



ユニキャスト RPF の設定

この章では、Cisco NX-OS デバイスで unicast reverse path forwarding (uRPF) を設定する方法を説明します。

この章は、次の項で構成されています。

- [ユニキャスト RPF について, on page 1](#)
- [ユニキャスト RPF の注意事項と制約事項 \(3 ページ\)](#)
- [ユニキャスト RPF のデフォルト設定, on page 6](#)
- [-R ラインカードを搭載した Cisco Nexus 9500 スイッチのユニキャスト RPF の設定, on page 6](#)
- [Cisco Nexus 9300 スイッチのユニキャスト RPF の設定 \(7 ページ\)](#)
- [ユニキャスト RPF の設定例, on page 10](#)
- [ユニキャスト RPF の設定の確認, on page 11](#)
- [ユニキャスト RPF に関する追加情報, on page 12](#)

ユニキャスト RPF について

ユニキャスト RPF 機能を使用すると、ネットワークに変形または偽造（スプーフィング）された IPv4 または IPv6 ソースアドレスが注入されて引き起こされる問題を、裏付けのない IPv4 または IPv6 パケットを廃棄する方法により緩和します。たとえば、Smurf や Tribal Flood Network (TFN) など、いくつかの一般的なサービス拒絶 (DoS) 攻撃は、偽造の送信元 IPv4 または IPv6 アドレスやすぐに変更される送信元 IPv4 または IPv6 アドレスを利用して、攻撃を突き止めたりフィルタリングしたりする手段を妨ぐことができます。ユニキャスト RPF では、送信元アドレスが有効で IP ルーティングテーブルと一致するパケットだけを転送することにより、攻撃を回避します。

インターフェイス上でユニキャスト RPF を有効にすると、スイッチはそのインターフェイス上で受信されたすべての入力パケットを検証することにより、送信元アドレスと発信元インターフェイスがルーティングテーブル内に現れ、しかもパケット受信場所のインターフェイスと一致することを確認します。この送信元アドレス検査は転送情報ベース (FIB) に依存しています。



Note ユニキャスト RPF は入力機能であり、接続のアップストリーム エンドにあるスイッチの入力インターフェイスにのみ適用されます。

ユニキャスト RPF は、FIB のリバースルックアップを実行することにより、スイッチインターフェイスでの受信パケットがそのパケットの送信元への最良リターンパス（リターンルート）で着信していることを確認します。パケットが最適なリバースパスルートのいずれかから受信された場合、パケットは通常どおりに転送されます。パケットを受信したインターフェイス上にリバースパスルートがない場合、攻撃者によって送信元アドレスが変更される可能性があります。ユニキャスト RPF がそのパケットのリバースパスを見つけられない場合は、パケットはドロップされます。



Note ユニキャスト RPF 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。つまり、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（ホップカウントや重みなど）が他のパスと等しく、そのルートが FIB 内にある限り、ユニキャスト RPF は機能します。ユニキャスト RPF は、Enhanced Interior Gateway Routing Protocol (EIGRP) バリエーションが使用されていて、送信元 IP アドレスに戻る同等でない候補パスが存在する場合にも機能します。

ユニキャスト RPF プロセス

ユニキャスト RPF には、キーの実装原則がいくつかあります。

- パケットは、パケットの送信元に対する最適なリターンパス（ルート）があるインターフェイスで受信される必要があります（このプロセスは対称ルーティングと呼ばれます）。FIB に受信インターフェイスへのルートと一致するルートが存在する必要があります。スタティックルート、ネットワーク文、ダイナミックルーティングによって FIB にルートが追加されます。
- 受信側インターフェイスでの IP 送信元アドレスは、そのインターフェイスのルーティングエントリと一致する必要があります。
- ユニキャスト RPF 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。

ダウンストリームネットワークにインターネットへの他の接続があっても、ダウンストリームネットワークにユニキャスト RPF を使用できます。



Caution 攻撃者が送信元アドレスへの最良パスを変更する可能性があるため、加重やローカルプリファレンスなどのオプションの BGP 属性を使用する際には、十分に注意してください。変更によって、ユニキャスト RPF の操作に影響が出ます。

ユニキャスト RPF と ACL を設定したインターフェイスでパケットが受信されると、Cisco NX-OS ソフトウェアは次の動作を行います。

1. インバウンドインターフェイスで入力 ACL をチェックします。
2. ユニキャスト RPF を使用し、FIB テーブル内のリバースルックアップを実行することにより、そのパケットが送信元への最良リターンパスで着信したことを確認します。
3. パケットの転送を目的として FIB ルックアップを実行します。
4. アウトバウンドインターフェイスで出力 ACL をチェックします。
5. パケットを転送します。

ユニキャスト RPF の注意事項と制約事項

ユニキャスト RPF (uRPF) に関する注意事項と制約事項は次のとおりです。

- uRPF は、次のプラットフォームでサポートされています。
 - N9K-X9636C-R と N9K-X9636Q-R ラインカード搭載の Cisco Nexus 9500 シリーズ スイッチ
 - N9K-X9636C-RX ラインカード搭載の Cisco Nexus 9500 シリーズ スイッチ
 - Cisco Nexus 9300 プラットフォーム スイッチ (9300-FXP スイッチを除く)
- Cisco NX-OS リリース 10.1(2) 以降、uRPF は次でサポートされます。
 - Cisco Nexus 9300-GX/GX2 シリーズ スイッチおよび FX ラインカードを備えた Cisco Nexus 9500 シリーズ スイッチ (IPv4 および IPv6 用)
 - EX ラインカードを搭載した Cisco Nexus 9500 シリーズ スイッチ
 - vPC をサポートする ToR および EoR スイッチ
- Cisco NX-OS リリース 9.2(1) 以降、uRPF は次でサポートされます。
 - Cisco Nexus 9300-EX シリーズ スイッチ (IPv4 のみ)
 - Cisco Nexus 9300-FX/FX2 シリーズ スイッチ (IPv4 および IPv6)
- Cisco NX-OS リリース 9.3(5) 以降、uRPF は Cisco Nexus 9300-FX3 プラットフォーム スイッチ (IPv4 および IPv6) でサポートされます。
- Cisco Nexus リリース 9.3(1) 以降、uRPF はモジュラ EX/FX ラインカードファミリの Cisco Nexus 9500 シリーズ スイッチでサポートされています (『[Cisco Nexus 9500 Cloud-Scale Line Cards and Fabric Modules Data Sheet](#)』を参照)。



(注) モジュラ EX/FX ラインカードの uRPF は、DUAL STACK MCAST ルーティングモードでのみサポートされます。uRPF をイネーブルにする前に、`system routing template-dual-stack-mcast` の設定を指定します。DUAL STACK MCAST ルーティングモードの設定方法については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

Cisco NX-OS リリース 10.1(2) 以降、モジュラ EX/FX ラインカードの uRPF はデフォルトルーティングモードでもサポートされません。

- uRPF は、ネットワーク内のより大きな部分からのダウンストリームのインターフェイスで適用する必要があります（ネットワークのエッジに適用するのが望ましい）。
- なるべくダウンストリームで uRPF を適用する方が、アドレススプーフィングの軽減やスプーフされたアドレスの送信元の特定の精度が高くなります。たとえば、集約デバイスで uRPF を適用すると、多くのダウンストリーム ネットワークまたはクライアントからの攻撃を軽減できるとともに、管理が簡単になりますが、攻撃の送信元は特定できません。ネットワーク アクセス サーバに uRPF を適用すると、攻撃の範囲を絞り、攻撃元を追跡しやすくなります。ただし、多数のサイトにユニキャスト RPF を展開すると、ネットワーク運用の管理コストが増加します。
- インターネット、イントラネット、およびエクストラネットのリソースにわたって uRPF を展開するエンティティ数が増えるほど、インターネットコミュニティ全体の大規模なネットワークの中断を軽減できる可能性と、攻撃元を追跡できる可能性が高くなります。
- uRPF は、総称ルーティング カプセル化 (GRE) トンネルのようなトンネルでカプセル化された IP パケットは検査しません。トンネリングとカプセル化のレイヤがパケットから除かれてから uRPF がネットワーク トラフィックを処理するように、ホーム ゲートウェイに uRPF を設定する必要があります。
- uRPF は、ネットワークからのアクセス ポイントが 1 つだけ、またはアップストリーム接続が 1 つだけの「単一ホーム」環境で使用できます。アクセス ポイントが 1 つのネットワークは対称ルーティングを提供します。これはつまり、パケットがネットワークに入るインターフェイスはその IP パケットの送信元への最良のリターンパスでもあるということです。
- uRPF は、ネットワーク内部のインターフェイスに使用しないでください。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あります。uRPF を設定するのは、元々対称であるか、対称に設定されている場合だけにしてください。
- uRPF を使用すると、送信元が 0.0.0.0 で宛先が 255.255.255.255 のパケットを通過させて、ブートストラッププロトコル (BOOTP) と Dynamic Host Configuration Protocol (DHCP) を正しく動作させることができます。

- uRPF が有効な場合、スイッチがインストールできる null0 へのスタティック ルートの量は、「show hardware internal forwarding table utilization」の「Max V4 Ucast DA TCAM table entries」の値に制限されます。
- Cisco NX-OS リリース 9.2(1) 以降、N9K-X9636C-R および N9K-X96136YC-R スイッチでは、使用可能な IPv4 および IPv6 ユニキャスト RPF コマンドのバージョンは 1 つだけです。ただし、これにより、IPv4 と IPv6 の両方でユニキャスト RPF が有効になります。
- 次のガイドラインと制限は、N9K-X9636C-R、N9K-X9636C-RX、または N9K-X9636Q-R ラインカードを搭載した Cisco Nexus 9500 シリーズ スイッチにのみ適用されます。
 - 厳密な uRPF を機能させるには、入力インターフェイスと送信元 IP アドレスが学習されたインターフェイスで有効にします。
 - スイッチ ハードウェアは、設定されたルーティング インターフェイスごとに厳密な uRPF を実装しません。
 - 厳密な uRPF は、厳密な uRPF 対応インターフェイスの学習ルートごとに実装されます。
 - ルートが ECMP として解決されると、strict uRPF はルーズモードにフォールバックします。
 - トラップ解決に関するハードウェアの制限により、uRPF はインバンド経由でスーパーバイザ宛パケットに適用されない場合があります。
 - IP トラフィックの場合は、IPv4 と IPv6 の設定を同時に有効にします。
 - ハードウェアの制限により、N9K-X9636C-R、N9K-X9636C-RX、および N9K-X9636Q-R ラインカードは次の組み合わせのみをサポートします。

uRPF の設定		送信元 IP アドレスのトラフィックチェックの適用			
IPv4	IPv6	IP Unipath	IP ECMP	MPLS Encap/VPN/ECMP	N9K-X9636C-RX ラインカードの Unipath MPLS VPN
無効	無効	許可	許可	許可	許可
Loose	Loose	uRPF loose	uRPF loose	uRPF loose	uRPF strict
Strict	Strict	uRPF strict	uRPF loose	uRPF loose	uRPF strict

- Strict uRPF は、宛先インターフェイスが次の Cisco NX-OS デバイスの ICMPv6 NA パケットを受信した場合でも、ICMPv6 NA パケットを廃棄します。
 - ラインカード : N9K-X9564PX、N9K-X9564TX、N9K-X9536PQ、X9408PC-CFP2、X9464TX、X9464TX2
 - アップリンク モジュール : N9K-M12PQ

- スイッチ : 93128TX、9396PX、9396TX、9372PX、9372PX-E、3164Q、31128PQ
- Strict uRPF は、次のプラットフォームの VxLAN 経由でインターフェイスに送信される ICMP トラフィックをブロックします。
 - Cisco Nexus 9200 プラットフォーム スイッチ
 - Cisco Nexus 9300--EX/FX/GX プラットフォーム スイッチ
 - N9K-X9700-EX および N9K-X9700-FX ライン カードを搭載した Nexus 9500 スイッチ
- Strict uRPF が構成されている場合は、サブネットの背後にある未解決のホストに対して urpf strict モードが機能するように、次のコマンドを追加します。
 - **no system multicast dcs-check**
 - **hardware profile multicast max-limit lpm-entries 0**

ユニキャスト RPF のデフォルト設定

次の表に、ユニキャスト RPF パラメータのデフォルト設定を示します。

Table 1: ユニキャスト RPF パラメータのデフォルト設定

パラメータ	デフォルト
ユニキャスト RPF	ディセーブル

-R ラインカードを搭載した Cisco Nexus 9500 スイッチのユニキャスト RPF の設定

-R ラインカードを使用して Cisco Nexus 9500 シリーズ スイッチの入力インターフェイスにユニキャスト RPF を設定できます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	グローバル設定モードを開始します。

	Command or Action	Purpose
ステップ 2	interface ethernet slot/port Example: switch(config)# interface ethernet 2/3 switch(config-if)#	インターフェイス設定モードを開始します。
ステップ 3	{ip ipv6} address ip-address/length Example: switch(config-if)# ip address 172.23.231.240/23	インターフェイスの IPv4 または IPv6 アドレスを指定します。
ステップ 4	{ip ipv6} verify unicast source reachable-via any Example: switch(config-if)# ip verify unicast source reachable-via any	IPv4 と IPv6 の両方に対するインターフェイスでユニキャスト RPF を設定します。 Note IPv4 または IPv6 の uRPF をイネーブルにすると (ip または ipv6 キーワードを使用)、uRPF は IPv4 と IPv6 の両方でイネーブルになります。
ステップ 5	(Optional) show ip interface ethernet slot/port Example: switch(config)# show ip interface ethernet 2/3	インターフェイスの IP 情報を表示します。
ステップ 6	(Optional) show running-config interface ethernet slot/port Example: switch(config)# show running-config interface ethernet 2/3	実行コンフィギュレーション内のインターフェイスの情報を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

Cisco Nexus 9300 スイッチのユニキャスト RPF の設定

Cisco NX-OS リリース 9.2(1) 以降を実行する Cisco Nexus 9300 プラットフォーム スイッチ (9300-FXP スイッチを除く) の入力インターフェイスで、次のいずれかのユニキャスト RPF モードを設定できます。

ストリクト ユニキャスト RPF モード

厳格モードでは、ユニキャスト RPF が FIB で一致するパケット送信元アドレスを見つけて、パケットを受信した入力インターフェイスが FIB 内のユニキャスト RPF インターフェイスのいずれかと一致した場合に、チェックに合格します。チェックに合格しないと、パケットは廃棄されます。このタイプのユニキャスト RPF チェックは、パケットフローが対称であると予想される場合に使用できます。

ルーズ ユニキャスト RPF モード

緩和モードでは、FIB でのパケット送信元アドレスのルックアップで一致が戻り、FIB の結果からその送信元が少なくとも1つの実インターフェイスで到達可能であることが示された場合に、チェックに合格します。パケットを受信した入力インターフェイスが FIB 内のインターフェイスのいずれかと一致する必要はありません。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] system urpf disable 例： switch(config)# no system urpf disable	スイッチでユニキャスト RPF を有効にします。 (注) ユニキャスト RPF 設定を適用するには、Cisco NX-OS ボックスをリロードする必要があります。
ステップ 3	interface ethernet slot/port 例： switch(config)# interface ethernet 2/3 switch(config-if)#	イーサネット インターフェイスを指定し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 4	{ip ipv6} address ip-address/length 例： switch(config-if)# ip address 172.23.231.240/23	インターフェイスの IPv4 または IPv6 アドレスを指定します。
ステップ 5	{ip ipv6} verify unicast source reachable-via {any [allow-default] rx} 例： switch(config-if)# ip verify unicast source reachable-via any	IPv4 および IPv6 用インターフェイスにユニキャスト RPF を設定します。 Cisco Nexus 9300-EX シリーズ スイッチ (IPv4 用) と Cisco Nexus 9300-FX/FX2 シリーズ スイッチでは、IPv4 および IPv6 uRPF を個別に有効にできます。

	コマンドまたはアクション	目的
		<p>(注) IPv4 または IPv6 のユニキャスト RPF を有効にすると (ip または ipv6 キーワードを使用)、ユニキャスト RPF は IPv4 と IPv6 の両方で有効になります。</p> <p>インターフェイスで使用できる IPv4 および IPv6 ユニキャスト RPF コマンドのバージョンは 1 つだけです。1 つのバージョンを設定する場合、すべてのモード変更はこのバージョンで行う必要があります、他のすべてのバージョンはそのインターフェイスによってブロックされます。</p> <ul style="list-style-type: none"> • any キーワードは緩和モードのユニキャスト RPF を指定します。 • allow-default キーワードを指定すると、送信元アドレスのルックアップでデフォルト ルートと一致させることが可能であり、これを検証に使用できます。 <p>(注) allow-default キーワードは、ALPM ルーティングモードでは適用されません。</p> <p>(注) allow-default キーワードを指定しない場合、送信元アドレス ルックアップ (ルーズなユニキャスト RPF チェックの場合) はデフォルト ルートと一致しません。</p> <ul style="list-style-type: none"> • rx キーワードは厳格モードのユニキャスト RPF を指定します。

	コマンドまたはアクション	目的
ステップ 6	exit 例： switch(config-if)# exit switch(config)#	インターフェイスコンフィギュレーションモードを終了します。
ステップ 7	(任意) show ip interface ethernet slot/port 例： switch(config)# show ip interface ethernet 1/54 grep -i "unicast reverse path forwarding" IP unicast reverse path forwarding: none	インターフェイスの IP 情報を表示し、ユニキャスト RPF が有効かどうかを確認します。
ステップ 8	(任意) show running-config interface ethernet slot/port 例： switch(config)# show running-config interface ethernet 2/3	実行コンフィギュレーション内のインターフェイスの情報を表示します。
ステップ 9	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

ユニキャスト RPF の設定例

次に、-R ラインカードを搭載した Cisco Nexus 9500 シリーズスイッチで IPv4 パケットの loose ユニキャスト RPF を設定する例を示します。

```
interface Ethernet2/3
 ip address 172.23.231.240/23
 ip verify unicast source reachable-via any
```

次に、-R ラインカードを搭載した Cisco Nexus 9500 シリーズスイッチで IPv6 パケットの loose ユニキャスト RPF を設定する例を示します。

```
interface Ethernet2/1
 ipv6 address 2001:0DB8:c18:1::3/64
 ipv6 verify unicast source reachable-via any
```

次に、Cisco Nexus 9300 プラットフォームスイッチで IPv4 パケットの loose ユニキャスト RPF を設定する例を示します。

```
no system urpf disable
interface Ethernet2/3
 ip address 172.23.231.240/23
```

```
ip verify unicast source reachable-via any
```

次に、Cisco Nexus 9300 プラットフォーム スイッチで IPv6 パケットの loose ユニキャスト RPF を設定する例を示します。

```
no system urpf disable
interface Ethernet2/1
  ipv6 address 2001:0DB8:c18:1::3/64
  ipv6 verify unicast source reachable-via any
```

次に、Cisco Nexus 9300 プラットフォーム スイッチで IPv4 パケットの strict ユニキャスト RPF を設定する例を示します。

```
no system urpf disable
interface Ethernet2/2
  ip address 172.23.231.240/23
  ip verify unicast source reachable-via rx
```

次に、Cisco Nexus 9300 プラットフォーム スイッチで IPv6 パケットの strict ユニキャスト RPF を設定する例を示します。

```
no system urpf disable
interface Ethernet2/4
  ipv6 address 2001:0DB8:c18:1::3/64
  ipv6 verify unicast source reachable-via rx
```

ユニキャスト RPF の設定の確認

ユニキャスト RPF の設定情報を表示するには、次のいずれかの操作を行います。

コマンド	目的
show running-config interface ethernet <i>slot/port</i>	実行コンフィギュレーション内のインターフェイスの設定を表示します。
show running-config ip [all]	実行コンフィギュレーション内の IPv4 設定を表示します。
show running-config ipv6 [all]	実行コンフィギュレーション内の IPv6 設定を表示します。
show startup-config interface ethernet <i>slot/port</i>	スタートアップ コンフィギュレーション内のインターフェイスの設定を表示します。
show startup-config ip	スタートアップ コンフィギュレーション内の IP 設定を表示します。

ユニキャスト RPF に関する追加情報

ここでは、ユニキャスト RPF の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアルタイトル
データ管理エンジン (DME) コマンド	Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference (Cisco Nexus 3000 および 9000 シリーズ NX-API REST SDK ユーザガイドと API リファレンス)
MPLS VPN	Cisco Nexus 9000 シリーズ NX-OS レイヤ 2 スイッチング コンフィギュレーションガイド (Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide)

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。