Configurazione dell'ASA per il passaggio del traffico IPv6

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Informazioni sulle funzionalità IPv6
Panoramica di IPv6
Miglioramenti IPv6 su IPv4
Funzionalità di indirizzamento estese
Semplificazione del formato dell'intestazione
Supporto migliorato per estensioni e opzioni
Funzionalità di etichettatura flusso
Funzionalità di autenticazione e privacy
Configurazione
Esempio di rete
Configura interfacce per IPv6
Configura routing IPv6
Configura routing statico per IPv6
Configurazione del routing dinamico per IPv6 con OSPFv3
Verifica
Risoluzione dei problemi
Risoluzione dei problemi relativi alla connettività L2 (ND)
Confronto tra ARP IPv4 e ND IPv6
Debug ND
Acquisizioni pacchetti ND
Syslog ND
Risoluzione dei problemi relativi al routing IPv6 di base
Debug del protocollo di routing per IPv6
Utili comandi Show per IPv6
Packet Tracer con IPv6
Elenco completo dei debug ASA correlati a IPv6
Problemi comuni correlati a IPv6
Subnet non configurate correttamente
Codifica EUI 64 modificata
I client utilizzano indirizzi IPv6 temporanei per impostazione predefinita
Domande frequenti su IPv6

È possibile passare il traffico per IPv4 e IPv6 sulla stessa interfaccia contemporaneamente?
È possibile applicare gli ACL IPv6 e IPv4 alla stessa interfaccia?
L'appliance ASA supporta QoS per IPv6?
È consigliabile utilizzare NAT con IPv6?
Perché gli indirizzi IPv6 locali del collegamento vengono visualizzati nell'output del comando ***show failover***?
Richieste di miglioramento/avvertenze note
Informazioni correlate

Introduzione

In questo documento viene descritto come configurare Cisco Adaptive Security Appliance (ASA) in modo che superi il traffico del protocollo Internet versione 6 (IPv6) nelle versioni 7.0(1) e successive.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per questo documento, è stato usato Cisco ASA versione 7.0(1) e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Attualmente, l'IPv6 è ancora relativamente nuovo in termini di penetrazione sul mercato. Tuttavia, l'assistenza alla configurazione IPv6 e le richieste di risoluzione dei problemi sono in costante aumento. Il presente documento ha lo scopo di rispondere a tali esigenze e di fornire:

- Panoramica generale sull'utilizzo di IPv6
- Configurazioni IPv6 di base sull'appliance ASA
- Informazioni su come risolvere i problemi di connettività IPv6 tramite l'appliance ASA
- Un elenco dei problemi e delle soluzioni IPv6 più comuni, identificati dal Cisco Technical

Assistance Center (TAC)

Nota: Poiché l'IPv6 è ancora nelle prime fasi come prodotto sostitutivo dell'IPv4 a livello globale, questo documento verrà aggiornato periodicamente per mantenere l'accuratezza e la pertinenza.

Informazioni sulle funzionalità IPv6

Di seguito sono riportate alcune importanti informazioni sulla funzionalità IPv6:

- Il protocollo IPv6 è stato introdotto per la prima volta nell'appliance ASA versione 7.0(1).
- Il supporto di IPv6 in modalità trasparente è stato introdotto nell'appliance ASA versione 8.2(1).

Panoramica di IPv6

Il protocollo IPv6 è stato sviluppato verso la metà degli anni '90, principalmente a causa del fatto che lo spazio di indirizzi IPv4 pubblico si è spostato rapidamente verso l'esaurimento'. Anche se Network Address Translation (NAT) ha notevolmente contribuito all'IPv4 e ha ritardato questo problema, è diventato innegabile che alla fine sarebbe stato necessario un protocollo sostitutivo. Il protocollo IPv6 è stato descritto nella RFC 2460 del dicembre 1998. Per ulteriori informazioni sul protocollo, consultare il documento RFC 2460 ufficiale, disponibile sul sito Web della Internet Engineering Task Force (IETF).

Miglioramenti IPv6 su IPv4

In questa sezione vengono descritti i miglioramenti apportati al protocollo IPv6 rispetto al protocollo IPv4 precedente.

Funzionalità di indirizzamento estese

Il protocollo IPv6 aumenta la dimensione dell'indirizzo IP da 32 a 128 bit per supportare più livelli di gerarchia di indirizzamento, un numero molto maggiore di nodi indirizzabili e una configurazione automatica più semplice degli indirizzi. La scalabilità del routing multicast viene migliorata aggiungendo un campo *ambito* agli indirizzi multicast. Viene inoltre definito un nuovo tipo di indirizzo, denominato *indirizzo anycast*. Questa opzione viene usata per inviare un pacchetto a uno dei nodi di un gruppo.

Semplificazione del formato dell'intestazione

Alcuni campi dell'intestazione IPv4 sono stati eliminati o resi facoltativi per ridurre i costi di elaborazione comuni della gestione dei pacchetti e per limitare il costo della larghezza di banda dell'intestazione IPv6.

Supporto migliorato per estensioni e opzioni

Le modifiche nel modo in cui le opzioni dell'intestazione IP sono codificate consentono un inoltro più efficiente, limiti meno rigidi sulla lunghezza delle opzioni e una maggiore flessibilità per l'introduzione di nuove opzioni in futuro.

Funzionalità di etichettatura flusso

Viene aggiunta una nuova funzionalità per abilitare l'etichettatura dei pacchetti che appartengono a particolari *flussi di* traffico per i quali il mittente richiede una gestione speciale, come QoS (Quality of Service) non predefinita o servizio *in tempo reale*.

Funzionalità di autenticazione e privacy

Le estensioni utilizzate per supportare l'autenticazione, l'integrità dei dati e la riservatezza dei dati (facoltativa) sono specificate per IPv6.

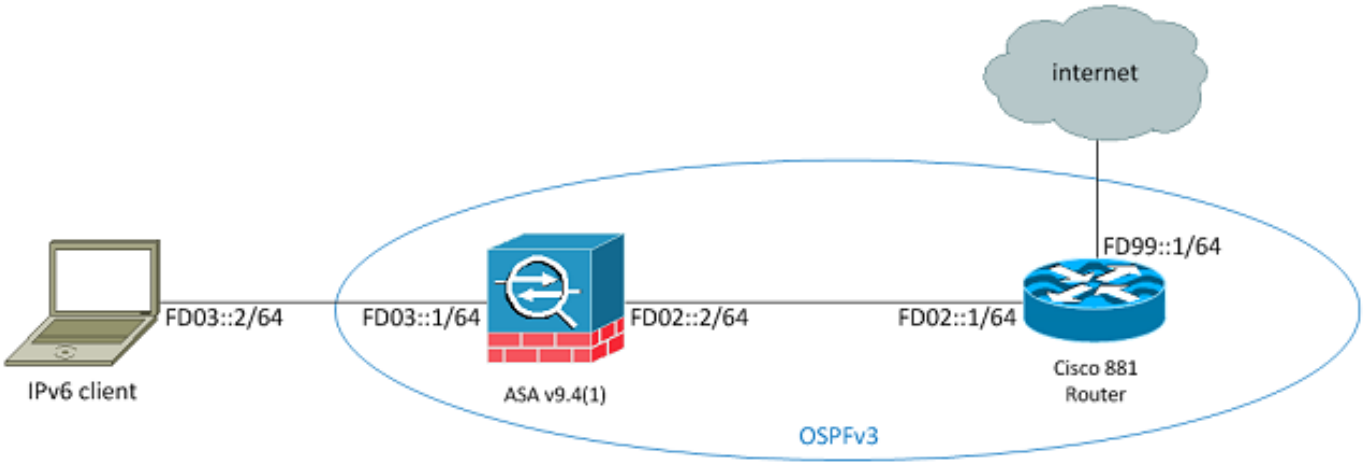
Configurazione

In questa sezione viene descritto come configurare Cisco ASA per l'utilizzo di IPv6.

> **Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Questa è la topologia IPv6 per gli esempi utilizzati in questo documento:



Configura interfacce per IPv6

Per passare il traffico IPv6 attraverso un'appliance ASA, è necessario prima abilitare IPv6 su almeno due interfacce. Nell'esempio viene descritto come abilitare IPv6 per passare il traffico dall'interfaccia interna su **Gi0/0** all'interfaccia esterna su **Gi0/1**:

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

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

Èora possibile configurare gli indirizzi IPv6 su entrambe le interfacce.

> **Nota:** Nell'esempio vengono utilizzati gli indirizzi nello spazio degli indirizzi locali univoci (ULA) di fc00::/7, quindi tutti gli indirizzi iniziano con **DF** (ad esempio, fdxx:xxxx:xxxx....). Inoltre, quando si scrivono indirizzi IPv6, è possibile utilizzare due punti (**::**) per rappresentare una linea di zeri in modo che **FD01::1/64** sia uguale a **FD01:0000:0000:0000:0000:0000:0000:0000:00001**.

```
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
```

A questo punto, è necessario avere la connettività di base di layer 2 (L2)/layer 3 (L3) a un router upstream sulla VLAN esterna all'indirizzo **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
```

Configura routing IPv6

Come con IPv4, anche se esiste una connettività IPv6 con gli host nella subnet a connessione diretta, è necessario disporre comunque delle route alle reti esterne per poterle raggiungere. Nel primo esempio viene illustrato come configurare una route statica predefinita per raggiungere tutte le reti IPv6 tramite l'interfaccia esterna con un indirizzo hop successivo **fd02::1**.

Configura routing statico per IPv6

Utilizzare queste informazioni per configurare il routing statico per 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)#
```

Come mostrato, ora è disponibile la connettività a un host su una subnet esterna:

```
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)#
```

> **Nota:** Se si desidera un protocollo di routing dinamico per gestire il routing per IPv6, è possibile configurare anche tale protocollo. Questa procedura viene descritta nella sezione successiva.

Configurazione del routing dinamico per IPv6 con OSPFv3

Innanzitutto, è necessario esaminare la configurazione OSPFv3 (Open Shortest Path First Version 3) sul Cisco serie 881 Integrated Services Router (ISR) a monte:

```
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.
```

Di seguito è riportata la configurazione dell'interfaccia interessata:

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

Èpossibile usare le acquisizioni dei pacchetti ASA per verificare che i pacchetti OSPF *Hello* vengano visti dall'ISR sull'interfaccia esterna:

```
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)#
```

Nella precedente acquisizione di pacchetti, è possibile osservare che i pacchetti OSPF (**ip-proto-89**) provengono dall'indirizzo locale del collegamento IPv6, che corrisponde all'interfaccia corretta dell'ISR:

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

Èquindi possibile creare un processo OSPFv3 sull'appliance ASA per stabilire una relazione con l'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
```

Applicare la configurazione OSPF all'interfaccia esterna ASA:

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

In questo modo l'ASA dovrebbe inviare i pacchetti broadcast OSPF Hello sulla subnet IPv6. Immettere il comando **show ipv6 ospf neighbors** per verificare le adiacenze con il router:

```
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
```

Èinoltre possibile confermare l'ID del router adiacente nell'RCI, in quanto per impostazione predefinita utilizza l'indirizzo IPv4 configurato con il valore più alto:

```
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#
```

L'appliance ASA deve aver acquisito la route IPv6 predefinita dall'ISR. Per confermare questa condizione, immettere il comando **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#
```

La configurazione di base delle impostazioni di interfaccia e delle funzionalità di routing per IPv6 sull'appliance ASA è ora completata.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Le procedure di risoluzione dei problemi per la connettività IPv6 seguono la maggior parte della stessa metodologia utilizzata per risolvere i problemi di connettività IPv4, con alcune differenze. Dal punto di vista della risoluzione dei problemi, una delle differenze più importanti tra IPv4 e IPv6 è che il protocollo ARP (Address Resolution Protocol) non esiste più in IPv6. Anziché utilizzare ARP per risolvere gli indirizzi IP sul segmento LAN locale, IPv6 utilizza un protocollo denominato ND (Neighbor Discovery).

Èinoltre importante comprendere che la tecnologia ND sfrutta il protocollo ICMPv6 (Internet Control Message Protocol versione 6) per la risoluzione degli indirizzi MAC (Media Access Control). Per ulteriori informazioni sulla DND IPv6, vedere la guida alla configurazione dell'IPv6 ASA nella sezione Individuazione router adiacenti IPv6 della *CLI Book 1: Guida alla configurazione della CLI per le operazioni generali della serie Cisco ASA, 9.4* o RFC 4861.

Attualmente, la maggior parte delle operazioni di risoluzione dei problemi relativi a IPv6 riguarda problemi di tipo ND, routing o configurazione subnet. Ciò è probabilmente dovuto al fatto che queste sono anche le differenze chiave tra IPv4 e IPv6. La funzione ND funziona in modo diverso rispetto alla funzione ARP e anche l'indirizzamento di rete interno è abbastanza diverso, in quanto l'uso di NAT è fortemente sconsigliato in IPv6 e l'indirizzamento privato non è più sfruttato come in IPv4 (dopo la RFC 1918). Una volta comprese queste differenze e/o risolti i problemi L2/L3, il processo di risoluzione dei problemi sul layer 4 (L4) e superiori è essenzialmente lo stesso utilizzato per l'IPv4, in quanto il protocollo TCP/UDP e i protocolli di livello superiore funzionano essenzialmente nello stesso modo (a prescindere dalla versione IP in uso).

Risoluzione dei problemi relativi alla connettività L2 (ND)

Il comando di base utilizzato per risolvere i problemi di connettività L2 con IPv6 è **show ipv6 neighbors [nameif]**, equivalente al comando **show arp** per IPv4.

Di seguito è riportato un esempio di output:

```
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)#
```

In questo output è possibile verificare la risoluzione corretta per l'indirizzo IPv6 di **fd02::1**, che appartiene al dispositivo con indirizzo MAC **c471.fe93.b516**.

> **Nota:** Si noti che lo stesso indirizzo MAC dell'interfaccia del router viene visualizzato due volte nell'output precedente perché il router ha anche un indirizzo locale del collegamento assegnato automaticamente per questa interfaccia. L'indirizzo locale del collegamento è un indirizzo specifico del dispositivo che può essere utilizzato solo per la comunicazione sulla rete connessa direttamente. I router non inoltrano i pacchetti tramite indirizzi locali del collegamento, ma solo per la comunicazione sul segmento di rete a connessione diretta. Molti protocolli di routing IPv6 (ad esempio OSPFv3) utilizzano indirizzi locali del collegamento per condividere le informazioni del protocollo di routing sul segmento L2.

Per cancellare la cache ND, immettere il comando **clear ipv6 neighbors**. Se l'operazione di ND non riesce per un determinato host, è possibile immettere il comando **debug ipv6 nd** nonché eseguire l'acquisizione dei pacchetti e verificare i syslog, per determinare che si verifica al livello L2. Tenere presente che il protocollo di rilevamento adiacente IPv6 utilizza messaggi ICMPv6 per risolvere gli indirizzi MAC degli indirizzi IPv6.

Confronto tra ARP IPv4 e ND IPv6

Si consideri la tabella di confronto ARP per IPv4 e ND per IPv6:

ARP IPv4	ND IPv6
RICHIESTA ARP (Chi ha 10.10.10.1?)	Richiesta router adiacente
ARP REPLY (10.10.10.1 è su dead.dead.dead)	Annuncio router adiacente

Nello scenario successivo, il ND non riesce a risolvere l'indirizzo MAC dell'host *fd02::1* che si trova sull'interfaccia esterna.

Debug ND

Di seguito è riportato l'output del comando **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: 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
```

In questo output di debug, *sembra* che gli annunci router adiacenti da **fd02::2** non vengano mai ricevuti. È possibile controllare le clip del pacchetto per confermare se è così.

Acquisizioni pacchetti ND

> **Nota:** A partire dalla versione ASA 9.4(1), gli elenchi degli accessi sono ancora necessari per le acquisizioni dei pacchetti IPv6. È stata inviata una richiesta di miglioramento per tenere traccia di questo problema con l'ID bug Cisco CSCtn09836.

Configurare l'Access Control List (ACL) e le acquisizioni dei pacchetti:

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

Eseguire il ping tra **fd02::1** e 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]
```

Come mostrato nelle acquisizioni dei pacchetti, vengono ricevute le pubblicità dei router adiacenti

da **fd02::1**. Tuttavia, gli annunci non vengono elaborati per qualche motivo, come mostrato negli output di debug. Per un ulteriore esame, è possibile visualizzare i syslog.

Syslog ND

Di seguito sono riportati alcuni esempi di registri di sistema ND:

```
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
```

All'interno di questi syslog, è possibile notare che i pacchetti di Annuncio router adiacente ND provenienti dall'ISR in **fd02::1** vengono scartati a causa di controlli non riusciti del formato EUI 64 (Modified EUI-64).

> **Suggerimento**: Per ulteriori informazioni su questo problema specifico, fare riferimento alla sezione *Codifica degli indirizzi EUI-64 modificata* di questo documento. Questa logica di risoluzione dei problemi può essere applicata anche a tutti i tipi di motivi di eliminazione, ad esempio quando gli ACL non consentono l'uso di ICMPv6 su un'interfaccia specifica o quando si verificano errori nel controllo Unicast Reverse Path Forwarding (uRPF), entrambi i quali possono causare problemi di connettività L2 con IPv6.

Risoluzione dei problemi relativi al routing IPv6 di base

Le procedure di risoluzione dei problemi per i protocolli di routing quando si utilizza IPv6 sono essenzialmente le stesse di quelle quando si utilizza IPv4. L'uso dei comandi **debug** e **show**, così come le acquisizioni dei pacchetti, sono utili per verificare il motivo per cui un protocollo di routing non si comporta come previsto.

Debug del protocollo di routing per IPv6

In questa sezione vengono forniti i comandi di debug utili per IPv6.

Debug globali del routing IPv6

Èpossibile utilizzare il comando **debug ipv6 routing** per risolvere i problemi relativi a tutte le modifiche apportate alla tabella di routing 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
```

Debug OSPFv3

Èpossibile utilizzare il comando **debug ipv6 ospf** per risolvere i problemi relativi a 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
```

Di seguito è riportato un esempio di output per tutti i debug abilitati dopo il riavvio del processo 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
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
```

Protocollo EIGRP (Enhanced Interior Gateway Routing Protocol)

L'EIGRP sull'appliance ASA non supporta l'uso del protocollo IPv6. Fare riferimento alla sezione Guidelines for EIGRP del *manuale CLI 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.4*.

Border Gateway Protocol (BGP)

Questo comando **debug** può essere usato per risolvere i problemi di BGP quando si usa IPv6:

```
ASAv# debug ip bgp ipv6 unicast  ?

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

Utili comandi Show per IPv6

Èpossibile utilizzare i seguenti comandi **show** per risolvere i problemi relativi al protocollo IPv6:

- **mostra route ipv6**
- **mostra descrizione interfaccia ipv6**
- **show ipv6 ospf <ID processo>**
- **mostra traffico ipv6**
- **mostra router adiacente ipv6**
- **mostra icmp ipv6**

Packet Tracer con IPv6

Èpossibile utilizzare la funzionalità di traccia dei pacchetti incorporata con IPv6 sull'appliance ASA allo stesso modo dell'IPv4. Di seguito è riportato un esempio in cui viene utilizzata la funzionalità

di traccia dei pacchetti per simulare l'host interno in **fd03::2**, che tenta di connettersi a un server Web in **5555::1** che si trova su Internet con il percorso predefinito appreso dall'interfaccia **881** tramite 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#
```

L'indirizzo MAC in uscita è l'indirizzo locale del collegamento dell'interfaccia 881. Come accennato in precedenza, per molti protocolli di routing dinamico i router utilizzano indirizzi IPv6 locali del collegamento per stabilire le adiacenze.

Elenco completo dei debug ASA correlati a IPv6

Di seguito sono riportati i debug che è possibile utilizzare per risolvere i problemi relativi al protocollo 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
```

Problemi comuni correlati a IPv6

In questa sezione viene descritto come risolvere i problemi più comuni relativi a IPv6.

Subnet non configurate correttamente

Molti casi di TAC IPv6 vengono generati a causa di una generale mancanza di informazioni sul funzionamento di IPv6 o a causa di tentativi dell'amministratore di implementare IPv6 utilizzando processi specifici di IPv4.

Ad esempio, TAC ha rilevato casi in cui a un amministratore è stato assegnato un blocco \56 di indirizzi IPv6 da un provider di servizi Internet (ISP). L'amministratore assegna quindi un indirizzo e la subnet \56 completa all'interfaccia esterna dell'ASA e sceglie un intervallo interno da utilizzare per i server interni. Con IPv6, tuttavia, tutti gli host interni devono utilizzare anche indirizzi IPv6 instradabili e il blocco di indirizzi IPv6 deve essere suddiviso in subnet più piccole, in base alle esigenze. In questo scenario è possibile creare molte subnet \64 come parte del blocco \56 allocato.

> **Suggerimento**: Per ulteriori informazioni, fare riferimento alla RFC 4291.

Codifica EUI 64 modificata

L'ASA può essere configurata in modo da richiedere indirizzi IPv6 con codifica EUI-64 modificati. In base alla RFC 4291, l'interfaccia EUI consente a un host di assegnarsi un identificatore di interfaccia IPv6 univoco a 64 bit (EUI-64). Questa funzionalità rappresenta un vantaggio rispetto a IPv4, in quanto elimina la necessità di utilizzare DHCP per l'assegnazione degli indirizzi IPv6.

Se l'appliance ASA è configurata in modo da richiedere questo miglioramento tramite il comando **ipv6 enforce-eui64 nameif**, è probabile che vengano eliminate molte richieste di individuazione di router adiacenti e annunci da altri host nella subnet locale.

> **Suggerimento**: Per ulteriori informazioni, fare riferimento al documento della Cisco Support Community sulla descrizione dell'indirizzo IPv6 EUI-64 bit.

I client utilizzano indirizzi IPv6 temporanei per impostazione predefinita

Per impostazione predefinita, molti sistemi operativi client, ad esempio Microsoft Windows versioni 7 e 8, Macintosh OS-X e sistemi basati su Linux, utilizzano indirizzi IPv6 *temporanei* autoassegnati per una maggiore riservatezza tramite la configurazione automatica degli indirizzi stateless (SLAAC) di IPv6.

In Cisco TAC sono stati rilevati alcuni casi in cui ciò ha causato problemi imprevisti negli ambienti, in quanto gli host generano traffico dall'indirizzo temporaneo e non da quello assegnato staticamente. Di conseguenza, gli ACL e i percorsi basati sull'host potrebbero causare l'eliminazione o il routing non corretto del traffico, compromettendo la comunicazione con l'host.

Per risolvere questa situazione, vengono utilizzati due metodi. Il comportamento può essere disabilitato singolarmente sui sistemi client o sui router ASA e Cisco IOS®. Sul lato ASA o router, è necessario modificare il flag del messaggio Router Advertisement (RA) che attiva questo comportamento.

Per disabilitare questo comportamento sui singoli sistemi client, consultare le sezioni seguenti.

Microsoft Windows

Per disabilitare questo comportamento sui sistemi Microsoft Windows, completare la procedura seguente:

1. In Microsoft Windows aprire un prompt dei comandi con privilegi elevati (esegui come amministratore).

2. Immettere questo comando per disabilitare la funzionalità di generazione degli indirizzi IP casuali e quindi premere **Invio**:

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

3. Immettere questo comando per forzare Microsoft Windows a utilizzare lo standard EUI-64:

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

4. Riavviare il computer per applicare le modifiche.

Macintosh OS-X

In un terminale, immettere questo comando per disabilitare lo SLAAC IPv6 sull'host fino al successivo riavvio:

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

Per rendere la configurazione permanente, immettere questo comando:

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

Linux

In una shell del terminale, immettere questo comando:

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

Disabilitazione globale di SLAAC dall'appliance ASA

Il secondo metodo utilizzato per risolvere questo problema è modificare il messaggio RA inviato dall'ASA ai client, in modo da attivare l'uso dello SLAAC. Per modificare il messaggio RSA, immettere questo comando dalla modalità di *configurazione interfaccia*:

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

Questo comando modifica il messaggio RA inviato dall'ASA in modo che il flag A-bit non sia impostato e i client non generino un indirizzo IPv6 temporaneo.

> **Suggerimento**: Per ulteriori informazioni, fare riferimento alla RFC 4941.

Domande frequenti su IPv6

In questa sezione vengono descritte alcune domande frequenti relative all'utilizzo di IPv6.

Èpossibile passare il traffico per IPv4 e IPv6 sulla stessa interfaccia contemporaneamente?

Sì. È sufficiente abilitare IPv6 sull'interfaccia e assegnare sia un indirizzo IPv4 che un indirizzo IPv6 all'interfaccia, che gestirà contemporaneamente entrambi i tipi di traffico.

Èpossibile applicare gli ACL IPv6 e IPv4 alla stessa interfaccia?

Questa operazione può essere eseguita nelle versioni ASA precedenti alla versione 9.0(1). A partire dalla versione 9.0(1), tutti gli ACL sull'appliance ASA sono *unificati*, ossia un ACL supporta una combinazione di voci IPv4 e IPv6 nello stesso ACL.

Nelle versioni ASA 9.0(1) e successive, gli ACL vengono semplicemente uniti e l'ACL singolo e unificato viene applicato all'interfaccia con il comando **access-group**.

L'appliance ASA supporta QoS per IPv6?

Sì. L'ASA supporta il policing e le code di priorità per IPv6 nello stesso modo in cui lo supporta con IPv4.

A partire dalla versione 9.0(1), tutti gli ACL sull'appliance ASA sono *unificati*, ossia un ACL supporta una combinazione di voci IPv4 e IPv6 nello stesso ACL. Di conseguenza, tutti i comandi QoS eseguiti su una mappa di classe corrispondente a un ACL eseguono un'azione sia sul traffico IPv4 che sul traffico IPv6.

Èconsigliabile utilizzare NAT con IPv6?

Sebbene NAT possa essere configurato per IPv6 sull'appliance ASA, l'utilizzo di NAT nell'IPv6 è fortemente sconsigliato e non necessario, data la quantità pressoché infinita di indirizzi IPv6 disponibili e instradabili globalmente.

Se in uno scenario IPv6 è richiesto NAT, è possibile trovare ulteriori informazioni su come configurarlo nella sezione Linee guida NAT IPv6 del *Manuale CLI 2: Guida alla configurazione della CLI del firewall Cisco serie ASA, 9.4*.

> **Nota:** Quando si implementa NAT con IPv6 è necessario tenere presenti alcune linee guida e limitazioni.

Perché gli indirizzi IPv6 locali del collegamento vengono visualizzati nell'output del comando *show failover*?

In IPv6, ND utilizza indirizzi locali del collegamento per eseguire la risoluzione degli indirizzi L2. Per questo motivo, gli indirizzi IPv6 per le interfacce monitorate nell'output del comando **show failover** mostrano l'indirizzo locale del collegamento e non l'indirizzo IPv6 globale configurato nell'interfaccia. Si tratta di un comportamento normale.

Richieste di miglioramento/avvertenze note

Di seguito sono riportate alcune note avvertenze relative all'utilizzo di IPv6:

- L'ID bug Cisco CSCtn09836Â *la clausola "match" dell'acquisizione ASA 8.x non intercetta il traffico IPv6*
- ID bug Cisco CSCuq85949Â *ENH: Supporto ASA IPv6 per WCCP*
- L'ID bug Cisco CSCut78380ÂÂ il *routing ECMP IPv6 dell'ASA non bilancia il carico del traffico*

Informazioni correlate

- RFC 2460 - Â Protocollo Internet, specifica versione 6 (IPv6)
- RFC 4291 - Â Architettura di indirizzamento IP versione 6
- RFC 4861Â Neighbor Discovery for IP versione 6 (IPv6)
- CLI Book 1: Guida alla configurazione della CLI per le operazioni generali della serie Cisco ASA, 9.4Â IPv6
- AnyConnect SSL su IPv4+IPv6 su configurazione ASA
- Documentazione e supporto tecnicoÂ Cisco Systems