CHAPTER 35

uRPF 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 機能を使用すると、スイッチを通過する不正な形式または偽造の IP 送信元アドレスによって発生する問題を軽減できます。

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。この章で使用される他のコマンドの説明については、コマンド リファレンスのマスター索引を参照するか、またはオンラインで検索してください。

機能に関連するハードウェア プラットフォームまたはソフトウェア イメージ情報を確認するには、Cisco.com にある Feature Navigator を使用して機能に関する情報を検索するか、または特定のリリースのソフトウェア 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。

この章は、次の内容で構成されています。

（注） この章で使用するスイッチ コマンドの構文および使用方法の詳細については、次の URL で『*Cisco Catalyst 4500 Series Switch Command Reference*』と関連資料を参照してください。

http://www.cisco.com/en/US/products//hw/switches/ps4324/index.html

『Catalyst 4500 Series Switch Command Reference』に掲載されていないコマンドについては、より詳細な Cisco IOS ライブラリを参照してください。次の URL で『*Cisco IOS Command Reference*』と関連資料を参照してください。

http://www.cisco.com/en/US/products/ps6350/index.html

ユニキャスト リバース パス転送の概要

ユニキャスト RPF 機能を使用して、検証可能な IP 送信元アドレスがない IP パケットを廃棄することで、不正な形式または偽造（偽装）の IP 送信元アドレスがネットワークで使用されることによって発生する問題を軽減できます。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、uRPF 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、そのような攻撃をそらします。この処理により、ISP のネットワーク、その顧客、および残りのインターネットが保護されます。

ここでは、次の情報について説明します。

ユニキャスト RPF の機能

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、スイッチ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、シスコ エクスプレス フォワーディング（CEF）がルータでイネーブルの場合にだけ利用可能です。これは、検索が転送情報ベース（FIB）に基づいて行われるためです。CEF では、その動作の一部として FIB が生成されます。

（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だけ適用されます。

ユニキャスト RPF は、スイッチ 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。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パ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、送信元アドレスが変更された可能性があります。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、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、ルーティング コスト（ホップ カウント、重みなど）に関して他のパスと同等で、ルートが FIB に存在する場合、ユニキャスト RPF は機能します。また、EIGRP バリアントが使用され、送信元 IP アドレスに戻る同等ではない候補パスが存在する場合も、ユニキャスト RPF は機能します。

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を受信した場合、次の処理が発生します。

ステップ 1　インバウンド インターフェイスで設定されたインバウンド ACL が確認されます。

ステップ 2　ユニキャスト RPF は、パケットが送信元に対する最適なリターン パスで到達したかどうかを確認します。この処理には、FIB テーブルの逆ルックアップを実行します。

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　出力 ACL は、アウトバウンド インターフェイスで確認されます。

ステップ 5　パケットは転送されます。

ここでは、次のユニキャスト RPF の強化について説明します。

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

図 35-1 に、ユニキャスト RPF と CEF を併用し、パケットのリターン パスを確認することで、IP 送信元アドレスを検証する方法を示します。この例では、ユーザがインターフェイス ギガビット イーサネット 1/1 から送信元アドレス 192.168.1.1 であるパケットを送信しました。ユニキャスト RPF は FIB で、ギガビット イーサネット 1/1 に対するパスが 192.168.1.1 にあるかどうかを確認します。一致するパスがある場合、パケットは転送されます。一致するパスがない場合、パケットはドロップされます。

図 35-1　IP 送信元アドレスを検証するユニキャスト RPF

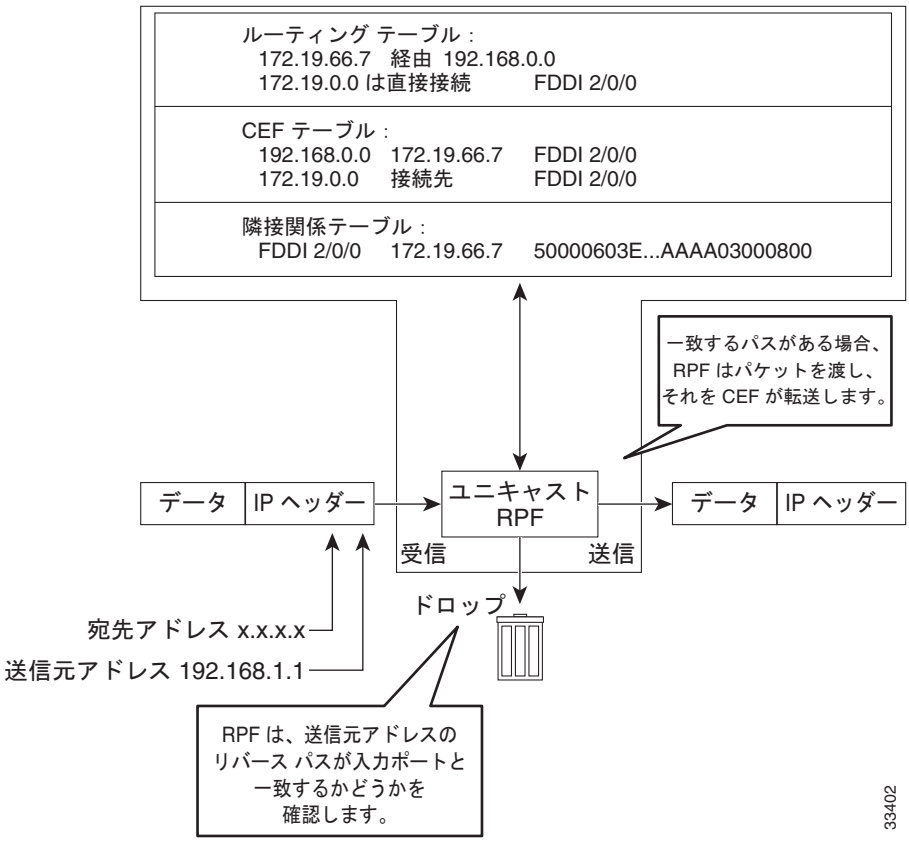
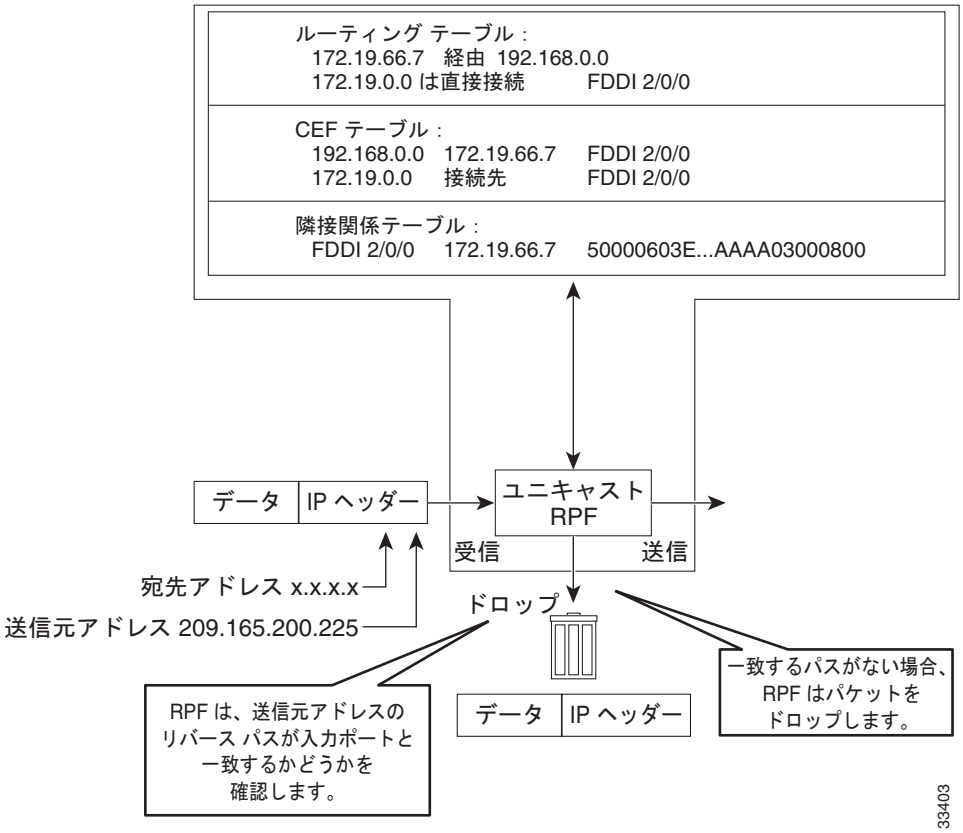


図 35-2 に、検証に失敗したパケットをユニキャスト RPF がドロップする方法を示します。この例では、お客様は送信元アドレスが 209.165.200.225 であるパケットを送信していて、そのパケットをギガビット イーサネット インターフェイス 1/1 で受信します。ユニキャスト RPF は FIB で、ギガビット イーサネット 1/1 に対するパスが 209.165.200.225 にあるかどうかを確認します。一致するパスがある場合、パケットは転送されます。ルーティング テーブルに、ユーザのパケットをギガビット イーサネット 1/1 上の送信元アドレス 209.165.200.225 に戻すリバース エントリはありません。そのため、パケットはドロップされます。

図 35-2　検証に失敗したパケットをドロップするユニキャスト RPF



ユニキャスト RPF の実装

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する必要があります（このプロセスは*対称ルーティング*と呼ばれます）。FIB には、受信側インターフェイスに対するルートと一致するルートが存在する必要があります。FIB にルートを追加する処理は、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 ルーティングで実行します。（ACL によって、パケットが最適ではない特定の非対称入力パスを通じて到達する場合に、ユニキャスト RPF を使用できます）。
- 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終端にあるルータの入力インターフェイスにだけ適用されます。

このような実装原理があるため、ダウンストリーム ネットワークまたは ISP からインターネットに対する他の接続がない場合でも、ユニキャスト RPF は、顧客のためだけでなく、ダウンストリーム ネットワークまたは ISP のためにもネットワーク管理者が使用できるツールになります。

注意　重みやローカル プリファレンスなど、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適なパスを変更できます。変更は、ユニキャスト RPF の動作に影響します。

ここでは、ユニキャスト RPF の実装に関する情報を説明します。

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 を展開するためのポリシーを決定する際には、次の点を考慮します。

- ユニキャスト RPF は、ネットワークの広範な部分からダウンストリームのインターフェイス（できればネットワークのエッジ）に適用する必要があります。
- ユニキャスト RPF の適用先がダウンストリームになるほど、アドレスの偽造を軽減し、偽造されたアドレスの送信元を特定するときに細かく制御できます。たとえば、ユニキャスト RPF を集約スイッチに適用すると、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。ネットワーク アクセス サーバにユニキャスト RPF を適用すると、攻撃の範囲を限定し、攻撃の送信元をトレースできますが、多くのサイトにユニキャスト RPF を配布するため、ネットワーク運用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の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多いほど、インターネット コミュニティを通じた大規模なネットワークの中断を軽減できる可能性が高くなり、攻撃の送信元をトレースできる可能性も高くなります。
- ユニキャスト RPF はトンネルでカプセル化された IP パケットを検査しません（GRE、LT2P、PPTP など）。ユニキャスト RPF はホーム ゲートウェイで設定する必要があるため、トンネリングおよびカプセル化レイヤがパケットから削除された後にのみ、ユニキャスト RPF は処理されます。

ユニキャスト RPF を使用する場所

ユニキャスト RPF は、ネットワークから出るアクセス ポイントが実質的に 1 つ（つまり、アップストリーム接続が 1 つ）のみのシングルホームの環境で使用できます。1 つのアクセス ポイントを持つネットワークは、対称ルーティングの最適な例です。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が、IP パケットの送信元に対する最適なリターン パスでもあるインターフェイスです。ユニキャスト RPF の最も一般的な使用場所は、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周辺機器、または顧客ネットワークの終端用の ISP 環境にあるネットワーク周辺機器です。

ISP に対して単一の接続ポイントを持つ企業ネットワーク

企業ネットワークでは、入力インターフェイスでトラフィックをフィルタリングする際に（*入力フィルタリング*と呼ばれるプロセス）ユニキャスト RPF を使用する 1 つの目的は、インターネットから着信した不正な形式のパケットから保護することです。従来、インターネットに対して 1 つの接続ポイントを持つローカル ネットワークは、受信インターフェイスとして ACL を使用して、偽造されたパケットがインターネットからローカル ネットワークに入らないようにしていました。

多くのシングルホームのユーザについては、ACL が役立ちますが、入力フィルタとして ACL を使用するときは、2 つの共通して参照される制約事項を含め、トレードオフがあります。

- 非常に高いパケット レートでの Packet Per Second（PPS）パフォーマンス

（注） この制限は、ソフトウェア転送パケット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（新しいアドレスがネットワークに追加されるかどうか）

ユニキャスト RPF は、これらの制約事項の両方に対処できる 1 つのツールです。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。リンクが 1 Mbps を超える場合、この処理速度は変わります。さらに、ユニキャスト RPF は FIB を使用するため、ACL のメンテナンスは必要ありません。その結果、従来の ACL のような管理コストは軽減されます。次の図と例は、入力フィルタリングのためにユニキャスト RPF を設定する方法を示します。

図 35-3 に、アップストリーム ISP に対して単一リンクがある企業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 スイッチのギガビット イーサネット インターフェイス 1/1 で適用されます。間違ったパケットが企業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 はエンタープライズ スイッチのギガビット イーサネット インターフェイス 2/1 で適用されます。

図 35-3　入力フィルタリングのためにユニキャスト RPF を使用した企業ネットワーク

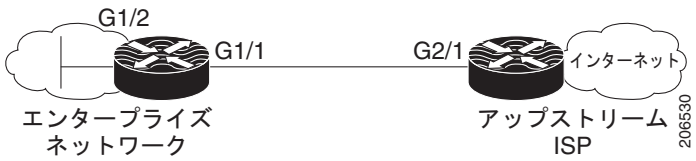


図 35-3 の関係図を使用すると、ISP スイッチの典型的な構成は（CEF が有効になっていると想定して）次のとおりです。

```
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 verify unicast source reachable-via rx allow-default
```

企業ネットワークのゲートウェイ スイッチの設定は、次のように表示されます（CEF が有効になっていると仮定します）。

```
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 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、単一のデフォルト ルートで機能します。追加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 は接続済みネットワークです。送信元アドレスが 192.168.10.0/22 の範囲内にあるインターネットからの着信パケットは、ユニキャスト RPF によってドロップされます。

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 の設定場所およびスイッチ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。たとえば、ISP 環境では、お客様向けの専用線集約スイッチであるスイッチが必要とするのは 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だけです。ユニキャスト RPF は顧客のインターフェイスで設定され、最小限のルーティング情報に関する要件が生じます。別のシナリオで、シングルホームの ISP は、インターネットに対するゲートウェイ リンクにユニキャスト RPF を配置する場合があります。フル インターネット ルーティング テーブルが必要です。ルーティング テーブル全体を必須にすることで、インターネット ルーティング テーブルに含まれないアドレスを使用する外部の DoS 攻撃から、ISP を保護できます。

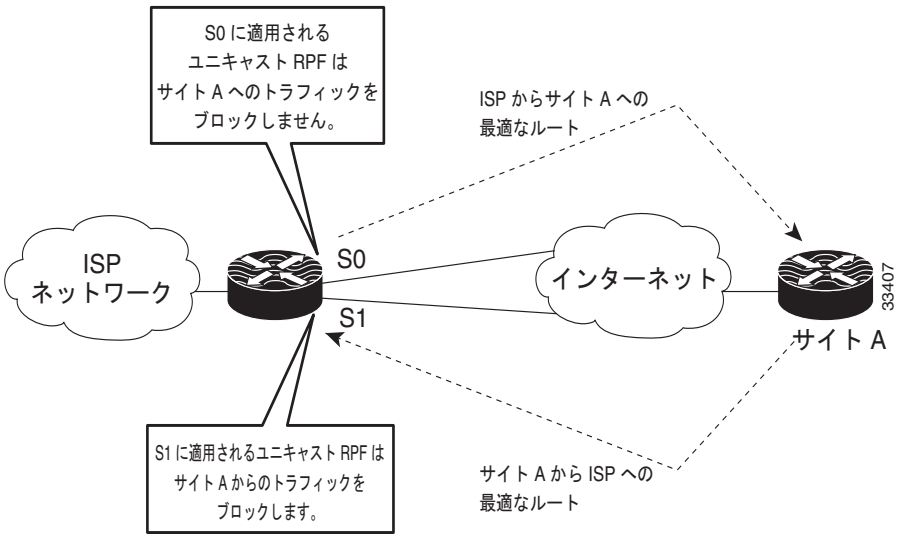
ユニキャスト RPF を使用すべきではない場所

ネットワーク内部のインターフェイスにはユニキャスト RPF を使用しないでください。内部インターフェイスは、ルーティングが非対称（図 35-4 を参照）な場合があります。つまり、パケットの送信元に対して複数のルートがあります。ユニキャスト RPF を適用するのは、もともと対称か、または対称に設定されている場合だけにしてください。管理者が、ユニキャスト RPF を有効にするインターフェイスを慎重に計画する限り、ルーティングの非対称は重大な問題にはなりません。

たとえば、ISP ネットワークのコアにあるスイッチよりも、ISP のネットワークのエッジにあるスイッチには、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設置されたスイッチでは、スイッチからの最適な転送パスがスイッチに戻るパケット用に選択されたパスであるかどうかが保証されません。ACL を使用して、スイッチ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 によって、パケットが最適ではない特定の非対称入力パスを通じて到達する場合に、ユニキャスト RPF を使用できます）。ただし、ネットワークのエッジ（ISP の場合は、ネットワークの顧客のエッジ）にのみ、ユニキャスト RPF を配置するのが最も単純です。

図 35-4 に、非対称ルーティング環境で、ユニキャスト RPF が正規のトラフィックをブロックする可能性がある場合を示します。

図 35-4　非対称ルーティング環境で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 を使用するユニキャスト RPF

ユニキャスト RPF では、0.0.0.0 の送信元と 255.255.255.255 の宛先を持つパケットを渡すことができます。そのため、Bootstrap Protocol（BOOTP）および Dynamic Host Configuration Protocol（DHCP）の関数は適切に動作します。

制約事項

マルチホーム クライアントへのユニキャスト RPF の適用に関する制約事項は、次のとおりです。

- マルチホーム接続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スイッチに対してマルチホーム接続をしないでください。
- リンクに沿って（インターネットに向けて）送信されるパケットは、リンクからアドバタイズされたルートと一致させる必要があります。一致しない場合、ユニキャスト RPF はそのパケットを不正な形式のパケットとしてフィルタします。

制限事項

ユニキャスト ルーズ モードはサポートされていません。

関連機能およびテクノロジー

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 がスイッチ上で適切に機能するにはシスコ エクスプレス フォワーディング（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は、内部ネットワークまたは外部ネットワークから送信され、ネットワーク インターフェイスで受信されたトラフィックに対してフィルタを適用します。入力フィルタリングでは、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送信元アドレスを持つ、他のネットワークまたはインターネットから着信したパケットはドロップされます。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スイッチで受信したトラフィックに適用できます。
  - 入力フィルタリングは、ネットワーク インターフェイス（送信側インターフェイス）を終了するトラフィックに対して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スイッチ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だけを許可できます。

  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。

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 アドレスの送信を軽減します（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が内部ネットワークから送信され、インターネットに到達するように許可します。その他すべての送信元アドレスは、内部ネットワークからインターネットに送信されません。
- 標準または拡張 ACL エントリを設定して、無効な送信元 IP アドレスを含む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 アドレスには次のような種類があります。
  - 予約済みアドレス
  - 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 アドレスなど）
  - 保護されたネットワークに関連付けられた有効なアドレス範囲に含まれない送信元アドレス

ユニキャスト RPF の設定作業

ここでは、ユニキャスト RPF の設定作業について説明します。一覧内の各作業は、必須と任意に分けています。

- 「ユニキャスト RPF の設定」（P.35-10）（必須）
- 「ユニキャスト RPF の確認」（P.35-10）（任意）

この章の最後にある「ユニキャスト RPF の設定例：着信および発信フィルタ」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、スイッチ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上でイネーブルになる入力側機能です。

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	`Switch(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。これは受信側インターフェイスです。ユニキャスト RPF は次の宛先にパケットを転送する前に、最適なリターン 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スイッチおよびスイッチ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 ?** コマンドを使用します。
ステップ 2	`Switch(config-if)# ip verify unicast source reachable-via rx allow-default`	インターフェイスでユニキャスト RPF をイネーブルにします。
ステップ 3	`Switch(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 と 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 が機能していることを確認するには、**show cef interface** コマンドを使用します。次に、ユニキャスト RPF がギガビット イーサネット インターフェイス 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 のモニタリングとメンテナンス

ユニキャスト RPF を監視し、保守するには、次の作業を実行します。

コマンド	目的
`Switch# 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。
`Switch(config-if)# no ip verify unicast`	インターフェイスでユニキャスト RPF をディセーブルにします。

ユニキャスト RPF は、不正な形式または偽造された送信元アドレスが原因でドロップまたは抑制されたパケットの数をカウントします。ユニキャスト RPF は、次の全体的な情報とインターフェイスごとの情報を含むドロップされたパケットまたは転送されたパケットをカウントします。

- 全体のユニキャスト RPF のドロップ
- インターフェイスごとのユニキャスト RPF のドロップ
- インターフェイスごとのユニキャスト RPF の抑制されたドロップ

show ip traffic コマンドはソフトウェアでのドロップ時に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。これにはハードウェアによってドロップされたものが含まれません。ユニキャスト RPF のドロップ数は、IP 統計情報セクションに含まれます。

```
Switch# 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数がゼロ以外の値の場合、次の 2 つのいずれかを意味する可能性があります。

- ユニキャスト RPF は、不正な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）。
- 非対称ルーティングが存在する環境でユニキャスト RPF を使用するようにルータが誤って設定されているため、ユニキャスト RPF は正規のパケットをドロップまたは抑制しています。つまり、送信元アドレスに対する最適なリターン パスとして複数のパスが存在する環境の場合です。

show ip interface コマンドを使用すると、特定のインターフェイスでドロップまたは抑制されたパケットの総数が表示されます。特定の ACL を使用するようにユニキャスト RPF が設定されている場合、ドロップの統計情報と共にその ACL の情報が表示されます。

```
Switch> show ip interface fast 2/1
```

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

show access-lists コマンドを使用すると、特定のアクセス リストの特定のエントリに見つかった一致の数が表示されます。

```
Switch> 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：着信および発信フィルタ

次の例では、ごくシンプルなシングルホームの ISP を使用して、ユニキャスト RPF と併用される入力および出力フィルタの概念について説明します。この例では、ISP が割り当てた Classless Interdomain Routing（CIDR; クラスレス ドメイン間ルーティング）ブロック 209.165.202.128/28 を示します。アップストリーム インターフェイスでインバウンドおよびアウトバウンド フィルタの両方があります。ただし、通常の ISP はシングルホームではありません。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、別のリンクを使用して戻る場合）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 rx allow-default
 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
```