IPv6 ファースト ホップ セキュリティ

この章は、次の項で構成されています。

address-config

IPv6 ネイバー バインディング ポリシー内のグローバル IPv6 アドレスに許可された設定方法を指定するには、ネイバー バインディング ポリシーのコンフィギュレーション モードで address-config コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

address-config [stateless | any] [dhcp]

no address-config

パラメータ

- **stateless**：NDP メッセージからバインドされたグローバル IPv6 の自動設定のみが許可されます。
- **any**：NDP メッセージ（ステートレスおよび手動）からバインドされたグローバル IPv6 の設定方法のすべてが許可されます。キーワードが定義されていない場合は、キーワード **any** が適用されます。
- **dhcp**：DHCPv6 からのバインドが許可されます。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

ネイバー バインディング ポリシー コンフィギュレーション モード。

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

キーワードが定義されていない場合は、**address-config any** コマンドが適用されます。

例

次の例では、DHCP アドレスの設定方法のみを許可するようにグローバル設定を変更する方法を示します。

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# address-config dhcp
switchxxxxxx(config-nbr-binding)# exit
```

address-prefix-validation

IPv6 ネイバー バインディング ポリシー内でバインドされたアドレス プレフィックス検証を定義するには、**address-prefix-validation** コマンドをネイバー バインディング ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

address-prefix-validation [enable | disable]

no address-prefix-validation

パラメータ

- **enable**：バインドされたアドレス プレフィックス検証を有効にします。キーワードが設定されていない場合、デフォルトでこのキーワードが適用されます。
- **disable**：バインドされたアドレス プレフィックス検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN に接続されているポリシー：グローバル設定された値。

コマンド モード

ネイバー バインディング ポリシー コンフィギュレーション モード。

使用上のガイドライン

このコマンドを含むポリシーがVLANに接続される場合、グローバル設定を上書きし、VLANのすべてのポートに適用されます。このコマンドをポートに接続されているポリシーで使用する場合、グローバル設定および VLAN 設定を上書きします。

例

次の例では、ネイバーバインディングでグローバルにバインドされたアドレスの検証を変更する policy1 を定義する方法を示します。

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# address-prefix-validation enable
switchxxxxxx(config-nbr-binding)# exit
```

clear ipv6 first hop security counters

IPv6 ファースト ホップ セキュリティ ポート カウンタをクリアするには、**clear ipv6 first hop security counters** コマンドを特権 EXEC モードで使用します。

構文

clear ipv6 first hop security counters [interface *interface-id*]

パラメータ

- **interface** *interface-id*：指定したイーサネット ポートまたはポート チャネルの IPv6 ファースト ホップ セキュリティ カウンタをクリアします。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、IPv6 ファースト ホップ セキュリティによって処理されるパケットのポート カウンタをクリアします。

キーワード **interface** を使用すると、特定のポートのすべてのカウンタをクリアできます。

キーワードを指定せずにコマンドを使用すると、すべてのカウンタがクリアされます。

例

次に、ポート gi1/0/1 の IPv6 ファースト ホップ セキュリティ カウンタをクリアする例を示します。

```
switchxxxxxx# clear ipv6 first hop security counters interface gi1/0/1
```

clear ipv6 first hop security error counters

IPv6ファーストホップセキュリティ グローバルエラーカウンタをクリアするには、**clear ipv6 first hop security error counters** コマンドを特権 EXEC モードで使用します。

構文

clear ipv6 first hop security error counters

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドはグローバル エラー カウンタをクリアします。

例

次の例では、IPv6 ファースト ホップ セキュリティ エラー カウンタをクリアします。

```
switchxxxxxx# clear ipv6 first hop security error counters
```

clear ipv6 neighbor binding prefix table

ネイバー プレフィックス テーブルからダイナミック エントリを削除するには、**clear ipv6 neighbor binding prefix table** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

clear ipv6 neighbor binding prefix table [**vlan** *vlan-id*] [*prefix-address*/*prefix-length*]

パラメータ

- ***vlan-id***：指定した VLAN に一致するダイナミック プレフィックスをクリアします。
- ***prefix-address*/ *prefix-length***：特定のダイナミックプレフィックスをクリアします。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドを使用すると、ネイバー プレフィックス テーブルのダイナミック エントリを削除できます。

clear ipv6 neighbor binding prefix table vlan *vlan-id prefix-address*/*prefix-length* コマンドを使用すると、特定の 1 つのエントリを削除できます。

clear ipv6 neighbor binding prefix table vlan *vlan-id* コマンドを使用すると、指定した VLAN に一致するダイナミック エントリを削除できます。

すべてのダイナミックエントリを削除するには、**clear ipv6 neighbor binding prefix table** コマンドを使用します。

例 1。次の例では、すべてのダイナミック エントリをクリアします。

```
switchxxxxxx# clear ipv6 neighbor binding prefix table
```

例 2。次の例では、VLAN 100 に一致するすべてのダイナミック プレフィックスをクリアします。

```
switchxxxxxx# clear ipv6 neighbor binding prefix table vlan 100
```

例 3。次の例では、特定の 1 つのプレフィックスをクリアします。

```
switchxxxxxx# clear ipv6 neighbor binding prefix table vlan 100 2002:11aa:0000:0001::/64
```

clear ipv6 neighbor binding table

ネイバー バインディング テーブルからダイナミック エントリを削除するには、**clear ipv6 neighbor binding table** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

clear ipv6 neighbor binding table [**vlan** *vlan-id*] [**interface** *interface-id*] [**ipv6** *ipv6-address*] [**mac** *mac-address*] [**ndp** | **dhcp**]

パラメータ

- **vlan** *vlan-id*：指定した VLAN に一致するダイナミック エントリをクリアします。
- **interface** *interface-id*：指定したポート（イーサネット ポートまたはポート チャネル）に一致するダイナミック エントリをクリアします。
- **ipv6** *ipv6-address*：指定した IPv6 アドレスに一致するダイナミック エントリをクリアします。
- **mac** *mac-address*：指定した MAC アドレスに一致するダイナミック エントリをクリアします。
- **ndp**：NDP メッセージからバインドされたダイナミック エントリをクリアします。
- **dhcp**：DHCPv6 メッセージからバインドされたダイナミック エントリをクリアします。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドを使用すると、ネイバー バインディング テーブルのダイナミック エントリが削除されます。削除するダイナミック エントリは、引数 *vlan-id*、引数 *interface-id*、IPv6 アドレス、MAC アドレス、またはバインドされたダイナミック エントリのメッセージ タイプ別に指定できます。

キーワード **ndp** およびキーワード **dhcp** が定義されていない場合、エントリはその送信元に関係なく削除されます。キーワードまたは引数が入力されていない場合は、すべてのダイナミック エントリが削除されます。すべてのキーワードと引数の組み合わせを使用できます。

例

次に、VLAN 100 とポート gi1/0/1 上に存在するすべてのダイナミックエントリをクリアする例を示します。

```
switchxxxxxx# clear ipv6 neighbor binding table vlan 100 interface gi1/0/1
```

device-role（IPv6 DHCP ガード）

IPv6 DHCP ガード ポリシー内のポートに接続されたデバイスのロールを指定するには、**device-role** コマンドを IPv6 DHCPv6 ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

device-role {client | server}

no device-role

パラメータ

- **client**：デバイスのロールを DHCPv6 クライアントに設定します。
- **server**：デバイスのロールを DHCPv6 サーバに設定します。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN に接続されているポリシー：クライアント。

コマンド モード

DHCP ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

IPv6 DHCP ガードは、DHCPv6 サーバ/リレーで送信された、およびクライアントとして設定されているポートで受信した次の DHCPv6 メッセージを廃棄します。

- ADVERTISE
- REPLY
- RECONFIGURE
- RELAY-REPL
- LEASEQUERY-REPLY

例

次の例では、ポリシー 1 という名前の IPv6 DHCP ガード ポリシーを定義し、ポートのロールにサーバを設定します。

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# device-role server
switchxxxxxx(config-dhcp-guard)# exit
```

device-role（ネイバー バインディング）

IPv6 ネイバー バインディング ポリシー内のポートに接続されたデバイスのロールを指定するには、**device-role** コマンドを IPv6 ネイバー バインディング ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

device-role {perimeter | internal}

no device-role

パラメータ

- **perimeter**：ポートが IPv6 ファースト ホップ セキュリティをサポートしていないデバイスに接続されるように指定します。
- **internal**：ポートが IPv6 ファースト ホップ セキュリティをサポートしているデバイスに接続されるように指定します。

デフォルト設定

ポートまたはポート チャネルに接続されたポリシー：VLAN に接続されたポリシーで設定された値。

VLAN に接続されているポリシー：境界。

コマンド モード

ネイバー バインディング ポリシー コンフィギュレーション モード。

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

NB 整合性は境界モードをサポートしています（RFC 6620 を参照）。

このモデルでは、次の 2 つのポート タイプを指定します。

- **Perimeter Port**：NB 整合性をサポートしていないデバイスに接続されたポートを指定します。NB 整合性により、このポートに接続されているネイバーのバインディングが確立されます。ソース ガードはこのポートでは機能しません。
- **Internal Port**：2 つ目のタイプでは、IPv6 ファースト ホップ セキュリティをサポートしているデバイスに接続されたポートを指定します。NB 整合性により、このポートに接続されているネイバーのバインディングは確立されませんが、境界ポートで確立されたバインディングは反映されます。

このロールが境界から内部に変更されると、ポートにバインドされたダイナミック IPv6 アドレスが削除されます。スタティック IPv6 アドレスが保持されます。

例

次の例では、ポリシー 1 という名前のネイバー バインディング ポリシーを定義し、ポートのロールに内部ポートを設定します。

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# device-role internal
switchxxxxxx(config-nbr-binding)# exit
```

device-role（RA ガード ポリシー）

IPv6 RA ガード ポリシー内のポートに接続されたデバイスのロールを指定するには、**device-role** コマンドを RA ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

device-role {host | router}

no device-role

パラメータ

- **host**：デバイスの権限をホストに設定します。
- **router**：デバイスの権限をルータに設定します。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：ホスト。

コマンド モード

RA ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

RA ガードは、ホストとして設定されているポートで受信された入力 RA、CPA、および ICMPv6 リダイレクト メッセージを廃棄します。

例

次の例では、ポリシー 1 という名前の RA ガード ポリシーを定義し、ポートのロールに **router** を設定します。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# device-role router
switchxxxxxx(config-ra-guard)# exit
```

device-role（ND インスペクション ポリシー）

IPv6 ND インスペクション ポリシー内のポートに接続されたデバイスのロールを指定するには、**device-role** コマンドを ND インスペクション ポリシー コンフィギュレーション モードで使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

device-role {host | router}

no device-role

パラメータ

- **host**：デバイスの権限をホストに設定します。
- **router**：デバイスの権限をルータに設定します。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：ホスト。

コマンド モード

ND インスペクション ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

NDインスペクションは、ポートのロールに応じてNDPメッセージの出力フィルタリングを実行します。次の表では、フィルタリング ルールを指定します。

メッセージ	ホスト	ルータ
RA	許可	許可
RS	拒否	許可
CPA	許可	許可
CPS	拒否	許可
ICMP Redirect	許可	許可

例

次の例では、ポリシー 1 という名前の ND インスペクション ポリシーを定義し、ポートのロールにルータを設定します。

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# device-role router
switchxxxxxx(config-nd-inspection)# exit
```

drop-unsecure

IPv6 NDインスペクション ポリシー内のオプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをドロップできるようにするには、drop-unsecure コマンドを ND インスペクション ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、no 形式のコマンドを使用します。

構文

drop-unsecure [enable | disable]

no drop-unsecure

パラメータ

- **enable**：オプションが指定されていないか無効なオプションが指定されているか、または署名が無効なメッセージのドロップを有効にします。キーワードが設定されていない場合、デフォルトでこのキーワードが適用されます。
- **disable**：オプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをドロップできません。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

ND インスペクション ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLANのポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

例

次の例では、policy1 という名前の ND インスペクション ポリシーを定義し、ND インスペクション ポリシー コンフィギュレーション モードでスイッチを配置して、オプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをスイッチがドロップできるようにします。

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# drop-unsecure

switchxxxxxx(config-nd-inspection)# exit
```

hop-limit

IPv6 RA ガード ポリシー内の RA メッセージでアドバタイズされた Cur ホップ制限値の検証を有効にするには、**hop-limit** コマンドを RA ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

hop-limit {[maximum {*value* | disable}] [minimum {*value* | disable}]}

no hop-limit [maximum] [minimum]

パラメータ

- **maximum** *value*：ホップカウント制限が **value** 引数以下であることを確認します。範囲 1 ～ 255。高位境界の値は、低位境界の値以上でなければなりません。
- **maximum disable**：ホップカウント制限の高位境界の検証を無効にします。
- **minimum** *value*：ホップ数制限が **value** 引数以上であることを確認します。範囲 1 ～ 255。
- **minimum disable**：ホップカウント制限の下位境界の検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

RA ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLANのポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

キーワード **disable** を使用すると、グローバル設定または VLAN 設定に関係なく検証を無効にできます。

例 1：次の例では、policy1 という名前の RA ガード ポリシーを定義し、RA ガード ポリシー コンフィギュレーション モードでスイッチを配置して、最小 Cur ホップ制限値を 5 に定義します。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# hop-limit minimum 5
switchxxxxxx(config-ra-guard)# exit
```

例 2：次の例では、policy1 という名前の RA ガード ポリシーを定義し、RA ガード ポリシー コンフィギュレーション モードでスイッチを配置して、Cur ホップ制限の高位境界の検証を無効にします。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# hop-limit maximum disable
switchxxxxxx(config-ra-guard)# exit
```

ipv6 dhcp guard

VLAN 上の DHCPv6 ガード機能を有効にするには、**ipv6 dhcp guard** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 dhcp guard

no ipv6 dhcp guard

デフォルト設定

VLAN 上の DHCPv6 ガードは無効になっています。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

DHCPv6 ガードは、DHCPv6 サーバ/リレーからクライアントに送信して DHCPv6 サーバとして設定されていないポートで受信したメッセージをブロックします。リレー エージェントによってクライアントからサーバに送信されるクライアント メッセージはブロックされません。

DHCPv6 ガードは、送信元ポートに接続されている DHCPv6 ガード ポリシーに基づいて受信した DHCPv6 メッセージを検証します。

例 1：次の例では、VLAN 100 上の DHCPv6 ガードを有効にします。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp guard
switchxxxxxx(config-if)# exit
```

例 2：次の例では、VLAN 100-107 上の DHCPv6 ガードを有効にします。

```
switchxxxxxx(config)# interface range vlan 100-107
switchxxxxxx(config-if-range)# ipv6 dhcp guard
switchxxxxxx(config-if-range)# exit
```

ipv6 dhcp guard attach-policy（ポート モード）

特定のポートに DHCPv6 ガード ポリシーを接続するには、**ipv6 dhcp guard attach-policy** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 dhcp guard attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 dhcp guard attach-policy [*policy-name*]

パラメータ

- ***policy-name***：DHCPv6 ガード ポリシー名（最大 32 文字）。
- **vlan** *vlan-list*：DHCPv6 ガードポリシーを *vlan-list* 内の VLAN に接続するように指定します。キーワード **vlan** が設定されていない場合、ポリシーは DHCPv6 ガードが有効になっているデバイス上のすべての VLAN に適用されます。

デフォルト設定

DHCPv6 ガード デフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、DHCPv6 ガード ポリシーをポートに接続できます。

コマンドを使用するたびに、同じポリシー内の以前のコマンドが上書きされます。

policy-name 引数で指定されたポリシーが定義されていない場合、コマンドは拒否されます。

vlan キーワードを使用した複数のポリシーは、共通の VLAN を持っていない場合は同じポートに接続できます。

入力パケットに適用されているルールのセットは次のように構築されます。

- パケットが到着した VLAN 上のインターフェイスに接続されたポートで設定されたルールがセットに追加されます。
- VLAN に接続されたポリシーで設定されたルールがセットに追加されます（追加されていない場合）。
- グローバル ルールがセットに追加されます（追加されていない場合）。

no ipv6 dhcp guard attach-policy を使用すると、ポートに接続されたすべてのユーザ定義済み DHCP ガード ポリシーを切り離すことができます。

ポートから特定のポリシーを切り離すには、**no ipv6 dhcp guard attach-policy** *policy-name* を使用します。

例 1：次に、DHCPv6 ガードポリシー policy1 を gi1/0/1 ポートに接続し、デフォルトのポリシー port_default を切り離す例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy1
switchxxxxxx(config-if)# exit
```

例 2：次に、DHCPv6 ガードポリシー policy1 を gi1/0/1 ポートに接続し、VLAN 1 ～ 10 と 12 ～ 20 に適用する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

例 3：次に、DHCPv6 ガードポリシー policy1 を gi1/0/1 ポートに接続して VLAN 1 ～ 10 に適用し、DHCPv6 ガードポリシー policy2 を gi1/0/1 ポートに接続して VLAN 12 ～ 20 に適用する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

例 4：次に、DHCPv6 ガードを gi1/0/1 ポートから policy1 を切り離す例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 dhcp guard attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 dhcp guard attach-policy（VLAN モード）

指定した VLAN に DHCPv6 ガード ポリシーを接続するには、**ipv6 dhcp guard attach-policy** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 dhcp guard attach-policy *policy-name*

no ipv6 dhcp guard attach-policy

パラメータ

- ***policy-name***：DHCPv6 ガード ポリシー名（最大 32 文字）。

デフォルト設定

DHCPv6 ガード デフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、DHCPv6 ガード ポリシーを VLAN に接続できます。

policy-name 引数で指定されたポリシーが定義されていない場合、コマンドは拒否されます。

コマンドの **no** 形式を使用すると、現在のポリシーを切り離してデフォルト ポリシーを再び接続できます。デフォルト ポリシーが接続されている場合、コマンドの **no** 形式は無効です。

例

次の例では、DHCPv6 ガード ポリシー policy1 は VLAN 100 に接続されています。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 dhcp guard policy

DHCP ガード ポリシーを定義して DHCPv6 ガード ポリシー コンフィギュレーション モードでスイッチを配置するには、**ipv6 dhcp guard policy** コマンドをグローバル コンフィギュレーション モードで使用します。DHCPv6 ガード ポリシーを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 dhcp guard policy *policy-name*

no ipv6 dhcp guard policy *policy-name*

パラメータ

- ***policy-name***：DHCPv6 ガード ポリシー名（最大 32 文字）。

デフォルト設定

DHCPv6 ガード ポリシーは設定されていません

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、DHCPv6 ガードポリシー名を定義し、DHCPv6 ガードポリシー コンフィギュレーション モードでルータを配置します。

同じタイプの各ポリシー（たとえば、DHCPv6 ガードポリシーなど）には一意の名前が必要です。異なるタイプのポリシーには同じポリシー名を設定できます。

スイッチは、「vlan_default」と「port_default」という 2 つの定義済みのデフォルト DHCPv6 ガード ポリシーをサポートします。

```
ipv6 dhcp guard policy vlan_default
      exit
      ipv6 dhcp guard policy port_default
      exit
```

デフォルト ポリシーは空で削除できませんが、変更することはできます。**no ipv6 dhcp guard policy** はデフォルト ポリシーを削除せずに、ユーザが定義したポリシー設定のみを削除します。

ipv6 dhcp guard policy コマンドを複数回使用すると、ポリシーを定義できます。

接続したポリシーを削除する前に、次の例 3 が示すように確認要求がユーザに表示されます。

例 1：次の例では、policy1 という名前の DHCPv6 ガード ポリシーを定義して、DHCPv6 でガード ポリシー コンフィギュレーション モードでルータを配置し、ポートが保護

されていないメッセージをドロップするように設定して、デバイス ロールをルータに設定します。

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# match server address list1
switchxxxxxx(config-dhcp-guard)# device-role server
switchxxxxxx(config-dhcp-guard)# exit
```

例 2：次の例では、policy1 という名前の DHCPv6 ガードを複数の手順で定義します。

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# match server address list1
switchxxxxxx(config-dhcp-guard)# exit
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# device-role server
switchxxxxxx(config-dhcp-guard)# exit
```

例 3：次の例では、接続している DHCPv6 ガード ポリシーを削除します。

```
switchxxxxxx(config)# no ipv6 dhcp guard policy policy1
Policy policy1 is applied on the following ports:
 gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

ipv6 dhcp guard preference

DHCPv6 サーバから送信されたメッセージ内の環境設定の検証をグローバルに有効にするには、**ipv6 dhcp guard preference** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 dhcp guard preference {[**maximum** *value*] [**minimum** *value*]}

no ipv6 dhcp guard preference [maximum] [minimum]

パラメータ

- **maximum** *value*：アドバタイズされたプリファレンス値は、**value** 引数以下です。範囲 0 ～ 255。高境界の値は、低境界の値以上である必要があります。
- **minimum** *value*：アドバタイズ設定値は **value** 引数以上です。範囲 0 ～ 255。

デフォルト設定

検証は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドにより、DHCPv6サーバから送信されたメッセージ内のプリファレンス値（RFC3315を参照）が *value* 引数を超えるまたは未満であることを検証できます。

注。DHCPv6 ガードが RELAY-REPL メッセージを受信する場合は、カプセル化されたメッセージから取得します。

minimum *value* キーワードと引数を設定すると、許容される最小値が指定されます。**value** 引数で指定した値未満のプリファレンス値を持つ受信済みDHCPv6返信メッセージはドロップされます。

maximum *value* キーワードと引数を設定すると、許容される最大値が指定されます。**value** 引数で指定した値を超えるプリファレンス値を持つ受信済みDHCPv6返信メッセージはドロップされます。

no ipv6 dhcp guard preference を使用すると、DHCPv6 返信メッセージ内でアドバタイズされたプリファレンス値の検証を無効にできます。

no ipv6 dhcp guard preference maximum を使用すると、DHCPv6 メッセージ内でアドバタイズされたプリファレンス値の最大境界の検証を無効にできます。

no ipv6 dhcp guard preference minimum コマンドを使用すると、DHCPv6 メッセージ内でアドバタイズされたプリファレンス値の最小境界の検証を無効にできます。

例 1：次の例では、2 つのコマンドを使用して、グローバル最小プリファレンス値に 10 を、グローバル最大プリファレンス値に 102 を定義します。

```
switchxxxxxx(config)# ipv6 dhcp guard preference minimum 10
switchxxxxxx(config)# ipv6 dhcp guard preference maximum 102
```

例 2：次の例では、1 つのコマンドを使用して、グローバル最小プリファレンス値に 10 を、グローバル最大プリファレンス値に 102 を定義します。

```
switchxxxxxx(config)# ipv6 dhcp guard preference minimum 10 maximum 102
```

ipv6 first hop security

VLAN 上で IPv6 ファースト ホップ セキュリティをグローバルに有効にするには、**ipv6 first hop security** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 first hop security

no ipv6 first hop security

デフォルト設定

VLAN 上で IPv6 ファースト ホップ セキュリティは無効になっています。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

ipv6 first hop security コマンドを使用すると、VLAN 上で IPv6 ファースト ホップ セキュリティを有効にできます。

例 1：次の例では、VLAN 100 上の IPv6 ファースト ホップ セキュリティを有効にします。

switchxxxxxx(config)# **interface vlan** 100

switchxxxxxx(config-if)# **ipv6 first hop security**

switchxxxxxx(config-if)# **exit**

例 2：次の例では、VLAN 100-107 上の IPv6 ファースト ホップ セキュリティを有効にします。

switchxxxxxx(config)# **interface range vlan** 100-107

switchxxxxxx(config-if-range)# **ipv6 first hop security**

switchxxxxxx(config-if-range)# **exit**

ipv6 first hop security attach-policy（ポート モード）

特定のポートに IPv6 ファースト ホップ セキュリティ ポリシーを接続するには、**ipv6 first hop security attach-policy** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 first hop security attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 first hop security attach-policy [*policy-name*]

パラメータ

- ***policy-name***：IPv6 ファーストホップ セキュリティ ポリシー名（最大 32 文字）。
- **vlan** *vlan-list*：IPv6 ファースト ホップ セキュリティ ポリシーが *vlan-list* で VLAN に接続されるように指定します。キーワード **vlan** が設定されていない場合、ポリシーは IPv6 ファースト ホップ セキュリティが有効になっているデバイス上のすべての VLAN に適用されます。

デフォルト設定

IPv6 ファーストホップ セキュリティのデフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、IPv6 ファースト ホップ セキュリティ ポリシーをポートに接続できます。

このコマンドの後続の各使用方法は、同じポリシーを使用したコマンドの以前の使用方法より優先されます。

コマンドを使用するたびに、同じポリシー内の以前のコマンドが上書きされます。

policy-name 引数で指定されたポリシーが定義されていない場合、コマンドは拒否されます。

vlan キーワードを使用した複数のポリシーは、共通の VLAN を持っていない場合は同じポートに接続できます。

入力パケットに適用されているルールのセットは次のように構築されます。

- パケットが到着した VLAN 上のインターフェイスに接続されたポートで設定されたルールがセットに追加されます。
- VLAN に接続されたポリシーで設定されたルールがセットに追加されます（追加されていない場合）。

- グローバル ルールがセットに追加されます（追加されていない場合）。

no ipv6 first hop security attach-policy コマンドを使用すると、ポートに接続されたすべてのユーザ定義済みポリシーを切り離すことができます。デフォルトのポリシーがもう一度接続されます。

no ipv6 first hop security attach-policy *policy-name* コマンドを使用すると、ポートから特定のポリシーを切り離すことができます。

例 1：次に、IPv6 ファースト ホップ セキュリティ ポリシー policy1 を gi1/0/1 ポートに接続する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy1
switchxxxxxx(config-if)# exit
```

例 2：次に、IPv6 ファースト ホップ セキュリティ ポリシー policy1 をポート gi1/0/1 に接続し、VLAN 1 ～ 10 と 12 ～ 20 に適用する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

例 3：次に、IPv6 ファースト ホップ セキュリティ ポリシー policy1 をポート gi1/0/1 に接続して VLAN 1 ～ 10 に適用し、IPv6 ファースト ホップ セキュリティ ポリシー policy2 をポート gi1/0/1 に接続して VLAN 12 ～ 20 に適用する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

例 4：次に、IPv6 ファースト ホップ セキュリティ ポリシー policy1 を gi1/0/1 ポートから切り離す例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 first hop security attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 first hop security attach-policy（VLAN モード）

特定の VLAN に IPv6 ファースト ホップ セキュリティ ポリシーを接続するには、**ipv6 first hop security attach-policy** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 first hop security attach-policy *policy-name*

no ipv6 first hop security attach-policy

パラメータ

- ***policy-name***：IPv6 ファーストホップ セキュリティ ポリシー名（最大 32 文字）。

デフォルト設定

IPv6 ファーストホップ セキュリティのデフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、IPv6 ファースト ホップ セキュリティ ポリシーを VLAN に接続できます。

policy-name 引数で指定されているポリシーが定義されていない場合、コマンドは拒否されます。

コマンドの **no** 形式を使用すると、現在のポリシーを切り離してデフォルト ポリシーを再び接続できます。デフォルト ポリシーが接続されている場合、コマンドの **no** 形式は無効です。

例

次の例では、IPv6 ファースト ホップ セキュリティ ポリシー policy1 は VLAN 100 に接続されています。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 first hop security logging packet drop

IPv6ファーストホップセキュリティ機能によってドロップされたパケットのロギングをグローバルに有効にするには、**ipv6 first hop security logging packet drop** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 first hop security logging packet drop

no ipv6 first hop security logging packet drop

デフォルト設定

ロギングは無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、ドロップされたパケットを記録できます。ロギングが有効になっている場合、スイッチはメッセージをドロップするたびにレート制限の SYSLOG メッセージを送信します。

例

次の例では、IPv6 ファースト ホップ セキュリティ機能によってドロップされたパケットのロギングを有効にする方法を示します。

```
switchxxxxxx(config)# ipv6 first hop security logging packet drop
```

ipv6 first hop security policy

IPv6 ファースト ホップ セキュリティを定義して IPv6 ファースト ホップ セキュリティ ポリシー コンフィギュレーション モードでスイッチを配置するには、**ipv6 first hop security policy** コマンドをグローバル コンフィギュレーション モードで使用します。IPv6 ファースト ホップ セキュリティ ポリシーを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 first hop security policy *policy-name*

no ipv6 first hop security policy *policy-name*

パラメータ

- ***policy-name***：IPv6 ファーストホップ セキュリティ ポリシー名（最大 32 文字）。

デフォルト設定

IPv6 ファースト ホップ セキュリティ ポリシーは設定されていません

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは IPv6 ファースト ホップ セキュリティ ポリシーを定義し、スイッチを IPv6 ファースト ホップ セキュリティ コンフィギュレーション モードにします。同じタイプの各ポリシー（たとえば、IPv6 ファースト ホップ セキュリティ ポリシーなど）には一意の名前が必要です。異なるタイプのポリシーには同じポリシー名を設定できます。スイッチは、「vlan_default」と「port_default」という 2 つの定義済みの空のデフォルト IPv6 ファースト ホップ セキュリティ ポリシーをサポートします。

```
ipv6 first hop security policy vlan_default
      exit
      ipv6 first hop security policy port_default
      exit
```

これらのポリシーは削除できませんが、変更することはできます。**no ipv6 first hop security policy** はこれらのポリシーを削除せずに、ユーザが定義したポリシー設定のみを削除します。

ipv6 first hop security policy コマンドを複数回使用すると、ポリシーを定義できます。

アタッチされているポリシーを削除すると、削除する前に自動的に切り離されます。

例

例 1：次の例では、policy1 という名前の IPv6 ファースト ホップ セキュリティ ポリシーを定義し、IPv6 ファースト ホップ セキュリティ ポリシー コンフィギュレーション モードでスイッチを配置し、ドロップされたパケットのロギングを有効にします。

```
switchxxxxxx(config)# ipv6 first hop security policy policy1
switchxxxxxx(config-ipv6-fhs)# logging packet drop
switchxxxxxx(config)# exit
```

例 2：次の例では、接続している IPv6 ファースト ホップ セキュリティ ポリシーを削除します。

```
switchxxxxxx(config)# no ipv6 first hop security policy policy1
Policy policy1 is applied on the following ports:
gi1/0/1, gi1/0/2

The policy1 will be detached and removed, are you sure [Y/N]Y
```

ipv6 nd inspection

VLAN 上で IPv6 ネイバー探索（ND）のインスペクション機能を有効にするには、**ipv6 nd inspection** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd inspection

no ipv6 nd inspection

デフォルト設定

VLAN 上の ND インスペクションは無効になっています。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

コマンドを使用すると、VLAN 上で ND インスペクションを有効にできます。IPv6 ND インスペクションは、ND インスペクションポリシーおよびグローバル ND インスペクション設定を使用してネイバー探索プロトコル（NDP）メッセージを検証します。NDインスペクションは、次の例外を含む VLAN 内の送信元ポートを除いたすべてのポートに NDP メッセージをブリッジします。RS メッセージと CPS メッセージはホストとして設定されているポートにブリッジされません（**device-role** コマンドを参照）。ND インスペクションは RA ガード後に実行されます。

例 1：次の例では、VLAN 100 上の ND インスペクションを有効にします。

switchxxxxxx(config)# **interface vlan** 100

switchxxxxxx(config-if)# **ipv6 nd inspection**

switchxxxxxx(config-if)# **exit**

例 2：次の例では、VLAN 100-107 上の ND インスペクションを有効にします。

switchxxxxxx(config)# **interface range vlan** 100-107

switchxxxxxx(config-if-range)# **ipv6 nd inspection**

switchxxxxxx(config-if-range)# **exit**

ipv6 nd inspection attach-policy（ポート モード）

特定のポートにNDインスペクション ポリシーを接続するには、**ipv6 nd inspection attach-policy** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd inspection attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 nd inspection attach-policy [*policy-name*]

パラメータ

- ***policy-name***：ND インスペクション ポリシー名（最大 32 文字）。
- **vlan** *vlan-list*：ND インスペクション ポリシーが *vlan-list* で VLAN に接続されるように指定します。キーワード **vlan** が設定されていない場合、ポリシーは ND インスペクションが有効になっているデバイス上のすべての VLAN に適用されます。

デフォルト設定

ND インスペクションのデフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

ND インスペクションポリシーをポートに接続するには、**ipv6 nd inspection attach-policy** コマンドを使用します。

コマンドを使用するたびに、同じポリシー内の以前のコマンドが上書きされます。

policy-name 引数で指定されたポリシーが定義されていない場合、コマンドは拒否されます。

vlan キーワードを使用した複数のポリシーは、共通の VLAN を持っていない場合は同じポートに接続できます。

入力パケットに適用されているルールのセットは次のように構築されます。

- パケットが到着した VLAN 上のインターフェイスに接続されたポートで設定されたルールがセットに追加されます。
- VLANに接続されたポリシーで設定されたルールがセットに追加されます（追加されていない場合）。
- グローバル ルールがセットに追加されます（追加されていない場合）。

ポートに接続されたユーザ定義済みのすべてのポリシーを切り離すには、**no ipv6 nd inspection attach-policy** を使用します。

no ipv6 nd inspection attach-policy *policy-name* コマンドを使用すると、ポートから特定のポリシーを切り離すことができます。

例 1：次に、ND インスペクションポリシー policy1 を gi1/0/1 ポートに接続する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy1
switchxxxxxx(config-if)# exit
```

例 2：次に、ND インスペクションポリシー policy1 をポート gi1/0/1 に接続して VLAN 1 ～ 10 と 12 ～ 20 に適用する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

例 3：次に、ND インスペクションポリシー policy1 を gi1/0/1 ポートに接続して VLAN 1 ～ 10 に適用し、ND インスペクションポリシー policy2 を gi1/0/1 ポートに接続して VLAN 12 ～ 20 に適用する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

例 4：次に、ND インスペクションがポート gi1/0/1 からポリシー policy1 を切り離す例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 nd inspection attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 nd inspection attach-policy（VLAN モード）

特定の VLAN に ND インスペクション ポリシーを接続するには、**ipv6 nd inspection attach-policy** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd inspection attach-policy *policy-name*

no ipv6 nd inspection attach-policy

パラメータ

- ***policy-name***：ND インスペクション ポリシー名（最大 32 文字）。

デフォルト設定

ND インスペクションのデフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用して、VLAN に ND インスペクション ポリシーを接続します。**policy-name** 引数で指定したポリシーが定義されていない場合、コマンドは拒否されます。コマンドの **no** 形式を使用すると、現在のポリシーを切り離してデフォルト ポリシーを再び接続できます。デフォルト ポリシーが接続されている場合、コマンドの **no** 形式は無効です。

例

次の例では、ND インスペクション ポリシー policy1 は VLAN 100 に接続されています。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 nd inspection drop-unsecure

CGA と RSA シグネチャ オプションが指定されていないメッセージをグローバルにドロップするには、**ipv6 nd inspection drop-unsecure** コマンドをグローバル コンフィギュレーション モードで使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

ipv6 nd inspection drop-unsecure

no ipv6 nd inspection drop-unsecure

デフォルト設定

すべてのメッセージがブリッジされます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

CGA および RSA シグネチャ オプションが含まれていない場合、**is** コマンドは NDP メッセージをドロップします。

このコマンドが設定されていない場合、**sec-level minimum** コマンドは無効です。

このコマンドが設定されている場合は、**sec-level minimum** コマンドのみが有効になり、設定された他のすべての ND インスペクション ポリシー コマンドは無視されます。

例

次の例では、オプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをスイッチがドロップします。

```
switchxxxxxx(config)# ipv6 nd inspection drop-unsecure
```

ipv6 nd inspection policy

ND インスペクション ポリシーを定義して IPv6 ND インスペクション ポリシー コンフィギュレーション モードでスイッチを配置するには、**ipv6 nd inspection policy** コマンドをグローバル コンフィギュレーション モードで使用します。ND インスペクション ポリシーを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 nd inspection policy *policy-name*

no ipv6 nd inspection policy *policy-name*

パラメータ

- ***policy-name***：ND インスペクション ポリシー名（最大 32 文字）。

デフォルト設定

ND インスペクション ポリシーは設定されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、ND インスペクション ポリシー名を定義し、ND インスペクション ポリシー コンフィギュレーション モードでルータを配置します。同じタイプの各ポリシー（たとえば、ND インスペクション ポリシーなど）には一意の名前が必要です。異なるタイプのポリシーには同じポリシー名を設定できます。

スイッチは、「vlan_default」と「port_default」という 2 つの定義済みの ND インスペクション ポリシーをサポートします。

```
ipv6 nd inspection policy vlan_default
      exit
      ipv6 nd inspection policy port_default
      exit
```

これらのポリシーは削除できませんが、変更することはできます。**no ipv6 nd inspection policy** はこれらのポリシーを削除せずに、ユーザが定義したポリシー設定のみを削除します。

ipv6 nd inspection policy コマンドを複数回使用すると、ポリシーを定義できます。

接続されているポリシーが削除される場合は、削除される前に自動的に切り離されます。

例 1。次の例では、policy1 という名前の ND インスペクション ポリシーを定義し、ND インスペクション ポリシー コンフィギュレーション モードでスイッチを配置して、ポートが保護されていないメッセージをドロップするように設定し、デバイス ロールをルータに設定します。

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# drop-unsecure
switchxxxxxx(config-nd-inspection)# device-role router
switchxxxxxx(config-nd-inspection)# exit
```

例 2。次の例では、いくつかの手順を実行してNDインスペクション ポリシーをpolicy1に定義します。

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# drop-unsecure
switchxxxxxx(config-nd-inspection)# exit
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# device-role router
switchxxxxxx(config-nd-inspection)# exit
```

例 3。次の例では、接続された ND インスペクション ポリシーを削除します。

```
switchxxxxxx(config)# no ipv6 nd inspection policy policy1
Policy policy1 is applied on the following ports:
gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

ipv6 nd inspection sec-level minimum

最小セキュリティ レベル値をグローバルに指定するには、**ipv6 nd inspection sec-level minimum** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd inspection sec-level minimum *value*

no ipv6 nd inspection sec-level minimum

パラメータ

- ***value***：最小セキュリティ レベルを設定します。範囲：0 ～ 7.

デフォルト設定

すべてのメッセージがブリッジされます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

drop-unsecured 機能が設定されると、is コマンドは最小セキュリティ レベル パラメータ値を指定します。

保護されていないメッセージが無効になると、このコマンドは無効になります。

例

次の例では、スイッチで最小 CGA セキュリティ レベルとして 2 を指定します。

```
switchxxxxxx(config)# ipv6 nd inspection sec-level minimum 2
```

ipv6 nd inspection validate source-mac

送信元/ターゲット リンク層オプションのリンク層アドレスに対して送信元 MAC アドレスをグローバルにチェックするには、**ipv6 nd inspection validate source-mac** コマンドをグローバル コンフィギュレーション モードで使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

ipv6 nd inspection validate source-mac

no ipv6 nd inspection validate source-mac

パラメータ

該当なし

デフォルト設定

このコマンドは、デフォルトで無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

スイッチが NDP メッセージを受信し、送信元/ターゲット リンク層オプションにリンク層アドレスが含まれる場合、送信元 MAC アドレスはリンク層アドレスに対してチェックされます。リンク層アドレスと MAC アドレスが異なる場合、このコマンドを使用するとパケットをドロップできます。

例

次の例では、NDP メッセージの送信元/ターゲット リンク層オプションのリンク層アドレスが MAC アドレスと一致しない場合にスイッチがこのメッセージをドロップできます。

```
switchxxxxxx(config)# ipv6 nd inspection validate source-mac
```

ipv6 nd raguard

VLAN上でルータアドバタイズメント（RA）ガード機能をグローバルに有効にするには、**ipv6 nd raguard** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd raguard

no ipv6 nd raguard

パラメータ

該当なし

デフォルト設定

VLAN 上の RA ガードは無効になっています。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

ipv6 nd raguard コマンドを使用すると、VLAN 上で IPv6 RA ガードを有効にします。RA ガードは、ルータとして設定されていないポートで受信した RA、CPA、および ICMP リダイレクトメッセージを破棄します（**device-role** コマンドを参照）。RA ガードは、送信元ポートに接続されている RA ガードポリシーに基づいて受信した RA メッセージを検証します。

RA ガードは ND インスペクション前に実行されます。

例 1：次の例では、VLAN 100 上の RA ガードを有効にします。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 nd raguard
switchxxxxxx(config-if)# exit
```

例 2：次の例では、VLAN 100-107 上の RA ガードを有効にします。

```
switchxxxxxx(config)# interface range vlan 100-107
switchxxxxxx(config-if-range)# ipv6 nd raguard
switchxxxxxx(config-if-range)# exit
```

ipv6 nd raguard attach-policy（ポート モード）

特定のポートにRA ガード ポリシーを接続するには、**ipv6 nd raguard attach-policy** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd raguard attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 nd raguard attach-policy [*policy-name*]

パラメータ

- ***policy-name***：RA ガード ポリシー名（最大 32 文字）。
- **vlan** *vlan-list*：RA ガード ポリシーが *vlan-list* で VLAN に接続されるように指定します。キーワード **vlan** が設定されていない場合、ポリシーは RA ガード ポリシーが有効になっているデバイス上のすべての VLAN に適用されます。

デフォルト設定

RA ガードのデフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、RA ガード ポリシーをポートに接続できます。コマンドを使用するたびに、同じポリシー内の以前のコマンドが上書きされます。*policy-name* 引数で指定されたポリシーが定義されていない場合、コマンドは拒否されます。

vlan キーワードを使用した複数のポリシーは、共通の VLAN を持っていない場合は同じポートに接続できます。

入力パケットに適用されているルールのセットは次のように構築されます。

- パケットが到着した VLAN 上のインターフェイスに接続されたポートで設定されたルールがセットに追加されます。
- VLANに接続されたポリシーで設定されたルールがセットに追加されます（追加されていない場合）。
- グローバル ルールがセットに追加されます（追加されていない場合）。

no ipv6 nd raguard attach-policy コマンドを使用すると、ポートに接続されたすべてのユーザ定義済みポリシーを切り離すことができます。

ipv6 nd raguard attach-policy *policy-name* コマンドを使用すると、ポートから特定のポリシーを切り離すことができます。

例 1：次に、RA ガードポリシー policy1 を gi1/0/1 ポートに接続する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy1
switchxxxxxx(config-if)# exit
```

例 2：次に、RA ガードポリシー policy1 を gi1/0/1 ポート に接続して VLAN 1 ～ 10 と 12 ～ 20 に適用する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

例 3：次に、RA ガードポリシー policy1 を gi1/0/1 ポートに接続して VLAN 1 ～ 10 に適用し、RA ガードポリシー policy2 を gi1/0/1 ポートに接続して VLAN 12 ～ 20 に適用する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

例 4：次に、RA ガードポリシー policy1 を gi1/0/1 ポートから切り離す例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 nd raguard attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 nd raguard attach-policy（VLAN モード）

指定した VLAN に RA ガード ポリシーを接続するには、**ipv6 nd raguard attach-policy** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd raguard attach-policy *policy-name*

no ipv6 nd raguard attach-policy

パラメータ

- ***policy-name***：RA ガード ポリシー名（最大 32 文字）。

デフォルト設定

RA ガードのデフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、RA ガード ポリシーを VLAN に接続できます。

policy-name 引数で指定されたポリシーが定義されていない場合、コマンドは拒否されます。

コマンドの **no** 形式を使用すると、現在のポリシーを切り離してデフォルト ポリシーを再び接続できます。コマンドの **No** 形式は、デフォルトのポリシーがアタッチされている場合は影響を与えません。

例

次の例では、RA ガード ポリシー policy1 は VLAN 100 に接続されています。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 nd raguard hop-limit

RA メッセージのアドバタイズされた Cur ホップ制限値をグローバルに検証するには、**ipv6 nd raguard hop-limit** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd raguard hop-limit {[maximum *value*] [minimum *value*]}

no ipv6 nd raguard hop-limit [maximum] [minimum]

パラメータ

- **maximum** *value*：ホップカウント制限が **value** 引数以下であることを確認します。範囲 1 ～ 255。高境界の値は、低境界の値以上である必要があります。
- **minimum** *value*：ホップ数制限が **value** 引数以上であることを確認します。範囲 1 ～ 255。

デフォルト設定

ホップカウント制限が検証されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドにより、RA メッセージのアドバタイズされた Cur ホップ制限値（RFC4861 を参照）が **value** 引数によって設定された値を超えている、または未満であることを検証できます。

minimum *value* のキーワードと引数を設定すると、攻撃者がホストで低 Cur ホップ制限値を設定するのを防ぎ、リモート宛先、つまり、デフォルトルータを超えてトラフィックを生成できないようにします。アドバタイズされる Cur ホップ制限値が指定されていない場合（これは 0 の値を設定するのと同じです）、パケットはドロップされます。

maximum *value* のキーワードと引数を設定すると、アドバタイズされた Cur ホップ制限値が **value** 引数によって設定された値以下であることを検証できます。アドバタイズされる Cur ホップ制限値が指定されていない場合（これは 0 の値を設定するのと同じです）、パケットはドロップされます。

no ipv6 nd raguard hop-limit maximum コマンドを使用すると、RA メッセージのアドバタイズされた Cur ホップ制限値の最大境界の検証を無効にできます。

no ipv6 nd raguard hop-limit minimum コマンドを使用すると、RA メッセージのアドバタイズされた Cur ホップ制限値の最小境界の検証を無効にできます。

例 1：次の例では、2 つのコマンドを使用して、最小 Cur ホップ制限値に 3 を、最大 Cur ホップ制限値に 100 を定義します。

```
switchxxxxxx(config)# ipv6 nd raguard hop-limit minimum 3
switchxxxxxx(config)# ipv6 nd raguard hop-limit maximum 100
```

例 2：次の例では、1 つのコマンドを使用して、最小 Cur ホップ制限値に 3 を、最大 Cur ホップ制限値に 100 を定義します。

```
switchxxxxxx(config)# ipv6 nd raguard hop-limit minimum 3 maximum 100
```

ipv6 nd raguard managed-config-flag

RA メッセージのアドバタイズされた管理対象アドレス設定フラグをグローバルに検証するには、**ipv6 nd raguard managed-config-flag** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd raguard managed-config-flag {on | off}

no ipv6 nd raguard managed-config-flag

パラメータ

- **on**：フラグの値は 1 である必要があります。
- **off**：フラグの値は 0 である必要があります。

デフォルト設定

検証は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドでは、RA メッセージのアドバタイズされた管理対象アドレス設定フラグ（または M フラグ）の検証を有効にできます（RFC4861 を参照）。このフラグは、ホストが信頼できない可能性のある DHCPv6 サーバを介してアドレスを強制的に取得するように、攻撃者によって設定される場合があります。

例

次の例では、フラグの値が 0 であるかどうかをチェックする M フラグ検証を有効にします。

```
switchxxxxxx(config)# ipv6 nd raguard managed-config-flag off
```

ipv6 nd raguard other-config-flag

RA メッセージのアドバタイズされた「その他の設定」フラグをグローバルに検証するには、**ipv6 nd raguard other-config-flag** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd raguard other-config-flag {on | off}

no ipv6 nd raguard other-config-flag

パラメータ

- **on**：フラグの値は 1 である必要があります。
- **off**：フラグの値は 0 である必要があります。

デフォルト設定

検証は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドでは、RA メッセージのアドバタイズされた「その他の設定」フラグ（または「O」フラグ）の検証を有効にできます（RFC4861 を参照）。このフラグは、ホストが信頼できない可能性のある DHCPv6 サーバを介して他の設定情報を強制的に取得するように、攻撃者によって設定される場合があります。

例

次の例では、フラグの値が 0 であるかどうかをチェックする O フラグ検証をコマンドが有効にする方法について示します。

```
switchxxxxxx(config)# ipv6 nd raguard other-config-flag off
```

ipv6 nd raguard policy

RA ガード ポリシー名を定義して IPv6 RA ガード ポリシー コンフィギュレーション モードでスイッチを配置するには、**ipv6 nd raguard policy** コマンドをグローバル コンフィギュレーション モードで使用します。RA ガード ポリシーを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 nd raguard policy *policy-name*

no ipv6 nd raguard policy *policy-name*

パラメータ

- ***policy-name***：RA ガード ポリシー名（最大 32 文字）。

デフォルト設定

RA ガード ポリシーは設定されていません

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、RA ガード ポリシー名を定義し、IPv6 RA ガード ポリシー コンフィギュレーション モードでスイッチを配置します。

同じタイプの各ポリシー（たとえば、RA ガード ポリシーなど）には一意の名前が必要です。異なるタイプのポリシーには同じポリシー名を設定できます。

スイッチは、「vlan_default」と「port_default」という 2 つの定義済みの RA ガード ポリシーをサポートします。

```
ipv6 nd raguard policy vlan_default
exit
ipv6 nd raguard policy port_default
exit
```

ポリシーは削除できませんが、変更することはできます。**no ipv6 nd raguard policy** はこれらのポリシーを削除せずに、ユーザが定義したポリシー設定のみを削除します。

VLAN に他のポリシーがアタッチされていない場合、デフォルトでは **vlan_default** ポリシーが VLAN にアタッチされています。ポートに他のポリシーがアタッチされていない場合、デフォルトでは **port_default** ポリシーがポートにアタッチされています。

ipv6 nd raguard policy コマンドを複数回使用すると、ポリシーを定義できます。アタッチされているポリシーを削除すると、削除する前に自動的に切り離されます。

例 1：次の例では、policy1 という名前の RA ガード ポリシーを定義して、RA ガード ポリシー コンフィギュレーション モードでルータを配置し、その他の設定フラグの検証を無効にして、デバイス ロールをルータに設定します。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# other-config-flag disable
switchxxxxxx(config-ra-guard)# device-role router
switchxxxxxx(config-ra-guard)# exit
```

例 2：次の例では、policy1 という名前の RA ガードを複数の手順で定義します。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# other-config-flag disable
switchxxxxxx(config-ra-guard)# exit
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# device-role router
switchxxxxxx(config-ra-guard)# exit
```

例 3：次の例では、接続している RA ガード ポリシーを削除します。

```
switchxxxxxx(config)# no ipv6 nd raguard policy policy1
Policy policy1 is applied on the following ports:
gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

ipv6 nd raguard router-preference

RA メッセージのアドバタイズされたデフォルト ルータ プリファレンス値の検証をグローバルに有効にするには、**ipv6 nd raguard router-preference** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd raguard router-preference {[**maximum** *value*] [**minimum** *value*]}

no ipv6 nd raguard router-preference [maximum] [minimum]

パラメータ

- **maximum** *value*：許可される最大のアドバタイズされるデフォルト ルータ設定値を指定します。次の値が許容されます：**low**、**medium** および **high**（RFC4191 を参照）。高境界の値は、低境界の値以上である必要があります。
- **minimum** *value*：許可される最小のアドバタイズされるデフォルト ルータ設定値を指定します。次の値が許容されます：**low**、**medium** および **high**（RFC4191 を参照）。

デフォルト設定

検証は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドでは、RA メッセージのアドバタイズされたデフォルト ルータ プリファレンス値の検証を有効にします（RFC4191 を参照）。

minimum *value* キーワードと引数を設定すると、許容される最小値が指定されます。*value* 引数より小さいデフォルト ルータ プリファレンス値を持つ受信 RA メッセージはドロップされます。

maximum *value* キーワードと引数を設定すると、許容される最大値が指定されます。*value* 引数より大きいデフォルト ルータ プリファレンス値を持つ受信 RA メッセージはドロップされます。

no ipv6 nd raguard router-preference コマンドを使用すると、RA メッセージのアドバタイズされたデフォルト ルータ プリファレンス値の検証を無効にできます。

no ipv6 nd raguard router-preference maximum コマンドを使用すると、RA メッセージのアドバタイズされたデフォルト ルータ プリファレンス値の最大境界の検証を無効にできます。

no ipv6 nd raguard router-preference minimum コマンドを使用すると、RA メッセージのアドバタイズされたデフォルト ルータ プリファレンス値の検証を無効にできます。

例 1：次の例では、**medium** の値だけが 2 つのコマンドを使用して受け入れられるように定義します。

```
switchxxxxxx(config)# ipv6 nd raguard router-preference minimum medium
switchxxxxxx(config)# ipv6 nd raguard router-preference maximum medium
```

例 2：次の例では、**medium** の値だけが 1 つのコマンドを使用して受け入れられるように定義します。

```
switchxxxxxx(config)# ipv6 nd raguard router-preference minimum medium maximum medium
```

ipv6 neighbor binding

VLAN 上でネイバー バインディング（NB）整合性機能をグローバルに有効にするには、**ipv6 neighbor binding** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 neighbor binding

no ipv6 neighbor binding

パラメータ

該当なし

デフォルト設定

VLAN 上の NB 整合性は無効になっています。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

NB 完全性は、機能が有効になっている VLAN に属する境界ポートに接続されたネイバーのバインディングを確立します。

例 1：次の例では、VLAN 100 上の NB 整合性を有効にします。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 neighbor binding
switchxxxxxx(config-if)# exit
```

例 2：次の例では、VLAN 100-107 上の NB 整合性を有効にします。

```
switchxxxxxx(config)# interface range vlan 100-107
switchxxxxxx(config-if-range)# ipv6 neighbor binding
switchxxxxxx(config-if-range)# exit
```

ipv6 neighbor binding address-config

グローバル IPv6 アドレスで許可された設定方法を指定するには、**ipv6 neighbor binding address-config** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 neighbor binding address-config [stateless | any] [dhcp]

no ipv6 neighbor binding address-config

パラメータ

- **stateless**：NDP メッセージからバインドされたグローバル IPv6 で自動設定のみが許可されます。
- **any**：NDP メッセージ（ステートレスおよび手動）からバインドされたグローバル IPv6 の設定方法のすべてが許可されます。キーワードが定義されていない場合は、キーワード **any** が適用されます。
- **dhcp**：DHCPv6 からのバインディングが許可されます。

デフォルト設定

デフォルト パラメータは Any です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、グローバル IPv6 アドレスで許可されている IPv6 アドレス設定方法を定義します。

stateless および **any** キーワードで次のことを指定します。

- グローバル IPv6 アドレスが NDP メッセージからバインドされます。これらのキーワードを設定しない場合は、リンクローカル アドレスのみが NDP メッセージからバインドされます。
- プレフィックス検証が有効になっている場合、NDP メッセージからバインドされているグローバル IPv6 アドレスをネイバー プレフィックス テーブルと比較してチェックする方法。

  stateless：IPv6 アドレスは NDP メッセージからバインドされます。A フラグが設定された学習済みプレフィックスまたは **autoconfig** キーワードが手動で設定されたプレフィックスに属するグローバル アドレスのみが許可されます。

any：IPv6 アドレスは NDP メッセージからバインドされます。NPT のプレフィックスに属するグローバル アドレスのみが許可されます。

dhcp キーワードを使用すると、DHCPv6 メッセージからのバインディングが可能になります。DHCPv6 メッセージからバインドされた IPv6 アドレスは、ネイバー プレフィックス テーブルと比較して検証されることはありません。DHCPv6 メッセージからバインドされた IPv6 アドレスは、NDP メッセージからバインドされた IPv6 アドレスを上書きします。

注。dhcp キーワードが設定されていない場合、スイッチは NDP メッセージの DHCPv6 によって割り当てられた IPv6 アドレスをバインドします。これは、ホストがこのアドレスの DAD プロセスを実行する必要があるからです。

キーワードが定義されていない場合は、**ipv6 neighbor binding address-config any** コマンドが適用されます。

例 1。次の例では、グローバル IPv6 アドレスのあらゆる設定方法を適用し、DHCPv6 メッセージからバインドされないように指定します。

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
switchxxxxxx(config)# ipv6 neighbor binding address-config any
```

例 2。次の例では、NDP からバインドされたグローバル IPv6 アドレスおよび DHCPv6 メッセージからバインドされたグローバル IPv6 アドレスが許可されるように指定します。

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
switchxxxxxx(config)# ipv6 neighbor binding address-config any dhcp
```

例 3。次の例では、NDP からバインドされたステートレス グローバル IPv6 アドレスのみを適用できるように指定します

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
switchxxxxxx(config)# ipv6 neighbor binding address-config stateless
```

例 4。次の例では、DHCPv6 の設定方法でステートレス IPv6 アドレスのみを設定および割り当て、NDP メッセージからバインディングのみがサポートされるように指定します。

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
switchxxxxxx(config)# ipv6 neighbor binding address-config stateless dhcp
```

例 5。次の例では、グローバル IPv6 アドレスが DHCPv6 のみで割り当てられるように指定します。

```
switchxxxxxx(config)# ipv6 neighbor binding address-config dhcp
```

ipv6 neighbor binding address-prefix

NDP メッセージからバインドされたグローバル IPv6 アドレスのスタティック プレフィックスを定義するには、**ipv6 neighbor binding address-prefix** コマンドをグローバル コンフィギュレーション モードで使用します。プレフィックスを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 neighbor binding address-prefix vlan *vlan-id ipv6-prefix*/*prefix-length* [**autoconfig**]

no ipv6 neighbor binding address-prefix [vlan *vlan-id*] [*ipv6-prefix*/*prefix-length*]

パラメータ

- ***ipv6-prefix***/*prefix-length*：IPv6 prefix.
- **vlan** *vlan-id*：指定した VLAN の ID。
- **autoconfig**：プレフィックスをステートレス設定に使用できます。

デフォルト設定

スタティック プレフィックスなし

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ipv6 neighbor binding address-prefix コマンドを使用すると、ネイバー プレフィックス テーブルにスタティック プレフィックスを追加できます。

ネイバー プレフィックス テーブルから 1 つの静的エントリを削除するには、**no ipv6 neighbor binding address-prefix vlan** *vlan-id ipv6-prefix*/*prefix-length* コマンドを使用します。

特定の VLAN で定義されているネイバー プレフィックス テーブルからすべての静的エントリを削除するには、**no ipv6 neighbor binding address-prefix vlan** *vlan-id* コマンドを使用します。

no ipv6 neighbor binding address-prefix コマンドを使用すると、ネイバー プレフィックス テーブルからすべてのスタティック エントリを削除できます。

例 1。次の例では、2 つのスタティック エントリを追加します。2 つ目のエントリは、ステートレス設定に使用できます。

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix vlan 100 2001:0DB8:101::/64
switchxxxxxx(config)# ipv6 neighbor binding address-prefix vlan 100 2001:0DB8:100::/64
autoconfig
```

例 2。次の例では、1 つのスタティック エントリを削除します。

```
switchxxxxxx(config)# no ipv6 neighbor binding address-prefix vlan 100 2001:0DB8:101::/64
```

例 3。次の例では、指定された VLAN 上で定義されているすべてのスタティック エントリを削除します。

```
switchxxxxxx(config)# no ipv6 neighbor binding address-prefix vlan 100
```

例 4。次の例では、すべてのスタティック エントリを削除します。

```
switchxxxxxx(config)# no ipv6 neighbor binding address-prefix
```

ipv6 neighbor binding address-prefix-validation

ネイバー プレフィックス テーブルと比較してバインドされた IPv6 アドレスの検証をグローバルに有効にするには、**ipv6 neighbor binding address-prefix-validation** コマンドをグローバル コンフィギュレーション モードで使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

ipv6 neighbor binding address-prefix-validation

no ipv6 neighbor binding address-prefix-validation

パラメータ

該当なし

デフォルト設定

機能は無効です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、バインドされたアドレス プレフィックス検証を有効にします。ネイバー バインディング機能が有効になっている場合、スイッチは ipv6 neighbor binding address-prefix コマンドをネイバー バインディング コンフィギュレーション モードを使用して、バインドされたアドレスがネイバー プレフィックス テーブルのプレフィックスのいずれか、または手動で設定したプレフィックス リストに属しているかどうかをチェックします。アドレスが属していない場合はバインドされません。

例

次の例では、ネイバー プレフィックス テーブルと比較してバインドされたアドレスの検証を有効にする方法を示します。

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
```

ipv6 neighbor binding attach-policy（ポート モード）

特定のポートにネイバー バインディング ポリシーを接続するには、**ipv6 neighbor binding attach-policy** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 neighbor binding attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 neighbor binding attach-policy [*policy-name*]

パラメータ

- ***policy-name***：ネイバー バインディング ポリシー名（最大 32 文字）。
- **vlan** *vlan-list*：ネイバー バインディング ポリシーが *vlan-list* で VLAN に接続されるように指定します。キーワード **vlan** が設定されていない場合、ポリシーはネイバー バインディング ポリシーが有効になっているデバイス上のすべての VLAN に適用されます。

デフォルト設定

ネイバー バインディングのデフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、ネイバー バインディング ポリシーをポートに接続できます。

コマンドを使用するたびに、同じポリシー内の以前のコマンドが上書きされます。

policy-name 引数で指定されたポリシーが定義されていない場合、コマンドは拒否されます。

vlan キーワードを使用した複数のポリシーは、共通の VLAN を持っていない場合は同じポートに接続できます。

入力パケットに適用されているルールのセットは次のように構築されます。

- パケットが到着した VLAN 上のインターフェイスに接続されたポートで設定されたルールがセットに追加されます。
- VLANに接続されたポリシーで設定されたルールがセットに追加されます（追加されていない場合）。
- グローバル ルールがセットに追加されます（追加されていない場合）。

no ipv6 neighbor binding attach-policy コマンドを使用すると、ポートに接続されたすべてのユーザ定義済みポリシーを切り離すことができます。

no ipv6 neighbor binding attach-policy *policy-name* コマンドを使用すると、ポートから特定のポリシーを切り離すことができます。

例 1：次に、ネイバー バインディング ポリシー policy1 を gi1/0/1 ポートに接続する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy1
switchxxxxxx(config-if)# exit
```

例 2：次に、ネイバー バインディング ポリシー policy1 をポート gi1/0/1 に接続し、VLAN 1 ～ 10 と 12 ～ 20 に適用する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

例 3：次の例では、ネイバー バインディング ポリシー policy1 はポート gi1/0/1 に接続され、VLAN 1 ～ 10 に適用されます。ネイバー バインディング ポリシー policy2 はポート gi1/0/1 に接続され、VLAN 12～ 20 に適用されます。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

例 4：次の例では、ネイバー バインディング完全性が gi1/0/1 ポートに接続されたポリシー policy1 を切り離します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 neighbor binding attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 neighbor binding attach-policy（VLAN モード）

特定の VLAN にネイバー バインディング ポリシーを接続するには、**ipv6 neighbor binding attach-policy** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 neighbor binding attach-policy *policy-name*

no ipv6 neighbor binding attach-policy

パラメータ

- ***policy-name***：ネイバー バインディング ポリシー名（最大 32 文字）。

デフォルト設定

ネイバー バインディングのデフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、ネイバー バインディング ポリシーを VLAN に接続できます。

policy-name 引数で指定されているポリシーが定義されていない場合、コマンドは拒否されます。

コマンドの **no** 形式を使用すると、現在のポリシーを切り離してデフォルト ポリシーを再び接続できます。コマンドの **No** 形式は、デフォルトのポリシーがアタッチされている場合は影響を与えません。

例

次の例では、ネイバー バインディング ポリシー policy1 は VLAN 100 に接続されています。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 neighbor binding lifetime

ネイバー バインディング テーブル エントリ有効期間のデフォルト値をグローバルに変更するには、**ipv6 neighbor binding lifetime** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 neighbor binding lifetime *value*

no ipv6 neighbor binding lifetime

パラメータ

- ***value***：有効期間（分単位）。指定できる範囲は 1 ～ 60 分です。

デフォルト設定

5 分

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ipv6 neighbor binding lifetime コマンドを使用すると、デフォルトの有効期間を変更できます。

例

次の例では、バインディング エントリの有効期間を 10 分に変更します。

```
switchxxxxxx(config)# ipv6 neighbor binding lifetime 10
```

ipv6 neighbor binding max-entries

バインディング テーブル キャッシュに挿入可能なダイナミック エントリの最大数をグローバルに指定するには、**ipv6 neighbor binding max-entries** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 neighbor binding max-entries {[**vlan-limit** *number*] [**interface-limit** *number*] [**mac-limit** *number*]}

no ipv6 neighbor binding max-entries [**vlan-limit**] [**interface-limit**] [**mac-limit**]

パラメータ

- **vlan-limit** *number*：VLAN の数ごとにネイバー バインディング制限を指定します。
- **interface-limit** *number*：ポートごとにネイバー バインディング制限を指定します。
- **mac-limit** *number*：MAC アドレスごとのネイバー バインディングの制限を指定します。

デフォルト設定

このコマンドは無効です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、バインディングテーブルのコンテンツを制限できます。このコマンドは、バインディング テーブル キャッシュに挿入可能なダイナミック エントリの最大数を指定します。この制限に達すると、新しいエントリは拒否され、新しいエントリを含むネイバー探索プロトコル（NDP）トラフィック送信元はドロップされます。

指定したエントリの最大数がデータベース内のエントリの現在の数より少ない場合は、エントリはクリアされず、通常のキャッシュ減少後に新しいしきい値に到達します。

例

次の例では、MAC ごとにキャッシュに挿入可能なエントリの最大数をグローバルに指定する方法を示します。

```
switchxxxxxx(config)# ipv6 neighbor binding max-entries mac-limit 2
```

ipv6 neighbor binding policy

ネイバーバインディングポリシーを定義してIPv6ネイバーバインディングポリシーコンフィギュレーション モードでスイッチを配置するには、**ipv6 neighbor binding policy** コマンドをグローバル コンフィギュレーション モードで使用します。ネイバー バインディング ポリシーを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 neighbor binding policy *policy-name*

no ipv6 neighbor binding policy *policy-name*

パラメータ

- ***policy-name***：ネイバー バインディング ポリシー名（最大 32 文字）。

デフォルト設定

ネイバー バインディング ポリシーが設定されていません

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドはネイバー バインディング ポリシー名を定義し、追加のコマンドをポリシーに追加できるように、ネイバーバインディングポリシーのコンフィギュレーションモードでルータを配置します。

スイッチは、「vlan_default」と「port_default」という 2 つの定義済みのネイバーバインディング ポリシーをサポートします。

```
ipv6 neighbor binding policy vlan_default
      exit
      ipv6 neighbor binding policy port_default
      exit
```

ポリシーは削除できませんが、変更することはできます。**no ipv6 neighbor binding policy** はこれらのポリシーを削除せずに、ユーザが定義したポリシー設定のみを削除します。

ipv6 neighbor binding policy コマンドを複数回使用すると、ポリシーを定義できます。

アタッチされているポリシーを削除すると、削除する前に自動的に切り離されます。

例 1：次の例では、policy1 という名前のネイバー バインディング ポリシーを定義して、ネイバー バインディング ポリシー コンフィギュレーション モードでルータを配置し、ロギングを有効にして、内部としてポートを定義します。

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# device-role internal
switchxxxxxx(config-nbr-binding)# logging binding
switchxxxxxx(config-nbr-binding)# exit
```

例 2：次の例では、policy1 という名前のネイバー バインディング ポリシーを複数の手順で定義します。

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# device-role internal
switchxxxxxx(config-nbr-binding)# exit
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
logging binding
witchxxxxxx(config-nbr-binding)# exit
```

例 3：次の例では、接続しているネイバー バインディング ポリシーを削除します。

```
switchxxxxxx(config)# no ipv6 neighbor binding policy policy1
Policy policy1 is applied on the following ports:
 gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

ipv6 neighbor binding static

ネイバー バインディング テーブルにスタティック エントリを追加するには、**ipv6 neighbor binding static** コマンドをグローバル コンフィギュレーション モードで使用します。スタティック エントリを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 neighbor binding static ipv6 *ipv6-address* **vlan** *vlan-id* **interface** *interface-id* **mac** *mac-address*

no ipv6 neighbor binding static ipv6 *ipv6-address* **vlan** *vlan-id*

パラメータ

- **ipv6** *ipv6-address*：スタティック エントリの IPv6 アドレス。
- **vlan** *vlan-id*：指定した VLAN の ID。
- **interface** *interface-id*：指定したポートにスタティック エントリを追加します。
- **mac** *mac-address*：スタティック エントリの MAC アドレス。

デフォルト設定

スタティック エントリなし。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、スタティック エントリをネイバー バインディング テーブルに追加するために使用します。スタティック エントリは、ポートのロールに関係なく設定されます。

エントリ（ダイナミックまたはスタティック）がすでに存在する場合は、新しいスタティック エントリによって既存のエントリが上書きされます。

ネイバー バインディング テーブルがオーバーフローした場合は、スタティック エントリは追加されません。

例

次の例では、スタティック エントリを追加します。

```
switchxxxxxx(config)# ipv6 neighbor binding static ipv6 2001:600::1 vlan 100 interface
gi1/0/1 mac 00BB.CC01.F500
```

ipv6 source guard

VLAN 上で IPv6 ソース ガード機能を有効にするには、**ipv6 source guard** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 source guard

no ipv6 source guard

デフォルト設定

VLAN 上でソース ガードは無効です。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

ソース IPv6 アドレスが別のポートにバインドされている場合、または不明な場合、IPv6 ソース ガードはポートで受信した IPv6 データ メッセージをブロックします。

例 1：次の例では、VLAN 100 上の IPv6 ソース ガードを有効にします。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 source guard
switchxxxxxx(config-if)# exit
```

例 2：次の例では、VLAN 100-107 上の IPv6 ソース ガードを有効にします。

```
switchxxxxxx(config)# interface range vlan 100-107
switchxxxxxx(config-if-range)# ipv6 source guard
switchxxxxxx(config-if-range)# exit
```

ipv6 source guard attach-policy（ポート モード）

特定のポートで IPv6 ソース ガード ポリシーを接続するには、**ipv6 source guard attach-policy** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 source guard attach-policy *policy-name*

no ipv6 source guard attach-policy

パラメータ

- ***policy-name***：IPv6 ガード ポリシー名（最大 32 文字）。

デフォルト設定

IPv6 ソース ガードのデフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

is コマンドは IPv6 ソース ガード ポリシーをポートに接続します。

後続の各 **ipv6 source guard attach-policy** コマンドは、同じポートの前のポリシー アタッチメントを上書きします。

IPv6 ソース ガード ポリシーを使用すると、不明な送信元 IPv6 アドレスまたは入力ポートと異なるポートにバインドされた送信元 IPv6 アドレスが指定された転送 IPv6 データ メッセージをブロックできます。

policy-name 引数で指定されているポリシーが定義されていない場合、コマンドは拒否されます。

入力パケットに適用されているルールのセットは次のように構築されます。

- ポリシーで設定されたルールがポートに接続されています。
- グローバル ルールがセットに追加されます（追加されていない場合）。

no ipv6 source guard attach-policy コマンドを使用すると、ポートに接続されたユーザ定義ポリシーを切り離して、「port_default」という名前のデフォルト ポリシーを再接続します。

例 1：次に、IPv6 送信元ガードポリシー policy1 を gi1/0/1 ポートに接続する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 source guard attach-policy policy1
switchxxxxxx(config-if)# exit
```

例 2：次に、IPv6 送信元ガードが policy1 を gi1/0/1 ポートから切り離す例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 source guard attach-policy
switchxxxxxx(config-if)# exit
```

ipv6 source guard policy

IPv6 ソース ガード ポリシー名を定義して IPv6 ソース ガード コンフィギュレーションでユーザを配置するには、**ipv6 source guard policy** コマンドをグローバル コンフィギュレーション モードで使用します。IPv6 ソース ガード ポリシー名を削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 source guard policy *policy-name*

no ipv6 source guard policy *policy-name*

パラメータ

- ***policy-name***：IPv6 ガード ポリシー名（最大 32 文字）。

デフォルト設定

IPv6 ソース ガード ポリシーが設定されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、IPv6 ソース ガード ポリシー名を定義し、IPv6 ソース ガード ポリシー コンフィギュレーション モードでルータを配置します。

同じタイプの各ポリシー（たとえば、IPv6 ソース ガード ポリシーなど）には一意の名前が必要です。異なるタイプのポリシーには同じポリシー名を設定できます。

スイッチは、「port_default」という名前の IPv6 ソース ガード ポリシーを 1 つサポートします。

```
ipv6 source guard policy port_default
      exit
```

ポリシーは削除できませんが、変更することはできます。**no ipv6 source guard policy** はポリシーを削除せずに、ユーザによって定義されたポリシー設定のみを削除します。

アタッチされているポリシーを削除すると、削除する前に自動的に切り離されます。

例 1：次の例では、policy1 という IPv6 ソース ガード ポリシーを定義し、IPv6 ソース ガード ポリシー コンフィギュレーション モードでルータを配置して、ポートを信頼済みとして設定します。

```
switchxxxxxx(config)# ipv6 source guard policy policy1
switchxxxxxx(config-ipv6-srcguard)# trusted-port
switchxxxxxx(config)# exit
```

例 2：次の例では、接続している IPv6 ソース ガード ポリシーを削除します。

```
switchxxxxxx(config)# no ipv6 source guard policy policy1
Policy policy1 is applied on the following ports:
gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

logging binding

IPv6 ネイバー バインディング ポリシー内のバインディング テーブル メイン イベントのロギングを有効にするには、**logging binding** コマンドをネイバー バインディング ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

logging binding [enable | disable]

no logging binding

パラメータ

- **enable**：バインディング テーブル メイン イベントのロギングを有効にします。キーワードが設定されていない場合、デフォルトでこのキーワードが適用されます。
- **disable**：バインディング テーブル メイン イベントのロギングを無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

ネイバー バインディング ポリシー コンフィギュレーション モード。

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

例

次の例では、policy1 という名前の IPv6 ネイバー バインディング ポリシー内でバインディング テーブル メイン イベントのロギングを有効にします。

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# logging binding enable
switchxxxxxx(config-nbr-binding)# exit
```

logging packet drop

IPv6 ファースト ホップ セキュリティ ポリシー内でドロップされたパケットのロギングを有効にするには、**logging packet drop** コマンドを IPv6 ファースト ホップ セキュリティ ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

logging packet drop [enable | disable]

no logging packet drop

パラメータ

- **enable**：ドロップされたパケットのロギングを有効にします。キーワードが設定されていない場合、デフォルトでこのキーワードが適用されます。
- **disable**：ドロップされたパケットのロギングを無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

IPv6 ファースト ホップ セキュリティ ポリシーのコンフィギュレーション モード

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

例

次の例では、policy1 という名前の IPv6 ファースト ホップ セキュリティ ポリシーが指定されたドロップされたメッセージのロギングを有効にします。

```
switchxxxxxx(config)# ipv6 first hop security policy policy1
switchxxxxxx(config-ipv6-fhs)# logging packet drop
switchxxxxxx(config-ipv6-fhs)# exit
```

managed-config-flag

IPv6 RA ガード ポリシー内でアドバタイズされる管理対象のアドレス設定フラグの検証を有効にするには、**managed-config-flag** コマンドを RA ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

managed-config-flag {on | off | disable}

no managed-config-flag

パラメータ

- **on**：フラグの値は 1 である必要があります。
- **off**：フラグの値は 0 である必要があります。
- **disable**：フラグの値を検証されません。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

RA ガード ポリシー コンフィギュレーション モード

例

次の例では、policy1 という名前の RA ガード ポリシーを定義し、RA ガード ポリシー コンフィギュレーション モードでスイッチを配置して、フラグの値が 0 であるかどうかをチェックする M フラグの検証を有効にします。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# managed-config-flag off
switchxxxxxx(config-ra-guard)# exit
```

match ra address

IPv6 RA ガード ポリシー内で受信した RA メッセージでルータの IPv6 アドレスの検証を有効にするには、**match ra address** コマンドを RA ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

match ra address {**prefix-list** *ipv6-prefix-list-name*} | **disable**

no match ra address

パラメータ

- **prefix-list** *ipv6-prefix-list-name*：照合する IPv6 プレフィックス リストです。
- **disable**：ルータの IPv6 アドレスの検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN に接続されているポリシー：ルータのアドレスは検証されません。

コマンド モード

RA ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドは、設定済みプレフィックス リストを使用して受信した RA メッセージでルータの IPv6 アドレスの検証を有効にします。ルータの送信元 IPv6 アドレスがプレフィックス リストと一致しない場合、またはプレフィックス リストが設定されていない場合は、RA メッセージがドロップされます。

disable キーワードを使用すると、VLAN 設定に関係なく IPv6 アドレスのルータの検証を無効にします。

例

次の例では、policy1 という名前の RA ガード ポリシーを定義し、RA ガード ポリシー コンフィギュレーション モードでスイッチを配置して、list1 という名前のプレフィックス リストに対してルータ アドレスを照会し、リンクローカル アドレス FE80::A8BB:CCFF:FE01:F700 のみが指定されたルータを許可する list1 という名前のプレフィックス リストを定義します。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# match ra address prefix-list list1
switchxxxxxx(config-ra-guard)# exit
switchxxxxxx(config)# ipv6 prefix-list list1 permit FE80::A8BB:CCFF:FE01:F700/128
```

match ra prefixes

IPv6 RA ガード ポリシー内で受信した RA メッセージでアドバタイズされたプレフィックスの検証を有効にするには、**match ra prefixes** コマンドを RA ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

match ra prefixes {**prefix-list** *ipv6-prefix-list-name*} | **disable**

no match ra prefixes

パラメータ

- **prefix-list** *ipv6-prefix-list-name*：照合する IPv6 プレフィックス リストです。
- **disable**：受信した RA メッセージ内のアドバタイズされたプレフィックスの検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：アドバタイズされたプレフィックスは検証されません。

コマンド モード

RA ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドは、設定済みプレフィックス リストを使用して受信した RA メッセージでアドバタイズされたプレフィックスの検証を有効にします。アドバタイズされたプレフィックスがプレフィックス リストと一致しない場合、またはプレフィックス リストが設定されていない場合は、RA メッセージがドロップされます。

disable キーワードを使用すると、グローバル設定と VLAN 設定の両方で受信した RA メッセージでアドバタイズされたプレフィックスの検証を無効にできます。

例

次の例では、policy1 という名前の RA ガード ポリシーを定義し、RA ガード コンフィギュレーション モードでスイッチを配置して、list1 という名前のプレフィックス リストに対して 2001:101::/64 プレフィックスを照会し、2001:100::/64 プレフィックスを拒否します。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# match ra prefixes prefix-list list1
switchxxxxxx(config-ra-guard)# exit
```

```
switchxxxxxx(config)# ipv6 prefix-list list1 deny 2001:0DB8:101::/64
switchxxxxxx(config)# ipv6 prefix-list list1 permit 2001:0DB8:100::/64
```

match reply

DHCPv6 ガード ポリシー内で設定されたプレフィックス リストに DHCPv6 サーバ/リレーによって送信されたメッセージで割り当てられた IPv6 アドレスの検証を有効にするには、**match reply** コマンドを DHCPv6 ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

match reply {**prefix-list** *ipv6-prefix-list-name*} | **disable**

no match reply

パラメータ

- ***ipv6-prefix-list-name***：照合される IPv6 プレフィックス リスト。
- **disable**：応答にアドバタイズされたプレフィックスの検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：アドバタイズされたプレフィックスは検証されません。

コマンド モード

DHCP ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

IPv6 DHCP ガードでは、割り当てられた IPv6 アドレスを検証して、DHCPv6 サーバ/リレーによって送信された次の DHCPv6 メッセージの IA_NA および IA_TA オプションで渡されたプレフィックス リストを設定できます。

- ADVERTISE
- REPLY
- RELAY-REPL

注 1：ステータス オプションの値（存在する場合）が次のオプションと異なる場合、割り当てられたアドレスは検証されません。

- Success
- UseMulticast

注 2：RELAY-REPL メッセージでは、DHCPv6 ガードは、DHCP-relay-message オプションでカプセル化されたメッセージを検証します。

disable キーワードを使用すると、応答で割り当てられた IPv6 アドレスの検証を無効にできます。

例

次の例では、policy1 という名前の DHCPv6 ガード ポリシーを定義し、DHCPv6 ガード ポリシー コンフィギュレーション モードでスイッチを配置して、list1 という名前のプレフィックス リストに対して割り当てられたアドレスを照会します。割り当てられたすべての IPv6 アドレスは 2001:0DB8:100:200/64 or to 2001:0DB8:100::/48 に属する必要があります。プレフィックス リストの各プレフィックスに対して、「**ge 128**」 パラメータを 128 未満のプレフィックス長で設定する必要があります。

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# match reply prefix-list list1
switchxxxxxx(config-dhcp-guard)# exit
switchxxxxxx(config)# ipv6 prefix-list list1 deny 2001:0DB8:100:200/64 ge 128
switchxxxxxx(config)# ipv6 prefix-list list1 permit 2001:0DB8:100::/48 ge 128
```

match server address

DHCPv6 ガードポリシー内で設定されたプレフィックス リストに DHCPv6 サーバまたは DHCPv6 リレーによって送信されたメッセージで送信元 IPv6 アドレスの検証を有効にするには、**match server address** コマンドを DHCPv6 ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

match server address {**prefix-list** *ipv6-prefix-list-name*} | **disable**

no match server address

パラメータ

- **prefix-list** *ipv6-prefix-list-name*：照合する IPv6 プレフィックス リストです。
- **disable**：DHCP サーバとリレーの IPv6 アドレスの検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN に接続されているポリシー：サーバのアドレスは検証されません。

コマンド モード

DHCP ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドは、設定したプレフィックス リストに DHCPv6 サーバおよび DHCPv6 リレーによって送信されたメッセージで送信元 IPv6 アドレスの検証を有効にします。送信元 IPv6 アドレスが設定されているプレフィックス リストと一致しない場合、またはプレフィックス リストが設定されていない場合、DHCPv6 応答はドロップされます。

IPv6 DHCP ガードは、DHCPv6 サーバ/リレーによって送信された次の DHCPv6 メッセージで送信元 IPv6 アドレスを検証します。

- ADVERTISE
- REPLY
- RECONFIGURE
- RELAY-REPL
- LEASEQUERY-REPLY

disable キーワードを使用すると、DHCP サーバおよびリレーの IPv6 アドレスの検証を無効にします。

例

次の例では、policy1 という名前の DHCPv6 ガード ポリシーを定義し、DHCPv6 ガード ポリシー コンフィギュレーション モードでスイッチを配置して、list1 という名前のプレフィックス リストに対してサーバまたはリレー アドレスを照会し、リンクローカル アドレス FE80::A8BB:CCFF:FE01:F700 のみが指定されたサーバを許可する list1 という名前のプレフィックス リストを定義します。

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# match server address prefix-list list1
switchxxxxxx(config-dhcp-guard)# exit
switchxxxxxx(config)# ipv6 prefix-list list1 permit FE80::A8BB:CCFF:FE01:F700/128
```

max-entries

IPv6 ネイバー バインディング ポリシー内のバインディング テーブル キャッシュに挿入できるダイナミック エントリの最大数を定義するには、**max-entries** コマンドをネイバー バインディング ポリシー コンフィギュレーション モードで使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

max-entries {[**vlan-limit** {*number* | **disable**}] [**interface-limit** {*number* | **disable**}] [**mac-limit** {*number* | **disable**}]}

no max-entries [**vlan-limit**] [**interface-limit**] [**mac-limit**]

パラメータ

- **vlan-limit** *number*：VLAN の数ごとにネイバー バインディング制限を指定します。パラメータはポートに接続されたポリシーで無視されます。
- **vlan-limit disable**：VLAN の数ごとにネイバー バインディング制限を無効にします。
- **interface-limit** *number*：ポートごとにネイバー バインディング制限を指定します。
- **interface-limit disable**：ポートごとにネイバー バインディング制限を無効にします。
- **mac-limit** *number*：MAC アドレスごとのネイバー バインディングの制限を指定します。
- **mac-limit disable**：MAC アドレスごとにネイバー バインディング制限を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

ネイバー バインディング ポリシー コンフィギュレーション モード。

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

例 1：次の例では、policy1 という名前のネイバー バインディング ポリシーを定義し、ネイバー バインディング ポリシー コンフィギュレーション モードでルータを配置して、ポートで許可される IPv6 アドレスの数を 25 に制限します。

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# max-entries interface-limit 25
switchxxxxxx(config)# exit
```

例 2：次の例では、policy1 という名前の RA ガード ポリシーを定義し、RA ガード ポリシー コンフィギュレーション モードでスイッチを配置して、MAC ごとに制限を無効にします。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# max-entries mac-limit disable

switchxxxxxx(config-ra-guard)# exit
```

other-config-flag

IPv6 RA ガード ポリシー内の RA メッセージでアドバタイズされたその他の設定フラグの検証を有効にするには、**other-config-flag** コマンドを RA ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

other-config-flag {on | off | disable}

no other-config-flag

パラメータ

- **on**：フラグの値は 1 である必要があります。
- **off**：フラグの値は 0 である必要があります。
- **disable**：フラグの値を検証されません。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

RA ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

disable キーワードを使用すると、グローバル設定と VLAN 設定の両方でフラグの検証を無効にします。

例

次の例では、policy1 という名前の RA ガードポリシーを定義し、RA ガードポリシー コンフィギュレーション モードでスイッチを配置して、フラグの値が 0 であるかどうかをチェックする O フラグの検証を有効にします。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# other-config-flag off
switchxxxxxx(config-ra-guard)# exit
```

preference

DHCPv6 ガード ポリシー内で DHCPv6 サーバによって送信されたメッセージでプリファレンスの検証を有効にするには、**preference** コマンドを DHCPv6 ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

preference {[**maximum** {*value* | **disable**}] [**minimum** {*value* | **disable**}]}

no preference [maximum] [minimum]

パラメータ

- **maximum** *value*：アドバタイズされたプリファレンス値は value 引数以下です。範囲 0 ～ 255。高境界の値は、低境界の値以上である必要があります。
- **maximum disable**：アドバタイズされたプリファレンス値の高位境界の検証を無効にします。
- **minimum** *value*：アドバタイズ設定値は **value** 引数以上です。範囲 0 ～ 255。
- **minimum disable**：アドバタイズされたプリファレンス値の下位境界の検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

DHCP ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

disable キーワードを使用すると、グローバル設定と VLAN 設定の両方で検証を無効にします。

例

次の例では、policy1 という名前の DHCPv6 ガード ポリシーを定義し、DHCPv6 ガード ポリシー コンフィギュレーション モードでスイッチを配置して、最小プリファレンス値を 10 に定義します。

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# preference minimum 10
switchxxxxxx(config-dhcp-guard)# exit
```

router-preference

IPv6 RA ガード ポリシー内の RA メッセージでアドバタイズされたデフォルト ルータ プリファレンス値の検証を有効にするには、**router-preference** コマンドを RA ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

router-preference [**maximum** {*value* | **disable**}] [**minimum** {*value* | **disable**}]

no router-preference [maximum] [minimum]

パラメータ

- **maximum** *value*：許可される最大のアドバタイズされるデフォルト ルータ設定値を指定します。次の値が許容されます：**low**、**medium** および **high**（RFC4191 を参照）。高境界の値は、低境界の値以上である必要があります。
- **maximum disable**：アドバタイズされたデフォルト ルータ プリファレンスの高位境界の検証を無効にします。
- **minimum** *value*：許可される最小のアドバタイズされるデフォルト ルータ設定値を指定します。次の値が許容されます：**low**、**medium** および **high**（RFC4191 を参照）。
- **minimum disable**：アドバタイズされたデフォルト ルータ プリファレンスの下位境界の検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

RA ガード ポリシー コンフィギュレーション モード

例

次の例では、policy1 という名前の RA ガードポリシーを定義し、RA ガードポリシー コンフィギュレーション モードでスイッチを配置して、最小デフォルト ルータ プリファレンス値を 中に定義します。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# router-preference minimum medium
switchxxxxxx(config-ra-guard)# exit
```

sec-level minimum

Ipv6 ND インスペクション ポリシー内で最小セキュリティ レベル値を指定するには、**sec-level minimum** コマンドを ND インスペクション ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

sec-level minimum *value* | disable

no sec-level minimum

パラメータ

- ***value***：最小セキュリティ レベルを設定します。値は 0 ～ 7 です。
- **disable**：セキュリティ レベル パラメータの検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

ND インスペクション ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

保護されていないメッセージのドロップが無効になると、このコマンドは無効になります。

例

次の例では、policy1 という名前の NDP インスペクション ポリシーを定義し、ND インスペクション ポリシー コンフィギュレーション モードでスイッチを配置して、最小 CGA セキュリティ レベルに 2 を指定します。

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# sec-level minimum 2
switchxxxxxx(config-nd-inspection)# exit
```

show ipv6 dhcp guard

DHCPv6 ガード グローバル コンフィギュレーションを表示するには、**show ipv6 dhcp guard** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 dhcp guard

コマンド モード

特権 EXEC モード

使用上のガイドライン

show ipv6 dhcp guard コマンドでは、DHCPv6 ガードのグローバル設定を表示します。

例

次に、**show ipv6 dhcp guard** コマンドの出力例を示します。

```
switchxxxxxx# show ipv6 dhcp guard
IPv6 DHCP Guard is enabled on VLANs:1-4,6,7,100-120
Default Preference
  minimum: 10
  maximum: 100
```

show ipv6 dhcp guard policy

DHCPv6 ガード機能を使用して設定されたすべてのポートで DHCPv6 ガード ポリシーを表示するには、**show ipv6 dhcp guard policy** コマンドを特権 EXEC モードで使用します。

構文

show ipv6 dhcp guard policy [*policy-name* | **active**]

パラメータ

- ***policy-name***：任意の名前で DHCPv6 ガード ポリシーを表示します。
- **active**：接続されている DHCPv6 ガード ポリシーを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、DHCPv6ガード機能を使用して設定されたすべてのポートでポリシー用に設定されたオプションを表示します。

例 1：次の例は、policy1 という名前のポリシーのポリシー設定を示します。

```
switchxxxxxx# show ipv6 dhcp guard policy policy1
DHCPv6 Guard Policy: policy1
  device-role: server
  preference
    minimum: 1
    maximum: 200
  server address prefix list: list1
  reply prefix list name: list10
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLAN
	gi1/0/1 ～ 2	1 ～ 58、68 ～ 4094
	gi1/0/3 ～ 4	1-4094
	Po1 ～ 4	1-4094

例 2：次の例は、接続されているポリシーを示します。

```
switchxxxxxx# show ipv6 dhcp guard policy active
Attached to VLAN:
  Policy Name   VLANs
  policy2       200-300
  vlan-default  1-199,301-4094
Attached to ports:
```

	[Policy Name]	Ports	VLAN
	policy1	gi1/0/1 ～ 2	1-100
	port-default	gi1/0/1 ～ 2	101 ～ 4094
		gi1/0/3 ～ 4	1 ～ 1094

例 3：次の例は、ユーザ定義ポリシーを示します。

```
switchxxxxxx# show ipv6 dhcp guard policy
policy1
policy2
```

show ipv6 first hop security

すべての IPv6 ファースト ホップ セキュリティ グローバル コンフィギュレーションを表示するには、**show ipv6 first hop security** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 first hop security

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、すべての IPv6 ファースト ホップ セキュリティ グローバル コンフィギュレーションを表示します。

例

次に、**show ipv6 first hop security** コマンドの例を示します。

```
switchxxxxxx# show ipv6 first hop security
IPv6 First Hop Security is enabled on VLANs:1-4,6,7,100-120
Logging Packet Drop: enabled
```

show ipv6 first hop security active policies

ポートおよびVLANに適用されたポリシーの情報を表示するには、**show ipv6 first hop security active policies** コマンドを特権 EXEC モードで使用します。

構文

show ipv6 first hop security active policies interface *interface-id* vlan *vlan-id*

パラメータ

- **interface** *interface-id*：ポート識別子（イーサネット ポートまたはポート チャネル）。
- **vlan** *vlan-id*：VLAN ID。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、任意のポートで受信したフレームおよび任意の VLAN に属するフレームに適用されたポリシーを表示します。ポリシーは、ポート、VLAN、およびグローバル コンフィギュレーションに接続されているポリシーを使用して自動的に計算されます

例

次に、gi1/0/1 と VLAN 100 で接続されているアクティブなポリシーを表示する例を示します。

```
switchxxxxxx# show ipv6 first hop security active policies interface gi1/0/1 vlan 100
IPv6 First Hop Security is enabled on VLANs:1-4,6,7,100-120
IPv6 DHCP Guard is enabled on VLANs:1-4
IPv6 ND Inspection is enabled on VLANs:1-4,6,7,100-120
IPv6 Neighbor Binding Integrity is enabled on VLANs:1-4,6,7,100-120
IPv6 RA Guard is enabled on VLANs:1-4,6,7,100-120
IPv6 Source Guard is enabled on VLANs:1-3,7,100-112
gi1/0/1, VLAN 100
IPv6 First Hop Security Policy:
  logging packet drop: enabled (from global configuration)
DHCPv6 Guard Policy:
  device-role: server (from policy1 attached to the port)
  reply prefix list name: list10 (from policy2 attached to the VLAN)
  server address prefix list name: list22 (from policy2 attached to the VLAN)
  preference
    minimum: 1 (from policy2 attached to the VLAN)
    maximum: 200 (from policy2 attached to the VLAN)
ND Inspection Policy:
  device-role: host (default)
  drop-unsecure: enabled (from policy2 attached to the VLAN)
  sec-level minimum: 3 (from policy1 attached to the port)
  validate source-mac: enabled (from global configuration)
Neighbor Binding Policy: policy1
  device-role: perimiter (default)
  logging binding: enabled (from policy1 attached to the port)
  address-prefix-validation: enabled (from policy2 attached to the VLAN)
```

```
  address-config: any (default)
  maximum entries
   VLAN: unlimited (from global configuration)
   Port: 1 (from policy1 attached to the port)
   MAC: 2 (from policy2 attached to the VLAN)
RA Guard Policy:
  device-role: router (from policy1 attached to the port)
  hop-limit:
    minimum: 10 (from policy2 attached to the VLAN)
    maximum: 20 (from global configuration)
  manage-config-flag: on(from policy2 attached to the VLAN)
  ra address verification::  disabled(default)
  ra prefixes prefix list name: list1(from policy2 attached to the VLAN)
  other-flag: disabled (default)
  router-preference:
    minimum: medium (from policy2 attached to the VLAN)
    maximum: medium (from policy2 attached to the VLAN)
IPv6 Source Guard Policy:
  trusted port: enabled (from policy1 attached to the port)
```

show ipv6 first hop security attached policies

ポートおよびVLANに接続されたポリシーの情報を表示するには、**show ipv6 first hop security attached policies** コマンドを特権 EXEC モードで使用します。

構文

show ipv6 first hop security attached policies interface *interface-id* vlan *vlan-id*

パラメータ

- **interface** *interface-id*：ポート識別子（イーサネット ポートまたはポート チャネル）。
- **vlan** *vlan-id*：VLAN ID。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、*vlan-id* 引数で指定された VLAN に接続されているすべての IPv6 ファースト ホップ セキュリティのポリシーと、*interface-id* 引数および *vlan-id* 引数で指定されたポートと VLAN に接続されているすべてのポリシーを表示します。

例

次に、gi1/0/1 と VLAN 100 に接続されているポリシーを表示する例を示します。

```
switchxxxxxx# show ipv6 first hop security attached policies interface gi1/0/1 vlan 100
Attached to VLAN 100
  RA Guard Policy: policy1
  Neighbor Bind Policy: policy2
Attached to port gi1/0/1 and VLAN 100
  IPv6 First Hop Security Policy: FHSpolicy
  ND Inspection Policy: policy1
  RA Guard Policy: policy3
  Neighbor Bind Policy: policy3
  IPv6 Source Guard Policy: policy4
```

show ipv6 first hop security counters

ポート カウンタでカウントされるパケットの情報を表示するには、**show ipv6 first hop security counters** コマンドを特権 EXEC モードで使用します。

構文

show ipv6 first hop security counters interface *interface-id*

パラメータ

- **interface** *interface-id*：指定しているイーサネット ポートまたはポート チャネルのカウンタを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、ポート カウンタでカウントされているスイッチによって処理されたパケットを表示します。スイッチは、ポートごとにキャプチャされたパケットをカウントし、パケットの受信、ブリッジ、またはドロップが行われたかどうかを記録します。パケットがドロップされると、ドロップの理由とドロップの原因となった機能の両方が表示されます。

例

次に、ポート gi1/0/1 でカウントされたパケットに関する情報を表示する例を示します。

```
switchxxxxxx# show ipv6 first hop security counters interface gi1/0/1
Received messages on gi1/0/1:
  Protocol   Protocol message
  NDP        RA[63] RS[0] NA[13] NS[0] REDIR[0]
  DHCPv6     ADV[0] REP[20] REC[0] REL-REP[0] LEAS-REP[10] RLS[0] DEC[0]
Dropped messages on gi1/0/1:
  Protocol   Protocol message
  NDP        RA[2] RS[0] NA[0] NS[0] REDIR[0]
  DHCPv6     ADV[1] REP[2] REC[0] REL-REP[1] LEAS-REP[0] RLS[0] DEC[0]
Dropped reasons on gi1/0/1:
  Feature         Number Reason
  DHCP Guard           2  Server message on client port
  DHCP Guard           1  Unauthorized assigned address
  DHCP Guard           1  Unauthorized server source address
  DHCP Guard           0  Unauthorized server preference
  RA guard             1  Router message on host port
  RA guard             1  Unauthorized source address
  RA guard             0  Unauthorized advertise prefix
  RA guard             0  Unauthorized router preference
  RA guard             0  Unauthorized other config flag
  RA guard             0  Unauthorized managed config flag
  RA guard             0  Unauthorized cur hop limit
  ND Inspection        0  Invalid source MAC
  ND Inspection        0  Unsecure message
  ND Inspection        0  Unauthorized sec level
```

```
Source guard          0  NoBinding
NB Integrity          0  Illegal ICMPv6 message
NB Integrity          0  Illegal DHCPv6 message
```

show ipv6 first hop security error counters

グローバル エラー カウンタを表示するには、**show ipv6 first hop security error counters** コマンドを特権 EXEC モードで使用します。

構文

show ipv6 first hop security error counters

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドはグローバル エラー カウンタを表示します。

例 1：次の例では、グローバル エラー カウンタを示します。

```
switchxxxxxx# show ipv6 first hop security error counters
Neighbor Binding Table Overflow counter: 0
Neighbor Prefix Table Overflow counter: 0
TCAM Overflow counter: 0
```

show ipv6 first hop security policy

IPv6 ファースト ホップ セキュリティ機能で設定したすべてのポートで IPv6 ファースト ホップ セキュリティ ポリシーを表示するには、**show ipv6 first hop security policy** コマンドを特権 EXEC モードで使用します。

構文

show ipv6 first hop security policy [*policy-name* | **active**]

パラメータ

- ***policy-name***：任意の名前の IPv6 ファースト ホップ ポリシーを表示します。
- **active**：接続されている Ipv6 ファースト ホップ セキュリティ ポリシーを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、IPv6 ファースト ホップ ガード機能を使用して設定されたすべてのポートでポリシー用に設定されたオプションを表示します。

例 1：次の例は、policy1 という名前のポリシーのポリシー設定を示します。

```
switchxxxxxx# show ipv6 first hop security policy policy1
IPv6D First Hop Security Policy: policy1
  logging packet drop: enabled
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLAN
	gi1/0/1 ～ 2	1 ～ 58、68 ～ 4094
	gi1/0/3 ～ 4	1-4094
	Po1 ～ 4	1-4094

例 2：次の例は、接続されているポリシーを示します。

```
switchxxxxxx# show ipv6 first hop security policy active
Attached to VLAN:
  Policy Name   VLANs
  policy2       200-300
  vlan-default  1-199,301-4094
Attached to ports:
```

	[Policy Name]	Ports	VLAN
	policy1	gi1/0/1 ～ 2	1-100
	port-default	gi1/0/1 ～ 2	101 ～ 4094
		gi1/0/3 ～ 4	1 ～ 1094

例 3：次の例は、ユーザ定義ポリシーを示します。

```
switchxxxxxx# show ipv6 first hop security policy
policy1
policy2
```

show ipv6 nd inspection

ND インスペクション グローバル コンフィギュレーションを表示するには、**show ipv6 nd inspection** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 nd inspection

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは ND インスペクション グローバル コンフィギュレーションを表示します。

例

次に、**show ipv6 nd snooping** コマンド出力の例を示します。

```
switchxxxxxx# show ipv6 nd snooping
IPv6 ND Inspection is enabled on VLANs:1-4,6,7,100-120
unsecure drop: enabled
sec-level minimum value: 2
source mac validation: disabled
```

show ipv6 nd inspection policy

ND インスペクション機能で設定したすべてのポートの IPv6 ND インスペクション ポリシーを表示するには、**show ipv6 nd inspection policy** コマンドを特権 EXEC モードで使用します。

構文

show ipv6 nd inspection policy [*policy-name* | **active**]

パラメータ

- ***policy-name***：任意の名前の ND インスペクション ポリシーを表示します。
- **active**：接続されている ND インスペクション ポリシーを表示します。

コマンド モード

特権 EXEC モード

例

例 1：次の例は、policy1 という名前のポリシーのポリシー設定を示します。

```
switchxxxxxx# show ipv6 nd inspection policy policy1
ND Inspection Policy: policy1
  device-role: router
  drop-unsecure: enabled
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLAN
	gi1/0/1 ～ 2	1 ～ 58、68 ～ 4094
	gi1/0/3 ～ 4	1-4094
	Po1	1-4094

例 2：次の例は、接続されているポリシーを示します。

```
switchxxxxxx# show ipv6 nd inspection policy active
Attached to VLANs:
  Policy Name   VLANs
  vlan-default  1-4094
Attached to ports:
```

	[Policy Name]	Ports	VLAN
	policy1	gi1/0/1 ～ 2	1-100
	port-default	gi1/0/1 ～ 2	101 ～ 4094
		gi1/0/3 ～ 4	1 ～ 1094

例 3：次の例は、ユーザ定義ポリシーを示します。

```
switchxxxxxx# show ipv6 nd inspection policy
policy1
policy2
```

show ipv6 nd raguard

RA ガード グローバル コンフィギュレーションを表示するには、**show ipv6 nd raguard** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 nd raguard

コマンド モード

特権 EXEC モード

例

次に、**show ipv6 nd raguard** コマンド出力の例を示します。

```
switchxxxxxx# show ipv6 nd raguard
IPv6 RA Guard is enabled on VLANs:1-4,6,7,100-120
"Managed address configuration" flag (M-flag:) off
"Other configuration" flag (O-flag): disabled
Hop Limit:
  minimum: 10
  maximum: 100
Default Router Preference:
  minimum: 1
  maximum: 1
```

show ipv6 nd raguard policy

RA ガード機能で設定したすべてのポートでルータ アドバタイズメント（RA）ガード ポリシーを表示するには、**show ipv6 nd raguard policy** コマンドを特権 EXEC モードで使用します。

構文

show ipv6 nd raguard policy [*policy-name* | **active**]

パラメータ

- ***policy-name***：任意の名前で RA ガード ポリシーを表示します。
- **active**：接続されているユーザ定義 RA ガード ポリシーを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、RA ガード機能を使用して設定されたすべてのポートでポリシー用に設定されたオプションを表示します。

例 1：次の例は、policy1 という名前のポリシーのポリシー設定を示します。

```
switchxxxxxx# show ipv6 nd raguard policy raguard1
RA Guard Policy: policy1
  device-role: router
  router address prefix list name: list1
  prefixes prefix list name: list2
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLAN
	gi1/0/1 ～ 2	1 ～ 58、68 ～ 4094
	gi1/0/3 ～ 4	1-4094
	Po1 ～ 4	1-4094

例 2：次の例は、接続されているポリシーを示します。

```
switchxxxxxx# show ipv6 nd raguard policy active
Attached to VLANs:
  Policy Name   VLANs
  vlan-default  1-4094
Attached to ports:
```

	[Policy Name]	Ports	VLAN
	port-default	gi1/0/1 ～ 4	1-4094

例 3：次の例は、ユーザ定義ポリシーを示します。

```
switchxxxxxx# show ipv6 nd raguard policy
policy1
policy2
```

show ipv6 neighbor binding

ネイバー バインディング グローバル コンフィギュレーションを表示するには、**show ipv6 neighbor binding** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 neighbor binding

コマンド モード

特権 EXEC モード

使用上のガイドライン

これにより、ネイバー バインディング グローバル コンフィギュレーションが表示されます。

例

次に、**show ipv6 neighbor binding** コマンド出力の例を示します。

```
switchxxxxxx# show ipv6 neighbor binding
Neighbor Binding Integrity is enabled on VLANs:1-4,6-7,100-120
Binding logging: disabled
Binding lifetime: 56 minutes
Address Configuration method: dhcp
Binding address prefix validation: disabled
Maximum entries
 VLAN: unlimited
 Port: 1
 MAC: 1
```

show ipv6 neighbor binding policy

ネイバー バインディング ポリシーを表示するには、**show ipv6 neighbor binding policy** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 neighbor binding policy [*policy-name* | active]

パラメータ

- ***policy-name***：ネイバー バインディング ポリシー名。
- **active**：接続されているネイバー バインディング ポリシーを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、すべてのポリシーまたは特定の 1 つのポリシーのいずれかを表示します。

例

例 1：次の例は、policy1 という名前のポリシーのポリシー設定を示します。

```
switchxxxxxx# show ipv6 neighbor binding policy policy1
Neighbor Binding Policy: policy1
  address configuration method: dhcp
  binding address prefix validation: disabled
  device-role: perimiter
  binding logging: disabled
  max-entries
   VLAN: unlimited
   Port: 10
   MAC: 2
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLAN
	gi1/0/1 ～ 2	1 ～ 58、68 ～ 4094
	gi1/0/3 ～ 4	1-4094
	Po1 ～ 4	1-4094

例 2：次の例は、接続されているポリシーを示します。

```
switchxxxxxx# show ipv6 neighbor binding policy active
Attached to VLAN:
  Policy Name     VLANs
  policy2         200-300
```

```
  vlan-default    1-199,301-4094
Attached to ports:
```

	[Policy Name]	Ports	VLAN
	policy1	gi1/0/1 ～ 4	1-100
	port-default	gi1/0/1 ～ 4	101 ～ 4094

例 3：次の例は、ユーザ定義ポリシーを示します。

```
switchxxxxxx# show ipv6 neighbor binding policy
policy1
policy2
```

show ipv6 neighbor binding prefix table

ネイバー プレフィックス テーブルのコンテンツを表示するには、**show ipv6 neighbor binding prefix table** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 neighbor binding prefix table [**vlan** *vlan-id*]

パラメータ

- **vlan** *vlan-id*：指定した VLAN と一致するプレフィックスを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドはネイバー プレフィックス テーブルを表示します。表示する出力は指定した VLANに制限できます。VLANが設定されていない場合は、すべてのプレフィックスが表示されます。

例

次に、学習したプレフィックスを表示する例を示します。

```
switchxxxxxx# show ipv6 neighbor binding prefix table
Flags: A - the prefix can be used for autoconfig (stateless configuration)
Neighbor Prefix Table has 4 entries
VLAN  Prefix         Type    Flags   Remaining Lifetime
   7  2004:1::/64   static    A
   7  2006:1::/64   dynamic              1230
   7  2008:1::/64   static
1027  2002:1::/64   dynamic   A            230
```

show ipv6 neighbor binding table

バインディング テーブルのコンテンツを表示するには、**show ipv6 neighbor binding table** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 neighbor binding table [**vlan** *vlan-id*] [**interface** *interface-id*] [**ipv6** *ipv6-address*] [**mac** *mac-address*]

パラメータ

- **vlan** *vlan-id*：指定した VLAN に一致するバインディング テーブル エントリを表示します。
- **interface** *interface-id*：指定したポート（イーサネット ポートまたはポート チャネル）に一致するバインディング テーブル エントリを表示します。
- **ipv6** *ipv6-address*：指定した IPv6 アドレスに一致するバインディング テーブル エントリを表示します。
- **mac** *mac-address*：指定した MAC アドレスに一致するバインディング テーブル エントリを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

これにより、バインディングテーブルのコンテンツが表示されます。表示出力は、指定された VLAN、ポート、IPv6 アドレス、または MAC アドレスで指定できます。キーワードまたは引数が入力されていない場合は、すべてのバインディングテーブルコンテンツが表示されます。

すべてのキーワードと引数の組み合わせを使用できます。

例

次に、バインディング テーブルのコンテンツを表示する例を示します。

```
switchxxxxxx# show ipv6 neighbor binding table
Binding Table has 4 entries
```

VLAN	IPv6 address	Inter	MAC address	Origin	State	Expir	TCAM
-----	----------	-------	--------------	------	-----	Time	Ovrfl
100	2001:300::1	gi1/0/1	AABB.CC01.F500	NDP	VALID	------	-----
100	2001:600::1	gi1/0/1	AABB.CC01.AAAA AABB.CC01.F110	NDP NDP	TENT	559	*
100	2001:100::2	gi1/0/2	AABB.CC01.F160	NDP	VALID	96	
200	2001:200::3	gi1/0/2			VALID	79	

```
Field Descriptions:
```

- **VLAN**：ホストが属する VLAN。
- **IPv6 address**：ホストの IPv6 アドレス。
- **Inter**：ホストが接続されているポート。
- **MAC address**：ホストの MAC アドレス。
- **Origin**：IPv6 アドレスが追加されたプロトコル。
- **Static**：**ipv6 neighbor binding static** コマンドで手動で定義された静的 IPv6 アドレス。
- **NDP**：NDP プロトコルメッセージから学習した IPv6 アドレス。
- **DHCP**：DHCPv6 プロトコルメッセージから学習した IPv6 アドレス。
- **State**：エントリの状態
- **TENT**：新しいホスト IPv6 アドレスは検証中です。有効期間が 1 秒未満のため、有効期間は表示されません。
- **VALID**：ホスト IPv6 アドレスがバインドされています。
- **Expir. Time**：確認されない場合、エントリが削除されるまでの残り時間（秒単位）。
- **TCAM Ovrflw**：TCAM がオーバーフローしているため、「*」がマークされたエントリは TCAM に追加されていません。

show ipv6 source guard

IPv6 ソース ガード グローバル コンフィギュレーションを表示するには、**show ipv6 source guard** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 source guard

パラメータ

該当なし

コマンド モード

特権 EXEC モード

使用上のガイドライン

これにより、IPv6 ソース ガード グローバル コンフィギュレーションが表示されます。

例

次に、**show ipv6 source guard** コマンド出力の例を示します。

```
switchxxxxxx# show ipv6 source guard
IPv6 Source Guard is enabled on VLANs:1-4,6,7,100-120
```

show ipv6 source guard policy

IPv6 ソース ガード ポリシーを表示するには、**show ipv6 source guard policy** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 source guard policy [*policy-name* | active]

パラメータ

- ***policy-name***：IPv6 ソース ガード ポリシー名。
- **active**：接続されている IPv6 ソース ガード ポリシーを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、設定したすべての IPv6 ソース ガード ポリシー、接続している特定の 1 つまたはすべての IPv6 ソース ガード ポリシーを表示します。

例 1：次の例は、policy1 という名前のポリシーのポリシー設定を示します。

```
switchxxxxxx# show ipv6 source guard policy policy1
Neighbor Binding Policy: policy1
  trusted port: disabled
  Attached to ports:
   Ports
   gi1/0/1-2
   gi1/0/4
   Po1-4
```

例 2：次の例は、接続されているポリシーを示します。

```
switchxxxxxx# show ipv6 source guard policy active
Attached to VLAN:
Attached to ports:
```

	[Policy Name]	Ports
	policy1	gi1/0/1 ～ 2
	port-default	gi1/0/1 ～ 2
		gi1/0/3

例 3：次の例は、ユーザ定義ポリシーを示します。

```
switchxxxxxx# show ipv6 source guard policy
policy1
policy2
```

trusted-port（IPv6 Source Guard）

IPv6 ソース ガード ポリシー内の信頼されたポートとしてポートを設定するには、**trusted-port** コマンドを IPv6 ソース ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

trusted-port

no trusted-port

デフォルト設定

信頼されていません。

コマンド モード

IPv6 ソース ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

信頼できるポートからブリッジされた IPv6 データ メッセージは IPv6 ソース ガードによって検証されません。

例

次の例では、ポートを信頼済みに定義するポリシーを定義します。

```
switchxxxxxx(config)# ipv6 ipv6 source guard policy policy1
switchxxxxxx(config-ipv6-srcguard)# trusted-port
switchxxxxxx(config-ipv6-srcguard)# exit
```

validate source-mac

IPv6 ND インスペクション ポリシー内のリンク層アドレスに対する MAC アドレスのチェックを有効にするには、**validate source-mac** コマンドを ND インスペクション ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

validate source-mac [enable | disable]

no validate source-mac

パラメータ

- **enable**：リンク層アドレスに対する MAC アドレスの検証を有効にします。キーワードが設定されていない場合、デフォルトでこのキーワードが適用されます。
- **disable**：リンク層アドレスに対する MAC アドレスの検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

ND インスペクション ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

例

次の例では、NDP メッセージのリンク層アドレスが MAC アドレスと一致しない場合にルータがこのメッセージをドロップできます。

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# validate source-mac
switchxxxxxx(config-nd-inspection)# exit
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。