CHAPTER 29

ユニキャスト RPF の設定

この章では、ユニキャスト Reverse Path Forwarding（ユニキャスト RPF）機能について説明します。ユニキャスト RPF 機能は、間違ったまたは偽造送信元 IP アドレスがルータを流れて発生する問題を軽減するのに役立ちます。

この章のユニキャスト RPF コマンドの詳細については、『*Cisco IOS Security Command Reference*』の「Unicast Reverse Path Forwarding Commands」の章を参照してください。この章に記載されたその他のコマンドに関するマニュアルを特定するには、コマンド リファレンスのマスター インデックスを使用するか、オンラインで検索してください。

機能に関するハードウェア プラットフォームまたはソフトウェア イメージの情報を確認するには、Cisco.com の Feature Navigator を使用してその機能に関する情報を検索するか、特定のリリースに対応するソフトウェア リリース ノートを参照してください。詳細については、「Using Cisco IOS Software」の章の「Identifying Supported Platforms」を参照してください。

章の内容

この章の内容は、次のとおりです。

- ユニキャスト RPF について
- ユニキャスト RPF の設定作業リスト
- ユニキャスト RPF のモニタリングおよびメンテナンス
- ユニキャスト RPF のモニタリングおよびメンテナンス
- ユニキャスト RPF の設定例

ユニキャスト RPF について

ユニキャスト RPF 機能は、検証可能な送信元 IP アドレスが不足している IP パケットを廃棄することで、間違ったまたは偽造（スプーフィングされた）送信元 IP アドレスがネットワークに流れて発生する問題を軽減するのに役立ちます。たとえば、Smurf や Tribal Flood Network（TFN）など、多くの一般的なタイプの DoS 攻撃は、偽造された、または次々に変わる送信元 IP アドレスを使用して、攻撃を突き止めたりフィルタしたりすることを攻撃者が阻止できるようにします。パブリック アクセスを提供する Internet Service Provider（ISP; インターネットサービスプロバイダー）の場合、ユニキャスト RPF が IP ルーティング テーブルと整合性の取れた有効な送信元アドレスを持つパケットだけを転送することによって、これらの攻撃をそらします。この処理により、ISP のネットワークとお客様、および残りのインターネットの他の部分が保護されます。

ここでは、次の情報について説明します。

- ユニキャスト RPF の概要
- ユニキャスト RPF の実装
- 制約事項
- 関連機能および技術
- ユニキャスト RPF 設定の前提条件

ユニキャスト RPF の概要

ユニキャスト RPF がインターフェイスでイネーブルのときは、ルータはそのインターフェイスに対する入力として受信したすべてのパケットを検証して、送信元アドレスおよび送信元インターフェイスがルーティング テーブルに存在し、パケットを受信したインターフェイスと一致することを確認します。「後方検索」機能は、Cisco Express Forwarding（CEF）がルータでイネーブルの場合にのみ利用可能です。これは、検索が Forwarding Information Base（FIB; 転送情報ベース）に基づいて行われるためです。FIB は CEF の動作の一部として生成されます。

（注）　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終端にあるルータ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、ルータ インターフェイスで受信したパケットが、パケットの送信元への最適な戻りパス（戻りルート）で到着しているかどうかを確認します。ユニキャスト RPF は、CEF テーブルの逆引きを行うことでこれを確認します。最適なリバース パス ルートのいずれかでパケットの受信が行われた場合は、パケットは通常通り転送されます。パケットを受信したインターフェイスと同じインターフェイスにリバース パス ルートがない場合は、送信元アドレスが変更されてい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。

（注）　ユニキャスト RPF では、「最適な」等コスト戻りパスのすべてが有効とされます。そのため、ユニキャスト RPF は、複数の戻りパスが存在する場合に、各パスがルーティング コスト（ホップ数、重みなど）に関してその他のパスと等しく、ルートが FIB に存在するという条件で動作します。ユニキャスト RPF はまた、EIGRP バリアントが使用されていて、送信元 IP アドレスに戻る不等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 および ACL が設定されているインターフェイスでパケットを受信する場合は、次の動作が発生します。

ステップ 1　受信インターフェイスで設定されている入力 ACL を確認します。

ステップ 2　ユニキャスト RPF は、FIB テーブルの逆引きを行うことで、パケットが送信元への最適な戻りパスで到着しているかどうかを確認します。

ステップ 3　パケット転送のため CEF テーブル（FIB）のルックアップを実行します。

ステップ 4　送信インターフェイス上の出力 ALC の確認が行われます。

ステップ 5　パケットが転送されます。

ここでは、ユニキャスト RPF 拡張の内容について説明します。

- アクセス コントロール リストおよびロギング
- インターフェイス単位の統計情報

図 29-1 は、ユニキャスト RPF および CEF が連動して、パケットの戻りパスを確認することで IP 送信元アドレスを確認する方法を示します。この例では、お客様は送信元アドレスが 192.168.1.1 であるパケットをインターフェイス GigabitEthernet 1/1 から送信しています。ユニキャスト RPF は、192.168.1.1 に GigabitEthernet 1/1 へのパスがあるかどうか FIB を確認します。一致するパスがある場合にパケットが送信されます。一致するものがない場合、パケットはドロップされます。

図 29-1　ユニキャスト RPF による IP 送信元アドレスの確認

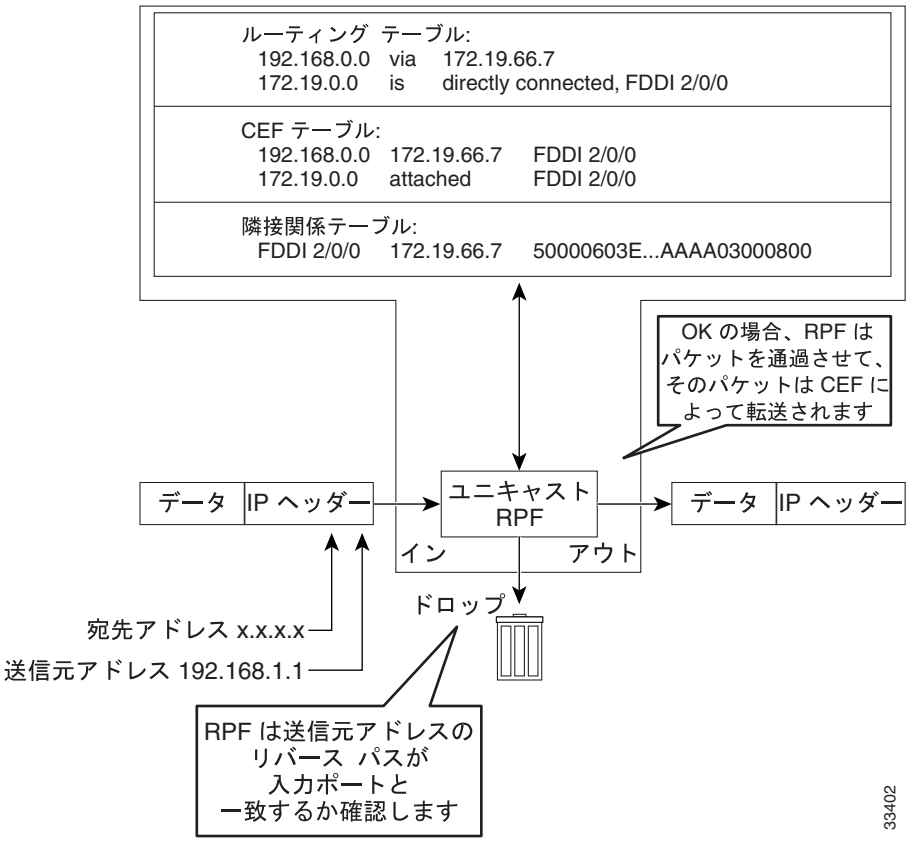
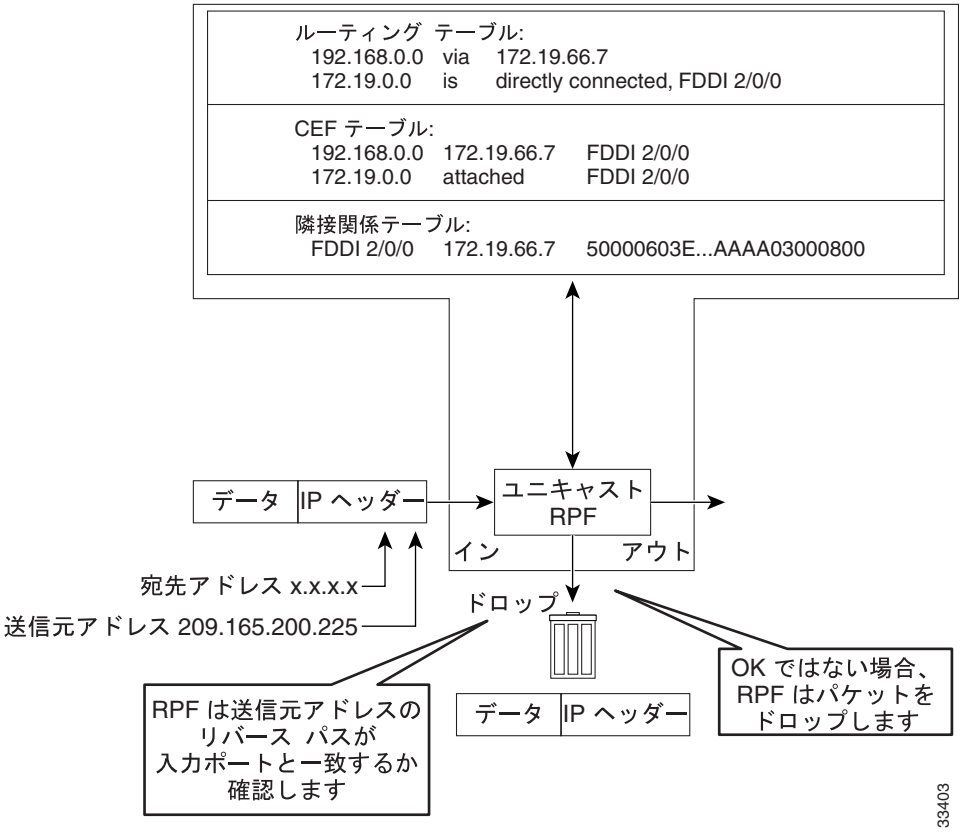


図 29-2 は、ユニキャスト RPF が確認に失敗したパケットをドロップする方法を示します。この例では、お客様は送信元アドレスが 209.165.200.225 であるパケットを送信していて、そのパケットをインターフェイス GigabitEthernet 1/1 で受信します。ユニキャスト RPF は、209.165.200.225 に GigabitEthernet 1/1 への戻りパスがあるかどうか FIB を確認します。一致するパスがある場合にパケットが送信されます。この場合、お客様のパケットを GigabitEthernet 1/1 上の送信元アドレス 209.165.200.225 に戻るルートのエントリがルーティング テーブルにないため、パケットはドロップされます。

図 29-2　ユニキャスト RPF による確認に失敗したパケットのドロップ



ユニキャスト RPF の実装

ユニキャスト RPF には、次の主要な実装原理があります。

- パケットの受信は、パケットの送信元への最適な戻りパス（ルート）があるインターフェイスで行われる必要があります（*対称ルーティング*と呼ばれるプロセス）。FIB に、受信する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。FIB へのルートの追加は、スタティック ルート、ネットワーク ステートメント、またはダイナミック ルーティングによって行われます（ACL は、パッケージが特定の、最適ではない非対称入力パスで到着すると分かっている場合には、ユニキャスト RPF の使用を許可します）。
- 受信するインターフェイスにある IP 送信元アドレスが、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終端にあるルータの入力インターフェイスにのみ適用されます。

これらの実装原理においては、ユニキャスト RPF は、ネットワーク管理者がお客様のためだけでなく、ダウンストリーム ネットワークまたは ISP にインターネットに対する別の接続がある場合でも、ダウンストリーム ネットワークまたは ISP のために使用可能なツールとなります。

注意　重みおよびローカル プリファレンスなどのオプションの BGP 属性を使用して、送信元アドレスに戻る最善のパスを変更できます。変更は、ユニキャスト RPF の動作に影響を与える場合があります。

ここでは、ユニキャスト RPF の実装について説明します。

- セキュリティ ポリシーとユニキャスト RPF
- ユニキャスト RPF を使用する場所
- ルーティング テーブルの要件
- ユニキャスト RPF を使用できない場所
- BOOTP および DHCP を使用したユニキャスト RPF

セキュリティ ポリシーとユニキャスト RPF

ユニキャスト RPF を展開するポリシーの決定時には、次の点を考慮してください。

- ユニキャスト RPF は、大規模なネットワークのダウンストリーム インターフェイス（ネットワークのエッジに存在することが望ましい）に適用する必要があります。
- ユニキャスト RPF をさらに下位のダウンストリームに適用すればするほど、アドレス スプーフィングの軽減時およびスプーフィングされたアドレスの送信元の特定時にさらにきめ細やかに対応できます。たとえば、ユニキャスト RPF を集約ルータに適用すると、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の軽減に役立ち、管理が簡単になりますが、攻撃の送信元の特定には有益ではありません。ユニキャスト RPF をネットワーク アクセス サーバに適用すると、攻撃の範囲の制限や、攻撃の送信元の追跡に役立ちますが、多くのサイト間でユニキャスト RPF を展開することで、ネットワーク オペレーションの管理コストが増大します。
- 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 リソース全体でユニキャスト RPF を展開するエンティティがさらに増加すれば、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中断がさらに軽減し、攻撃の送信元を追跡する機会がさらに増えます。
- ユニキャスト RPF は、GRE、LT2P、または PPTP などのトンネルにカプセル化した IP パケット を検査しません。ユニキャスト RPF が、トンネリングが行われて暗号化レイヤがパケットから取り除かれたあとにだけネットワーク トラフィックを処理するには、ユニキャスト RPF をホーム ゲートウェイで設定する必要があります。

ユニキャスト RPF を使用する場所

ユニキャスト RPF は、原則的にネットワーク内のアクセス ポイントが 1 つだけ（つまり、アップストリーム接続が 1 つだけ）である「シングルホーム」環境であれば使用できます。アクセス ポイントが 1 つあるネットワークは、対称ルーティングの良い例となります。これは、パケットがネットワークに入るときのインターフェイスが、IP パケットの送信元への最適な戻りパスでもあるということを表します。ユニキャスト RPF は、インターネット、イントラネット、またはエクストラネット環境のネットワーク境界または顧客ネットワーク終端の ISP 環境において最適に使用されます。

次のセクションで、2 つのネットワーク環境におけるユニキャスト RPF 実装の概要について説明します。

- ISP への接続を 1 つ備えるエンタープライズ ネットワーク
- ネットワーク アクセス サーバ アプリケーション（ユニキャスト RPF を PSTN/ISDN PoP 集約ルータに適用）

ISP への接続を 1 つ備えるエンタープライズ ネットワーク

エンタープライズ ネットワークでは、ユニキャスト RPF を使用して入力インターフェイスでのトラフィックをフィルタリングする（*入力フィルタリング*と呼ばれるプロセス）目的の 1 つは、インターネットから誤ったパケットが届かないようにすることです。従来、インターネットへの接続が 1 つあるローカル ネットワークは、受信するインターフェイスで ACL を使用して、スプーフィングされたパケットがインターネットからローカル ネットワークに入ってこないようにしていました。

ACL は、シングルホームを使用する多くのお客様については効果的に機能しますが、ACL を入力フィルタとして使用する場合には、次の 2 つの一般的に言及される制限を含めたトレードオフが存在します。

- 非常に高速なパケット レートでのパケット / 秒（PPS）パフォーマンス

（注） この制限は、ソフトウェア パケットの転送にのみ適用されます。ハードウェア パケットの転送は、ACL および uRPF の両方で同じです。

- ACL のメンテナンス（ネットワークに新しいアドレスが追加された場合）

ユニキャスト RPF は両方の制限に対応するツールです。ユニキャスト RPF を使用すると、入力フィルタリングは CEF PPS レートで行われます。この処理スピードは、リンク速度が 1 Mbps を超えたときに効果があります。さらに、ユニキャスト RPF は FIB を使用するため、ACL メンテナンスが不要になり、したがって従来の ACL の管理オーバーヘッドが減少します。次に、ユニキャスト RPF を入力フィルタリング向けに設定する方法を示す図および例を示します。

図 29-3 に、アップストリーム ISP へのリンクが 1 つあるエンタープライズ ネットワークを示します。この例では、間違ったパケットがインターネットから届かないようにするために、ユニキャスト RPF はエンタープライズ ルータのインターフェイス GigabitEthernet 1/1 で適用されます。また、間違ったパケットがエンタープライズ ネットワークから届かないようにするために、ユニキャスト RPF は ISP ルータのインターフェイス GigabitEthernet 2/1 で適用されます。

図 29-3　入力フィルタリングのためにユニキャスト RPF を使用するエンタープライズ ネットワーク

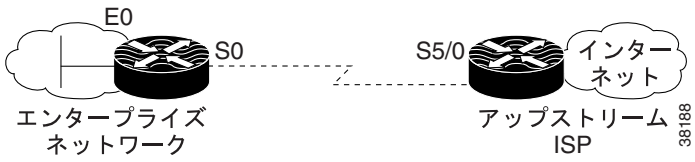


図 29-3 の関係図を使用すると、ISP ルータの典型的な構成は（CEF が有効になっていると想定して）次のとおりです。

```
interface Gigabit Ethernet 2/1
  description Link to Enterprise Network
  ip address 192.168.3.1 255.255.255.255
  no switchport
  ip address 10.1.1.2 255.255.255.0
  ip route 192.168.10.0 255.255.255.0 10.1.1.1
  ip verify unicast source reachable-via rx allow-default
```

エンタープライズ ネットワークのゲートウェイ ルータ設定は（CEF が有効になっていると想定して）次のとおりです。

```
interface Gigabit Ethernet 1/2
 description ExampleCorp LAN
 ip address 192.168.10.1 255.255.252.0
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp

interface Gigabit Ethernet 1/1
 description Link to Internet
 no switchport
 ip address 10.1.1.1 255.255.255.0
 ip route 0.0.0.0 0.0.0.0 10.1.1.2
 ip verify unicast source reachable-via allow-default
 no ip proxy-arp
 no ip redirects
 no ip directed-broadcast
```

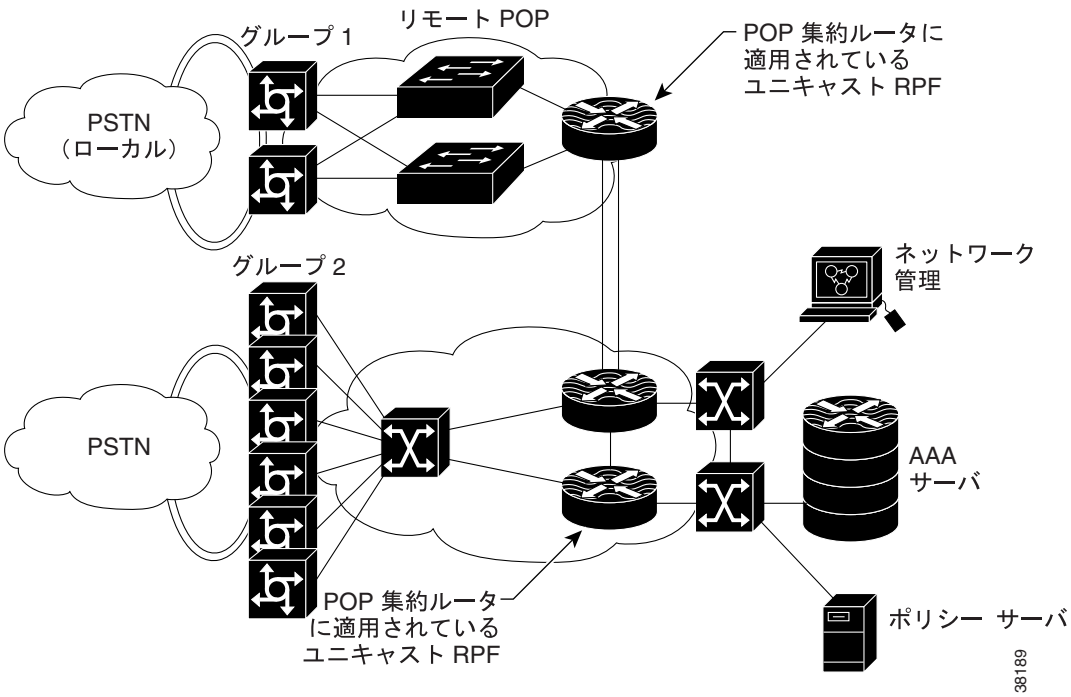
ユニキャスト RPF は、1 つのデフォルト ルートで動作することに注意してください。追加のルートまたはルーティング プロトコルはありません。ネットワーク 192.168.10.0/22 は接続されたネットワークです。したがって、送信元アドレスが 192.168.10.0/22 の範囲内の、インターネットから届くパケットは、ユニキャスト RPF によってドロップされます。

ネットワーク アクセス サーバ アプリケーション（ユニキャスト RPF を PSTN/ISDN PoP 集約ルータに適用）

集約ルータは、シングルホームを使用するお客様にとってはユニキャストを使用する最適な場所です。ユニキャスト RPF は、インターネットへの接続に専用線または PSTN/ISDN/xDSL を使用するお客様にとって等しく効果的に動作します。実際、ダイヤルアップ接続は偽造 IP アドレスを使用した DoS 攻撃の送信元とみなされることが非常に多くあります。ネットワーク アクセス サーバが CEF をサポートしているかぎり、ユニキャスト RPF は動作します。この関係図では、お客様の集約ルータに完全なインターネット ルーティング テーブルを用意する必要はありません。集約ルータは、プレフィクス情報（IP アドレス ブロック）をルーティングする必要があります。したがって、Interior Gateway Protocol（IGP; 内部ゲートウェイ プロトコル）または Internal Border Gateway Protocol（IBGP; 内部ボーダー ゲートウェイ プロトコル）で設定または再配布された情報であれば、ユニキャストはその機能を十分に発揮できます。

図 29-4 は、お客様にダイヤルアップ接続を提供する ISP ルータとの ISP アクセス ポイント向けの集約ルータおよびアクセス ルータへのユニキャスト RPF の適用を示します。この例では、ユニキャスト RPF は ISP 集約ルータの受信する（入力）インターフェイスの、お客様のダイヤルアップ接続ルータからのアップストリームに適用されます。

図 29-4　お客様の PSTN/ISDN 接続に適用されるユニキャスト RPF



ルーティング テーブルの要件

ユニキャスト RPF が正しく動作するには、CEF テーブルに適切な情報が存在する必要があります。この要件は、ルータに完全なインターネット ルーティング テーブルが存在する必要があるという意味ではありません。CEF テーブルに必要なルーティング情報の量は、ユニキャスト RPF の設定場所およびルータがネットワークで実行している機能によって異なります。例えば、ISP 環境では、お客様向けの専用線集約ルータであるルータが必要とするのは IGP または IBGP（ネットワークでどちらの技術を使用しているかにより異なります）で再配布されたスタティック ルートに関する情報のみです。ユニキャスト RPF がお客様のインターフェイス上で設定されるため、必要になるのは最低限のルーティング情報のみです。また別のシナリオで、シングルホームの ISP が、ユニキャスト RPF をインターネットにリンクするゲートウェイ上に配置する場合は、完全なインターネット ルーティング テーブルが必要になります。完全なルーティング テーブルを要求することで、インターネット ルーティング テーブルにないアドレスを使用する外部 DoS 攻撃から ISP を保護するのに役立ちます。

ユニキャスト RPF を使用できない場所

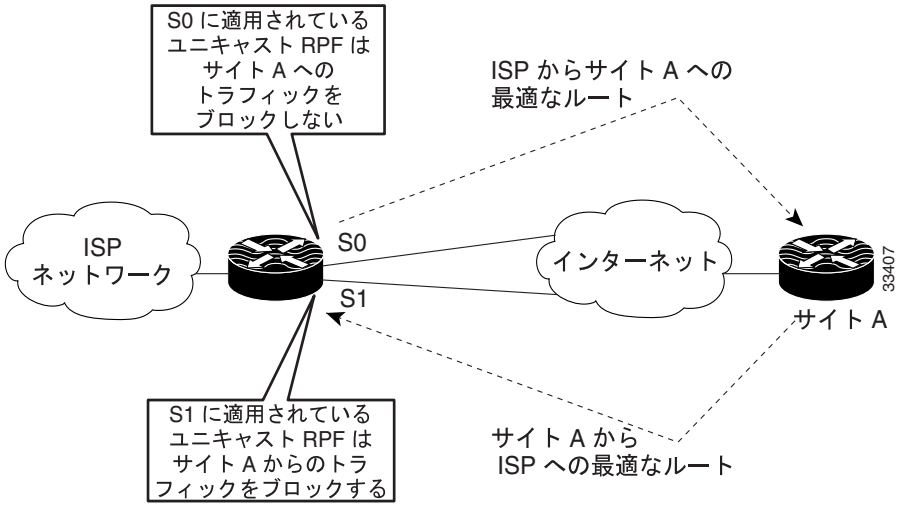
ユニキャスト RPF は、ネットワークの内側にあるインターフェイスで使用しないでください。内側にあるインターフェイスでは、ルーティングの非対称性（図 29-5 を参照）が発生しやすく、パケットの送信元への複数のルートが存在することになるためです。ユニキャスト RPF は、対称性が自然に発生するか、対称性が設定されている環境にのみ適用する必要があります。管理者がユニキャスト RPF を有効化するインターフェイスを注意深く計画するかぎり、ルーティングの非対称性は深刻な問題ではありません。

たとえば、ISP ネットワークのコアにあるルータよりも、ISP のネットワークのエッジにあるルータには、対称リバース パスがあることが多くあります。ISP ネットワークのコアにあるルータには、ルータからの最適な転送パスが、パケットがルータに戻るときに選択されるパスであるという保証がありません。したがって、ACL を使用して、ルータが着信パケットを受け入れる場合を除いて、ユニキャスト RPF を非対称ルーティングが発生する可能性がある場所に適用することを推奨しま

せん。ACL は、パケットが特定の、最適ではない非対称入力パスで到着すると分かっている場合には、ユニキャスト RPF の使用を許可します。ただし、ISP にとっては、ユニキャスト RPF をネットワークのエッジまたはお客様のネットワークのエッジにのみ配置するのが最も簡単です。

図 29-5 は、ユニキャスト RPF が非対称ルーティング環境で正規のトラフィックをブロックする方法を示します。

図 29-5　非対称ルーティング環境においてトラフィックをブロックするユニキャスト RPF



BOOTP および DHCP を使用したユニキャスト RPF

Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）および Dynamic Host Configuration Protocol（DHCP）機能が正しく動作するようにするために、ユニキャスト RPF は、送信元として 0.0.0.0、宛先として 255.255.255.255 を持つパケットの通過を許可します。

制約事項

マルチホームを使用するクライアントへのユニキャスト RPF の適用には、いくつかの基本的な制約事項があります。

- マルチホーミングはクライアントが冗長サービスを構築する目的と合わないため、クライアントは同じルータに対してマルチホームをしないでください。
- お客様は、（インターネットから）リンクに流れるパケットが、リンクからアドバタイズされたルートと一致することを確認する必要があります。一致しない場合、ユニキャスト RPF はそれらのパケットを間違ったパケットとしてフィルタリングします。

関連機能および技術

ユニキャスト RPF に関連する機能および技術に関する詳細については、次の項目を参照してください。

- ユニキャスト RPF がルータ上で適切に機能するには CEF が必要です。CEF の詳細については、『*Cisco IOS Switching Services Configuration Guide*』を参照してください。

- Cisco IOS Access Control List（ACL; アクセス コントロール リスト）を使用して*入力*および*出力*フィルタリングのポリシーを組み合わせると、スプーフィング攻撃の軽減に対するユニキャスト RPF の効果が大きくなります。
  - 入力フィルタリングでは、内部または外部ネットワークのネットワーク インターフェイスで受信したトラフィックにフィルタを適用します。入力フィルタリングを使用すると、別のネットワークまたはインターネットから到着したパケットのうち、その送信元アドレスがローカル ネットワーク、プライベート、またはブロードキャスト アドレスと一致するパケットがドロップされます。たとえば ISP 環境では、入力フィルタリングはクライアント（お客様）またはインターネットのいずれかのルータで受信したトラフィックに適用できます。
  - 出力フィルタリングでは、ネットワーク インターフェイス（送信するインターフェイス）から送信されるトラフィックにフィルタを適用します。ネットワークをインターネットまたは他のネットワークに接続するルータ上のパケットをフィルタリングすることで、ネットワークから送信するために有効な送信元 IP アドレスを持つパケットのみを許可できます。

  ネットワーク フィルタリングの詳細については、『RFC 2267』および『*Cisco IOS IP Configuration Guide*』を参照してください。
- Cisco IOS ソフトウェアは、DoS 攻撃を軽減するために役立つ機能をさらに提供しています。
  - Committed Access Rate（CAR; 専用アクセス レート）。CAR を使用すると、アクセス リストと一致するネットワーク トラフィックに対して、帯域ポリシーを強制できます。たとえば CAR は、ICMP トラフィックなどの量が少ないと思われるトラフィックにレート制限を課すことができます。CAR の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』を参照してください。
  - Context-based Access Control（CBAC; コンテキストベース アクセス コントロール）。CBAC は、保護されたネットワークから発信されていないネットワーク トラフィックを選択的にブロックします。CBAC は、タイムアウトおよびしきい値を使用してセッション ステート情報を管理します。これは、完全に確立された状態ではなくなっているセッションをいつドロップするか決定するのに役立ちます。ネットワーク セッションのタイムアウト値を設定することは、システム リソースを解放し、特定の時間が経過したあとでセッションをドロップするので、DoS 攻撃の軽減に役立ちます。CBAC の詳細については、『*Cisco IOS Security Configuration Guide*』を参照してください。
  - TCP 代行受信。TCP 代行受信機能はソフトウェアに実装され、DoS 攻撃の一種である TCP SYN フラッディング攻撃から TCP サーバを保護します。SYN フラッディング攻撃は、ハッカーが接続要求を集中させてサーバにフラッディングさせるときに発生します。CBAC と同様に、TCP 代行受信機能もまた、タイムアウトおよびしきい値を使用してセッション ステート情報を管理します。これは、完全に確立された状態ではなくなっているセッションをいつドロップするか決定するのに役立ちます。TCP 代行受信の詳細については、『*Cisco IOS Security Configuration Guide*』を参照してください。

ユニキャスト RPF 設定の前提条件

ユニキャスト RPF を設定する前に、ACL を次のように設定します。

- 標準または拡張 ACL を設定して、無効な IP アドレスの送信を削減します（出力フィルタリングを実行します）。有効な送信元アドレスのみネットワークに出入りすることを許可して、それ以外の送信元すべてがインターネットに向けてネットワークを出ないようにします。
- 標準または拡張 ACL エントリを設定して、無効な送信元 IP アドレスを持つパケットをドロップ（拒否）します（入力フィルタリングを実行します）。無効な送信元 IP アドレスには、次の種類があります。
  - 予約されたアドレス
  - ループバック アドレス
  - プライベート アドレス（RFC 1918、「*Address Allocation for Private Internets*」）
  - ブロードキャスト アドレス（マルチキャスト アドレスを含む）
  - 保護されたネットワークに関連する有効なアドレスの範囲外の送信元アドレス

ユニキャスト RPF の設定作業リスト

次のセクションでは、ユニキャスト RPF の設定作業について説明します。リスト内の各作業は、任意または必須です。

- ユニキャスト RPF の設定（必須）
- ユニキャスト RPF の確認（任意）

この章の最後にある「ユニキャスト RPF の設定例」を参照してください。

ユニキャスト RPF の設定

ユニキャスト RPF は、いかなる種類のカプセル化でもサポートし、ルータによって受信された IP パケットの操作を行うインターフェイスまたはサブインターフェイス上でイネーブルとなる入力側の機能です。

ユニキャスト RPF を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config-if)# interface type`	ユニキャスト RPF を適用する入力インターフェイスを選択します。これは受信するインターフェイスで、これによってユニキャスト RPF はパケットを次の宛先に転送する前に最適な戻りパスを確認できます。 インターフェイスのタイプは使用しているルータおよびルータに取り付けられているインターフェイス カードのタイプ専用です。利用可能なインターフェイスのタイプの一覧を表示するには、**interface ?** コマンドを入力します。
ステップ 2	`Router(config-if)# ip verify unicast source reachable-via rx allow-default`	インターフェイスのユニキャスト RPF をイネーブルにします。
ステップ 3	`Router(config-if)# exit`	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。ユニキャスト RPF を適用するインターフェイスごとに、ステップ 2 および 3 を繰り返します。

ユニキャスト RPF の確認

ユニキャスト RPF が動作可能かどうかを確認するには、**show cef interface** コマンドを使用します。次に、ユニキャスト RPF がインターフェイス GigabitEthernet 3/1 でイネーブルになっている例を示します。

```
Switch# show cef interface gigabitEthernet 3/1
GigabitEthernet3/1 is up (if_number 79)
  Corresponding hwidb fast_if_number 79
  Corresponding hwidb firstsw->if_number 79
  Internet address is 10.1.1.1/24
  ICMP redirects are always sent
  IP unicast RPF check is enabled <======
  Input features: uRPF <=====
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  BGP based policy accounting on input is disabled
  BGP based policy accounting on output is disabled
  Hardware idb is GigabitEthernet3/1
  Fast switching type 1, interface type 155
  IP CEF switching enabled
  IP CEF switching turbo vector
  IP Null turbo vector
  IP prefix lookup IPv4 mtrie 8-8-8-8 optimized
  Input fast flags 0x4000, Output fast flags 0x0
  ifindex 78(78)
  Slot 3 Slot unit 1 VC -1
  Transmit limit accumulator 0x0 (0x0)
  IP MTU 1500
```

ユニキャスト RPF のモニタリングおよびメンテナンス

ここでは、ユニキャスト RPF のモニタリングおよびメンテナンスに使用されるコマンドについて説明します。

コマンド	目的
Router# **show ip traffic**	ユニキャスト RPF によるドロップまたはドロップ抑制に関するグローバル ルータの統計情報を表示します。
Router(config-if)# **no ip verify unicast**	インターフェイスのユニキャスト RPF をディセーブルにします。

ユニキャスト RPF は、間違ったまたは偽造送信元アドレスのためドロップまたは抑制されたパケット数をカウントします。ユニキャスト RPF は、次のインターフェイス単位のグローバル情報を含めてドロップまたは転送されたパケット数をカウントします。

- グローバル ユニキャスト RPF ドロップ
- インターフェイス単位のユニキャスト RPF ドロップ
- インターフェイス単位のユニキャスト RPF ドロップ抑制

show ip traffic コマンドは、ルータのすべてのインターフェイスについてドロップまたは抑制されたパケットの合計数（グローバル カウント）を示します。ユニキャスト RPF ドロップ カウントは、IP 統計情報セクションに表示されます。

```
Router# show ip traffic

IP statistics:
  Rcvd:  1471590 total, 887368 local destination
         0 format errors, 0 checksum errors, 301274 bad hop count
         0 unknown protocol, 0 not a gateway
         0 security failures, 0 bad options, 0 with options
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 0 alert, 0 other
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 couldn't fragment
  Bcast: 205233 received, 0 sent
  Mcast: 463292 received, 462118 sent
  Sent:  990158 generated, 282938 forwarded
  ! The second line below ("0 unicast RPF") displays Unicast RPF packet dropping
  information.
  Drop:  3 encapsulation failed, 0 unresolved, 0 no adjacency
         0 no route, 0 unicast RPF, 0 forced drop
```

ドロップまたは抑制されたパケットのカウントがノンゼロ値である場合は、次の 2 つのいずれかを意味します。

- ユニキャスト RPF は、不良送信元アドレスを持つパケットをドロップまたは抑制しています（通常の動作）。
- ユニキャスト RPF は、非対称ルーティングが存在する（つまり、送信元アドレスに対する最適な戻りパスとして複数のパスが存在する）環境においてユニキャスト RPF を使用するためにルートが誤って設定されているため、正規のパケットをドロップまたは抑制しています。

show ip interface コマンドは、特定のインターフェイスにおいてドロップまたは抑制されたパケットの合計を示します。ユニキャスト RPF が特定の ACL を使用するよう設定されている場合は、このドロップ統計情報とともに ACL 情報が表示されます。

```
Router> show ip interface ethernet0/1/1

   Unicast RPF ACL 197
   1 unicast RPF drop
   1 unicast RPF suppressed drop
```

show access-lists コマンドは、特定のエントリについて特定のアクセス リスト内で一致する項目が見つかった数を表示します。

```
Router> show access-lists

Extended IP access list 197
     deny ip 192.168.201.0 0.0.0.63 any log-input (1 match)
     permit ip 192.168.201.64 0.0.0.63 any log-input (1 match)
     deny ip 192.168.201.128 0.0.0.63 any log-input
     permit ip 192.168.201.192 0.0.0.63 any log-input
```

ユニキャスト RPF の設定例

ここでは、次の設定例を示します。

- 専用線集約ルータでのユニキャスト RPF の例
- Cisco AS5800 でのダイヤルアップ ポートを使用したユニキャスト RPF の例
- 着信および発信フィルタを使用したユニキャスト RPF の例
- ACL およびロギングを使用したユニキャスト RPF の例

専用線集約ルータでのユニキャスト RPF の例

次のコマンドは、ユニキャスト RPF をシリアル インターフェイス上でイネーブルにします。

```
ip cef
! or "ip cef distributed" for RSP+VIP based routers
!
interface serial 5/0/0
 ip verify unicast reverse-path
```

Cisco AS5800 でのダイヤルアップ ポートを使用したユニキャスト RPF の例

次の例では、Cisco AS5800 でユニキャスト RPF をイネーブルにします。**interface Group-Async** コマンドを使用すると、すべてのダイヤルアップ ポートにユニキャスト RPF を適用することが容易になります。

```
ip cef
!
interface Group-Async1
 ip verify unicast reverse-path
```

着信および発信フィルタを使用したユニキャスト RPF の例

次に、非常に簡単なシングルホームを使用する ISP を使用して、ユニキャスト RPF とともに使用する入力および出力フィルタの概念の例を示します。この例は、アップストリーム インターフェイスで着信および発信フィルタの両方を使用する、ISP が割り当てた Classless Interdomain Routing（CIDR）ブロック 209.165.202.128/28 を示します。ISP は一般的にシングルホームを使用しないことに注意してください。したがって、非対称フローについての規定（発信トラフィックが 1 つのリンクから発信され、別のリンクから戻る場合）を設計して ISP の境界ルータ上のフィルタに組み込む必要があります。

```
ip cef distributed
!
interface Serial 5/0/0
 description Connection to Upstream ISP
 ip address 209.165.200.225 255.255.255.252
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 ip verify unicast reverse-path
 ip access-group 111 in
 ip access-group 110 out
!
access-list 110 permit ip 209.165.202.128 0.0.0.31 any
access-list 110 deny ip any any log
access-list 111 deny ip host 0.0.0.0 any log
access-list 111 deny ip 127.0.0.0 0.255.255.255 any log
access-list 111 deny ip 10.0.0.0 0.255.255.255 any log
access-list 111 deny ip 172.16.0.0 0.15.255.255 any log
access-list 111 deny ip 192.168.0.0 0.0.255.255 any log
access-list 111 deny ip 209.165.202.128 0.0.0.31 any log
access-list 111 permit ip any any
```

ACL およびロギングを使用したユニキャスト RPF の例

次に、ユニキャスト RPF を使用して ACL およびロギングを使用する例を示します。この例では、拡張 ACL 197 が特定のアドレス範囲についてネットワーク トラフィックを拒否または許可するエントリを示します。ユニキャスト RPF は、インターフェイス Ethernet0 で設定され、そのインターフェイスに到着したパケットを確認します。

たとえば、インターフェイス Ethernet0 に到着する送信元アドレスが 192.168.201.10 であるパケットは、ACL 197 にある拒否（deny）ステートメントのため、ドロップされます。この場合、ACL 情報はログに記録され（ロギング オプションが ACL エントリについてオンになっている）、ドロップされたパケットはインターフェイス単位でグローバルにカウントされます。インターフェイス Ethernet0 に到着する送信元アドレスが 192.168.201.100 であるパケットは、ACL 197 にある許可（permit）ステートメントのため、転送されます。ドロップまたは抑制されたパケットに関する ACL 情報はログ サーバに記録されます（ロギング オプションが ACL エントリについてオンになっている）。

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.0
 ip verify unicast reverse-path 197
!
int eth0/1/2
 ip address 192.168.201.1 255.255.255.0
!
access-list 197 deny   ip 192.168.201.0 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 0.0.0.63 any log-input
access-list 197 deny   ip 192.168.201.128 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 0.0.0.63 any log-input
access-list 197 deny ip host 0.0.0.0 any log
```