



IPv6 のユニキャストリバースパス転送

IPv6 のユニキャストリバースパス転送機能により、IPv6 デバイスを経由する不正形式または偽造（スプーフィング）IPv6 送信元アドレスを原因とする問題が軽減されます。

- 機能情報の確認, 1 ページ
- IPv6 のユニキャストリバースパス転送の前提条件, 1 ページ
- IPv6 のユニキャストリバースパス転送について, 2 ページ
- IPv6 のユニキャストリバースパス転送の設定方法, 3 ページ
- IPv6 のユニキャストリバースパス転送の設定例, 5 ページ
- その他の関連資料, 5 ページ
- IPv6 のユニキャストリバースパス転送の機能情報, 6 ページ

機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェアリリースに対応したリリースノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IPv6 のユニキャストリバースパス転送の前提条件

- ユニキャストリバースパス転送 (uRPF) を使用するには、ルータでシスコエクスプレス フォワーディングスイッチングまたは分散型シスコエクスプレス フォワーディングスイッ

■ IPv6 のユニキャストリバースパス転送について

チングをイネーブルにします。シスコエクスプレスフォワーディングスイッチングの入力インターフェイスを設定する必要はありません。シスコエクスプレスフォワーディングがデバイス上で実行されているかぎり、個々のインターフェイスは他のスイッチングモードで設定できます。

- uRPF が機能するためには、デバイスでシスコエクスプレスフォワーディングがグローバルに設定されている必要があります。uRPF は、シスコエクスプレスフォワーディングがないと動作しません。
- uRPF は、ネットワーク内部のインターフェイスでは使用できません。内部インターフェイスは、ルーティングを非対称にする可能性が高く、パケットの送信元へのルートが複数存在する場合が多いからです。uRPF は、元々対称であるか、対称に設定されている場合にだけ適用してください。

たとえば、ISP のネットワークのエッジにあるデバイスは、ISP ネットワークのコアにあるデバイスよりも対称リバースパスを持つ可能性が高くなります。ISP ネットワークのコアにあるデバイスでは、デバイスからの最良の転送パスがデバイスへ返されるパケットに対して選択されるパスとなることが保証されません。したがって、非対称ルーティングの可能性がある uRPF の適用は推奨されません。ネットワークのエッジにだけ、または ISP の場合はネットワークのカスタマー エッジにだけ uRPF を配置します。

IPv6 のユニキャストリバースパス転送について

ユニキャストリバースパス転送

IPv6 のユニキャストリバースパス転送機能を使用すると、IPv6 デバイスを経由する不正形式またはスプーフィング IPv6 送信元アドレスを原因とする問題が軽減されます。不正形式または偽造送信元アドレスは、送信元 IPv6 アドレススプーフィングに基づくサービス拒絶 (DoS) 攻撃を示すことがあります。

インターフェイスで uRPF がイネーブルになっている場合、デバイスはそのインターフェイスで受信したすべてのパケットを調べます。デバイスは、送信元アドレスがルーティングテーブルにあり、パケットが受信されるインターフェイスと一致するか確認します。この「後方参照」機能を使用できるのは、シスコエクスプレスフォワーディングがデバイスでイネーブルにされている場合のみです。これは、ルックアップが転送情報ベース (FIB) の存在に依存しているためです。シスコエクスプレスフォワーディングでは、その動作の一部として FIB が生成されます。



(注)

uRPF は入力機能であり、接続のアップストリーム エンドのデバイスの入力インターフェイスだけに適用されます。

uRPF 機能では、デバイスインターフェイスで受信されたパケットが、パケットの送信元への最もリターンパスの 1 つで着信するかどうかが検証されます。この機能では、シスコエクスプレスフォワーディングテーブルのリバースルックアップが実行されます。uRPF がパケットのリバースパスを見つけることができない場合、uRPF は、アクセスコントロールリスト (ACL) が

指定されているかどうかに応じてパケットをドロップまたは転送できます。ACLが指定されている場合は、パケットがuRPFチェックに失敗した場合にだけ、パケットが（ACLのdenyステートメントを使用して）ドロップされる必要があるか、（ACLのpermitステートメントを使用して）転送される必要があるかを確認するためにACLがチェックされます。パケットがドロップされるか転送されるかにかかわらず、パケットは、uRPFドロップのグローバルIPトラフィック統計情報とuRPFのインターフェイス統計情報でカウントされます。

ACLが指定されていない場合、デバイスは偽造または不正形式のパケットを即時にドロップし、ACLロギングは行われません。デバイスおよびインターフェイスuRPFカウンタが更新されます。

uRPFイベントは、ACLエントリのロギングオプションを指定することでロギングできます。ログ情報を使用して、送信元アドレスや時間など、攻撃に関する情報を収集できます。



(注)

uRPFでは、コストが等しいすべての「最良」リターンパスが有効と見なされます。複数のリターンパスが存在していても、各パスのルーティングコスト（ホップ数や加重など）が他のパスと等しく、そのルートがFIB内にあるかぎり、uRPFは機能します。

IPv6 のユニキャストリバースパス転送の設定方法

ユニキャストRPFの設定

はじめる前に

uRPFを使用するには、デバイスでシスコエクスプレスフォワーディングスイッチングまたは分散型シスコエクスプレスフォワーディングスイッチングをイネーブルにします。シスコエクスプレスフォワーディングスイッチングの入力インターフェイスを設定する必要はありません。シスコエクスプレスフォワーディングがデバイス上で実行されているかぎり、個々のインターフェイスは他のスイッチングモードで設定できます。



(注)

デバイスでシスコエクスプレスフォワーディングがグローバルに設定されている必要があります。uRPFは、シスコエクスプレスフォワーディングがないと動作しません。



(注)

uRPF は、ネットワーク内部のインターフェイスでは使用できません。内部インターフェイスは、ルーティングを非対称にする可能性が高く、パケットの送信元へのルートが複数存在する場合が多いからです。uRPF は、元々対称であるか、対称に設定されている場合にだけ適用してください。

たとえば、ISP のネットワークのエッジにあるデバイスは、ISP ネットワークのコアにあるデバイスよりも対称リバースパスを持つ可能性が高くなります。ISP ネットワークのコアにあるデバイスでは、デバイスからの最良の転送パスがデバイスへ返されるパケットに対して選択されるパスとなることが保証されません。したがって、非対称ルーティングの可能性がある uRPF の適用は推奨されません。ネットワークのエッジにだけ、または ISP の場合はネットワークのカスタマー エッジにだけユニキャスト uRPF を配置するのが最も単純です。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **ipv6 verify unicast source reachable-via {rx | any} [allow-default] [allow-self-ping] [access-list-name]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 3	interface type number 例： Device(config)# interface gigabitethernet 0/0/0	インターフェイスのタイプと番号を指定し、デバイスをインターフェイスコンフィギュレーションモードにします。
ステップ 4	ipv6 verify unicast source reachable-via {rx any} [allow-default] [allow-self-ping] [access-list-name]	送信元アドレスが FIB テーブルに存在していることを確認し、uRPF をイネーブルにします。

コマンドまたはアクション	目的
<p>例：</p> <pre>Device(config-if)# ipv6 verify unicast source reachable-via any</pre>	

IPv6 のユニキャストリバースパス転送の設定例

例：IPv6 のユニキャストリバースパス転送の設定

```
Device# show ipv6 traffic
IPv6 statistics:
Rcvd: 0 total, 0 local destination
      0 source-routed, 0 truncated
      0 format errors, 0 hop count exceeded
      0 bad header, 0 unknown option, 0 bad source
      0 unknown protocol, 0 not a router
      0 fragments, 0 total reassembled
      0 reassembly timeouts, 0 reassembly failures
      0 unicast RPF drop, 0 suppressed RPF drop
Sent: 0 generated, 0 forwarded
      0 fragmented into 0 fragments, 0 failed
      0 encapsulation failed, 0 no route, 0 too big
```

その他の関連資料

関連資料

関連項目	参照先
IPv6 のアドレッシングと接続	『 <i>IPv6 Configuration Guide</i> 』
IPv4 スイッチングの設定	『 <i>IP Switching Cisco Express Forwarding Configuration Guide</i> 』
Cisco IOS コマンド	『 <i>Cisco IOS Master Commands List, All Releases</i> 』
IPv6 コマンド	『 <i>Cisco IOS IPv6 Command Reference</i> 』

関連項目	参照先
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	『IPv6 RFCs』

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカルサポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンラインリソースを提供しています。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 のユニキャストリバースパス転送の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェアリリーストレインで各機能のサポートが導入されたときのソフトウェアリリースだけを

示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 1: IPv6 のユニキャストリバースパス転送の機能情報

機能名	リリース	機能情報
IPv6 のユニキャストリバースパス転送	12.2(50)SY Cisco IOS XE Release 2.1	uRPF 機能を使用すると、IPv6 デバイスを経由する不正形式またはスプーフィング IPv6 送信元アドレスを原因とする問題が軽減されます。不正な形式の送信元アドレスまたは偽装された送信元アドレスは、送信元 IPv6 アドレスのスプーフィングに基づく DoS 攻撃である場合があります。 ipv6 verify unicast source reachable-via 、 show ipv6 traffic の各コマンドが追加または変更されています。

