Ipv6 トラフィックを通過させるための ASA の設定

内容

概要

このドキュメントでは、インターネット プロトコル バージョン 6（IPv6）トラフィックを伝送するために Cisco 適応型セキュリティ アプライアンス（ASA）を設定する方法について、ASA バージョン 7.0(1) 以降に関して説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco ASA バージョン 7.0(1) 以降に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

現在、IPv6 は、市場への普及の面ではまだ新しいものといえます。しかし、IPv6 の設定アシスタンスやトラブルシューティングに関しての要求には着実に増えてきました。このドキュメントの目的はこのようなニーズに応え、さらに以下を提供することです。

- IPv6 使用に関する一般的な概要
- ASA での基本的な IPv6 設定
- ASA を介した IPv6 接続のトラブルシューティングの方法に関する情報
- Cisco Technical Assistance Center（TAC）が特定した、最も多く見られる IPv6 の問題と解決方法。

注：IPv6 は世界で IPv4 を代替するにはまだ初期の段階にある点を考慮し、このドキュメントは正確で必要な情報を盛り込むことができるように定期的に更新されます。

IPv6 機能の情報

IPv6 の機能に関する重要な情報を次に示します。

- IPv6 プロトコルは、ASA のバージョン 7.0(1) で最初に導入されました。
- トランスペアレント モードで IPv6 のサポートは ASA バージョン 8.2(1) に導入されました。

IPv6 の概要

IPv6 プロトコルは、1990 年代の中期から後期にかけて開発されました。この時期に公共の IPv4 アドレス空間の枯渇が加速したことが、開発が進んだ主な要因です。ネットワーク アドレス変換（NAT）の登場は IPv4 にとって劇的に役に立ち、この問題への対処を先延ばしにすることができましたが、最終的にはこれに代わるプロトコルが必要となることは否定できなくなりました。IPv6 プロトコルの詳細の仕様は 1998 年 12 月の RFC 2460 で正式に決まりました。このプロトコルについての詳細は、Internet Engineering Task Force（IETF）の Web サイトにある公式の RFC 2460 のドキュメントを参照してください。

IPv4 に対する IPv6 の改良点

このセクションでは、IPv6 プロトコルに含まれる改善と、従来の IPv4 プロトコルを対比させて説明します。

アドレッシング機能の拡張

IPv6 プロトコルでは、IP アドレスのサイズが 32 ビットから 128 ビットに拡大しました。これにより、サポートされるアドレシング階層が増大し、より多くのノードにアドレスの割り当てが可能になり、アドレスの自動設定が簡略化されました。マルチキャストルーティングのスケーラビリティは、マルチキャストアドレスにスコープフィールドを追加することで向上します。さらに、エニーキャストアドレスと呼ばれる新しいタイプのアドレスが定義されます。これは、グループ内の任意のノードにパケットを送信するために使用されます。

ヘッダー形式の簡略化

IPv4 ヘッダーの一部が削除され、または省略可能になりました。これにより、一般的なケースのパケット処理のコストが低減し、IPv6 ヘッダーの帯域幅コストが制限されます。

拡張とオプションのサポート改善

IP ヘッダー オプションのエンコード方法が変わったことにより、フォワーディングが効率化され、オプションの長さに対する制限が緩和されるとともに、今後新しいオプションを導入する際の柔軟性が向上しました。

フロー ラベル機能

この新機能で、送信者が特定のトラフィック フローに属するパケットにラベリングを行うことにより、そのトラフィック フローに対して、デフォルト以外の Quality of Service（QoS）やリアルタイム サービスなどの特別な処理を要求できるようになりました。

認証とプライバシーの機能

IPv6 には、認証、データの整合性、機密（オプション）をサポートするための機能拡張が仕様に盛り込まれています。

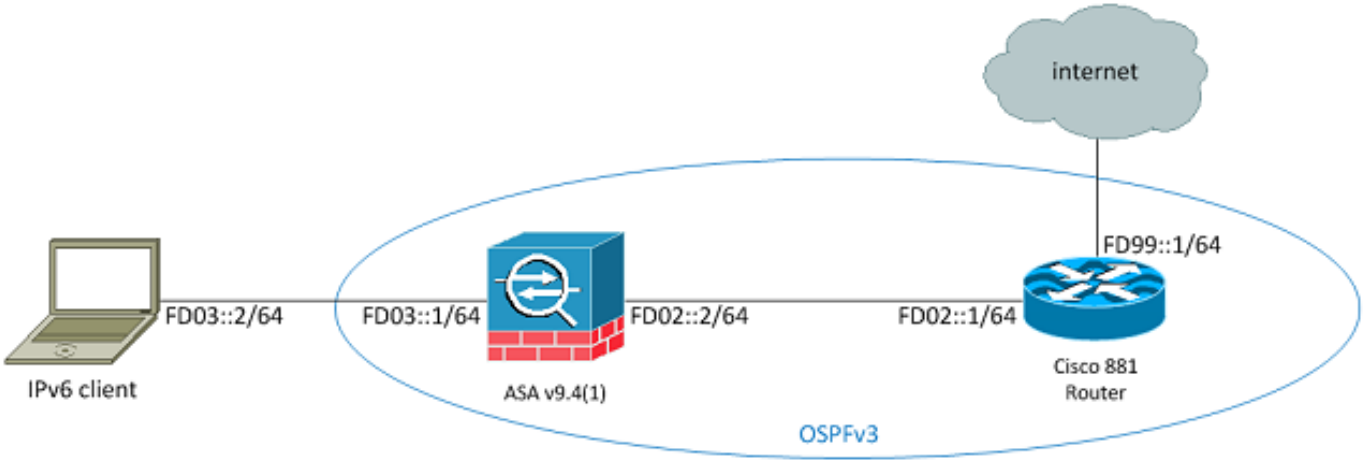
設定

このセクションでは、Cisco ASA を IPv6 で使用するための設定方法について説明します。

> **注**：このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントの各例における IPv6 とトポロジを以下に示します。



IPv6 のインターフェイスの設定

IPv6 トラフィックを ASA を介して伝送するには、まず、少なくとも 2 つのインターフェイスで IPv6 を有効にする必要があります。この例では、内部インターフェイス **Gi0/0 から外部インターフェイス Gi0/1** にトラフィックを通すために IPv6 を有効にする方法を説明します。

```
ASAv(config)# interface GigabitEthernet0/0
```

```
ASAv(config-if)# ipv6 enable

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

今度は、両方のインターフェイスに IPv6 アドレスを設定できます。

> **注**：この例では、fc00::/7のユニークローカルアドレス(ULA)空間のアドレスが使用されているため、すべてのアドレスはFD(fdxx:xxxx:xxxxなど)で始まります。.) . また、IPv6 アドレスの表記では、ダブルコロン (::) を使って一連のゼロを表記できるため、FD01::1/64 は FD01:0000:0000:0000:0000:0000:0000:00001 と同じです。

```
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
```

これでアドレス fd02::1 にて外部 VLAN の上流に位置するルータへの基本的なレイヤ 2 (L2)/レイヤ 3 (L3) 接続が確立されたはずです。

```
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
```

IPv6 ルーティングの設定

IPv4 と同様に、直接接続されたサブネット上のホストに IPv6 接続があったとしても、到達経路を知るために外部ネットワークへのルートが必要です。最初の例では、ネクスト ホップ アドレス fd02::1 で外部インターフェイスを介してすべての IPv6 ネットワークに到達するための静的なデフォルトルートの設定方法を示しています。

IPv6 のスタティック ルーティングの設定

次の情報を使用して、IPv6 のスタティック ルーティングを設定します。

```
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)#
```

表示のとおり、これで外部サブネットでのホストへの接続ができました。

```
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)#
```

> **注**：IPv6 ルーティングを動的に行いたい場合、ダイナミック ルーティング プロトコルも設定できます。このことについては、次のセクションで説明します。

OSPFv3 での IPv6 のダイナミック ルート設定

まず、アップストリームの Cisco 881 シリーズ サービス統合型ルータ（ISR）の Open Shortest Path First バージョン 3（OSPFv3）の設定を確認する必要があります。

```
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.
```

該当するインターフェイス設定は次のようになります。

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

```
ipv6 ospf 1 area 0
C881#
```

ASA パケット キャプチャを使い、OSPF の *Hello パケットが外部インターフェイスの ISR から見えることを確認できます。*

```
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)#
```

前述のパケット キャプチャで、OSPF（ip-proto-89）パケットが ISR の正しいインターフェイスに該当する IPv6 リンクローカル アドレスから到着することを確認できます。

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

今度は、ISR との隣接関係を確立するため ASA で OSPFv3 プロセスを作成できます。

```
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
```

ASA の外部インターフェイスに OSPF 設定を適用します。

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

これにより、ASA は IPv6 サブネットに OSPF ブロードキャスト Hello パケットを送出します。**show ipv6 ospf neighbor コマンドを入力し、ルータとの隣接関係を確認します。**

```
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
```

ISR は、デフォルトで最も高く設定された IPv4 アドレスを ID に使用するため、ISR でネイバー ID を確認できます。

```
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#
```

これで ASA は ISR からデフォルトの IPv6 ルートを学習できているはずです。これを確認するには、**show ipv6 route コマンドを入力します。**

```
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#
```
ASA での IPv6 用のインターフェイス設定とルーティング機能の基本設定はこれで完了です。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

IPv6 接続のトラブルシューティング手順は IPv4 接続のトラブルシューティングと同じ方法に従いますが、いくつかの違いがあります。トラブルシューティングの観点から見ると、IPv4とIPv6の最も重要な相違点の1つは、IPv6にAddress Resolution Protocol(ARP)が存在しないことです。ローカルLANセグメントのIPアドレスを解決するためにARPを使用します。

また、ND が Media Access Control（MAC）アドレス解決に Internet Control Message Protocol バージョン 6（ICMPv6）を活用することを理解することも重要です。IPv6 ND の詳細については、IPv6 ネイバー検索（*CLI ブック 1：Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）9.4 ）*、*または* RFC 4861 内の ASA IPv6 コンフィギュレーション ガイドを参照してください。

現在、ほとんどの Ipv6 関連のトラブルシューティングは ND、ルーティング、またはサブネット設定の問題のいずれかに関連しています。これは、IPv4とIPv6の主な違いでもあります。IPv6でNATを使用することは推奨されず、プライベートアドレッシングはIPv4（RFC 1918以降）で利用されなくなったため、NDはARPとは異なります.. これらの違いを理解し、L2/L3 の問題を解決すれば、TCP/UDP と高位層のプロトコルの機能は（IP のバージョンを問わず）本質的に同じなため、レイヤ 4（L4）以上のトラブルシューティング プロセスは、IPv4 と本質的に同じになります。

L2 接続のトラブルシューティング（ND）

L2 の IPv6 接続をトラブルシュートするために使用される最も基本的なコマンドは、**show ipv6 neighbor [nameif] コマンドです。これは、IPv4 の show arp コマンドに相当するものです。**

次に出力例を示します。

```
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)#
```
この出力では、MAC アドレス **c471.fe93.b516** を持つデバイスに属する IPv6 アドレス **fd02::1** が正常に解決されたことが確認できます。

注：前述の出力ではルータ インターフェイスの同じ MAC アドレスが 2 回現れますが、これは、ルータがこのインターフェイスにリンクローカル アドレスを自ら割り当てたことが原因です。リンクローカル アドレスはデバイス固有のアドレスで、直接接続されたネットワークでの通信にのみ使用できます。ルータは、リンクローカル アドレスを介してパケットを転送しません。これらは、直接接続されたネットワークのセグメントでの通信のみを行います。多くの IPv6 ルーティング プロトコル（OSPFv3 など）は、L2 セグメントのルーティングプロトコルを共有するためにリンクローカル アドレスを使用します。

ND キャッシュをクリアするには、**clear ipv6 neighbors コマンドを入力します。**ND が特定のホストについて失敗する場合、**debug ipv6 nd** コマンドを入力し、またパケット キャプチャを実行して syslog を確認し、問題が L2 で発生していることを確かめることができます。IPv6 の ND は MAC アドレスの IPv6 アドレスへの解決に ICMPv6 メッセージを使用することに注意してください。

IPv4 ARP 対 IPv6 ND

IPv4 向けの ARP のテーブルと、IPv6 の ND の比較表を以下に示します。この表について考えます。

IPv4 ARP	IPv6 ND
ARP 要求（10.10.10.1 は誰なのか）	ネイバー要請
ARP 応答（10.10.10.1 は dead.dead.dead に存在）	ネイバー アドバタイズメント

次のシナリオでは、ND は MAC アドレス *fd02::1 の解決に失敗します。このホストは外部インターフェイスにあるホストです。*

ND のデバッグ

ここに示したのは、**debug ipv6 nd コマンドの出力結果です。**

```
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
```

このデバッグ出力では、**fd02::2 からのネイバー アドバタイズメントがまったく受信されていないように見えます。**パケット キャプチャを確認して、実際はどうであるかを調べることができます。

ND パケット キャプチャ

> **注：**ASA リリース 9.4(1) の時点では、IPv6 パケット キャプチャにはアクセスリストが引き続き必要です。Cisco Bug ID CSCtn09836 でこのことに対する機能拡張の要求を追跡できるよう指定されています。

アクセス コントロール リスト（ACL）とパケット キャプチャを設定します。

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

ASA から、fd02::1 に ping を行います。

```
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]
```

パケット キャプチャで示されたように、**fd02::1 からのネイバー アドバタイズメントが到着しています。**ただし、デバッグ出力に示されるように、アドバタイズメントは何らかの理由で処理されません。詳細な調査のために、syslogを表示できます。

ND の Syslog

以下は、ND の Syslog の例です。

```
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
```

これらの syslog の中で、**fd02::1 にある ISR からの ND ネイバー アドバタイズメント パケットは修正 Extended Unique Identifier（修正 EUI -64）のフォーマット チェックが失敗したことにより破棄されていることが確認できます。**

> **ヒント**：この特定の問題についての詳細は「*修正 EUI -64 アドレスエンコーディング*」を参照してください。このトラブルシューティングのロジックは、ACL が特定のインターフェイスで ICMPv6 を許可しない場合や Unicast Reverse Path Forwarding（uRPF）チェックが失敗する場合など、さまざまな種類の破棄の理由にも適用できます。上記の 2 つは、IPv6 での L2 接続の問題の原因となることがあります。

基本的な IPv6 ルーティングのトラブルシューティング

IPv6 を使用した場合のルーティング プロトコルのトラブルシューティング手順は、IPv4 を使用する場合と基本的に同じです。**debug および show コマンドの使用とパケット キャプチャは、ルーティング プロトコルが期待どおりに動作しない理由を確認するのに役立ちます。**

IPv6 のルーティング プロトコルのデバッグ

このセクションでは、IPv6 で役立つ debug コマンドを説明します。

グローバル IPv6 ルーティングのデバッグ

debug ipv6 routing のデバッグにより、IPv6 ルーティング テーブルの変更のすべてをトラブルシューティングできます。

```
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
```

OSPFv3 のデバッグ

debug ipv6 ospf コマンドにより、OSPFv3 の問題をトラブルシューティングできます。

```
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
```

OSPFv3 プロセスが再起動した後で有効にしたすべてのデバッグの出力例を示します。

```
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
```

ASA上のEIGRPはIPv6の使用をサポートしていません。CLIブック1の「EIGRPのガイドライン」セクションを*参照してください。Cisco ASA シリーズ CLI コンフィギュレーション ガイド 9.4（一般的な操作）」）を参照してください。*

ボーダー ゲートウェイ プロトコル（BGP）

この debug コマンドは、IPv6 を使用する場合の BGP のトラブルシューティングに使用できます。

```
ASAv# debug ip bgp ipv6 unicast  ?

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

IPv6 の便利な show コマンド

次の show コマンドを使用して、IPv6 に関連する問題のトラブルシューティングを行うことができます。

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

IPv6 のパケット トレーサ

IPv4と同じ方法でASA上のIPv6に組み込みのパケットトレーサ機能を使用できます。パケットトレーサ機能を使用して**fd03::2の内部ホストをシミュレートする例を示します**。 OSPF経由で881インターフェイスから学習したデフォルトルートを持つインターネット：

```
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#
```

出力 MAC アドレスは 881 インターフェイスのリンクローカル アドレスであることに注意してください。前述のように、大部分のダイナミック ルーティング プロトコルで、ルータは隣接関係の確立にリンクローカルの IPv6 アドレスを使用しています。

IPv6 関連の ASA のデバッグの完全なリスト

IPv6 の問題のトラブルシューティングに使用できるデバッグは次のとおりです。

```
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
```

IPv6 に関する一般的な問題

ここでは、最も多く見られる IPv6 関連の問題の解決方法について説明します。

不適切に設定されたサブネット

IPv6 に関連して Cisco Technical Assistance Center（TAC）に寄せられる問題の多くは、IPv6 がどのように関する機能するかについての知識の全般的な欠乏や、または IPv4 固有のプロセスを IPv6 にあてはめて実装する試みからきています。

たとえば、TAC ではインターネット サービス プロバイダー（ISP）によって管理者が IPv6 アドレスの /56 ブロックに割り当てられているケースを見たことがあります。 そうすると、管理者はアドレスと完全な /56 サブネットを ASA の外部インターフェイスに割り当て、いくつかの内部範囲を内部サーバで使用するために選択します。しかし、IPv6 では、すべての内部ホストもルーティング可能な IPv6 アドレスを使用する必要があり、IPv6 アドレス ブロックを必要に応じて小さなサブネットに分割する必要があります。このシナリオでは、割り当て済みの /56 ブロックの一部として、多くの /64 サブネットを作成できます。

> **ヒント**：詳細については、RFC 4291 を参照してください。

修正 EUI 64 エンコーディング

ASA は、修正 EUI -64 エンコーディングされた IPv6 アドレスを必須とするよう設定できます。RFC 4291 によれば、EUI では、ホストが自分自身に一意の 64 ビットの IPv6 インターフェイス ID（EUI-64）を割り当てることができます。 この機能は、IPv6 アドレス付与で DHCP を不要とするもので、IPv4 に対するメリットでもあります。

ASA がこの拡張機能を必須とするよう ipv6 enforce-eui64 nameif コマンドにより設定した場合、ローカル サブネットの他のホストからの多くのネイバー検索要請とアドバタイズメントをドロップすることになります。

> **ヒント**：詳細については、シスコ サポート コミュニティのドキュメント「IPv6 の EUI-64 ビット アドレスを理解する」を参照してください。

デフォルトでのクライアントの一時的な IPv6 アドレス使用

デフォルトでは、Microsoft Windows バージョン 7 および 8、マッキントッシュ OS-X や Linux システムなどの多くのクライアントのオペレーティング システム（OS）は、プライバシー向上のために IPv6 ステートレス アドレス自動設定（SLAAC）により自分自身に付与した*一時的な IPv6 アドレスを使用します。*

Cisco TAC では、このことによる動作環境上の予期されない問題がいくつか発生していました。これらの問題は、ホストが静的に割り当てられたアドレスではなく、一時アドレスからトラフィックを生成することが原因です。その結果、ACL とホストに基づいたルートがトラフィックの破棄や不適切なルーティングにつながり、これはホストの通信の失敗の原因となります。

この状況を解決するために使用される 2 つの方法があります。この挙動をクライアントシステムで個別に抑えるか、または ASA と Cisco IOS® ルータでこの動作を無効にすることができます。ASA、ルータ側では、この挙動を引き起こすルータ アドバタイズメント（RA）メッセージのフラグを変

更する必要があります。

個々のクライアントシステムでこの挙動を無効にするには、以下のセクションを参照してください。

Microsoft Windows

Microsoft Windows システムでこの挙動を無効にするには、次の手順を実行します:

1. Microsoft Windows で、管理者特権でのコマンド プロンプトを開きます（管理者として実行）。
2. ランダム IP アドレス生成機能を無効にするには、次のコマンドを入力して [Enter] を押します。

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

3. Microsoft Windows で EUI-64 規格の使用を必須とするには、このコマンドを入力します。

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

4. 変更を適用するため、マシンを再起動します。

マッキントッシュ OS-X

IPv6 SLAAC をホスト上で次のリブートまで無効にするには、端末でこのコマンドを入力します。

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

設定をいつも有効にするには、このコマンドを入力します。

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

Linux

端末のシェルで、このコマンドを入力します。

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

ASA から SLAAC をグローバルに無効にする

この挙動の問題を解決する 2 番目の方法は、SLAAC の使用をトリガーするため ASA からクライアントに送信される RA メッセージを変更することです。RA メッセージを変更するには、*インターフェイス コンフィギュレーション モードでこのコマンドを入力します。*

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

このコマンドで ASA が送信する RA メッセージを変更し、A- ビットのフラグを抑制することで、クライアントは一時的な IPv6 アドレスを生成しなくなります。

ヒント：詳細については、RFC 4941 を参照してください。

IPv6 FAQ

このセクションでは、IPv6 の使用についてよくある質問の説明をします。

同時に同じインターフェイスで IPv4 と IPv6 の両方のトラフィックを伝送できますか。

はい。インターフェイスで IPv6 を有効にし、インターフェイスに IPv4 および IPv6 アドレスの両方を割り当てるだけで、両方の種類のトラフィックを同時に扱えます。

同じインターフェイスで IPv6 および IPv4 ACL を適用できますか。

ASA バージョン 9.0(1) 以前では、これが可能です。 ASA バージョン 9.0(1) の時点で、ASA のすべての ACL は*統合*されました。つまり、単一の ACL で IPv4 と IPv6 の両方のエントリをサポートします。

ASA バージョン 9.0(1) 以降では、ACL は単に結合され、単一の統合 ACL が **access-group コマンドでインターフェイスに適用されています。**

ASA は IPv6 の QoS をサポートしますか。

はい。ASA では、IPv6 でのポリシングと優先度キューイングを IPv4 と同様にサポートしています。

ASA バージョン 9.0(1) の時点で、ASA のすべての ACL は*統合*されました。つまり、単一の ACL で IPv4 と IPv6 の両方のエントリをサポートします。その結果、ACL に一致するクラス マップに設定されたすべての QoS コマンドは IPv4 と IPv6 の両方のトラフィックに対して実行されます。

IPv6 で NAT を使用する必要はありますか。

ASA では IPv6 にも NAT を設定できますが、IPv6 での NAT の使用はまったく推奨されませんし、アドレスが無数に用意でき、グローバルなルーティングが可能な以上、NAT は不要です。

IPv6 シナリオで NAT が必要な場合、設定方法については[IPv6 NAT ガイドライン（「*CLI ブック 2：Cisco ASA シリーズ ファイアウォール CLI コンフィギュレーション ガイド 9.4*」）を参照してください。

注：IPv6 で NAT を実装する場合に従うべきガイドラインと制限事項があります。

show failover コマンドの出力に IPv6 リンクローカル アドレスが表示されるのはなぜですか。

IPv6 では、ND は L2 アドレス解決のためにリンクローカル アドレスを使用します。このため、

show failover コマンド出力にある、モニタ対象となっているインターフェイスの IPv6 アドレスには、このインターフェイスに設定されているグローバル IPv6 アドレスではなく、リンクローカル アドレスが表示されます。これは正常な動作です。

既知の注意事項/機能拡張要求

IPv6 の使用に関連した既知の注意事項のいくつかを次に示します。

- Cisco Bug ID CSCtn09836 âÂÂ *ASA 8.x キャプチャの「match」句が IPv6 トラフィックを捕捉しない*
- Cisco Bug ID CSCuq85949 âÂÂ *ENH:ASA による WCCP の IPv6 サポート*
- Cisco Bug ID CSCut78380 âÂÂ ASA IPv6 ECMP ルーティングでトラフィックのロード バランシングが行われない

関連情報

- RFC 2460 âÂÂ, Internet Protocol, Versionb 6 (IPv6) Specification
- RFC 4291 âÂÂ, IP Version 6 Addressing Architecture
- RFC 4861 âÂÂ Neighbor Discovery for IP Version 6 (IPv6)
- CLI ブック 1：Cisco ASA シリーズ CLI コンフィギュレーション ガイド 9.4 âÂÂ IPv6 (一般的な操作)
- IPv4+IPv6 を介して ASA コンフィギュレーションに対する AnyConnect SSL
- テクニカル サポートとドキュメント - Cisco Systems