CHAPTER 21

IPv6 の設定

IPng（next generation）と呼ばれていた Internet Protocol version 6（IPv6）は、IP の最新バージョンにあたります。IPv6 は、アドレス スペースが拡張されるなど、以前の IP バージョンと比べて多数の利点を備えています。IPv6 は、PRE2 プロセッサを実行している Cisco 10000 シリーズ ルータで利用でき、他のシスコ社のプラットフォームでは Cisco IOS Release 12.2(28)SB のリリースから利用されています。

これらの IPv6 機能の Cisco プラットフォームにおける設定および使用方法については、次の URL にある『*Cisco IOS IPv6 Implementation Library*』を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00805766e4.html.

この章では、IPv6 機能の次の内容について説明します。

IPv6 機能の履歴

Cisco IOS リリース	説明	必要な PRE
12.2(28)SB	この機能が Cisco 10000 シリーズ ルータに導入されました。	PRE2
12.2(31)SB2	PRE3 のサポートが追加されました。 拡張 Access Control List（ACL; アクセス制御リスト）のサポートが追加されました。	PRE3

サポートされる機能

Cisco 10000 シリーズ ルータは、次の IPv6 PXF 機能をサポートしています。

- IPv4 との共存
- IPv6 アドレッシング
- IPv6 拡張ヘッダー。拡張ヘッダーの PXF 処理には、次の内容が含まれます。
  - ホップバイホップ拡張ヘッダー付きパケットの迂回
  - フラグメントの照合とルーティング ヘッダーの存在の確認
  - レイヤ 4 情報に到達するための拡張ヘッダーの省略
  - 「不明の送信」ACL フラグを照合するフラグ設定
- IPv6 Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）
- IPv6 NDP
- IPv6 レイヤ 2 カプセル化。内容は次のとおりです。
  - Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）
  - Multilink PPP（MLSP; マルチリンク PPP）
  - High-level Data Link Control（HDLC; ハイレベル データリンク コントロール）
  - VLAN
  - ポイントツーポイント フレームリレー
  - ポイントツーポイント ATM
- IPv6 ルーティング。内容は次のとおりです。
  - スタティック
  - Routing Information Protocol Next-Generation（RIPng）
  - Open Shortest Path First Version 3（OSPFv3）
  - Border Gateway Protocol - version 4（BGP4+）
  - Intermediate System-to-Intermediate System version 6（ISISv6）
- IPv6 トンネリング（手動および Generic Routing Encapsulation［GRE; 総称ルーティング カプセル化］）
  - 手動で設定された双方向の IPv6-in-IPv4 GRE トンネル
  - 手動で設定された双方向の IPv4-over-IPv4 トンネル
    最大 1000 の IPIP または GRE トンネル
- HA/ISSU の共存（IPv6 は RPR+ をサポートします）
- IPv6 ユニキャスト転送

  Cisco 10000 シリーズ ルータは、次のグローバルな IPv6 特有のパケット カウンタを維持します（指定されている場合を除く）。
  - forwarded — 転送された IPv6 パケット数

- no adjacency — adj_index=0 によってパントされた IPv6 パケット数。各 VCCI の統計情報は、この特有のパントが発生した場合（迂回の要因）に収集されます。
- adj_discard — 隣接関係の廃棄によってドロップされた IPv6 パケット数。各 VCCI の統計情報は、この特有のドロップ（カラム 5）が発生した場合に収集されます。
- adj_punt — 隣接関係のパントによってパントされた IPv6 パケット数
- adj_glean — 隣接関係のグリーニングによってパントされた IPv6 パケット数
- adj_drop — 隣接関係のドロップによってパントされた IPv6 パケット数（RP は ICMP を生成してからドロップします）
- adj_null — 隣接関係の無効によってパントされた IPv6 パケット数
- adj_receive — 隣接関係の受信によってパントされた IPv6 パケット数
- adj_unknown — 不明な隣接関係（たとえば、0x80）によってパントされた IPv6 パケット数

- ストリクト Reverse Path Forwarding（RPF）

  RPF ストリクト チェック モードは、送信元 IP アドレスが Forwarding Information Base（FIB; 転送情報ベース）テーブル内に存在し、入力ポートに到達可能かどうかを確認します。

- セキュリティ ACL

  IPv6 の場合、Access Control Entry（ACE; アクセス コントロール エントリ）には次の新しいフィールドが含まれます。

  - フロー ラベル
  - ルーティング ヘッダーの存在
  - 「不明の送信」

- QoS

  QoS の照合は次のフィールドのサブセットでのみ実行されます（IPv4 と IPv6 で共通です）。

  - dscp/precedence
  - access group（IPv4 と IPv6 に共通している ACE エントリのみを照合）
  - class
  - qos group
  - mpls
  - input if
  - l2 cos
  - discard class

  match protocol コマンドには現在、このプロトコルを一致基準として指定する **ipv6** キーワードが含まれます。**match ip dscp** コマンドと **match ip precedence** コマンドは IPv4 トラフィックにのみ適用されます。**match dscp** コマンドと **match precedence** コマンドは IPv4 と IPv6 の両方のトラフィックに適用されます。

  パケットのマーク付けでは、**set ip dscp** コマンドと **set ip precedence** コマンドが **set dscp** コマンドと **set precedence** コマンドに変更されました。この 2 つのコマンドは現在 IPv4 と IPv6 の両方のトラフィックに適用されます。

- ICMP の処理と生成はルート プロセッサで実行され、PXF では処理されません。

IPv6 の制限事項

このリリースの Cisco 10000 ルータでは、すべてのタイプの IPv6 トンネリングがサポートされていません。サポートされていない内容は、次のとおりです。

- 自動 6to4
- ISATAP
- 自動 IPv4 互換性
- IPv6 over L2TPv3
- 6over4（RFC 2529）
- IPv6 GRE の IPv6
- IPv6 over UTI

IPv6 では次のセキュリティ ACL 機能がサポートされていません。

- 差分コンパイル（Cisco 10000 ルータは事前にコンパイルされた ACL を使用します）
- シングルステップ分類
- ACL ロギング
- 時間ベースの ACL
- リフレクシブ ACL
- 受信パス ACL
- MiniACL

IPv6 に特有の次の 2 つのフィールドでは QoS の照合が行われません。

- IPv6 src/dst アドレス
- IPv6 ACL

IPv6 拡張 ACL

アクセス リストは、ルータ インターフェイスでブロックおよび転送されたトラフィックを判別するので、送信元アドレスと宛先アドレス、特定のインターフェイスにとってインバウンドかアウトバンドかといった情報に基づいてフィルタリングを実行することができます。各アクセス リストの末尾には、暗黙の拒否（deny）ステートメントがあります。IPv6 ACL は、**ipv6 access-list** コマンドをグローバル コンフィギュレーション モードで **deny** と **permit** キーワードとともに使用して定義され、拒否条件と許可条件が設定されます。

Cisco IOS Release 12.2(31)SB2 以上のリリースでは、標準 IPv6 ACL 機能が拡張され、より詳細な制御を行うための IPv6 オプション ヘッダーとオプションの上位層プロトコル タイプ情報に基づいたトラフィック フィルタリングがサポートされるようになりました（機能は IPv4 の拡張 ACL に類似しています）。

要件

Cisco IOS Release 12.2(13)T および 12.0(23)S 以上のリリースの下位互換性では、***deny*** と ***permit*** キーワードを使用した **ipv6 access-list** コマンドを引き続きグローバル コンフィギュレーション モードで入力できますが、拒否条件と許可条件がグローバル コンフィギュレーション モードで定義された IPv6 ACL は、IPv6 アクセス リスト コンフィギュレーション モードに変換されます。変換された IPv6 ACL の設定例については、「IPv6 ACL の作成および適用 : 例」（p.21-8）を参照してください。

制約事項

一意の名前で IPv6 ACL が定義されます（IPv6 は番号付き ACL をサポートしていません）。IPv4 ACL と IPv6 ACL では、共通の名前を共有できません。

- 各 IPv6 ACL には、IPv6 近接探索を可能にする暗黙の許可ルールがあります。ACL に **deny ipv6 any any** ステートメントを入力すれば、これらのルールを無効にすることができます。IPv6 近接探索プロセスは IPv6 ネットワーク層サービスを使用するので、デフォルトにより、暗黙のうちに IPv6 ACL によってインターフェイスへの IPv6 近接探索パケットの送受信が許可されます。IPv4 の場合、IPv6 近接探索プロセスに相当する Address Resolution Protocol（ARP; アドレス解決プロトコル）が別個のデータ リンク層プロトコルを使用するので、デフォルトにより、暗黙のうちに IPv4 ACL によってインターフェイスへの ARP パケットの送受信が許可されます。

IPv6 トラフィック フィルタリングの設定

IPv6 トラフィック フィルタリングをイネーブルにするには、次の手順を実行する必要があります。

1. IPv6 ACL を作成します。
2. トラフィックをパスまたはブロックするように IPv6 ACL を設定します。
3. インターフェイスに IPv6 ACL を適用します。

IPv6 ACL の作成および設定

サマリー ステップ

1. **enable**
2. **configure** ***terminal***
3. **ipv6 access-list** *access-list-name*

4. **permit** *protocol* {*source-ipv6-prefix/prefix-length* | ***any*** | ***host*** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | ***any*** | ***host*** *destination-ipv6-address*} [*operator* [*port-number*]] [***dest-option-type*** [*doh-number* | *doh-type*]] [***dscp*** *value*] [***flow-label*** *value*] [***fragments***] [***log***] [***log-input***] [***mobility***] [***mobility-type*** [*mh-number* | *mh-type*]] [***reflect*** *name* [***timeout*** *value*]] [***routing***] [***routing-type*** *routing-number*] [***sequence*** *value*] [***time-range*** *name*]
or
deny *protocol* {*source-ipv6-prefix/prefix-length* | ***any*** | ***host*** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | ***any*** | ***host*** *destination-ipv6-address*} [*operator* [*port-number*]] [***dest-option-type*** [*doh-number* | *doh-type*]] [***dscp*** *value*] [***flow-label*** *value*] [***fragments***] [***log***] [***log-input***] [***mobility***] [***mobility-type*** [*mh-number* | *mh-type*]] [***routing***] [***routing-type*** *routing-number*] [***sequence*** *value*] [***time-range*** *name*] [***undetermined-transport***]

詳細なステップ

	コマンドまたはアクション	目的
ステップ 1	**enable** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure *terminal*** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 access-list** *access-list-name* `Router(config)# ipv6 access-list outbound`	IPv6 ACL を定義し、IPv6 アクセス コンフィギュレーション モードを開始します。ルータのプロンプトが Router(config-ipv6-acl)# に変わります。 • *access-list name* 引数は、IPv6 ACL の名前を指定します。IPv6 ACL の名前にはスペースや引用符を加えることはできません。また数字で開始することができません。

	コマンドまたはアクション	目的
ステップ 4	**permit** *protocol* {*source-ipv6-prefix/prefix-length* | ***any*** | ***host*** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | ***any*** | ***host*** *destination-ipv6-address*} [*operator* [*port-number*]] [***dest-option-type*** [*doh-number* | *doh-type*]] [***dscp*** *value*] [***flow-label*** *value*] [***fragments***] [***log***] [***log-input***] [***mobility***] [***mobility-type*** [*mh-number* | *mh-type*]] [***reflect*** *name* [***timeout*** *value*]] [***routing***] [***routing-type*** *routing-number*] [***sequence*** *value*] [***time-range*** *name*] または **deny** *protocol* {*source-ipv6-prefix/prefix-length* | ***any*** | ***host*** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | ***any*** | ***host*** *destination-ipv6-address*} [*operator* [*port-number*]] [***dest-option-type*** [*doh-number* | *doh-type*]] [***dscp*** *value*] [***flow-label*** *value*] [***fragments***] [***log***] [***log-input***] [***mobility***] [***mobility-type*** [*mh-number* | *mh-type*]] [***routing***] [***routing-type*** *routing-number*] [***sequence*** *value*] [***time-range*** *name*] [***undetermined-transport***] `Router(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/32 eq telnet any reflect reflectout` `Router(config-ipv6-acl)# deny tcp host 2001:0db8:1::1 any log-input`	IPv6 ACL の許可条件または拒否条件を指定します。 • *protocol* 引数は、インターネット プロトコルの名前または番号を指定します。***ahp***、***esp***、***icmp***、***ipv6***、***pcp***、***sctp***、***tcp***、または ***udp*** のいずれかのキーワード、あるいは IPv6 プロトコル番号を表す 0 ～ 255 の範囲の整数を入力できます。 • *source-ipv6-prefix/prefix-length* 引数と *destination-ipv6-prefix/prefix-length* 引数は、許可条件を設定する送信元と宛先 IPv6 ネットワークまたはネットワーク クラスを指定します。 **（注）** これらの引数は、16 ビット値を使用したコロン区切りの 16 進数でアドレスを指定する形式（RFC 2373 で規定）である必要があります。 • ***any*** キーワードは、IPv6 プレフィクス ::/0 の省略形です。 • ***host*** *source-ipv6-address* キーワードと引数は、許可条件を設定する送信元 IPv6 ホスト アドレスを指定します。 • *source-ipv6-address* 引数は、16 ビット値を使用したコロン区切りの 16 進数でアドレスを指定する形式（RFC 2373 で規定）である必要があります。 サポートされている引数とキーワードの詳細については、『*IPv6 for Cisco IOS Command Reference*』の「**permit** コマンドと **deny** コマンド」を参照してください。

インターフェイスへの IPv6 ACL の適用

サマリー ステップ

1. **enable**
2. **configure** ***terminal***
3. **interface** *type number*
4. **ipv6 traffic-filter** *access-list-name* {***in*** | ***out***}

詳細なステップ

	コマンドまたはアクション	目的
ステップ 1	**enable** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure *terminal*** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* `Router(config)# interface ethernet 0`	インターフェイスのタイプと番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 traffic-filter** *access-list-name* {***in*** | ***out***} `Router(config-if)# ipv6 traffic-filter outbound out`	指定した IPv6 アクセス リストを前のステップで指定したインターフェイスに適用します。 • **in** キーワードは、指定したインターフェイスの着信 IPv6 トラフィックをフィルタリングします。 • **out** キーワードは、指定したインターフェイスの発信 IPv6 トラフィックをフィルタリングします。

IPv6 ACL の確認

次の例では、**show ipv6 access-list** コマンドを使用して、IPv6 ACL が正しく設定されていることを確認しています。

```
Router> show ipv6 access-list

IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30

IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::32 eq bgp host 2001:0DB8:2::32 eq 11000 timeout 300
(time          left 243) sequence 1
    permit tcp host 2001:0DB8:1::32 eq telnet host 2001:0DB8:2::32 eq 11001 timeout
300          (time left 296) sequence 2

IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

（注） 出力の各フィールドの詳細については、『*IPv6 for Cisco IOS Command Reference*』の「**show ipv6 access-list** コマンド」を参照してください。

IPv6 ACL の作成および適用：例

次の例は、OUTBOUND および INBOUND という 2 つの IPv6 ACL を設定し、イーサネット インターフェイス 0 のアウトバウンドおよびインバウンド トラフィックに両方の ACL を適用します。OUTBOUND リスト内の最初と 2 番めの許可エントリは、ネットワーク 2001:0DB8:0300:0201::/32 から送出されたすべての TCP および User Datagram Protocol（UDP）パケットがイーサネット インターフェイス 0 から出て行くことを許可します。また、エントリは REFLECTOUT という名前の一時的な IPv6 リフレクシブ ACL を設定して、イーサネット インターフェイス 0 の回帰（着信）TCP およ

び UDP パケットをフィルタリングします。OUTBOUND リストの最初の拒否エントリは、ネットワーク fec0:0:0:0201::/64 から送信されたすべてのパケット（送信元 IPv6 アドレスの最初の 64 ビットとしてサイトローカル プレフィクス fec0:0:0:0201 を持つパケット）がイーサネット インターフェイス 0 から出て行くことを拒否します。

INBOUND リスト内の **evaluate** コマンドは、REFLECTOUT という名前の一時的な IPv6 リフレクシブ ACL をイーサネット インターフェイス 0 の着信 TCP および UDP パケットに適用します。OUTBOUND リストによって発信 TCP または UDP パケットがイーサネット インターフェイス 0 上で許可された場合、INBOUND リストは REFLECTOUT リストを使用して、回帰（着信）TCP および UDP パケットを照合（評価）します。

```
ipv6 access-list OUTBOUND
 permit tcp 2001:0DB8:0300:0201::/32 any reflect REFLECTOUT
 permit udp 2001:0DB8:0300:0201::/32 any reflect REFLECTOUT
 deny fec0:0:0:0201::/64 any

ipv6 access-list INBOUND
 evaluate REFLECTOUT

interface ethernet 0
 ipv6 traffic-filter OUTBOUND out
 ipv6 traffic-filter INBOUND in
```

（注） OUTBOUND または INBOUND ACL の最後のエントリとして **permit any any** ステートメントが含まれていないので、イーサネット インターフェイス 0 への出入りが許可されるのが、ACL に設定された許可エントリに一致する TCP と UDP パケット、ACL 内の暗黙の許可条件に一致する ICMP パケットだけになります（ACL の末尾にある暗黙の deny all [すべてを拒否] 条件は、インターフェイス上の他のすべてのパケット タイプを拒否します）。

次の例は、HTTP アクセスを日中の特定の時間に制限し、許可されていない時間のアクティビティを記録するように設定します。

```
time-range lunchtime
 periodic weekdays 12:00 to 13:00

ipv6 access-list OUTBOUND
 permit tcp any any eq www time-range lunchtime
 deny tcp any any eq www log-input
 permit tcp 2001:0DB8::/32 any
 permit udp 2001:0DB8::/32 any
```