IPv6 رورم ةكرح ريرمتل ASA نيوكت

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين جهاز الأمان القابل للتكيف (ASA) من Cisco لتمرير حركة مرور بروتوكول الإنترنت الإصدار 6 (IPv6) في إصدارات ASA 7.0(1) والإصدارات الأحدث.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى Cisco ASA Version 7.0(1) والإصدارات الأحدث.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

وفي الوقت الحالي، لا يزال الإصدار السادس من بروتوكول الإنترنت جديدا نسبيا من حيث تغلغل الأسواق. ومع ذلك، فقد تزايدت بشكل مضطرد طلبات المساعدة في تكوين بروتوكول IPv6 واستكشاف المشكلات وإصلاحها. والغرض من هذا المستند هو تلبية تلك الاحتياجات وتوفير ما يلي:

- نظرة عامة على إستخدام IPv6
- تكوينات IPv6 الأساسية على ASA
- معلومات حول كيفية أستكشاف أخطاء اتصال IPv6 وإصلاحها من خلال ASA
- قائمة بمشكلات وحلول IPv6 الأكثر شيوعا، كما هو محدد بواسطة مركز المساعدة التقنية (TAC) من Cisco

ملاحظة: نظرا لأن الإصدار السادس من بروتوكول الإنترنت (IPv6) لا يزال في المراحل المبكرة كبديل للإصدار الرابع من بروتوكول الإنترنت (IP) على مستوى العالم، فسيتم تحديث هذا المستند بشكل دوري من أجل الحفاظ على الدقة والملاءمة.

معلومات ميزة IPv6

فيما يلي بعض المعلومات الهامة حول وظائف IPv6:

- تم إدخال بروتوكول IPv6 لأول مرة في الإصدار 7.0(1) من ASA.
- تم تقديم دعم IPv6 في الوضع الشفاف في الإصدار 8.2(1) من ASA.

نظرة عامة على IPv6

وقد تم تطوير بروتوكول IPv6 في منتصف وأواخر التسعينات، ويرجع ذلك في المقام الأول إلى أن مساحة عنوان IPv4 العامة انتقلت بسرعة صوب الاستنفاد. على الرغم من أن ترجمة عنوان الشبكة (NAT) ساعدت IPv4 بشكل كبير وأخرت هذه المشكلة، أصبح من غير الممكن إنكار الحاجة إلى بروتوكول بديل في نهاية المطاف. وتم رسميا في كانون الأول/ديسمبر 1998 تفصيل بروتوكول IPv6 في إطار المعيار RFC 2460. يمكنك قراءة المزيد حول البروتوكول في المستند الرسمي RFC 2460، الموجود على موقع الويب الخاص بفرقة العمل الهندسية للإنترنت (IETF).

تحسينات IPv6 عبر IPv4

يصف هذا القسم التحسينات المضمنة مع بروتوكول IPv6 مقابل بروتوكول IPv4 القديم.

إمكانات عنونة موسعة

يزيد بروتوكول IPv6 حجم عنوان IP من 32 وحدة بت إلى 128 وحدة بت لدعم مزيد من مستويات تسلسل العناوين الهرمي، وعدد أكبر بكثير من العقد القابلة للتوجيه، وتبسيط التكوين التلقائي للعناوين. يتم تحسين قابلية تطوير توجيه البث المتعدد من خلال إضافة حقل *نطاق* إلى عناوين البث المتعدد. بالإضافة إلى ذلك، يتم تحديد نوع جديد من العناوين، يسمى *عنوان AnyCast*. ويتم إستخدام هذا الأمر لإرسال حزمة إلى أي عقدة واحدة في مجموعة.

تبسيط تنسيق الرأس

تم إسقاط بعض حقول رأس IPv4 أو جعلها إختيارية من أجل تقليل تكلفة معالجة الحالة العامة لمعالجة الحزم ومن أجل الحد من تكلفة النطاق الترددي العريض لرأس IPv6.

دعم محسن للملحقات والخيارات

تتيح التغييرات في طريقة ترميز خيارات رأس IP إعادة توجيه أكثر فعالية وقيود أقل صرامة على طول الخيارات ومرونة أكبر لتقديم خيارات جديدة في المستقبل.

إمكانية وضع العلامات على التدفق

تتم إضافة إمكانية جديدة لتمكين وضع العلامات على الحزم التي تنتمي إلى *تدفقات* حركة مرور معينة يطلب المرسل التعامل معها بشكل خاص، مثل جودة الخدمة (QoS) غير الافتراضية أو الخدمة *في الوقت الفعلي*.

إمكانات المصادقة والخصوصية

يتم تحديد الملحقات التي يتم إستخدامها لدعم المصادقة وتكامل البيانات وسرية البيانات (الاختيارية) ل IPv6.

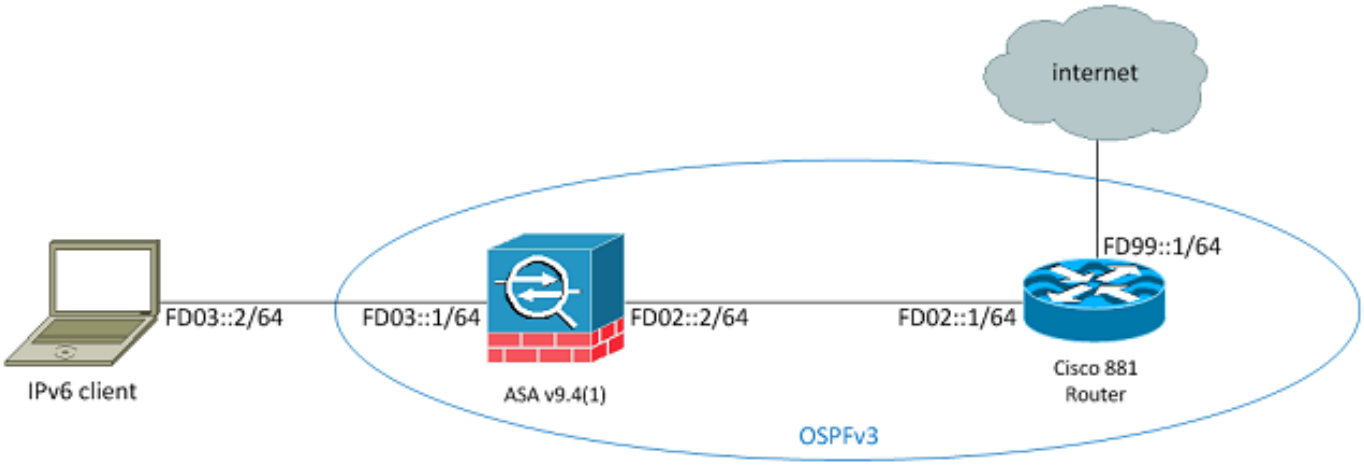
التكوين

يصف هذا القسم كيفية تكوين Cisco ASA لاستخدام IPv6.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

هذا هو مخطط IPv6 للأمثلة التي يتم إستخدامها في هذا المستند بالكامل:



تكوين الواجهات ل IPv6

لكي تمر حركة مرور IPv6 عبر ASA، يجب عليك أولا تمكين IPv6 على واجهتين على الأقل. يوضح هذا المثال كيفية تمكين IPv6 لتمرير حركة المرور من الواجهة الداخلية على **Gi0/0** إلى الواجهة الخارجية على **Gi0/1**:

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

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

يمكنك الآن تكوين عناوين IPv6 على كلا الواجهات.

ملاحظة: في هذا المثال، يتم إستخدام العناوين الموجودة في مساحة العناوين المحلية الفريدة (ULA) من FC00::/7، لذلك تبدأ جميع العناوين ب **FD** (مثل fdxx:xxxx:xxx....). أيضا، عندما تكتب عناوين IPv6، يمكنك إستخدام علامات نقطتين (:) لتمثيل خط من الأصفار حتى أن **FD01::1/64** هو نفسه **FD01:0000:000:000:0000:0000:000000:000000000000**.

```
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
```

أنت سوفت الآن يتلقى الأساسي طبقة 2 (L2)/طبقة 3 (L3) توصيل إلى مسحاج تخديد أعلى على VLAN خارجي في العنوان **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
```

تكوين توجيه IPv6

وكما هو الحال مع IPv4، فحتى مع وجود اتصال IPv6 مع الأجهزة المضيفة على الشبكة الفرعية المتصلة مباشرة، يجب أن يكون لديك أيضا المسارات إلى الشبكات الخارجية لمعرفة كيفية الوصول إليها. يوضح المثال الأول كيفية تكوين مسار افتراضي ثابت للوصول إلى جميع شبكات IPv6 عبر الواجهة الخارجية باستخدام عنوان الخطوة التالية **fd02::1**.

تكوين التوجيه الثابت ل IPv6

استعملت هذا معلومة in order to شكلت تحشد ساكن إستاتيكي ل 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
ASAv(config)#via fd02::1, outside
```

كما هو موضح، هناك الآن اتصال بمضيف على شبكة فرعية خارجية:

```
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
```

ملاحظة: إذا كان بروتوكول التوجيه الديناميكي مطلوبا لمعالجة التوجيه ل IPv6، فيمكنك تكوين ذلك أيضا. وهذا موصوف في الجزء التالي.

تكوين التوجيه الديناميكي ل IPv6 باستخدام OSPFv3

أولا، يجب عليك فحص تكوين الإصدار الأول 3 (OSPFv3) لأقصر مسار مفتوح على موجه الخدمات المدمجة سلسلة Cisco 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 ---!
```

وفيما يلي تكوين الواجهة ذات الصلة:

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

يمكنك إستخدام التقاط حزمة ASA للتحقق من رؤية حزم *OSPF* Hello من ISR على الواجهة الخارجية:

```
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

packets captured 367
```

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

في التقاط الحزمة السابقة، يمكنك أن ترى أن حزم ip-proto-89) OSPF) تصل من العنوان المحلي للإرتباط IPv6، والذي يماثل الواجهة الصحيحة على ISR:

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

يمكنك الآن إنشاء عملية OSPFv3 على ASA لإنشاء تجاور مع ISR:

```
                                                ASAv(config)# ipv6 router ospf 1
                                          ASAv(config-rtr)# passive-interface default
                                       ASAv(config-rtr)# no passive-interface outside
                                          ASAv(config-rtr)# log-adjacency-changes
                                       ASAv(config-rtr)# redistribute connected
                                                ASAv(config-rtr)# exit
```

تطبيق تكوين OSPF على الواجهة الخارجية ASA:

```
                                       ASAv(config)# interface GigabitEthernet0/1
                                             ASAv(config-if)# ipv6 ospf 1 area 0
                                                       ASAv(config-if)# end
```

يجب أن يتسبب ذلك في أن يرسل ASA حزم OSPF Hello الخاصة بالبث على الشبكة الفرعية IPv6. أدخل الأمر **show ipV6 ospf المجاور** للتحقق من التجاور مع الموجه:

```
                                                ASAv# show ipv6 ospf neighbor

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

كما يمكنك تأكيد معرف الجوار على ISR، حيث إنه يستخدم أعلى عنوان IPv4 تم تكوينه للمعرف بشكل افتراضي:

```
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#
```

يجب أن يكون ASA قد تعلم الآن المسار الافتراضي IPv6 من ISR. لتأكيد ذلك، أدخل الأمر **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
```

اكتمل الآن التكوين الأساسي لإعدادات الواجهة وميزات التوجيه ل IPv6 على ASA.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

تتبع إجراءات أستكشاف الأخطاء وإصلاحها لاتصال IPv6 معظم المنهجية المستخدمة لاستكشاف أخطاء اتصال IPv4 وإصلاحها، مع بعض الاختلافات. من منظور أستكشاف الأخطاء وإصلاحها، يتمثل أحد أهم الفروق بين بروتوكول IPv4

و IPv6 في أن بروتوكول تحليل العنوان (ARP) لم يعد موجودا في بروتوكول IPv6. بدلا من إستخدام ARP لحل عناوين IP على مقطع الشبكة المحلية، يستخدم IPv6 بروتوكول يسمى اكتشاف الجوار (ND).

ومن المهم أيضا فهم أن ND يستغل بروتوكول رسائل التحكم في الإنترنت الإصدار 6 (ICMPv6) لحل عنوان التحكم في الوصول إلى الوسائط (MAC). يمكن العثور على مزيد من المعلومات حول IPv6 ND في دليل تكوين ASA IPv6 في قسم اكتشاف الجوار ل IPv6 في *دليل تكوين واجهة سطر الأوامر (CLI) 1: Cisco ASA Series General Operations CLI*، *الإصدار 9.4* أو في RFC 4861.

حاليا، يتضمن معظم أستكشاف الأخطاء وإصلاحها المتعلقة ب IPv6 مشاكل تكوين الشبكة الفرعية أو التوجيه أو الشبكة الفرعية. ويعزى ذلك على الأرجح إلى حقيقة أن هذه أيضا هي الفروق الرئيسية بين IPv4 و IPv6. يعمل بروتوكول ND بشكل مختلف عن ARP، كما أن عنونة الشبكة الداخلية مختلفة تماما، حيث إن إستخدام NAT مثبط بشدة في IPv6 ولم يعد العنونة الخاصة يتم الاستفادة منها بالطريقة التي كانت عليها في IPv4 (بعد RFC 1918). بمجرد فهم هذه الفروق و/أو حل مشاكل L2/L3، تكون عملية أستكشاف الأخطاء وإصلاحها في الطبقة 4 (L4) وما فوقها هي بشكل أساسي نفس العملية المستخدمة ل IPv4 لأن بروتوكول TCP/UDP وبروتوكولات الطبقة العليا يعملان بشكل أساسي بنفس الطريقة (بغض النظر عن إصدار IP الذي يتم إستخدامه).

أستكشاف أخطاء اتصال المستوى الثاني وإصلاحها (ND)

الأمر الأكثر أساسية الذي يتم إستخدامه لاستكشاف أخطاء اتصال L2 وإصلاحها باستخدام IPv6 هو الأمر **show ipV6 neighbor [namelf]**، والذي يعادل **show arp** ل IPv4.

فيما يلي مثال للمخرجات:

```
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
```

في هذا الإخراج، يمكنك رؤية الدقة الناجحة لعنوان IPv6 على **FD02::1**، والذي ينتمي إلى الجهاز باستخدام عنوان MAC **c471.fe93.b516**.

ملاحظة: قد تلاحظ أن نفس عنوان MAC لواجهة الموجه يظهر مرتين في الإخراج السابق لأن الموجه يحتوي أيضا على عنوان محلي ذاتي التعيين للارتباط لهذه الواجهة. العنوان المحلي هو عنوان خاص بجهاز لا يمكن إستخدامه إلا للاتصال على الشبكة المتصلة مباشرة. لا تقوم الموجهات بإعادة توجيه الحزم عبر العناوين المحلية من الارتباط، ولكنها بدلا من ذلك مخصصة للاتصال فقط على مقطع الشبكة المتصلة مباشرة. يستخدم العديد من بروتوكولات توجيه IPv6 (مثل OSPFv3) عناوين الارتباط المحلية لمشاركة معلومات بروتوكول التوجيه على مقطع L2.

لمسح ذاكرة التخزين المؤقت ل ND، أدخل الأمر **clear IPv6 neighbors**. إذا فشل الكثافة الطبيعية لمضيف معين، يمكنك إدخال الأمر **debug ipV6 and** ، بالإضافة إلى إجراء التقاط الحزم والتحقق من syslogs، لتحديد ما يحدث على مستوى L2. تذكر أن بروتوكول IPv6 يستخدم رسائل ICMPv6 لحل عناوين MAC لعناوين IPv6.

IPv6 ND مقابل IPv4 ARP

ولنتأمل جدول مقارنة ARP للإصدار الرابع من بروتوكول الإنترنت والإصدار السادس من بروتوكول الإنترنت (IP):

IPv4 ARP	بروتوكول IPv6 ND
طلب ARP (من لديه 10.10.10.1؟)	إستدراج الجار
ARP REPLY (10.10.10.1 على Dead.Dead.Dead)	إعلان الجار

في السيناريو التالي، يفشل البعد الرقمي في حل عنوان MAC من *FD02:1* المضيف الذي يكون موجودا على الواجهة الخارجية.

تصحيح أخطاء ND

فيما يلي إخراج الأمر **debug ipV6**:

```
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
```

في إخراج تصحيح الأخطاء هذا، *يظهر* أن الإعلانات المجاورة من **fd02:2** لا يتم إستلامها أبدا. يمكنك التحقق من التقاط الحزمة لتأكيد ما إذا كانت هذه هي الحالة بالفعل.

التقاط حزمة ND

ملاحظة: حتى الإصدار 9.4(1) من ASA، لا تزال قوائم الوصول مطلوبة لالتقاط حزم IPv6. تم تقديم طلب تعزيز لتعقب هذا الإجراء باستخدام معرف تصحيح الأخطاء من CSCtn09836 Cisco.

تكوين قائمة التحكم في الوصول (ACL) وتقاطعات الحزم:

```
ASAv(config)# access-list test_ipv6 extended permit ip any6 any6
ASAv(config)# cap capout interface outside access-list test_ipv6
```

ابدأ إختبار اتصال إلى **FD02::1** من ASA:

```
ASAv(config)# show cap capout
....
fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has 10:55:10.275284 :23
                                                        [fd02::1 [class 0xe0
fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1 10:55:10.277588 :24
                                                        [class 0xe0]
fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has 10:55:11.287735 :26
                                                        [fd02::1 [class 0xe0
fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1 10:55:11.289642 :27
                                                        [class 0xe0]
fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has 10:55:12.293365 :28
                                                        [fd02::1 [class 0xe0
fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1 10:55:12.298538 :29
                                                        [class 0xe0]
fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has 10:55:14.283341 :32
                                                        [fd02::1 [class 0xe0
fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1 10:55:14.285690 :33
                                                        [class 0xe0]
fd02::2 > ff02::1:ff00:1: icmp6: neighbor sol: who has 10:55:15.287872 :35
                                                        [fd02::1 [class 0xe0
fd02::1 > fd02::2: icmp6: neighbor adv: tgt is fd02::1 10:55:15.289825 :36
                                                        [class 0xe0]
```

كما هو موضح في حزم الالتقاط، يتم تلقي الإعلانات المجاورة من **fd02:1**. ومع ذلك، لا تتم معالجة الإعلانات لسبب ما، كما هو موضح في مخرجات تصحيح الأخطاء. لمزيد من الفحص، يمكنك عرض syslogs.

ND Syslogs

هنا بعض مثال و syslog:

```
                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
```

ضمن هذه syslogs، أنت يستطيع رأيت أن ال ND مجاور إعلان ربط من ال isr في **fd02::1** سقطت بسبب فشل تعديل موسع معرف فريد (64 (EUI (يعدل EUI-64) تدقيق تنسيق.

تلميح: راجع قسم *ترميز عنوان EUI-64 المعدل* في هذا المستند للحصول على مزيد من المعلومات حول هذه

المشكلة المحددة. يمكن تطبيق منطق أستكشاف الأخطاء وإصلاحها هذا على جميع أنواع أسباب الإسقاط أيضا، مثل عندما لا تسمح قوائم التحكم في الوصول (ACL) بالإصدار السادس من ICMPv6 على واجهة معينة أو عند حدوث حالات فشل في إعادة توجيه المسار العكسي للبث الأحادي (uRPF)، ويمكن أن يتسبب كلا منهما في حدوث مشاكل في اتصال المستوى الثاني مع IPv6.

أستكشاف أخطاء توجيه IPv6 الأساسية وإصلاحها

تكون إجراءات أستكشاف الأخطاء وإصلاحها لبروتوكولات التوجيه عند إستخدام IPv6 هي بشكل أساسي نفسها تلك التي يتم إستخدامها عند إستخدام IPv4. يكون إستخدام أوامر **debug** و**show**، بالإضافة إلى التقاط الحزم، مفيدا مع محاولات التحقق من سبب عدم تصرف بروتوكول التوجيه كما هو متوقع.

تصحيح أخطاء بروتوكول التوجيه ل IPv6

يوفر هذا القسم أوامر تصحيح الأخطاء المفيدة ل IPv6.

تصحيح أخطاء توجيه IPv6 العمومي

يمكنك إستخدام تصحيح أخطاء **توجيه IPv6** لاستكشاف أخطاء جميع تغييرات جدول توجيه IPv6 وإصلاحها:

```
ASAv# clear ipv6 ospf 1 proc

Reset OSPF process? [no]: yes
ASAv# IPv6RT0: ospfv3 1, Route update to STANDBY with epoch: 2 for
aaaa:aaaa:aaaa::/64:2001
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
aaaa:aaaa:aaaa::/64:2001
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
aaaa:aaaa:aaaa::/64:2001
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
```

تصحيح أخطاء OSPFv3

يمكنك إستخدام الأمر **debug ipV6 ospf** لاستكشاف أخطاء OSPFv3 وإصلاحها:

```
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
```

فيما يلي مثال على الإخراج لجميع عمليات تصحيح الأخطاء التي يتم تمكينها بعد إعادة تشغيل عملية OSPFv3:

```
                                                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 processingo
                                           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
                                                    retransmission list 14.38.104.1
                                                                              ....

                                                    !--- 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
```

بروتوكول توجيه العبارة الداخلي المحسن (EIGRP)

لا يدعم EIGRP على ASA إستخدام IPv6. راجع قسم إرشادات EIGRP من *كتاب CLI 1: دليل تكوين واجهة سطر الأوامر (CLI) للعمليات العامة من السلسلة Cisco ASA، الإصدار 9.4* للحصول على مزيد من المعلومات.

بروتوكول البوابة الحدودية (BGP)

يمكن إستخدام الأمر **debug** هذا لاستكشاف أخطاء BGP وإصلاحها عند إستخدام IPv6:

```
? ASAv# debug ip bgp ipv6 unicast

X:X:X:X::X IPv6 BGP neighbor address
keepalives BGP keepalives
updates BGP updates
<cr>
```

أوامر show مفيدة ل IPv6

يمكنك إستخدام أوامر **العرض** هذه لاستكشاف أخطاء IPv6 وإصلاحها:

- **عرض مسار بروتوكول IPv6**
- **show ipV6 interface brief**

- show ipV6 ospf <معرف العملية>
- عرض حركة مرور IPv6
- إظهار جار IPv6
- show ipV6 icmp

حزم التتبع مع IPv6

يمكنك إستخدام وظيفة تعقب الحزم المدمجة مع IPv6 على ASA بنفس الطريقة مع IPv4. هنا مثال حيث الربط tracer استعملت وظيفة in order to حاكت المضيف داخلي في **FD03::2**، أي يحاول أن يربط إلى ويب نادل في **1::5555** أن يكون موقع على الإنترنت مع التقصير ممر أن يكون علمت من **881** قارن عن طريق 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=0x7fffd59ca0f0, 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=0x7fffd589cc30, 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#
```

لاحظت أن المخرج {mac address{upper ال link-local عنوان من ال 881 قارن. وكما تمت الإشارة مسبقا، بالنسبة للعديد من بروتوكولات التوجيه الديناميكية، تستخدم الموجهات عناوين IPv6 المحلية الخاصة بالارتباط لإنشاء عمليات تجاور.

قائمة كاملة بتصحيح أخطاء ASA المتعلقة ب IPv6

فيما يلي تصحيح الأخطاء التي يمكن إستخدامها لاستكشاف أخطاء IPv6 وإصلاحها:

```
? 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
```

المشاكل الشائعة المتعلقة ب IPv6

يوضح هذا القسم كيفية أستكشاف أخطاء IPv6 الأكثر شيوعا ذات الصلة وإصلاحها.

الشبكات الفرعية التي تم تكوينها بشكل غير صحيح

يتم إنشاء العديد من حالات IPv6 TAC بسبب نقص عام في المعرفة حول كيفية عمل IPv6، أو بسبب محاولات المسؤول تنفيذ IPv6 باستخدام عمليات خاصة ب IPv4.

على سبيل المثال، شهد TAC حالات تم فيها تعيين \56 كتلة من عناوين IPv6 للمسؤول بواسطة موفر خدمة الإنترنت (ISP). بعد ذلك يقوم المسؤول بتعيين عنوان والشبكة الفرعية \56 بالكامل إلى واجهة ASA الخارجية ويختار بعض النطاق الداخلي لاستخدامه مع الخوادم الداخلية. ومع ذلك، مع IPv6، يجب أن تستخدم جميع الأجهزة المضيفة الداخلية أيضا عناوين IPv6 القابلة للتوجيه، كما يجب تقسيم كتلة عنوان IPv6 إلى شبكات فرعية أصغر عند الحاجة. في هذا السيناريو، يمكنك إنشاء العديد من الشبكات الفرعية \64 كجزء من الكتلة \56 التي تم تخصيصها.

تلميح: راجع RFC 4291 للحصول على معلومات إضافية.

تشفير EUI 64 المعدل

يمكن تكوين ASA من أجل طلب عناوين IPv6 معدلة مشفرة وفقا لمعيار EUI-64. تتيح واجهة EUI، وفقا لمعيار RFC 4291، للمضيف تخصيص معرف واجهة IPv6 فريد من فئة 64 بت (EUI-64) لنفسه. هذه الميزة هي ميزة عبر IPv4، لأنها تزيل متطلبات إستخدام DHCP لتعيين عنوان IPv6.

إذا تم تكوين ASA لطلب هذا التحسين عبر أمر **اسم IPv6 enforcement-eui64**، فمن المرجح أن يقوم بإسقاط العديد من عروض أستكشاف الجوار والإعلانات من الأجهزة المضيفة الأخرى على الشبكة الفرعية المحلية.

تلميح: للحصول على مزيد من المعلومات، ارجع إلى مستند مجتمع دعم Cisco فهم عنوان IPv6 EUI-64 Bit.

يستخدم العملاء عناوين IPv6 المؤقتة بشكل افتراضي

بشكل افتراضي، يستخدم العديد من أنظمة تشغيل العملاء (OSs)، مثل Microsoft Windows بالإصدارين 7 و 8 و Macintosh OS-X والأنظمة المستندة إلى Linux، عناوين IPv6 *المؤقتة* المخصصة ذاتيا للخصوصية الموسعة عبر التكوين التلقائي لعنوان IPv6 عديم الحالة (SLAAC).

شهد Cisco TAC بعض الحالات التي تسبب فيها ذلك مشاكل غير متوقعة في البيئات لأن البيئات المضيفة تقوم بإنشاء حركة مرور من العنوان المؤقت وليس العنوان المعين بشكل ثابت. ونتيجة لذلك، قد تتسبب قوائم التحكم في الوصول (ACL) والمسارات المستندة إلى المضيف في إسقاط حركة المرور أو توجيهها بشكل غير صحيح، مما يؤدي إلى فشل اتصال المضيف.

هناك طريقتان تستخدمان لمعالجة هذا الوضع. يمكن تعطيل هذا السلوك بشكل فردي على أنظمة العميل، أو يمكنك تعطيل هذا السلوك على موجهات ASA و Cisco IOS®. على جانب ASA أو الموجه، يجب عليك تعديل علامة رسالة إعلان الموجه (RA) التي تعمل على تشغيل هذا السلوك.

أحلت التالي قسم in order to أعجزت هذا تصرف على كل زبون نظام.

مايكروسوفت ويندوز

أكمل الخطوات التالية لتعطيل هذا السلوك على أنظمة Microsoft Windows:

1. في Microsoft Windows، افتح موجه أوامر HIGH (تشغيل كمسؤول).
2. أدخل هذا الأمر لتعطيل ميزة إنشاء عنوان IP العشوائي، ثم اضغط على مفتاح **Enter**:

```
netsh interface ipv6 set global randomizeidentifiers=disabled
```

3. أدخل هذا الأمر لإجبار Microsoft Windows على إستخدام معيار EUI-64:

```
netsh interface ipv6 set privacy state=disabled
```

4. أعد تمهيد الجهاز لتطبيق التغييرات.

نظام التشغيل Macintosh OS-X

دخلت في انتهائية، هذا أمر in order to أعجزت IPv6 SLAAC على المضيف حتى التالي reboot:

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

دخلت in order to جعلت التشكيل دائم، هذا أمر:

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

لينكس

في طبقة طرفية، دخلت هذا أمر:

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

تعطيل SLAAC بشكل عام من ASA

الطريقة الثانية التي يتم إستخدامها لمعالجة هذا السلوك هي تعديل رسالة RA التي يتم إرسالها من ASA إلى العملاء، والتي تقوم بتشغيل إستخدام SLAAC. دخلت in order to عدلت ال RA رسالة، هذا أمر من *قارن تشكيل* أسلوب:

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

يقوم هذا الأمر بتعديل رسالة RA التي يتم إرسالها بواسطة ASA حتى لا يتم تعيين علامة البت، ولا يقوم العملاء بإنشاء عنوان IPv6 مؤقت.

تلميح: راجع RFC 4941 للحصول على معلومات إضافية.

الأسئلة المتداولة حول IPv6

يصف هذا القسم بعض الأسئلة المتداولة فيما يتعلق باستخدام IPv6.

هل يمكنني تمرير حركة مرور البيانات لكل من IPv4 و IPv6 على نفس الواجهة، في نفس الوقت؟

نعم. أنت ينبغي ببساطة مكنت IPv6 على القارن وعينت على حد سواء IPv4 وعنوان IPv6 إلى القارن، وهو يعالج كلا نوع الحركة مرور في وقت واحد.

هل يمكنني تطبيق قوائم التحكم في الوصول إلى IPv6 و IPv4 على نفس الواجهة؟

يمكنك تنفيذ هذا الإجراء في إصدارات ASA الأقدم من الإصدار 9.0(1). اعتبارا من الإصدار 9.0(1) من ASA، تكون جميع قوائم التحكم في الوصول (ACL) على ASA *موحدة*، مما يعني أن قائمة التحكم في الوصول (ACL) تدعم مزيجا من إدخالات كل من IPv4 و IPv6 في قائمة التحكم في الوصول نفسها.

في ASA الإصدارات 9.0(1) والإصدارات الأحدث، يتم دمج قوائم التحكم في الوصول (ACL) ببساطة معا ويتم تطبيق قائمة التحكم في الوصول (ACL) الموحدة الأحادية على الواجهة عبر الأمر **access-group**.

هل يدعم ASA جودة الخدمة ل IPv6؟

نعم. يدعم ASA تنظيم قوائم الانتظار حسب الأولوية ل IPv6 بنفس الطريقة التي يدعمها مع IPv4.

اعتبارا من الإصدار 9.0(1) من ASA، تكون جميع قوائم التحكم في الوصول (ACL) على ASA *موحدة*، مما يعني أن قائمة التحكم في الوصول (ACL) تدعم مزيجا من إدخالات كل من IPv4 و IPv6 في قائمة التحكم في الوصول نفسها. ونتيجة لذلك، تتخذ أي أوامر جودة الخدمة التي يتم تطبيقها على خريطة فئة تطابق قائمة التحكم في الوصول (ACL) إجراء على كل من حركة مرور IPv4 و IPv6.

هل يجب إستخدام NAT مع IPv6؟

على الرغم من أنه يمكن تكوين NAT للإصدار السادس من بروتوكول IPv6 على بروتوكول ASA، إلا أن إستخدام

NAT في الإصدار السادس من بروتوكول IPv6 غير مدعوم وغير ضروري إلى حد كبير، نظرا للكمية غير المحدودة تقريبا من عناوين IPv6 المتوفرة والموجهة عالميا.

إذا كان NAT مطلوبا في سيناريو IPv6، فيمكنك العثور على مزيد من المعلومات حول كيفية تكوينه في قسم إرشادات IPv6 NAT في *دليل تكوين واجهة سطر الأوامر (2 (CLI: دليل تكوين واجهة سطر الأوامر (CLI) لجدار الحماية من سلسلة Cisco ASA، الإصدار 9.4*.

ملاحظة: هناك بعض المبادئ التوجيهية والقيود التي يجب مراعاتها عند تنفيذ NAT مع IPv6.

لماذا أرى عناوين IPv6 المحلية للارتباط في إخراج الأمر *show failover*؟

في IPv6، تستخدم الشبكة العنكبوتية العناوين المحلية لإجراء تحليل عنوان L2. ولهذا السبب، تعرض عناوين IPv6 للواجهات المراقبة في إخراج الأمر show failed over العنوان المحلي للارتباط وليس عنوان IPv6 العام الذي تم تكوينه على الواجهة. وهذا هو السلوك المتوقع.

طلبات التصحيحات/التحسين المعروفة

فيما يلي بعض التحذيرات المعروفة فيما يتعلق باستخدام IPv6:

- معرف تصحيح الأخطاء من Cisco CSCtn09836Â *ASA 8.x لا يمسك عبارة تطابق" لالتقاط IPv6*
- معرف تصحيح الأخطاء من Cisco CSCuq85949Â *ENH*: دعم *ASA IPv6 ل WCCP*
- معرف تصحيح الأخطاء من Cisco CSCut78380Â*ASA IPv6 ECMP لا يحمل حركة مرور التوازن*

معلومات ذات صلة

- المعيار RFC 2460مناقشة بروتوكول الإنترنت، الإصدار 6 (بروتوكول IPv6) مواصفات
- المعيار RFC 4291 قسمنقل IP الإصدار 6 الذي يخاطب المعمارية
- المعيار RFC 4861a اكتشاف الجوار للإصدار السادس من بروتوكول الإنترنت (IPv6)
- CLI Book 1: دليل تكوين واجهة سطر الأوامر لعمليات Cisco ASA Series General Operations CLI، الإصدار 9.4a IPv6
- تكوين AnyConnect SSL عبر IPv4+IPv6 إلى ASA
- الدعم التقني والتوثيقأ Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).