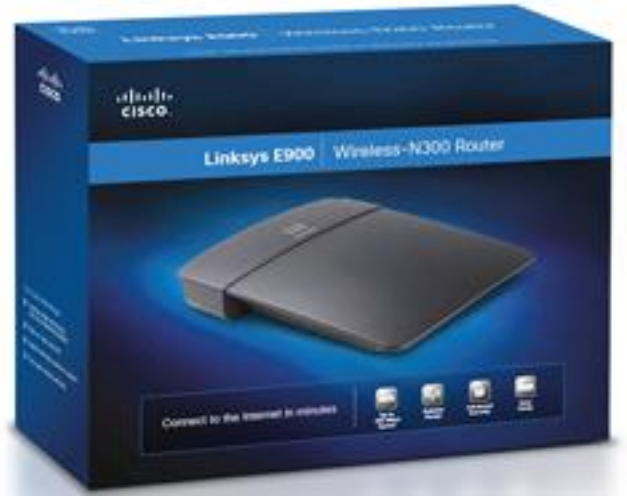
Приз за знания

Принимайте активное участие в Cisco Expo и получите в подарок Linksys E900.

Как получить подарок:

- внимательно слушать лекции по технологиям Cisco
- посещать демонстрации, включенные в основную программу
- пройти тесты на проверку знаний



Тесты будут открыты:

с 15:00 25 октября по 16:30 26 октября

www.ceq.com.ua

Cisco Expo 2012

Лучшие практики и рекомендуемые дизайны по построению LAN-сетей на базе возможностей оборудования Cisco

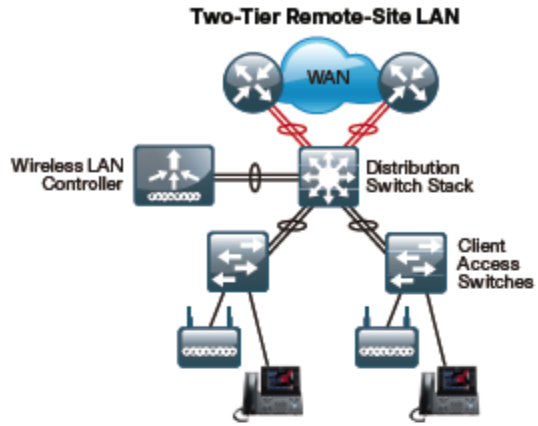
Максим Порицкий
системный инженер, CCIE R&S
mporitsk@cisco.com

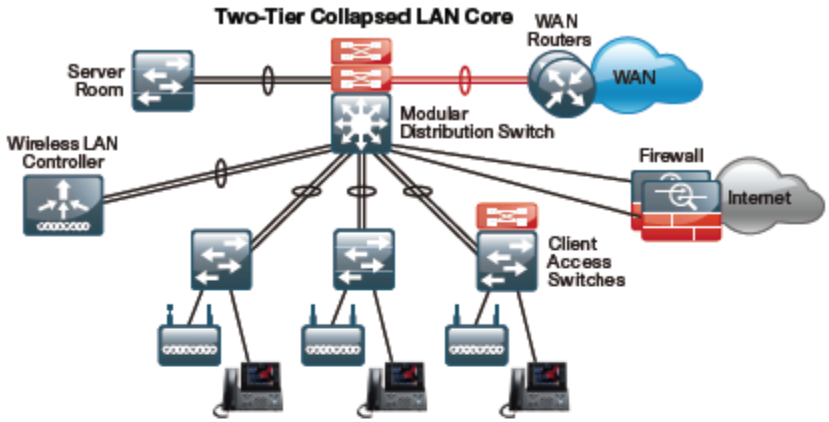
Содержание

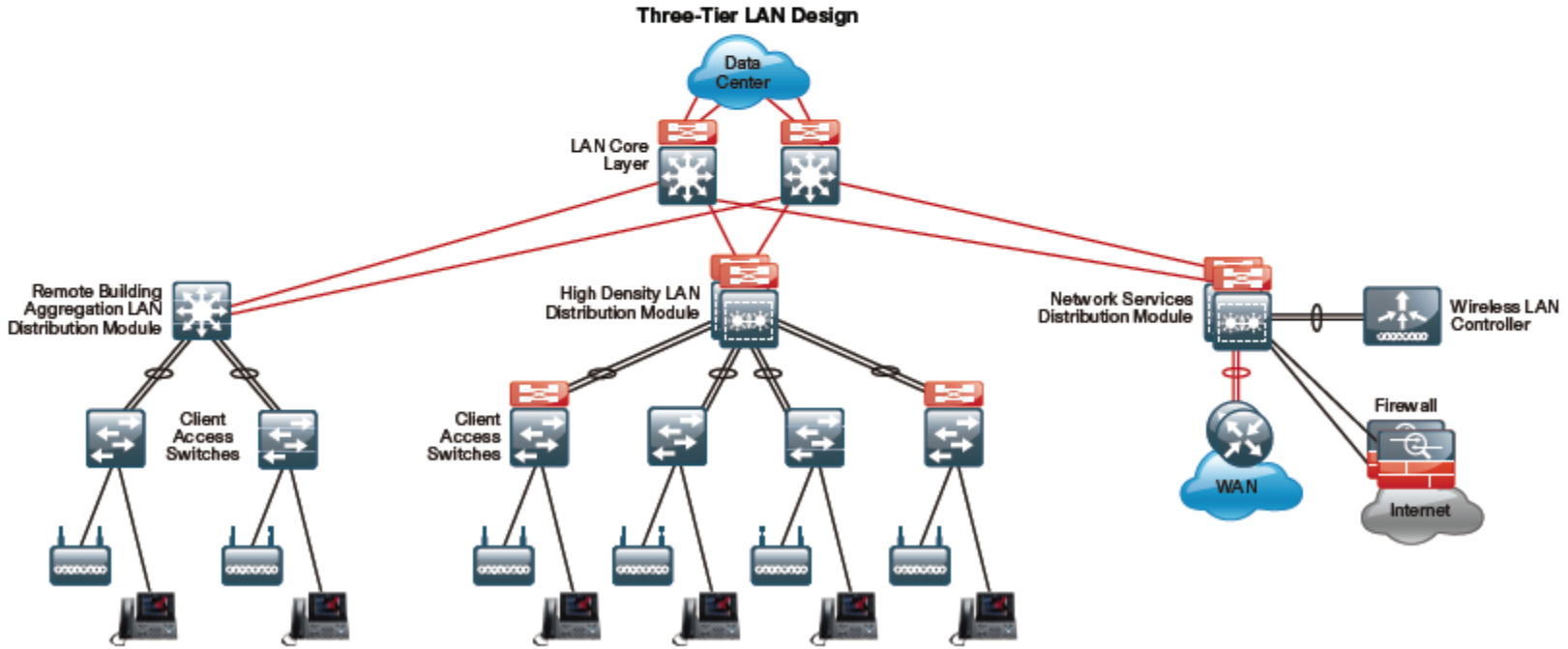
- Введение в LAN
- Рекомендации по настройке и лучшие практики (L1, L2, L3-уровни)
- Рекомендации по настройке и лучшие практики (безопасность)
- Рекомендации по настройке и лучшие практики (протоколы, сервисы)
- Уникальный совокупный функционал
- Позиционирование оборудования в LAN

Введение в LAN

SBA ? О каких LAN-сетях мы поговорим ?







Требования к LAN / цели построения LAN-сетей

Обеспечение работы бизнеса:

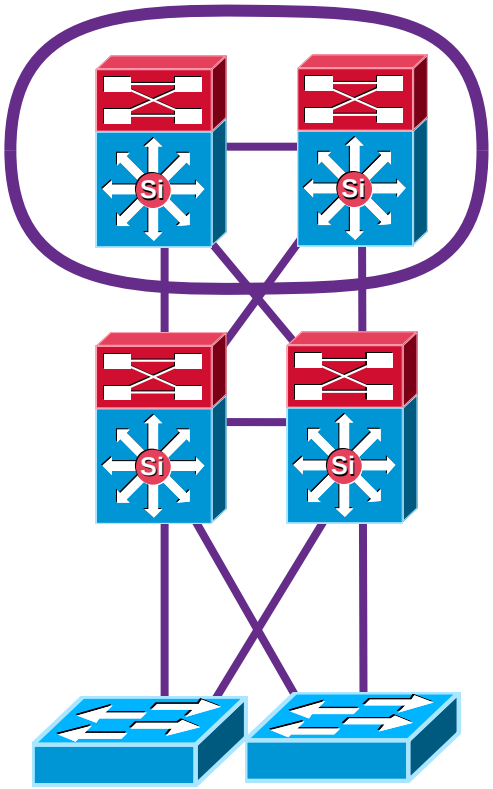
- Обеспечение отказоустойчивого и доступного сервиса
- Быстрая восстанавливаемость сервисов
- Оптимизация использования сервисов
- Безопасность использования сервисов
- Обеспечение разных типов доступа (проводного и беспроводного) к сервисам

Принципы построения LAN-сетей

- Иерархичность (hierarchy) – роли и задачи
- Модульность (modularity) - специфический функционал
- Восстанавливаемость (resiliency) – способность противостоять ошибочным или злоумышленным воздействиям
- Адаптация (Flexibility) - способность модификации, наращиваемости без существенных изменений сети

Иерархичность - уровень ядра

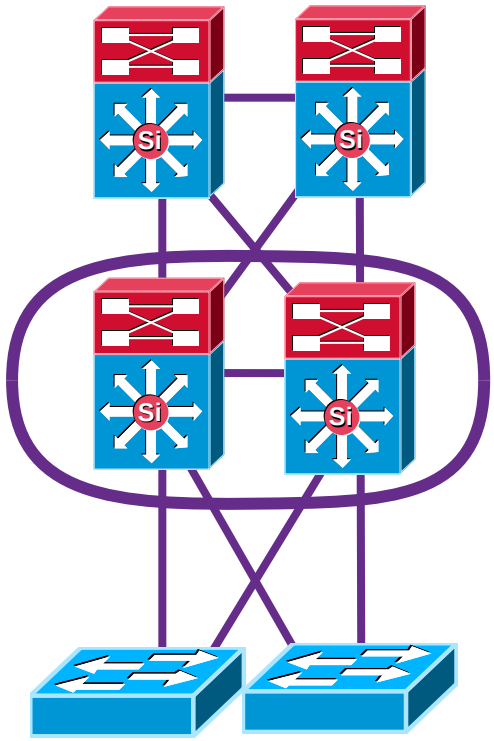
- Центральный, критичный элемент LAN
- Объединение модулей, высокоскоростная коммутация/маршрутизация
- Нет сервисов, серверов/пользователей
- Высокая отказоустойчивость → модернизация (HW, SW) → нет простоя сервиса



Иерархичность - уровень распределения

- Граничный элемент между ядром и доступом
- Агрегация соединений от уровня доступа и подключение к ядру
- Функционал:

✓ Применение сетевых политик к трафику
✓ Изоляция проблем уровня доступа
✓ Суммаризация маршрутов, быстрая сходимость
✓ Балансировка нагрузки
✓ Резервирования шлюза по умолчанию для уровня доступа



Иерархичность - уровень доступа

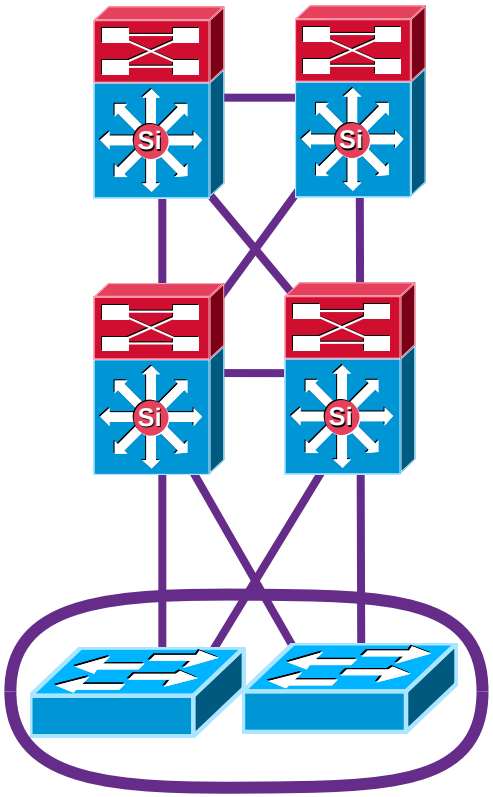
- Граничный элемент между сетевой инфраструктурой и пользовательскими устройствами
- Подключение пользовательских устройств
- Функционал:

✓ Автообнаружение и автоконфигурациия устройств

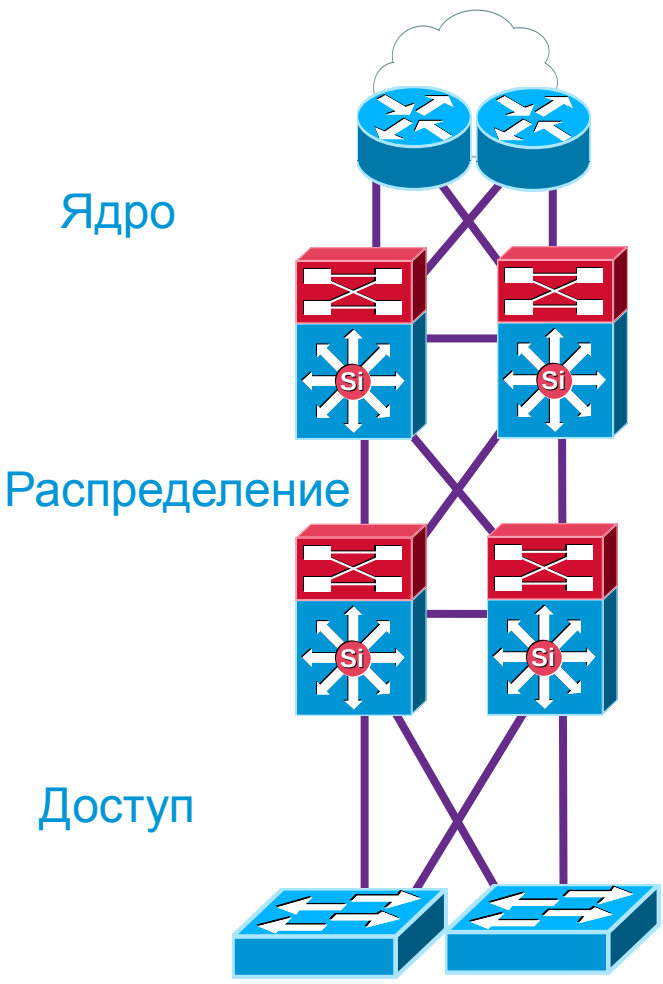
✓ Обеспечение идентификации и безопасного доступа

✓ Обеспечение качества обслуживания для разного трафика и приложений

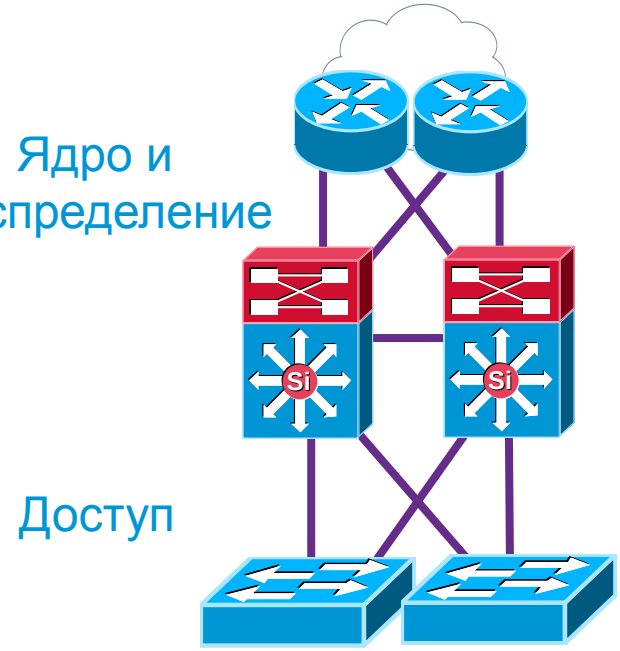
✓ Другие интеллектуальные сетевые сервисы



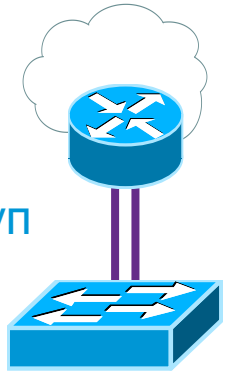
Всегда ли нужно 3 уровня иерархии ?



Центральный офис



Небольшой центральный офис
Удаленный офис



Небольшой удаленный офис

- Типовые дизайны SBA
- Важность и требования → дизайн

Модульность

- Отдельный функциональный блок, интегрируемый в кампус
- Специфическая общедоступная функциональность (WAN, DC, Internet)
- Характеристики:

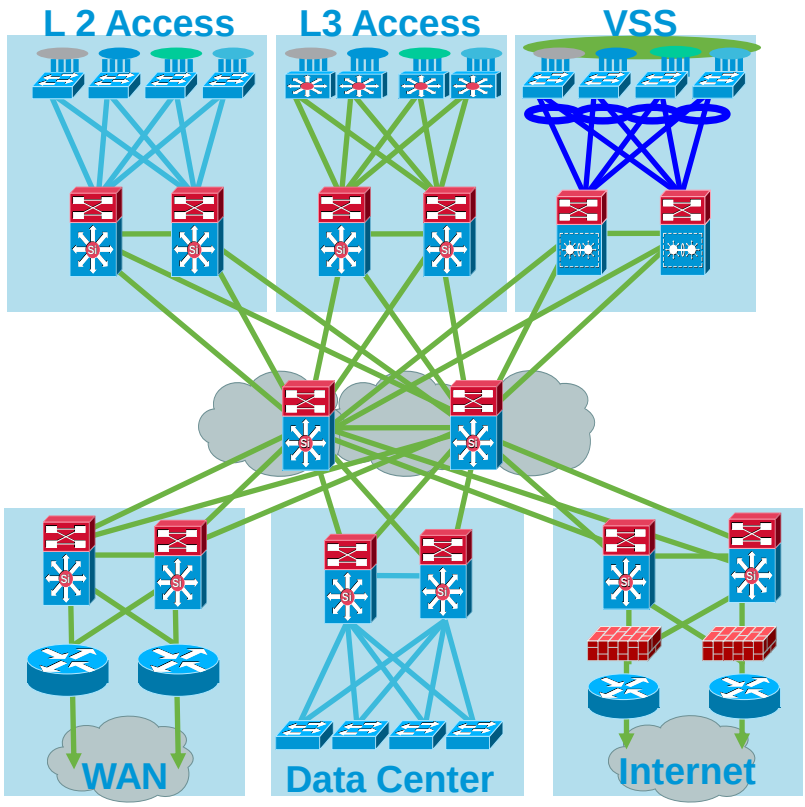
✓ Простота эксплуатации

✓ Изолированность → нет распространения проблем

✓ Высокая доступность

✓ Прогнозируемость – модернизация (HW, SW) – контролируемый процесс

✓ Масштабируемость



Восстанавливаемость

- Способность противостоять ошибочным или злоумышленным воздействиям

- Широкий спектр технологий:

✓ Технологии безопасности

✓ Обнаружение и реагирование на несвойственное поведения сети

✓ Технологии качество обслуживания разного трафика и приложений

✓ Интеллектуальные сетевые сервисы

Адаптация

- Способность модификации, наращиваемости без существенных изменений сети
- Поэтапные изменения без влияния на всю сеть
- Широкая функциональность оборудования
- Возможность обеспечить требования завтрашнего бизнеса

Рекомендации по настройке и лучшие практики (L1, L2, L3)

Физический уровень - лучшие практики

Для уменьшения времени сходимости и его прогнозируемости:

- Используйте 1Г и 10Г оптические соединения point-to-point между коммутаторами для уменьшения времени сходимости
- IEEE 802.3ae (10Г) и 802.3z (1Г) имеют встроенные механизмы обнаружения сбоев (локальных/удаленных каналов связи/узла)

- Настройка параметров уведомления о падении канала (debounce timer): 1/10Г оптика = 10мс, 10/100М, 1/10Г медь = 300мс
- Настройка дополнительных задержек (carrier timer) о падении канала = 0 мс

Физический уровень - лучшие практики

Для уменьшения времени сходимости и его прогнозируемости:

- Используйте физические интерфейсы L3 вместо L2 интерфейсов ассоциированных с L3 SVI

1. Link Down
2. Interface Down
3. Routing Update

~ 8 мсек потери

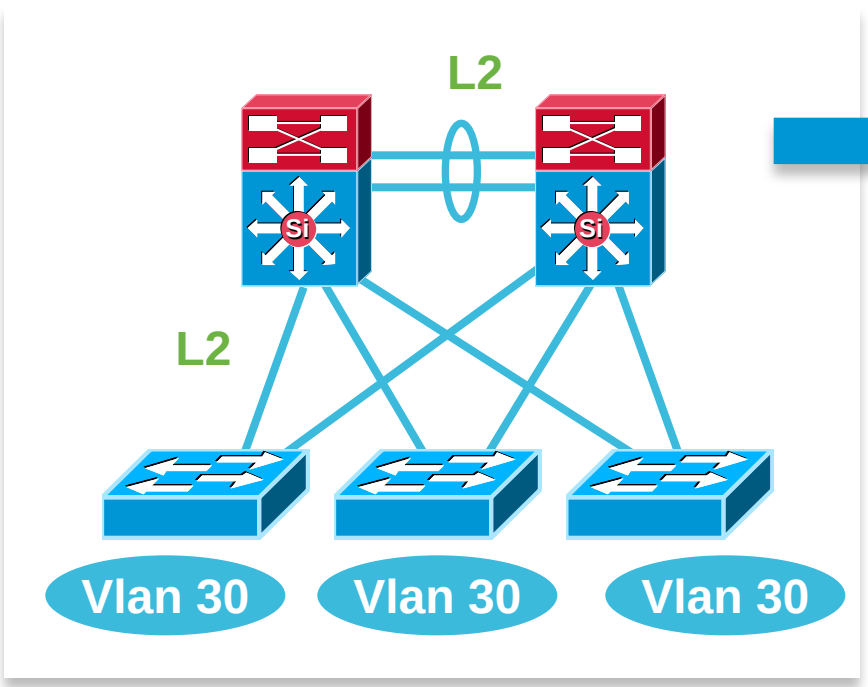
```
21:38:37.042 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet3/1, changed state to down
21:38:37.050 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet3/1, changed state to down
21:38:37.050 UTC: IP-EIGRP(Default-IP-Routing-Table:100): Callback: route_adjust GigabitEthernet3/1
```

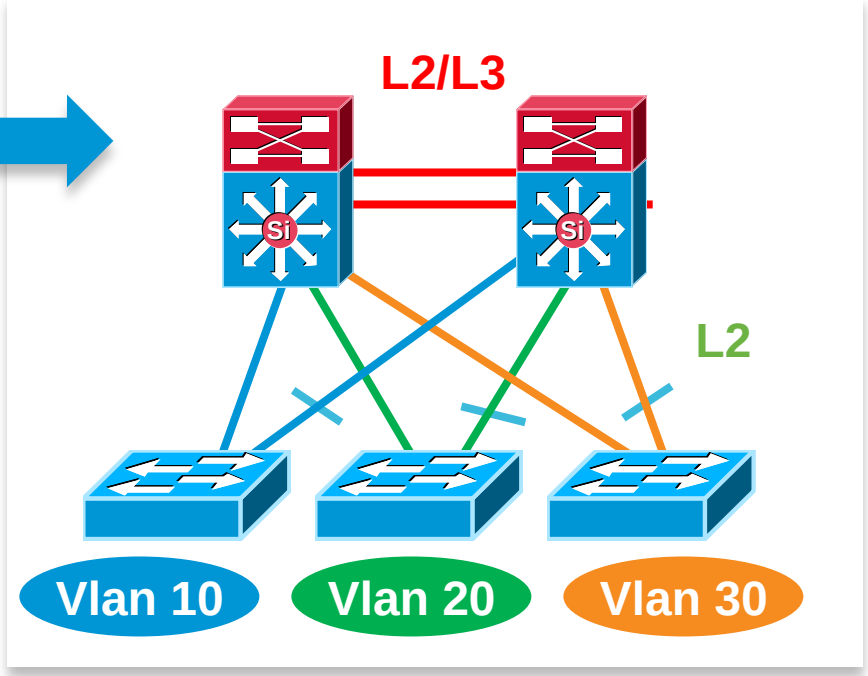
1. Link Down
2. Interface Down
3. Autostate (ряд проверок, синх. с STP)
4. SVI Down
5. Routing Update

~ 150–200 мсек потери

```
21:32:47.813 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/1, changed state to down
21:32:47.821 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet2/1, changed state to down
21:32:48.069 UTC: %LINK-3-UPDOWN: Interface Vlan301, changed state to down
21:32:48.069 UTC: IP-EIGRP(Default-IP-Routing-Table:100): Callback: route, adjust Vlan301
```

Ограничить распространение VLAN

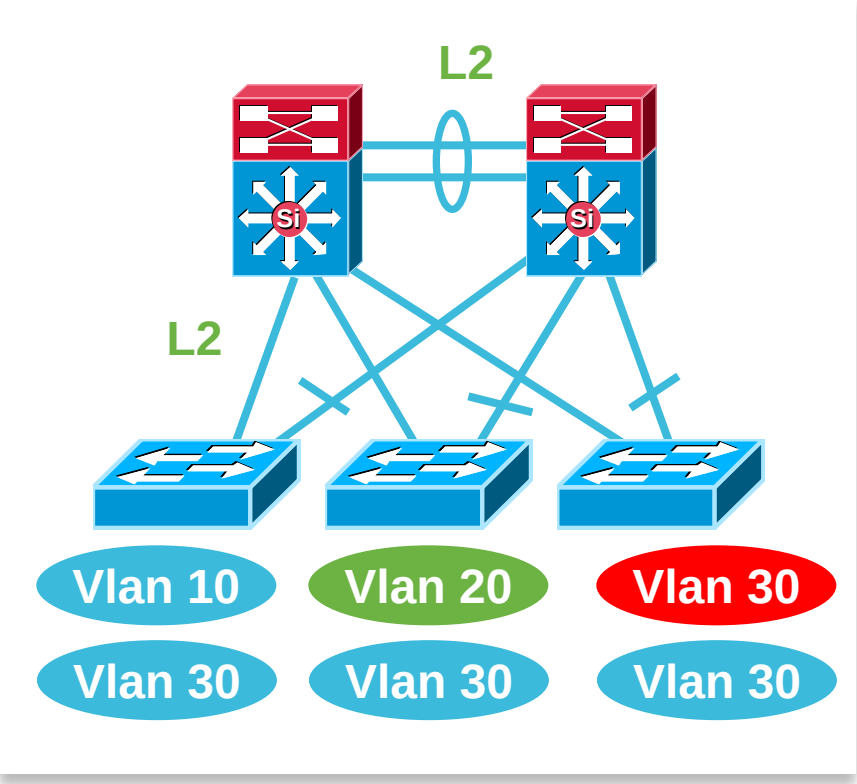




- При распространения VLAN-ов по всей сети сходимость STP/RSTP менее прогнозируема

- При ограничение конкретных VLAN-ов коммутаторами доступа, сходимость STP/RSTP прогнозируема

Использовать Rapid PVST+ вместо классического STP

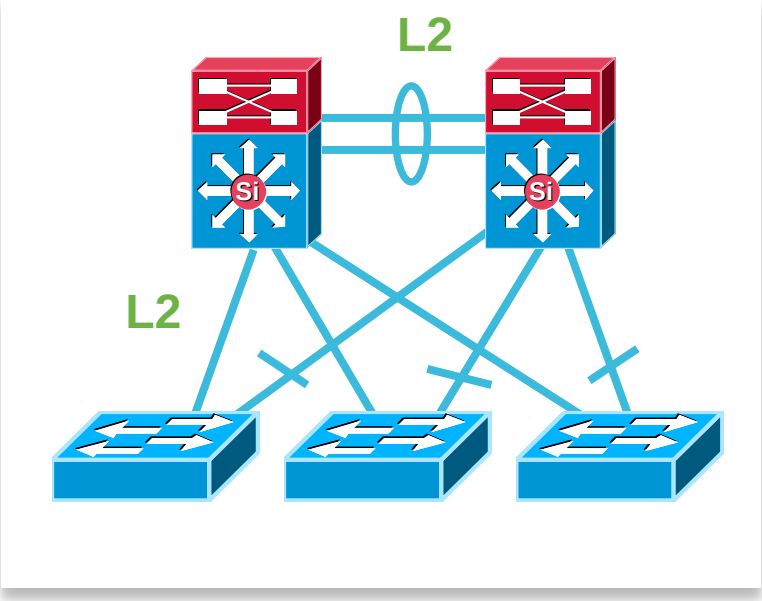


Набор встроенных улучшений:

- UplinkFast
- BackboneFast
- PortFast
- Loop Guard
- Root Guard
- BPDU Guard

- При необходимости распространения VLAN-ов по всей сети используйте Rapid PVST+ для улучшения сходимость

Защита от петель - LoopGuard

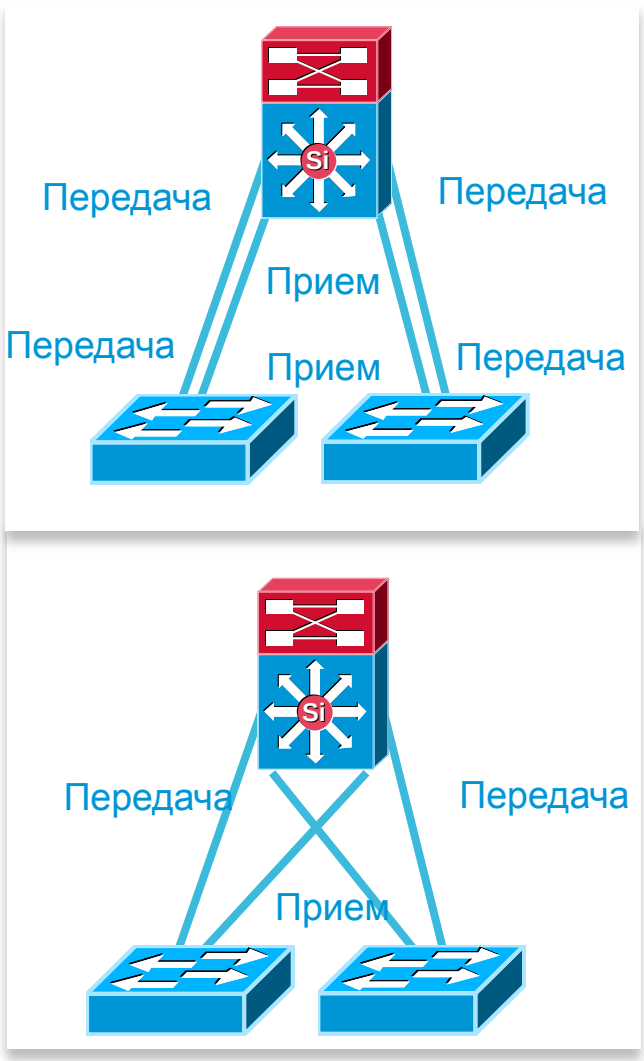


LoopGuard

- LoopGuard – защита от петель (из-за однонаправленных коммуникаций*), вызванных программным сбоем (например, STP)
- Работает на базе STP BPDU
- Не получив BPDU → “loop-inconsistent” (blocked) состояние
- Автоматическое восстановление
- Наибольший эффект при включении на всей сети

* - порты в UP, A→B=ok, B→A=not ok

Защита от петель - Unidirectional Link Detection Protocol

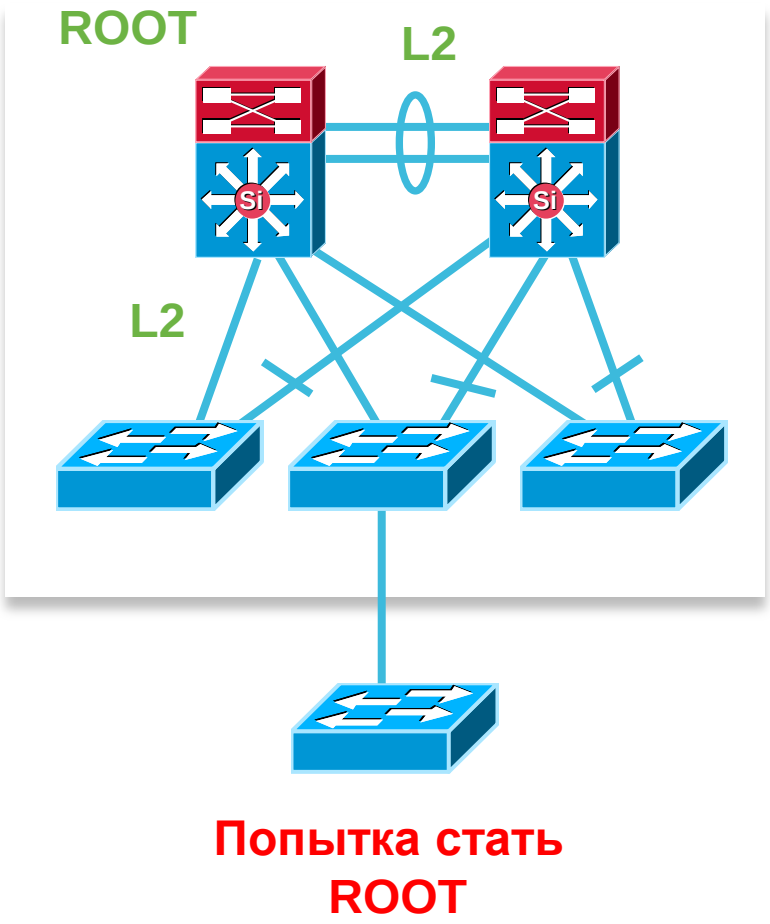


UDLD

- UDLD – защита от петель (из-за однонаправленных коммуникаций*), вызванных аппаратным сбоем / ошибкой коммутации
- Работает на базе UDLD протокола (L2 + L1 OSI)
- Не получив UDLD packets (device ID / port ID) → “disabled” состояние
- Ручное или автоматическое (errdisable) восстановление
- Эффективно работает на всех оптических коммуникациях

* - порты в UP, A→B=ok, B→A=not ok

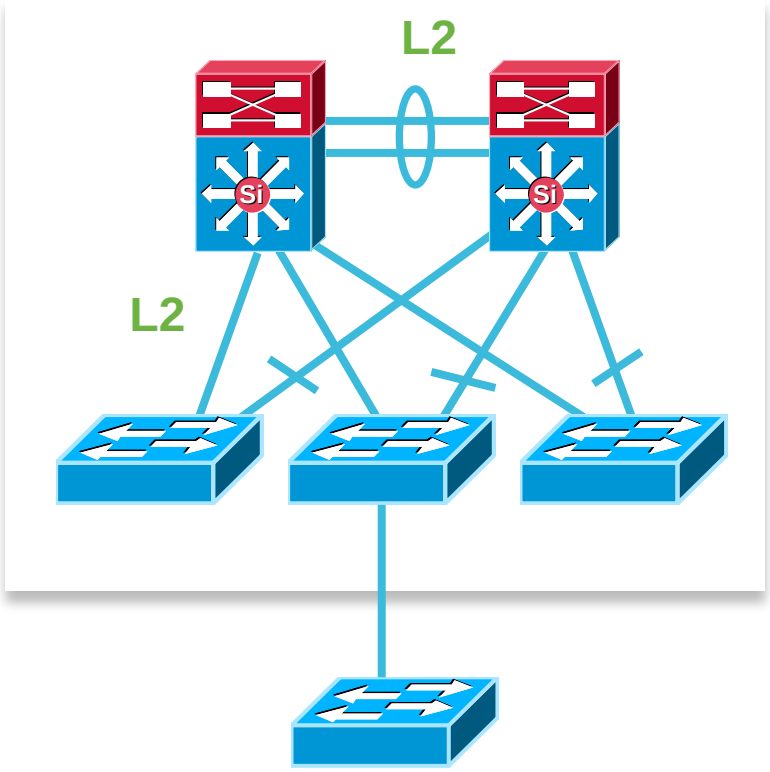
Защита от подмены STP Root - RootGuard



RootGuard

- RootGuard – защита от появления неавторизированного Root коммутатора
- Работает на базе STP BPDU
- Получил лучшее BPDU (lower bridge ID) → “root-inconsistent” (blocked) состояние
- Автоматическое восстановление

Защита от посторонних коммутаторов – BPDUGuard

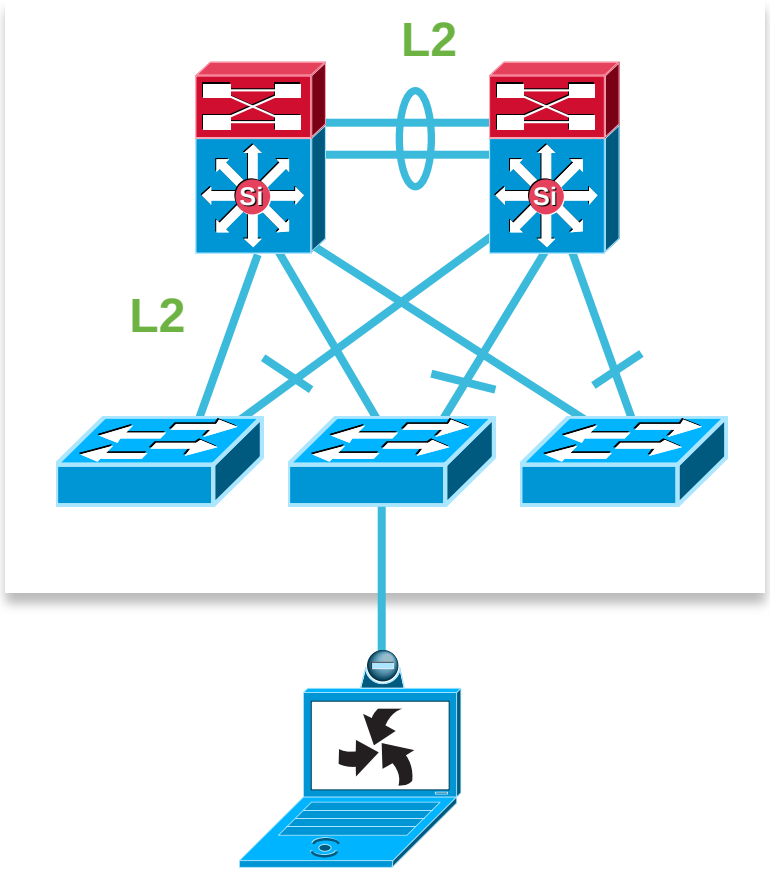


Попытка добавить коммутатор

BPDUGuard

- BPDUGuard – защита от появления неавторизированного коммутатора
- Работает на базе STP BPDU
- Получил BPDU → “error-disabled” (blocked) состояние
- Ручное или автоматическое (errdisable) восстановление

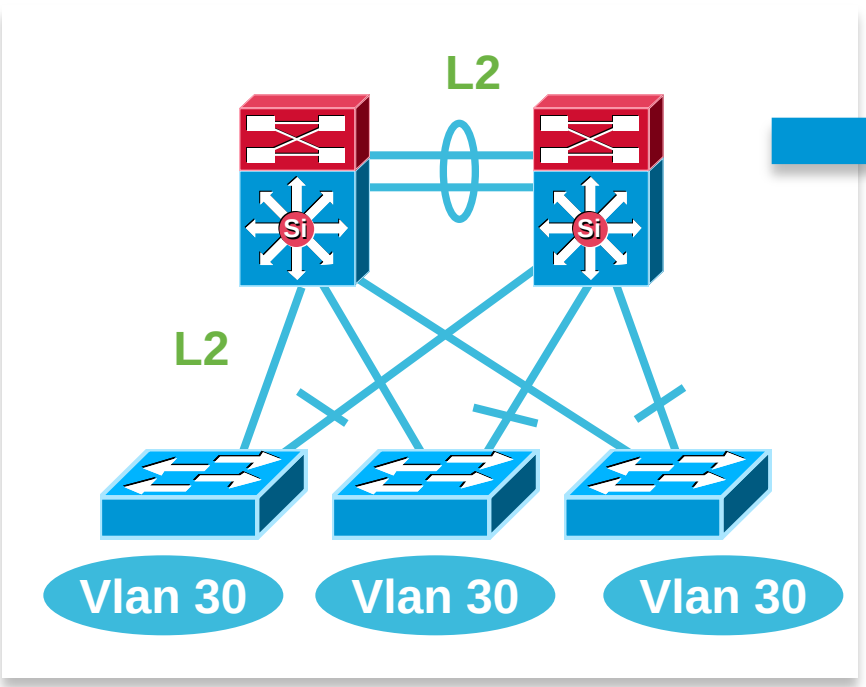
Быстрое подключение конечных устройств - PortFast



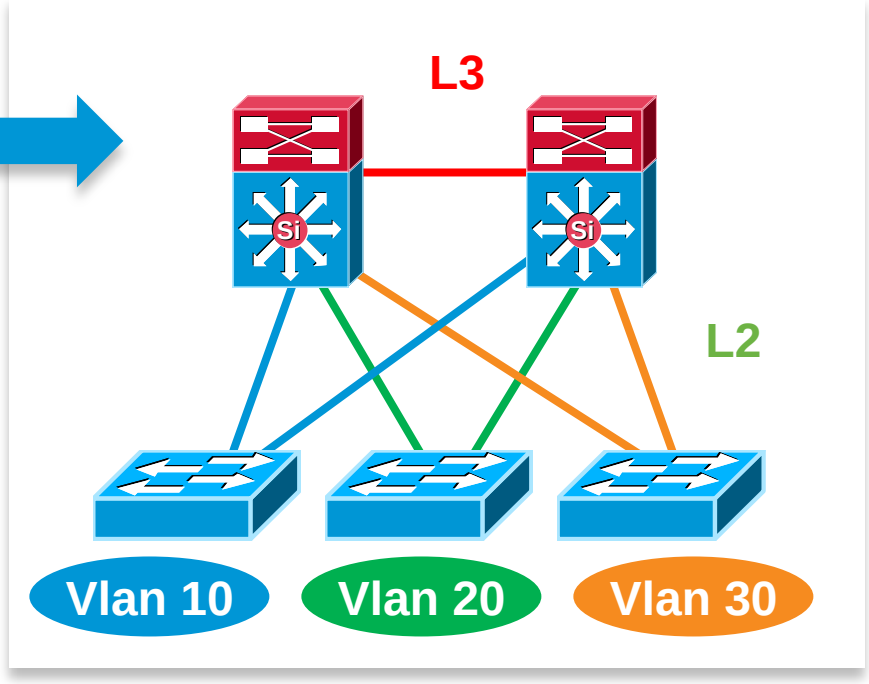
PortFast

- PortFast – ускоренный переход интерфейса в состояние UP, минуя “listening and learning”
- Используется на блоке портов для подключения конечных пользовательских устройств

Использовать “безпетельный” дизайн

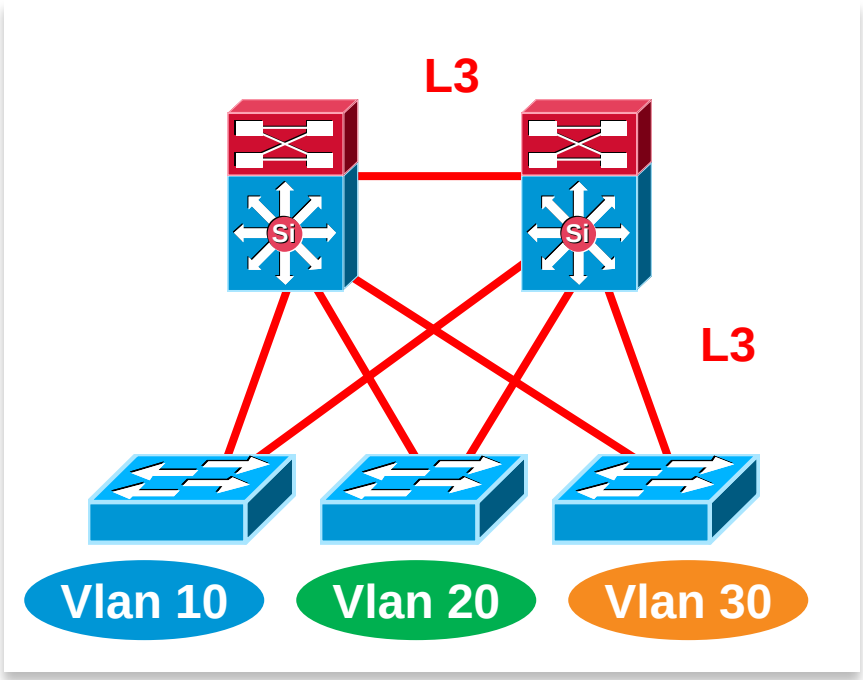


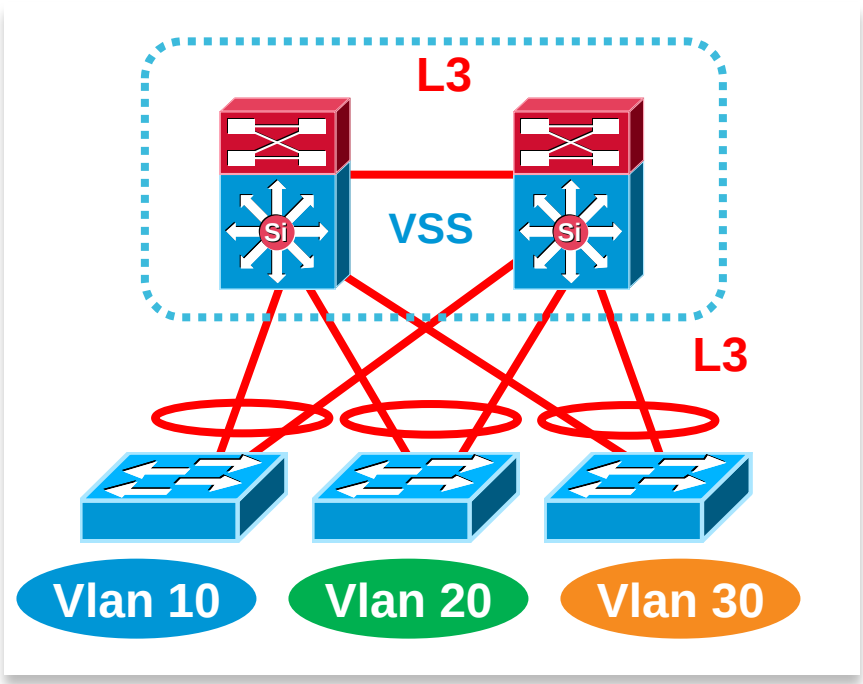
- Соединения уровня 2 между коммутаторами распределения
- Распространения VLAN-ов по всей сети
- Присутствуют петли уровня 2
- Есть заблокированные соединения



- Соединения уровня 3 между коммутаторами распределения
- Ограничение конкретных VLAN-ов коммутаторами доступа
- Нет петель уровня 2
- Нет заблокированных соединений

L3 дизайн





Рекомендации по настройке и лучшие практики (безопасность)

Безопасность на интерфейсах - Port Security

- Ограничение трафика на основе MAC-адресов (по кол-ву или разрешенному пулу) с заданием соответствующей политики на порту коммутатора

Злоумышленник

Передаваемые MAC

00:10:10:10:10:10
00:10:10:10:10:11
00:10:10:10:10:12
00:10:10:10:10:13
00:10:10:10:10:14
00:10:10:10:10:15
00:10:10:10:10:16
00:10:10:10:10:17
00:10:10:10:10:18
00:10:10:10:10:19
00:10:10:10:10:1A
00:10:10:10:10:1B

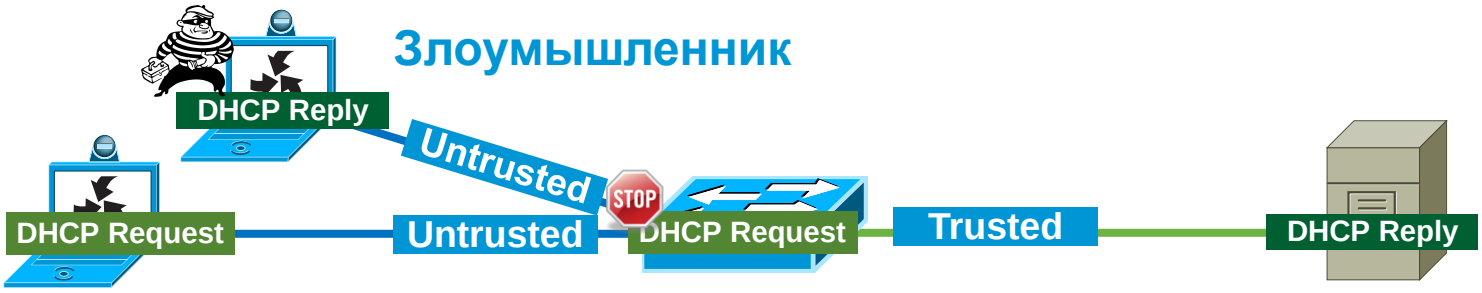
Превышение порога

Конфигурация на клиентском интерфейсе:

```
switchport port-security
switchport port-security maximum 11
switchport port-security aging time 2
switchport port-security aging type
inactivity
switchport port-security violation
restrict
```

Защита от подмены DHCP - DHCP Snooping

- Защита пользователя от ложных ответов на его DHCP запросы, за счет механизма доверенных/недоверенных интерфейсов и поддержки единой базы MAC-IP



DHCP Snooping Binding Table

MAC Address	IP Address	VLAN	Interface
00:50:56:BA:13:DB	10.4.80.10	10	GigabitEthernet2/0/1

Глобальная конфигурация коммутатора:

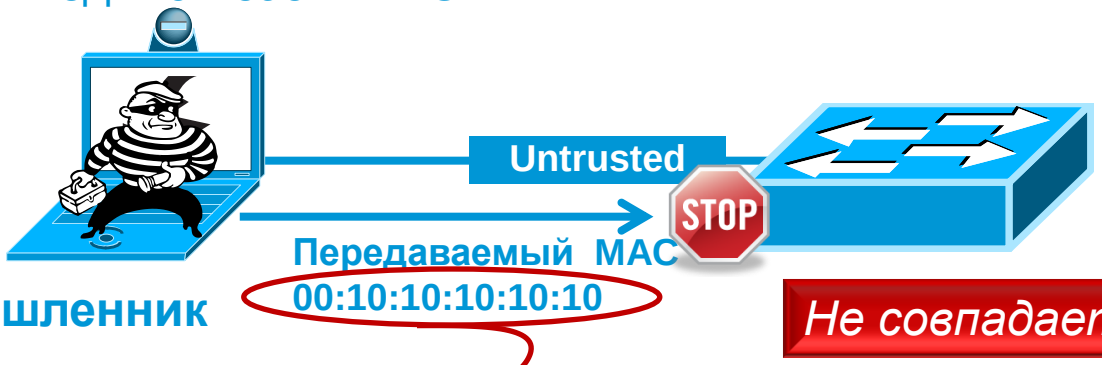
```
ip dhcp snooping vlan [data vlan], [voice vlan]
no ip dhcp snooping information option
ip dhcp snooping
```

Конфигурация клиентского интерфейса:

```
ip dhcp snooping limit
rate 100
```

Защита от подмены ARP-пакетов - Dynamic ARP Inspection

- Защита от подмены MAC/IP (правильность ARP-запросов/ARP-ответов), за счет динамического анализа пакетов в сети и соответствия записям единой базы MAC-IP



DHCP Snooping Binding Table

MAC Address	IP Address	VLAN	Interface
00:50:56:BA:13:DB	10.4.80.10	10	GigabitEthernet2/0/1

Глобальная конфигурация коммутатора:

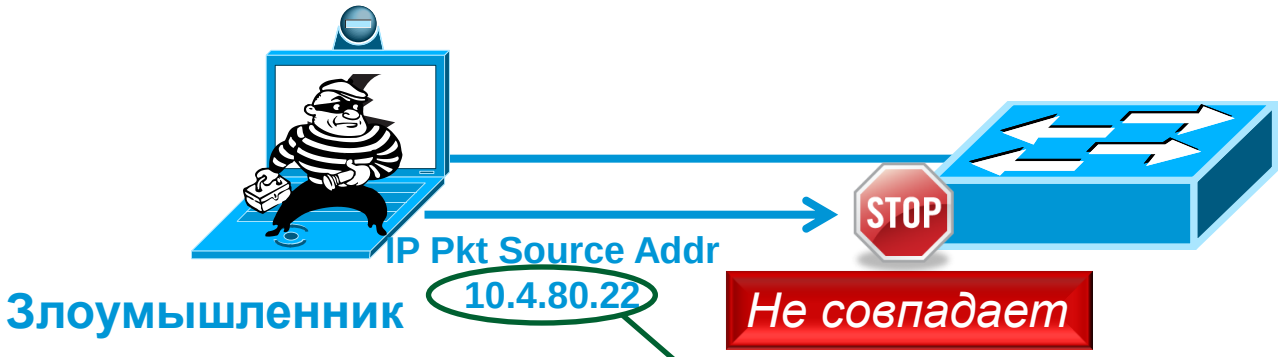
```
ip arp inspection vlan [data vlan],
[voice vlan]
```

Конфигурация клиентского интерфейса:

```
ip arp inspection limit
rate 100
```

Защита от подмены IP - IP Source Guard

- Защита от подмены IP на L2 интерфейсах, за счет динамического анализа пакетов в сети и соответствия записям единой базы MAC-IP



DHCP Snooping Binding Table

MAC Address	IP Address	VLAN	Interface
00:50:56:BA:13:DB	10.4.80.10	10	GigabitEthernet2/0/1

Конфигурация клиентского интерфейса:

```
ip verify source
```

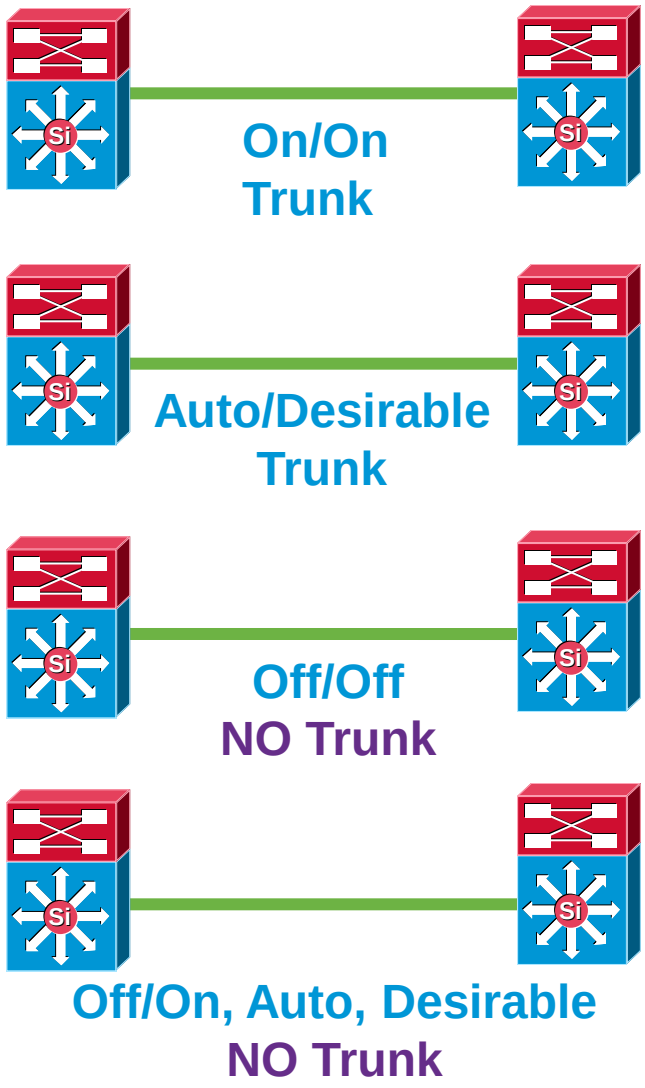
Рекомендации по настройке и лучшие практики (протоколы, сервисы)

Рекомендации по настройке Trunk/DTP

- Измените номер native VLAN (по умолчанию VLAN1)
- Ограничить все неиспользуемые на транке VLAN-ы

- Dynamic Trunk Protocol (DTP) – протокол автоматического установления транкового соединения между коммутаторами
- 4 режима транка
- Установление типа инкапсуляции 802.1Q или ISL

«Жёсткие» установки режима транка (ON) и типа инкапсуляции (Non-negotiate) для оптимальной конвергенции



Рекомендации по настройке VTP

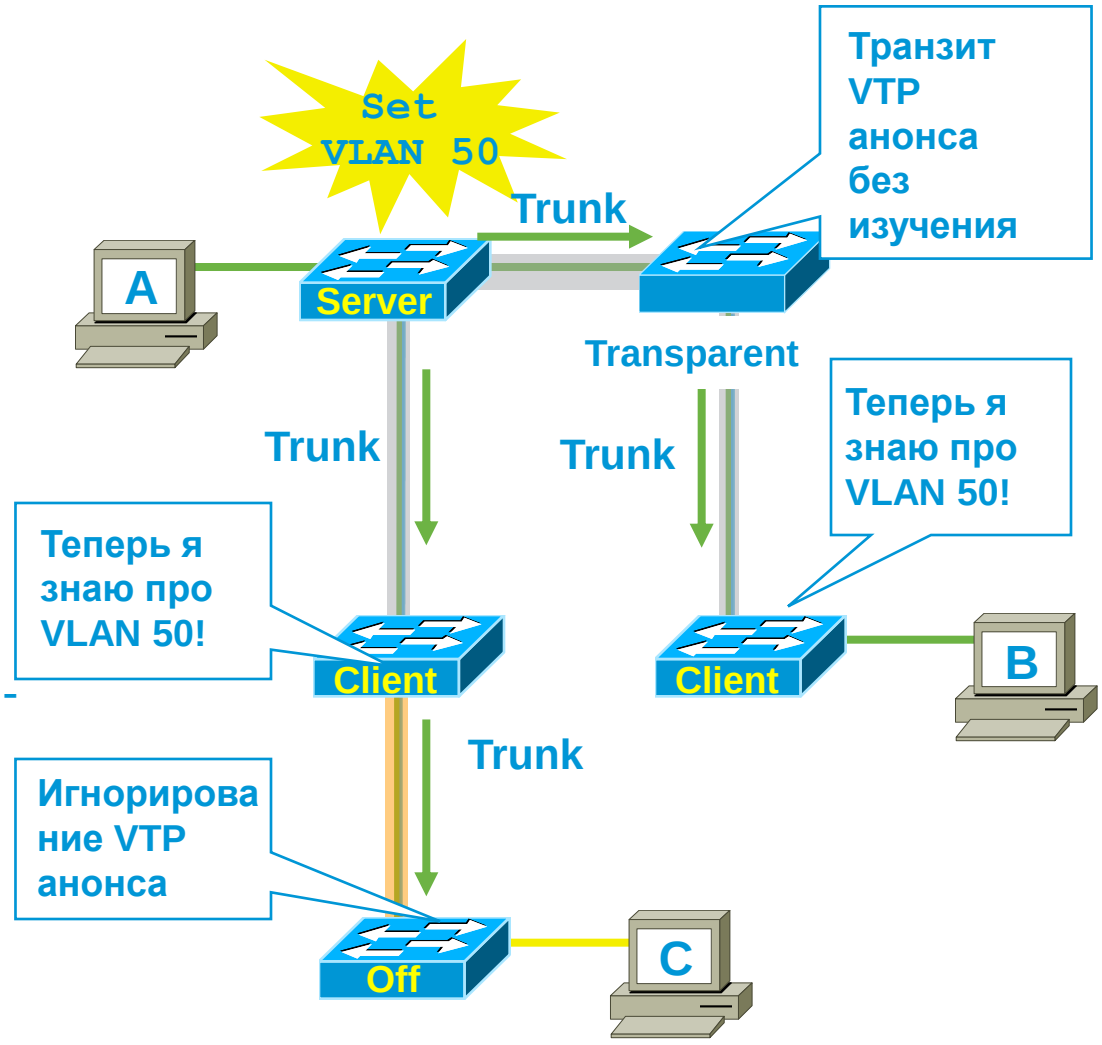
- Virtual Trunk Protocol (VTP) - централизованное управление VLAN
- Коммутатор VTP server распространяет БД VLAN на клиентские коммутаторы VTP
- Работает только на транках
- 4 режима:

✓ Server: обновляет VLAN БД на клиентах и др. серверах VTP

✓ Client: получает обновления - не может внести изменения

✓ Transparent: прозрачное прохождение VTP

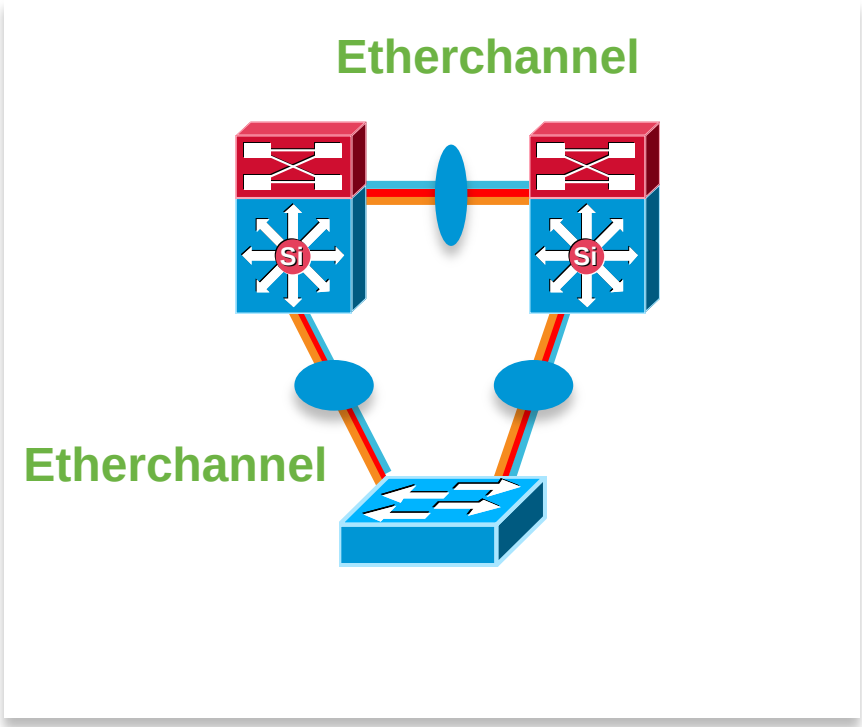
✓ Off: игнорирование VTP анонсов



Используйте VTP transparent режим для снижения вероятности ошибки

Рекомендации по настройке Etherchannel

- Обычно используется между уровнями распределениями и ядра, на соединениях внутри ядра и распределения
- Протоколы динамического согласования Etherchannel (PaGP, LACP)
- Используется для обеспечения отказоустойчивости соединения и расширения BW (8, 16 каналов)
- EtherChannel Min-Links
- Настройка хэша L3/L4 позволяет достичь равномерной загруженности каналов
- L2, L3 - Etherchannel
- Объединение каналов между разными картами (VSS), устройствами (stack, vPC)

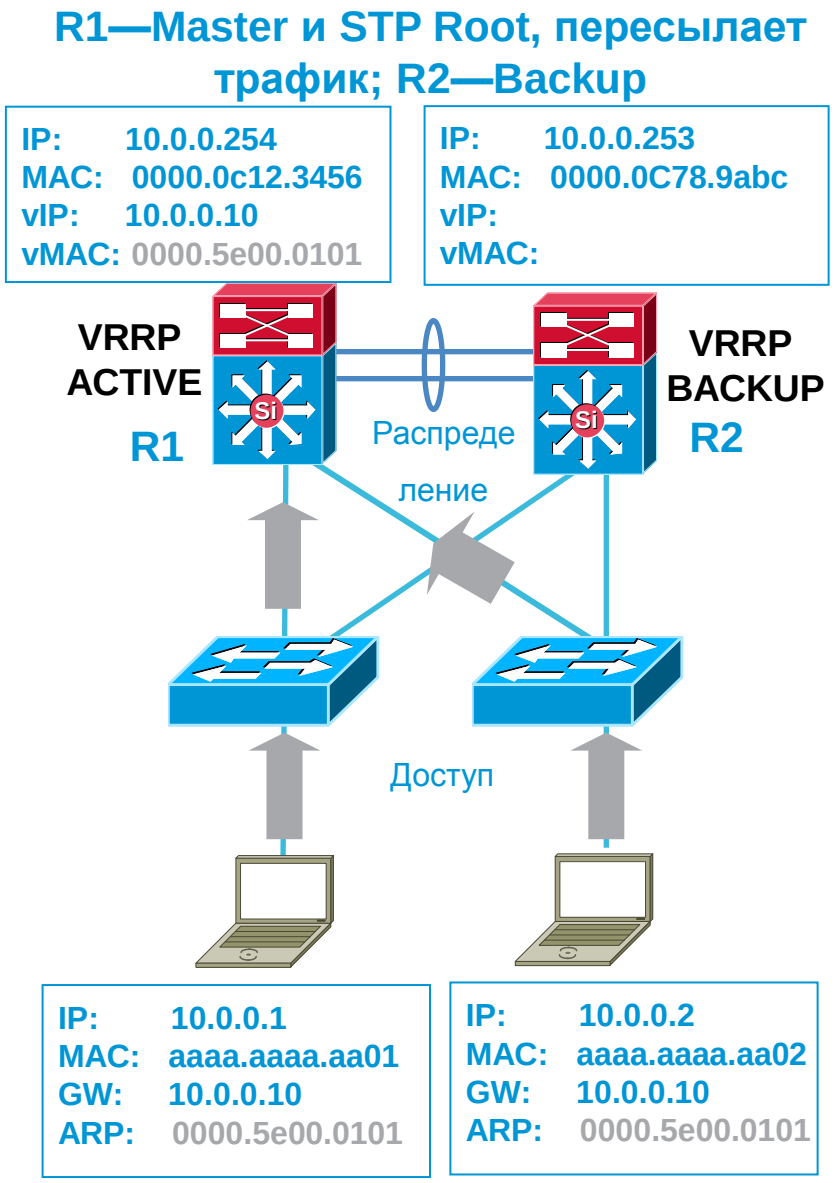


“port-channel load-balance src-dst-ip”

Равномерная загрузка каналов Etherchannel

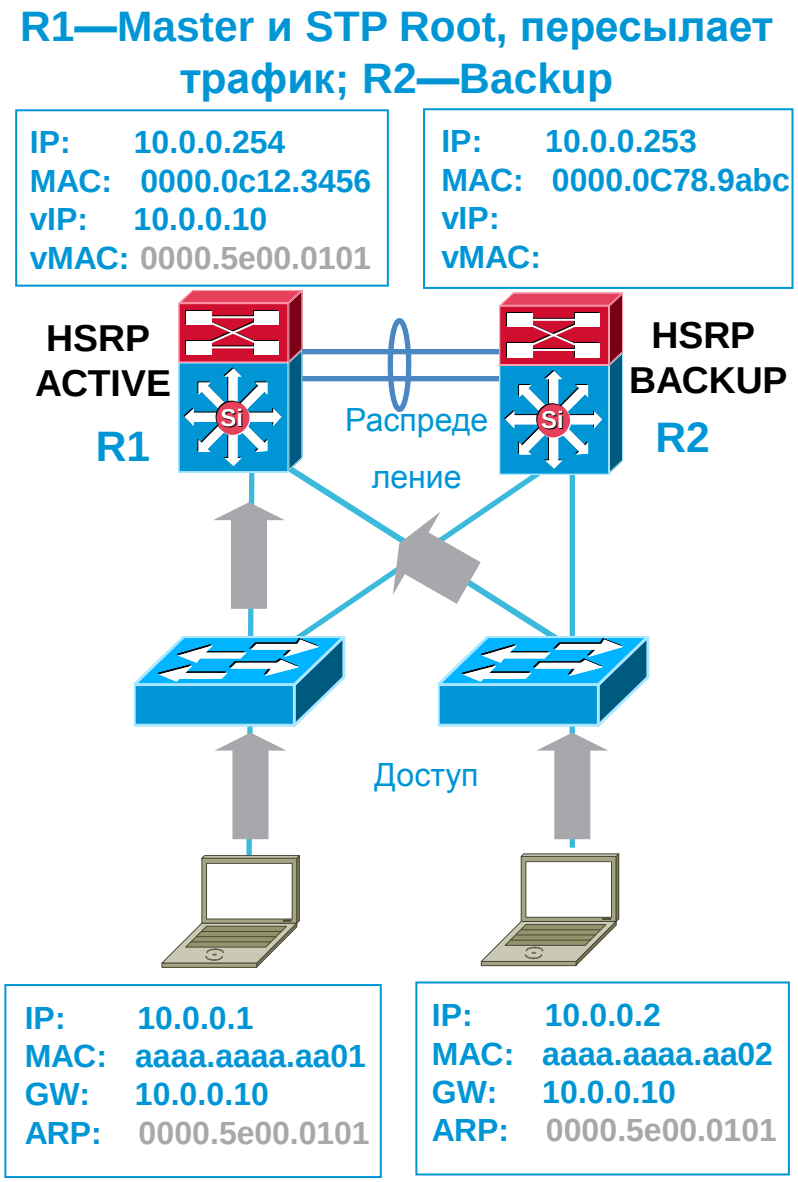
Обеспечение отказоустойчивости шлюза по умолчанию - VRRP

- Стандарт IETF RFC 2338 (Апрель 1998)
- Группа маршрутизаторов работает как один виртуальный с одним виртуальным IP адресом и MAC адресом
- Один (master) маршрутизатор пересылает пакеты для/из локальной сети
- Остальные маршрутизаторы работают как резервные
- Используйте VRRP, если требуется поддержка оборудования других производителей



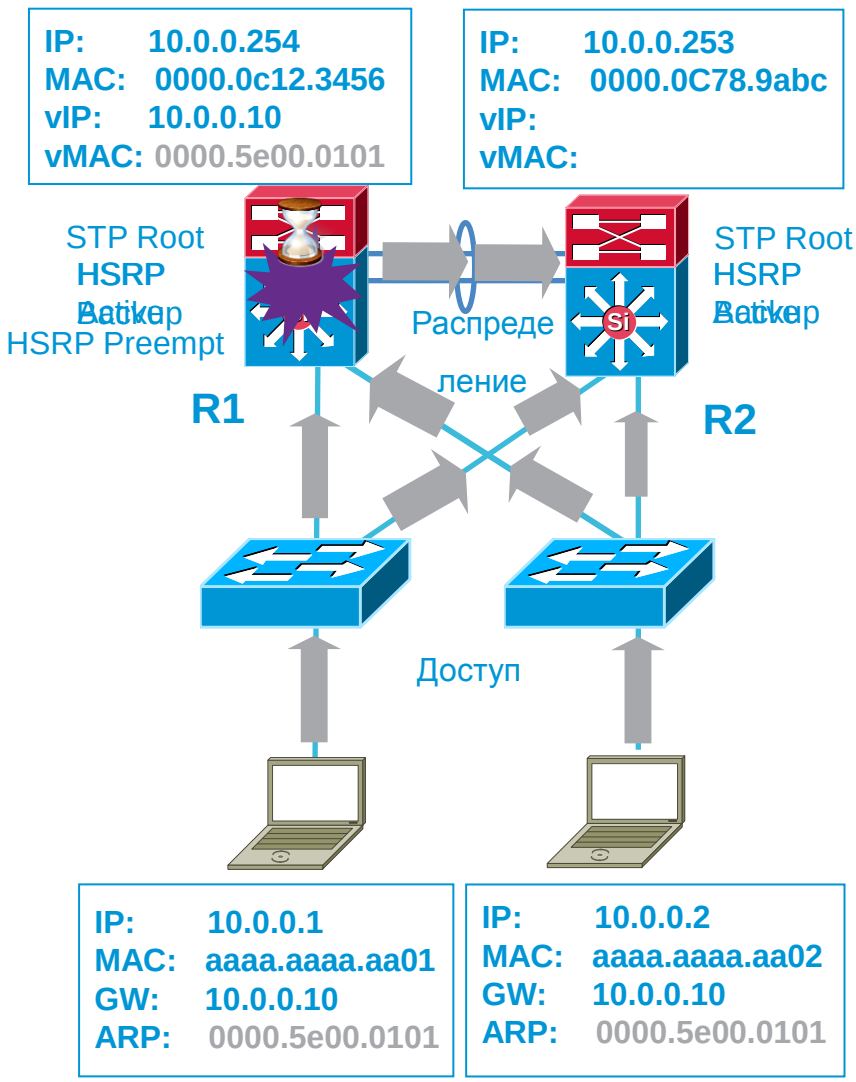
Обеспечение отказоустойчивости шлюза по умолчанию - HSRP

- Группа маршрутизаторов работает как один виртуальный с одним виртуальным IP адресом и MAC адресом
- Один (active) маршрутизатор пересылает пакеты для/из локальной сети
- Остальные маршрутизаторы работают как горячий резерв
- Используйте HSRP, если только Cisco-сеть и интересуют дополнительные возможности



Обеспечение отказоустойчивости шлюза по умолчанию – HSRP Preempt

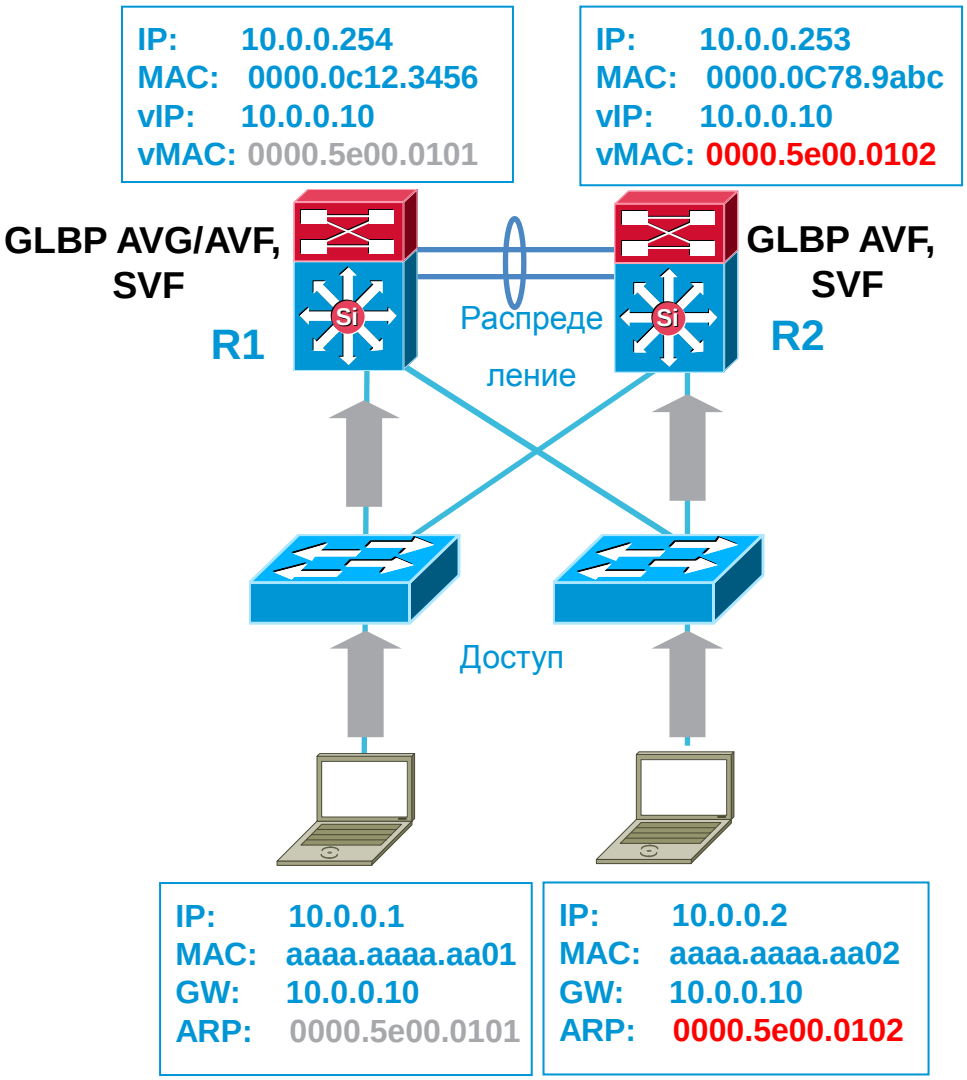
- STP root и HSRP active должен быть одним и тем же коммутатором
- При сбое синхронизация “STP root и HSRP active ”– ok
- После восстановления STP root и HSRP active на разных устройствах → транзитный линк (лишний хоп)
- HSRP preemption позволит перенести шлюз по умолчанию в соответствии с топологией STP



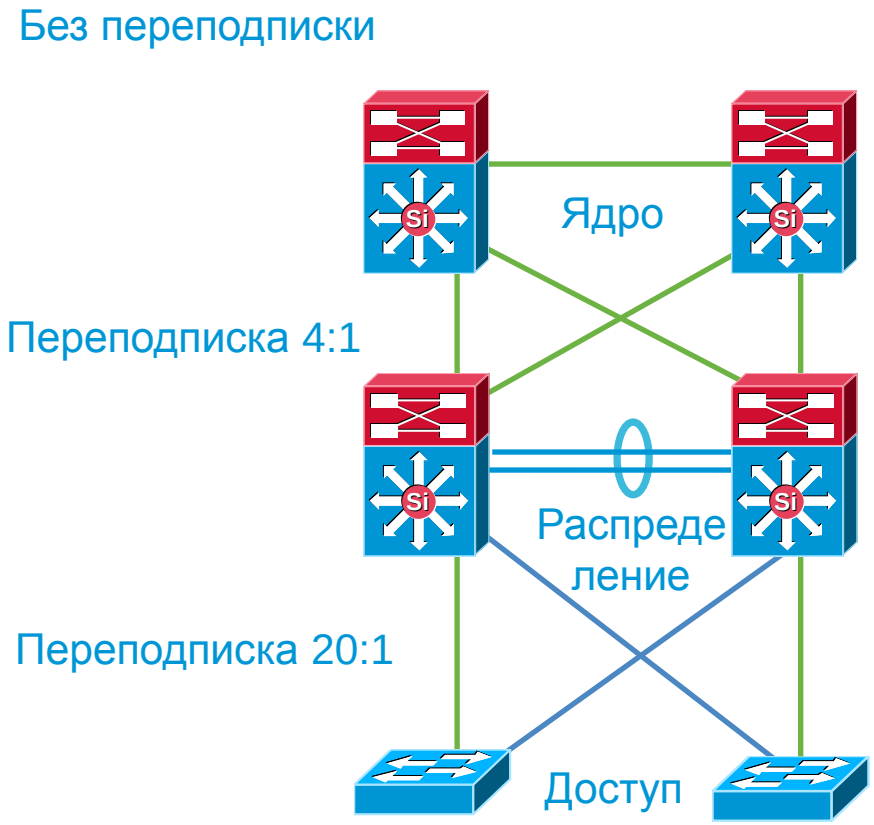
Обеспечение отказоустойчивости шлюза по умолчанию – GLBP

R1- AVG; R1, R2 – оба пересылают трафик;

- Все преимущества HSRP + балансировка нагрузки между шлюзами → использует всю доступную полосу
- Группа маршрутизаторов работают как один виртуальный, разделяют один виртуальный IP адрес, но используют несколько виртуальных MAC адресов
- Позволяют трафику из одной подсети использовать несколько шлюзов по умолчанию с одним виртуальным IP адресом



Переподписка (Oversubscription) в LAN



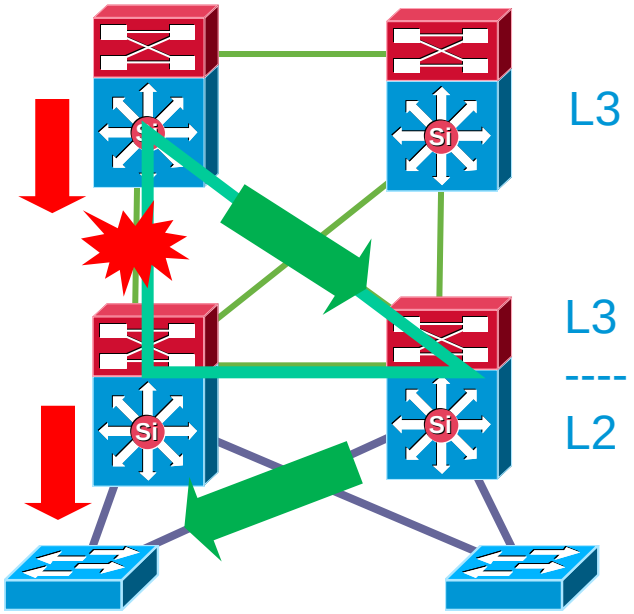
- Допускается проектирование LAN с переподпиской
- “Заторы” – QoS

Качество обслуживания (QoS) в LAN

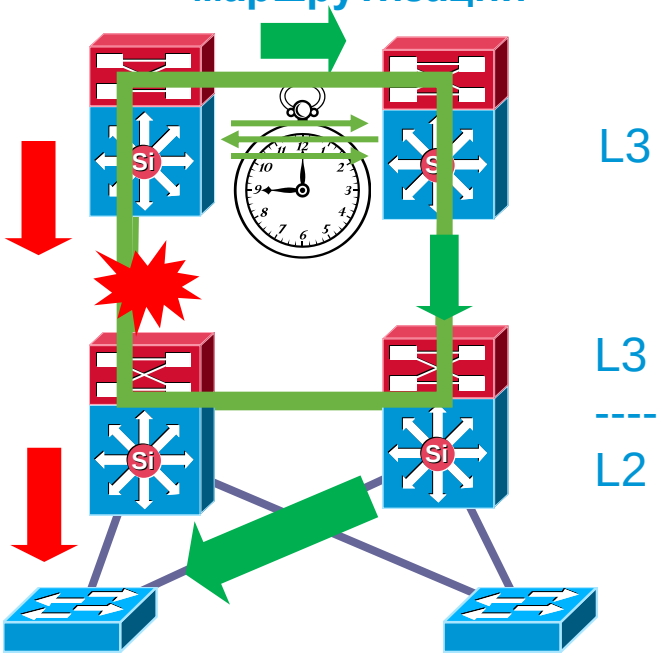
- Классифицировать и маркировать – ближе к источнику
- Не доверять пользовательским маркировкам
- Использовать DSCP вместо 802.1Q/p CoS – 64 vs 8
- 1-8 классов трафика
- Конфигурация на access и uplink портах через макросы
- Ограничивать (police) нежелательный трафик ближе к источнику vs FW
- Внедрять QoS где возможны скопления – oversubscription speed vs WAN Edge
- Strict Priority – не более 33% от общей BW
- Best Effort class – default class - не более 25% от общей BW
- Использовать WRED для всех TCP-потоков для раннего предотвращения скоплений (DSCP-based WRED)

Маршрутизация в LAN: треугольники VS квадраты

«Треугольник»: Потеря соединения/узла не требует конвергенции протокола маршрутизации



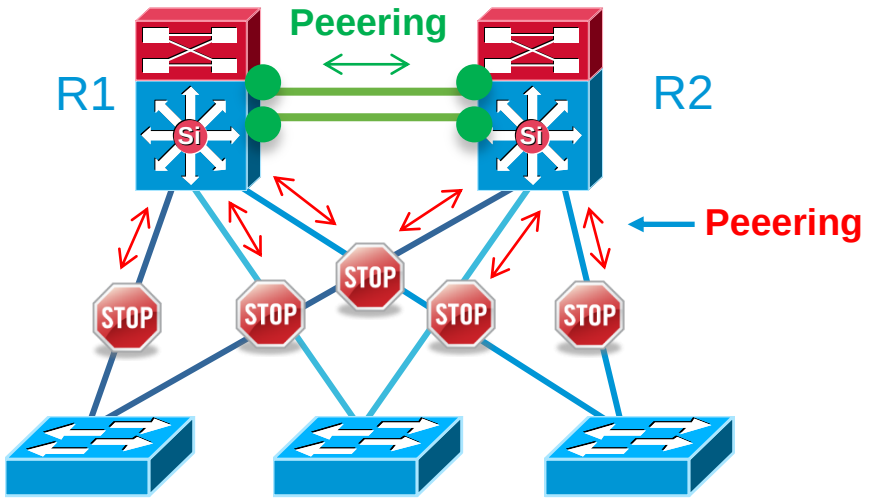
«Квадрат»: Потеря соединения/узла требует конвергенции протокола маршрутизации



- Эквивалентные резервированные соединения уровня 3 поддерживают быструю сходимость → нет необходимости для OSPF или EIGRP в расчёте нового пути
- Link Down - быстрое обнаружение → исключение канала→ использование альтернативного канала

Маршрутизация в LAN: L3 соседство и транзит

- Ограничивайте ненужные соседские отношения протоколов маршрутизации через транзитные узлы (например, уровень доступа) за счет использования пассивных интерфейсов
- Избегаем затрат памяти, излишних обновлений маршрутизации
- Суммаризируем на уровне агрегации



Пример OSPF:

```
Router(config)#router ospf 1
Router(config-router)#passive-
interface Vlan 99
```

```
Router(config)#router ospf 1
Router(config-router)#passive-
interface default
Router(config-router)#no passive-
interface Vlan 99
```

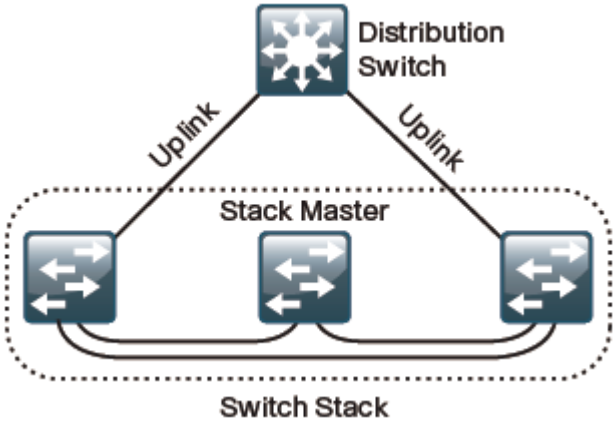
Пример EIGRP:

```
Router(config)#router eigrp 1
Router(config-router)#passive-
interface Vlan 99
```

```
Router(config)#router eigrp 1
Router(config-router)#passive-
interface default
Router(config-router)#no passive-
interface Vlan 99
```

Стекирование 3750X, 2960S

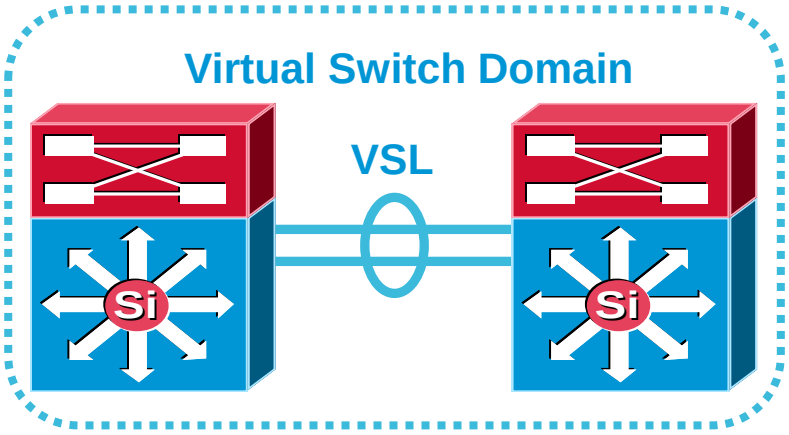
- Стек мастер – управляет работой стека
- 3750-X = 9 устройств, 2960-S/SF = 4 устройства
- Выбирайте мастер на коммутаторе без uplink-портов
- Первоначальный MAC мастера = стек MAC после сбоя (многие cross-стек сервисы и протоколы привязаны к нему и могут restart)




```
switch [switch number] priority 15
stack-mac persistent timer 0
```

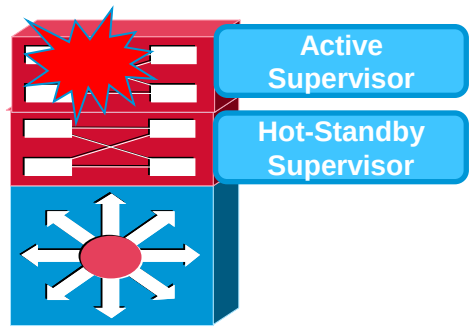
VSS, ISSU, NSF/SSO – 6500, 4500

- Catalyst 6500 – Virtual Switching System (VSS) 2T/4T
- Catalyst 4500 – VSS (в конце 2012)
- Control plane = active-standby operating model (active - EIGRP, STP, CDP ….)
- Data plane = active-active operating model
- VSL = min 2 x 10G на разных картах или портах Sup – sync
- ISSU – минимизация (sub-second) воздействия на сервис при обновлении ПО
- NSF/SSO - минимизация (sub-second) воздействия на сервис при переключении Sup и непрерывность пересылки пакетов data plane



Switch 1 + Switch 2

VSS - Single Logical Switch



4500-E

Управление устройством

- Управление устройством через шифрованные средства
- ✓ SSH and HTTPS – использовать безопасные (шифрование) протоколы
- ✓ Небезопасные средства выключить – Telnet, HTTP

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
  transport input ssh
```

- Для управления устройством NMS
- ✓ SNMP(v2c) should be configured for both a read-only and a read-write community string

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

Управление устройством

- Управление устройством (SSH and HTTPS) контролируется централизованной системой AAA
- Основная система TACACS+ , резервная – локальная база на устройстве

```
enable secret c1sco123
service password-encryption
!
username admin password c1sco123
aaa new-model
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+ local
aaa authorization console
ip http authentication aaa
tacacs-server host 10.4.48.15 key SecretKey
```

- В качестве source-interface для протоколов и сервисов используйте loopback

```
interface loopback 1
 ip address 10.1.1.1 255.255.255.255
!
snmp-server trap-source loopback 1
ip ssh source-interface loopback 1
```

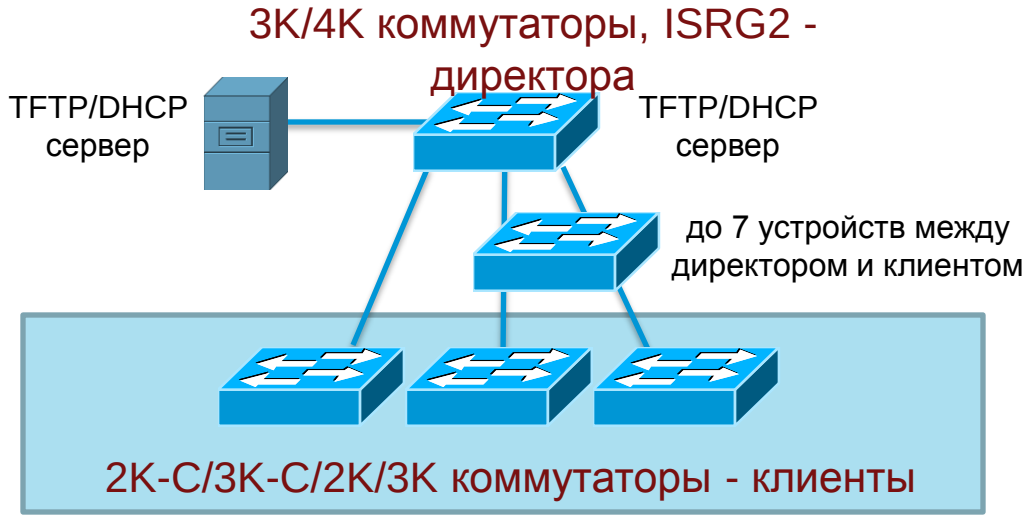
Уникальный совокупный функционал

Упрощенная инсталляция
Smart install

2K-C	3K-C	2K	3K	4K

Технология, обеспечивающая простоту установки образа ПО и настройки коммутаторов с минимальным участием пользователя

- Обнаружение → CDP, LLDP или DHCP-коммуникацию
- Опции DHCP → инсталляция клиентского коммутатора
- ПО и конфигурационный файл → группа (например, по Product ID, MAC)
- Обновление ПО и конфигурационного файла “по требованию”
- Централизованная база → backup
- Замена коммутатора → конфигурация



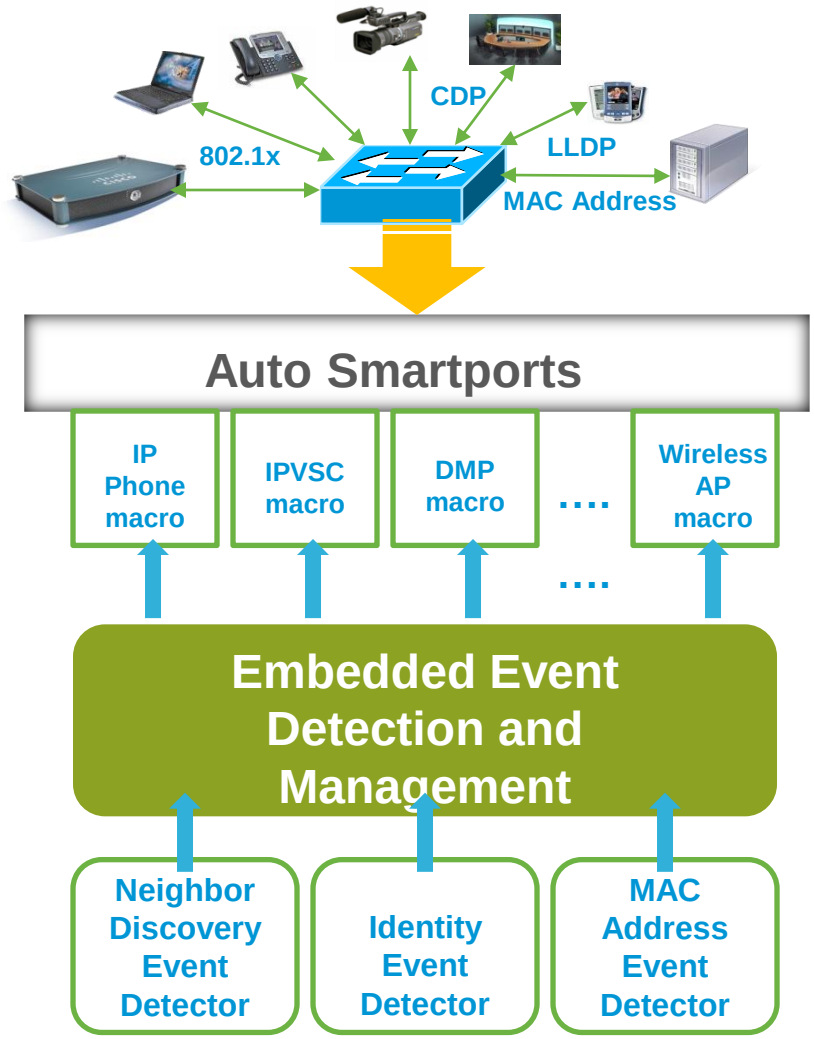
Упрощенная конфигурация

Auto smartports

2K-C	3K-C	2K	3K	4K	6K

Функционал автоматической настройки порта доступа коммутатора в зависимости от устройства, подключаемого к порту на основе лучших практик Cisco (L2, QoS, Security и т.д.)

- Идентификация → CDP, LLDP, LLDP-MED, MAC
- Широкий список устройств
- Автоматическое присвоение и удаление конфигурации на порту
- Интеграция с инфраструктурой идентификации (802.1x, MAC authentication bypass, web-authentication)
- Возможность создания пользовательских макросов
- Smart Install + Auto Smartports



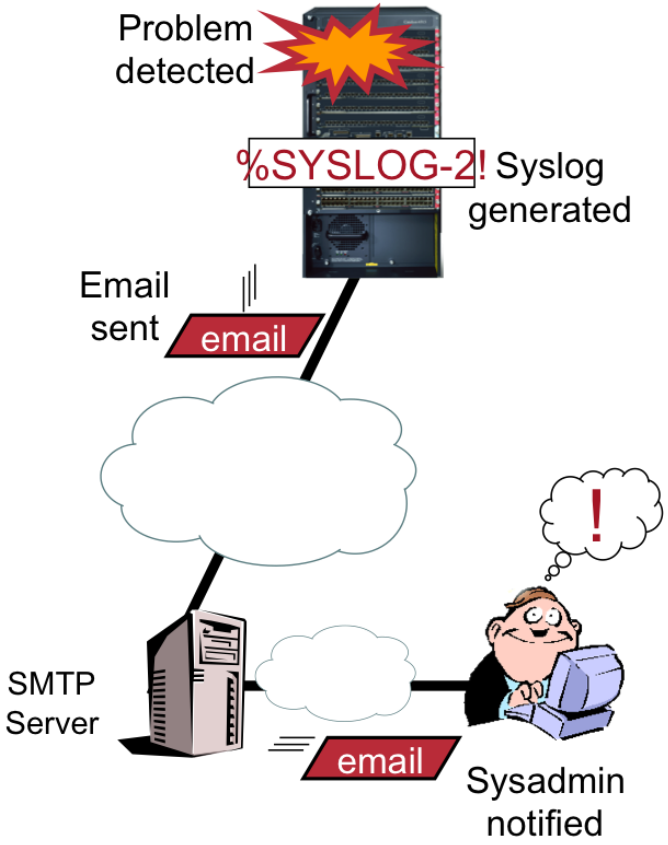
Упрощенный поиск неисправностей

Generic Online Diagnostics (GOLD)

2K-C	3K-C	2K	3K	4K	6K

Функционал проактивной диагностики работоспособности коммутатора

- Быстрая идентификация возможных аппаратных сбоев → действия по их устранению (sup, карта)
- Запуск тестов во время загрузки, по требованию, по расписанию
- Уведомления по syslog, SNMP
- Интеграция с EEM → выполнение скриптов



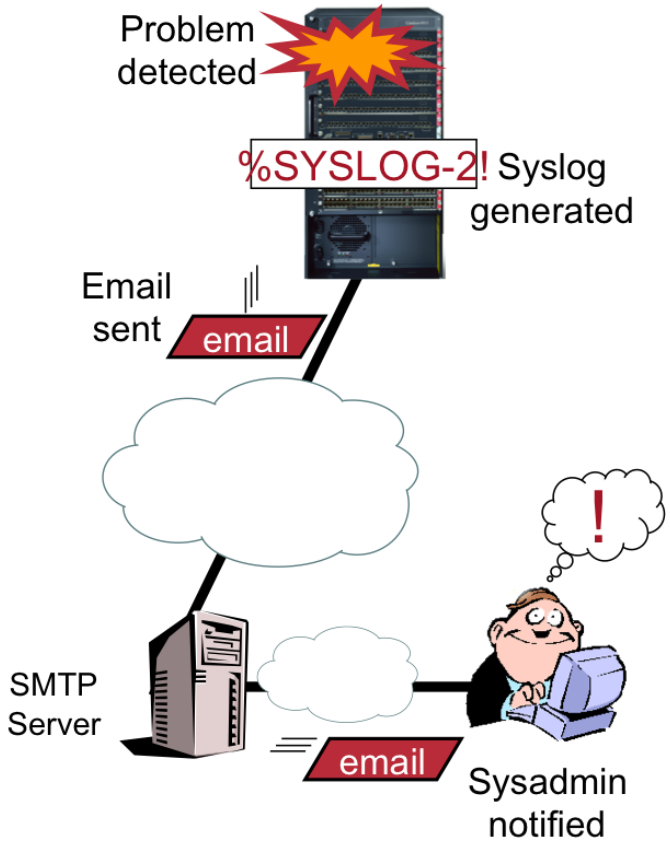
Упрощенный поиск неисправностей

Call Home

2K-C	3K-C	2K	3K	4K	6K

Функционал автоматического обнаружения и уведомления о выявленных неисправностях на базе GOLD

- Автоматическое обнаружение и уведомление о критических системных событиях → email, web-портал
- Автоматический сбор критичной для анализа информации
- Рассылка множеству получателей в необходимом формате, с необходимой информацией
- Открытие кейсов в Cisco TAC



EnergyWise

2K-C	3K-C	2K	3K	4K	6K

Технология, позволяющая отслеживать и автоматически управлять уровнем энергопотребление устройств, подключенных к IP-сети, а также создавать комплексные отчеты по энергопотреблению

- Обширная PoE инфраструктура
- Широкий перечень эко-партнеров
- Эффективное управление энергопотреблением
- Не требует дополнительных вложений
- Возможность расширение → SDK и API (агенты в партнерском оборудовании)

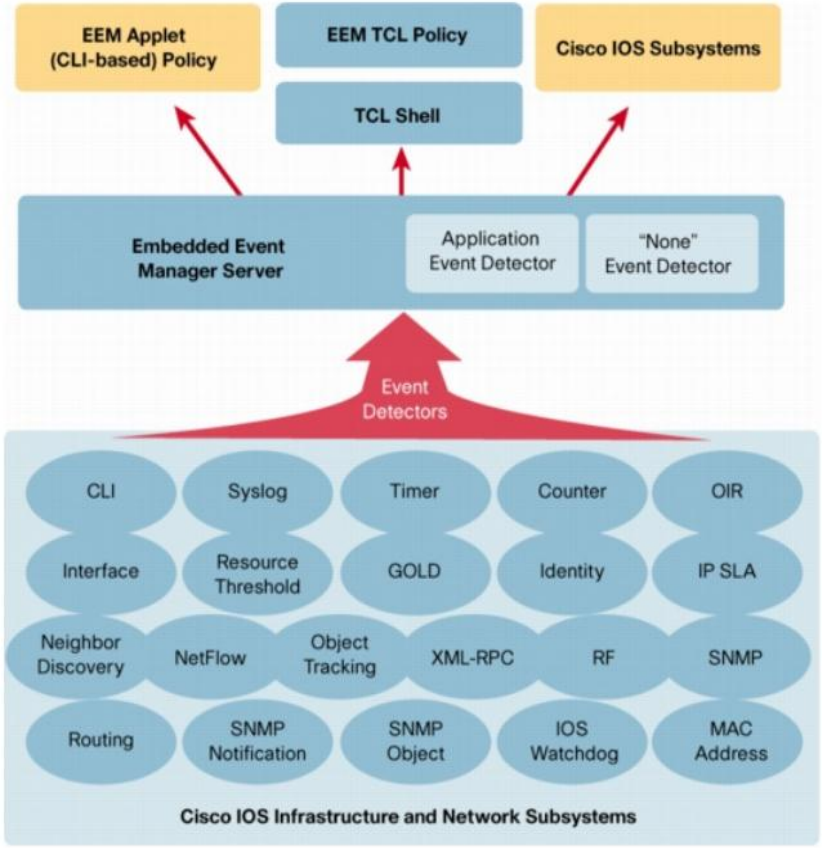
Автоматизация действий

Embedded Event Manager (EEM)

3K-C	3K	4K	6K

Встроенный в IOS функционал, позволяющий коммутатору выполнять автоматизированные действия (политики) при выявлении, в реальном режиме времени, различных событий

- NMS – взгляд снаружи, EEM - взгляд изнутри
- Событие → Менеджер → выполнение политик
- Более 20 детекторов событий, перечень которых постоянно увеличивается
- Программируемые политики поведения на выявленные события (CLI-команды, TCL-скрипты, IOS.sh)
- Высокая производительность – реакция на более чем 100 событий в секунду
- Embedded Event Manager Scripting Community

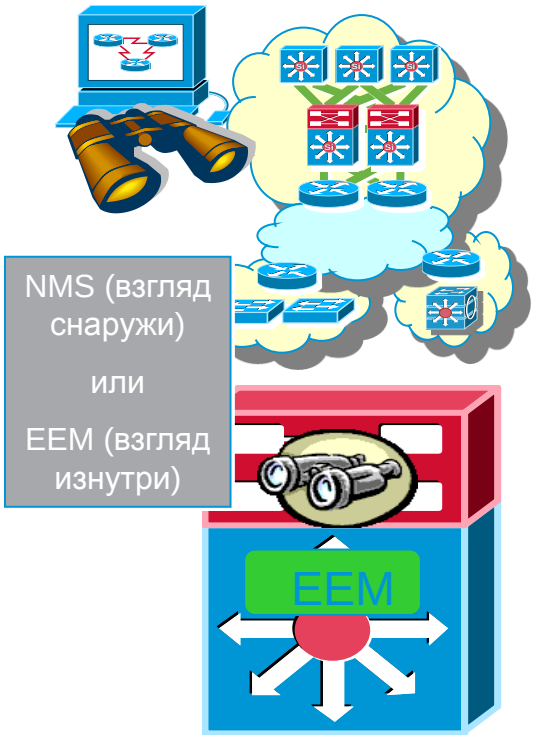


Автоматизация действий
Embedded Event Manager (EEM)

3K-C	3K	4K	6K

Задача: “Отслеживать по email кто, когда и какие изменения делает с ACL на коммутаторе”

Решение: “При обнаружении CLI-команд, связанных с конфигурацией ACL будет запущен скрипт, выполняющий сбор интересующей нас информации и отправки её на указанный email”



MediaNet

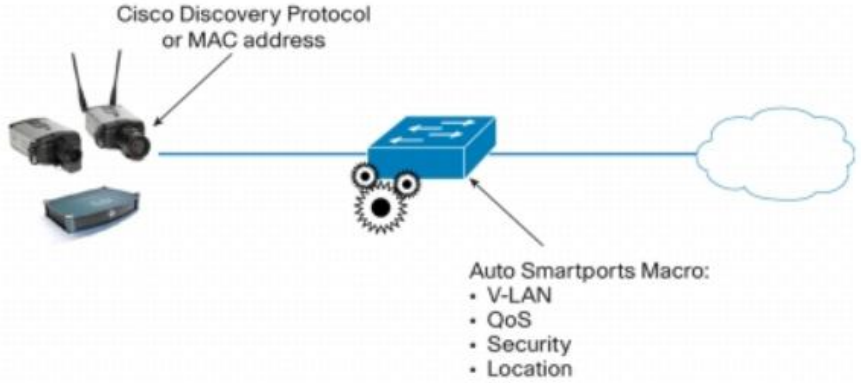
Набор функционала и технологий на сетевом оборудовании и медиа-устройствах, позволяющий реализовать end-to-end сеть оптимизированную для передачи медиа-трафика:

- Понимание устройств
- Понимание сервиса
- Понимание сети

MediaNet

2K-C | 3K-C | 2K | 3K | 4K | 6K

- CDP, MAC – обнаружение устройств
- Auto SmartPorts, Auto QoS – автоконфигурация
- IOS Location – автоматизация конфигурации расположение устройства (DMP, IP-камера)
- Media Services Interface (MSI) – программный компонент на медиа-устройстве (запуск Mediatrace, сбор статистики по производительности)
- NBAR2, FNF – глубокий анализ сетевого трафика для выявления приложений
- IOS Performance Monitor, IOS Mediatrace, IP SLA - сбор статистики о производительности медиа-сервисов, тестирование сети, экспорт для анализа и выявления проблем
- Prime Infrastructure – управление, мониторинг, инвентаризация



Flexible Netflow

3K | 4K | 6K

Технология учета сетевой активности: кто, когда, что, куда и как передает по сети, с возможностью дальнейшего экспортирования для анализа

- Аппаратная реализация с высокой производительностью без влияния на работоспособность системы: 32K, 128K, 1M (13M) flow-записей
- Гибкая конфигурация Flow records
- Поддержка Netflow v9 (наиболее гибкий) формат экспорта для широкого ранга коллекторов
- Глубокая инспекция трафика позволяет анализировать ключевые и не ключевые поля, включая Layer 2, Layer 3 (IPv4 или IPv6), Layer 4 заголовки.
- Реализация нескольких “flow cache” (flow monitor) для различных задач, с их одновременной работой
- Гибкая интеграция с EEM позволяет создавать настраиваемые сценарии реакции на основе обнаруженных событий

Flexible Netflow

3K | 4K | 6K

Flow record – ключевые поля - configurable

Глубокая инспекция трафика позволяет анализировать ключевые и не ключевые поля, включая Layer 2, Layer 3 (IPv4 или IPv6), Layer 4 заголовки

Interface
Input

Layer 2
Dot1q priority
Dot1q Vlan ID
Source MAC address
Destination MAC address

IPv4
Source IP address
Destination IP address
Protocol
Precedence
DSCP
Is-multicast
TTL
Total Length

IPv6
Source IP address
Destination IP address
Protocol
Traffic Class
Flow Label
Total Length
Extension Headers**
DSCP
Next-header**
Hop-Limit
Is-multicast

Transport
ICMP Code
ICMP Type
IGMP Type
TCP Source Port
TCP Destination Port
UDP Source Port
UDP Destination Port

** будущие релизы

Flexible Netflow

3K | 4K | 6K

Flow record – не ключевые поля - configurable

Глубокая инспекция трафика позволяет анализировать ключевые и не ключевые поля, включая Layer 2, Layer 3 (IPv4 или IPv6), Layer 4 заголовки

Counters
Bytes (32 bit counters)
Bytes Long (64 bit counters)
Packets (32 bit counters)
Packets Long (64 bit counters)

Routing
Forwarding Status

IPv4
TTL Minimum
TTL Maximum
Fragmentation Flags
TCP Flags
TOS
First Seen
Last Seen

IPv6
Total Length Minimum
Total Length Maximum
Option Header
Hop-limit minimum
Hop-limit maximum

Flexible Netflow

3K | 4K | 6K

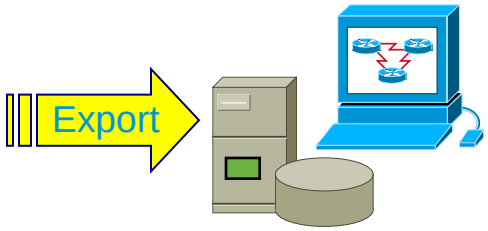
Реализация нескольких “flow cache” (flow monitor) для различных задач, с их одновременной работой

Traditional NetFlow

Fixed 7 keys

NetFlow Cache

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	SrcPort	DstPort
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	00A2	00A2
Fa1/0	173.100.3.2	Fa0/0	10.0.227.12	6	15	15
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	00A1	00A1
Fa1/0	173.100.6.2	Fa0/0	10.0.227.12	6	19	19



Flow Monitor 1

Flow cache 1

DstIPadd	Protocol	TOS
10.0.227.12	11	80
10.0.227.12	6	40
10.0.227.12	11	80
10.0.227.12	6	40

Flow Monitor 2

Flow cache 2

Protocol	TOS	Flgs
11	80	10
6	40	0
11	80	10
6	40	0

Flow Monitor 3

Flow cache 3

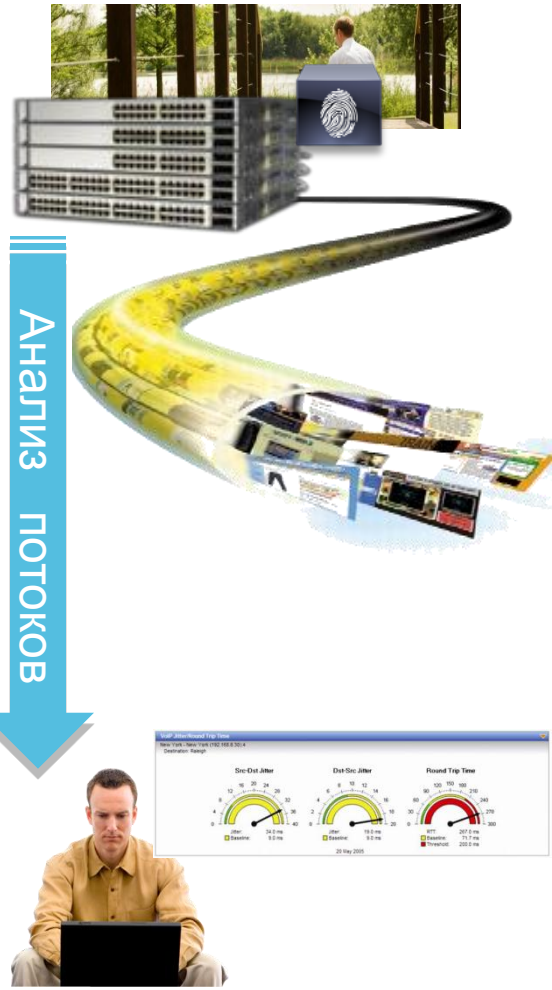
SrcIf	SrcIPadd	DstIf
Fa1/0	173.100.21.2	Fa0/0
Fa1/0	173.100.3.2	Fa0/0
Fa1/0	173.100.20.2	Fa0/0
Fa1/0	173.100.6.2	Fa0/0

Flexible Netflow

Уровень 2 OSI

3K | 4K | 6K

- Только на этом уровне можно получить доступ к такой информации как MAC-адрес, VLAN ID, L2 QoS
- Обнаружение источника потока
- Знание месторасположения устройства
- Идентификация пользователя

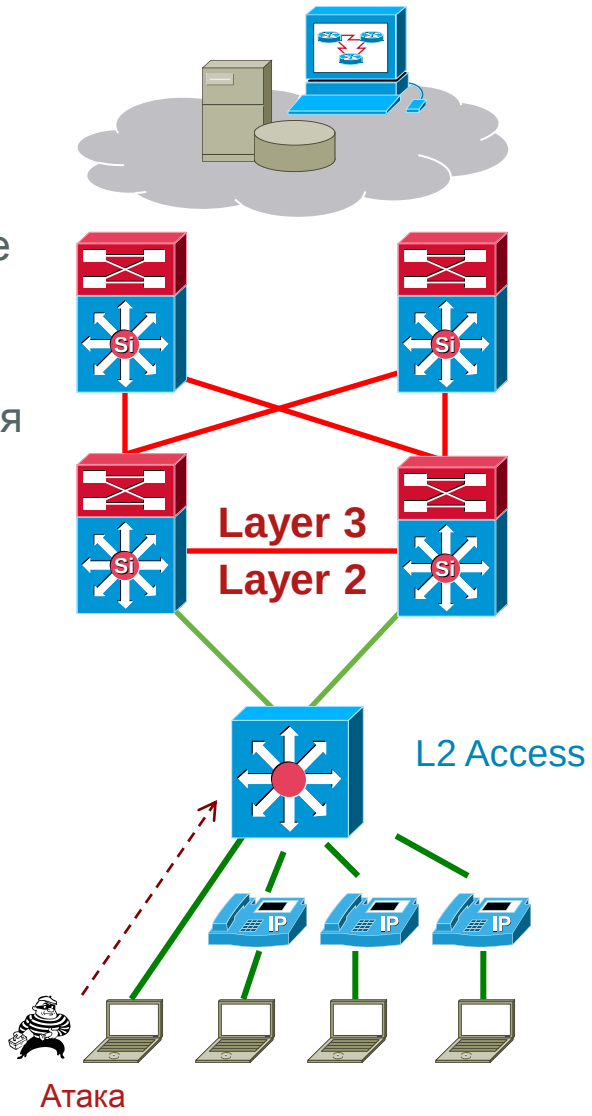


Flexible Netflow

Уровень 2 OSI

3K | 4K | 6K

- Информация из кеша о MAC-адресе и интерфейсе подключения
- Имея информацию о расположении, подключенных к коммутатору устройствах – определяем месторасположение атакующей станции
- Коммутатор доступа экспортирует из кеша информацию на коллектор, который по OUI может определить производителя оборудования
- Идентификация пользователя во время доступа к сети



Flow Table – 51 records

Start Active Time	Client Host	Client MAC Address
May 20, 2011 6:51:43 PM (1 minute 59s ago)	10.201.3.62	c4:2c:03:0c:96:86 (Apple)

Interface	Dire...	Current Utilization	Current Traffic (bps)
Gi1/0/10	Outbound	0.11%	1.14M
Gi1/0/10	Inbound	0.01%	140.22k
Te1/1/1	Inbound	0.01%	1.14M

Flexible Netflow

Интеграция с EEM

3K | 4K | 6K

Мониторинга поведения различных приложений для обнаружения аномалий

Пример 1 : Предотвращение аномального трафика

Аномальный объем трафика с IP-телефона

Netflow cache

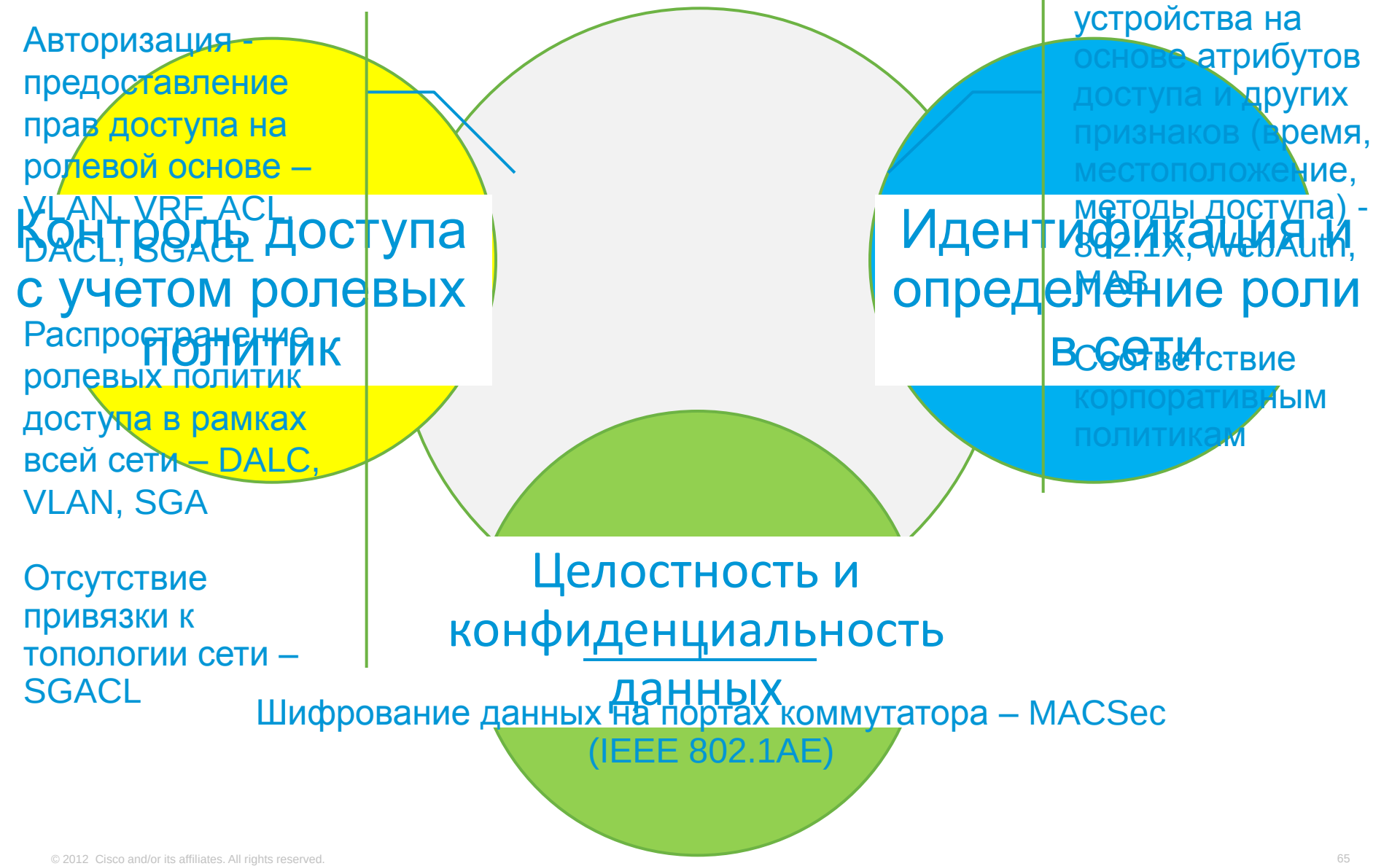
srcIf	SrcIPadd	DstIf	DstIPadd	bytes
Fa1/0	173.1.1.2	Fa0/0	10.0.277.1	34346
Fa1/0	173.1.1.2	Fa0/0	10.0.277.1	300
Fa1/0	173.1.1.2	Fa0/0	10.0.277.1	1000

NetFlow ED triggers policies to monitor flow rate. Typically, voice conversations are 64kbps

```
*Feb 18 01:24:30.455: %LINK-5-
CHANGED: Interface FastEthernet
1/0, changed state to
administratively down
```

interface Fa1/0 is shut down when the flow rate exceeds 100Kbps

C6K Sup2T - TrustSec



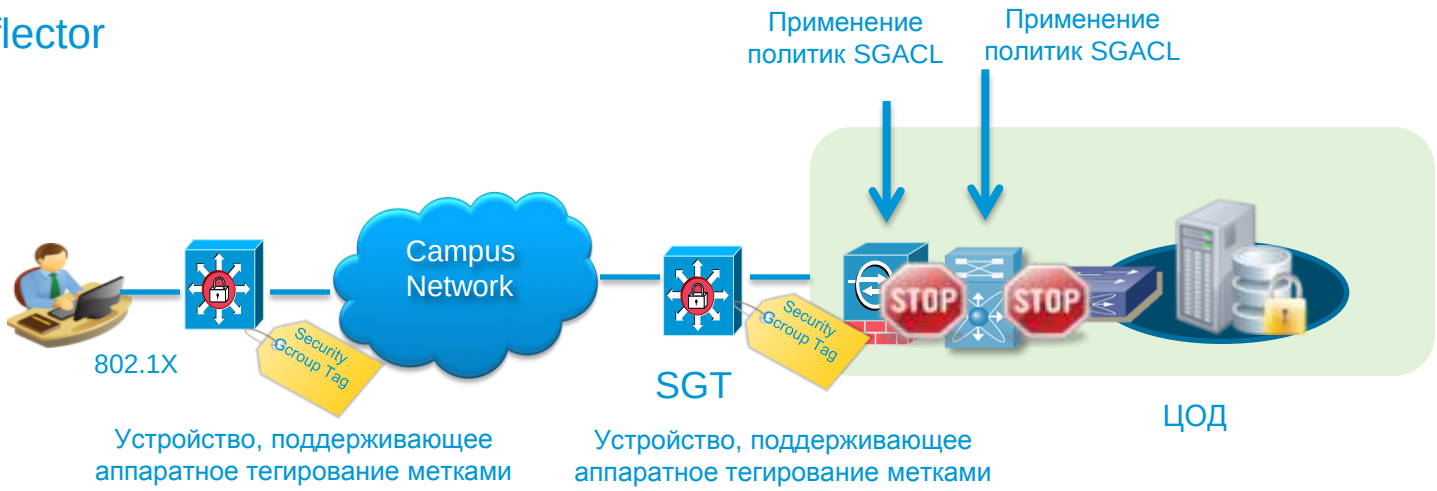
TrustSec

Security Group Tags (SGT)
Security Group Access Control Lists (SGACL)

3K 6K

Метод организация ролевого сетевого доступа на базе меток, присвоенных на аппаратном уровне

- Security Group Tag (SGT) - идентификационная метка, которой тегируются все пакеты пользователя для организации ролевого сетевого доступа
- Не зависит от топологии сети
- SGT отображают роль пользователя / устройства в сети
- Security Group ACLs реализуют политику доступа на основе анализа меток (SGT), присвоенных пакетам пользовательского трафика либо сетевым устройствам
- TrustSec Reflector



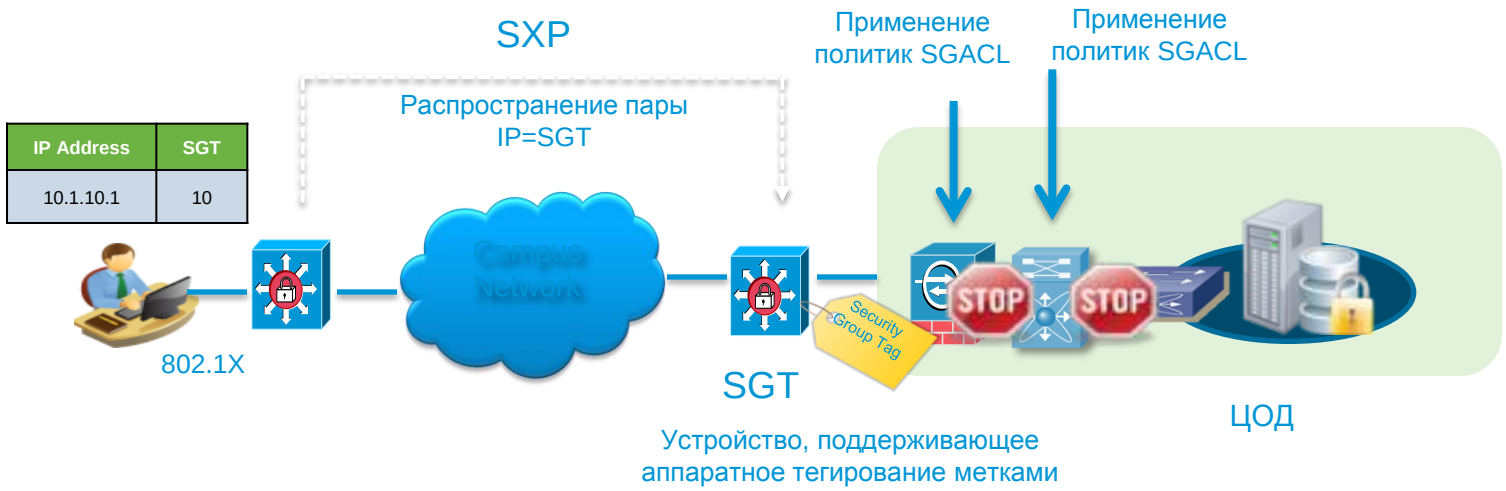
TrustSec

SGT Exchange Protocol (SXP)

3K | 4K | 6K

Протокол, разработанный для передачи соответствия “IP-адрес = метка групповой безопасности (SGT)” от сетевых устройств, которые аппаратно не поддерживают тегирования метками тем устройствам, которые это делают

- Тег групповой безопасности (SGT) назначается на основе идентификационных атрибутов (имя пользователя, местоположение, состояния устройства, тип подключения, тип устройства)
- При помощи протокола SXP эта пара передается на ближайшее устройство, способное выполнять аппаратное тегирование



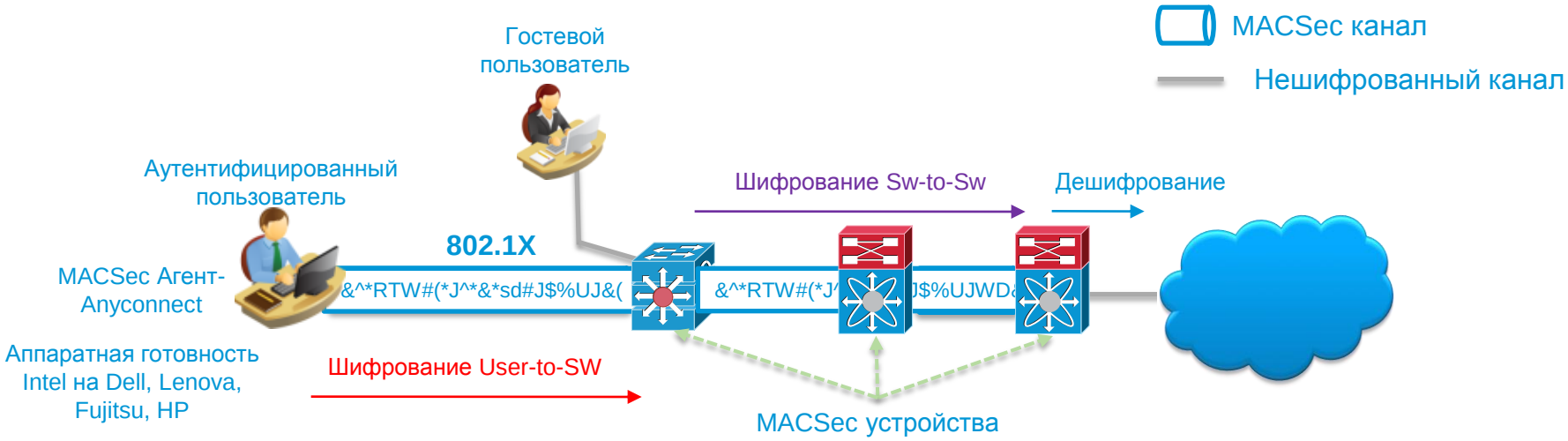
TrustSec

MAC Security (MACsec)
IEEE 802.1AE

User-to-Switch	3K-C	3K	4K	
Switch-to-Switch	3K-C	3K	4K	6K

Технология, обеспечения шифрования (AES-128) на канальном уровне (L2) в соответствии со стандартом IEEE 802.1AE

- Скорость шифрования = канальной скорости
- Шифрование на пользовательских портах (User-to-Switch)
- Шифрование на внешних портах (Switch-to-Switch)



Позиционирование оборудования

Коммутаторы доступа

Catalyst Compact Switches
Компактный L2/L3 коммутатор для предоставления возможностей подключения вне коммутационных комнат, с обеспечение актуальных на сегодня для бизнеса сетевых сервисов и простотой эксплуатации

Позиционирование

Розничная торговля

Производство

Здравоохранение

Образование

Развлекательный и гостиничный бизнес

Офисные рабочие места

Переговорные комнаты

Инновации, уникальная совокупность функционала

EnergyWise
MACSec
Embedded Event Manager
Location
PoE pass-through
Cisco TrustSec SXP v2

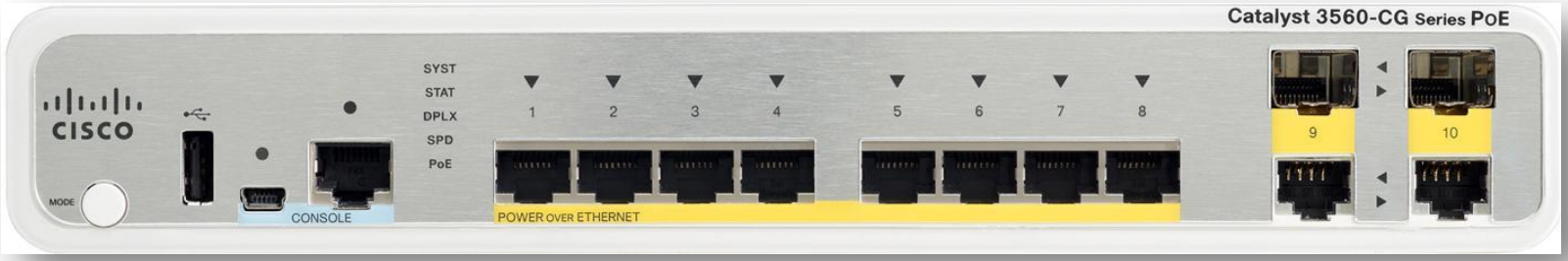
PoE+/UPOE
CWDM

USB storage&console

AutoInstall
AutoSmartPort
Call Home
GOLD

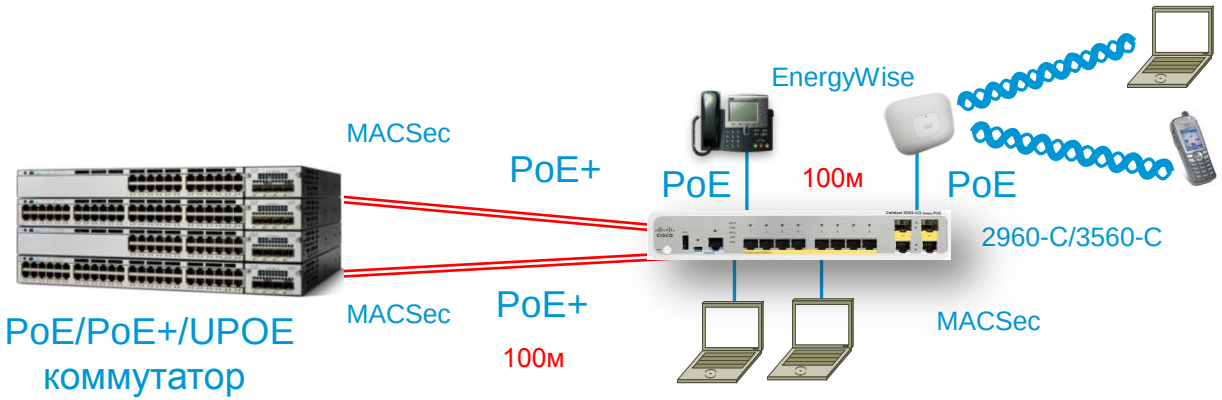
Catalyst 2960-C, 3560-C

- Бесшумный (отсутствует вентилятор)
- Неблокируемая коммутация на всех портах (line rate)
- Встроенный БП или внешний адаптер
- Доступ (гибкость):
  - 8/12 x 10/100 Мбит/с
  - 8 x 10/100/1000 Мбит/с
- Внешние порты (отказоустойчивые):
  - 2 x 1 Гбит/с медь
  - 2 x 1 Гбит/с combo (медь, оптика)
- USB порты для внешнего устройства хранения данных и локальной конфигурации (удобство локального администрирования)



Catalyst 2960-C, 3560-C

- Питание от PoE/PoE+/UPOE (технология PoE pass-through) с питанием подключенных устройств
- PoE/PoE+ IEEE 802.3at (30 Вт) на пользовательских портах (PoE - 124 Вт)
- EnergyWise - для управления энергопотреблением на уровне физического порта
- MACSec – аппаратное шифрование на L2 (IEEE 802.1AE) на пользовательских портах и внешних портах (3560-C); Cisco TrustSec SXP v2 (2960-C, 3560-C)
- MediaNet - автоконфигурация медиа-устройств, отслеживание их месторасположения, применение политик
- Широкий перечень поддерживаемых SFP (CWDM – сохранение инвестиций в оптику)



Коммутаторы доступа

Catalyst 2960-S/2960-SF

Безопасный, масштабируемый, сервисный коммутатор L2+, сочетающий в себе простоту эксплуатации и расширенный сетевой функционал

Позиционирование

Уровень L2 доступа объектов корпоративного и среднего уровней бизнеса:

- Центральный офис
- Удаленные офисы (регион, область, район)
- Данные, голос

Инновации, уникальная совокупность функционала

EnergyWise
Location
Cisco TrustSec SXP v2

24xPoE+ без external PS

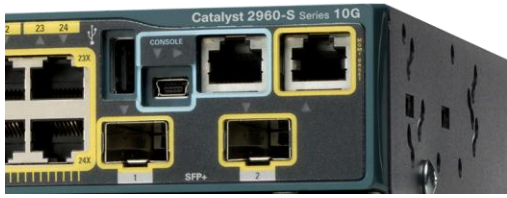
FlexStack
1/10G на одной платформе

Redundant PS (RPS)
CWDM

USB storage&console
Out-of band-management

AutoInstall
AutoSmartPort
Call Home
GOLD

Catalyst 2960-S/2960-SF



- Доступ:

- 24/48 x 10/100/1000 Мбит/с

- 24/48 x 10/100 Мбит/с

- Внешние порты (встроенные):

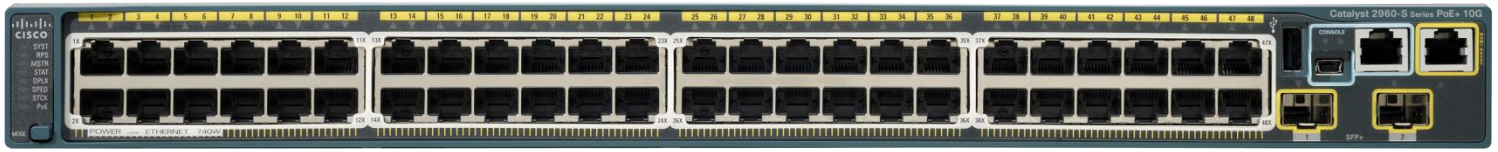
- 4 x 1 Гбит/с, SFP

- 2 x 1 Гбит/с, SFP / 2 x 10 Гбит/с, SFP+ (миграция)

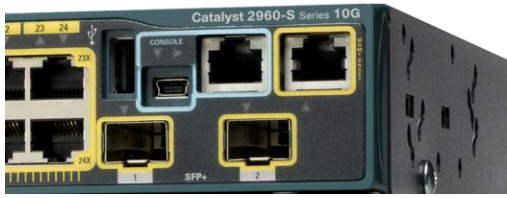
- Стек (2960-S/SF LAN Base): 20 Гбит/с (технология FlexStack)

- Выделенный порт для управления (безопасность)

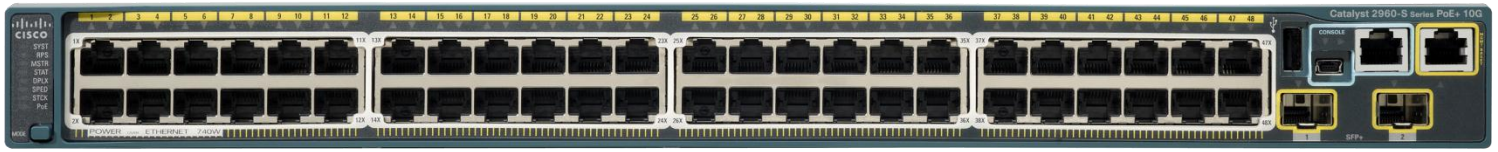
- USB порты для внешнего устройства хранения данных и локальной конфигурации



Catalyst 2960-S/2960-SF



- PoE+ IEEE 802.3at (30 Вт) - 24 порта без внешних систем
- Поддержка резервируемое питания за счет RPS
- EnergyWise - для управления энергопотреблением на уровне физического порта
- Cisco TrustSec SXP v2
- MediaNet - автоконфигурация медиа-устройств, отслеживание их месторасположения, применение политик
- Широкий перечень поддерживаемых SFP (CWDM – сохранение инвестиций в оптику)



Коммутаторы доступа, распределения, ядра

Catalyst 3750-X, 3560-X

Безопасный, масштабируемый, отказоустойчивый, L3 коммутатор, сочетающий в себе надежную эксплуатацию и инновационный сетевой функционал

Позиционирование

Уровень L3 доступа объектов корпоративного и среднего уровней бизнеса:

- Центральный офис

- Удаленные офисы (регион, область)

Повышенная отказоустойчивость и масштабируемость

Данные, голос видео, VDI/VXI

Инновации, уникальная совокупность функционала

EnergyWise
MACSes (downlink, uplink)
TrustSec – SXP
Flexible Netflow
MediaNet - Location, IPSLA VO

48xPoE+ без external PSU
Redundant PS + support RPS
StackWisePlus
StackPower

1/10G на одной платформе
CWDM/DWDM, DOM
USB storage&console
Out-of band-management

AutoInstall
AutoSmartPort
Call Home,GOLD
Embedded Event Manager

Catalyst 3750-X, 3560-X

- Доступ:
  - 24/48 x 10/100/1000 Мбит/с
  - 12/24 x 100/1000, GE SFP (GLC-GE-100FX-экономия)
- Внешние порты (на модулях):
  - 4 x 1 Гбит/с, SFP
  - 2 x 10 Гбит/с, SFP+ или 2 x 1 Гбит/с, SFP (экономия)
  - 2 x 10 Гбит/с Base-T
    (55м – Cat6,100м-Cat7a, 7, 6a - экономия)
- Стек (3750-X): 64 Гбит/с (технологи StackWisePlus)
- Выделенный порт для управления
- USB порты для внешнего устройства хранения данных и локальной конфигурации
- PoE+ IEEE 802.3at (30 Вт) - 48 портов без внешних систем
- Отказоустойчивость: БП, вентиляторные блоки
- Поддержка RPS

Catalyst 3750-X, 3560-X

- Стек по питанию (3750-X) - технологи StackPower
- EnergyWise - для управления энергопотреблением на уровне физического порта
- TrustSec – SXP, SGT (ограничено)
- MACSec – аппаратное шифрование на L2 (IEEE 802.1AE) на пользовательских портах и внешних интерфейсах
- Flexible NetFlow – расширенный функционал аппаратной реализации NetFlow с поддержкой 32000 записей
- MediaNet – автоконфигурация медиа-устройств, отслеживание их месторасположения, применение политик, тестирования сети на готовность к video
- Широкий перечень поддерживаемых SFP (CWDM/DWDM, DOM)

Коммутаторы распределения, ядра

Catalyst 4500-E/4500-X

Безопасный, модульный, отказоустойчивый, с централизованной архитектурой коммутации, инновационным аппаратным и программным функционалом

Позиционирование

Центральный офис:

- Уровень L2/L3 доступа/агрегация для уровня корпоративного бизнеса

- Ядро для уровня среднего бизнеса

Инновации, уникальная совокупность функционала

Отказоустойчивость
Модульная ОС
NSF/SSO
ISSU

POE+ (30 Вт)
UPOE (60 Вт)

EnergyWise
TrustSec-SXP
MACSec
Flexible NetFlow
MediaNet - Location

AutoInstall
AutoSmartPort
Call Home
GOLD
Embedded Event Manager

Catalyst 4500-E/4500-X

- Фиксированная архитектура (1/10G) – 8,16, 32, 40 портов
- Модульная архитектура (3, 6, 7,10)
- Модульная ОС (сосуществование third-party приложений)
- Централизованная архитектура коммутации
- Производительность коммутации – до 848 Гбит/с
- Скорость подключения линейных карт – 48 Гбит/с

- Отказоустойчивость: CPU, БП, вентиляторные блоки
- In-Service Software Upgrade (ISSU) < 200 ms
- Nonstop Forwarding / Stateful Switchover (NSF/SSO)
- PoE+ IEEE 802.3at (30 Вт) – на 148 портах (при 1 x 6 КВт БП)
- Универсальное PoE+ (60 Вт) – на 74 портах (при 1 x 6 КВт БП)

Catalyst 4500-E/4500-X

- EnergyWise - для управления энергопотреблением на уровне физического порта
- TrustSec – SXP
- MACSec – аппаратное шифрование на канальном уровне (IEEE 802.1AE)
- MediaNet – автоконфигурация медиа-устройств, отслеживание их месторасположения, применение политик
- Flexible NetFlow – расширенный функционал аппаратной реализации NetFlow с поддержкой 128000 записей

Коммутаторы ядра

Catalyst 6500-E

Безопасный, модульный, полностью отказоустойчивый, высокопроизводительный, виртуализированный, наиболее инновационный и передовой коммутатор

Позиционирование

Центральный офис:

- Ядро для уровня корпоративного бизнеса

ЦОД:

- Сервисный уровень

Инновации, уникальная совокупность функционала

Отказоустойчивость
Модульная ОС
NSF/SSO
ISSU
VSS, VSS 4T

POE+ (30 Вт)
EnergyWise

TrustSec-SXP
TrustSec – SGT/SGACL
MACSec
Flexible NetFlow
MediaNet - location

AutoInstall
AutoSmartPort
Call Home
GOLD
Embedded Event Manager

Catalyst 6500-E

- Модульная архитектура (3, 4, 6, 9, 13)
- Модульная ОС
- ★ Virtual Switching System (VSS)
- Централизованная или распределенная (DFC) архитектура коммутации
- ★ Производительность коммутации – 2 Тбит/с (4 Тбит/с - VSS)
- ★ Скорость подключения линейных карт – 80 Гбит/с
- Плотность портов - 180 x 10 Гбит/с и 534 x 1 Гбит/с (360 x 10 Гбит/с и 1068 x 1 Гбит/с - VSS)
- Отказоустойчивость: CPU, БП, вентиляторные блоки
- ★ In-Service Software Upgrade (ISSU)
- ★ Nonstop Forwarding / Stateful Switchover (NSF/SSO)
- PoE, IEEE 802.3af (15.4 Вт) – на 500+ портах (при 1 БП)
- PoE+, IEEE 802.3at (30 Вт) – на 250+ портах (при 1 БП)

Catalyst 6500-E

- EnergyWise - для управления энергопотреблением на уровне физического порта
- TrustSec – SGT/SGACL, SXP, Reflector
- MACSec – аппаратное шифрование на канальном уровне (IEEE 802.1AE)
- MediaNet – автоконфигурация медиа-устройств, отслеживание их месторасположения, применение политик
- Flexible NetFlow – расширенный функционал аппаратной реализации NetFlow с поддержкой 1M записей (13M на шасси)

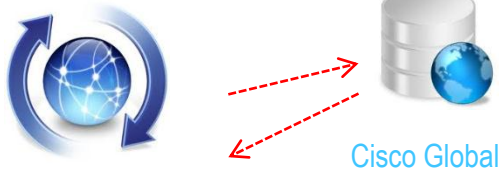
Cisco Smart Business Architecture (SBA)

SBA (Design Zone for Smart Business Architecture)

- Customer access: http://www.cisco.com/go/sba
- Partner access: http://www.cisco.com/go/sbachanne

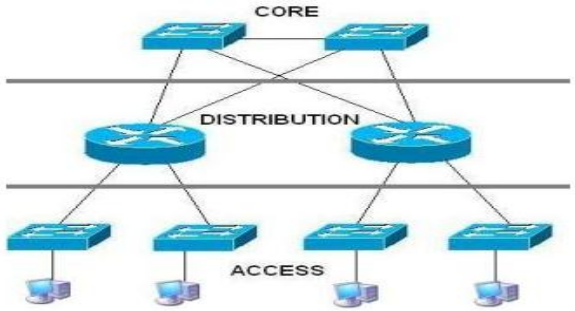
SmartCare

Support Dashboard



Software Module

Cisco Global Support DB



Cisco Network

24/7 Мониторинг сети
- Инвентаризация
- Нагрузка
- Производительность
- Ошибки
- Сбои

Автоматизированные уведомления об инцидентах по электронной почте
- Полуавтоматическая диагностика

Автоматическая подготовка информации
- Доступность сервисов
- Инвентаризация
- Версионность
- Бреши в защите
- Filed Notices

И, конечно, TAC, новые версии ПО, замена оборудования.

Thank you.