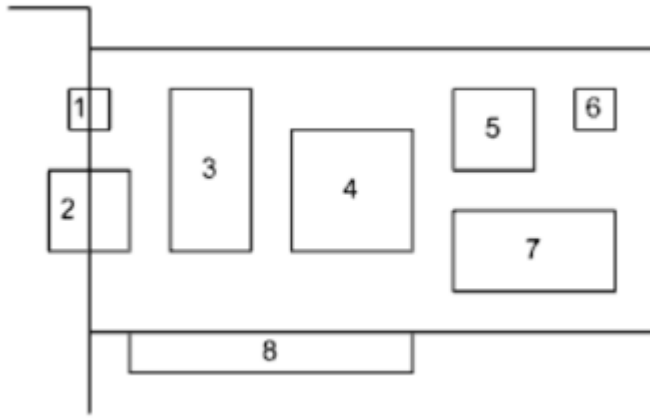


1. Назначение и структура сетевых адаптеров

Сетевые адаптеры необходимы для подключения пользовательских станций (компьютеров) к компьютерным сетям.



Обобщенная структура включает в себя:

1. Блок индикации.
2. Разъем для подключения к СрПД.
3. Приемопередатчик (блок развязки для подключения к определенной СрПД).
4. Сетевой контроллер.
5. Блок перемычек. (может устанавливать номер прерывания, адреса портов ввода-вывода и памяти) Отсутствует для адаптера PNP.
6. ПЗУ для хранения настроек по умолчанию.
7. Гнездо для boot ROM.
8. Разъем для подключения к шине расширения компьютера.

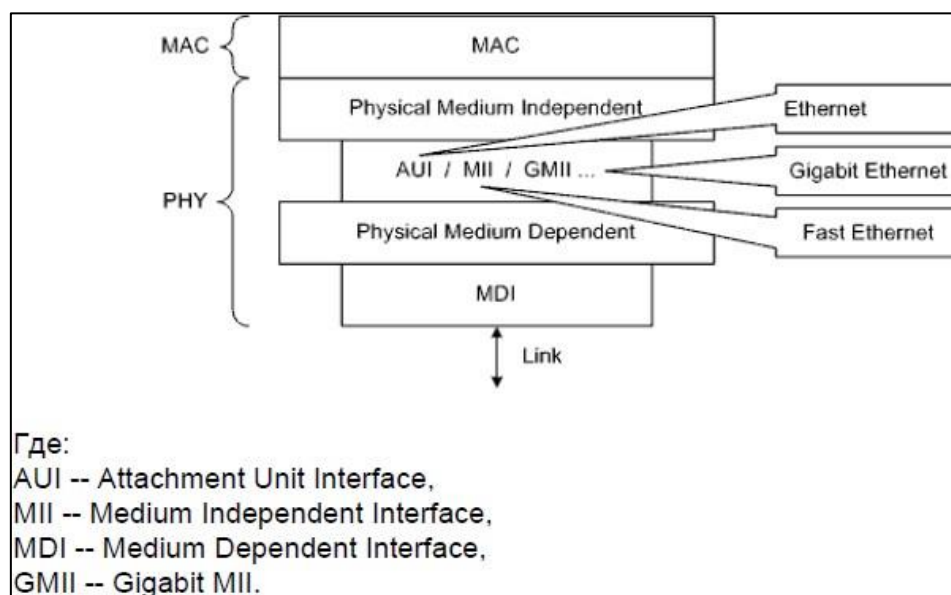
2. Соответствие компонентов сетевых адаптеров модели OSI

Блок PHYsical не обязательно интегрирован в кристалл контроллера – он может быть изготовлен на основе отдельной микросхемы.

По факту интерфейсы AUI (репитеры и всё пассивное, что коннектится к интерфейсу) и MII (сами интерфейсы) соответствуют физическим разъемам.

Ситуация с интерфейсом GMII (Gigabit MII) 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.



Соответственно, где PHY - это L1 (physical), MAC – L2 (Data link)

3. Характеристики и критерии выбора сетевых адаптеров

Характеристики и критерии выбора сетевых адаптеров:

- 1) СрПД. (Serial / Telephone Pair / Twisted Pair)
- 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, скорости и тд.
- 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

Поколения сетевых адаптеров Ethernet:

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

2. Шина ISA; 16 битов; дискретная элементная база; управление переключателями; 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 переключателями, 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.

(можно запомнить, как 1-3 – подключение к коаксиальному, до 32 бит | 4-5 подключение к витой паре, 32-64 бита.)

5. Назначение и классификация пассивного сетевого оборудования

Сетевое оборудование предназначено не для анализа передаваемой информации, а, в первую очередь, для обеспечения требующихся технических характеристик, называют пассивным.

Общая классификация:

1. Оконечные концентраторы-- работают с сигналами на физическом уровне модели OSI и тем самым осуществляют передачу принимаемых пакетов во всех направлениях
2. Повторители-- осуществляют усиление принимаемых сигналов
3. Приемопередатчики -- подключают к коммутаторам и маршрутизаторам посредством стандартных разъемов, осуществляют передачу пакетов в определенные СрПД и прием пакетов из них.
4. Модули -- оригинальные модули маршрутизаторов и коммутаторов (некоторые модули можно рассматривать как активное сетевое оборудование).
5. Медиаконвертеры -- осуществляют преобразование СрПД
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.

Общая классификация:

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

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

3. Шлюзы – осуществляют «перенаправление» сетевых сервисов прикладного уровня.

// + можно нарисовать в каких сегментах сети находится коммутатор и маршрутизатор

7. Структура коммутатора и методы коммутации

Коммутаторы можно свести к трем базовым структурным схемам:

1. На основе коммутационной матрицы -- пакеты между портами проходят по выделенным путям, проложенным через коммутационную матрицу.
2. На основе разделяемой шины -- пакеты проходят через связывающую все порты общую высокоскоростную шину.
3. На основе разделяемой памяти -- пакеты перемещаются между портами посредством размещения в общей для всех портов памяти.

Следует различать программную и аппаратную буферизацию.

Основные методы коммутации:

1. Store and Forward -- с промежуточной буферизацией -- коммутатор получает пакет полностью перед его ретрансляцией; анализируется DST address и checksum.
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 получения 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).

В таблице хранится соответствие MAC-адресов и портов.

При приеме 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 неизвестным юникаст-MAC-адресом назначения ретранслируются всеми портами.

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

Smart-коммутаторы при ретрансляции пакетов учитывают виланы.

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

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

9. Гибридные технологии L2 -- L3

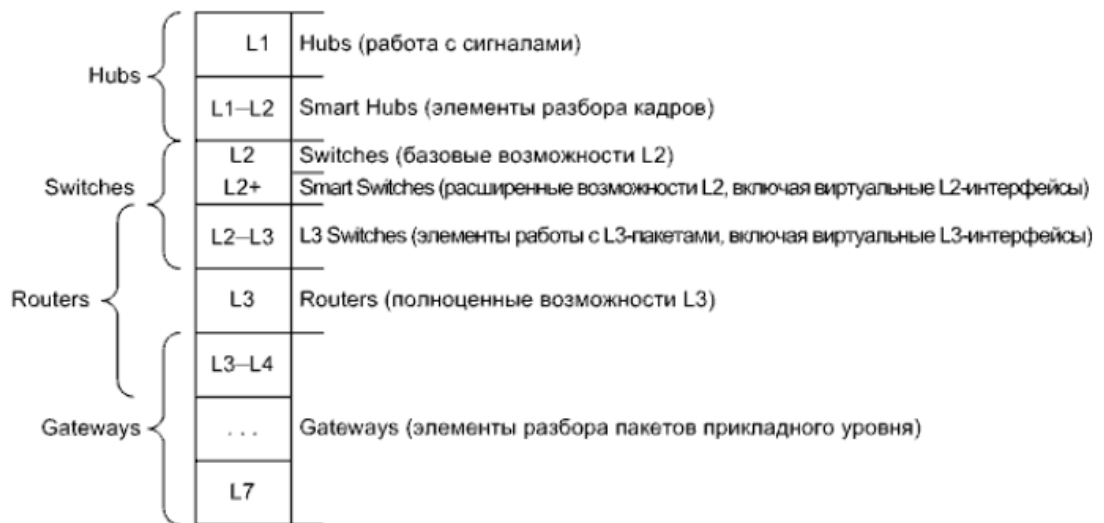
В случае с более совершенными коммутаторами, добавлены возможности работы с адресами сетевого уровня.

Традиционно выделяют три основных типа коммутаторов 3-го 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

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 автоматического 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:

1. Intel (в готовом виде уже давно не производит) (Shiva, Express, NetStructure),
2. HP (3COM) (OfficeConnect, Baseline, SuperStack), HPE (ProCurve), Aruba (HPE),
3. Cisco (множество серий коммутаторов Catalyst и маршрутизаторов), Avaya(Nortel) (Passport, Baystack, Netgear, много серий), Alcatel-Lucent (Nokia) (много серий),
4. Juniper (много серий),
5. Allied Telesis (много серий),
6. Commscope (Ruckus)
7. Zyxel (Omni LAN, Dimension),
8. Broadcom (Persona),
9. Marvell (Prestera), и некоторые другие.

Low-end:

1. Huawei,
2. D-Link,
3. Compeh,
4. CeLAN,
5. Realtek и другие.

12. Коммутаторы Cisco

Коммутаторы Cisco делятся на 5 основных целевых категорий (Access, Core and distribution, Data center and cloud, Industrial Ethernet, Small business and LAN compact).

Основу всех трех основных сегментов рынка (SOHO, SMB, Enterprise) составляют различные серии флагманских коммутаторов Catalyst

Для сегмента рынка SOHO доступны несколько серий не Catalyst-коммутаторов, которые немного дешевле, но поддерживают все основные возможности.

Коммутаторы Nexus предназначены для центров обработки данных, имеют основные порты 10 Gigabit Ethernet (за очень редким исключением). Уже доступны модели с основными портами 100 Gigabit Ethernet, причем некоторые с low latency – особый класс оборудования (системы реального времени с регламентированными коммутационными задержками).

Некоторые серии поддерживают модули, стекирование.

Для наращивания портов коммутаторов Nexus вместо стекирования используют внешние устройства-расширители. У относительно дешевых коммутаторов нет тумблеров питания.



Catalyst 2960

13. Cisco IOS и коммутаторы

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.

Коммутаторы серии 2960 поставляли со встроенным web-интерфейсом -- адаптированным вариантом SDM (2960+ поставляют с CP for Catalyst).

Исключением, в смысле администрирования, являются не Catalyst-коммутаторы. Они вовсе не имеют CLI («младшие» серии) либо имеют упрощенный CLI, называемый Textview («старшие» серии), зато имеют полноценный встроенный web-интерфейс

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.

14. Конфигурирование порта Ethernet коммутатора 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
```

```
Switch(config)#interface gil/1
```

```
Switch(config-if)#media-type sfp // Small form-factor port
```

```
Switch(config-if)#exit
```

```
Switch(config)#interface gil/0/1
```

```
Switch(config-if)#flowcontrol receive on
```

```
Switch(config-if)#exit
```

```
Switch(config)#interface range gi0/1 - 10
```

```
Switch(config-if-range)#power inline never !Отключить PoE
```

```
Switch(config-if-range)#exit
```

15. Таблица коммутатора Cisco 2960

// + рассказать, что такое CAM-таблица, для чего используется

Для просмотра таблицы используют команду `show mac-address-table` на L2 коммутаторах и команду `show mac address-table` L3 коммутаторах.

В таблице содержится:

1. информация о VLAN
2. mac-адрес устройства назначения
3. тип коммутации (статическая, динамическая)
4. порт, на который должен выйти пакет (может выходить на самого себя, в этом случае указывается CPU, или в агрегированный канал, «Po1»)

```
Switch#show mac address-table
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
-----
A11     0100.0ccc.cccc   STATIC    CPU !С учетом виланов
A11     0100.0ccc.cccd   STATIC    CPU ! (входит в мультикаст-группы служебных
A11     0180.c200.0000   STATIC    CPU !протоколов второго уровня)
...
A11     0180.c200.0010   STATIC    CPU
A11     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
```

Добавлять статическое поле необходимо командой

```
mac address-table static MAC-ADDRESS vlan X interface fe0/1
```

Динамические поля добавляются автоматически во время работы коммутатора.

16. Понятие виланов, их достоинства и недостатки

Виртуальные ЛКС -- Virtual LANs (VLANs) 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.

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

Основные достоинства виланов:

1. Контроль трафика, в первую очередь широковещательного.
2. Дополнительная защита информации.
3. Адаптированность 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.

Виланы связаны с технологиями коммутации пакетов. Место виланов – часть СПД, примыкающая к пользовательским станциям

При рассмотрении виланов выделяют три группы понятий:

1. Физические порты (physical ports), то есть точки подключения сетевого оборудования (сетевых адаптеров, коммутаторов и другого).
2. Физические соединения (каналы) (links) между физическими портами.
3. Виртуальные сетевые интерфейсы и подинтерфейсы (subinterfaces) сетевого оборудования. (Не путать с логическими сетевыми интерфейсами при IP aliasing.)

17. Классификации и реализации виланов

Критерии классификации виланов:

1. Порт-, интерфейс- либо канал-ориентированность: port-based, interface based, 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

Классификация на основе тегов:

1. Data VLAN -- «рабочий» вилан -- предназначен для передачи пользовательского трафика
2. Management VLAN -- административный вилан -- предназначен для администрирования (выделяют исходя из соображений безопасности).
3. Native VLAN -- вилан для оригинального трафика -- предназначен для передачи нетегированного трафика.
4. Default VLAN -- вилан по умолчанию -- в данный вилан включаются все порты коммутатора по умолчанию (не может быть ни изменен, ни удален; зарезервирован VID = 1).
5. Private VLAN -- приватный вилан -- предназначен для частичного запрета трафика в рамках вилана .
6. Reserved VLAN -- зарезервированный вилан -- предназначен для передачи специфического трафика (например, голосового; VID может быть как из зарезервированного, так и с незарезервированного диапазона)

Основные практические примеры виланов:

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.

18. 802.1Q

// + добавить классификацию виланов на основе тегов.

IEEE 802.1Q — открытый стандарт, который описывает процедуру тегирования трафика для передачи информации о принадлежности к VLAN

Поля тега:

1. Tag Protocol Identifier (TPID) – 16 бит -- идентификатор протокола тегировки
2. Priority Code Point (PCP) – 3 бита -- код приоритета
3. Drop Eligible Indicator (DEI) – 1 бит -- индикатор разрешения отброса кадра либо индикатор канонического формата MAC-адреса
4. VLAN Identifier (VID) – 12 бит -- идентификатор вилана

Тег вставляется между MAC-адресом источника и полем Length/Type.

Концепция 802.1Q допускает многократную тегировку кадров (**QinQ**), но длина кадра может превысить значение MTU. Сетевое оборудование обрабатывает теги, находящиеся ближе к началу кадра.

Физические каналы между коммутаторами называют транками, а примыкающие к ним порты называют транковыми портами или, по-другому, тегирующими портами. Транковый порт привязан ко всем имеющимся виланам либо к списку разрешенных. Транковый порт предназначен для работы с тегированными кадрами, но должен «понимать» и нетегированные.

Физические порты, обращенные к пользовательским станциям, называют портами доступа (access ports) или, по-другому, нетегирующими портами (untagged ports). Порт доступа предназначен для внесения кадров в конкретный вилан и изъятия кадров оттуда. Поэтому порт доступа должен быть ассоциирован только с одним виланом. Для привязки порта к вилану используется параметр ПИ-ВИ-АЙДИ. В нормальной ситуации коммутатор принимает через порт доступа только нетегированные кадры.

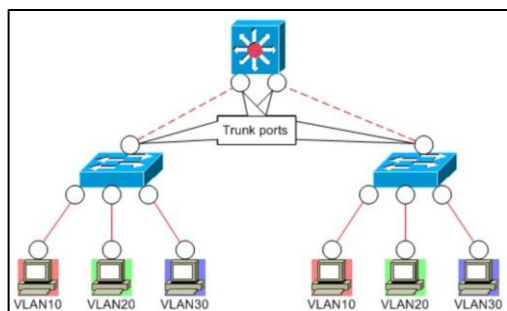
19. Маршрутизация между виланами

Так как с точки зрения IP-адресации каждый вилан является виртуальным аналогом физического сегмента и соответствует IP-подсети, то необходима возможность передачи пакетов из одного вилана в другие

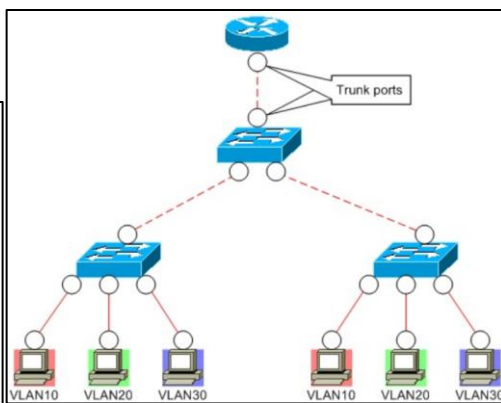
Для обеспечения этого необходима маршрутизация между виланами (inter-VLAN routing).

Маршрутизация между виланами может выполняться:

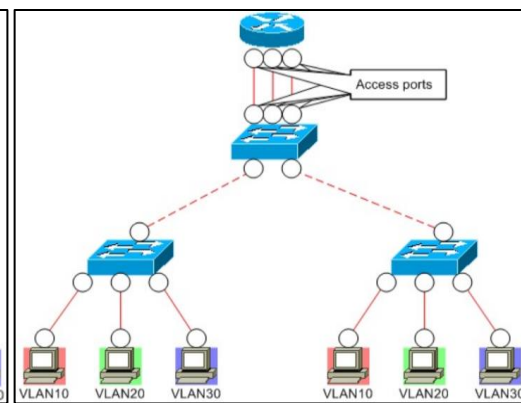
1. L3-коммутатором с виртуальными сетевыми интерфейсами в разных IP-подсетях.
2. Маршрутизатором с относящимися к разным IP-подсетям виртуальными подинтерфейсами одного реального сетевого интерфейса (иногда называют router-on-a-stick).
3. Маршрутизатором с относящимися к разным IP-подсетям сетевыми интерфейсами (иногда называют классической маршрутизацией между виланами).



via L3-switch



Router-on-a-stick



Classic IVR

Типичный L3-коммутатор отличается от маршрутизатора большим числом физических портов и отсутствием «физически выраженных» сетевых интерфейсов (можно сказать, что L3-коммутатор – это один «большой» сетевой интерфейс с больши'м числом точек подключения).

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 сетевыми интерфейсами (тегированный и нетегированный трафик).

Конфигурация:

На Windows интерфейсу можно назначить VID посредством менеджера устройств. Надо войти в «Device manager», выбрать необходимый интерфейс и зайти в его настройки. Во вкладке «Advanced» выбрать VLAN ID и сконфигурировать.

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.

Конфигурация:

/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

Пример создания пользовательского вилана.

```
Switch(config)#vlan 10
Switch(config-vlan)#name STUDENTS
```

Для сохранения информации о виланах создается специальная база данных vlan.dat

Пример назначения порта доступа.

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

Пример назначения транкового порта

```
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
```

Кроме статического задания транка, существует возможность его динамического формирования с помощью DTP (Dynamic Trunking Protocol).

В результате, порт может находиться в одном из следующих транковых режимов:

1. dynamic auto (по умолчанию).
2. dynamic desirable.
3. trunk.

	Access	Trunk	Dynamic auto	Dynamic desirable
Access	Access	Not Recommended	Access	Access
Trunk	Not Recommended	Trunk	Trunk	Trunk
Dynamic auto	Access	Trunk	Access	Trunk
Dynamic desirable	Access	Trunk	Trunk	Trunk

Таблица состояний порта

22. Конфигурирование маршрутизации между виланами в IOS

SVIs для администрирования доступны на всех управляемых коммутаторах Cisco, в том числе на 2960. «Рабочие» SVIs доступны на L3-коммутаторах, таких как 3560. Начиная с IOS версии 12.2, SVI необходимо административно включать.

Пример создания и конфигурирования SVI (Switch Virtual Interface) -- ассоциированного с виланом виртуального сетевого интерфейса (L3-интерфейса).

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

Если IP-адрес нужен только в рамках административного вилана, то для указания шлюза по умолчанию предназначена команда `ip default-gateway`.

```
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. При этом IP-адрес можно назначить только после включения инкапсуляции и IP-адрес подинтерфейса совместим с IP-адресом интерфейса (с проверкой уникальности подсетей).

```
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 – это единая зона ответственности, состоящая из соединенных между собой коммутаторов. В рамках СПД может существовать несколько VTP-доменов. Каждый VTP-домен уникальным образом именуют. Коммутатор может входить в состав только одного VTP-домена.

Режимы работы коммутаторов:

1. VTP-сервер.
2. VTP-клиент.
3. Прозрачный режим.

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

VTP-клиент не предназначен для внесения информации о виланах. VTP-клиент работает на основе сведений, получаемых от VTP-сервера.

В прозрачном режиме коммутатор не участвует в работе VTP-домена, с которым связан, но пересылает VTP-сообщения начиная со 2й версии.

Для обеспечения синхронизации VTP-конфигураций на коммутаторах вводятся ревизионные номера, которые увеличиваются при изменениях виланов.

Обмен по протоколу VTP осуществляется посредством VTP-сообщений, передаваемых по зарезервированному мультикаст-МАС-адресу.

VTP-сообщения бывают трех видов:

1. Summary -- содержат обобщенную информацию, порождаются сервером, посылаются незамедлительно при любых изменениях и затем периодически.
2. Subset -- содержат информацию о виланах, порождаются сервером, посылаются при любых изменениях или по запросу.
3. Request -- запросы от клиентов к серверу о конфигурации, посылаются при подключении клиентов к домену, также посылаются если текущий ревизионный номер меньше полученного посредством summary, в ответ сервер посылает summary + subset.

Если в домен попал VTP-клиент с ревизионным номером больше, чем у сервера, то клиент на время становится сервером. В результате, его конфигурация «разносится» по домену.

24. Конфигурирование VTP

Примеры задания VTP-режима.

```
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
```

Пример задания версии.

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

Возможность VTP-сдерживания может быть оговорена индивидуально для каждого из портов с задействованием специального списка (pruning eligible list).

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`. (показывает версию VTP, домен, и т.д.)

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

Так как пакеты второго уровня (фреймы) не имеют поля TTL, то есть возможности возникновения бесконечных циклов при их ретрансляции.

STP (Spanning Tree Protocol) – алгоритм построения из группы произвольно соединенных между собой L2-устройств виртуального дерева. Заложенный в STP алгоритм позволяет находить один из лучших вариантов среди множества возможных. Spanning Tree призван бороться с заикливанием в СПД при резервировании физических каналов.

STP-домен может находиться в одном из трех состояний:

1. Первоначальная STP-конвергенция -- 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). BPDUs коммутаторами передаются и принимаются, но не ретранслируются.

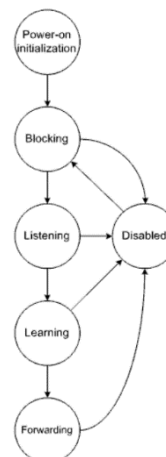
В устоявшемся STP-доме корнем дерева является коммутатор, называемый корневым мостом.

В результате работы алгоритма каждому отдельно взятому порту каждого из коммутаторов назначается одна из следующих STP-ролей:

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
2. Прослушивание
3. Изучение
4. Ретрансляция
5. Запрет



26. STP-конвергенция

// + можно картинку нарисовать, с 3 коммутаторами и их портами

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 -- ассоциирован с каждым мостом, должен быть уникален.
2. Стоимость пути -- ассоциирована с каждым портом, оценивается в рамках STP-домена.
3. Идентификатор порта -- 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.

Алгоритм выбора порта:

1. Корневые и назначенные порты выбираются исходя из наименьшей стоимости пути к корневому мосту.
2. При совпадении стоимости учитывается идентификатор моста.
3. Выбирается порт с наименьшим цифровым значением идентификатора;

Если из оставшихся портов два связанных порта входят в образовавшуюся петлю, то решается, какой из них активировать, а какой зарезервировать и блокировать.

Роль порта в процессе STP-конвергенции может изменяться неоднократно.

В последствии, если какая-либо часть STP-домена претерпела изменение, то оно обнаруживается 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 802.1Q-транки, 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.

28. Конфигурирование STP в IOS

Командой `no spanning-tree vlan` можно отключить STP (по умолчанию включен и не требует конфигурирования) .

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`.

```
Switch(config)#no spanning-tree extend system-id
Switch(config)#spanning-tree pathcost method long
```

Пример попытки 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
```

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.

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

Включение PortFast и BPDUGuard.

```
Switch(config)#interface fa0/2
Switch(config-if)#spanning-tree portfast
Switch(config-if)#spanning-tree bpduguard enable
```

29. Понятие агрегации каналов

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

Резервируют каналы, связывающие сетевые адаптеры серверов с активным сетевым оборудованием, и каналы, связывающие активное сетевое оборудование между собой.

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, что открывает возможности более гибкого распределения 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.

Критерии классификации транков:

1. Канал- (порт-), интерфейс- либо станционная ориентированность: perlink (per-port), per-interface, per-node basis (порт без канала не имеет смысла).
2. Уровень модели OSI: L2, L3 и выше.
3. Целевое сетевое оборудование: switch -- switch, NIC -- switch.
4. Постоянство членства: static, dynamic.

Основные реализации транков:

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

2. Broadcom SLB (Smart Load Balancing) -- аналог Intel ALB.
Два варианта.

Auto-fallback disable – после сбоя связующего адаптера эта функция ему не возвращается, в отличие от Failover

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

4. 802.3ad 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, обеспечивается разделение трафика, сбойный канал исключается из группы.

5. 802.3ad LACP (Link Aggregation Control Protocol) -- в отличие от SLA, dynamic. Позволяет автоматизировать формирование транков из пар портов, используются специальные сообщения LACPDU (LACP Data Units).

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

31. Поддержка агрегации каналов в Windows и Linux

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.

(Включается отдельной функцией на Windows Server в «Add roles and features» и конфигурацией в появившемся NLB-менеджере).

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

Microsoft NIC Teaming -- поддерживается в Windows Server 2012/2019 -- per-link плюс per-interface, L2 плюс L3, NIC -- switch, static + dynamic. Три режима: Switch Independent, Static Teaming, LACP.

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.

```
ifcfg-bond0:
```

```
DEVICE=bond0
```

```
ONBOOT=yes
```

```
IPADDR=192.168.11.15
```

```
NETMASK=255.255.255.224
```

```
USERCTL=no
```

```
ifcfg-eth0 (eth1 и так далее):
```

```
DEVICE=eth0
```

```
ONBOOT=yes
```

```
SLAVE=yes
```

```
MASTER=bond0
```

```
USERCTL=no
```

32. Конфигурирование EtherChannels

// + общая часть про 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.

```
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/active/auto/etc.
Switch(config-if-range)#exit

Switch(config)#interface port-channel 1
Switch(config-if)#spanning-tree portfast
Switch(config-if)#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
```

Некоторые параметры необходимо (и логично) задавать на уровне реальных интерфейсов, а некоторые -- на уровне виртуального интерфейса. Интересно, что некоторые параметры автоматически дублируются (как при вводе на уровне реальных интерфейсов, так и при вводе на уровне виртуального интерфейса), а некоторые необходимо дублировать.

Иногда автоматическое дублирование при «очистке» не срабатывает.

Так же предусмотрены варианты балансировки нагрузки на основе MAC-адресов

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


33. Понятие кластеризации активного сетевого оборудования

Отказ одного из граничных маршрутизаторов, обращенного к ООД и в рядовом случае являющегося для ООД шлюзом по умолчанию, порождает проблемы, поскольку, в отличие от специализированного сетевого оборудования, пользовательские станции как правило не обременяют поддержкой соответствующих протоколов.

Для защиты от подобных неполадок из группы маршрутизирующих устройств формируют кластеры, которым назначают виртуальные IP-адреса и соответствующие виртуальные MAC-адреса из специальных диапазонов.

Существуют технологии, позволяющие формировать кластеры и из коммутаторов.

Создавать кластеры проводного оборудования уровня доступа неуместно отдельно взятый ПК не рассчитан на одновременное подключение к нескольким коммутаторам, правда и неисправности на уровне доступа обнаруживать относительно легко.

Практически все технологии агрегирования каналов в то же время обеспечивают резервирование.

34. Технологии кластеризации активного сетевого оборудования

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 **First Hop Redundancy Protocols**.

Основные технологии, связанные с маршрутизаторами:

1. VRRP (Virtual Router Redundancy Protocol) -- протокол резервирования маршрутизаторов путем объединения их в виртуальный маршрутизатор.
2. Cisco HSRP (Hot Standby Router Protocol) -- протокол «горячей» замены маршрутизатора.
3. Cisco GLBP (Gateway Load Balancing Protocol) -- протокол балансировки нагрузки между шлюзами. HSRP + балансировка нагрузки.

Основные технологии, связанные с коммутаторами:

1. Intel Adapter Fault Tolerance. 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. 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 ставят в зависимость от состояния upstream-портов, что позволяет более правильно распределять нагрузку в некоторых типовых топологиях с резервированием.
5. Cisco Virtual Switching System. Предоставлена возможность формировать на базе высокопроизводительных платформ мощные коммутационные кластеры, используются расширения PAgP.

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).

Конфигурирование маршрутизирующих кластеров в IOS пример:

// Через HSRP (Hot Standby Router Protocol)

```
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
! Preemt обозначает наивысший приоритет

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

// Через GLBP (Gateway loading balance protocol)

```
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

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.

36. Назначение, использование и альтернативы Cisco Port Security

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

После включения Port Security, со ставшим таким образом защищенным портом (secure port) могут ассоциироваться статические и динамические доверительные MAC-адреса, 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.

После включения опционального sticky address learning динамические доверительные адреса (в том числе изученные до включения этой возможности) считаются «липкими» и сохраняются не только в САМ-таблице, а и в рабочей конфигурации. «Липкие» адреса не теряются при выключении-включении порта.

Можно явно указать какие адреса считать «липкими». Можно задать время валидности доверительных адресов.

Если MAC-адрес источника из принятого портом кадра не содержится в списке доверительных адресов или содержится в списке доверительных адресов, **привязанных к другому порту**, то это рассматривается как попытка несанкционированного доступа.

Можно выбрать один из нескольких режимов реагирования на таковую ситуацию (violation mode): protect, restrict, shutdown, shutdown VLAN.

Срабатывание Port Security в режиме shutdown переключает порт в особое состояние -- down (err-disabled). Для возврата порта в нормальное состояние необходимо административно выключить и затем снова включить порт, 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

// + можно добавить общую часть про port security

Пример конфигурирования Port Security.

// Включение port-security

```
Switch(config)# interface fa0/7
Switch(config-if)#switchport mode access ! Или trunk
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 3 vlan access
!Опциональный учёт виланов
```

// Настройка наказания несанкционированного доступа

```
Switch(config-if)#switchport port-security violation protect
Switch(config-if)#switchport port-security mac-address 1234.5678.9abc
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security mac-address sticky
9876.5432.1234
```

// Настройка валидного времени адреса порта

```
Switch(config-if)#switchport port-security aging time 1440 !Минут
Switch(config-if)#switchport port-security aging type inactivity
Switch(config-if)#switchport port-security aging static
```

Основная команда для определения состояния Port Security -- это

```
show port-security.
```

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 механизм описания правил фильтрации пакетов, который может быть задействован различными подсистемами маршрутизаторов и коммутаторов.

Фундаментально ACLs делят на три типа:

1. Port ACLs -- применимы к L2-интерфейсам.
2. Router ACLs -- применимы к L3-интерфейсам.
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.

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

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 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. Особенны тем, что их можно редактировать.

С точки зрения диапазона ACL бывают:

1. Стандартные IP ACLs - позволяют выполнять фильтрацию только на основе IP-адресов источников.
2. Расширенные IP ACLs - позволяют выполнять фильтрацию на основе IP-адресов источников, IP-адресов назначения, L4-протоколов и номеров программных портов.
3. Расширенные MAC ACLs - позволяют выполнять фильтрацию на основе MAC-адресов источников, MAC-адресов назначения и L3-протоколов.

39. Структура Cisco ACLs

Один отдельно взятый ACL состоит из некоторого количества упорядоченных элементов -- ACEs (Access Control Entries).

Каждый элемент представляет собой отдельное правило фильтрации. 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 такая автоматическая перенумерация происходит и после перезагрузки.

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

40. Правила фильтрации в Cisco ACLs и их обработка

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.

Условия в ACEs могут содержать следующие операторы: eq, gt, lt, neq и range.

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.

Наиболее полные варианты команд для ввода правил ACLs имеют достаточно сложный формат. Более того, набор допустимых аргументов вариативен, то есть наличие и значение некоторых аргументов зависит от наличия и значения других аргументов.

IOS упреждает конфликты между ACEs в ACL, не позволяя вводить соответствующие правила.

Если при вводе команды программный порт был указан цифрой, хотя предусмотрен и символьный вариант ввода, то при переносе в рабочую конфигурацию произойдет автоматическая замена на символьный вариант.

// + ACE в ACL может быть с комментарием -- remark (до ста символов включительно). Комментарий вносят до либо после правила, к которому его относят (в какое место будет записан -- там и будет).

41. Нумерованные стандартные IP ACLs и их примеры

// + общая часть про ACL

Нумерованными (numbered) -- идентифицируются уникальными номерами. «Рядовые». Особенны тем, что не подлежат редактированию.

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.
```

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

42. Именованные стандартные IP ACLs и их примеры

// + общая часть про ACL

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).

Пример редактирования именованного стандартного IP ACL.

```
Router(config)#ip access-list standard TEST
Router(config-std-nacl)#no 10
Router(config-std-nacl)#32 permit host 192.168.0.3
Router(config-std-nacl)#exit
```

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

(32 и 10 в данном ACL – это ACE sequence number)

43. Нумерованные расширенные IP ACLs и их примеры

// + общая часть про ACL

Нумерованными (numbered) -- идентифицируются уникальными номерами. «Рядовые». Особенны тем, что не подлежат редактированию.

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

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

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

44. Именованные расширенные IP ACLs и их примеры

// + общая часть про ACL

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).

Пример создания именованного расширенного IP ACL.

```
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
```

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

45. Правила и примеры привязки классических ACLs

// + общая часть про ACLs

Основное правило при выборе места для ACL заключается в том, что список нужно помещать туда, где он наиболее эффективен, то есть наилучшим образом сдерживает нежелательный трафик.

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.

ACL обязательно нужно привязать к чему-либо, иначе ACL не имеет смысла.

Команда привязки выглядит следующим образом:

Router(config-if)#ip access-group {номер списка или имя ACL} {in | out},
где in: входящее направление out: исходящее направление

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 (access-class вместо access-group).

```
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
```

Для просмотра состояния ACLs используют команду show access-lists. При этом для каждого правила в скобках показывается число попаданий (на высокопроизводительных платформах с аппаратным ускорением могут отображаться некорректно). Очистить счетчики попаданий можно командой clear access-list counters.

46. VLAN maps и их примеры

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.

Пример создания VLAN map.

```
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
```

Пример привязки VLAN map

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

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` (Neighbor Discovery – Neighbor Advertisement) и `permit icmp any any nd-ns` (Neighbor Solicitation).

Пример IPv6 ACL.

```
Switch(config)#ipv6 access-list ACL6
Switch(config-ipv6-acl)#deny tcp FE80:0:0:2::/64 any gt 1000 log
Switch(config-ipv6-acl)#permit ipv6 any any
Switch(config-ipv6-acl)#exit

Switch(config)#interface gi0/6
Switch(config-if)#no switchport
Switch(config-if)#ipv6 traffic-filter ACL6 in
Switch(config-if)#exit
```

Gt 1000 обозначает что все порты, которые не well-known отбрасываются

48. Комплексные ACLs и их примеры (лекция 04g | 4.8.10.1-9)

Стандартные и расширенные ACL могут быть основой для комплексных ACL для улучшения функциональности.

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

```
R3(config)#access-list 101 tcp any eq 80 any established
R3(config)#line vty 0 4 !Интерфейс подключения сервера
R3(config-line)# ip access-class 101 out
```

2. 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.

```
R3(config)#access-list 101 dynamic SOMENAME timeout 15 permit ip
192.168.1.0 0.0.0.255 192.168.30.0 0.0.0.255
R3(config)#interface serial 0/0/1 !Интерфейс подключения клиента
R3(config-if)#ip access-group 101 in
R3(config)#line vty 0 4 !Интерфейс подключения сервера
R3(config-line)#access-enable host timeout 5
```

3. 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.

```
R3(config)#ip access-list 101 permit tcp any any eq 80 reflect QWE12
R3(config)#line vty 0 4 !Интерфейс подключения сервера
R3(config-line)# ip access-group 101 out
R3(config)#interface serial 0/0/1 !Интерфейс подключения клиента
R3(config-if)#evaluate QWE12
```

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

```
R3(config)#time-range WORKTIME
R3(config-time-range)#periodic Monday 8:00 to 17:00
R3(config)#access-list 101 permit tcp any any time-range WORKTIME
```

Далее настраивается как обычный ACL

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).

Пример конфигурации Port Mirroring:

```
Switch(config)#monitor session 1 source vlan 10 rx
Switch(config)#monitor session 1 destination interface g0/1
```

g0/1 в данной ситуации порт, на который отправляется дублируемая информация

Существуют технологии сдерживания штормов кадров под обобщенным названием Storm Control.

Параметр storm-control задаёт количество бродкастов в секунду. Всё, что выше этого значения, отбрасывается. Порт при этом продолжает работать для пересылки всего остального трафика. Максимальный уровень широковещательного трафика задаётся либо в процентах от полосы пропускания (безразмерные значения), либо в битах в секунду (bps).

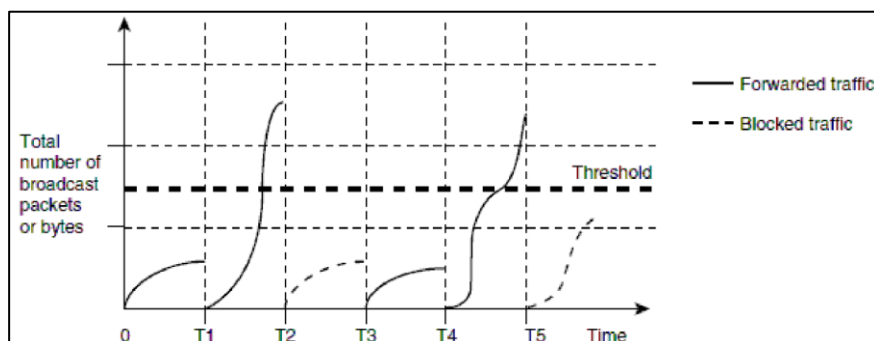
Типичной реакцией на шторм является отключение порта, чтобы восстановить работу порта требуется прописать соответствующие настройки.

Пример конфигурации Storm Control:

Возможны два варианта – однопороговый (указывается порог отключения порта) и двупороговый (дополнительно указывается порог включения порта)

```
Switch(config-if)#storm-control {broadcast | multicast | unicast}
    level {level [level-low] |
    bps bps [bps-low] |      ! Порог отключения порта
    pps pps [pps-low]}      ! Порог повторного включения порта
                           при отключении
```

```
Switch(config-if)#storm-control multicast level 30.00 10.00
Switch(config-if)#storm-control action shutdown !Действие порога
Switch(config)# errdisable recovery cause storm-control !Восстановление
```



Пример работы Storm Control

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

// + Можно нарисовать картинку, как выглядит стек коммутаторов

Разработаны протоколы, позволяющие активному сетевому оборудованию одного производителя определять наличие друг друга. Применительно к оборудованию Cisco, соответствующий протокол называют CDP (Cisco Discovery Protocol).

Новое условное графическое обозначение.



-- стек коммутаторов

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 также «чисто» виртуальное стекирование.

Применительно к оборудованию Cisco, разработаны несколько групп соответствующих технологий. (перечислены основные)

Технология	Платформа	Кол-во коммутаторов в стеке	Общая пропускная способность стековой шины
StackWise	3750, 3750G	9	32 Гбит/с
StackWise Plus	3750-E, 3750-X	9	64 Гбит/с
StackWise-160	3650	9	160 Гбит/с
StackWise-480	3850	9	480 Гбит/с
FlexStack	2960-S, 2960-SF	4	40 Гбит/с
FlexStack Plus	2960-X, 2960-XR	8	80 Гбит/с
Virtual Stacking	2960-L	-	-

Обычно стек состоит из идентичных коммутаторов (homogeneous stack), но может состоять из коммутаторов разных моделей одной серии или из коммутаторов разных, но совместимых серий (mixed stack).

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.

51. Конфигурирование стека коммутаторов в IOS

// + общая база про стекирование (что такое, из чего состоит)

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 X priority`. Приоритет задают числом от 1 до 15.

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

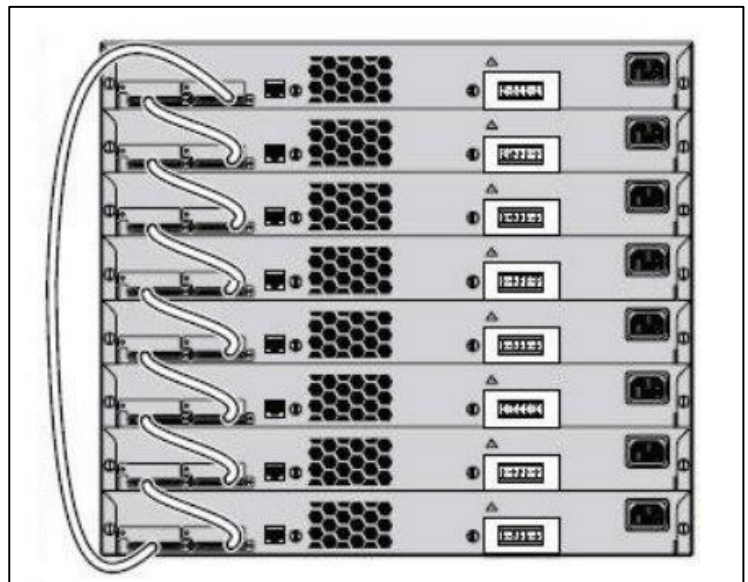
Пример конфигурации стека:

```
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 !2 - 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`.

Данная команда показывает номер коммутатора, роль (primary/secondly), MAC-адрес, приоритет и состояние (ready/disabled)

+ Можно нарисовать картинку, как выглядит стек коммутаторов (каждый соединяется с нижним, а нижний -- с верхним):



52. Семейство стандартов Wi-Fi

Основой для построения беспроводных ЛКС -- Wireless LANs (WLANs) -- является семейство стандартов **IEEE 802.11**, определяющих правила взаимодействия беспроводных устройств и известных под общей аббревиатурой Wi-Fi (Wireless Fidelity).

(тут можно нарисовать картинку Wi-Fi Certified, Alliance, Wi-Fi6 и тд)

Разработка и внедрение более новых стандартов (таких как **802.11n**, **802.11ac**, **802.11ax**) происходили и происходят постепенно, причем реализации появляются на рынке еще в процессе «обкатки» стандартов (до официального утверждения).

В настоящее время под аббревиатурой Wi-Fi понимают следующие ключевые стандарты:

Стандарт IEEE	Год	Главное отличие	Модуляция	Макс. пропускная способность	Частота (GHz)
802.11ax	2019	OFDMA	OFDMA/MU-MIMO	500Mb-10Gb	2.4, 5
802.11ac	2014	MU-MIMO/256QAM	MU-MIMO/256QAM	400Mb-7Gb	5
802.11n	2008	MIMO/64QAM	MIMO/64QAM	600Mb	2.4, 5
802.11g	2003	-	OFDM	54Mb	2.4
802.11a	1999	5 GHz	OFDM	54Mb	5
802.11b	1999	-	OFDM	11Mb	2.4
802.11	1997	-	OFDM	2Mb	2.4

53. Физический уровень Wi-Fi

// (вспомнить несложную картинку на слайде 5.0.2.7а, 5 лекции)

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).

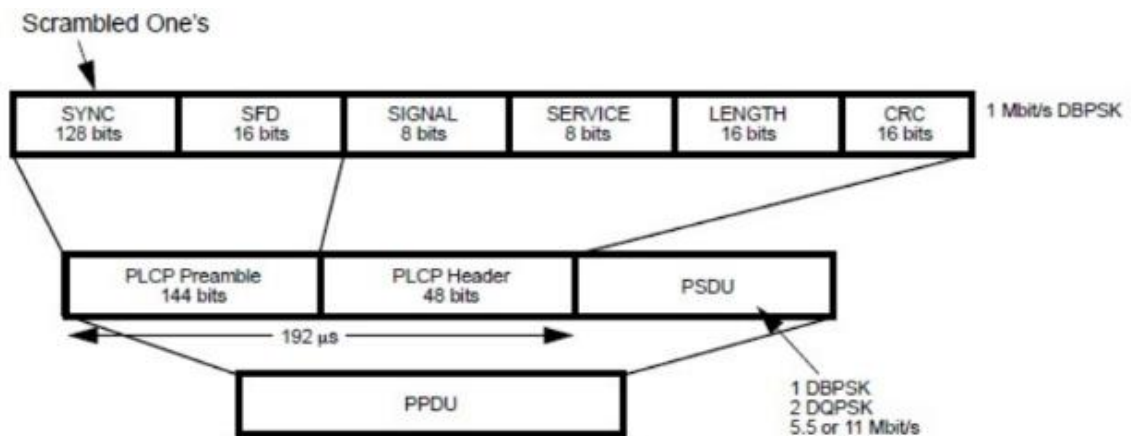
При этом MPDUs (собственно кадры Wi-Fi, рассмотренные ранее, Mac Protocol Data Units) вкладываются в PPDUs (PLCP Protocol Data Units) -- вкладываются как PSDUs (PLCP Service Data Units).

Формат PPDU очень вариативен, однако базой служит формат протокола 802.11: в каждом кадре есть преамбула, хедер и данные (PSDU – PLCP Service Data Unit), однако с продвижением стандартов данный формат претерпел значительные изменения, дополняясь вспомогательными полями.

При передаче полей PPDU (кроме PSDU), несмотря на их цифровую природу, строго **выдерживают соответствующие временные интервалы**.

PLCP-преамбула состоит из SYNC, SFD (Start Frame Delimiter);
PLCP-хедер состоит из Signal, Service, Length и CRC
далее идут данные

НАРИСОВАТЬ КАРТИНКУ, МОЖНО БЕЗ УЧЁТА БИТ:



Начиная с 802.11n, поддерживается **агрегация PDUs**, причем в двух формах: A-MSDU (Aggregate Mac Service Data Unit) -- опциональное слияние MSDUs с одинаковыми адресами RA и TA, и A-MPDU (Aggregate Mac Protocol Data Unit) – слияние MPDUs.

Начиная с 802.11ax, поддерживается **динамическая фрагментация MSDU**, то есть кроме фрагментов одинаковой длины, допускаются фрагменты разной длины.

Агрегация и фрагментация, а также моделируемые символы и защитные интервалы разной длительности позволяют повысить гибкость.

54. Каналы Wi-Fi

В Wi-Fi 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 и освоены в первую очередь.

Базовый алгоритм Wi-Fi предполагает использование в качестве канала одной +/- узкой полосы частот.

Ширина канала может быть: 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.

«Распараллеливание» реализуют не одновременным использованием нескольких каналов, а «слиянием» (своеобразной агрегацией) каналов.

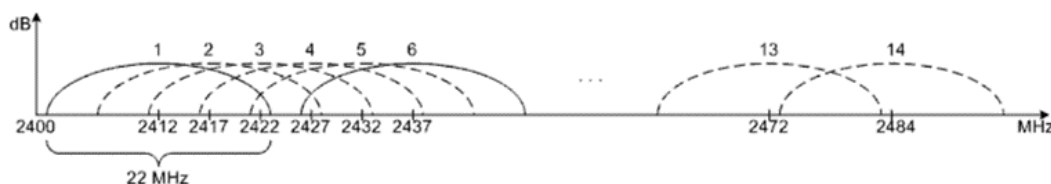
Обобщенно, один канал представлен одной несущей. Однако, по правилам модуляции OFDM, несущую делят на множество поднесущих -- от 64 в каналах шириной 20 MHz до 512 в каналах шириной 160 MHz. (нарисовать картинку с множеством несущих по OFDM). Увеличение ширины канала позволяет увеличить количество поднесущих и, следовательно, скорость.

Часть поднесущих используют для служебных целей: нулевые (null) позволяют лучше изолировать каналы, а так называемые пилотные (pilot) позволяют лучше детектировать каналы.

Каналы Wi-Fi нумеруются.

Наборы каналов вариативны, так как на использование тех или иных каналов в разных странах наложены свои ограничения. (упомануть про беларусь-израиль)

На практике перекрытие каналов порождает проблемы, поэтому его следует избегать. В этом смысле показательна область 2,4 GHz с каналами 802.11b:



55. Модуляция и кодирование в рамках Wi-Fi

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. И канальное кодирование может быть многоуровневым.

Поддержка различной модуляции, как и кодирования, может быть, как обязательной, так и опциональной.

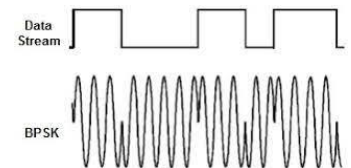
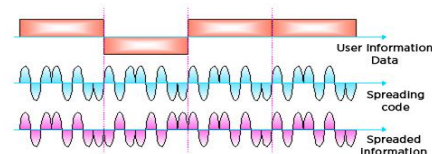
С учетом совместимости, модуляция (кодирование) автоматически подбирается в зависимости от требующейся скорости.

Начиная с 802.11n, формализован более цельный параметр физического уровня под названием MCS (Modulation and Coding Scheme) – это индекс, позволяющий определить модуляцию и скорость канального кодирования.

Поскольку используются избыточные канальные коды, изменение коэффициента избыточности приводит к изменению скорости.

- **Некоторые модуляции:**

1. Квадратно-амплитудная (QAM (8, 16, 64));
2. OFDM (Orthogonal Frequency Division Multiplexing) – мультиплексирование с ортогональным частотным разделением (картинка с множеством поднесущих)
3. MIMO (Multiple-Input Multiple-Output) -- множественный доступ. Кодирование: Код Хэмминга, циклический код, БЧК.
4. MU-MIMO (Multi User MIMO)
5. DSSS (Direct Sequence Spread Spectrum) – широкополосная модуляция с прямым расширением спектра.
6. BPSK (Binary Phase Shift Keying) и QPSK (Quadrature Phase Shift Keying) – соответственно двоичное и квадратичное манипулирование фазовыми сдвигами.
7. FHSS (Frequency Hopping Spread Spectrum) – широкополосная модуляция со скачкообразным изменением частоты



56. Стандарты беспроводной связи, кроме Wi-Fi

// + что-нибудь про Wi-Fi написать из общего, например что есть разные стандарты WiFi

Нужно отметить, что кроме WLAN еще выделяют WWANs, WMANs, WPANs и другие беспроводные сети.

Стандарты:

1. Satellite broadband -- спутниковая связь; LMDS (Local Multipoint Distribution Service) и MMDS (Multichannel Multipoint Distribution Service); скорость ориентировочно до 10 Mbit/s.

2. Cellular broadband -- мобильная связь; поддержка доступна начиная со второго поколения мобильных телефонов 2G: GSM, CDMA (Code-division multiple access) и TDMA (time); 3G; 4G: WiMAX и LTE; 5G

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, ...

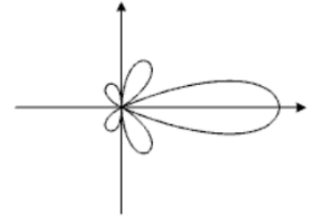
57. Антенны для беспроводного сетевого оборудования и сопутствующие расчеты

На данный момент используют внутренние и внешние антенны самых разных конструкций вплоть до ФАР (фазированных антенных решеток).

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.

Диаграмма направленности параболической антенны:



Направленная параболическая антенна обеспечивает усиление:

$$G = 4\pi A / \lambda^2, \text{ dB},$$

где A -- площадь; λ -- длина волны несущей.

Основой устойчивой связи является прямая видимость между передающей и принимающей антеннами.

Затухание радиоволн в беспрепятственной воздушной среде рассчитывают по упрощенной формуле:

$$L = 32,44 + 20\lg(F) + 20\lg(D), \text{ dB},$$

где F -- частота в GHz; D -- расстояние (в метрах).

Типичная Wi-Fi-антенна дает дополнительное усиление до 6 dBi.

Так же антенны могут делиться на 3 основные и 2 дополнительные категории:

1. Omnidirectional -- всенаправленные (для применения на открытых пространствах).
2. Dipole -- дипольные (позволяют корректировать направленность).
3. Directional -- направленные (для применения в ограниченных пространствах), включая:
 4. + patch -- патч-антенны или, по-другому, полосковые (для применения при небольшой дальности).
 5. + uagi -- так называемые «яги» или, по-другому, «волновой канал» (для применения при повышенной дальности).

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 (выпускают до сих пор). 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.

Точки доступа делят на два типа:

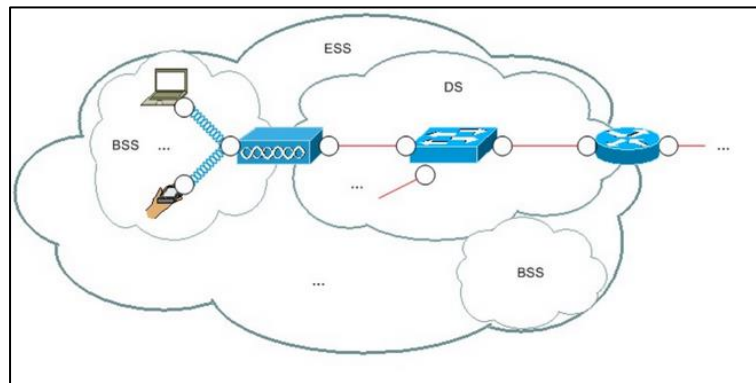
1. Автономные (autonomous, stand-alone, heavy) -- самодостаточны в смысле работоспособности и администрирования.
2. Так называемые легковесные (lightweight) -- администрируют централизованно посредством контроллеров -- WLCs (Wireless LAN Controllers).

59. Структура беспроводной сети

В основу беспроводных сетей (не только Wi-Fi) положена сотовая структура. В общем случае предполагают наличие точек доступа – режим инфраструктуры. СПД может состоять из одной либо нескольких сот (cells). Каждая сота управляется персональной точкой доступа.

Типовая структура сети:

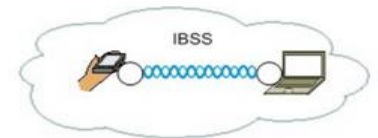
1. Точка доступа и ассоциированные с ней беспроводные пользовательские устройства образуют базовую зону обслуживания -- BSS (Basic Service Set).
2. Точки доступа многосотовой сети взаимодействуют между собой посредством распределенной системы -- DS (Distribution System).
DS – это обычная проводная инфраструктура второго уровня.
3. Совокупность BSSes и DS образует расширенную зону обслуживания – ESS (Extended Service Set) представляет собой отдельную сущность беспроводного сегмента.



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**. (можно написать про бесшовный роуминг)

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



Отдельно взятые ESAs (Extended Service Area) и BSAs (Basic Service Area) идентифицируют с помощью SSIDs (Service Set IDentifiers).

Все соты имеют общий уникальный идентификатор SSID, плюс каждая из сот имеет собственный уникальный идентификатор BSSID.

BSSID используется как один из четырех адресов в кадре Wi-Fi, тем самым позволяя распознавать соту.

60. Идентификация и виланы в беспроводных сетях

Концепция виланов вполне совместима с WLANs, правда с учетом особенностей.

Беспроводные виланы представлены различными SSIDs, существующими 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.

Для обеспечения защиты информации предусмотрен комплекс мер, отчасти выраженный в WEP (Wired Equivalent Privacy) и WPA (Wi-Fi Protected Access).

// + можно написать про WPA, WPA2, WPA2Enterprise (Radius)

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).

62. Беспроводное сетевое оборудование Cisco

По состоянию на октябрь 2021 года беспроводное оборудование Cisco делят на **пять основных целевые категории**:

1. Indoor access points
2. Outdoor/Industrial access points
3. Wireless Controllers (WLC)
4. Cloud-managed access points
5. Controllers access points.

Приблизительно в 2000 году, в результате приобретения компании **Aironet**, Cisco начала производство точек доступа enterprise/industrial -- подторговой 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.

Так же на данный момент Cisco перспективно развивает архитектуру **Cisco Meraki Cloud Managed**, которая включает в себя 3 основных компонента:

1. MR Cloud Managed Wireless APs -- управляемые из облака беспроводные точки доступа серии MR.
2. Meraki Cloud Controller (MCC) -- контроллер на базе облака.
3. Web-based Dashboard -- панель управления на основе web-интерфейса.

63. Беспроводные технологии Cisco

Основные технологии:

1. Технология Cisco CleanAir позволяет обеспечить интеллектуальное сосуществование точки доступа с другими точками доступа в «агрессивном» окружении, решая проблему интерференции.
2. Технология Cisco OfficeExtend позволяет защищенным образом связать WLAN удаленного офиса и основную корпоративную WLAN.
3. Технология Cisco Wireless Mesh, позволяет строить на базе расставленных в outdoor-окружении специальных точек доступа полнофункциональную сеть с произвольной физической топологией, динамически формировать каналы, находить ближайший WLC, оптимизировать трафик.
4. Протокол для mesh-сетей – AWPP (Adaptive WirelessPath Protocol). Она позволяет оптимизировать трафик и находить ближайшие WLC (Wireless LAN Controller). По этому протоколу достигается самый оптимальный маршрут путём определения стоимости путей рассчитываемой по хопам и пропускной способности.

Все вышеперечисленное «собрано» в архитектуру Cisco Unified Wireless Network.

Еще одним интересным направлением является интеграция беспроводных технологий с облачными. В 2012 году Cisco приобрела перспективную компанию Meraki.

Архитектура Cisco Meraki Cloud Managed включает три основных компонента:

1. MR Cloud Managed Wireless APs -- управляемые из облака беспроводные точки доступа серии MR.
2. Meraki Cloud Controller (MCC) -- контроллер на базе облака.
3. Web-based Dashboard -- панель управления на основе web-интерфейса.

// + нарисовать картинку с Meraki Cloud Managed (5.0.9.7), где облако, от которого отходят линии беспроводной связи на оконечные устройства, и это всё управляется с Web-интерфейса. Сам контроллер расположен в облаке.

64. Конфигурирование беспроводного маршрутизатора Linksys

// По сути происходит так же, как и в Cisco Packet Tracer в 3 лабе

Для конфигурирования маршрутизатора необходимо подключиться ко включенному маршрутизатору путём беспроводного соединения, посмотреть Default Gateway, и ввести этот адрес в любом браузере, после этого откроется WEB-интерфейс для конфигурирования беспроводного маршрутизатора.

1. На вкладке Setup в Internet Setup выбрать Static IP
 - a. В поле Internet IP Address пишем адрес из добавленного вилана, subnet mask – его маску. Default gateway адрес маршрутизатора.
 - b. Во вкладке Network setup конфигурируется маршрутизация внутри беспроводной сети.
2. Переходим на вкладку Wireless
 - a. В поле SSID пишем название своей сети
 - b. Выбираем подвкладку Wireless Security, там выбираем WPA2 Enterprise. После этого в появившихся полях заполняете Shared Secret – задается пароль и IP адрес сервера
 - c. Выбираем подвкладку Wireless MAC Filter. Выбираем Enable и из двух точек нижнюю. В поля для mac адресов вписываем mac адреса беспроводных устройств.

65. Интеграция компьютерных сетей в системы связи

Исторически происходила интеграция компьютерных сетей в системы связи, однако существуют и обратные технологии, подразумевающие интеграцию систем связи в компьютерные сети, например, VoIP. Соответственно, КС переплетаются с традиционной связной инфраструктурой.

Почти все WAN-технологии изначально разработаны для передачи разнородного трафика (голос, видео, электронные данные).

Выделяют два направления интеграции:

1. КС интегрируют в системы связи.
2. Системы связи интегрируют в КС.

Для передачи обычных голосовых сообщений, а также 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 девяносто процентному уровню разборчивости.

В системах аналоговой связи применяют мультиплексирование с частотным разделением каналов -- Frequency Division Multiplexing (FDM). Таким образом, в результирующем объединенном сигнале каждый канал занимает полосу частот 4 kHz.

На базе ТЧ-каналов формируют так называемые групповые тракты:

1. первичный К-12 (12 ТЧ-каналов, 60 -- 180 kHz),
2. вторичный К-60 (60 ТЧ-каналов, 312 -- 552 kHz),
3. третичный К-300 (300 ТЧ-каналов, 812 -- 2044 kHz) и другие

В свою очередь цифровая связь имеет **три фундаментальные отличия** от аналоговой:

1. Тактирование (clocking).
2. Сигнализация (signaling).
3. Кадробразование (framing).

Сигнализация позволяет создавать, отслеживать и удалять физические соединения в такого рода коммуникационных системах.

В общем случае, возможны **два типа сигнализации**:

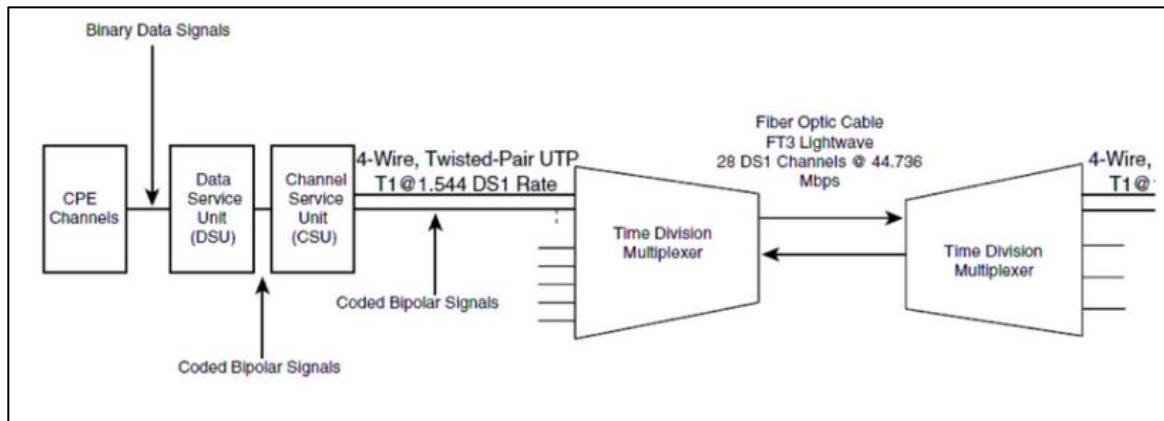
1. CCS (Common Channel Signaling) -- управление всеми информационными каналами происходит через один сигнализирующий.
2. CAS (Channel Associated Signaling) -- для каждого информационного канала предусмотрен персональный сигнализирующий.

66. Структура и синхронизация цифровых сетевых интерфейсов

// + часть про сигнализацию и отличия цифровой сети от аналоговой

С точки зрения структуры сетевой интерфейс состоит из следующих элементов:

1. ЦАП и АЦП
2. Coder/Decoder
3. DSUs (Data Service Units) - передатчики и приемники отдельных каналов
4. CSUs (Channel Service Units) - средства контроля целостности потоков и тестирования в каналах (обычно объединены с DSUs)
5. TDMs (Time Division Multiplexers) - мультиплексоры



ОБЯЗАТЕЛЬНО НАРИСОВАТЬ!!

С точки зрения синхронизации надо учитывать два обстоятельства:

1. Источники синхронизации могут быть локальными и глобальными, причем в отношении как отдельных мультиплексоров, так и выделенных групп
2. Элементы синхронизации включаются в передаваемые кадры

Выделяют **4 режима синхронизации** передатчиков и приемников мультиплексоров в составе СПД:

1. Асинхронный - источники синхронизации не связаны между собой и относительно нестабильны (не более одного проскальзывания за 7 секунд).
2. Плезеохронный - большинство источников синхронизации не связаны между собой, но они относительно стабильны (не более одного проскальзывания за 17 часов).
3. Псевдосинхронный - все источники синхронизации высокостабильны и многие из них привязаны к одному эталонному глобальному источнику (не более одного проскальзывания за 70 суток).
4. Синхронный - все источники синхронизации привязаны к одному эталонному глобальному источнику (проскальзываний фактически нет). Не существует

67. Плезиохронная и псевдосинхронная цифровая иерархия

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

1. Асинхронный -- источники синхронизации не связаны друг с другом и относительно нестабильны
2. Плезиохронный -- большинство источников синхронизации не связаны друг с другом, но они относительно стабильны
3. Псевдосинхронный -- все источники синхронизации высокостабильны и многие из них привязаны к одному эталонному глобальному источнику
4. Синхронный -- все источники синхронизации привязаны к одному эталонному глобальному источнику

Для реализаций **первых двух** режимов характерно наличие независимых источников синхронизации, что приводит к необходимости «выравнивать» цифровые потоки. При накоплении погрешности задействуются прозрачные методы вставки или удаления битов (stuffing).

Для реализаций **последних двух** режимов характерно наличие централизованной синхронизации с большим числом резервных источников, а также включение в цифровые потоки метаданных об этих потоках.

Асинхронный режим массово не применяли и не применяют. Полностью синхронный режим пока недостижим.

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

Таким образом, в настоящее время применяют только два режима и их комбинации.

Плезиохронная цифровая иерархия -- PDH базируется на электрических средах.

Воплощениями псевдосинхронной цифровой иерархии стали **SONET** (Synchronous Optical NETwork) в Северной Америке и **SDH** (Synchronous Digital Hierarchy) в Европе.

Как SONET, так и SDH могут базироваться на электрических – Electrical Signaling (ES) и оптических -- Optical Signaling (OS) средах.

По факту заключается в разделении доступа к каналу связи.

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.

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

Физический канал между граничащими CPE и SPE принято называть «**последней милей**» или «локальной петлей».

К абонентскому оборудованию относят модемы, телефонные аппараты и офисные АТС.

К провайдерскому оборудованию относят коммутаторы и модули, устанавливаемые в маршрутизаторы и АТС.

Основные критерии классификации модемов:

1. Технология и СрПД.
2. Для коммутируемой либо выделенной линии.
3. Аналоговые или цифровые.
4. Аппаратные или программные.
5. Внешние или внутренние.

69. Последовательные сетевые интерфейсы

Основные моменты, связанные с последовательными цифровыми интерфейсами:

1. В стандартах четко разделены роли DCE (data communication equipment) и DTE (data terminal equipment);
2. При непосредственном соединении двух последовательных сетевых интерфейсов имеют смысл только подключения DTE -- DCE и DTE -- DTE, при этом в первом случае применяют «прямые» кабели, а во втором -- кросс-кабели;
3. DTE и DCE отличаются формой контактов;
4. Список цепей для взаимодействия DCE и DTE унифицирован и функционально полон;
5. Цепи могут быть как несбалансированными, и сбалансированными;
6. Благодаря более эффективному заполнению полосы пропускания, в СПД значительно чаще применяют именно синхронный, а не асинхронный режим;
7. В синхронном режиме синхронизация, как правило, осуществляется не путем вставки в информационные цепи синхробайтов, а путем тактирования через отдельные цепи;
8. В нормальной ситуации источником тактирования является DCE, но иногда эту роль возлагают на DTE;
9. 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;
10. Последовательные интерфейсы образуют не только point-to-point-топологии, но и различные point-to-multipoint-топологии;
11. Как и положено, компьютерная информация передается по последовательным интерфейсам в виде пакетов (кадров), при этом возможны канальное кодирование, канальное сжатие и канальное фрагментирование;
12. Отличительной особенностью последовательных интерфейсов является отсутствие MAC-адресов.

// как запомнить – 1-4 про DCE/DTE, 5-8 балансировка, синхронизация, 9 – тактирование DTE/DCE, 10-12 – доп. информация

70. Протокол PPP и смежные протоколы

PPP — это протокол, который позволяет устанавливать канальное point-to-point-соединение. Затем это соединение может использоваться практически любыми протоколами третьего уровня

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).

LCP используется для согласования, конфигурирования, контроля соединения. Позволяет задать максимальную длину пакета, аутентификацию и т.д. Работа LCP базируется на механизме запросов-подтверждений.

Набор NCPs позволяет адаптировать подготовленное соединение к нуждам протоколов третьего уровня и позволяет согласовать возможности сжатия пакетов, правила назначения IP-адресов и так далее.

PPP поддерживает два алгоритма аутентификации на канальном уровне:

1. PAP -- «двойное рукопожатие», разовый обмен незашифрованными PAP-сообщениями.
2. CHAP -- «тройное рукопожатие», периодический обмен зашифрованными CHAP-сообщениями.

Еще две серьезные возможности PPP:

1. Multilink – задействование нескольких параллельных физических каналов путём соединения ресурсов (фрагментация, перемежение, балансировка нагрузки и другое).
2. Bridging -- поддержка мостов.

71. Конфигурирование последовательных сетевых интерфейсов в IOS

Рассмотрим конфигурирование последовательных сетевых интерфейсов на следующем примере:

```
Router(config)#interface se0/0/0
Router(config-if)#clock rate 64000 ! В БИТАХ В СЕКУНДУ
Router(config-if)#encapsulation ppp
Router(config-if)#ppp multilink
```

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

// PAP

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

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
```

///CHAP

```
R1(config)#username R2 password cisco !Тут прописываем роутер, с
                                         которым хотим установить связь!

R1(config)#interface se0/1/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication chap

R2(config)#username R1 password cisco!Тут прописываем роутер, с
                                         которым хотим установить связь!

R2(config)#interface se0/1/1
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication chap
```

72. Обзор технологии Dial-up и структура Dial-up RAS

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


На абонентской стороне устанавливают внутренний либо внешний Dial-up-модем, **на провайдерской** -- внутренний либо внешний модемный пул.

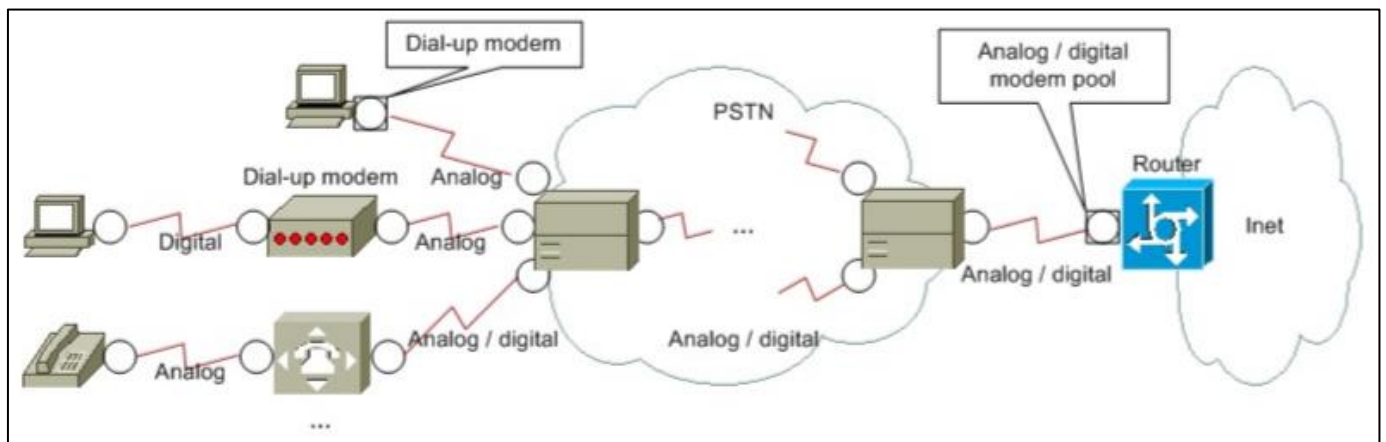
Посредником является то, что в настоящее время принято называть традиционной телефонной сетью общего пользования – **PSTN** (public switching telephone network). В настоящее время почти все АТС цифровые и применяют в основном цифровые модемные пулы.

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.

Новые условные графические обозначения.

-  -- аналоговый телефон
-  -- модем
-  -- АТС
-  -- офисная АТС
-  -- CSU/DSU
-  -- сервер RAS

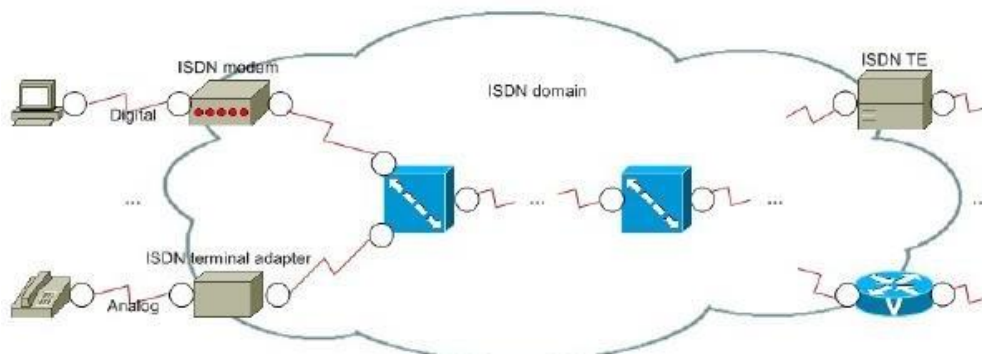


Нарисовать структуру домена обязательно!!!

73. Обзор технологии ISDN и структура ISDN-домена

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

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



Новые условные графические обозначения.



-- WAN-коммутатор (в том числе ISDN)



-- вспомогательное пассивное оборудование

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) -- обычн packet-switched 16 kbit/s.
2. B-канал (Bearer channel) -- используется для пересылки электронных данных, голоса и видео -- circuit- либо packet-switched 64kbit/s.
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
2. PRI (Primary Rate Interface) -- первичный -- схема: 23B (1,472 Mbit/s) + 1D либо 30B (1,92 Mbit/s) + 1D

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).

74. Обзор технологии ATM и структура ATM-домена

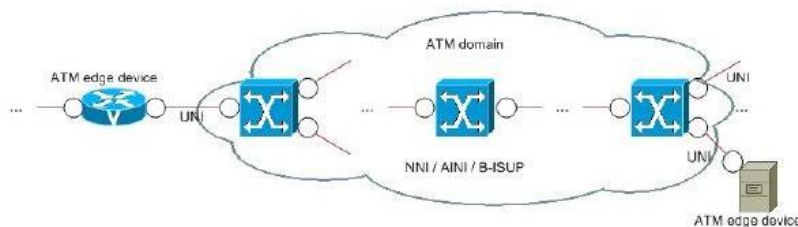
Технология АТМ уходит корнями в ISDN.

Серьезными достоинствами АТМ являются заложенные поддержка качества обслуживания разнородного трафика и ориентированность на соединение. АТМ обеспечивает скорость до 40 Gbit/s и больше.

Новые условные графические обозначения.



-- АТМ-коммутатор



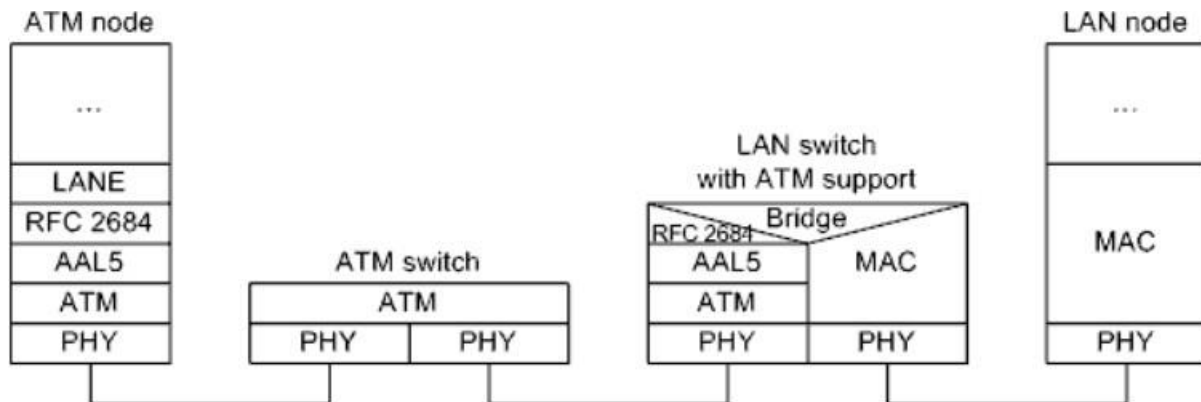
АТМ-домен состоит из некоторого количества объединенных АТМ-коммутаторов и подключенных к ним граничных АТМ-устройств. Граничными АТМ-устройствами могут быть маршрутизаторы, пользовательские станции, коммутаторы с поддержкой АТМ и так далее.

Согласно идее АТМ, информация передается посредством фиксированной длины кадров 53 байта, называемых ячейками.

Для обеспечения возможности создания SVCs (switched virtual circuit) со стороны граничных АТМ-устройств используется специальный механизм - сигнализация. Для обеспечения сигнализации создают сигнализационную PVC (постоянная), валидную в пределах VP (Virtual Path).

75. Примеры инкапсуляции в ATM-системе

В ATM используется многопротокольная инкапсуляция по правилам RFC 2684, 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.



Способ инкапсуляции AALx определяет форматы пакетов и то, как они вкладываются друг в друга. Наиболее часто применяется инкапсуляция AAL5.

76. Семейство стандартов xDSL

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

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)
2. SDSL (Symmetric DSL).
3. SHDSL (Single-pair HDSL)
4. ADSL (Asymmetric DSL)
5. VDSL (Very high bit rate DSL).

xDSL	Среда передачи данных	Модуляция	Ориентировочная максимальная скорость, Mbit/s	Ориентировочная критическая дальность, km
HDSL	2 phone pairs (либо 1, либо 3)	2B+1Q, CAP	2,0 duplex	4,0
SDSL	1 phone pair	not standardized, many vendors	2,3 duplex	3,0
SHDSL	1 phone pair (но может быть и 2)	TCPAM	2,3 duplex	4,0
SHDSL bis	1 phone pair (но может быть и 2)	TCPAM	2,3 duplex	3,0
ADSL	1 phone pair (либо ISDN-среды)	DMT	0,8 up, 8,0 down	3,0
ADSL2	1 phone pair	DMT	1,0 up, 12,0 down	2,0
ADSL2+	1 phone pair	DMT	2,0 up, 24,0 down	1,5
ADSL2++	1 phone pair	DMT	3,0 up, 48,0 down	1,0
VDSL	twisted pair, fiber	QAM	12,0 up, 52,0 down, 26,0 duplex	1,0
VDSL2	twisted pair, fiber	DMT	100,0 duplex	0,5

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

77. Каналы и модуляция в рамках xDSL

Модуляции:

1. CAP (Carrierless Amplitude and Phase Modulation) -- не требующая наличия несущей амплитудно-фазовая.
2. TSPAM (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

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:**

1. ADSL (асимметричные),
2. SDSL (симметричные) и
3. 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).

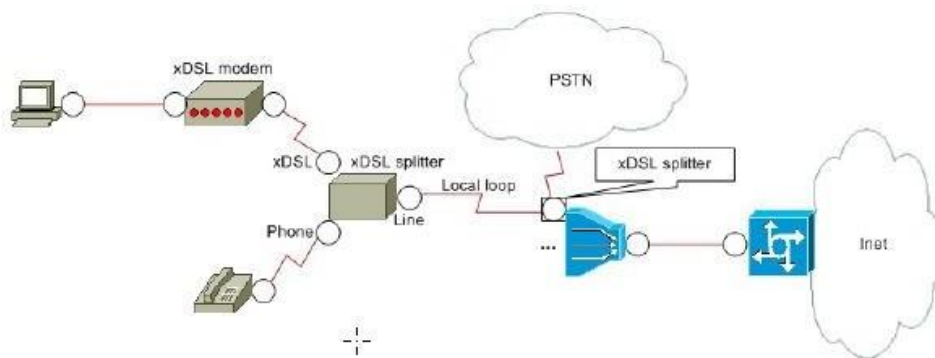
Часть каналов, расположенных в нижней области рабочей полосы частот, используется как upstream, оставшиеся -- как downstream.

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

78. Структура xDSL RAS

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.



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. Инфраструктура (второго и третьего уровней) между DSLAM и RAS-сервером может быть достаточно сложной и состоять из множества разных устройств.

Надстройкой над xDSL является архитектура ATM.

Как правило, протоколы третьего уровня задействуют ATM через PPP-прослойку. **При этом возможны два варианта, выраженные в соответствующих протоколах:**

1. PPPoA (PPP over ATM) -- напрямую.
2. PPPoE (PPP over Ethernet) -- посредством эмуляции Ethernet.

79. Примеры инкапсуляции в xDSL-системе

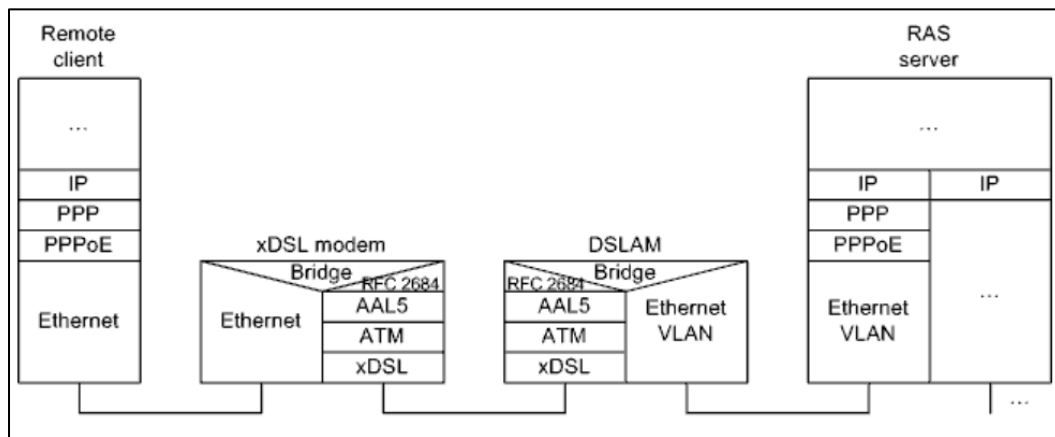
Надстройкой над xDSL является архитектура АТМ. Как правило, протоколы третьего уровня задействуют АТМ через PPP-прослойку.

При этом возможны два варианта, выраженные в соответствующих протоколах:

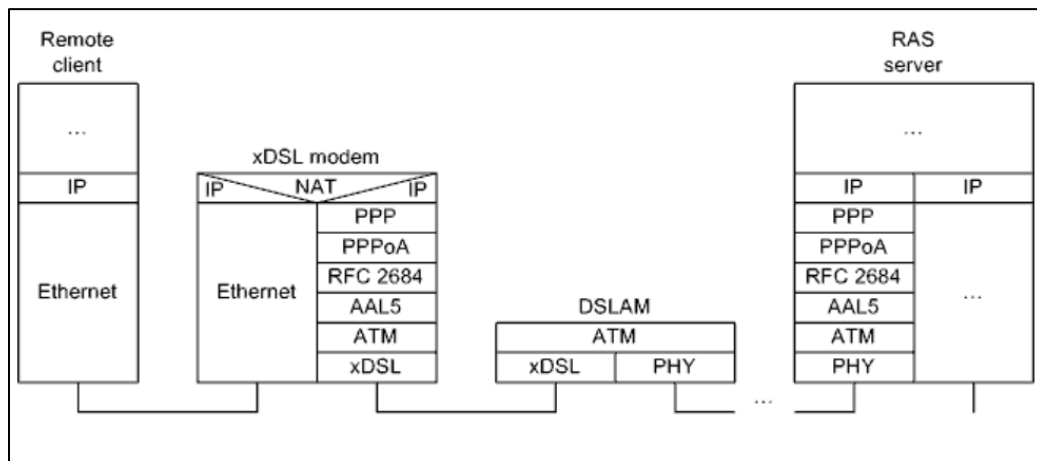
1. PPPoA (PPP over ATM) (RFC 2364) -- напрямую (но в связке с многопротокольной инкапсуляцией).
2. PPPoE (PPP over Ethernet) (RFC 2516) -- посредством эмуляции Ethernet (так же в связке с многопротокольной инкапсуляцией).

В общем случае, возможно множество вариантов организации xDSL-системы.

Одним примером может служить xDSL-система, в которой используется PPPoE, PPPoE-клиент установлен на удаленной пользовательской станции, DSLAM работает с виLANами:



Другим примером может служить xDSL-система, в которой используется PPPoA, PPPoA-клиент интегрирован в xDSL-модем, DSLAM и RAS связаны по АТМ.

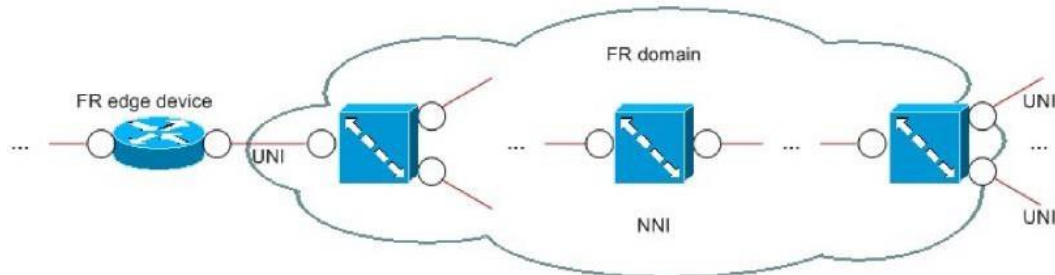


80. Обзор технологии FR и структура FR-домена

Технология FR (Frame Relay) произошла от X.25 и Narrowband ISDN.

Как и ATM, связана с NBMA (Non Broadcast Multiple Access) - топологиями, но устанавливать соединения не позволяет.

Структура напоминает структуру ATM и ISDN:



Поддерживаются как PVC, так и SVC.

VCs идентифицируются значимыми только в пределах физических каналов десятибитными идентификаторами DLCIs (Data-Link Connection Identifiers).

Значения DLCI от 0 до 15 и от 992 до 1023 зарезервированы. Для сигнализации используется $DLCI = 0$. За мультикаст-группами зарезервированы DLCIs от 1019 до 1022 включительно.

Касательно пакетов услуг обычно выделяют:

1. AR (Access Rate) -- полоса пропускания локальной петли (обычно совпадает с текущей скоростью физического порта).
2. CIR (Committed Informational Access Rate) – гарантированная провайдером goodput.
3. CBIR (Committed Burst AR) -- кратковременно доступная дополнительная полоса пропускания.
4. BE (Burst Excess) -- резервная, но недоступная, полоса пропускания.

Превышающие CIR кадры метятся особым образом (Discard Eligible) и при перегрузках отбрасываются.

FR может задействовать различные СрПД. Особенностью последовательных сетевых интерфейсов Cisco является то, что они поддерживают инкапсуляцию FR.

81. Виртуальные цепи ATM, FR и подобных технологий

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).

Виртуальные цепи ATM бывают трех видов:

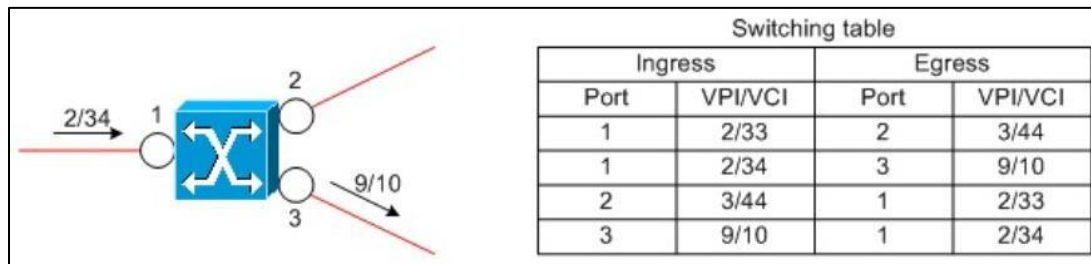
1. PVCs (Permanent Virtual Circuits) -- и на граничных ATM-устройствах, и на ATM-коммутаторах, пары VPI/VCI администраторы задают статически.
2. SVCs (Switched Virtual Circuits) -- пары VPI/VCI и таблицы коммутации формируются ATM-коммутаторами динамически и автоматически.
3. Soft PVCs -- гибриды PVCs и SVCs, связь между граничными ATM-устройствами и ATM-коммутаторами организована по PVC-правилам, а между ATM-коммутаторами -- по SVC-правилам.

82. Принцип работы ATM- и FR-коммутаторов

Принцип работы ATM-коммутатора.

Коммутация выполняется исходя из значения VPI/VCИ в заголовке ячейки. Пара VPI/VCИ значима только в пределах физического канала и поэтому может меняться в процессе пересылки ячейки по АТМ-домену.

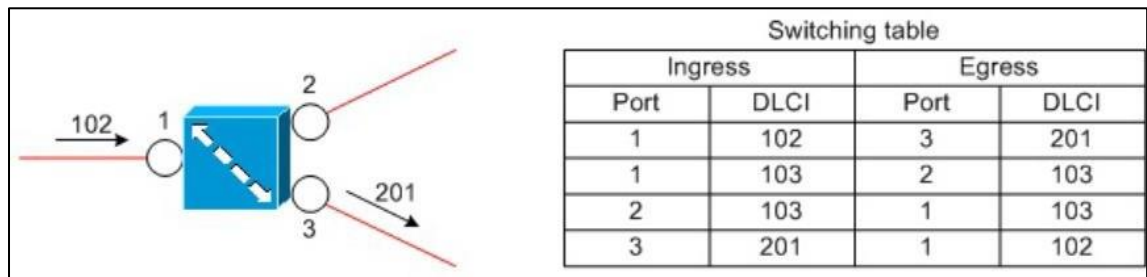
С каждым VPI/VCИ НА КОНКРЕТНОМ ПОРТЕ! ассоциируется конкретный выходной VPI/VCИ на выходном порте



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

Принцип работы FR-коммутатора.

С каждым входным DLCИ НА КОНКРЕТНОМ ПОРТЕ! ассоциируется конкретный выходной DLCИ на выходном порте



83. Протоколы *ILMI* и *ELMI*

Для отслеживания состояния VCs между оконечными устройствами и коммутаторами, а также VCs между коммутаторами, был разработан специальный интерфейс-протокол, получивший название **ILMI** (Integrated Local Management Interface) или просто LMI.

ILMI разработан по образцу SNMP и позволяет:

1. Определять состояние сетевого интерфейса
2. Определять наличие PVCs
3. Определять соответствие конфигураций непосредственно связанных устройств
4. Собирать статистику
5. Расширить возможности мультикаст- и глобальной адресации.

ILMI базируется на периодическом обмене сообщениями (keepalives).

В FR, так же, как и в ATM, имеется LMI, точнее **ELMI (Enhanced LMI)**. Также происходит периодический обмен.

За достаточно длительную историю FR были разработаны три стандарта LMI :

1. Annex A -- общепромышленный стандарт, задействуется DLCI = 0.
2. Annex D -- альтернативный общепромышленный стандарт, так же задействуется DLCI = 0.
3. «Gang of Four» - разработан Cisco, DEC, StrataCom и Nortel - задействуется DLCI = 1023.