

Поддержка устаревших протоколов на Catalyst 4000 Supervisor III / IV

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[IPX-маршрутизация](#)

[Поддерживаемые характеристики](#)

[Ограничения](#)

[Маршрутизация AppleTalk](#)

[Поддерживаемые характеристики](#)

[Ограничения](#)

[Маршрутизация с помощью внешнего маршрутизатора](#)

[Дополнительные методы повышения производительности](#)

[DLSw](#)

[Пакеты не-IP фильтрации с расширенными списками доступа к MAC-адресам и СХЕМАМИ](#)

[VLAN](#)

[Прочие неподдерживаемые функции](#)

[Высокая загрузка CPU после включения IPX или AppleTalk маршрутизации](#)

[Дополнительные сведения](#)

Введение

В этом документе описывается, почему такие традиционные протоколы, как IPX, AppleTalk и DLSw, наилучшим образом поддерживаются в коммутаторе Catalyst 4000/4500, оборудованном новейшим модулем Supervisor III/IV. Это Supervisor I, разработанные к IP версии 4 аппаратного коммутатора (IPv4) пакеты.

Предварительные условия

Требования

Читатели данной документации должны ознакомиться с тем, как настроить IPX, AppleTalk и DLSw. Для получения информации об этих протоколах обратитесь к этим страницам технической поддержки:

- [Страница поддержки технологии IPX](#)

- [Страница поддержки технологии AppleTalk](#)
- [Страница поддержки технологии DSLw](#)

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Catalyst 4507R с Supervisor IV
- Релиз 12.1 программного обеспечения Cisco IOS (13) EW

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.](#)

IPX-маршрутизация

Маршрутизация IPX поддерживается в Cisco IOS Software Release 12.1 (12c) EW и позже. В начальном релизе производительность находится в диапазоне 20 - 30 kpps; с программного обеспечения Cisco IOS версии 12.1(13)EW это было увеличено до 80 - 90 kpps.

Рекомендуется использовать программное обеспечение Cisco IOS версии 12.1(19)EW или позже из-за доступности исправления программного обеспечения для [идентификатора ошибки Cisco CSCea85204 \(только зарегистрированные клиенты\)](#). Эта скорость переадресации разделена всеми потоками, которые выполняют коммутатор. Эта передача увеличивает Загрузку ЦПУ из-за обработки программного обеспечения. Также, достигнутая скорость переадресации зависит от ЦП коммутатора; например, сколько политики Протокола BGP, Протокола EIGRP или маршрутов Протокола OSPF и Коммутируемых виртуальных интерфейсов (SVI), которые имеет коммутатор.

Примечание: Пакеты IPV4 продолжают маршрутизироваться в аппаратных средствах, даже при том, что пакеты IPX программно маршрутизуемы.

Поддерживаемые характеристики

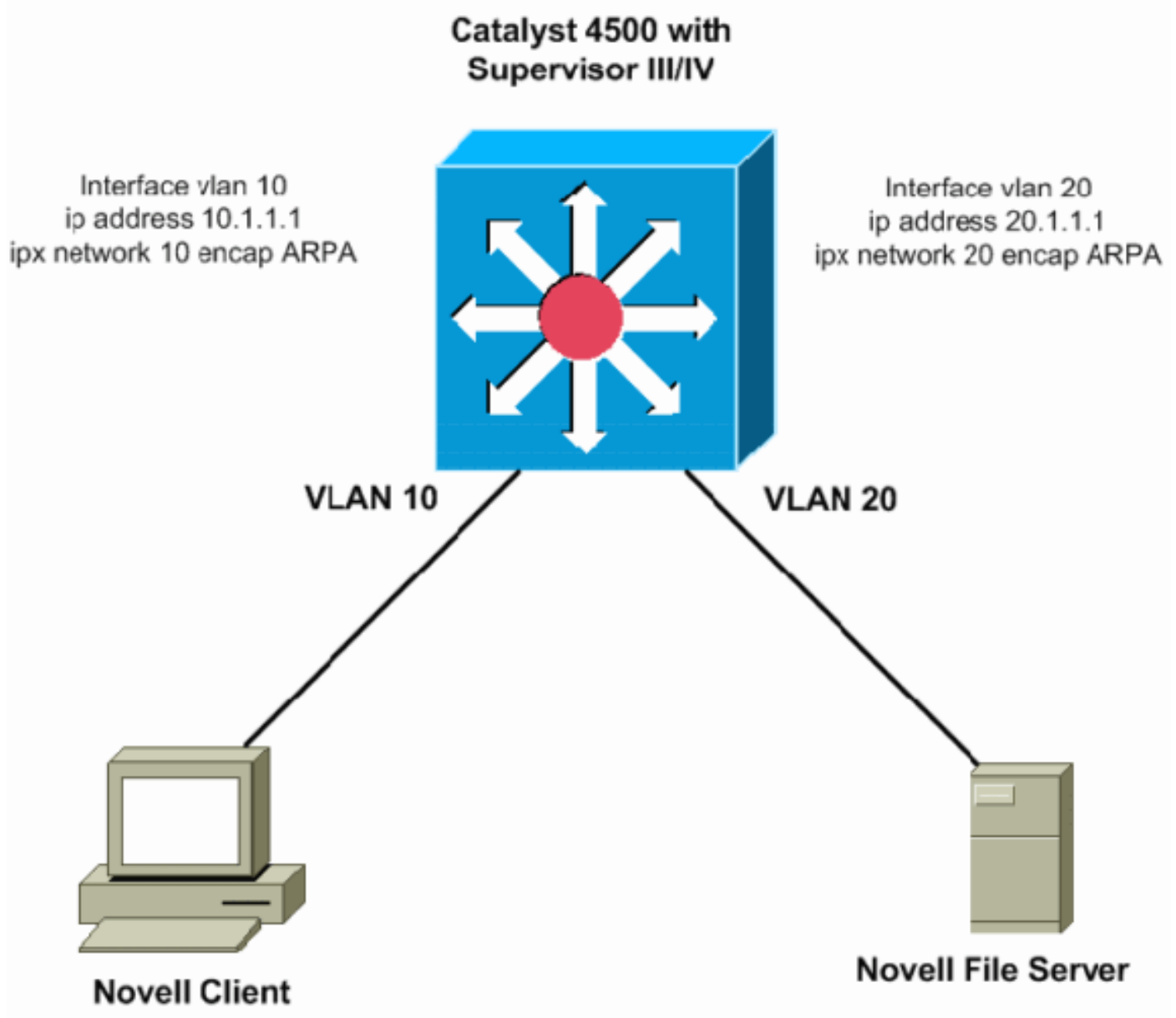
- Список контроля доступа (ACL) MAC для IPX поддерживается в Cisco IOS Software Release 12.1 (12c) EW и позже, который может использоваться для управления пакетами IPX.
- Протокол информации ipx - маршрутизации (RIP) (протокол объявления служб [SAP])
- Протокол EIGRP IPX
- сжатие заголовка

Примечание: EIGRP IPX является протоколом предпочитаемого протокола маршрутизации между маршрутизаторами для лучшей производительности, поскольку EIGRP делает обновления SAP с приращением. EIGRP IPX может быть включен на бессерверных сегментах. Для получения информации о EIGRP IPX обратитесь к [Пониманию IPX-EIGRP](#).

Ограничения

- Аппаратное обеспечение не принимает участия в маршрутизации пакетов IPX. Это делается с помощью программных средств обработки.
- Стандарт Novell IPX (800-899), IPX расширился (900-999), Получить самый близкий сервер (GNS) или фильтры SAP (1000-1099), списки доступа в настоящее время не поддерживаются.
- Для маршрутизации программного обеспечения IPX они не поддерживаются: Протокол разрешения следующего скачка (NHRP) Протокол служб связей Netware (NLSP) кадры большого размера

Этот рисунок иллюстрирует типичный сценарий с IPX маршрутизации Catalyst 4000/4500 с модулем Supervisor III/IV. В этом сценарии клиенты находятся в VLAN 10, и серверы находятся в VLAN 20. IPX настроен на VLAN 10 и 20 интерфейсах, как показано в этой схеме:



Маршрутизация AppleTalk

Маршрутизация AppleTalk поддерживается в Cisco IOS Software Release 12.1 (12c) EW и

позже. В начальном релизе производительность находится в диапазоне 20 - 30 kpps; с программного обеспечения Cisco IOS версии 12.1(13)EW это было увеличено до 80 - 90 kpps. Рекомендуется использовать программное обеспечение Cisco IOS версии 12.1(19)EW или позже из-за доступности исправления программного обеспечения для [идентификатора ошибки Cisco CSCea85204 \(только зарегистрированные клиенты\)](#). Эта скорость переадресации разделена всеми потоками, которые выполняют коммутатор. Эта передача увеличивает Загрузку ЦПУ из-за обработки программного обеспечения. Также, достигнутая скорость переадресации зависит от ЦП коммутатора: например, сколько политики BGP, EIGRP или маршрутов OSPF и SVI, которые имеет коммутатор.

Примечание: Пакеты IPv4 продолжают маршрутизироваться в аппаратных средствах, даже при том, что Пакеты AppleTalk программно маршрутизуемы.

Поддерживаемые характеристики

- ACL MAC для AppleTalk поддерживается в Cisco IOS Software Release 12.1 (12c) EW и позже, который может использоваться для управления пакетами IPX.
- Маршрутизация протокола доставки дейтаграмм (DDP)
- Протокол обслуживания таблицы маршрутизации (RTMP)
- Протокол присвоения имен (NBP)
- Протокол AppleTalk Echo (AEP)
- AppleTalk EIGRP

Примечание: AppleTalk EIGRP является протоколом предпочитаемого протокола маршрутизации между маршрутизаторами для лучшей производительности, поскольку EIGRP делает инкрементные обновления. Для получения дополнительной информации о AppleTalk EIGRP, обратитесь к разделу [Расширенного IGRP AppleTalk Настройки AppleTalk Настройки](#).

Ограничения

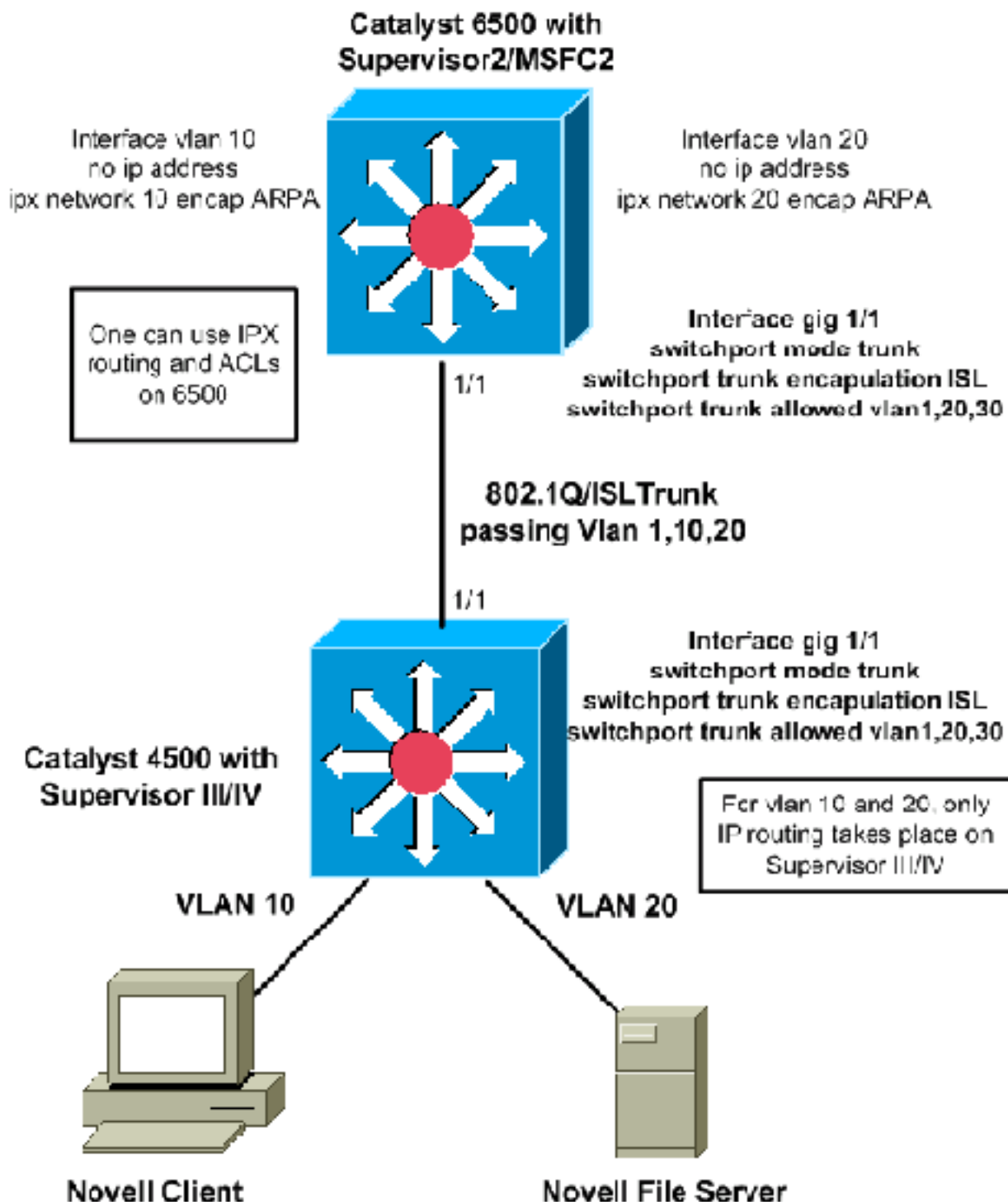
- Для маршрутизации пакетов AppleTalk оборудование не используется. Это делается с помощью программных средств обработки.
- ACL AppleTalk в настоящее время не поддерживаются.
- Для маршрутизации программного обеспечения AppleTalk они не поддерживаются: Протокол маршрутизации на основе обновления AppleTalk (AURP) Протокол управления AppleTalk для PPP кадры большого размера

Маршрутизация с помощью внешнего маршрутизатора

Если ваша сеть требует лучшей производительности маршрутизации устаревших протоколов, тогда ранее упомянутых, можно хотеть использовать внешний маршрутизатор (Уровень 3 [L3] устройство). Таким устройством L3 могла быть Функциональная Карта Многоуровневого Коммутатора (MSFC) Catalyst 6000, Catalyst 5000 RSM, коммутатор L3 (такой как 2948G-L3), или любой маршрутизатор. Эти устройства выполняют маршрутизацию IPX с аппаратным ускорением, производительность намного выше, чем у Supervisor III/IV. Supervisor III / IV может направить IP в пути аппаратной коммутации, но внешнее устройство направляет устаревшие протоколы.

Следующая схема иллюстрирует сценарий, в котором IPX маршрутизируется на Catalyst

6500 ядра/распределения на MSFC, в то время как IP маршрутизируется между VLAN 10 и VLAN 20 в Catalyst 4500 с Supervisor III / IV. Два коммутатора соединены магистралью, который позволяет требуемые VLAN. Преимущество этого типа дизайна является способностью использовать стандартные ACL IPX и увеличение производительности из-за помощи с аппаратными средствами передачи этих пакетов между этими двумя VLAN. Можно также использовать протоколы маршрутизации IPX на Catalyst 6500 или на внешнем маршрутизаторе, для передачи с узлами для обмена базы данных маршрутизации:



[Дополнительные методы повышения производительности](#)

Это разделяет, предоставляет некоторые дополнительные улучшения возможной производительности, которые могут быть сделаны к IPX или к AppleTalk, включающему внешний маршрутизатор.

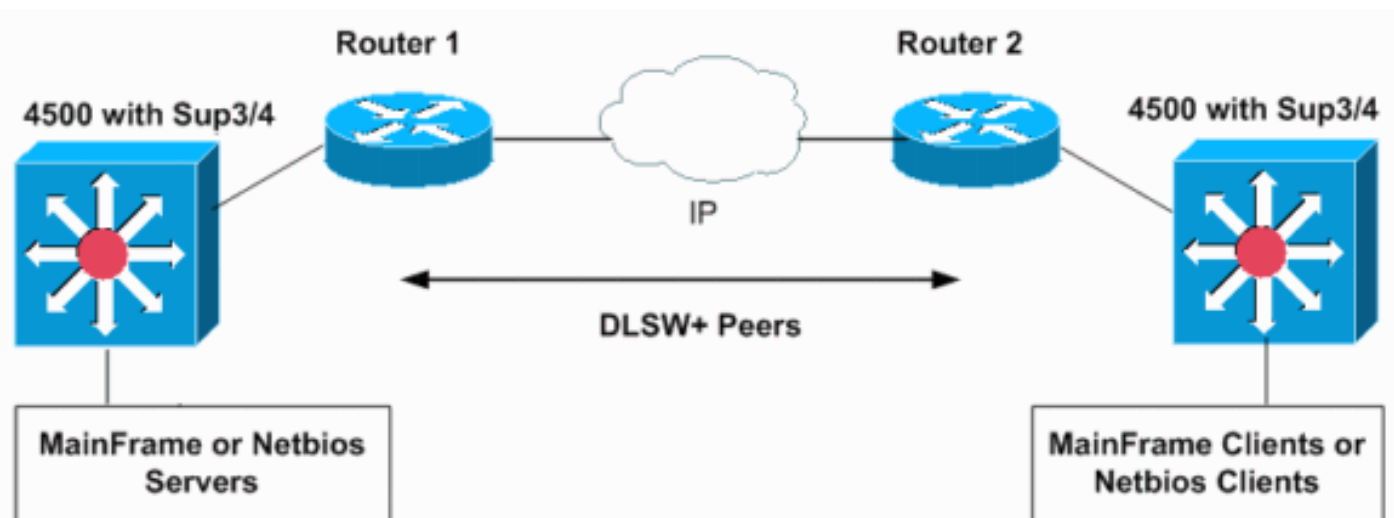
- Ссылка между внешним маршрутизатором и Коммутатором Catalyst могла быть превращена в ссылку port-channel, чтобы получить более высокую пропускную способность между ними и иметь резервирование для ссылки.
- IP - трафик может фильтроваться из ссылки так, чтобы вся пропускная способность использовалась для не-IP трафика. Это - пример конфигурации для отфильтровывания IP - трафика через Качество обслуживания (QoS):

1. Выполните **qos** команды глобальной конфигурации QoS, для включения QoS на Супервизоре.
2. Определите ACL для соответствия со всем IP - трафиком.
`access-list 101 permit ip any any`
3. Определите class-map, который совпадает с ACL, определенным в Шаге 2.
`class-map match-any ip-drops`
`match access-group 101`
4. Определите политику: определите ограничитель, который отбросит весь трафик для класса, определенного в Шаге 3. Определите политику всего трафика с помощью минимальной глубины детализации 32 кбит/с. Супервизор отбросит весь IP - трафик с этим внешним ограничителем 32 кбит/с (эхо-запросы IP Cisco IOS могут не быть в состоянии пройти).
`policy-map drop-ip`
`class ip-drops`
`police 32000 bps 1000 byte conform-action drop exceed-action drop`
5. Примените политику обслуживания, исходящую на интерфейс, который соединяется с внешним маршрутизатором.
`interface GigabitEthernet 1/1`
`service-policy output drop-ip`

Для проверки действия применения политик выполните команду `interface-id show policy-map interface`.

DLSw

DLSw не поддерживается на Supervisor III / IV. Для сетей с SNA и Протоколами "IP", можно направить IP - трафик на III/IV Catalyst 4000 Supervisor и соединить трафик SNA с DLSw, включающим программное обеспечение Cisco IOS на внешнем маршрутизаторе:



Следующие конфигурации показывают, как соединить трафик SNA на VLAN 10 и 20 на двух MSFC2 Catalyst 6500 в двух отдельных доменах SNA. Магистралы "802.1q" на Supervisor III / IV могут использоваться для переноса (соединяют) SNA или Трафик NetBIOS к маршрутизатору Cisco или к Коммутаторам Catalyst 6500.

<pre>hostname MSFCRouter-1 interface loopback1 ip address 1.1.1.1 ! int vlan10 ip add 10.10.10.254 255.255.255.0 bridge-group 1 ! bridge 1 protocol ieee dlsw local-peer peerid 1.1.1.1 dlsw remote-peer 0 tcp 2.2.2.2 dlsw bridge-group 1</pre>	<pre>hostname MSFCRouter-2 interface loopback1 ip address 2.2.2.2 ! int vlan20 ip add 10.10.20.254 255.255.255.0 bridge-group 2 ! bridge 2 protocol ieee dlsw local-peer peerid 2.2.2.2 dlsw remote-peer 0 tcp 1.1.1.1 dlsw bridge-group 2</pre>
---	---

Это показывает конфигурации сети для Коммутаторов Catalyst 6500 в других доменах. Если сети VLAN 10 и 20 находятся на одном коммутаторе или MSFC, то DLSw не требуется. Будут работать простые мостовые группы IEEE на одном MSFC.

[Пакеты не-IP фильтрации с расширенными списками доступа к MAC-адресам и СХЕМАМИ VLAN](#)

Supervisor III / IV не поддерживает IPX, AppleTalk или другие ACL устаревшего протокола. Чтобы отфильтровать их, можно использовать ACL, расширенные MAC, в сочетании с картой доступа VLAN. Схемы VLAN могут управлять доступом ко всему трафику VLAN. Можно применить схемы VLAN на коммутаторе ко всем пакетам, направляемым в или из VLAN, а также через мосты в пределах VLAN. В отличие от списков управления доступом к маршрутизатору, схемы VLAN не определены направлением (ввод или вывод).

В сценарии данного примера эти два критерия являются целями конфигурирования:

- Запретить IPX-трафик от узла 000.0c00.0111 к узлу 000.0c00.0211, однако при этом разрешить весь трафик протоколов IPX и не-IP через VLAN 20.
- Запрет всего трафика AppleTalk для VLAN 10.

Примечание: В пакеты IP нельзя проникнуть ACL MAC.

Примечание: Названные расширенные списки ACL MAC не могут быть применены к L3 интерфейсам.

1. Определите расширенные списки доступа к MAC-адресам для определения представляющего интерес трафика для схем VLAN.


```
Switch(config)# mac access-list extended denyIPXACL
Switch(config-ext-macl)# permit host 000.0c00.0111 host 000.0c00.0211
protocol-family ? appletalk arp-non-ipv4 decnet ipx ipv6 rarp-ipv4 rarp-non-ipv4 vines xns
Switch(config-ext-macl)# $00.0c00.0111 host 000.0c00.0211 protocol-family ipx
Switch(config-ext-macl)# exit
Switch(config)# mac access-list extended denyatalk
Switch(config-ext-macl)# permit any any protocol-family appletalk
Switch(config)#
```
2. Выполните команду *access-list-name show access-list* для проверки настроенного расширенного списка доступа к MAC-адресам. ACL в предыдущем примере является denyIPXACL и denyatalk.


```
Switch# show access-lists denyIPXACL
Extended MAC access list
denyIPXACL permit host 0000.0c00.0111 host 0000.0c00.0211 protocol-family ipx
Switch# show access-lists denyatalk
Extended MAC access list
denyatalk permit any any protocol-family appletalk
```

3. Определите действие с картами доступа VLAN.


```
Switch(config)# vlan access-map denyIPX
Switch(config-access-map)# match mac address denyIPXACL
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan access-map denyapple
Switch(config-access-map)# match mac address denyatalk
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
```
4. Выполните команду *названия* `show vlan access-map` для проверки определенного карты доступа VLAN.


```
Switch# show vlan access-map denyIPX
Vlan access-map "denyIPX" 10 Match clauses: mac address: denyIPXACL Action: drop
Switch# show vlan access-map denyapple
Vlan access-map "denyapple" 10 Match clauses: mac address: denyatalk Action: drop
```
5. Выполните команду `vlan-list vlan-list` *названия* `vlan filter` для сопоставления схемы VLAN с VLAN. В данном примере вы хотите фильтровать IPX между определенными хостами в VLAN 20 и запретить AppleTalk на VLAN 10.


```
Switch(config)# vlan filter denyIPX vlan-list 20
Switch(config)# vlan filter denyapple vlan-list 10
```
6. Выполните команду `vlan vlan-id show vlan filter`, чтобы проверить, что существует Vlan filter.


```
Switch# show vlan filter vlan 20
Vlan 20 has filter denyIPX.
Switch# show vlan filter vlan 10
Vlan 10 has filter denyapple.
```

Прочие неподдерживаемые функции

Supervisor III / IV не поддерживает эти функции:

- Мостовое соединение нейтрализации или мостовое соединение между сетями VLAN для мостового соединения немаршрутизируемых протоколов
- Маршрутизация DECnet

См. [предыдущий раздел](#), для наблюдения примера того, как использовать внешний маршрутизатор для достижения этой функциональности.

Высокая загрузка CPU после включения IPX или AppleTalk маршрутизации

После включения IPX или Маршрутизации AppleTalk использование ЦПУ увеличится на основе суммы Трафика IPX или AppleTalk, который маршрутизируется в программном обеспечении через коммутатор. При запуске команды `show processor cpu` выходные данные могут показать, что процесс Cat4k Mgmt LoPri использует ЦП. Это означает, что пакеты коммутируются процессом.

```
Switch# show processes cpu
CPU utilization for five seconds: 99%/0%; one minute: 86%; five minutes: 54%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
1 8 607 13 0.00% 0.00% 0.00% 0 Load Meter
2 496 4549 109 0.00% 0.01% 0.00% 0 Spanning Tree
3 0 1 0 0.00% 0.00% 0.00% 0 Deferred Events
4 4756 480 9908 0.00% 0.08% 0.11% 0 Check heaps
5 0 1 0 0.00% 0.00% 0.00% 0 Chunk Manager
6 0 1 0 0.00% 0.00% 0.00% 0 Pool Manager
7 0 2 0 0.00% 0.00% 0.00% 0 Timers
8 4 2 2000 0.00% 0.00% 0.00% 0 Serial Backgroun
9 4 64 62 0.00% 0.00% 0.00% 0 ARP Input
10 24 3 8000 0.00% 0.00% 0.00% 0 Entity MIB API
11 0 1 0 0.00% 0.00% 0.00% 0 SERIAL A'detect
12 0 1 0 0.00% 0.00% 0.00% 0 Critical Bkgnd
13 25436 864 29439 0.00% 0.00% 0.00% 0 Net Background
14 0 58 0 0.00% 0.00% 0.00% 0 Logger
15 52 2607 19 0.00% 0.00% 0.00% 0 TTY Background
16 440 2666 165 0.00% 0.00% 0.00% 0 Per-Second Jobs
17 112328 410885 273 1.66% 2.37% 2.74% 0 Cat4k Mgmt HiPri
18 1197172 21536 55589 98.56% 84.14% 49.15% 0 Cat4k Mgmt LoPri
19 0 1 0 0.00% 0.00% 0.00% 0
Routekernel Proc
```

Примечание: Если вам не включили IPX или Маршрутизацию AppleTalk, но все еще видели, Cat4k Mgmt LoPri использует высокую загрузку CPU, то вам, вероятно, придется устранить неполадки, какие пакеты переданы к ЦП для обработки. [Обратитесь в техническую поддержку Cisco](#) при необходимости в дальнейшей поддержке.

Дополнительные сведения

- [Настройка сетевой безопасности с ACL](#)
- [Страницы технической поддержки Catalyst 4500](#)
- [Страницы поддержки продуктов LAN](#)
- [Страница поддержки коммутационных решений для локальной сети](#)
- [Cisco Systems – техническая поддержка и документация](#)