





До долбаного отказа!!!!!!!!!!!

[**1 Назначение и структура сетевых адаптеров 3**](#_awqkfwj3onxc)

[**2 Соответствие компонентов сетевых адаптеров модели OSI 4**](#_mrour6bm7zw3)

[**3 Характеристики и критерии выбора сетевых адаптеров 5**](#_xcntdlwxhhkx)

[**4 Поколения сетевых адаптеров 6**](#_k6okvvwgg8dq)

[**5 Назначение и классификация пассивного сетевого оборудования 7**](#_lj4l3h8k1f0)

[**6 Назначение и классификация активного сетевого оборудования 8**](#_gopyffok43e3)

[**7 Структура коммутатора и методы коммутации 9**](#_58e6hzssyrc)

[**8 Структура таблицы коммутатора Ethernet и ее использование 10**](#_z155gez9n05y)

[**9 Гибридные технологии L2 -- L3 11**](#_fg4e7ahbv1s5)

[**10 Характеристики и критерии выбора активного сетевого оборудования 12**](#_wjjddehbszub)

[**11 Производители сетевого оборудования различных категорий 13**](#_ivwrkldn5jek)

[**12 Коммутаторы Cisco 14**](#_aahfl76687l8)

[**13 Cisco IOS и коммутаторы 15**](#_7w9wb953ujho)

[**14 Конфигурирование порта Ethernet коммутатора Cisco 16**](#_v9ky9itdtjcz)

[**15 Таблица коммутатора Cisco 2960 17**](#_taywdms7bjrh)

[**16 Понятие виланов, их достоинства и недостатки 18**](#_fbfl6lcz2qtt)

[**17 Классификации и реализации виланов 19**](#_xfafgw7h0uu3)

[**18 802.1Q 20**](#_kcnqq98wnzn5)

[**19 Маршрутизация между виланами 21**](#_5tg7j2hvofb)

[**20 Поддержка виланов в Windows и Linux 22**](#_f7nvg62nwvg7)

[**21 Конфигурирование виланов в IOS 23**](#_re338workeiv)

[**22 Конфигурирование маршрутизации между виланами в IOS 24**](#_a28aes2yuv9x)

[**23 Протокол VTP и его использование 25**](#_24q09lheap1r)

[**24 Конфигурирование VTP 26**](#_b8jtt4kv9op0)

[**25 Назначение и терминология протокола STP 27**](#_is7sgbfuh21w)

[**26 STP-конвергенция 28**](#_vos49mkn9a95)

[**27 Модификации протокола STP 29**](#_itylbwx0fnge)

[**28 Конфигурирование STP в IOS 30**](#_et0djf6vwswc)

[**29 Понятие агрегации каналов 31**](#_jt4ehq9qkscr)

[**30 Технологии агрегации каналов 32**](#_c3bs44mu7xui)

[**31 Поддержка агрегации каналов в Windows и Linux 33**](#_piohpomwe4e)

[**32 Конфигурирование EtherChannels 34**](#_2df0f6gctom)

[**33 Понятие кластеризации активного сетевого оборудования 35**](#_m4mb7ee9t3ij)

[**34 Технологии кластеризации активного сетевого оборудования 36**](#_48lyf88kansd)

[**35 Конфигурирование маршрутизирующих кластеров в IOS 37**](#_3trz5fw1rb9x)

[**36 Назначение, использование и альтернативы Cisco Port Security 38**](#_b4jfvr4sqygr)

[**37 Конфигурирование Cisco Port Security 39**](#_v3shllz49og9)

[**38 Назначение и классификация Cisco ACLs 40**](#_9fd7mdrcfkrk)

[**39 Структура Cisco ACLs 41**](#_7hia0oag2ixa)

[**40 Правила фильтрации в Cisco ACLs и их обработка 42**](#_lbybm86yjqds)

[**41 Нумерованные стандартные IP ACLs и их примеры 43**](#_hahv5n8njtch)

[**42 Именованные стандартные IP ACLs и их примеры 44**](#_2nhhw6kdsswc)

[**43 Нумерованные расширенные IP ACLs и их примеры 45**](#_n2h7e4oybvzu)

[**44 Именованные расширенные IP ACLs и их примеры 46**](#_wwo4mr8k92vv)

[**45 Правила и примеры привязки классических ACLs 47**](#_yi3x9s62qng)

[**46 VLAN maps и их примеры 48**](#_igl5mr97ommb)

[**47 IPv6 ACLs и их примеры 49**](#_5vgew6j61qby)

[**48 Комплексные ACLs и их примеры 50**](#_80ymfmq25n8g)

[**49 Port Mirroring и Storm Control, их примеры 51**](#_wcr3z42up177)

[**50 Протоколы для активного сетевого оборудования одного производителя и стекирование коммутаторов, их примеры 52**](#_bszj1fpj8a63)

[**51 Конфигурирование стека коммутаторов в IOS 53**](#_10yt0h2is6tl)

[**52 Семейство стандартов Wi-Fi 54**](#_9k97feig59uj)

[**53 Физический уровень Wi-Fi 55**](#_wadns3cppigi)

[**54 Каналы Wi-Fi 56**](#_3a0fu7i8k1nl)

[**55 Модуляция и кодирование в рамках Wi-Fi 57**](#_1r44ybb2cix6)

[**56 Стандарты беспроводной связи, кроме Wi-Fi 58**](#_79dukchsikr8)

[**57 Антенны для беспроводного сетевого оборудования и сопутствующие расчеты 59**](#_mvgmu34cprqj)

[**58 Назначение и классификация беспроводного сетевого оборудования 60**](#_sqiarjbvue8l)

[**59 Структура беспроводной сети 61**](#_baem9sq1btsw)

[**60 Идентификация и виланы в беспроводных сетях 62**](#_ijyfvoudmhy4)

[**61 Развертывание беспроводной сети 63**](#_ngfmv1c0995f)

[**62 Беспроводное сетевое оборудование Cisco 64**](#_61usluk6wkou)

[**63 Беспроводные технологии Cisco 65**](#_edfy3av6njlv)

[**64 Конфигурирование беспроводного маршрутизатора Linksys 66**](#_6q88qkpgeinf)

[**65 Интеграция компьютерных сетей в системы связи 67**](#_i09nrx6mqk8c)

[**66 Структура и синхронизация цифровых сетевых интерфейсов 68**](#_7mzguqmw5mat)

[**67 Плезиохронная и псевдосинхронная цифровая иерархия 69**](#_5ygncjfebphy)

[**68 Абонентское и провайдерское оборудование 70**](#_devk4vs19t1p)

[**69 Последовательные сетевые интерфейсы 71**](#_wmizey1os9cc)

[**70 Протокол PPP и смежные протоколы 72**](#_y72vd566knel)

[**71 Конфигурирование последовательных сетевых интерфейсов в IOS 73**](#_v71lvfqonff3)

[**72 Обзор технологии Dial-up и структура Dial-up RAS 74**](#_5i8p70luc4l2)

[**73 Обзор технологии ISDN и структура ISDN-домена 75**](#_oev7a6lp2m01)

[**74 Обзор технологии ATM и структура ATM-домена 76**](#_ejk1jk752pmn)

[**75 Примеры инкапсуляции в ATM-системе 77**](#_qm7ka7ikyscj)

[**76 Семейство стандартов xDSL 79**](#_aa47wb1ss456)

[**77 Каналы и модуляция в рамках xDSL 80**](#_rda7m0nvoemq)

[**78 Структура xDSL RAS 81**](#_fr3yc3g0xj8z)

[**79 Примеры инкапсуляции в xDSL-системе 82**](#_4vo3hmhawxw5)

[**80 Обзор технологии FR и структура FR-домена 83**](#_l7qafgh37ch0)

[**81 Виртуальные цепи ATM, FR и подобных технологий 84**](#_um8xboyzwyau)

[**82 Принцип работы ATM- и FR-коммутаторов 85**](#_nd0j5vc26laq)

[**83 Протоколы ILMI и ELMI 86**](#_xwci2po4aom4)

# 

# 1 Назначение и структура сетевых адаптеров

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

Обобщенная структура включает в себя:

1) Блок индикации.

2) Разъем для подключения к СрПД.

3) Приемопередатчик (блок развязки для подключения к определенной СрПД).

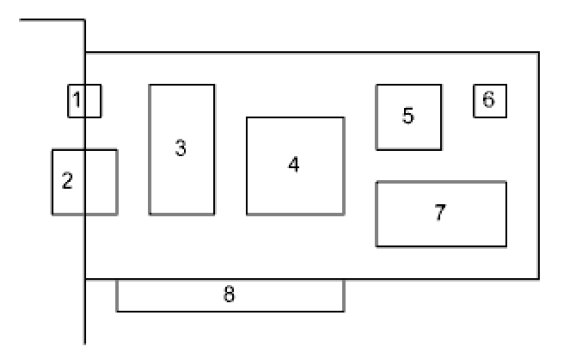
4) Сетевой контроллер.

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 или boot ROM.

8) Разъем для подключения к шине расширения компьютера.



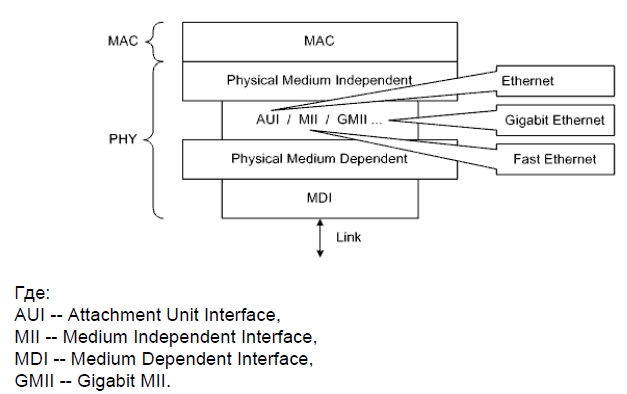
[**https://community.fs.com/ru/article/nic-card-guide-for-beginners-functions-types-and-selection-tips.html**](https://community.fs.com/ru/article/nic-card-guide-for-beginners-functions-types-and-selection-tips.html) **(Если интересно разобраться)**

# 2 Соответствие компонентов сетевых адаптеров модели OSI

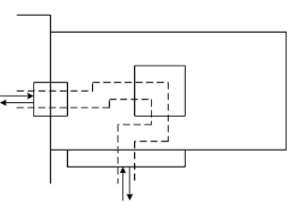
Блок PHY (PHYsical), он же трансивер, не обязательно интегрирован в кристалл контроллера -- он может быть изготовлен на основе отдельной микросхемы. В случае c Ethernet структура PHY постепенно претерпевала изменения и, в результате, собственно внешний трансивер (как и внутренний) может подключаться по-разному. На практике, при подключении внешних трансиверов, интерфейсы AUI и MII соответствуют физическим разъемам (DA-15 плюс кабель, и сорока контактные разъемы D Miniature соответственно).

Ситуация с интерфейсом GMII и его модификациями иная. После появления Gigabit Ethernet широкое применение нашли трансиверы: сначала GBIC (GigaBit Interface Converter), затем SFP (Small Form-factor Pluggable), и затем SFP+ (уже 10 Gigabit Ethernet). При этом физическое подключение происходит через интерфейс SGMII (Serial GMII), а преобразования данных между GMII и SGMII (serialization/deserialization) выполняет блок PMA (Physical Medium Attachment).

Внешние трансиверы обычно подключают к коммутаторам.



# 3 Характеристики и критерии выбора сетевых адаптеров



Стоит учесть «Узкие места», влияющие на суммарную производительность. В идеальном случае пропускные способности СрПД, контроллера и шины расширения (для ПК) должны совпадать.

1) СрПД.

2) Область применения: desktop, server, mobile.

3) Степень интеграции: add-on, on-board.

4) Управляемость: management, unmanagement.

5) Режим работы: half duplex, full duplex.

6) Технические характеристики: размеры буферов и так далее.

7) Количество предоставляемых сетевых интерфейсов: single, dual, quad.

8) Дополнительные возможности: аппаратная поддержка шифрования,

сбор статистики и другое.

9) Возможности энергосбережения: ACPI, WOL и другие.

10) Вариант поставки: OEM, Retail

Производители сетевых адаптеров (и сетевых контроллеров): High-end: Intel, HPE, CSPi и некоторые другие.

Low-end: Realtek, D-link, Compex, TRENDnet, Surecom и многие другие.

# 4 Поколения сетевых адаптеров

Поколения сетевых адаптеров Ethernet (типичные характеристики и типичные представители):

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

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

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

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

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

# 5 Назначение и классификация пассивного сетевого оборудования

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

Общая классификация:

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

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

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

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

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

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

# 6 Назначение и классификация активного сетевого оборудования

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

*Предназначено для передачи, приёма, обработки, перенаправления и распределения информации под управлением специальных протоколов сетевого и канального уровня.(не лк)*

Общая классификация:

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

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

Этот список можно смело дополнить еще одним типом оборудования:

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

# 7 Структура коммутатора и методы коммутации

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

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

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

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

Основные методы коммутации:

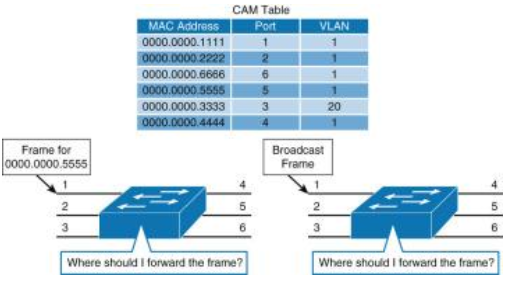
1. Store&Forward -- с промежуточной буферизацией -- коммутатор получает пакет полностью перед его ретрансляцией; анализируется адрес назначения и проверяется контрольная сумма.

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

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

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

# 8 Структура таблицы коммутатора Ethernet и ее использование



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

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

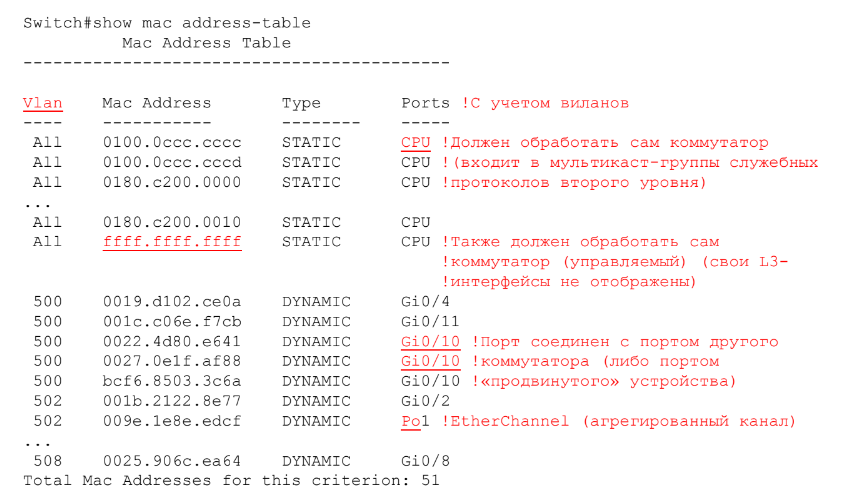
При приеме юникаст-кадра некоторым портом, коммутатор **связывает MAC-адрес источника с номером этого порта** **и заносит в таблицу** (этот процесс называют изучением). При ретрансляции кадров, порт для передачи определяется исходя из MAC-адреса назначения по таблице.

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

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

При ретрансляции пакетов (Smart-коммутаторами) учитываются виланы.

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

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

# 9 Гибридные технологии L2 -- L3

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

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

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

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

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

# 10 Характеристики и критерии выбора активного сетевого оборудования

Характеристики и критерии выбора активного сетевого оборудования:

1. Область применения: workgroup -- для рабочих групп, backbone (core) – магистральные.

2. Тип и число физических портов: 4 (+1), 8, 12, 16, 24, 48 (другие редко).

3. Уровень модели OSI: L2, L2+, L3, L3+.

4. Набор поддерживаемых протоколов маршрутизации(для L3-устройств).

5. Управляемость: unmanaged -- неуправляемые, managed --управляемые (свой IP адрес, выделенная консоль RS-232C, web-интерфейс, SNMP).

6. Структура: fixed -- фиксированная, modular -- модульная.

7. Возможность масштабирования: unstackable -- нестекируемые, stackable -- стекируемые.

8. Наличие разъемов расширений: стандартных и оригинальных.

9. Технические характеристики: размеры таблиц, времена задержек и другие.

10. Суммарная пропускная способность (стоит выделить отдельно).

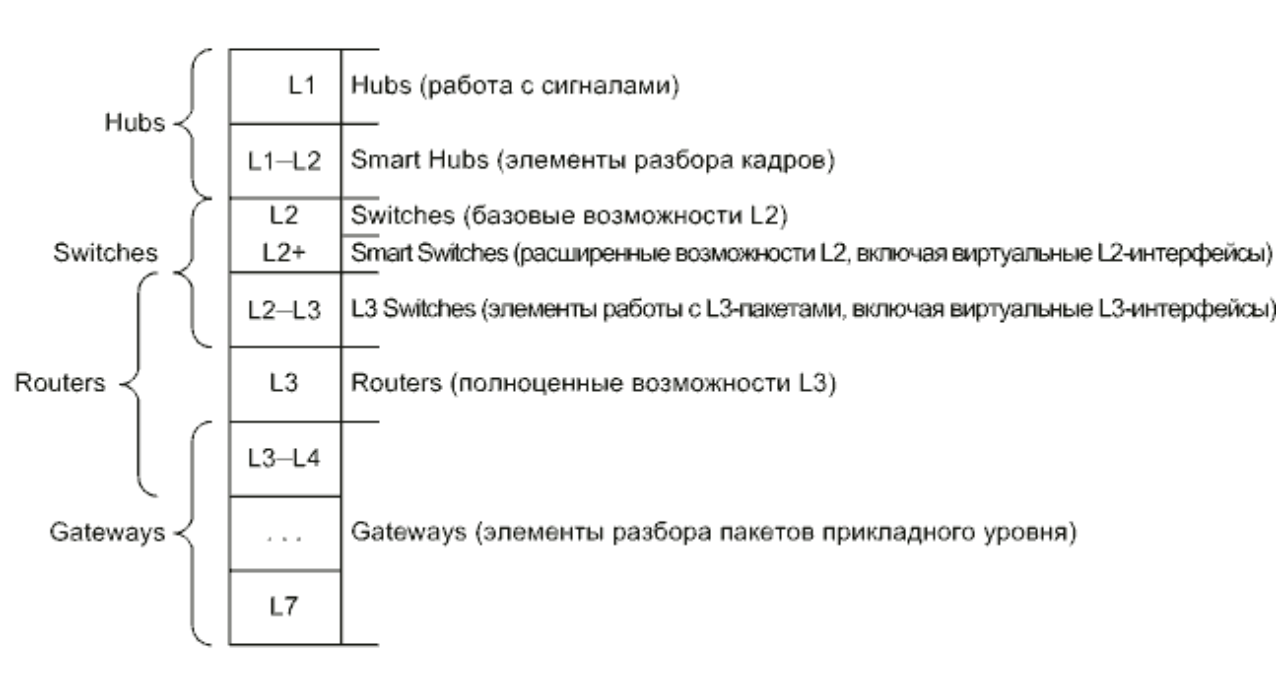
11. Возможность автоматического определения скорости и режима (физического соединения): auto-negotiation и auto-MDI/MDIX.

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:

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

HP (3COM) (OfficeConnect, Baseline, SuperStack),

HPE (ProCurve),

Aruba (HPE),

Cisco (множество серий коммутаторов Catalyst и маршрутизаторов),

Avaya (Nortel) (Passport, Baystack, Netgear, много серий),

Alcatel-Lucent (Nokia) (много серий),

Juniper (много серий),

Allied Telesis (много серий),

Commscope (Ruckus),

Zyxel (Omni LAN, Dimension),

Broadcom (Persona), Marvell (Prestera)

и некоторые другие.

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

# 12 Коммутаторы Cisco

Коммутаторы Cisco делили на шесть основных целевых категорий (LAN access, LAN compact, LAN core and distribution, Data center, Industrial Ethernet, Small-business) и множество серий.

По состоянию на сентябрь 2022 г. категорий уже пять (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 именно для центров обработки данных - даже первые модели имеют основные порты 10 Gigabit Ethernet.А сейчас уже доступны модели с основными портами 100 Gigabit Ethernet, причем некоторые с малой латентностью (low latency) – особый класс оборудования (по сути, системы реального времени с регламентированными коммутационными задержками).

Некоторые серии поддерживают модули.

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

Некоторые серии поддерживают стекирование.

AUX-порты в коммутаторы Cisco не устанавливают.

У дешевых коммутаторов нет тумблеров питания.

Для переключения режима индикации используют кнопку Mode.

Как и маршрутизатор, коммутатор представляет собой микро-ЭВМ, только с более специализированной элементной базой.

В лабах использовали 2960 (имба).

# 13 Cisco IOS и коммутаторы

Актуальны следующие версии IOS для коммутаторов:

12.2 -- для 2960, 3560, 3750 и других «современников»,

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.

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 (поэтому и не Catalyst)

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

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

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

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

Коммутаторы соответствующих серий поставляют с IOS XE в режиме install.

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

# 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 gi1/1

Switch(config-if)#media-type sfp

Switch(config-if)#exit

Switch(config)#interface gi1/0/1

Switch(config-if)#flowcontrol receive on

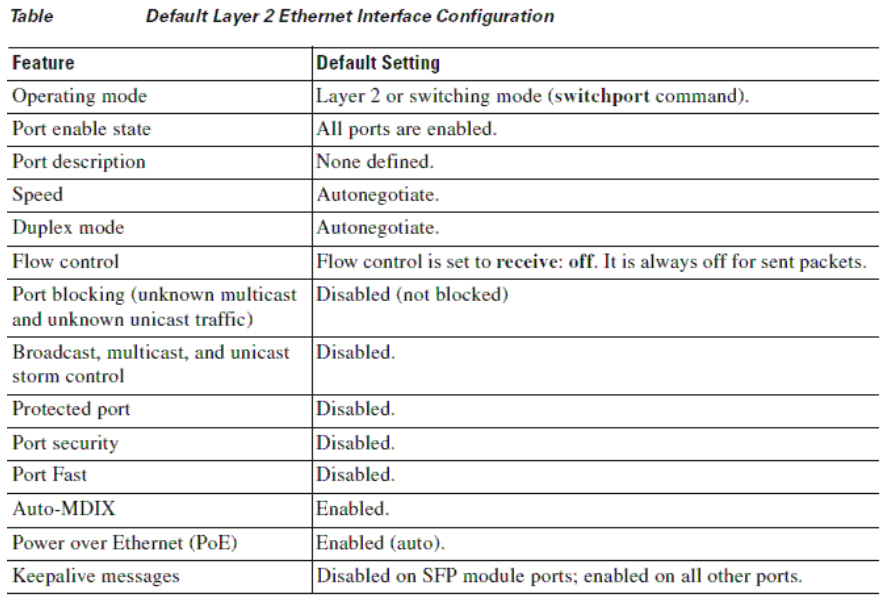
Switch(config-if)#exit

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

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

Switch(config-if-range)#exit

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



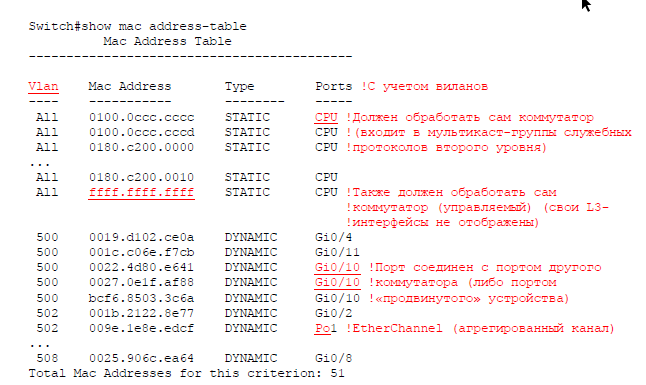
Для просмотра CAM-таблицы используют команду show mac addreess-table

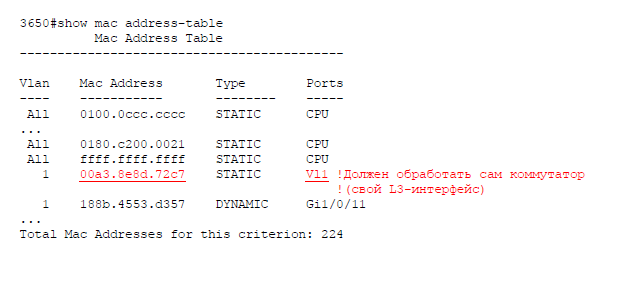
Для привязки статических MAC адресов: mac-address-table static

# 15 Таблица коммутатора Cisco 2960

Для просмотра CAM-таблицы используют команду show mac address-table

(Описать столбцы таблицы, привести 2 примера, расписать красный тхт)

**

**

# 16 Понятие виланов, их достоинства и недостатки

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

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

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

Основные достоинства виланов:

1. Использование виланов помогает контролировать трафик, в первую очередь широковещательный.

2. С помощью виланов обеспечивают дополнительную защиту информации.

3. Виланы лучше адаптированы к изменениям в составе сетевого оборудования.

Основные недостатки виланов:

1. Необходимость наличия значительно более дорогостоящего сетевого оборудования (например, сетевые адаптеры типа server и коммутаторы не ниже уровня L2+).

2. Применение виланов приводит к увеличению вычислительной нагрузки по причине вносимых количественных и качественных дополнений.

# 17 Классификации и реализации виланов

*Критерии классификации виланов:*

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

Здесь уместна еще одна классификация виланов на основе тегов:

1. Data VLAN -- «рабочий» вилан -- предназначен для передачи пользовательского трафика (может быть назначен любой незарезервированный VID).

2. Default VLAN -- вилан по умолчанию -- в данный вилан включаются все порты коммутатора по умолчанию (не может быть ни изменен, ни удален; зарезервирован VID = 1).

3. Management VLAN -- административный вилан -- предназначен для администрирования (выделяют исходя из соображений безопасности; от пользовательских виланов отличается только назначением).

4. Native VLAN -- вилан для оригинального трафика -- предназначен для передачи нетегированного трафика (по умолчанию это вилан с VID = 1; может быть назначен любой незарезервированный VID).

5. Private VLAN -- приватный вилан -- предназначен для частичного запрета трафика в рамках вилана (позволяет масштабировать виланы).

6. Reserved VLAN -- зарезервированный вилан -- предназначен для передачи специфического трафика (например, голосового; VID может быть как из зарезервированного, так и с незарезервированного диапазона; в Cisco IOS зарезервированы VIDs: 0, 1, 1002 -- 1005, 1006 -- 1024, 4095).

***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.

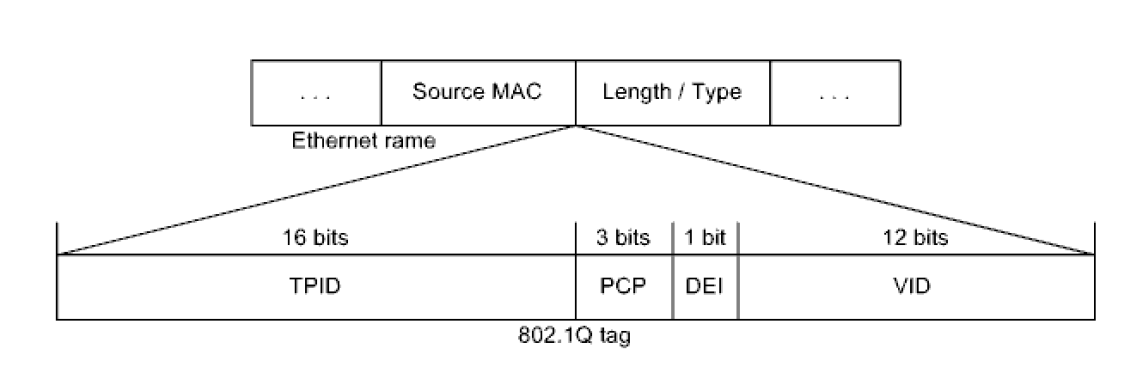
1. Физические порты (physical ports), то есть точки подключения сетевого оборудования (сетевых адаптеров, коммутаторов и другого).

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.)

# 18. 802.1Q

**

**IEEE 802.1Q** — открытый стандарт, который описывает процедуру тегирования трафика

для передачи информации о принадлежности к [VLAN](https://ru.wikipedia.org/wiki/VLAN) по сетям стандарта [IEEE 802.3](https://ru.wikipedia.org/wiki/IEEE_802.3) [Ethernet](https://ru.wikipedia.org/wiki/Ethernet).

Рассмотрим более подробно реализации 802.1Q.

Поля:

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

2. PCP либо User\_Priority -- код приоритета либо приоритет пользователя.

3. Drop Eligible Indicator (DEI) либо -- индикатор разрешения отброса кадра либо индикатор канонического формата MAC-адреса (в обычном кадре Ethernet равно нулю).

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

Также стоит учитывать, что Концепция 802.1Q допускает многократную тегировку кадров (QinQ), но нужно помнить что каждый тег увеличивает кадр, а значит длина кадра может превысить значение MTU. Сетевое оборудование обрабатывает теги, находящиеся «на вершине» (наиболее близкие к началу кадра).

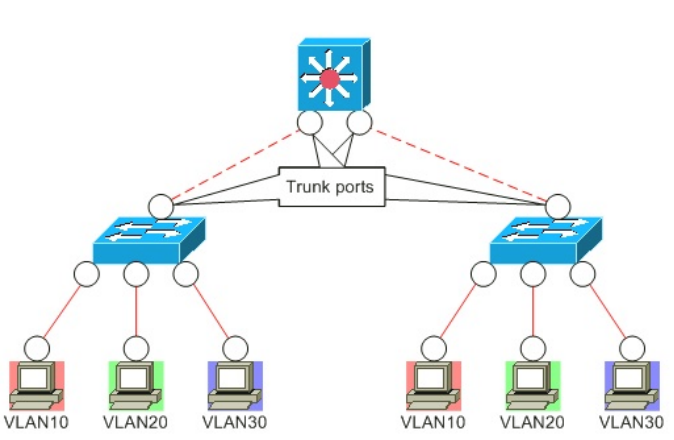
*При использовании стандарта Ethernet II, 802.1Q вставляет тег перед полем «Тип протокола». Так как фрейм изменился, пересчитывается контрольная сумма.*

*В стандарте 802.1Q существует понятие Native VLAN. По умолчанию это VLAN с номером 1. Трафик, передающийся в этом VLAN, не тегируется. При этом на оборудовании некоторых производителей предусмотрена возможность включения тегирования трафика в Native VLAN.(не лк)*

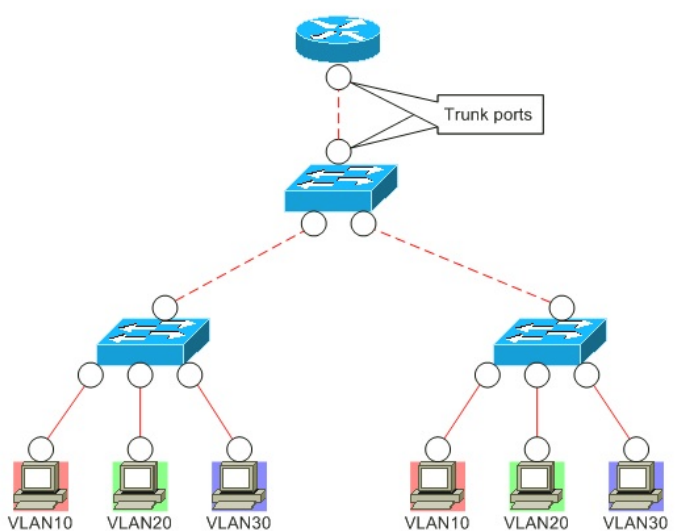
# 19 Маршрутизация между виланами

С точки зрения IP-адресации каждый вилан 802.1Q является виртуальным аналогом физического сегмента (в большинстве случаев оконечного) и соответствует IP-подсети -- со всеми вытекающими последствиями.

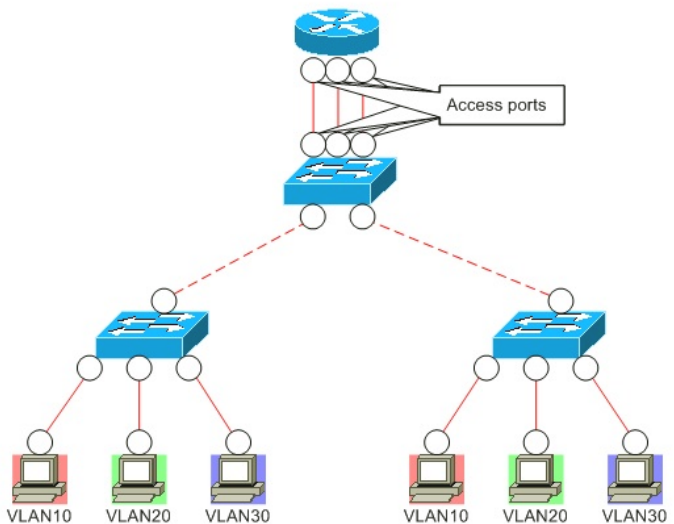
Для обеспечения возможности передачи пакетов из одного вилана в другие необходима маршрутизация между виланами (inter-VLAN routing).

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-stick).



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

Типичный L3-коммутатор отличается от маршрутизатора больши'м 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 мультиплексируемыми сетевыми интерфейсами (тегированный и нетегированный трафик).

В Linux поддержка виланов выражена в подинтерфейсах.

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

Номер подинтерфейса соответствует VID в кадре (тегированный трафик),

eth0 соответствует native VLAN (нетегированный трафик).

Подинтерфейсы eth0 могут сосуществовать с eth0.

# 21 Конфигурирование виланов в IOS

Информация о виланах хранится в vlan.dat (подсистема памяти Flash)

Пример создания пользовательского вилана.

Switch>enable

Switch#configure terminal

Switch(config)#vlan 10

Switch(config-vlan)#name STUDENTS

Switch(config-vlan)#exit

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

Пример назначения порта доступа.

Switch(config)#interface fa0/11

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

Switch(config-if)#exit

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

Switch(config-if)#exit

Если кроме 802.1Q поддерживается ISL (как на 3560), то по умолчанию происходит автосогласование типа инкапсуляции. Рекомендуется использовать команду switchport trunk encapsulation dot1q – для явного указания.

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

В результате, порт может находиться в одном из следующих транковых

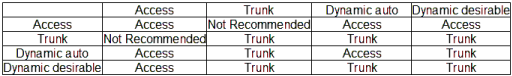
режимов:

1. dynamic auto (по умолчанию).

2. dynamic desirable.

3. trunk.

Формирование транка зависит от режима каждого из портов, образующих соответствующую пару, следующим образом.

****

# 22 Конфигурирование маршрутизации между виланами в IOS

Пример создания и конфигурирования SVI (Switch Virtual Interface) --

ассоциированного с виланом виртуального сетевого интерфейса (L3-интерфейса).

Начиная с IOS версии 12.2, SVI необходимо административно включать (после создания, по аналогии с другими L3-интерфейсами).

Switch(config)#interface vlan 10

Switch(config-if)#ip address 192.168.11.11 255.255.255.0

Switch(config-if)#no shutdown

Switch(config-if)#exit

Если IP-адрес нужен только в рамках административного вилана, то для

указания шлюза по умолчанию предназначена команда ip default-gateway. Поскольку коммутатор Cisco по умолчанию является устройством второго уровня, IP-маршрутизация на нем по умолчанию выключена (в отличии от маршрутизатора -- устройства третьего уровня).

Switch(config)#ip default-gateway 192.168.11.1

Switch(config)#ip routing

...

Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.11.1

Пример создания и конфигурирования подинтерфейсов на

маршрутизаторе. 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 поддерживает только так называемые normal-range VLANs (VIDs от 1 до 1005). Extended-range VLANs (VIDs больше 1005) игнорируются.

Разработаны три версии протокола VTP: 1, 2 и 3. В границах VTP-домена допускается применение только одной версии.

Существенным отличием VTPv2 от VTPv1 является то, что коммутаторы в прозрачном VTP-режиме ретранслируют VTP-сообщения.

В отношении VTP коммутатор может функционировать в одном из трех

режимов (VTP mode):

1. VTP-сервер (VTP server).

2. VTP-клиент (VTP client).

3. Прозрачный режим (VTP transparent).

VTP-сервер предназначен для создания, модификации или удаления виланов, а также задания конфигурационных параметров применительно ко всему VTP-домену.

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

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

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

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

VTP-сообщения бывают трех видов:

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

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

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

*Также можно добавить про VTP pruning…*

# 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 (pruningeligible

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

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 (vlan.dat).

Основная команда для определения состояния подсистемы VTP:

show vtp status.

# 25 Назначение и терминология протокола STP

Пакеты второго уровня (фреймы) не имеют поля TTL, что приводит к возможности возникновения бесконечных циклов при их ретрансляции. Группа протоколов второго уровня под общим названием Spanning Tree призвана бороться с зацикливанием в СПД при резервировании физических каналов.

Собственно STP – это, по сути, один из алгоритмов построения из группы произвольно соединенных между собой L2-устройств виртуального дерева, то есть графа, не содержащего логических петель. Заложенный в STP алгоритм позволяет находить один из лучших вариантов среди множества возможных.

Некоторые модификации STP совместимы с виланами.

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

1. **Первоначальная STP-конвергенция** (STP convergence) -- первоначальное построение дерева.

2. **Устоявшееся состояние** -- полезная работоспособность.

3. **Повторная STP-конвергенция** -- перестроение дерева по причине топологических изменений с последующим возвращением в устоявшееся состояние.

По протоколу STP коммутаторы обмениваются сообщениями BPDUs.

STP-роли портов:

1. **Корневой (root)** -- разрешено передавать кадры, ближайший обращенный к корневому мосту.

2. **Назначенный (designated)** -- разрешено передавать кадры, обращенный в сторону от корневого моста.

3. **Альтернативный (alternate)** или, иначе, резервный (backup) – запрещено передавать кадры.



В каждый момент времени каждый порт коммутатора находится в одном

из следующих STP-состояний:

1. **Блокировка (blocking)** -- не участвует в пересылке кадров.

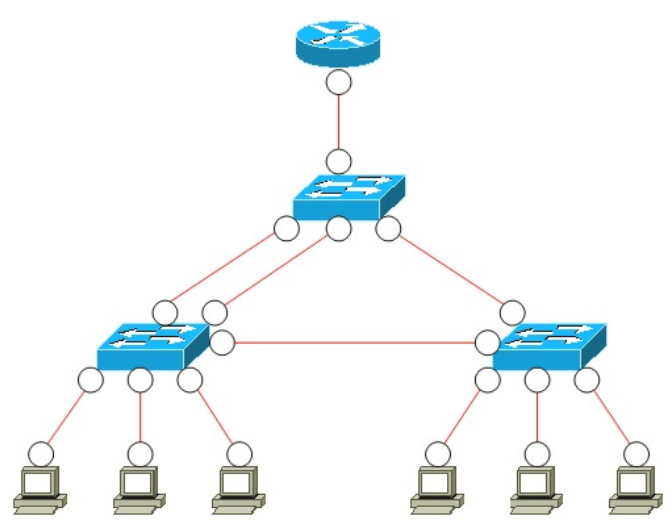
2. **Прослушивание (listening)** -- принимается решение о возможности

участия в пересылке кадров.

3. **Изучение (learning)** -- готовится к участию в пересылке кадров.

4. **Ретрансляция (forwarding)** -- участвует в пересылке кадров.

5. **Запрет (disabled)** -- вообще не участвует в работе, то есть не подключен к СрПД, административно выключен, или не поддерживает STP.



Пример СПД с возможностью зацикливания:

# 26 STP-конвергенция

STP-конвергенция протекает в три фазы:

1. **Выбор корневого моста.**

2. **Выбор корневых портов.**

3. **Выбор назначенных и альтернативных портов**

В процессе упомянутых выборов анализируются следующие параметры:

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

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

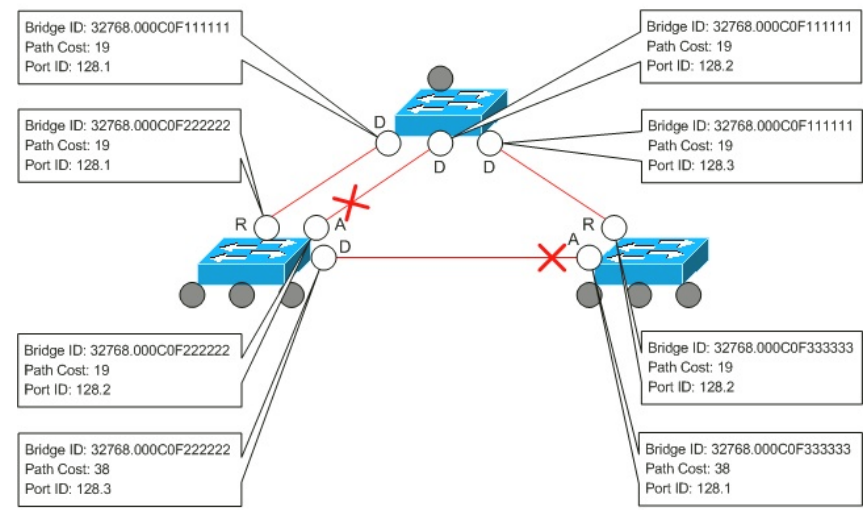
3. **Идентификатор порта (port identifier)** -- ассоциирован с каждым портом, оценивается в рамках коммутатора.

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

Изначально каждый коммутатор считает себя корневым мостом, но после обмена BPDUs корневым становится мост с наивысшим приоритетом, то есть с наименьшим цифровым значением идентификатора моста. При совпадении приоритетов мостов учитывается MAC-адрес. В дальнейшем корневой мост используется как точка отсчета.

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

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

При совпадении идентификаторов портов учитываются номера портов.

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

Назначенный порт выбирается исходя из наименьшей стоимости пути к корневому мосту. При совпадении стоимости учитывается идентификатор порта. Выбирается порт с наименьшим идентификатором. Роль порта в процессе STP-конвергенции может изменяться неоднократно.

В последствии, если какая-либо часть STP-домена претерпела изменение, то оно обнаруживается (регулярный обмен BPDUs) и специальноe 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). Дерево STP строится для каждого из виланов.

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. Если в PVST каждый вилан имеет свое STP дерево, то в MSTP каждый вилан не обязан иметь собственный STP процесс, их можно объединять.

*Почитать про модификации:* [*https://habr.com/ru/articles/143768/*](https://habr.com/ru/articles/143768/)

В качестве альтернативы Spanning Tree применимы другие технологии, например, **Cisco Flex Links** (порту назначают дублирующий порт). Некоторые реализации собственно Ethernet (в том числе от Cisco) поддерживают механизм **Ethernet keep-alive**, также позволяющий обнаружить зацикливание (через порт периодически передается специальный «нулевой» кадр типа 9000h с MAC-адресом источника и MAC-адресом назначения, равными MAC-адресу, относящемуся к порту).

# 28 Конфигурирование STP в IOS

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

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

Совместимость с 802.1D либо 802.1t контролируют командами

*spanning-tree extend system-id* (на большинстве современных платформ «инверсный» вариант команды недоступен) и spanning-tree pathcost method.

*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*

*Switch(config-if)#exit*

**Чатик дал покушать**

Switch# configure terminal

Switch(config)# spanning-tree mode pvst

Switch(config)# spanning-tree vlan 1 priority 0 !Если хотим сделать рутом

Switch# show spanning-tree

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

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

**Включение PortFast и BPDU Guard.**

Switch(config)#interface fa0/2

Switch(config-if)#spanning-tree portfast

...

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

Switch(config-if)#exit

////////////////////////////////////

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).

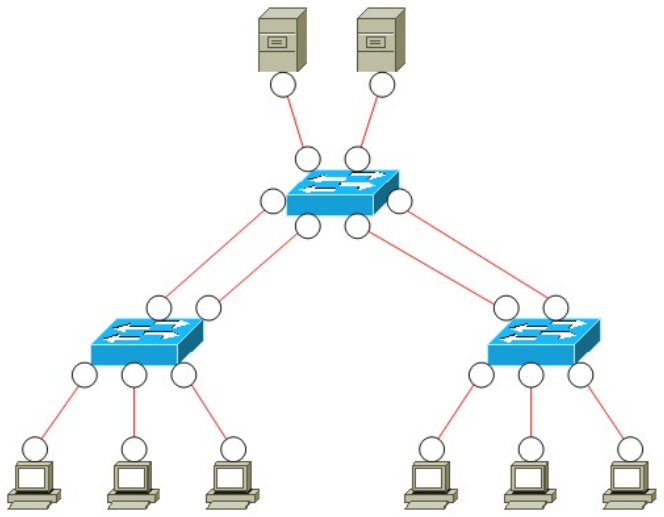
Пример задания таймера.

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

# 

# 29 Понятие агрегации каналов

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



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

С точки зрения STP, транк рассматривается как единая сущность.

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

Максимальное количество членов транка часто ограничено двумя либо восемью.

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.

(Возможно множество вариантов, но стоит выделить два: обычно резервируют каналы, связывающие сетевые адаптеры серверов с активным сетевым оборудованием, и каналы, связывающие активное сетевое оборудование между собой.)

4. Постоянство членства: static, dynamic.

# 30 Технологии агрегации каналов

Основные реализации транков:

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

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

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

**2. Broadcom SLB (Smart Load Balancing)** -- аналог Intel ALB плюс RLB. Два варианта. Вариант Auto-fallback disable отличается от варианта Failover тем, что в случае восстановления после сбоя связующего адаптера эта функция (связующего адаптера) ему не возвращается.

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

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

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

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

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

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

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

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

Современные EtherChannels поддерживают LACP.

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

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

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

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

# 

# 31 Поддержка агрегации каналов в Windows и Linux

**9. 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 подключаются к коммутаторам произвольным образом, поддержка со стороны коммутаторов не требуется.

В windows server 2016/2019 настройка производится в NLB-менеджере. Можно посмотреть свойства кластера NLB и свойства хоста NLB. Также можно включить NLB на уровне сетевого интерфейса.

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

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

Три режима: Switch Independent, Static Teaming, LACP.

**11. 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.

Конфиг в линуксе (/etc/sysconfig/network-scripts/ifcfg-bond0):

**DEVICE=bond0**

ONBOOT=yes

BOOTPROTO=none

**IPADDR=192.168.11.15**

**NETMASK=255.255.255.224**

USERCTL=no

Конфиг в линуксе (/etc/sysconfig/network-scripts/ifcfg-eth0 (eth1 и так далее)):

DEVICE=eth0

ONBOOT=yes

BOOTPROTO=none

**SLAVE=yes**

**MASTER=bond0**

USERCTL=no

/etc/modprobe.conf:

alias bond0 bonding

options bond0 mode=balance-alb miimon=100 !Режим и интервал проверки в ms

Make sure everything is working. Type the following cat command to query the current status of Linux kernel bounding driver, enter:

# cat /proc/net/bonding/bond0

# 

# 32 Конфигурирование EtherChannels

Switch(config)#interface range gi0/1-2

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 10

Switch(config-if-range)#channel-group 1 mode on

Switch(config-if-range)#exit

Switch(config)#interface port-channel 1

Switch(config-if)#spanning-tree portfast

Switch(config-if)#exit

Switch(config)#interface range gi0/3-4

Switch(config-if-range)#no switchport

Switch(config-if-range)#no ip address

Switch(config-if-range)#channel-group 2 mode active

Switch(config-if-range)#exit

Switch(config)#interface port-channel 2

Switch(config-if)#no switchport

Switch(config-if)#ip address 192.168.0.11 255.255.255.0

Switch(config-if)#exit

Предусмотрены шесть вариантов балансировки нагрузки на основе

анализа MAC- и IP-адресов источника и назначения.

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

**Или:**

Switch(config-if-range)# channel-group 1 mode active

Switch(config-if-range)# exit

Switch(config)# interface Port-channel 1

Switch(config-if)# ip address 192.168.1.1 255.255.255.0

Switch# show etherchannel summary

Основная команда для просмотра состояния EtherChannels -- это show etherchannel

# 33 Понятие кластеризации активного сетевого оборудования

Отказ активного сетевого оборудования может происходить по самым разным причинам в самых разных частях СПД.

Отказ того или иного промежуточного маршрутизатора в звене связанных маршрутизаторов вполне успешно разрешается, например, за счет динамической маршрутизации.

Но 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.

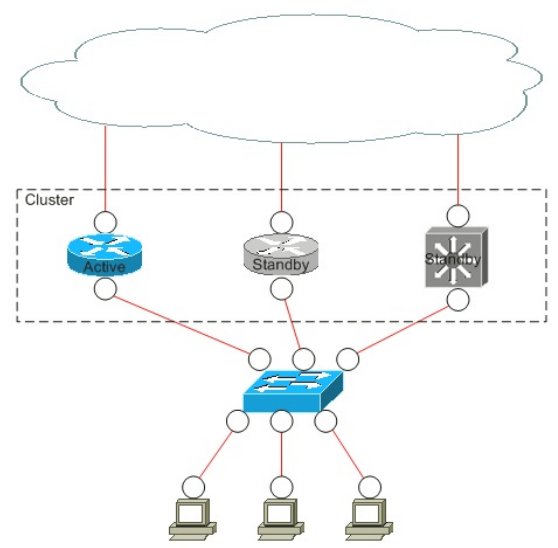
Для защиты от подобных неполадок из группы маршрутизирующих устройств формируют кластеры (router clusters), которым назначают виртуальные IP-адреса (и соответствующие виртуальные MAC-адреса из специальных диапазонов).

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

Увы, 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.

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

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

В настоящее время наблюдается все больший уклон в виртуализацию.

Пример организации кластера из L3-устройств в СПД

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

# 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 **FHRPs (First Hop Redundancy Protocols).**

Основные протоколы:

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

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

**3. HSRP - Hot Standby Router Protocol**

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

Основные технологии, связанные с коммутаторами:

1. **Intel Adapter Fault Tolerance (AFT).**

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

2. **Intel Switch Fault Tolerance (SFT).**

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

3. **HP NFT Only -- аналог Intel AFT.**

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

4. **Cisco & IBM Link-State Tracking.**

Состояние downstream-портов (обращенных в сторону ООД) ставят в

зависимость от состояния upstream-портов (обращенных в сторону СПД), что

позволяет более правильно распределять нагрузку в некоторых типовых топологиях с резервированием.

5. **Cisco Virtual Switching System (VSS).**

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

# 35 Конфигурирование маршрутизирующих кластеров в IOS

Примеры формирования кластеров с помощью Cisco IOS.

Активный маршрутизатор выбирается исходя из приоритета. Приоритет

задают числом от 0 до 255. Чем больше число, тем выше приоритет. При равенстве чисел сравниваются IP-адреса. Чем больше IP-адрес, тем выше

приоритет.

После восстановления маршрутизатора с наивысшим приоритетом после

сбоя он опционально снова может гарантированно стать активным (preemption).

Возможна аутентификация (символьная строка).

R1(config)#interface gi0/1

R1(config-if)#standby 1 ip 192.168.11.1

R1(config-if)#standby 1 priority 150

R1(config-if)#standby 1 preempt

R1(config-if)#exit

R2(config)#interface gi0/1

R2(config-if)#standby 1 ip 192.168.11.1

R2(config-if)#exit

R1(config)#interface gi0/1

R1(config-if)#glbp 1 ip 192.168.11.1

R1(config-if)#glbp 1 priority 150

R1(config-if)#glbp 1 preempt

R1(config-if)#glbp 1 load-balancing round-robin

R1(config-if)#exit

R2(config)#interface gi0/1

R2(config-if)#glbp 1 ip 192.168.11.1

R2(config-if)#glbp 1 load-balancing round-robin

R2(config-if)#exit

Основные команды для просмотра состояния кластера - это show

standby и show glbp.

Чатик выдал

В Cisco IOS (Internetwork Operating System), конфигурирование маршрутизирующих кластеров обычно выполняется с использованием технологии HSRP (Hot Standby Router Protocol) или VRRP (Virtual Router Redundancy Protocol). Эти протоколы предоставляют механизм для обеспечения отказоустойчивости на уровне маршрутизации.

Ниже представлены примеры конфигурации маршрутизирующих кластеров с использованием HSRP и VRRP в Cisco IOS

interface GigabitEthernet0/0

ip address 192.168.1.1 255.255.255.0

standby 1 ip 192.168.1.254

standby 1 priority 110

standby 1 preempt

interface GigabitEthernet0/1

ip address 192.168.2.1 255.255.255.0

standby 2 ip 192.168.2.254

standby 2 priority 100

standby 2 preempt

В этом примере:

GigabitEthernet0/0 и GigabitEthernet0/1 - интерфейсы маршрутизатора.

standby 1 и standby 2 - номера групп HSRP.

ip address - IP-адреса интерфейсов.

standby ip - виртуальные IP-адреса HSRP групп.

standby priority - приоритет маршрутизаторов в группе.

standby preempt - разрешение приоритетному маршрутизатору стать активным при восстановлении.

VRRP (Virtual Router Redundancy Protocol):

bash

Copy code

interface GigabitEthernet0/0

ip address 192.168.1.1 255.255.255.0

vrrp 1 ip 192.168.1.254

vrrp 1 priority 110

interface GigabitEthernet0/1

ip address 192.168.2.1 255.255.255.0

vrrp 2 ip 192.168.2.254

vrrp 2 priority 100

В этом примере:

GigabitEthernet0/0 и GigabitEthernet0/1 - интерфейсы маршрутизатора.

vrrp 1 и vrrp 2 - номера групп VRRP.

ip address - IP-адреса интерфейсов.

vrrp ip - виртуальные IP-адреса VRRP групп.

vrrp priority - приоритет маршрутизаторов в группе.

Выбор между HSRP и VRRP зависит от предпочтений и совместимости с существующими устройствами в сети. Оба протокола обеспечивают механизм горячей замены и повышения отказоустойчивости в случае сбоя одного из маршрутизаторов.

# 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 (secure MAC addresses), но их суммарное количество не должно превышать установленного максимума.

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

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

После включения опционального более «серьезного » изучения (sticky address learning) динамические доверительные адреса (в том числе изученные до включения этой возможности ) считаются «липкими» (sticky) и, в результате, сохраняются не только в CAM-таблице, а и в рабочей конфигурации. В добавок, можно явно указать какие адреса считать «липкими». «Липкие» адреса не теряются при выключении -включении порта (физическая перекоммутация, административное выключение -включение и так далее).

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

Способы настройки Port-Security:  
1) ***Статические* MAC-адреса** – MAC-адреса, которые вручную настроены на порту, из режима конфигурации порта при помощи команды switchport port-security mac-address [MAC-адрес] . MAC-адреса, сконфигурированные таким образом, сохраняются в таблице адресов и добавляются в текущую конфигурацию коммутатора.

2) ***Динамические* MAC-адреса** - MAC-адреса, которые динамически изучаются и хранятся только в таблице адресов. MAC-адреса, сконфигурированные таким образом, удаляются при перезапуске коммутатора.

3) ***Sticky* MAC-адреса** - MAC-адреса, которые могут быть изучены динамически или сконфигурированы вручную, затем сохранены в таблице адресов и добавлены в текущую конфигурацию. switchport port-security mac-address sticky

В случаях нарушения безопасности может работать в 4 режимах:

1. **Protect** (отбрасывание всех пакетов)
2. **Restrict** (отбрасывание всех пакетов + уведомление о нарушении + счетчик ошибок)
3. **Shutdown** (административное выключение)
4. **Shutdown VLAN** (отключается весь VLAN)

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

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

Альтернативы: ***Port Blocking*** (запрет передачи портом незнакомого юникаст- и мультикаст-трафика), ***Protected Ports*** (трафик между protected-портами запрещен).

# 37 Конфигурирование Cisco Port Security

Пример конфигурирования Port Security.

Включают отдельной командой -- switchport port-security (только один аргумент; опциональные параметры задают аргументами, следующими за этим, что Port Security не включает).

Switch(config)# interface fa0/7

Switch(config-if)#switchport mode access !Либо trunk

Switch(config-if)#switchport port-security

Switch(config-if)#switchport port-security maximum 3 vlan access !Опциональный

!учет виланов

Switch(config-if)#switchport port-security violation protect

Switch(config-if)#switchport port-security mac-address 6045.cba7.f876

Switch(config-if)#switchport port-security mac-address sticky

Switch(config-if)#switchport port-security mac-address sticky 7054.d2bf.5b81

!Таким же образом вносится в рабочую конфигурацию

!автоматически (после предыдущей команды)

Switch(config-if)#switchport port-security aging time 1440 !Минуты

Switch(config-if)#switchport port-security aging type inactivity

Switch(config-if)#switchport port-security aging static

Switch(config-if)#exit

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

# 38 Назначение и классификация Cisco ACLs

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

Каждый элемент представляет собой отдельное правило фильтрации **(ACE – access control entry)**.

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.

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

Фундаментально ACLs делят на три типа:

1. **Port ACLs** -- применимы к L2-интерфейсам (физическим портам).

2. **Router ACLs** -- применимы к L3-интерфейсам (обычным сетевым интерфейсам, SVIs и L3-EtherChannels).

3. **VLAN ACLs** (VLAN maps) -- применимы к виланам.

С точки зрения направленности потока пакетов ACLs могут быть:

1. **Входными (inbound)** -- предназначены для фильтрации входящего трафика, проверка происходит еще до маршрутизации.

2. **Выходными (outbound)** -- предназначены для фильтрации исходящего трафика, проверка происходит после маршрутизации.

С точки зрения синтаксиса ACLs могут быть:

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

2. **Именованными (named)** -- идентифицируются уникальными названиями. Совместимы не со всеми командами.

Наибольший интерес представляют следующие виды ACLs:

1. **Стандартные (standard)** **IP ACLs** (зарезервированы номера 1 -- 99, 1300 -- 1999) -- позволяют выполнять фильтрацию только на основе IP-адресов источников. Применимы к L2- и к L3-интерфейсам.

2. **Расширенные (extended)** **IP ACLs** (зарезервированы номера 100 -- 199, 2000 -- 2699) -- позволяют выполнять фильтрацию на основе IP-адресов источников, IP-адресов назначения, L4-протоколов и номеров программных портов. Применимы к L2- и к L3-интерфейсам.

3. **Расширенные MAC ACLs** (зарезервированы номера 1100 -- 1199) -- позволяют выполнять фильтрацию на основе MAC-адресов источников, MAC-адресов назначения и L3-протоколов. Применимы к L2-интерфейсам.

<https://habr.com/ru/articles/154879/> - Cisco IOS ACL

# 39 Структура Cisco ACLs

Один отдельно взятый ACL, то есть список, 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.

Условия в ACEs могут содержать следующие операторы: **eq** (equal), **gt** (greater than), **lt** (less than), **neq** (not equal) и **range** (inclusive range).

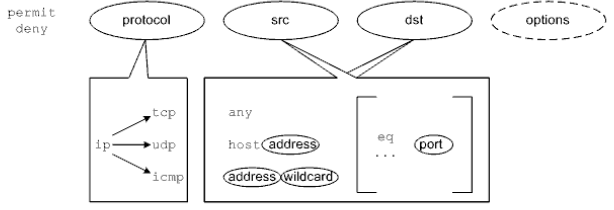
При этом ACEs автоматически последовательно нумеруются, начиная с 10 с шагом 10, что открывает возможность вставлять дополнительные ACEs в «нужные места», но редактировать список произвольным образом возможности нет.

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

C одним интерфейсом одного уровня в одном направлении по одному протоколу может быть связан только один ACL. При повторном связывании, предыдущий ACL вытесняется новым.

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.



# 

# 40 Правила фильтрации в Cisco ACLs и их обработка

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.

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.

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

# 41 Нумерованные стандартные IP ACLs и их примеры

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

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

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

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

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

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

**Чатик выдал**

***Пример 1: Запретить трафик с определенного источника***

access-list 1 deny host 192.168.1.2

access-list 1 permit any

***Пример 2: Разрешить трафик только для определенной подсети***

access-list 2 permit 10.1.1.0 0.0.0.255

access-list 2 deny any

***Пример 3: Разрешить или запретить группу IP-адресов***

access-list 3 permit 192.168.1.0 0.0.0.255

access-list 3 permit 192.168.2.0 0.0.0.255

access-list 3 deny any

***Пример 4: Запретить трафик от конкретных хостов***

access-list 4 deny host 172.16.1.1

access-list 4 deny host 172.16.1.2

access-list 4 permit any

Примечания:

В ACL номера 1-99 и 1300-1999 являются стандартными.

Действия (deny, permit) выполняются в порядке, указанном в списке ACL. В приведенных примерах, если пакет соответствует первому условию, последующие условия не применяются.

Не забывайте применять ACL к интерфейсам с использованием команды access-group.

# 42 Именованные стандартные IP ACLs и их примеры

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).

Создание ACL:  
 Router(config)#ip access-list standard TEST

Router(config-std-nacl)#deny host 192.168.0.3 // seq 10

Router(config-std-nacl)#deny host 192.168.0.4 // seq 20

Router(config-std-nacl)#permit any // seq 30

Router(config-std-nacl)#exit

Редактирование ACL:

Router(config)#ip access-list standard TEST

Router(config-std-nacl)#no 20 // удаляем 20

Router(config-std-nacl)#15 deny host 192.168.0.5

Router(config-std-nacl)#exit

Изменение последовательности ACL:

Router(config)#ip access-list TEST resequence 100 10

(100 - start number, 10 - increment)

Если был лист 10, 15, 20, то станет 100, 110, 120

# 43 Нумерованные расширенные IP ACLs и их примеры

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

В то время как standart ACL позволяют фильтровать только по адресу источника, exteded ACL позволяют фильтровать по более широкому списку параметров как источника, так и назначения.

Расширенные (extended) ACL предоставляют более широкий список параметров для правил фильтрации:

* Протокол, инкапсулированный в IP-пакет
* IP адрес источника
* Порт источника
* IP адрес назначения
* Порт назначения

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 80

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

# 44 Именованные расширенные IP ACLs и их примеры

В то время как standart ACL позволяют фильтровать только по адресу источника, exteded ACL позволяют фильтровать по более широкому списку параметров как источника, так и назначения.

Расширенные (extended) ACL предоставляют более широкий список параметров для правил фильтрации:

* Протокол, инкапсулированный в IP-пакет
* IP адрес источника
* Порт источника
* IP адрес назначения
* Порт назначения

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

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

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 80

Router(config-ext-nacl)#permit tcp any any

Router(config-ext-nacl)#exit

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).

# 45 Правила и примеры привязки классических ACLs

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

смысла. При применении надо будет указать направление фильтрации: in (вход) – трафик приходит с провода на интерфейс роутера, out (выход) – трафик с интерфейса уходит на провод.

Примеры привязки ACLs к интерфейсам:

Router(config)#interface gi0/0

Router(config-if)#ip access-group 99 in

Router(config-if)#exit

Router(config)#interface gi0/1

Router(config-if)#ip access-group WEB out

Router(config-if)#exit

Привязка ACL к линии возможна, но имеет особенности:

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

Router(config)#access-list 23 deny any

Router(config)#line vty 0 4

Router(config-line)#ip access-class 23 in

Router(config-line)#exit

Также ACL можно применить при настройке NAT/PAT:

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

Router(config)#access-list 23 deny any

Router(config)#ip nat inside source list 23 interface Gi0/1 overload

Для просмотра состояния ACLs используют команду show access-list.

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 и привязки 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

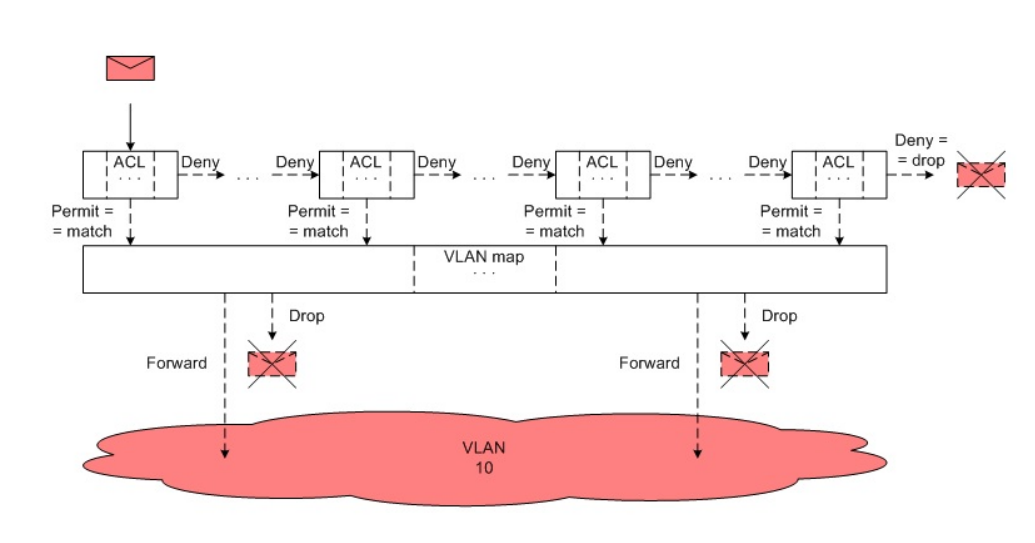
Switch(config)#vlan access-map MAP1 20

Switch(config-access-map)#match ip address 190 191

Switch(config-access-map)#action drop

Switch(config-access-map)#exit

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

permit icmp any any nd-ns.

Два правила permit позволяют работать обнаружению соседей, аналог ARP для IPv6.

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

*Не из лк*

RouterLAN(config)#**ipv6** access-list OUTBOUND

RouterLAN(config-ipv6-acl)#permit tcp host 2002::1 eq 22 any established

RouterLAN(config-ipv6-acl)#permit tcp 2001::/64 any eq 443

RouterLAN(config-ipv6-acl)#exit

RouterLAN(config)#**ipv6** access-list INBOUND

RouterLAN(config-ipv6-acl)#permit tcp any eq 443 2001::/64 established

RouterLAN(config-ipv6-acl)#permit tcp any host 2002::1 eq 22

RouterLAN(config-ipv6-acl)#exit

RouterLAN(config)#interface fa0/1

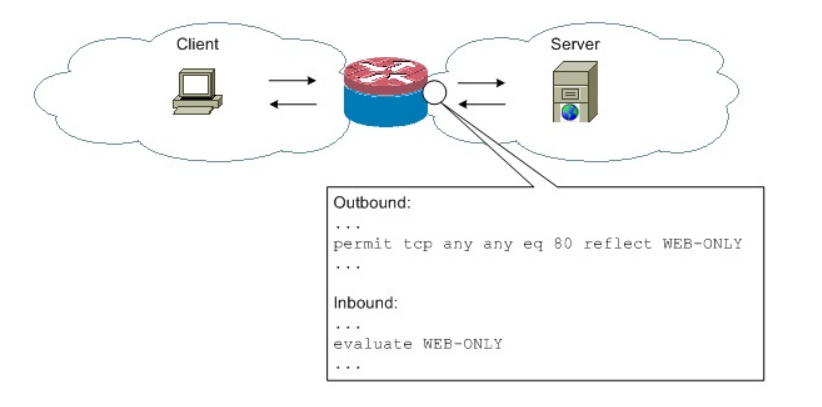
RouterLAN(config-if)#ipv6 **traffic-filter** INBOUND in

RouterLAN(config-if)#ipv6 **traffic-filter** OUTBOUND out

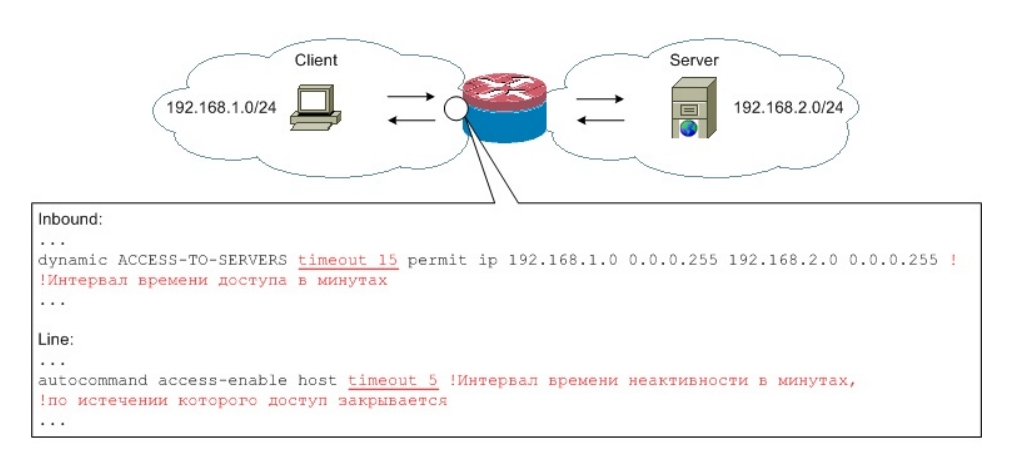
RouterLAN(config-if)#end

# 48 Комплексные ACLs и их примеры

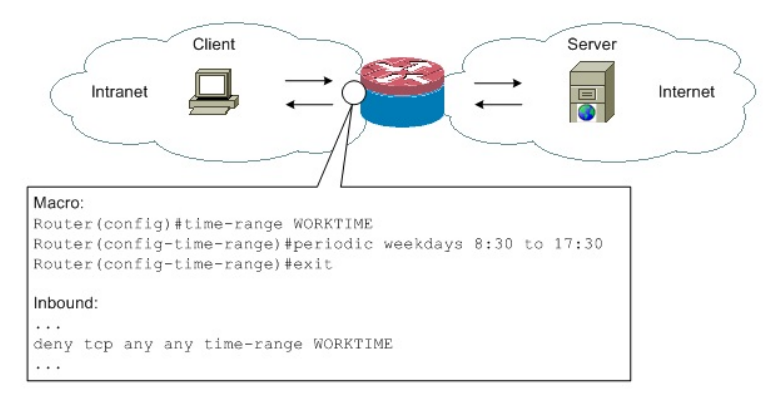
Идея ***рефлексивных*** ACLs заключается в том, чтобы для некоторого правила некоторого ACL автоматически активировать его особым образом описанное «обратное» правило другого ACL, «открывающее дверь» для ответного трафика.



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



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



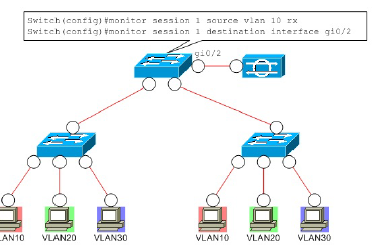
Более сложные технологии фильтрации являются дальнейшим развитием идеи автоматизации создания и активации правил. Для облегчения работы с ACLs, если не обойтись без очень большого числа правил фильтрации, Cisco предлагает так называемые группы объектов (object groups). Cisco FPM (Flexible Packet Matching) позволяет осуществлять фильтрацию пакетов по специальным шаблонам с точностью до бита.

# 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).

**

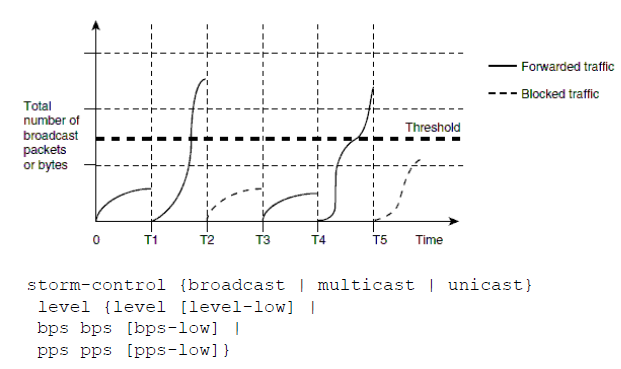
Широковещательный шторм (*Broadcast storm*) — лавина (всплеск) [широковещательных](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%80%D0%BE%D0%BA%D0%BE%D0%B2%D0%B5%D1%89%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%B0%D0%B4%D1%80%D0%B5%D1%81) пакетов (на [втором уровне](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%83%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C) модели [OSI](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%B0%D1%8F_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_OSI) — [кадров](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%B4%D1%80_(%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D0%BD%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B8))). Размножение широковещательных сообщений активным сетевым оборудованием приводит к [экспоненциальному росту](https://ru.wikipedia.org/wiki/%D0%AD%D0%BA%D1%81%D0%BF%D0%BE%D0%BD%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%80%D0%BE%D1%81%D1%82) их числа и парализует работу сети. Такие пакеты, в частности, используются сетевыми сервисами для оповещения станций о своём присутствии. Считается нормальным, если широковещательные пакеты составляют не более 10 % от общего числа пакетов в сети.

Существуют технологии сдерживания штормов кадров под обобщенным названием *Storm Control*. Команда, например, storm-control broadcast level 10

Параметр storm-control задаёт количество бродкастов в секунду. Всё, что свыше 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. Cisco Storm Control:



# 

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

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

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

Виды стэкирования:

1. ***Традиционное стекирование*** – посредством специальных разъемов как правило расположенных на задней панели
2. ***Стекирование посредством Ethernet-портов*** с высокой пропускной способностью расположенных на передней панели (distributed, horizontal, front panel stacking).
3. ***«Чисто» виртуальное стекирование*.**

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.

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

Согласно правилам хорошего тона, стековые порты следует соединять кольцом.

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

Учет номера позволяет обратиться к определенному порту определенного коммутатора. Если коммутатор является стекируемым, то номер включен в систему нумерации портов изначально (даже если по факту коммутатор не является членом стека). По умолчанию номер равен единице, может быть изменен командой:

switch ... renumber.

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

Номер может быть изменен как до, так и после начала членства коммутатора в стеке. Если номер не назначен вручную, то назначается автоматически: выбирается минимальный доступный. Если обнаружен конфликт номеров, то так же выбирается минимальный доступный. Изменение номера учитывается только после перезагрузки

Центром администрирования и управления стеком является один из коммутаторов -- *стек -мастер*. Системные настройки *стек -мастера* относятся ко всему стеку.

*Стек-мастер* выбирается автоматически исходя из приоритета (s*tack member priority*). По умолчанию приоритет равен единице, может быть изменен:

switch ... priority

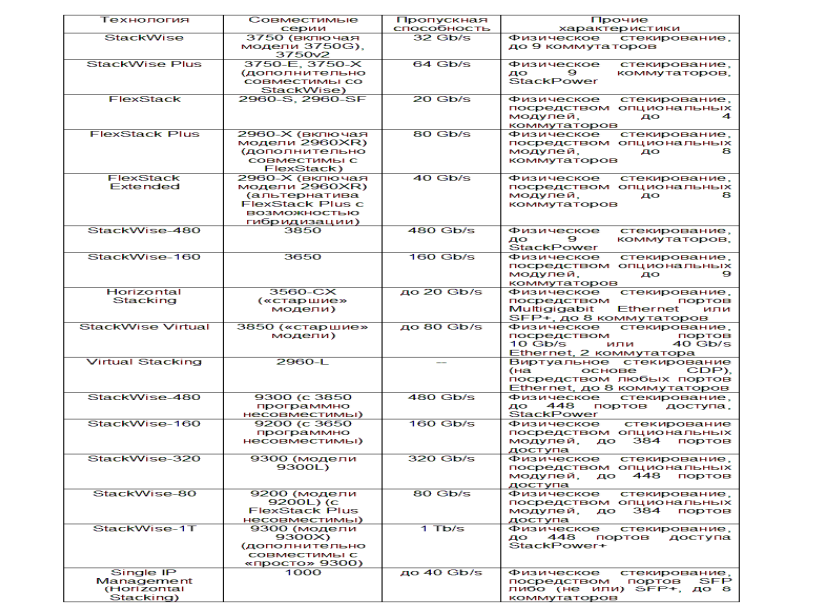
Приоритет задают числом от 1 до 15. Приоритет хранится в переменной окружения SWITCH\_PRIORITY. Изменение приоритета учитывается только при следующем выборе (перевыборе).

Рекомендуемый вариант назначения предпочтительного коммутатора *стек-мастером* -- это увеличение приоритета. *Стек-мастером* становится коммутатор с наибольшим цифровым значением приоритета. При равенстве приоритетов учитываются конфигурации портов. Выбирается коммутатор с конфигурацией портов, отличной от конфигурации портов по умолчанию. При наличии нескольких таковых коммутаторов учитываются лицензии. Выбирается коммутатор с самой «старшей» лицензией.

Ну и в последнюю очередь, учитываются MAC-адреса. Выбирается коммутатор с наименьшим MAC-адресом.

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

Технологии стэкирования циско – **StackWise (32gb), StackWise Plus(64gb), FlexStack(20gb), FlexStack Plus(80gb), FlexStack Extended(40gb), Horizontal Stacking(20gb)**:



# 

# 51 Конфигурирование стека коммутаторов в IOS

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

3750g(config)#switch 1 renumber 2

...

3750g(config)#switch 1 priority 15

...

3750g(config)#stack-mac persistent timer 0 !В минутах (0 -- бесконечность)

...

3750g(config)#interface gi2/0/1 !Номер коммутатора в стеке

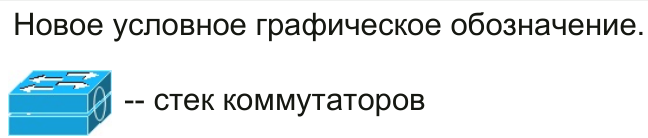
…

Для просмотра состояния стека используют команду:

show platform stack-manager all,

Для того или иного коммутатора в отношении стека:

show switch



# 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).

В настоящее время под аббревиатурой Wi-Fi понимают следующие

ключевые стандарты:



Стандарт *802.11a* - применяется схема модуляции сигнала - мультиплексирование с разделением по ортогональным частотам (*OFDM*). Три обязательные скорости передачи данных (6, 12 и 24 Мбит/с) и пять дополнительных (9, 18, 24, 48 и 54 Мбит/с). Также имеется возможность одновременного использования двух каналов, что повышает скорость передачи данных в 2 раза. Раб. диапазон 5 ггц.

Стандарт *802.11b* - основан на методе широкополосной модуляции с прямым расширением спектра (*DSSS*). Весь рабочий диапазон делится на 14 каналов, разнесенных на 25 МГц для исключения взаимных помех. Макс. теор. скорость передачи - 11 Мбит/с. Раб. диапазон 2.4 ггц.

Стандарт *802.11g* - является дальнейшим усовершенствованием спецификации IEEE 802.11b. Скорость передачи данных в радиоканале достигает 54 Мбит/с. Функционирует в диапазоне 2,4 ГГц (*OFDM*)

Стандарт *802.11n*. - Макс. теор. скорость передачи - 600 Мбит/с, применяя передачу данных сразу по четырём антеннам. По одной антенне – до 150 Мбит/с.

Устройства 802.11n функционируют в частотных диапазонах 2,4 – 2,5 или 5,0 ГГц. В основе стандарта IEEE 802.11n лежит технология OFDM-MIMO.

# 53 Физический уровень Wi-Fi

Очевидно, физический уровень Wi-Fi устроен сложно.

В отличие от Ethernet, переход от канального уровня к физическому

предполагает дополнительную инкапсуляцию и заключается в том, что *CSMA/CA* (равно *DCF*) задействует **PLCP** (**Physical Layer Convergence Protocol**).

При этом **MPDUs - MAC Protocol Data Unit**s (собственно кадры Wi-Fi)

вкладываются в **PPDUs (PLCP Protocol Data Units)** -- вкладываются как **PSDUs (PLCP Service Data Units)**.

Формат *PPDU* очень вариативен.

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

*PLCP*-преамбула состоит из предопределенных соответствующим образом модулируемых символов (symbols) разной длительности (коротких или длинных).

Начиная с 802.11n, поддерживается агрегация *PDUs*, причем в двух

формах: **A-MSDU (Aggregate MSDU - MAC Service Data Units)** -- опциональное слияние *MSDUs* с одинаковыми адресами *RA* и *TA*, и **A-MPDU (Aggregate MPDU)** – слияние *MPDUs*.

В *PLCP*-заголовке содержатся специальные поля, описывающие процесс передачи *PSDU*. В процессе передачи *PPDU*, для лучшего разделения модулируемых символов, «проскальзывают» защитные интервалы (guard intervals, не путать с межкадровыми). Необходимость «выравнивания» составляющих *PPDU* (в том числе разнородных) обуславливает наличие различных хвостовиков (tails, речь не о хвостовиках кадров), наполнителей и расширителей

Начиная с *802.11ax,* поддерживается динамическая фрагментация *MSDU (A-MSDU*), то есть кроме фрагментов одинаковой длины (исключая последний), допускаются фрагменты разной длины.

Агрегация и фрагментация, а также моделируемые символы и защитные интервалы разной длительности позволяют повысить гибкость (адаптируемость к условиям передачи).

Таким образом, используют четыре частотные области (bands): 2,4, 5, 6 и 60 GHz. Области 2,4 и 5 GHz известны как **ISM (Industrial, Scientific and Medical)** и U-NII (Unlicensed National Information Infrastructure) соответственно (законодательство США) и освоены в первую очередь. В области 5 GHz четко выражены три поддиапазона (sub-bands).

# 54 Каналы Wi-Fi

Базовый алгоритм Wi-Fi предполагает использование в качестве канала одной более или менее узкой полосы частот.

Каналы могут быть шириной примерно 20, 40, 80 и 160 MHz. Так же допустимы каналы, сформированные из пар несмежных каналов шириной 80 MHz. «Распараллеливание» реализуют не одновременным использованием нескольких каналов (с канальным перемежением и фрагментацией), 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).

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

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

Наличие поднесущих, на следующем шаге развития, позволяет по-своему повысить гибкость. Так, по правилам модуляции *OFDMA* из поднесущих разрешено формировать так называемые блоки ресурсов – чтобы ресурсы канала можно было динамически распределять для обеспечения «параллельного» взаимодействия более чем двух устройств

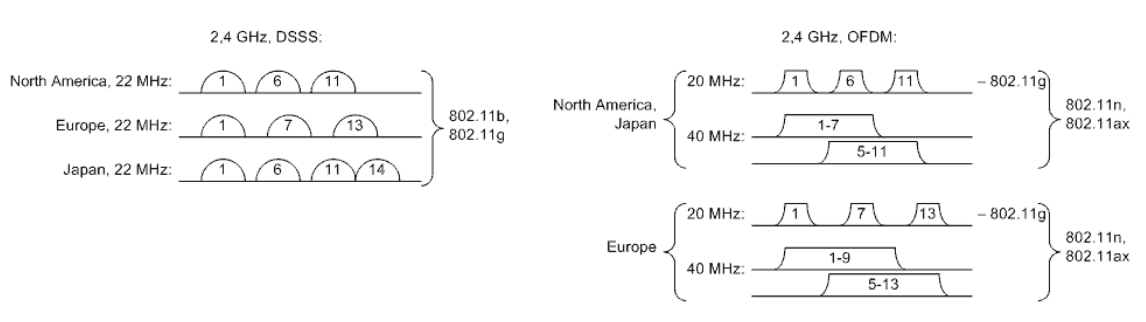
Наборы каналов вариативны, так как на использование тех или иных каналов в разных странах наложены свои ограничения.

Допустимо перекрытие каналов, что актуально в отношении сложно организованных и конфликтующих беспроводных сегментов. Но на практике перекрытие каналов порождает проблемы, поэтому его следует избегать.

Каналы 802.11b:



Каналы в области 2.4 GHz:



При изготовлении беспроводного оборудования производители закладывают (на аппаратном уровне) поддержку целевого региона (regulatory domain). Изначально выделяли североамериканский (FCC), европейский (ETSI) и японский (TELEC) регионы. Остальные страны примыкали к североамериканскому либо европейскому. Это по -прежнему основные регионы. По мере освоения новых частот возникает все большее разнообразие и список регионов расширяется. В частности, с появлением 802.11ac для США ввели альтернативный регион (с большим количеством каналов), и ввели глобальный регион. В настоящее время, формально, Беларусь отнесена к израильскому региону (в отличие от всех остальных стран Европы). Подключаемое беспроводное устройство согласует регион с помощью управляющих кадров со специальным информационным элементом в поле данных.

# 55 Модуляция и кодирование в рамках Wi-Fi

В стандартах 802.11 описан ряд способов модуляции и кодирования:

1. **PPM (Pulse Position Modulation)** -- модуляция позициями импульсов (изначально в 802.11, для IR).

2. **FHSS (Frequency Hopping Spread Spectrum)** -- широкополосная модуляция со скачкообразным изменением частоты (изначально в 802.11, для 2,4 GHz).

3. **DSSS (Direct Sequence Spread Spectrum)** -- широкополосная модуляция с прямым расширением спектра.

4. **BPSK (Binary Phase Shift Keying)** и **QPSK (Quadrature Phase Shift Keying)** -- соответственно двоичное и квадратичное манипулирование фазовыми сдвигами.

5. **DBPSK (Differential BPSK)** и **DQPSK (Differential QPSK)** – дифференциальные варианты *BPSK* и *QPSK*.

6 **SQPSK (Spread QPSK)** -- раздвоенный вариант *QPSK*.

7. **CCK (Complementary Code Keying)** -- манипулирование дополнительными кодами.

8. **BCC (Binary Convolutional Coding)** -- двоичное сверточное кодирование.

9. **PBCC (Packet Binary Convolutional Coding)** -- пакетный вариант BCC.

10. **OFDM (Orthogonal Frequency Division Multiplexing)** – мультиплексирование c ортогональным частотным разделением.

+11. **OFDMA (Orthogonal Frequency Division Multiple Access)** – множественный доступ c ортогональным частотным разделением.

12. **QAM (Quadrature Amplitude Modulation)** -- квадратурная амплитудная модуляция.

13. **MIMO (Multiple Input, Multiple Output)** -- множественный ввод-вывод(с использованием нескольких антенн).

+14. **SU-MIMO (Single-User MIMO)** -- однопользовательский вариант MIMO.

+15. **MU-MIMO (Multi-User MIMO)** -- многопользовательский вариант MIMO.

16. **LDPC (Low-Density Parity Check)** -- низкоплотная проверка паритета.

17. **DMG Control** -- контроль DMG (контроль в особом режиме называемом DMG).

18. **SC (Single Carrier)** -- использование одной несущей.

И некоторые другие.

Физическая модуляция сильно переплетена с канальным кодированием в отношении PPDU.

Канальное кодирование может быть как проявлением модуляции, так и дополнительным преобразованием данных.

Модуляция может быть многоуровневой (например, в связке с OFDM, к отдельно взятой поднесущей может применяться QAM).

И канальное кодирование может быть многоуровневым (например, LDPC всегда предшествует простейшее «перемешивание» -- scrambling -- с целью равномерного распределения нулей и единиц).

Поддержка той или иной модуляции (кодирования) может быть как обязательной, так и опциональной.

С учетом совместимости, модуляция (кодирование) автоматически подбирается в зависимости от требующейся скорости. В рамках одного стандарта, одни и те же каналы могут использоваться по-разному. 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 (но не сам канальный код -- другой параметр). Поскольку используются избыточные (в англоязычной терминологии FEC -- Forward Error Correction) канальные коды, изменение коэффициента избыточности (coding rate) приводит к изменению скорости.

# 56 Стандарты беспроводной связи, кроме Wi-Fi

Следует упомянуть и прочие стандарты беспроводной пересылки данных на различные расстояния с различной скоростью.

Но прежде нужно отметить, что кроме WLAN еще выделяют WWANs (Wireless Wide Area Networks), WMANs (Wireless Metropolian Area Network), WPANs (Wireless Personal Area Networks) и другие беспроводные сети.

Теперь стандарты:

1. **Satellite broadband** -- спутниковая связь; LMDS и MMDS; скорость ориентировочно до 10 Mbit/s.

2. **Cellular broadband** -- мобильная связь; поддержка доступна начиная со второго поколения мобильных телефонов (2G); 2G: GSM, CDMA и TDMA; 3G: EDGE, CDMA2000, HSPA+, UMTS; 4G: WiMAX и LTE; 5G (пока много вопросов).

3. **WiMAX** (Worldwide Interoperability for Microwave Access) -- для городских и глобальных сетей; 802.16; расстояние до 50 km; скорость до 1 Gbit/s.

4. **Bluetooth** -- для персональных сетей; 802.15; три версии; расстояние (v3) до 100 m (long range), до 10 m (ordinary range), до 10 cm (short range); скорость (v3) до 24 Mbit/s.

5. **NFC** (Near-Field Communication) -- для широкого применения на очень коротких расстояниях; до 10 cm; скорость до 0,5 Mbit/s.

И другие: HomeRF, Wireless 1394, xG, ...

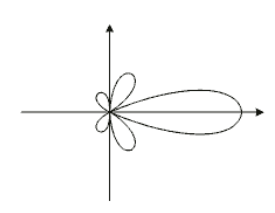
# 57 Антенны для беспроводного сетевого оборудования и сопутствующие расчеты

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

Например, применительно к SOHO, очень часто используют антенны Single Detachable Reverse SMA.

Антенна излучает энергию во всех направлениях, но неравномерно.

Основным параметром, определяющим эффективность антенны в

определенном направлении является диаграмма направленности -- зависимость мощности излучения от пространственных координат.

Направленная параболическая антенна обеспечивает усиление сигнала:

G = 4πA / λ2 , 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 + 20lg (F) + 20lg (D) , dB,

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

Типичный Wi-Fi-передатчик имеет мощность около 20 dBm (≈ 200 mW) на всех используемых частотах, типичный приемник имеет чувствительность около -80 dBm (0,00000001 mW). Это обеспечивает запас по затуханию около 100 dB.

Типичная Wi-Fi-антенна дает дополнительное усиление до 6 dBi (если антенна подключена через кабель, то и в кабеле возникает небольшое затухание). При применении Wi-Fi по назначению (мощность передатчиков ограничена стандартами) этого вполне достаточно. При расчетах нужно также учитывать, что просто размещение подключаемого мобильного устройства относительно антенны уже может дать затухание около 5 dB.

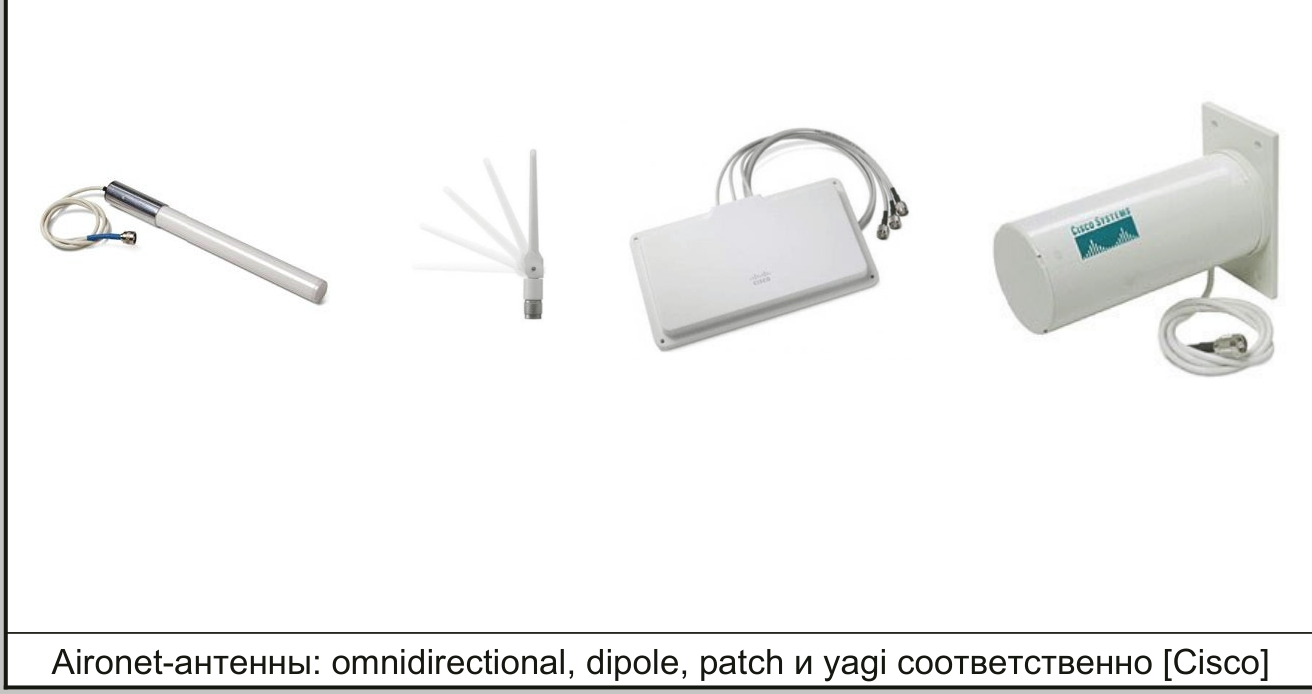
Еще одна серьезная проблема заключается в интерференции волн от

разных передатчиков, особенно если априори необходимо обеспечить

сплошное покрытие.

Кроме использования разных частот, весьма действенным способом

борьбы с интерференцией является использование направленных антенн (beamforming).



# 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).

Некоторые могут работать и в том, и в другом режиме.

WLCs позиционируют как средство для облегчения администрирования при массовом использовании точек доступа. Попытки стандартизировать проприетарный протокол Cisco для взаимодействия между точками доступа и WLCs сначала привели к созданию LWAPP (LightWeight Access Point Protocol) (RFC 5412), который в настоящее время считают устаревшим. Позже, статус официального стандарта был придан расширению LWAPP под названием CAPWAP (Control And Provisioning of Wireless Access Points) (RFC 5415), но и оно пока не приобрело широкую поддержку у производителей.

Более того, касательно SOHO, тенденции интеграции (например, поддержка USB) уже привели к возникновению еще одного типа оборудования -- медиацентров (media centers). Существующие медиацентры сочетают ряд функций: access point, router, media player и другие.

# 59 Структура беспроводной сети

Топологически, в основу беспроводных сетей (не только Wi-Fi) положена так называемая ***сотовая структура***.

В общем случае предполагают наличие точек доступа – режим инфраструктуры (infrastructure).

СПД может состоять из одной либо нескольких *сот (cells)*. Каждая сота управляется персональной точкой доступа.

Точка доступа и ассоциированные с ней беспроводные пользовательские устройства образуют базовую зону обслуживания -- ***BSS (Basic Service Set)***.

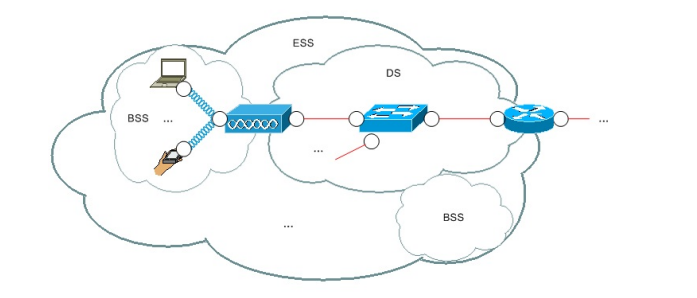
Точки доступа многосотовой сети взаимодействуют между собой посредством распределенной системы -- ***DS (Distribution System)*.**

DS -- это обычная проводная инфраструктура второго уровня (наполнение стандартами не регламентировано).

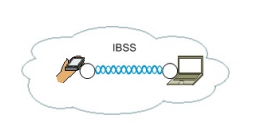
Совокупность BSSes и DS образует расширенную зону обслуживания – ESS.

Для обеспечения возможности перемещения мобильных беспроводных пользовательских устройств из одних сот в другие предусмотрен роуминг (roaming, mobility -- в терминологии Cisco).

Таким образом, ESS -- представляет собой отдельную сущность беспроводного сегмента (в общем случае, устроенного сложно).

****

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



Отдельно взятые ESAs и BSAs идентифицируют с помощью SSIDs (Service Set IDentifiers) длиной до 32 байтов (набор недопустимых символов зависит от конкретной реализации).

От SSID (иногда называют ESSID) следует отличать BSSID.

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

SSID вкладывается в поле данных при формировании управляющего кадра как один из информационных элементов.

BSSID используется как один из четырех адресов в кадре Wi-Fi.

# 

# 60 Идентификация и виланы в беспроводных сетях

Отдельно взятые ESAs и BSAs *идентифицируют* с помощью SSIDs (Service Set IDentifiers) длиной до 32 байтов (набор недопустимых символов зависит от конкретной реализации).

От SSID (иногда называют ESSID) следует отличать BSSID.

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

SSID вкладывается в поле данных при формировании управляющего кадра как один из информационных элементов.

BSSID используется как один из четырех адресов в кадре Wi-Fi

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

Беспроводные виланы представлены различными SSIDs, сосуществующими в рамках одной ESS (иногда приравнивают к multiple SSIDs).

При рассмотрении классического порта доступа подразумевают, что стационарная пользовательская станция имеет доступ только к одному физическому порту, однако «спрятать» от мобильной пользовательской станции доступные SSIDs невозможно.

Точка доступа должна ставить в соответствие беспроводные виланы

(SSIDs) проводным (VIDs), следовательно, должна работать в режиме моста.

Для управления самой точкой доступа создают административный вилан.

Вне административного вилана может быть создан отдельный вилан,

посредством которого легковесная точка доступа взаимодействует с WLC.

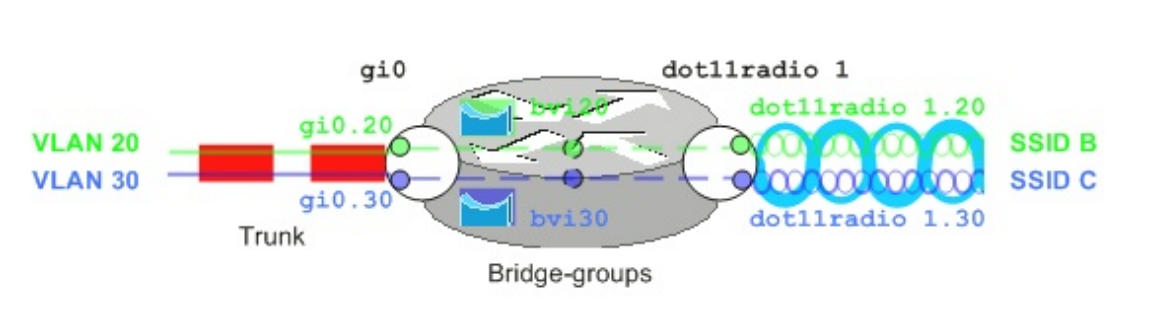
Расширения виланов 802.1X также применимы, в том числе для

динамического включения пользователей в виланы.

Для обеспечения защиты информации предусмотрен комплекс мер,

отчасти выраженный в WEP (Wired Equivalent Privacy) и WPA (Wi-Fi Protected

Access).



# 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). В квадрате со стороной 20 метров или в круге радиусом 15.

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).

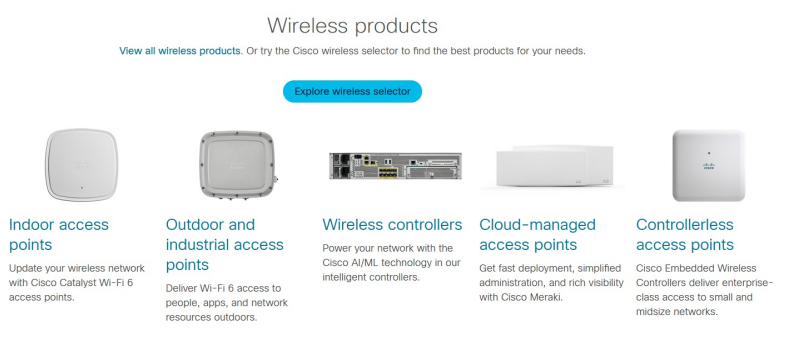
8. Настроить дополнительные сетевые сервисы на точках доступа (обычно DHCP или NAT).

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 категорий: Indoor access points, Outdoor and Industrial access points, Wireless controllers, Cloud-managed access points, controllers access points.



Приблизительно в 2000 году, в результате приобретения компании

Aironet, Cisco начала производство точек доступа enterprise/industrial -- под

торговой маркой Aironet, и постепенно нарастила номенклатуру изделий.

С 2003 по 2013 год Cisco владела компанией Linksys (торговая марка

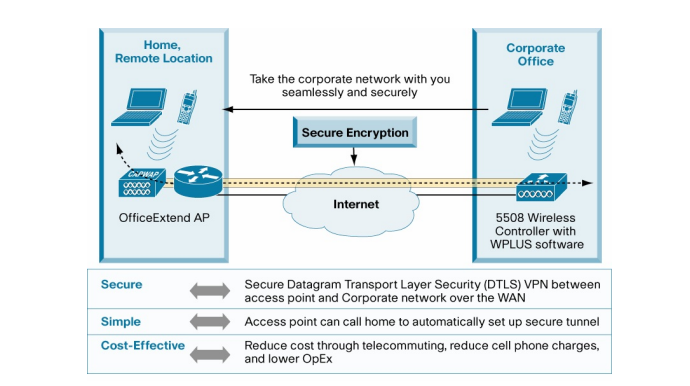
Linksys by Cisco), которой была отведена «львиная доля» направления SOHO/SMB. С 2010 года Cisco представлена своими моделями этого направления.

C 2005 года Cisco выпускает легковесные точки доступа и WLCs.

# 63 Беспроводные технологии Cisco

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

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



Несколько особняком стоит оригинальная технология **Cisco Wireless Mesh**, позволяющая без усилий строить на базе расставленных в outdoor-окружении специальных точек доступа полнофункциональную сеть с произвольной физической топологией, динамически формировать каналы, находить ближайший WLC, оптимизировать трафик (своеобразная динамическая маршрутизация).

Для этих целей разработан новый протокол -- **AWPP (Adaptive Wireless Path Protocol**).

Все вышеперечисленное «собрано» в архитектуру Cisco Unified Wireless Network, состоящую из пяти основных компонентов.

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.

В настоящее время наибольший интерес представляют точки доступа серий: 1130AG (802.11a, 802.11g) (по -прежнему); 2600 (802.11n); 1850 и 2800 (802.11ac Wave 2); 9120 (802.11ax).

Большинство моделей доступны в нескольких исполнениях: автономном (как вариант, с интегрированным WLC) либо легковесном, с внутренними либо внешними антеннами (challenging environment).

Наиболее актуальные серии WLCs: 2500, 5500; 3500, 9800. Программа CCNA пока еще ориентирована на точки доступа Linksys (подходят любые, так как web-интерфейс аналогичен).

# 64 Конфигурирование беспроводного маршрутизатора Linksys

Вот общий гайд по настройке беспроводного маршрутизатора Linksys:

***Шаг 1: Подключение к маршрутизатору***

Подключите компьютер к беспроводному маршрутизатору Linksys с использованием Ethernet-кабеля или подключитесь через Wi-Fi. Затем откройте веб-браузер и введите IP-адрес маршрутизатора в адресной строке. Обычно, IP-адрес по умолчанию для маршрутизаторов Linksys – 192.168.1.1. Проверьте документацию к вашему устройству.

***Шаг 2: Вход в панель управления маршрутизатора***

Вас попросят ввести имя пользователя и пароль. Если вы не меняли эти данные, используйте значения по умолчанию. Обычно, для Linksys это "admin" в обоих полях. Но, опять же, проверьте документацию.

***Шаг 3: Настройка основных параметров***

Внутри панели управления вы найдете различные вкладки и настройки. Вот несколько основных шагов:

Настройка беспроводной сети (Wi-Fi): Перейдите в раздел "Wireless" или "Wi-Fi", где вы сможете изменить имя сети (SSID), метод безопасности (например, WPA2), и установить пароль.

Настройка пароля для входа в маршрутизатор: В разделе "Administration" или "Management" вы можете изменить пароль для доступа к панели управления маршрутизатора.

Обновление программного обеспечения (Firmware): Проверьте раздел "Firmware" или "Software Update" и убедитесь, что ваш маршрутизатор использует последнюю версию программного обеспечения.

***Шаг 4: Настройка других параметров (опционально)***

В зависимости от ваших потребностей, вы также можете настроить другие параметры, такие как фильтрация MAC-адресов, настройка портов, включение гостевой сети и др.

***Шаг 5: Сохранение изменений***

После внесения всех изменений, не забудьте сохранить их, обычно это делается с помощью кнопки "Save" или "Apply".

***Шаг 6: Перезагрузка маршрутизатора***

После сохранения изменений, возможно, потребуется перезагрузить маршрутизатор для применения настроек

# 

# 65 Интеграция компьютерных сетей в системы связи

КС переплетаются с традиционной связной инфраструктурой, при этом выделяют два направления интеграции:

1. КС интегрируют в системы связи.

2. Системы связи интегрируют в КС.

Для передачи обычных голосовых сообщений, а также компьютерной информации, используют стандартный так называемый канал тональной частоты.

В свое время, для передачи речи была установлена полоса частот 300 -- 3400 Hz, что соответствует девяностопроцентному уровню разборчивости.

В системах аналоговой связи применяют мультиплексирование с частотным разделением каналов -- Frequency Division Multiplexing (FDM). Каждый телефонный сигнал в результирующем объединенном сигнале занимает полосу частот 4 kHz.

На базе ТЧ-каналов формируют так называемые групповые тракты:

* первичный К-12 (12 ТЧ-каналов, 60 -- 180 kHz),
* вторичный К-60 (60 ТЧ-каналов, 312 -- 552 kHz),
* третичный К-300 (300 ТЧ-каналов, 812 – 2044 kHz)
* другие (более или менее стандартизированные).

# 66 Структура и синхронизация цифровых сетевых интерфейсов

В случае цифровой связи, для преобразования аналоговых сигналов в цифровые применяют импульсно-кодовую модуляцию (ИКМ) -- Pulse Code Modulation (PCM).

При этом, частота дискретизации равна 8 kHz, а разрядность равна 8.

Следовательно, для формирования ТЧ-канала необходима пропускная способность 64 kbit/s. Таковой канал называют основным цифровым каналом -- Digital Signal level 0 (DS0).

Именно на базе DS0 построена иерархия цифровой связи.

При этом, применяют мультиплексирование с временны'м разделением каналов -- Time Division Multiplexing (TDM).

Непрерывную последовательность битов в смешанном после мультиплексирования потоке, которая относится к определенному цифровому каналу до мультиплексирования, называют тайм-слотом (timeslot).

Возможны два принципиально разных типа TDMs:

1. Синхронные -- время формирования тайм-слотов четко связано с тактированием и предопределено.

2. Асинхронные -- тайм-слоты формируются по мере надобности.

Главным аспектом является согласованность работы связанных мультиплексоров. Нужно учитывать два обстоятельства:

-- источники синхронизации могут быть локальными и глобальными, причем в отношении как отдельных мультиплексоров, так и выделенных групп;

-- элементы синхронизации включаются и в передаваемые кадры.

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.

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.

# 67 Плезиохронная и псевдосинхронная цифровая иерархия

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

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

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

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

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

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). «Выравнивание» на более высоких уровнях иерархии еще больше «запутывает» данные и делает невозможным их прямое извлечение.

Для реализаций последних двух режимов характерно наличие

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

Плезиохронная цифровая иерархия -- PDH (Plesiochronous Digital Hierarchy) -- уже описана выше (G.704). PDH базируется на электрических средах (G.703). Воплощениями псевдосинхронной цифровой иерархии стали SONET (Synchronous Optical NETwork) (Telcordia GR-253-CORE, ATIS 0900105.06) в Северной Америке и SDH (Synchronous Digital Hierarchy) (G.783) в Европе. Как SONET, так и SDH могут базироваться на электрических -- Electrical Signaling (ES) и оптических -- Optical Signaling (OS) средах (SONET: те же стандарты Telcordia и ATIS, SDH: G.703 и G.957). В качестве первичных цифровых каналов приняты Optical Carrier level 1 (OC-1), Synchronous Transport Signal level 1 (STS-1) и Synchronous Transport Module level 1 (STM-1). Применение коэффициентов кратности дает соответствующий ряд скоростей.

# 68 Абонентское и провайдерское оборудование

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

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

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

Зоны ответственности абонента и провайдера разграничивает *демаркационная линия*. 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, в первую очередь, различные модемы, различные телефонные аппараты и офисные АТС. Хотя на стороне абонента может быть и достаточно сложная инфраструктура.

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

# 69 Последовательные сетевые интерфейсы

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

Основные моменты, связанные с последовательными интерфейсами:

-- в стандартах четко разделены роли DCE и DTE;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# 70 Протокол PPP и смежные протоколы

РРР -- это очень гибкий протокол второго уровня, который позволяет

устанавливать канальное point-to-point-соединение. Затем это соединение может использоваться практически любыми протоколами третьего уровня, причем «одновременно» (SLIP поддерживает только IP).

Над PPP концентрируется очень большое количество протоколов.

Из четырех групп можно выделить две основные:

1. LCPs (Link-layer Control Protocols).

2. NCPs (Network Control Protocols).

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

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

Работа LCP базируется на механизме запросов-подтверждений.

Набор NCPs позволяет адаптировать подготовленное соединение к

нуждам протоколов третьего уровня и включает: IPCP (IP Control Protocol),

IPv6CP, IPXCP, CCP (Compression CP) и так далее.

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

PPP поддерживает два алгоритма аутентификации на канальном уровне:

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

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

Еще две серьезные возможности PPP:

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

2. Bridging -- поддержка мостов.

# 71 Конфигурирование последовательных сетевых интерфейсов в IOS

Пример настройки последовательного сетевого интерфейса

маршрутизатора Cisco (по умолчанию считается DTE):

Router(config)#interface se0/0/0

Router(config-if)#clock rate 64000

Router(config-if)#encapsulation ppp

Router(config-if)#ppp multilink

Router(config-if)#exit

Пример настройки PAP-аутентификации между двумя маршрутизаторами:

R1(config)#username router2 password cisco

R1(config)#interface se0/0/1

R1(config-if)#encapsulation ppp

R1(config-if)#ppp authentication pap

R1(config-if)#exit

R2(config)#interface se0/0/0

R2(config-if)#encapsulation ppp

R2(config-if)#ppp pap sent-username router2 password cisco

R2(config-if)#exit

Пример настройки CHAP-аутентификации между двумя маршрутизаторами:

R1(config)#username R2 password cisco

R1(config)#interface se0/1/0

R1(config-if)#encapsulation ppp

R1(config-if)#ppp authentication chap

R1(config-if)#exit

R2(config)#username R1 password cisco

R2(config)#interface se0/1/1

R2(config-if)#encapsulation ppp

R2(config-if)#ppp authentication chap

R2(config-if)#exit

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

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

Dial-up ограниченно применяют до сих пор.

Традиционные модемы используют сложившуюся телефонную

инфраструктуру и соответственно ту же полосу частот, что и телефоны (0 -- 4 kHz).

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

Посредником является то, что в настоящее время принято называть

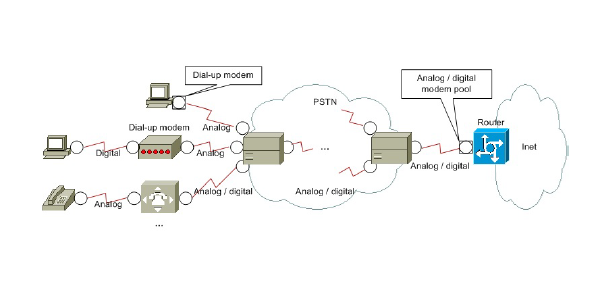
традиционной телефонной сетью общего пользования -- PSTN (Public Switched Telephone Network) или, по-другому, POTS (Plain Old Telephone Service). PSTN охватывает сеть возможно разных АТС (лучше telephone exchanges).

В настоящее время почти все ATC цифровые и применяют основном

цифровые модемные пулы.

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

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



Технология Dial-up прошла много стадий развития, начиная со стандарта

V.21.

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

# 73 Обзор технологии ISDN и структура ISDN-домена

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

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

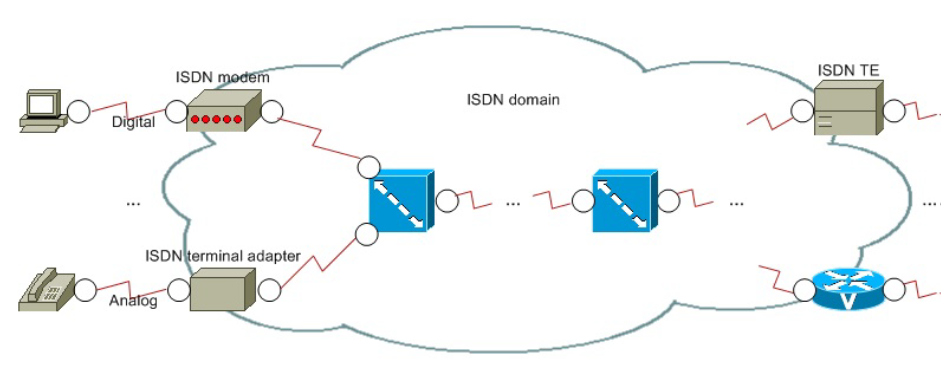
В архитектуре и структуре ISDN-домена выделяют четыре плана (control, management, transport, user), для каждого из которых предусмотрены набор интерфейсов и набор устройств.

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.

Недостаточно сильная стандартизация процесса сигнализации привела к несовместимости оборудования и возникновению трех разных основных типов ISDN- коммутаторов. Проблема несовместимости в США была решена внедрением стандарта National ISDN.



# 74 Обзор технологии ATM и структура ATM-домена

Технология ATM уходит корнями в B-ISDN. ATM условно относят к технологиям коммутации пакетов.

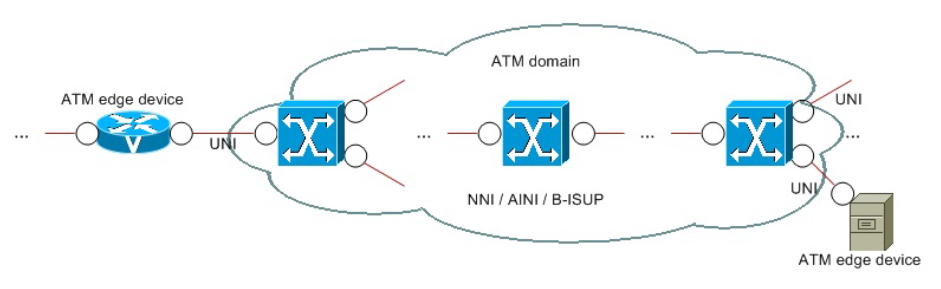
Серьезными достоинствами ATM являются заложенные поддержка качества обслуживания разнородного трафика и ориентированность на соединение. ATM обеспечивает скорость до 40 Gbit/s и больше.

ATM-домен состоит из некоторого количества объединенных ATM-коммутаторов и подключенных к ним граничных АТМ-устройств.

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

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

Для обеспечения возможности создания SVCs (динамическая виртуальная цепь) со стороны граничных ATM-устройств используется специальный механизм - сигнализация. Для обеспечения сигнализации создают сигнализационную PVC (постоянная), валидную в пределах VP.



# 75 Примеры инкапсуляции в ATM-системе

Применительно к ATM, канальный уровень имеет очень сложную структуру.

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

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

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

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

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

Примером инкапсуляции является

AAL (ATM Adaptation Layer — уровень адаптации ATM) — правила, определяющие способ подготовки информации для передачи по сети ATM. Один из уровней ATM.

Задача AAL — разбиение потока данных на ATM-ячейки и обратная сборка при приеме.

AAL1 - Передача голоса

AAL2 - Передача видео

AAL3 - Передача данных

AAL4 - Работа с IP сетью

AAL5 - сигнальная информация IP over ATM, Ethernet over ATM

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

На граничном ATM-устройстве, поступающие с третьего уровня пакеты могут использовать ATM не только напрямую (native), а и посредством эмуляции MAC-уровня LAN -- LANE (LAN Emulation). В любом случае, используется многопротокольная инкапсуляция по правилам RFC 2684 (усовершенствование RFC 1483), которая бывает двух видов: LLC (Logical Link Control) и SNAP (Subnetwork Access Protocol). В результате, пакеты разных L3-протоколов могут пересылаться по одной виртуальной цепи.

Пример создания двух PVCs со статическим связыванием на маршрутизаторе Cisco для взаимодействия с двумя другими маршрутизаторами.

Router(config)#interface atm1/0

Router(config-if)#ip address 192.168.0.1 255.255.255.0

Router(config-if)#atm pvc 2 0 200 aal5snap

Router(config-if)#atm pvc 3 0 300 aal5snap

Router(config-if)#map-group ATM-PVC-MAP1

Router(config-if)#exit

Router(config)#map-list ATM-PVC-MAP1

Router(config-map-list)#ip 192.168.0.2 atm-vc 2 broadcast

Router(config-map-list)#ip 192.168.0.3 atm-vc 3 broadcast

Router(config-map-list)#exit

Router(config-if)#pvc ISP 0/400

Router(config-if-atm-vc)# ...

Router(config)#interface atm1/0.1 multipoint

Router(config-subif)# ...

Пример включения InARP.

Router(config)#interface atm1/0

Router(config-if)#ip address 192.168.0.1 255.255.255.0

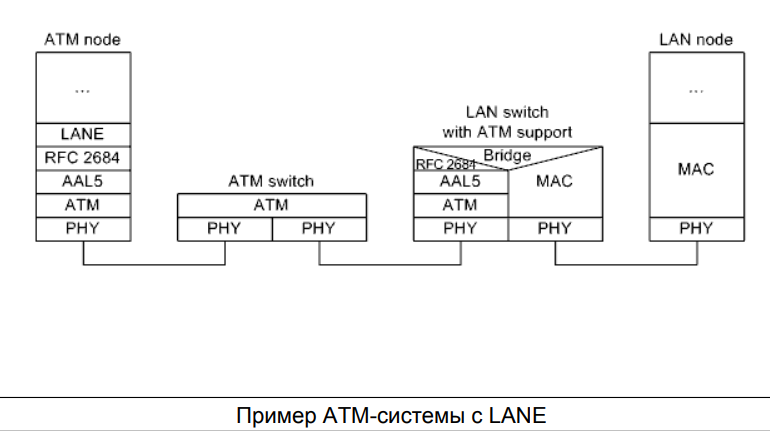
Router(config-if)#atm pvc 2 0 200 aal5snap inarp 5

Router(config-if)#atm pvc 3 0 300 aal5snap inarp 5

Router(config-if)#exit

# 75 Примеры инкапсуляции в ATM-системе

Услугами ATM могут пользоваться самые разные приложения, взаимодействующие по разным семействам протоколов. На граничном ATM-устройстве, поступающие с третьего уровня пакеты могут использовать ATM не только напрямую (native), а и посредством эмуляции MAC-уровня LAN -- LANE (LAN Emulation). В любом случае, используется многопротокольная инкапсуляция по правилам RFC 2684 (усовершенствование RFC 1483), которая бывает двух видов: LLC (Logical Link Control) и SNAP (Subnetwork Access Protocol). В результате, пакеты разных L3-протоколов могут пересылаться по одной виртуальной цепи.



# 

# 76 Семейство стандартов xDSL

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

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

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

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

В настоящее время семейство стандартов xDSL включает:

1. HDSL.

2. SDSL.

3. SHDSL.

4. SHDL.

5. ADSL.

6. ADSL2.

7. ADSL2+.

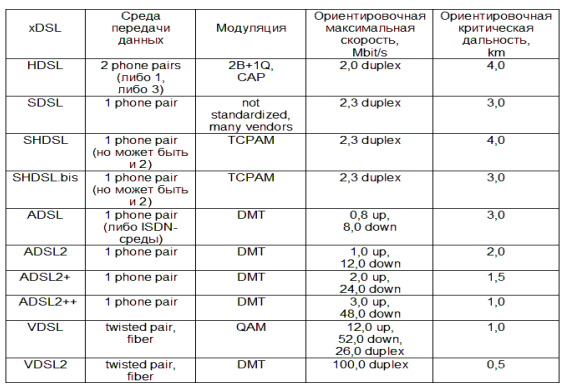
8. ADSL2++.

9. VDSL.

10. VDSL2.

Можно упомянуть недостаточно стандартизированные и уже неактуальные технологии: IDSL (ISDN DSL), RADSL (Rate Adaptive DSL), CDSL (Consumer DSL) и другие.

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) -- нетребующая наличия несущей амплитудно-фазовая.

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

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

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

Скорость, хоть и в разной степени, но всегда зависит от расстояния, которое в любом случае не превышает несколько километров

Под критической дальностью в таблице понимается расстояние, на котором происходит резкое ухудшение показателей.

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 (аsymmetric) каналов

-- исходя из двух взаимосвязанных характеристик: частоты канала и возможности задействовать канал в определенном направлении).

Таким образом, можно говорить о трех устоявшихся группах технологий:

ADSL (асимметричные), SHDSL (симметричные) и VDSL (гибридные). Но явно доминируют именно ADSL.

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

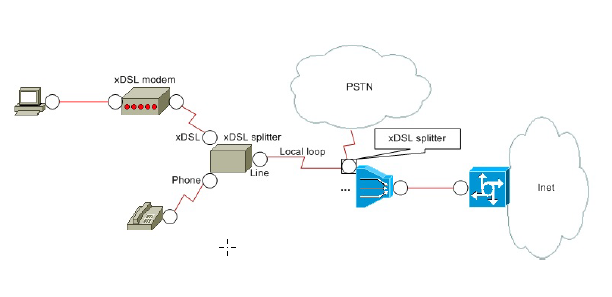
Часть каналов, расположенных в нижней области рабочей полосы частот, используется как upstream, оставшиеся -- как downstream.

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

# 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.



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

На стороне провайдера сплиттеры обычно встроены в DSLAM.

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

Может применяться даже L2-туннелирование через L3-СПД с помощью протокола L2TP (Layer 2 Tunneling Protocol).

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) (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 виланами.

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

# 

# 79 Примеры инкапсуляции в xDSL-системе

Пример настройки PPPoE-клиента.

Router(config)#interface dialer1

Router(config-if)#ip address negotiated

Router(config-if)#ip mtu 1492

Router(config-if)#ip virtual-reassembly

Router(config-if)#encapsulation ppp

Router(config-if)#dialer pool 1

...

Router(config)#interface fa0

Router(config-if)#no ip address

Router(config-if)#ip virtual-reassembly

Router(config-if)#pppoe-client dial-pool-number 1

...

Пример настройки PPPoE-сервера.

Router(config)#local pool EXAMPLE-PPPOE-POOL 192.168.0.2 192.168.0.254

...

Router(config)#interface virtual-vemplate1

Router(config-if)#ip address 192.168.0.1 255.255.255.0

Router(config-if)#ip virtual-reassembly

Router(config-if)#peer default ip address pool EXAMPLE–PPPOE-POOL

...

Router(config)#bba-group pppoe global

Router(config-bba-group)#virtual-template 1

Router(config-bba-group)#sessions max limit 100

Router(config-bba-group)#sessions per-mac limit 1

Router(config-bba-group)#sessions auto cleanup

...

Router(config)#interface fa0/0

Router(config-if)#no ip address

Router(config-if)#pppoe enable group global

...

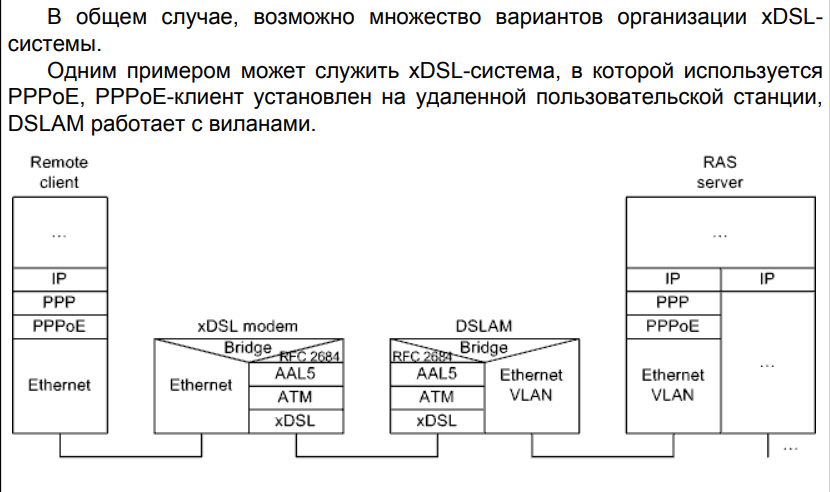
Router(config)#aaa new-model

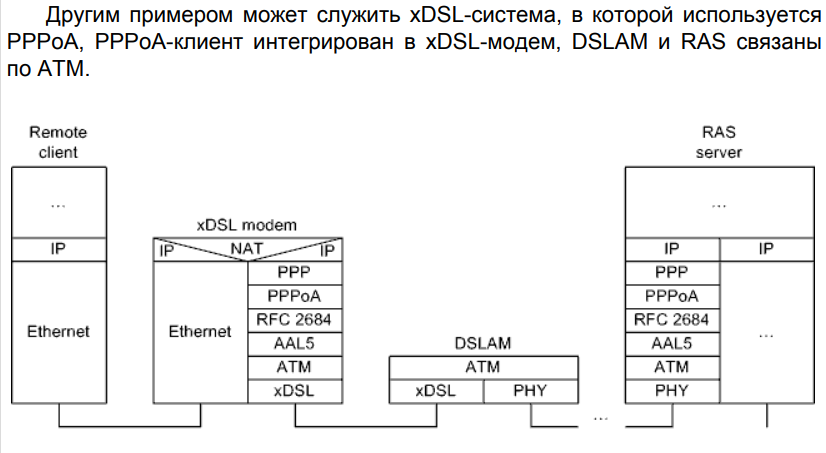
Router(config)#aaa authentication ppp default local

Router(config)#username user1@pppoe password 0 password1

...

# 79 Примеры инкапсуляции в xDSL-системе



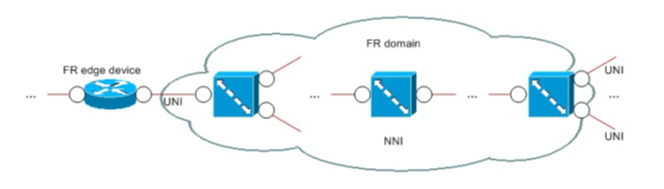


# 80 Обзор технологии FR и структура FR-домена

Технология FR (Frame Relay) произошла от X.25. FR условно относят к технологиям коммутации пакетов.

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

Поддерживаются как PVCs, так и SVCs.



VCs идентифицируют значимыми только в пределах физических каналов десятибитными идентификаторами DLCIs.

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

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

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

В пределах физического канала может существовать множество VCLs.

Каждый VCL, а следовательно и VC со стороны абонента,

идентифицируют парой:

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

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

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

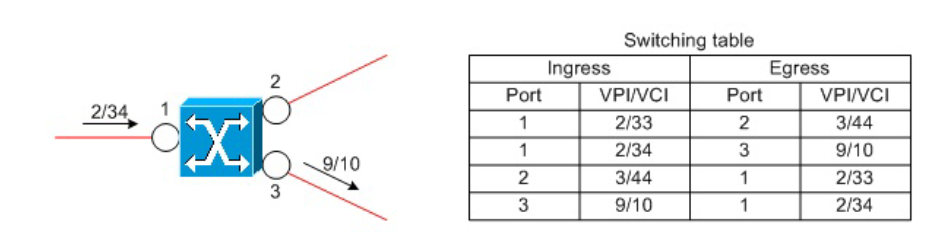
формируются ATM-коммутаторами динамически и автоматически.

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.

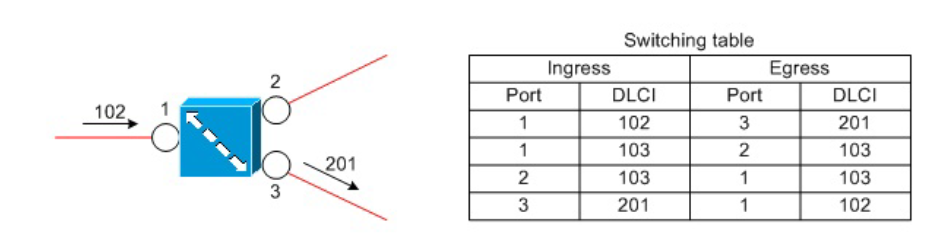


Таким образом, коммутация выполняется исходя из значения VPI/VCI в заголовке ячейки.

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

Значения VCI от 0 до 31 зарезервированы. Ячейки с нулевыми значениями VPI и VCI считаются пустыми

Принцип работы FR-коммутатора.



# 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 образу **SNMP(Simple Network Management Protocol)** и позволяет: определять состояние сетевого интерфейса, определять наличие PVCs, определять соответствие конфигураций непосредственно связанных устройств, собирать статистику; плюс расширить возможности мультикаст- и глобальной адресации.

ILMI базируется на периодическом обмене сообщениями (keepalives)(по умолчанию 5 сек).

За ILMI по умолчанию закреплена пара VPI/VCI равная 0/16 (можно переназначить).

В FR, так же как и в ATM, имеется LMI, точнее ELMI **(Enhanced LMI)**. Так же 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» -- задействуется DLCI = 1023.