

Настройте ASA для передачи трафика IPv6

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Информация о функции IPv6](#)

[Обзор IPv6](#)

[Улучшения IPv6 по сравнению с IPv4](#)

[Расширенные возможности адресации](#)

[Упрощение формата заголовка](#)

[Улучшенная поддержка расширений и опций](#)

[Возможность маркировки потока](#)

[Аутентификация и возможности конфиденциальности](#)

[Настройка](#)

[Схема сети](#)

[Настройте интерфейсы для IPv6](#)

[Настройте маршрутизацию IPv6](#)

[Настройте статичную маршрутизацию для IPv6](#)

[Настройте динамическую маршрутизацию для IPv6 с OSPFv3](#)

[Проверка](#)

[Устранение неполадок](#)

[Устраните неполадки подключения L2 \(ND\)](#)

[ARP IPv4 по сравнению с IPv6 ND](#)

[ND отладки](#)

[ND захваты пакета](#)

[ND системные журналы](#)

[Устраните неполадки основной маршрутизации IPv6](#)

[Отладки протокола маршрутизации для IPv6](#)

[Полезные команды show для IPv6](#)

[Пакетные трассировщики с IPv6](#)

[Полный список связанных с IPv6 отладок ASA](#)

[Общие связанные с IPv6 проблемы](#)

[Неправильно настроенные подсети](#)

[Модифицированное кодирование EUI 64](#)

[Клиенты используют временные адреса IPv6 по умолчанию](#)

[Часто задаваемые вопросы IPv6](#)

[Я могу передать трафик и для IPv4 и для IPv6 на том же интерфейсе в то же время?](#)

[Я могу применить и IPv6 и ACL IPv4 к тому же интерфейсу?](#)

[ASA поддерживает QoS для IPv6?](#)

[Я должен использовать NAT с IPv6?](#)

[Почему я вижу, что локальные для канала адреса IPv6 в команде *show failover* выводят?](#)

[Известные Предупреждения/Запросы на расширение](#)

[Дополнительные сведения](#)

Введение

Этот документ описывает, как настроить устройство адаптивной защиты Cisco (ASA) для передачи трафика Версии 6 (IPv6) Протокола Интернета в Версиях ASA 7.0 (1) и позже.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на Версиях Cisco ASA 7.0 (1) и позже.

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.

Общие сведения

В настоящее время IPv6 является все еще относительно новым с точки зрения проникновения на рынок. Однако помощь по конфигурации IPv6 и устраняющие неполадки запросы постоянно увеличивались. Цель этого документа состоит в том, чтобы обратиться к тем потребностям и предоставить:

- Общий обзор использования IPv6
- Основные конфигурации IPv6 на ASA
- Информация о том, как устранить неполадки подключения IPv6 через ASA
- Список наиболее распространенных проблем IPv6 и решений, как определено Центром технической поддержки Cisco (TAC)

Примечание: Учитывая, что IPv6 находится все еще в ранних стадиях как замена IPv4 глобально, этот документ будет периодически обновляться для поддержания точности и уместности.

Информация о функции IPv6

Вот немного важной информации о функциональности IPv6:

- Протокол IPv6 был сначала представлен в Версии ASA 7.0 (1).
- Поддержка IPv6 в прозрачном режиме была представлена в Версии ASA 8.2 (1).

Обзор IPv6

Протокол IPv6 был разработан в середине к концу 1990-х, прежде всего вследствие того, что общее пространство адреса IPv4 переместилось быстро к истощению. Несмотря на то, что Технология NAT существенно помогла IPv4 и задержала эту проблему, это стало бесспорным, что в конечном счете будет необходим заменяющий протокол. Протокол IPv6 был официально подробно изложен в RFC 2460 в декабре 1998. Можно читать больше о протоколе в официальном [документе RFC 2460](#), расположенном на веб-сайте инженерной группы по развитию Интернета (IETF).

Улучшения IPv6 по сравнению с IPv4

В этом разделе описываются улучшения, которые включены с протоколом IPv6 по сравнению с более старым протоколом IPv4.

Расширенные возможности адресации

Протокол IPv6 увеличивает размер IP-адреса с 32 битов до 128 битов для поддержки большего количества уровней адресации к иерархии, намного большему количеству адресуемых узлов и более простой автоматической конфигурации адресов. Масштабируемость многоадресной маршрутизации улучшена добавлением *поля score* к адресам групповой адресации. Кроме того, новый тип адреса, названного *альтернативным адресом*, определен. Это используется для передачи пакета к любому узлу в группе.

Упрощение формата заголовка

Некоторые поля заголовка IPv4 были отброшены или сделаны дополнительные для сокращения затрат на обработку общего падежа пакетной обработки и для ограничения стоимости полосы пропускания заголовка IPv6.

Улучшенная поддержка расширений и опций

Изменения в способе, которым закодированы опции IP - заголовка, обеспечивают более

эффективную передачу, менее строгие пределы на длине опций и большую гибкость для введения новых опций в будущем.

Возможность маркировки потока

Новая возможность добавлена для включения маркировки пакетов, которые принадлежат потокам отдельного трафика, на которые отправитель запрашивает специальную обработку, такую как Качество обслуживания (QoS) по умолчанию или *сервис реального времени*.

Аутентификация и возможности конфиденциальности

Расширения, которые используются для поддержки аутентификации, целостности данных и (дополнительной) конфиденциальности данных заданы для IPv6.

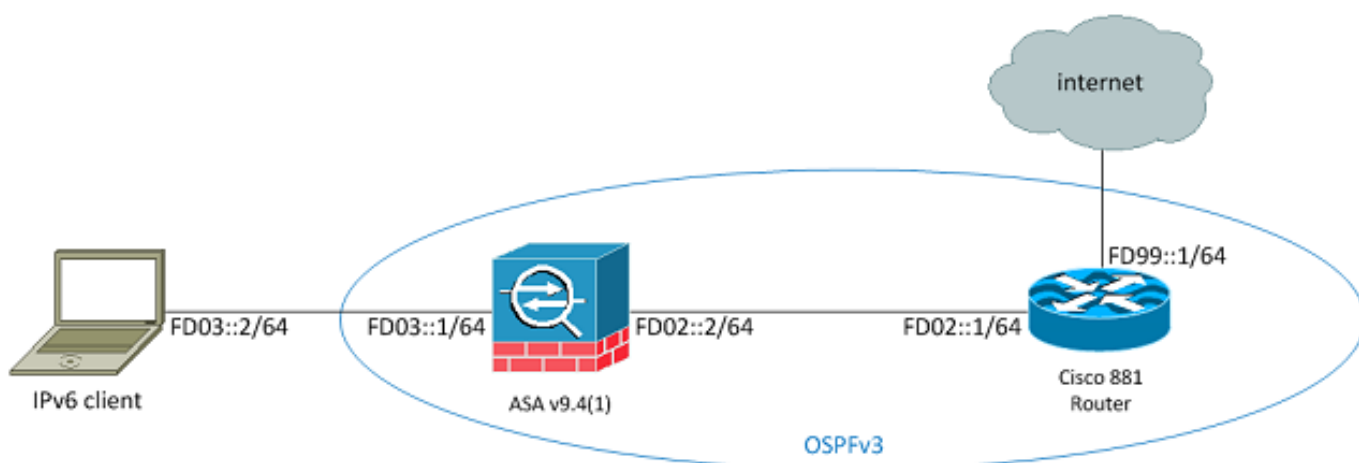
Настройка

В этом разделе описывается настроить Cisco ASA для использования IPv6.

Примечание: [Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд \(только для зарегистрированных клиентов\).](#)

Схема сети

Это - топология IPv6 для примеров, которые используются всюду по этому документу:



Настройте интерфейсы для IPv6

Для передачи трафика IPv6 через ASA необходимо сначала включить IPv6 по крайней мере на двух интерфейсах. Данный пример описывает, как включить IPv6 для передачи трафика

от внутреннего интерфейса на **Gi0/0** к внешнему интерфейсу на **Gi0/1**:

```
ASAv(config)# interface GigabitEthernet0/0
ASAv(config-if)# ipv6 enable
```

```
ASAv(config)# interface GigabitEthernet0/1
ASAv(config-if)# ipv6 enable
```

Можно теперь настроить адреса IPv6 на обоих из интерфейсов.

Примечание: В данном примере используются адреса в пространстве Уникальных локальных адресов (ULA) fc00::/7, таким образом, все адреса начинаются с **FD** (такой как, fdxx:xxxx:xxxx....). Кроме того, при записи адресов IPv6 можно использовать двойные двоеточия (::) для представления линии нулей так, чтобы **FD01:: 1/64** совпадает с **FD01:0000:0000:0000:0000:0000:0000:0001**.

```
ASAv(config)# interface GigabitEthernet0/0
ASAv(config-if)# ipv6 address fd03::1/64
ASAv(config-if)# nameif inside
ASAv(config-if)# security-level 100
```

```
ASAv(config)# interface GigabitEthernet0/1
ASAv(config-if)# ipv6 address fd02::2/64
ASAv(config-if)# nameif outside
ASAv(config-if)# security-level 0
```

У вас должен теперь быть базовый уровень 2 (L2) / Уровень 3 (L3) подключение к вышестоящему маршрутизатору на внешней VLAN в адресе **fd02:: 1**:

```
ASAv(config-if)# ping fd02::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to fd02::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Настройте маршрутизацию IPv6

Так же, как с IPv4, даже при том, что существует подключение IPv6 с хостами на подключенной напрямую подсети, у вас должны все еще быть маршруты к внешним сетям, чтобы знать, как достигнуть их. Первый пример показывает, как настроить статический маршрут по умолчанию для достижения всех сетей IPv6 через внешний интерфейс с адресом следующего узла **fd02::1**.

Настройте статичную маршрутизацию для IPv6

Используйте эту информацию для настройки статичной маршрутизации для IPv6:

```
ASAv(config)# ipv6 route outside 0::0/0 fd02::1
ASAv(config)# show ipv6 route
```

```
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, B - BGP
L fd02::2/128 [0/0]
via ::, outside
C fd02::/64 [0/0]
```

```
via ::, outside
L fd03::1/128 [0/0]
via ::, inside
C fd03::/64 [0/0]
via ::, inside
L fe80::/10 [0/0]
via ::, inside
via ::, outside
L ff00::/8 [0/0]
via ::, inside
via ::, outside
S   ::/0 [1/0]
via fd02::1, outsideASAv(config)#
```

Как показано существует теперь подключение к хосту на внешней подсети:

```
ASAv(config)# ping fd99::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to fd99::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ASAv(config)#
```

Примечание: Если протокол динамической маршрутизации желаем для обработки маршрутизации для IPv6, то можно настроить это также. Это описано в следующем разделе.

Настройте динамическую маршрутизацию для IPv6 с OSPFv3

Во-первых, необходимо исследовать Открытый Кратчайший путь Первая конфигурация Версии 3 (OSPFv3) на восходящей Cisco Маршрутизатор ISR (ISR) серии 881:

```
C881#show run | sec ipv6
ipv6 unicast-routing

!--- This enables IPv6 routing in the Cisco IOS®.

.....
ipv6 ospf 1 area 0
address-family ipv6 unicast
passive-interface default
no passive-interface Vlan302

!--- This is the interface to send OSPF Hellos to the ASA.

default-information originate always

!--- Always distribute the default route.

redistribute static
ipv6 route ::/0 FD99::2

!--- Creates a static default route for IPv6 to the internet.
```

Вот конфигурация соответствующего интерфейса:

```
C881#show run int vlan302
interface Vlan302
....
ipv6 address FD02::1/64
ipv6 ospf 1 area 0
```

C881#

Можно использовать захваты пакета ASA, чтобы проверить, что *Пакеты приветствия OSPF* замечены по ISR на внешнем интерфейсе:

```
ASAv(config)# show run access-list test_ipv6
access-list test_ipv6 extended permit ip any6 any6
ASAv(config)# show cap
capture capout type raw-data access-list test_ipv6 interface outside
[Capturing - 37976 bytes]
ASAv(config)# show cap capout

367 packets captured

1: 11:12:04.949474 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
2: 11:12:06.949444 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
  3: 11:12:07.854768          fe80::c671:feff:fe93:b516 > ff02::5: ip-proto-89 40
[hlim 1]
4: 11:12:07.946545 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
5: 11:12:08.949459 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
6: 11:12:09.542772 fe80::217:fff:fe17:af80 > ff02::5: ip-proto-89 40
[hlim 1]
....
 13: 11:12:16.983011          fe80::c671:feff:fe93:b516 > ff02::5: ip-proto-89 40
[hlim 1]
14: 11:12:18.947170 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
neighbor sol: who has fe80::250:56ff:fe9d:34a8 [class 0xe0]
15: 11:12:19.394831 fe80::217:fff:fe17:af80 > ff02::5: ip-proto-89 40
[hlim 1]
16: 11:12:19.949444 fe80::250:56ff:fe9d:34a8 > ff02::1:ff9d:34a8: icmp6:
  21: 11:12:26.107477          fe80::c671:feff:fe93:b516 > ff02::5: ip-proto-89 40
[hlim 1]
ASAv(config)#
```

В перехвате предыдущего пакета вы видите, что OSPF (**ip-proto-89**) пакеты поступает от IPv6 локальный для канала адрес, который соответствует корректному интерфейсу на ISR:

```
C881#show ipv6 interface brief
.....
Vlan302 [up/up]
  FE80::C671:FEFF:FE93:B516
FD02::1
C881#
```

Можно теперь создать процесс OSPFv3 на ASA для установления смежности с ISR:

```
C881#show ipv6 interface brief
.....
Vlan302 [up/up]
  FE80::C671:FEFF:FE93:B516
FD02::1
C881#
```

Примените конфигурацию OSPF к внешнему интерфейсу ASA:

```
C881#show ipv6 interface brief
.....
Vlan302 [up/up]
  FE80::C671:FEFF:FE93:B516
FD02::1
C881#
```

Это должно заставить ASA передавать широковещательные Пакеты приветствия OSPF на подсети IPv6. Введите команду **show ipv6 ospf neighbor** для проверки смежности с маршрутизатором:

```
ASAv# show ipv6 ospf neighbor
```

```
Neighbor ID Pri State Dead Time Interface ID Interface
 14.38.104.1 1 FULL/BDR 0:00:33 14 outside
```

Можно также подтвердить идентификатор соседнего узла на ISR, поскольку это использует самый высокий настроенный адрес IPv4 для ID по умолчанию:

```
C881#show ipv6 ospf 1
Routing Process "ospfv3 1" with ID 14.38.104.1
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary router
Redistributing External Routes from,
static
Originate Default Route with always
```

!--- Notice the other OSPF settings that were configured.

```
Router is not originating router-LSAs with maximum metric
....
```

```
C881#
```

ASA должен был теперь изучить IPv6 route по умолчанию из ISR. Для подтверждения этого введите команду **show ipv6 route**:

```
ASAv# show ipv6 route
```

```
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, B - BGP
O 2001:aaaa:aaaa:aaaa::/64 [110/10]
via ::, outside
L fd02::2/128 [0/0]
via ::, outside
C fd02::/64 [0/0]
via ::, outside
L fd03::1/128 [0/0]
via ::, inside
C fd03::/64 [0/0]
via ::, inside
L fe80::/10 [0/0]
via ::, inside
via ::, outside
L ff00::/8 [0/0]
via ::, inside
via ::, outside
OE2 ::/0 [110/1], tag 1
```

!--- Here is the learned default route.

```
via fe80::c671:feff:fe93:b516, outside
```

```
ASAv#
```

Базовая конфигурация интерфейсных параметров настройки и средств маршрутизации для IPv6 на ASA теперь завершена.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Процедуры устранения проблем для подключения IPv6 придерживаются большей части той же методологии, которая используется для устранения проблем подключения IPv4 с несколькими различиями. С точки зрения устранения проблем, одного из наиболее важных различий между IPv4 и IPv6 то, что Протокол ARP больше не существует в IPv6. Вместо использования ARP для решения IP-адресов на локальном сегменте LAN IPv6 использует протокол под названием Обнаружение соседей (ND).

Также важно понять, что ND усиливает Версию 6 (ICMPv6) Internet Control Message Protocol для разрешения Адреса для управления доступом к среде (MAC). Дополнительные сведения о IPv6 ND могут быть найдены в Руководстве по конфигурации IPv6 ASA в разделе [Обнаружения IPv6 Neighbor](#) Книги 1 CLI: Руководство Конфигурации интерфейса командой строки Общих функционирований Серии Cisco ASA, 9.4 или в [RFC 4861](#).

В настоящее время большая часть связанного с IPv6 устранения проблем включает или ND, маршрутизация или проблемы конфигурации подсети. Это - вероятная причина к факту, что это также основные различия между IPv4 и IPv6. ND работает по-другому, чем ARP, и адресация внутренней сети также очень отличается, поскольку использованию NAT высоко обескураживают в IPv6, и частная адресация больше не усиливается способ, которым это было в IPv4 (после RFC 1918). Как только эти различия поняты, и/или проблемы L2/L3 решены, процесс устранения проблем на Уровне 4 (L4) и выше является по существу тем же как используемым для IPv4, потому что TCP/UDP и высокоуровневые протоколы функционируют по существу то же (независимо от Версии IP, которая используется).

Устраните неполадки подключения L2 (ND)

Большая часть основной команды, которая используется для устранения проблем подключения L2 с IPv6 является `show ipv6 neighbor [nameif]` команда, которая является эквивалентом `show arp` для IPv4.

Ниже представлен пример выходных данных:

```
ASAv(config)# show ipv6 neighbor outside
IPv6 Address Age Link-layer Addr State Interface
fd02::1                0 c471.fe93.b516 REACH  outside
fe80::c671:feff:fe93:b516 32 c471.fe93.b516 DELAY  outside
fe80::e25f:b9ff:fe3f:1bbf 101 e05f.b93f.1bbf STALE  outside
fe80::b2aa:77ff:fe7c:8412 101 b0aa.777c.8412 STALE  outside
fe80::213:c4ff:fe80:5f53 101 0013.c480.5f53 STALE  outside
fe80::a64c:11ff:fe2a:60f4 101 a44c.112a.60f4 STALE  outside
fe80::217:fff:fe17:af80 99 0017.0f17.af80 STALE  outside
ASAv(config)#
```

В этих выходных данных вы видите успешное разрешение для адреса IPv6 `fd02:: 1`, который принадлежит устройству с MAC-адресом `c471.fe93.b516`.

Примечание: Вы могли бы заметить, что MAC - адрес интерфейса того же маршрутизатора появляется дважды в предыдущих выходных данных, потому что маршрутизатор также имеет самоназначенный локальный для канала адрес для этого интерфейса. Локальный для канала адрес является специфичным для устройства адресом, который может только использоваться для связи на сети с прямым подключением. Маршрутизаторы не делают передач пакетов через локальные для канала адреса, а скорее они только для связи на сегменте сети с прямым подключением. Много протоколов маршрутизации IPv6 (таких как OSPFv3) используют локальные для канала адреса, чтобы поделиться информацией протокола маршрутизации на сегменте L2.

Для очистки кэша ND введите команду **clear ipv6 neighbors**. Если ND отказывает для определенного хоста, можно ввести команду **debug ipv6 nd**, а также выполнить захваты пакета и проверить системные журналы, чтобы решить это, которое происходит на уровне L2. Помните, что IPv6 ND использует сообщения ICMPv6 для решения MAC-адресов для адресов IPv6.

ARP IPv4 по сравнению с IPv6 ND

Рассмотрите эту сравнительную таблицу ARP для IPv4 и ND для IPv6:

ARP IPv4

ЗАПРОС ARP (Кто имеет 10.10.10.1?)

ОТВЕТ ARP (10.10.10.1 в простое. отключено. отключено)

IPv6 ND

Запрос соседа

Объявление соседа

В следующем сценарии ND не в состоянии решать MAC-адрес *fd02::1* хост, который расположен на внешнем интерфейсе.

ND отладки

Вот выходные данные команды **debug ipv6 nd**:

```
ICMPv6-ND: Sending NS for fd02::1 on outside
```

```
!--- "Who has fd02::1"
```

```
ICMPv6-ND: Sending NS for fd02::1 on outside
```

```
ICMPv6-ND: Sending NS for fd02::1 on outside
```

```
ICMPv6-ND: INCMPI deleted: fd02::1
```

```
ICMPv6-ND: INCMPI -> DELETE: fd02::1
```

```
ICMPv6-ND: DELETE -> INCMPI: fd02::1
```

```
ICMPv6-ND: Sending NS for fd02::1 on outside
```

```
ICMPv6-ND: Sending NS for fd02::1 on outside
```

```
ICMPv6-ND: Sending NA for fd02::2 on outside
```

```
!--- "fd02::2 is at dead.dead.dead"
```

```
ICMPv6-ND: Sending NS for fd02::1 on outside
```

```
ICMPv6-ND: INCMPI deleted: fd02::1
```

```
ICMPv6-ND: INCMPI -> DELETE: fd02::1
```

```
ICMPv6-ND: DELETE -> INCMPI: fd02::1
```

```
!--- Here is where the ND times out.
```

```
ICMPv6-ND: Sending NS for fd02::1 on outside
```

```
ICMPv6-ND: Sending NS for fd02::1 on outside
```

В этих выходных данных отладки *кажется* что Объявления соседа от **fd02:: 2** никогда не получаются. Можно проверить захваты пакета, чтобы подтвердить, имеет ли это фактически место.

ND захваты пакета

Примечание: С Выпуска 9.4 (1) ASA access-lists все еще требуется для захватов пакета IPv6. Запрос на расширение был подан для отслеживания этого с идентификатором ошибки Cisco [CSCtn09836](#).

Настройте Список контроля доступа (ACL) и захваты пакета:

```
ICMPv6-ND: Sending NS for fd02::1 on outside
```

```
!--- "Who has fd02::1"
```

```
ICMPv6-ND: Sending NS for fd02::1 on outside
```

```
ICMPv6-ND: Sending NS for fd02::1 on outside
```

```
ICMPv6-ND: INCMP deleted: fd02::1
```

```
ICMPv6-ND: INCMP -> DELETE: fd02::1
```

```
ICMPv6-ND: DELETE -> INCMP: fd02::1
```

```
ICMPv6-ND: Sending NS for fd02::1 on outside
```

```
ICMPv6-ND: Sending NS for fd02::1 on outside
```

```
ICMPv6-ND: Sending NA for fd02::2 on outside
```

```
!--- "fd02::2 is at dead.dead.dead"
```

```
ICMPv6-ND: Sending NS for fd02::1 on outside
```

```
ICMPv6-ND: INCMP deleted: fd02::1
```

```
ICMPv6-ND: INCMP -> DELETE: fd02::1
```

```
ICMPv6-ND: DELETE -> INCMP: fd02::1
```

```
!--- Here is where the ND times out.
```

```
ICMPv6-ND: Sending NS for fd02::1 on outside
```

```
ICMPv6-ND: Sending NS for fd02::1 on outside
```

Иницируйте эхо-запрос к **fd02:: 1** от ASA:

```
ASAv(config)# show cap capout
```

```
....
```

```
23: 10:55:10.275284 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has fd02::1 [class 0xe0]
```

```
24: 10:55:10.277588 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1 [class 0xe0]
```

```
26: 10:55:11.287735 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has fd02::1 [class 0xe0]
```

```
27: 10:55:11.289642 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1 [class 0xe0]
```

```
28: 10:55:12.293365 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has fd02::1 [class 0xe0]
```

```
29: 10:55:12.298538 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1 [class 0xe0]
```

```
32: 10:55:14.283341 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has fd02::1 [class 0xe0]
```

```
33: 10:55:14.285690 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1
```

```
[class 0xe0]
35: 10:55:15.287872 fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has
fd02::1 [class 0xe0]
36: 10:55:15.289825 fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1
[class 0xe0]
```

Как показано в захватах пакета, Объявления соседа от **fd02:: 1** получены. Однако рекламные объявления не обработаны по некоторым причинам, как показано в выходных данных отладки. Для дальнейшего исследования можно просмотреть системные журналы.

ND системные журналы

Вот является некоторый пример ND системными журналами:

```
May 13 2015 10:55:10: %ASA-7-609001: Built local-host identity:fd02::2
May 13 2015 10:55:10: %ASA-6-302020: Built outbound ICMP connection for faddr
ff02::1:ff00:1/0 gaddr fd02::2/0 laddr fd02::2/0(any)
May 13 2015 10:55:10: %ASA-3-325003: EUI-64 source address check failed. Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:10: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
May 13 2015 10:55:11: %ASA-3-325003: EUI-64 source address check failed. Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:11: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
May 13 2015 10:55:12: %ASA-3-325003: EUI-64 source address check failed. Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:12: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
May 13 2015 10:55:14: %ASA-3-325003: EUI-64 source address check failed. Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:14: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
May 13 2015 10:55:15: %ASA-3-325003: EUI-64 source address check failed. Dropped
packet from outside:fd02::1/0 to fd02::2/0 with source MAC address c471.fe93.b516.
May 13 2015 10:55:15: %ASA-3-313008: Denied IPv6-ICMP type=136, code=0 from fd02::1
on interface outside
```

В этих системных журналах вы видите что пакеты Объявления соседа ND от ISR в **fd02:: 1** отброшены из-за отказавшего Модифицированного Расширенного уникального идентификатора (EUI) 64 (Модифицированный EUI-64) проверки формата.

Совет: См. *Модифицированный раздел Кодирования Адреса EUI-64* этого документа для получения дополнительной информации об этой определенной проблеме. Эта логика устранения проблем может быть применена ко всем видам причин отбрасывания также, такой как тогда, когда ACL не разрешают ICMPv6 на определенном интерфейсе или когда сбой проверки Одноадресной пересылки по обратному пути (uRPF) происходят, оба из которых могут вызвать проблемы с подключением L2 с IPv6.

Устраните неполадки основной маршрутизации IPv6

Процедуры устранения проблем для протоколов маршрутизации, когда IPv6 используется, являются по существу тем же как теми, когда используется IPv4. Использование **команд debug и show**, а также захваты пакета, полезно с попытками установить причину, что протокол маршрутизации не ведет себя как ожидалось.

Отладки протокола маршрутизации для IPv6

Этот раздел предоставляет полезные команды отладки для IPv6.

Глобальные отладки маршрутизации IPv6

Можно использовать отладку **debug ipv6 routing** для устранения проблем всех изменений таблицы маршрутизации IPv6:

```
ASAv# clear ipv6 ospf 1 proc

Reset OSPF process? [no]: yes
ASAv# IPv6RT0: ospfv3 1, Route update to STANDBY with epoch: 2 for
2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ospfv3 1, Delete 2001:aaaa:aaaa:aaaa::/64 from table
IPv6RT0: ospfv3 1, Delete backup for fd02::/64
IPv6RT0: ospfv3 1, Route update to STANDBY with epoch: 2 for ::/0
IPv6RT0: ospfv3 1, Delete ::/0 from table
IPv6RT0: ospfv3 1, ipv6_route_add_core for 2001:aaaa:aaaa:aaaa::/64 [110/10],
next-hop :: nh_source :: via interface outside route-type 2
IPv6RT0: ospfv3 1, Add 2001:aaaa:aaaa:aaaa::/64 to table
IPv6RT0: ospfv3 1, Added next-hop :: over outside for 2001:aaaa:aaaa:aaaa::/64,
[110/10]
IPv6RT0: ospfv3 1, ipv6_route_add_core Route update to STANDBY with epoch: 2 for
2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ipv6_route_add_core: input add 2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ipv6_route_add_core: output add 2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ospfv3 1, ipv6_route_add_core for fd02::/64 [110/10], next-hop ::
nh_source :: via interface outside route-type 2
IPv6RT0: ospfv3 1, ipv6_route_add_core for ::/0 [110/1], next-hop
fe80::c671:feff:fe93:b516
nh_source fe80::c671:feff:fe93:b516 via interface outside route-type 16
IPv6RT0: ospfv3 1, Add ::/0 to table
IPv6RT0: ospfv3 1, Added next-hop fe80::c671:feff:fe93:b516 over outside for ::/0,
[110/1]
IPv6RT0: ospfv3 1, ipv6_route_add_core Route update to STANDBY with epoch: 2 for ::/0
IPv6RT0: ipv6_route_add_core: input add ::/0
IPv6RT0: ipv6_route_add_core: output add ::/0
IPv6RT0: ospfv3 1, ipv6_route_add_core for 2001:aaaa:aaaa:aaaa::/64 [110/10],
next-hop :: nh_source :: via interface outside route-type 2
IPv6RT0: ospfv3 1, Route add 2001:aaaa:aaaa:aaaa::/64 [owner]
IPv6RT0: ospfv3 1, ipv6_route_add_core Route update to STANDBY with epoch: 2 for
2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ipv6_route_add_core: input add 2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ipv6_route_add_core: output add 2001:aaaa:aaaa:aaaa::/64
IPv6RT0: ospfv3 1, ipv6_route_add_core for fd02::/64 [110/10], next-hop ::
nh_source :: via interface outside route-type 2
IPv6RT0: ospfv3 1, Reuse backup for fd02::/64, distance 110
IPv6RT0: ospfv3 1, ipv6_route_add_core for ::/0 [110/1], next-hop
fe80::c671:feff:fe93:b516 nh_source fe80::c671:feff:fe93:b516 via interface outside
route-type 16
IPv6RT0: ospfv3 1, Route add ::/0 [owner]
IPv6RT0: ospfv3 1, ipv6_route_add_core Route update to STANDBY with epoch: 2 for ::/0
IPv6RT0: ipv6_route_add_core: input add ::/0
IPv6RT0: ipv6_route_add_core: output add ::/0
```

Отладки OSPFv3

Можно использовать команду **debug ipv6 ospf** для устранения проблем проблем OSPFv3:

```
ASAv# debug ipv6 ospf ?
```

```
adj OSPF adjacency events
database-timer OSPF database timer
events OSPF events
flood OSPF flooding
graceful-restart OSPF Graceful Restart processing
hello OSPF hello events
ipsec OSPF ipsec events
lsa-generation OSPF lsa generation
lsdb OSPF database modifications
packet OSPF packets
retransmission OSPF retransmission events
spf OSPF spf
```

Вот пример выходных данных для всех отладок, которые включены после того, как процесс OSPFv3 перезапущен:

```
ASAv# clear ipv6 ospf 1
OSPFv3: rcv. v:3 t:1 l:44 rid:192.168.128.115
aid:0.0.0.0 chk:a9ac inst:0 from outside
OSPFv3: Rcv hello from 192.168.128.115 area 0 from outside fe80::217:fff:fe17:af80
interface ID 142
OSPFv3: End of hello processingpr
OSPFv3: rcv. v:3 t:1 l:44 rid:14.38.104.1
aid:0.0.0.0 chk:bbf3 inst:0 from outside
OSPFv3: Rcv hello from 14.38.104.1 area 0 from outside fe80::c671:feff:fe93:b516
interface ID 14
OSPFv3: End of hello processinggo
ASAv# clear ipv6 ospf 1 process
```

Reset OSPF process? [no]: yes

```
ASAv#
OSPFv3: Flushing External Links
Insert LSA 0 adv_rtr 172.16.118.1, type 0x4005 in maxage
OSPFv3: Add Type 0x4005 LSA ID 0.0.0.0 Adv rtr 172.16.118.1 Seq 80000029 to outside
14.38.104.1 retransmission list
....
```

!--- The neighbor goes down:

```
OSPFv3: Neighbor change Event on interface outside
OSPFv3: DR/BDR election on outside
OSPFv3: Elect BDR 14.38.104.1
OSPFv3: Elect DR 192.168.128.115
OSPFv3: Schedule Router LSA area: 0, flag: Change
OSPFv3: Schedule Router LSA area: 0, flag: Change
OSPFv3: Schedule Prefix DR LSA intf outside
OSPFv3: Schedule Prefix Stub LSA area 0
OSPFv3: 14.38.104.1 address fe80::c671:feff:fe93:b516 on outside is dead, state DOWN
....
```

!--- The neighbor resumes the exchange:

```
OSPFv3: Rcv DBD from 14.38.104.1 on outside seq 0xd09 opt 0x0013 flag 0x7 len 28
mtu 1500 state EXSTART
OSPFv3: First DBD and we are not SLAVE
OSPFv3: rcv. v:3 t:2 l:168 rid:14.38.104.1
aid:0.0.0.0 chk:5aa3 inst:0 from outside
OSPFv3: Rcv DBD from 14.38.104.1 on outside seq 0x914 opt 0x0013 flag 0x2 len 168
mtu 1500 state EXSTART
OSPFv3: NBR Negotiation Done. We are the MASTER
OSPFv3: outside Nbr 14.38.104.1: Summary list built, size 0
OSPFv3: Send DBD to 14.38.104.1 on outside seq 0x915 opt 0x0013 flag 0x1 len 28
```

```
OSPFv3: rcv. v:3 t:2 l:28 rid:192.168.128.115
      aid:0.0.0.0 chk:295c inst:0 from outside
OSPFv3: Rcv DBD from 192.168.128.115 on outside seq 0xfeb opt 0x0013 flag 0x7 len 28
      mtu 1500 state EXSTART
OSPFv3: NBR Negotiation Done. We are the SLAVE
OSPFv3: outside Nbr 192.168.128.115: Summary list built, size 0
OSPFv3: Send DBD to 192.168.128.115 on outside seq 0xfeb opt 0x0013 flag 0x0 len 28
OSPFv3: rcv. v:3 t:2 l:28 rid:14.38.104.1
      aid:0.0.0.0 chk:8d74 inst:0 from outside
OSPFv3: Rcv DBD from 14.38.104.1 on outside seq 0x915 opt 0x0013 flag 0x0 len 28
      mtu 1500 state EXCHANGE
....
```

!--- The routing is re-added to the OSPFv3 neighbor list:

```
OSPFv3: Add Router 14.38.104.1 via fe80::c671:feff:fe93:b516, metric: 10
Router LSA 14.38.104.1/0, 1 links
  Link 0, int 14, nbr 192.168.128.115, nbr int 142, type 2, cost 1
  Ignore newdist 11 olddist 10
```

Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP на ASA не поддерживает использование IPv6. См. [Рекомендации для раздела EIGRP Книги 1 CLI: Руководство Конфигурации интерфейса командой строки Общих функционирований Серии Cisco ASA, 9.4](#) для получения дополнительной информации.

Border Gateway Protocol (BGP)

Когда IPv6 используется, эта команда отладки может использоваться для устранения проблем BGP:

```
ASAv# debug ip bgp ipv6 unicast ?
X:X:X:X::X IPv6 BGP neighbor address
keepalives BGP keepalives
updates BGP updates
<cr>
```

Полезные команды show для IPv6

Можно использовать эти команды показа для решения проблем IPv6:

- **show ipv6 route**
- **show ipv6 interface brief**
- **ID <process show ipv6 ospf>**
- **show ipv6 traffic**
- **show ipv6 neighbor**
- **покажите ipv6 icmp**

Пакетные трассировщики с IPv6

Можно использовать встроенную пакетную функциональность трассировщика с IPv6 на ASA таким же образом как с IPv4. Вот пример, где функциональность пакетного трассировщика используется для моделирования внутреннего хоста в **fd03::2**, который пытается соединиться с Web-сервером в **5555::1**, который расположен в Интернете с маршрутом по умолчанию, который изучен из этого **881** интерфейса через OSPF:

```
ASAv# packet-tracer input inside tcp fd03::2 10000 5555::1 80 detailed
```

```
Phase: 1
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
Forward Flow based lookup yields rule:
```

```
in id=0x7ffffd59ca0f0, priority=1, domain=permit, deny=false
```

```
hits=2734, user_data=0x0, cs_id=0x0, l3_type=0xdd86
```

```
src mac=0000.0000.0000, mask=0000.0000.0000
```

```
dst mac=0000.0000.0000, mask=0100.0000.0000
```

```
input_ifc=inside, output_ifc=any
```

```
Phase: 2
```

```
Type: ROUTE-LOOKUP
```

```
Subtype: Resolve Egress Interface
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
found next-hop fe80::c671:feff:fe93:b516 using egress ifc outside
```

```
Phase: 3
```

```
Type: NAT
```

```
Subtype: per-session
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
Forward Flow based lookup yields rule:
```

```
in id=0x7ffffd589cc30, priority=1, domain=nat-per-session, deny=true
```

```
hits=1166, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0,
```

```
protocol=6
```

```
src ip/id>::/0, port=0, tag=any
```

```
dst ip/id>::/0, port=0, tag=any
```

```
input_ifc=any, output_ifc=any
```

```
<<truncated output>>
```

```
Result:
```

```
input-interface: inside
```

```
input-status: up
```

```
input-line-status: up
```

```
output-interface: outside
```

```
output-status: up
```

```
output-line-status: up
```

```
Action: allow
```

```
ASAv#
```

Заметьте, что выходной MAC-адрес является локальным для канала адресом этого 881 интерфейса. Как упомянуто ранее, для многих протоколов динамической маршрутизации, маршрутизаторы используют локальные для канала адреса IPv6 для установления смежностей.

Полный список связанных с IPv6 отладок ASA

Вот отладки, которые могут использоваться для решения проблем IPv6:

```
ASAv# debug ipv6 ?
```

```
dhcp IPv6 generic dhcp protocol debugging
dhcprelay IPv6 dhcp relay debugging
icmp ICMPv6 debugging
interface IPv6 interface debugging
mld IPv6 Multicast Listener Discovery debugging
nd IPv6 Neighbor Discovery debugging
ospf OSPF information
packet IPv6 packet debugging
routing IPv6 routing table debugging
```

Общие связанные с IPv6 проблемы

В этом разделе описывается решить наиболее распространенные связанные с IPv6 проблемы.

Неправильно настроенные подсети

Много кейсов ТАС (Центра технической поддержки) IPv6 генерируются из-за общего отсутствия знаний о том, как IPv6 функционирует, или из-за администратора пытается внедрить IPv6 с использованием специфичных для IPv4 процессов.

Например, ТАС видел случаи, где администратору назначил \56 блоков адресов IPv6 интернет-провайдер (ISP). Администратор тогда назначает адрес и полные \56 подсетей к внешнему интерфейсу ASA и выбирает некоторый внутренний диапазон для использования для внутренних серверов. Однако с IPv6, все внутренние хосты должны также использовать маршрутизуемые адреса IPv6, и блок адреса IPv6 должен быть разломан на меньшие подсети по мере необходимости. В этом сценарии можно создать многих \64 подсети как часть этих \56 блоков, которые были выделены.

Совет: См. [RFC 4291](#) для дополнительных сведений.

Модифицированное кодирование EUI 64

ASA может быть настроен для требования модифицируемых EUI-64-encoded адресов IPv6. EUI, согласно RFC 4291, позволяет хосту назначать себя уникальный 64-разрядный идентификатор интерфейса IPv6 (EUI-64). Этой функцией является преимущество перед IPv4, поскольку это удаляет требование для использования DHCP для присвоения адреса IPv6.

Если ASA будет настроен, чтобы потребовать, чтобы это усовершенствование через **ipv6 `принудило-eui64` команду `nameif`**, то это, вероятно, отбросит много запросов Обнаружения соседей и Рекламных объявлений от других хостов на локальной подсети.

Совет: Для получения дополнительной информации обратитесь к [IPv6 Понимания](#)

Клиенты используют временные адреса IPv6 по умолчанию

По умолчанию много клиентских операционных систем (ОС), такие как Версии 7 и 8 Microsoft Windows, OS X Macintosh, и основанные на Linux системы, используют самоназначенные *временные* адреса IPv6 для расширенной конфиденциальности через IPv6 Автонастройка адреса Не сохраняющая состояние (SLAAC).

Центр технической поддержки Cisco видел некоторые случаи, где это вызвало неожиданные проблемы в средах, потому что хосты генерируют трафик от временного адреса а не статически назначенного адреса. В результате ACL и основанные на хосте маршруты могли бы заставить трафик или становиться отброшенным или неправильно маршрутизировать, который заставляет связь хоста отказывать.

Существует два метода, которые используются для адресации к этой ситуации. Поведение может быть отключено индивидуально на системах клиента, или можно отключить это поведение на маршрутизаторах Cisco IOS® и ASA. На ASA или стороне маршрутизатора, необходимо модифицировать флажок сообщений Объявления маршрутизатора (RA), который инициирует это поведение.

См. следующие разделы для отключения этого поведения в отдельных системах клиентов.

Microsoft Windows

Выполните эти шаги для отключения этого поведения в системах Microsoft Windows:

1. В Microsoft Windows, открытом Поднятая Командная строка (выполненный как администратор).
2. Введите эту команду, чтобы отключить случайную опцию генерации IP-адреса, и затем нажать **Enter**:
`netsh interface ipv6 set global randomizeidentifiers=disabled`
3. Введите эту команду, чтобы вынудить Microsoft Windows использовать стандарт EUI-64:
`netsh interface ipv6 set privacy state=disabled`
4. Перезагрузите машину для применения изменений.

OS Macintosh X

В терминале введите эту команду для отключения IPv6 SLAAC на хосте до следующей перезагрузки:

```
sudo sysctl -w net.inet6.ip6.use_tempaddr=0
```

Для создания конфигурации постоянной, введите эту команду:

```
sudo sh -c 'echo net.inet6.ip6.use_tempaddr=0 >> /etc/sysctl.conf'
```

Linux

В предельной оболочке введите эту команду:

```
sysctl -w net.ipv6.conf.all.use_tempaddr=0
```

Отключите SLAAC глобально от ASA

Второй метод, который используется для адресации к этому поведению должен модифицировать сообщение RA, которое передается от ASA до клиентов, который инициирует использование SLAAC. Для изменения сообщения RA введите эту команду от *Режима конфигурации интерфейса*:

```
ASAv(config)# interface gigabitEthernet 1/1
ASAv(config-if)# ipv6 nd prefix 2001::db8/32 300 300 no-autoconfig
```

Эта команда модифицирует сообщение RA, которое передается ASA так, чтобы флаг A-бита был "not set", и клиенты не генерируют временный адрес IPv6.

Совет: См. [RFC 4941](#) для дополнительных сведений.

Часто задаваемые вопросы IPv6

В этом разделе описываются некоторые часто задаваемые вопросы в отношении использования IPv6.

Я могу передать трафик и для IPv4 и для IPv6 на том же интерфейсе в то же время?

Да. Необходимо просто включить IPv6 на интерфейсе и назначить и IPv4 и адрес IPv6 к интерфейсу, и это обрабатывает оба типа трафика одновременно.

Я могу применить и IPv6 и ACL IPv4 к тому же интерфейсу?

Можно сделать это в версиях ASA ранее, чем Версия 9.0 (1). С Версии ASA 9.0 (1) *объединены* все ACL на ASA, что означает, что ACL поддерживает соединение и IPv4 и записей IPv6 в том же ACL.

В Версиях ASA 9.0 (1) и позже, ACL просто объединены вместе, и одиночный, унифицированный ACL применен к интерфейсу через команду **access-group**.

ASA поддерживает QoS для IPv6?

Да. Применение политик поддержек ASA и постановка в очередь с установлением приоритета для IPv6 таким же образом, что это делает с IPv4.

С Версии ASA 9.0 (1) *объединены* все ACL на ASA, что означает, что ACL поддерживает соединение и IPv4 и записей IPv6 в том же ACL. В результате любые команды QoS, которые предписаны на class-мар, который совпадает с ACL, принимают меры и на IPv4 и на трафике IPv6.

Я должен использовать NAT с IPv6?

Несмотря на то, что NAT может быть настроен для IPv6 на ASA, использованию NAT в IPv6 высоко обескураживают и ненужное учитывая почти бесконечную сумму доступных, глобально маршрутизуемых адресов IPv6.

Если NAT требуется в сценарии IPv6, можно найти дополнительные сведения о том, как настроить его в [IPv6 NAT](#) раздел [Рекомендаций](#) Книги 2 CLI: Руководство Конфигурации интерфейса командой строки Межсетевое экрана Серии Cisco ASA, 9.4.

Примечание: Существуют некоторые рекомендации и ограничения, которые нужно рассмотреть, когда вы внедряете NAT с IPv6.

Почему я вижу, что локальные для канала адреса IPv6 в команде *show failover* выводят?

В IPv6, ND локальные для канала адреса использования для выполнения определения адресов L2. Поэтому адреса IPv6 для отслеживаемых интерфейсов в выходных данных *show* команды *show failover* локальный для канала адрес а не глобальный адрес IPv6, который настроен на интерфейсе. Это ожидаемое состояние.

Известные Предупреждения/Запросы на расширение

Вот некоторые известные предупреждения в отношении использования IPv6:

- Пункт "соответствия" перехвата [идентификатора ошибки Cisco CSCtn09836 Г|| ASA 8.x](#) не ловит трафик IPv6
- [Идентификатор ошибки Cisco CSCuq85949 Г|| ENH](#) : IPv6 ASA поддерживает для WCCP
- Маршрутизация [идентификатора ошибки Cisco CSCut78380 Г|| ASA IPv6 ECMP](#) не балансирует нагрузку трафика

Дополнительные сведения

- [Протокол Интернета RFC 2460 Г||, Спецификация Версии 6 \(IPv6\)](#)
- [Архитектура адресации RFC 4291 Г|| IPv6](#)
- [Обнаружение соседей RFC 4861 Г|| для IP версии 6 \(IPv6\)](#)
- [Книга 1 CLI: Руководство Конфигурации интерфейса командой строки Общих функционирований Серии Cisco ASA, 9.4 Г|| IPv6](#)
- [SSL AnyConnect по IPv4+IPv6 к конфигурации ASA](#)
- [Техническая поддержка и Cisco Systems Г|| Документации](#)