



URPF について

偽装した IP アドレスを使用し（この手口は IP アドレス スプーフィングと呼ばれます）、サービス プロバイダーによる検出を回避するために送信元 IP アドレスを頻繁に変更することは、DoS 攻撃を計画するハッカーの常套手段となっています。

Unicast Reverse Path Forwarding (URPF) は、ルータで受信されたパケットの送信元 IP アドレスを検証するためのメカニズムです。URPF を設定されたルータは、FIB テーブルでリバースパス ルックアップを実行して、送信元 IP アドレスの存在を確認します。送信元 IP アドレスがテーブルにリストされていれば、送信元は到達可能かつ有効です。送信元 IP アドレスが FIB テーブルにない場合、パケットはルータによって悪意のあるものとして扱われ、廃棄されます。

ルータでは、ルーズモードでの URPF の使用がサポートされています。URPF ルーズモードは、ルータが FIB 内の送信元 IP アドレスのプレフィックスのみを検証し、パケットがルータに到達するために使用するインターフェイスは検証しないように設定されている場合に有効となっています。ルーズモードを設定することで、代替インターフェイスを使用してルータに到達する正当なトラフィックが悪意のあるものと誤解されることがなくなります。URPF ルーズモードは、マルチホーム プロバイダー エッジ ネットワークで非常に役立ちます。

- [URPF ルーズモードの設定 \(1 ページ\)](#)

URPF ルーズモードの設定

ここでは、IPv4 と IPv6 の両方のネットワークに対し、ルータに URPF ルーズモードを設定する方法について説明します。

はじめる前に

ルータに URPF ルーズモードを設定する前に、ここで説明するように、ラインカードのデフォルト スケールを無効にする必要があります。



- (注) IPv6 uRPF 設定では、すべてのタイプのカード（TCAM カードと非 TCAM カードの両方）に対し、**hw-module fib ipv6 scale internet-optimized-disable** コマンドが必要です。デフォルトでは、IPv6 はプレフィックスに内部メモリを使用します。したがって、**hw-module fib ipv6 scale internet-optimized-disable** コマンドを設定してから、ラインカードをリロードする必要があります。



- (注) ライン カードは、デフォルト スケールを無効にした後でリロードする必要があります。このようにするのは、**hw-module** コマンドの設定がすぐに有効になるようにするためです。

すべてのタイプの非 TCAM ライン カードの場合：

```
RP/0/RP0/cpu 0: router(config)# hw-module fib ipv4 scale host-optimized-disable
RP/0/RP0/cpu 0: router(config)# hw-module fib ipv6 scale internet-optimized-disable
RP/0/RP0/cpu 0: router(config)# commit
RP/0/RP0/cpu 0: router(config)# end
RP/0/RP0/cpu 0: router# reload location all
Proceed with reload? [confirm]
```

設定

ルータに URPF ルーズ モードを設定するには、次の設定を使用します。



- (注) URPF を動作させるには、（この項で説明するとおり）IPv4 コマンドと IPv6 コマンドの両方を設定する必要があります。

```
RP/0/RP0/cpu 0: router(config)# interface bundle-ether1
RP/0/RP0/cpu 0: router(config-if)# ipv4 address 10.0.0.1 255.255.255.0
RP/0/RP0/cpu 0: router(config-if)# ipv4 verify unicast source reachable-via any
RP/0/RP0/cpu 0: router(config-if)# ipv6 address 2001::1/64
RP/0/RP0/cpu 0: router(config-if)# ipv6 verify unicast source reachable-via any
RP/0/RP0/cpu 0: router(config-if)# commit
```

実行コンフィギュレーション

次のように設定されていることを確認します。

```
RP/0/RP0/cpu 0: router(config-if)# show running-config
Thu Jul 27 14:40:38.167 IST
...
!
interface Bundle-Ether1
  ipv4 address 10.0.0.1 255.255.255.0
  ipv4 verify unicast source reachable-via any
  ipv6 address 2001::1/64
  ipv6 verify unicast source reachable-via any
!
```

これで、ルータに URPF ルーズ モードが正常に設定されました。

