернативный общепромышленный стандарт, так же задействуется DLCI = 0. 3. «Gang of Four» (= Cisco) -- разработан Cisco, DEC, StrataCom и Nortel -- задействуется DLCI = 1023



Формат кадра FR LMI [Cisco]

В IOS поддерживаются все три стандарта LMI: q933a, ansi, cisco (по умолчанию cisco). По умолчанию включено автосогласование (LMI autosense)