



## トンネリング for IPv6 の実装

---

この章では、IPv4 だけのネットワークから、IPv4 と IPv6 ベースの統合ネットワークへの移行をサポートするために、Cisco IOS ソフトウェアで使用されるオーバーレイ トンネリング技術を設定する方法について説明します。トンネリングでは、IPv4 パケットに IPv6 パケットをカプセル化し、その IPv4 ネットワークをリンク層メカニズムとして使用します。

### 機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、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。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「[トンネリング for IPv6 の実装の機能情報](#)」(P.26) を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスしてください。Cisco.com のアカウントは必要ありません。

### 目次

- 「[トンネリング for IPv6 の実装の制約事項](#)」(P.2)
- 「[トンネリング for IPv6 の実装に関する情報](#)」(P.2)
- 「[トンネリング for IPv6 の実装方法](#)」(P.8)
- 「[トンネリング for IPv6 の実装の設定例](#)」(P.18)
- 「[その他の関連資料](#)」(P.23)
- 「[トンネリング for IPv6 の実装の機能情報](#)」(P.26)

# トンネリング for IPv6 の実装の制約事項

- Cisco IOS Release 12.0(21)ST と Cisco IOS Release 12.0(22)S および以前のリリースにおける Cisco 12000 シリーズ Gigabit Switch Router (GSR; ギガビット スイッチ ルータ) では、IPv6 トンネル化パケットの処理に非常に低いプライオリティが設定されています。このため、これらのリリースを使用する GSR では、IPv6 トンネルの使用は、ネットワーク トラフィックが低レベルに維持されており、プロセススイッチング リソースの必要性が最小限に抑えられているトポロジだけに制限することを強く推奨します。
- Cisco IOS Release 12.0(23)S における手動で設定された IPv6 トンネル トラフィックの処理は、GSR の Route Processor (RP; ルート プロセッサ) ではなく、ラインカードの CPU 上のソフトウェアで行われるため、パフォーマンスが向上します。

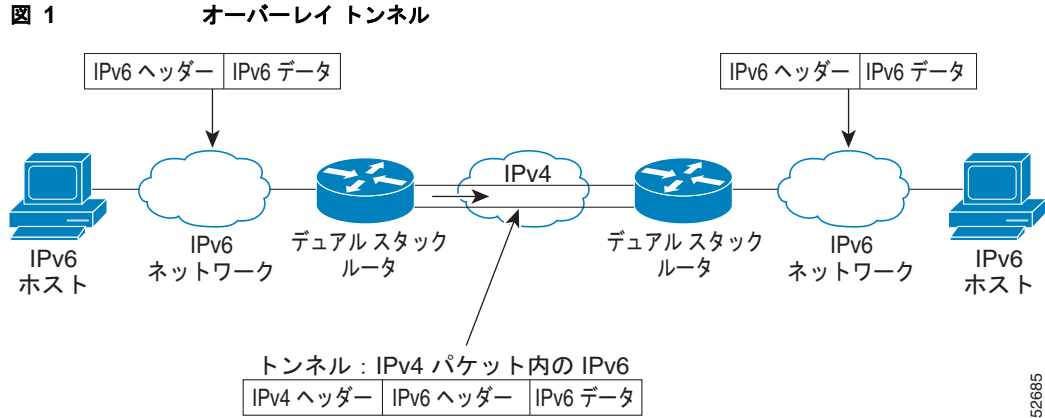
# トンネリング for IPv6 の実装に関する情報

- 「オーバーレイ トンネル for IPv6」 (P.2)
- 「手動で設定された IPv6 トンネル」 (P.4)
- 「IPv6 トラフィック用の GRE/IPv4 トンネル サポート」 (P.4)
- 「IPv6 トランスポートを介した GRE サポート」 (P.5)
- 「IPv6 を介した mGRE トンネル サポート」 (P.5)
- 「IPv4 パケットと IPv6 パケットの GRE/CLNS トンネル サポート」 (P.5)
- 「自動 6to4 トンネル」 (P.5)
- 「自動 IPv4 互換 IPv6 トンネル」 (P.6)
- 「IPv6 Rapid Deployment トンネル」 (P.6)
- 「ISATAP トンネル」 (P.6)
- 「仮想トンネル インターフェイスを使用する IPv6 IPsec サイト間保護」 (P.7)

## オーバーレイ トンネル for IPv6

オーバーレイ トンネリングでは、IPv6 パケットを IPv4 パケットにカプセル化して、IPv4 インフラストラクチャ全体（コア ネットワークまたはインターネット）に配信します（図 1 を参照）。オーバーレイ トンネルを使用することで、孤立した IPv6 ネットワークと通信できます。このとき、孤立した複数の IPv6 ネットワーク間にある IPv4 インフラストラクチャをアップグレードする必要はありません。オーバーレイ トンネルは、境界ルータ間、または境界ルータとホスト間に設定できますが、両方のエンドポイントが IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。Cisco IOS IPv6 では、次のタイプのオーバーレイ トンネリング メカニズムをサポートしています。

- 手動
- Generic Routing Encapsulation (GRE; 総称ルーティング カプセル化)
- IPv4 互換
- 6to4
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)



52685



(注)

オーバーレイ トンネルによって、インターフェイスの Maximum Transmission Unit (MTU; 最大伝送ユニット) が 20 オクテット少なくなります (IPv4 の基本パケットヘッダーにオプションフィールドが含まれていないと仮定した場合)。オーバーレイ トンネルを使用するネットワークは、トラブルシューティングが難しくなります。そのため、孤立した IPv6 ネットワークを接続するオーバーレイ トンネルを IPv6 の最終的なネットワークアーキテクチャとは考えないでください。オーバーレイ トンネルの使用は、IPv4 と IPv6 の両方のプロトコルスタック、または IPv6 プロトコルスタックだけをサポートするネットワークへの移行方法と見なす必要があります。

表 1 は、IPv4 ネットワーク上での IPv6 パケットの伝送にどのトンネルタイプを設定すればよいかを決定する場合に役立ちます。

表 1 IPv4 ネットワーク上で IPv6 パケットを伝送するトンネルタイプの推奨される使用方法

トンネリングタイプ	推奨される使用方法	使用上の注意事項
手動	サイト内、またはサイト間で使用できる単純なポイントツーポイント トンネル	IPv6 パケットだけを伝送できます。
GRE および IPv4 互換	サイト内、またはサイト間で使用できる単純なポイントツーポイント トンネル	IPv6、Connectionless Network Service (CLNS; コネクションレス型ネットワーク サービス)、およびその他の多数のタイプのパケットを伝送できます。
IPv4 互換	ポイントツーマルチポイント トンネル	::/96 プレフィクスを使用します。このトンネルタイプの使用は推奨しません。
6to4	孤立した IPv6 サイトの接続に使用できるポイントツーマルチポイント トンネル	サイトでは、2002::/16 プレフィクスからのアドレスを使用します。
ISATAP	サイト内のシステムの接続に使用できるポイントツーマルチポイント トンネル	サイトでは、任意の IPv6 ユニキャストアドレスを使用できます。

個々のトンネルタイプについて、このマニュアルで詳しく説明しています。実装する特定のトンネルタイプに関する情報を確認および理解することを推奨します。必要なトンネルタイプに精通している場合は、表 2 で、有用と思われるトンネル設定パラメータの概要を参照してください。

表 2 トンネリング タイプ別のトンネル設定パラメータ

トンネリング タイプ	トンネル設定パラメータ			
	トンネル モード	トンネルの 送信元	トンネルの宛先	インターフェイス プレフィクス またはアドレス
手動	ipv6ip	IPv4 アドレス、または IPv4 が設定されたインターフェイスへの参照。	IPv4 アドレス。	IPv6 アドレス。
GRE/IPv4	gre ip		IPv4 アドレス。	IPv6 アドレス。
IPv4 互換	ipv6ip auto-tunnel		必須ではありません。これらはすべて、ポイントツーマルチポイントのトンネリングタイプです。IPv4 宛先アドレスは、パケット単位で、IPv6 宛先から計算されます。	必須ではありません。インターフェイスアドレスは、 <code>::tunnel-source/96</code> として生成されます。
6to4	ipv6ip 6to4		IPv6 アドレス。プレフィクスには、トンネル送信元 IPv4 アドレスが埋め込まれている必要があります。	
ISATAP	ipv6ip isatap		変更された <code>eui-64</code> 形式での IPv6 プレフィクス。IPv6 アドレスは、プレフィクスおよびトンネル送信元 IPv4 アドレスから生成されます。	

## 手動で設定された IPv6 トンネル

手動で設定されたトンネルは、IPv4 バックボーンを介した 2 つの IPv6 ドメイン間の固定リンクに相当します。主に、2 つのエッジルータ間またはエンドシステムとエッジルータ間に定期的でセキュアな通信を必要とする安定した接続のために、またはリモート IPv6 ネットワークへの接続のために使用されます。

IPv6 アドレスは、トンネルインターフェイス上で手動で設定され、手動で設定された IPv4 アドレスは、トンネル送信元およびトンネル宛先に割り当てられます。設定されたトンネルの両端にあるホストまたはルータは、IPv4 プロトコルスタックと IPv6 プロトコルスタックの両方をサポートしている必要があります。手動で設定されたトンネルは、境界ルータ間または境界ルータとホスト間で設定できます。シスコ エクスプレス フォワーディング スイッチングは、手動で設定された IPv6 トンネルに使用できます。または、シスコ エクスプレス フォワーディング スイッチングは、プロセス スイッチングが必要な場合はディセーブルにできます。

## IPv6 トラフィック用の GRE/IPv4 トンネル サポート

IPv6 トラフィックは、任意の標準的なポイントツーポイント カプセル化スキームの実装に必要なサービスを提供するように設計された、標準 GRE トンネリング テクノロジーを使用する IPv4 GRE トンネル経由で伝送できます。GRE トンネルは、手動で設定された IPv6 トンネルと同様、リンクごとに個別のトンネルが設定された 2 つのポイント間のリンクです。これらのトンネルは、特定のパスセンジャまたはトランスポート プロトコルに結合されていませんが、この場合、キャリア プロトコルとして GRE を使用するパスセンジャ プロトコルとして IPv6 を伝送し、トランスポート プロトコルとして IPv4 または IPv6 を伝送します。

GRE トンネルは、2 つのエッジルータ間またはエッジルータとエンドシステム間に定期的でセキュアな通信を必要とする安定した接続のために主に使用されます。エッジルータとエンドシステムは、デュアルスタック実装である必要があります。

## IPv6 トランスポートを介した GRE サポート

GRE には、パッセンジャ プロトコルを識別するプロトコル フィールドが含まれています。GRE トンネルを使用すると、Intermediate System-to-Intermediate System (IS-IS) または IPv6 をパッセンジャ プロトコルとして指定できます。これにより、IS-IS トラフィックと IPv6 トラフィックの両方が同じトンネルを通過できます。GRE にプロトコル フィールドが含まれていない場合は、トンネルが IS-IS パケットまたは IPv6 パケットを伝送していたかどうかは識別できません。GRE 内で IS-IS および IPv6 をトンネル化するには、GRE プロトコル フィールドが必要です。

## IPv6 を介した mGRE トンネル サポート

サービス プロバイダーがコア インフラストラクチャに IPv6 を導入できるように、IPv6 を介した Multipoint Generic Routing Encapsulation (mGRE; マルチポイント総称ルーティング カプセル化) トンネルがサポートされます。Dynamic Multipoint Virtual Private Network (DMVPN) のユーザは、ローカル ネットワークで IPv4 または IPv6 のいずれかを実行できるため、オーバーレイ エンドポイントは IPv4 または IPv6 のいずれかになります。IPv6 トランスポート エンドポイントでは、オーバーレイ エンドポイントは IPv4 または IPv6 のいずれかのプライベート ネットワーク アドレスになります。IPv6 を介した DMVPN については、『[IPv6 Configuration Guide](#)』を参照してください。

GRE には、パッセンジャ プロトコルを識別するプロトコル フィールドが含まれています。GRE トンネルを使用すると、Intermediate System-to-Intermediate System (IS-IS) または IPv6 をパッセンジャ プロトコルとして指定できます。これにより、IS-IS トラフィックと IPv6 トラフィックの両方が同じトンネルを通過できます。GRE にプロトコル フィールドが含まれていない場合は、トンネルが IS-IS パケットまたは IPv6 パケットを伝送していたかどうかは識別できません。GRE 内で IS-IS および IPv6 をトンネル化するには、GRE プロトコル フィールドが必要です。

## IPv4 パケットと IPv6 パケットの GRE/CLNS トンネル サポート

CLNS ネットワークを介した IPv4 パケットと IPv6 パケットの GRE トンネリングを使用すると、Cisco CLNS Tunnel (CTunnel; CLNS トンネル) を他のベンダーのネットワーク機器と相互運用できます。この機能を使用すると、RFC 3147 に準拠できます。

ヘッダー フィールドで定義されている GRE のオプション サービス (チェックサム、キー、シーケンスなど) は、サポートされていません。これらのサービスの要求を受信したパケットはすべてドロップされます。

この機能に関する詳細については、『[Cisco IOS ISO CLNS Configuration Guide](#)』を参照してください。

## 自動 6to4 トンネル

自動 6to4 トンネルを使用すると、孤立した IPv6 ドメインを、IPv4 ネットワークを介してリモート IPv6 ネットワークに接続できます。自動 6to4 トンネルと、手動で設定されたトンネルとの主な違いは、トンネルがポイントツーポイントではなく、ポイントツーマルチポイントである点です。自動 6to4 トンネルでは、ルータは、IPv4 インフラストラクチャを仮想 NonBroadcast MultiAccess (NBMA; 非ブロードキャスト マルチアクセス) リンクとして処理するため、ペアでは設定されません。IPv6 アドレスに埋め込まれた IPv4 アドレスは、自動トンネルのもう一方のエンドを検出するために使用されます。

自動 6to4 トンネルは、孤立した IPv6 ネットワーク内の境界ルータに設定できます。これにより、IPv4 インフラストラクチャを介した別の IPv6 ネットワーク内の境界ルータへのパケット単位のトンネルが作成されます。トンネル宛先は、プレフィクス 2002::/16 で始まる IPv6 アドレス (形式は

2002:router-IPv4-address::/48) から抽出される、境界ルータの IPv4 アドレスによって決定されます。埋め込まれた IPv4 アドレスのあとには、サイト内のネットワークへの番号付けに使用できる 16 ビットが続きます。6to4 トンネルの両端の境界ルータは、IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。6to4 トンネルは、境界ルータ間または境界ルータとホスト間に設定されます。

6to4 トンネルの最も単純な展開シナリオは、複数の IPv6 サイトを相互接続することです。各 IPv6 サイトには、共有 IPv4 ネットワークへの 1 つ以上の接続があります。この IPv4 ネットワークは、グローバル インターネットまたは企業バックボーンである場合があります。主な要件は、各サイトがグローバルに一意的な IPv4 アドレスを持っていることです。Cisco IOS ソフトウェアでは、このアドレスを使用して、グローバルに一意的な 6to4/48 IPv6 プレフィクスを構成します。他のトンネリング メカニズムと同様に、ホスト名を IPv4 と IPv6 両方の IP アドレスにマッピングする Domain Name System (DNS; ドメイン ネーム システム) によって、アプリケーションは必要なアドレスを選択できます。

## 自動 IPv4 互換 IPv6 トンネル

自動 IPv4 互換トンネルでは、IPv4 互換 IPv6 アドレスを使用します。IPv4 互換 IPv6 アドレスは、アドレスの上位 96 ビットにゼロを持つ IPv6 ユニキャストアドレス、および下位 32 ビット内の IPv4 アドレスです。これらのアドレスは 0:0:0:0:A.B.C.D または ::A.B.C.D として記述できます。ここで、「A.B.C.D」は、埋め込まれた IPv4 アドレスを表します。

トンネル宛先は、IPv4 互換 IPv6 アドレスの下位 32 ビット内の IPv4 アドレスによって自動的に決定されます。IPv4 互換トンネルの両端のホストまたはルータは、IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。IPv4 互換トンネルは、境界ルータ間または境界ルータとホスト間に設定できます。IPv4 互換トンネルを使用すると、IPv6 over IPv4 トンネルを簡単に作成できますが、この技術は、大規模ネットワーク用に拡張することはできません。

## IPv6 Rapid Deployment トンネル

IPv6 Rapid Deployment (6RD) 機能は、6to4 機能を拡張したものです。6RD 機能により、サービスプロバイダーは、IPv4 による IPv6 のカプセル化を使用して、自身の IPv4 ネットワーク上でユニキャスト IPv6 サービスをお客様に提供できます。

6RD と 6to4 トンネリングの主な違いは次のとおりです。

- 6RD では、アドレスが 2002::/16 プレフィクスを持っている必要はないため、プレフィクスは、サービスプロバイダーの独自のアドレスブロックから取得できます。この機能により、6RD の操作ドメインを SP ネットワーク内にすることができます。6RD 対応サービスプロバイダー ネットワークに接続されたカスタマー サイトと一般的な IPv6 インターネットの観点からすると、提供される IPv6 サービスは、ネイティブ IPv6 と同等です。
- IPv4 宛先の 32 ビットすべてを IPv6 ペイロードヘッダーで伝送する必要はありません。IPv4 宛先は、ペイロードヘッダー内にあるビットデータとルータ上の情報を組み合わせて求められます。さらに、IPv4 アドレスは、6to4 の場合とは異なり、IPv6 ヘッダー内での位置が固定ではありません。

## ISATAP トンネル

ISATAP は、基礎となる IPv4 ネットワークを IPv6 の NBMA リンク レイヤとして使用する、自動オーバーレイ トンネリング メカニズムです。ISATAP は、ネイティブ IPv6 インフラストラクチャをまだ使用できない (希薄 IPv6 ホストがテスト用に展開されている場合など) サイト内で IPv6 パケットを転送するように設計されています。ISATAP トンネルを使用すると、サイト内の個々の IPv4 または IPv6 デュアルスタック ホストは、基本的には IPv4 インフラストラクチャを使用して IPv6 ネットワークを作成することで、同じ仮想リンク上のこうした他のホストと通信できます。

ISATAP ルータは、標準のルータ アドバタイズメント ネットワーク 設定サポートを ISATAP サイトに提供します。この機能によって、クライアントは、イーサネットに接続されている場合と同様に、クライアント自身を自動的に設定できます。また、サイト外の接続を提供するように設定することもできます。ISATAP では、リンク ローカルまたはグローバル (6to4 プレフィクスを含む) な任意のユニキャスト IPv6 プレフィクス (/64) で構成される、適切に定義された IPv6 アドレス形式を使用します。これにより、IPv6 ルーティングをローカルに、またはインターネット上で実行できます。IPv4 アドレスは、IPv6 アドレスの最後の 32 ビットに符号化され、自動 IPv6-in-IPv4 トンネリングを可能にします。

ISATAP トンネリング メカニズムは他の自動トンネリング メカニズム (IPv6 6to4 トンネリングなど) と同様ですが、ISATAP はサイト間ではなく、サイト内の IPv6 パケットを転送するよう設計されています。

ISATAP トンネリング メカニズムは、IPv6 6to4 トンネリングなどの他の自動トンネリング メカニズムと似ていますが、ISATAP は、サイト間ではなく、サイト内で IPv6 パケットを転送するように設計されています。

ISATAP では、64 ビットの IPv6 プレフィクスおよび 64 ビットのインターフェイス ID が含まれているユニキャスト アドレスを使用します。インターフェイス ID は、アドレスが IPv6 ISATAP アドレスであることを示すために最初の 32 ビットに値 000:5EFE が含まれる、変更された EUI-64 形式で作成されます。表 3、パート 1 に、ISATAP アドレス形式を示します。

表 3、パート 1 IPv6 ISATAP のアドレス形式

64 ビット	32 ビット	32 ビット
リンク ローカルまたはグローバル IPv6 ユニキャスト プレフィクス	0000:5EFE	ISATAP リンクの IPv4 アドレス

表 3、パート 1 に示すように、ISATAP アドレスは、IPv6 プレフィクスと ISATAP インターフェイス ID で構成されています。インターフェイス ID には、基礎となる IPv4 リンクの IPv4 アドレスが含まれています。次の例では、プレフィクスが 2001:DB8:1234:5678::/64 で、埋め込まれた IPv4 アドレスが 10.173.129.8 である場合、実際の ISATAP アドレスがどのようになるかを示します。ISATAP アドレスでは、IPv4 アドレスは、0AAD:8108 の 16 進 (たとえば、2001:DB8:1234:5678:0000:5EFE:0AAD:8108) で表されます。

## 仮想トンネル インターフェイスを使用する IPv6 IPsec サイト間保護

IPv6 IPsec 機能では、ネイティブ IPsec IPv6 カプセル化を使用して、すべてのタイプの IPv6 ユニキャストおよびマルチキャストトラフィックのサイト間 IPv6 暗号保護を提供します。IPsec Virtual Tunnel Interface (VTI; 仮想トンネル インターフェイス) 機能では、IKE を管理プロトコルとして使用することでこれを実現します。

IPsec VTI では、ネイティブ IPsec トンネリングがサポートされ、物理インターフェイスの大半のプロパティが含まれています。IPsec VTI によって、複数のインターフェイスにクリプト マップを適用する必要性が軽減され、ルーティング可能なインターフェイスが提供されます。

IPsec VTI を使用すると、IPv6 ルータは、セキュリティ ゲートウェイとして機能し、他のセキュリティ ゲートウェイ ルータとの IPsec トンネルを確立し、パブリック IPv6 インターネット経由で送信される内部ネットワークのトラフィックに IPsec 暗号保護を提供できます。

VTI の詳細については、「[Implementing IPsec in IPv6 Security](#)」を参照してください。

# トンネリング for IPv6 の実装方法

- 「手動 IPv6 トンネルの設定」 (P.8)
- 「GRE IPv6 トンネルの設定」 (P.9)
- 「自動 6to4 トンネルの設定」 (P.11)
- 「IPv4 互換 IPv6 トンネルの設定」 (P.13)
- 「6RD トンネルの設定」 (P.14)
- 「ISATAP トンネルの設定」 (P.15)
- 「IPv6 トンネルの設定と動作の確認」 (P.16)

## 手動 IPv6 トンネルの設定

手動 IPv6 トンネルを設定するには、次の作業を実行します。

### 前提条件

手動で設定された IPv6 トンネルでは、IPv6 アドレスは、トンネルインターフェイス上で設定され、手動で設定された IPv4 アドレスは、トンネル送信元およびトンネル宛先に割り当てられます。設定されたトンネルの両端にあるホストまたはルータは、IPv4 プロトコルスタックと IPv6 プロトコルスタックの両方をサポートしている必要があります。

### 手順の概要

1. `enable`
2. `configure terminal`
3. `interface tunnel tunnel-number`
4. `ipv6 address ipv6-prefix/prefix-length [eui-64]`
5. `tunnel source {ip-address | interface-type interface-number}`
6. `tunnel destination ip-address`
7. `tunnel mode ipv6ip`
8. `end`

### 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>enable</code>  例： Router> enable	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ2	<code>configure terminal</code>  例： Router# 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。



	コマンドまたはアクション	目的
ステップ3	<code>interface tunnel tunnel-number</code>  例： Router(config)# interface tunnel 0	トンネル インターフェイスと番号を指定し、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	<code>ipv6 address ipv6-prefix/prefix-length [eui-64]</code>  例： Router(config-if)# ipv6 address 3ffe:b00:c18:1::3/127	インターフェイスに割り当てられている IPv6 ネットワークを指定し、インターフェイスで IPv6 処理をイネーブルにします。
ステップ5	<code>tunnel source {ip-address   interface-type interface-number}</code>  例： Router(config-if)# tunnel source ethernet 0	トンネル インターフェイスの送信元 IPv4 アドレスまたは送信元インターフェイス タイプと番号を指定します。  • インターフェイスが指定されている場合、そのインターフェイスは IPv4 アドレスを使用して設定されている必要があります。
ステップ6	<code>tunnel destination ip-address</code>  例： Router(config-if)# tunnel destination 192.168.30.1	トンネル インターフェイスの宛先 IPv4 アドレスまたはホスト名を指定します。
ステップ7	<code>tunnel mode ipv6ip</code>  例： Router(config-if)# tunnel mode ipv6ip	手動 IPv6 トンネルを指定します。  (注) <code>tunnel mode ipv6ip</code> コマンドでは、IPv6 をパセージャ プロトコルとして指定し、IPv4 を手動 IPv6 トンネル用のカプセル化プロトコルおよびトランスポート プロトコルの両方として指定します。

## GRE IPv6 トンネルの設定

IPv6 ネットワーク上で GRE トンネルを設定するには、次の作業を実行します。GRE トンネルは、IPv6 ネットワーク レイヤ上で実行し、IPv6 トンネルの IPv6 パケットおよび IPv6 トンネルの IPv4 パケットを転送するように設定できます。

### 前提条件

GRE IPv6 トンネルが設定されている場合、IPv6 アドレスは、トンネル送信元およびトンネル宛先に割り当てられます。トンネル インターフェイスは、割り当て済みの IPv4 アドレスまたは IPv6 アドレスを持つことができます（ここでは説明していません）。設定されたトンネルの両端にあるホストまたはルータは、IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。

### 手順の概要

1. `enable`
2. `configure terminal`
3. `interface tunnel tunnel-number`
4. `ipv6 address ipv6-prefix/prefix-length [eui-64]`

5. **tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*}
6. **tunnel destination** {*host-name* | *ip-address* | *ipv6-address*}
7. **tunnel mode** {*aurp* | *cayman* | *dvmrp* | *eon* | *gre* | *gre multipoint* | *gre ipv6* | *ipip* | *decapsulate-any* | *iptalk* | *ipv6* | *mpls* | *nos*}
8. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<b>enable</b>  例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"><li>必要に応じてパスワードを入力します。</li></ul>
ステップ2	<b>configure terminal</b>  例： Router# 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	<b>interface tunnel tunnel-number</b>  例： Router(config)# interface tunnel 0	トンネル インターフェイスおよび番号を指定し、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	<b>ipv6 address ipv6-prefix/prefix-length [eui-64]</b>  例： Router(config-if)# ipv6 address 3ffe:b00:c18:1::3/127	インターフェイスに割り当てられている IPv6 ネットワークを指定し、インターフェイスでの IPv6 処理をイネーブルにします。
ステップ5	<b>tunnel source</b> { <i>ip-address</i>   <i>ipv6-address</i>   <i>interface-type interface-number</i> }  例： Router(config-if)# tunnel source ethernet 0	トンネル インターフェイスの送信元 IPv4 アドレスまたは送信元インターフェイス タイプと番号を指定します。 <ul style="list-style-type: none"><li>インターフェイスが指定されている場合、そのインターフェイスは IPv4 アドレスを使用して設定されている必要があります。</li></ul>
ステップ6	<b>tunnel destination</b> { <i>host-name</i>   <i>ip-address</i>   <i>ipv6-address</i> }  例： Router(config-if)# tunnel destination 2001:DB8:1111:2222::1/64	宛先 IPv6 アドレスまたはトンネル インターフェイスのホスト名を指定します。
ステップ7	<b>tunnel mode</b> { <i>aurp</i>   <i>cayman</i>   <i>dvmrp</i>   <i>eon</i>   <i>gre</i>   <i>gre multipoint</i>   <i>gre ipv6</i>   <i>ipip</i>   <i>decapsulate-any</i>   <i>iptalk</i>   <i>ipv6</i>   <i>mpls</i>   <i>nos</i> }  例： Router(config-if)# tunnel mode gre ipv6	GRE IPv6 トンネルを指定します。 <b>(注)</b> <b>tunnel mode gre ipv6</b> コマンドでは、GRE をトンネルのカプセル化プロトコルとして指定します。

## 自動 6to4 トンネルの設定

自動 6to4 トンネルを設定するには、次の作業を実行します。

### 前提条件

6to4 トンネルでは、トンネル宛先は、2002: *border-router-IPv4-address*::/48 形式でプレフィクス 2002::/16 に連結される、境界ルータ IPv4 アドレスによって決まります。6to4 トンネルの両端の境界ルータは、IPv4 プロトコルスタックと IPv6 プロトコルスタックの両方をサポートしている必要があります。

### 制約事項

IPv4 互換トンネル 1 つだけの設定、および 6to4 IPv6 トンネル 1 つだけの設定が、1 台のルータ上でサポートされます。同じルータ上でこれら両方のトンネルタイプを設定する場合は、これらのタイプが同じトンネル送信元を共有しないようにすることを強く推奨します。

6to4 トンネルと IPv4 互換トンネルがインターフェイスを共有できない理由は、両方が NBMA 「ポイントツーマルチポイント」アクセスリンクであり、多重化パケットストリームからのパケットを着信インターフェイスの単一パケットストリームに整理するにはトンネル送信元だけを使用できる点です。したがって、IPv4 プロトコルタイプが 41 のパケットがインターフェイスに到着すると、このパケットは IPv4 アドレスに基づいて、IPv6 トンネルインターフェイスにマッピングされます。ただし、6to4 トンネルと IPv4 互換トンネルの両方が同じ送信元インターフェイスを共有する場合、ルータは、着信パケットの割り当て先となる IPv6 トンネルインターフェイスを特定できません。

手動で設定された IPv6 トンネルの場合、手動トンネルは「ポイントツーポイント」リンクであり、トンネルの IPv4 送信元と IPv4 宛先が両方とも定義されているため、同じ送信元インターフェイスを共有できます。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel *tunnel-number***
4. **ipv6 address *ipv6-prefix/prefix-length* [eui-64]**
5. **tunnel source {*ip-address* | *interface-type interface-number*}**
6. **tunnel mode ipv6ip 6to4**
7. **exit**
8. **ipv6 route *ipv6-prefix/prefix-length* tunnel *tunnel-number***
9. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>enable</code>  例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"><li>必要に応じてパスワードを入力します。</li></ul>
ステップ2	<code>configure terminal</code>  例： Router# 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	<code>interface tunnel tunnel-number</code>  例： Router(config)# interface tunnel 0	トンネル インターフェイスおよび番号を指定し、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	<code>ipv6 address ipv6-prefix/prefix-length [eui-64]</code>  例： Router(config-if)# ipv6 address 2002:c0a8:6301:1::1/64	インターフェイスに割り当てられた IPv6 アドレスを指定し、インターフェイスでの IPv6 処理をイネーブルにします。 <ul style="list-style-type: none"><li>最初の 2002::/16 プレフィクスに続く 32 ビットは、トンネル送信元に割り当てられた IPv4 アドレスに対応します。</li></ul>
ステップ5	<code>tunnel source {ip-address   interface-type interface-number}</code>  例： Router(config-if)# tunnel source ethernet 0	トンネル インターフェイスの送信元インターフェイスのタイプおよび番号を指定します。 <b>(注)</b> <code>tunnel source</code> コマンドで指定したインターフェイスのタイプおよび番号は、IPv4 アドレスを使用して設定する必要があります。
ステップ6	<code>tunnel mode ipv6ip 6to4</code>  例： Router(config-if)# tunnel mode ipv6ip 6to4	6to4 アドレスを使用する IPv6 オーバーレイ トンネルを指定します。
ステップ7	<code>exit</code>  例： 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、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ8	<code>ipv6 route ipv6-prefix/prefix-length tunnel tunnel-number</code>  例： Router(config)# ipv6 route 2002::/16 tunnel 0	指定したトンネル インターフェイスに IPv6 6to4 プレフィクス 2002::/16 のスタティック ルートを設定します。 <b>(注)</b> 6to4 オーバーレイ トンネルを設定する場合は、6to4 トンネル インターフェイスに IPv6 6to4 プレフィクス 2002::/16 のスタティック ルートを設定する必要があります。 <ul style="list-style-type: none"><li><code>ipv6 route</code> コマンドで指定したトンネル番号は、<code>interface tunnel</code> コマンドで指定したトンネル番号と同じである必要があります。</li></ul>

## IPv4 互換 IPv6 トンネルの設定

IPv4 互換 IPv6 トンネルを設定するには、次の作業を実行します。

### 前提条件

IPv4 互換トンネルでは、トンネル宛先は、IPv4 互換 IPv6 アドレスの下位 32 ビット内の IPv4 アドレスによって自動的に決定されます。IPv4 互換トンネルの両端のホストまたはルータは、IPv4 プロトコルスタックと IPv6 プロトコルスタックの両方をサポートしている必要があります。

### 手順の概要

1. `enable`
2. `configure terminal`
3. `interface tunnel tunnel-number`
4. `tunnel source {ip-address | interface-type interface-number}`
5. `tunnel mode ipv6ip auto-tunnel`
6. `end`

### 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>enable</code>  例： Router> enable	特権 EXEC モードをイネーブルにします。  • 必要に応じてパスワードを入力します。
ステップ2	<code>configure terminal</code>  例： Router# 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	<code>interface tunnel tunnel-number</code>  例： Router(config)# interface tunnel 0	トンネル インターフェイスおよび番号を指定し、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	<code>tunnel source {ip-address   interface-type interface-number}</code>  例： Router(config-if)# tunnel source ethernet 0	トンネル インターフェイスの送信元インターフェイスのタイプおよび番号を指定します。  (注) <code>tunnel source</code> コマンドで指定されたインターフェイスのタイプおよび番号は、IPv4 アドレスだけを使用して設定されています。
ステップ5	<code>tunnel mode ipv6ip auto-tunnel</code>  例： Router(config-if)# tunnel mode ipv6ip auto-tunnel	IPv4 互換 IPv6 アドレスを使用して IPv4 互換トンネルを指定します。

## 6RD トンネルの設定

6RD トンネルを設定するには、次の作業を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel *tunnel-number***
4. **tunnel source {ip-address | interface-type interface-number}**
5. **tunnel mode ipv6ip [6rd | 6to4 | auto-tunnel | isatap]**
6. **tunnel 6rd prefix *ipv6-prefix/prefix-length***
7. **tunnel 6rd ipv4 {prefix-length *length* | suffix-length *length*}**
8. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<b>enable</b>  例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"><li>プロンプトが表示されたら、パスワードを入力します。</li></ul>
ステップ2	<b>configure terminal</b>  例： Router# 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	<b>interface tunnel <i>tunnel-number</i></b>  例： Router(config)# interface tunnel 1	トンネル インターフェイスおよび番号を指定し、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	<b>tunnel source {ip-address   interface-type interface-number}</b>  例： Router(config-if)# tunnel source Ethernet2/0	トンネル インターフェイスの送信元インターフェイスのタイプおよび番号を指定します。
ステップ5	<b>tunnel mode ipv6ip [6rd   6to4   auto-tunnel   isatap]</b>  例： Router(config-if)# tunnel mode ipv6ip 6rd	スタティック IPv6 トンネル インターフェイスを設定します。
ステップ6	<b>tunnel 6rd prefix <i>ipv6-prefix/prefix-length</i></b>  例： Router(config-if)# tunnel 6rd prefix 2001:B000::/32	IPv6 rapid 6RD トンネル上で共通の IPv6 プレフィックスを指定します。

	コマンドまたはアクション	目的
ステップ1	<pre>tunnel 6rd ipv4 {prefix-length length} {suffix-length length}</pre> <p>例:</p> <pre>Router(config-if)# tunnel 6rd ipv4 prefix-length 16 suffix 8</pre>	ドメイン内のすべての 6RD ルータに共通の IPv4 トランスポートアドレスのプレフィクス長およびサフィクス長を指定します。

## ISATAP トンネルの設定

ISATAP トンネルを設定するには、次の作業を実行します。

### 前提条件

ISATAP トンネルの設定で使用される **tunnel source** コマンドは、設定済みの IPv4 アドレスを持つインターフェイスをポイントする必要があります。アドバタイズされた ISATAP IPv6 アドレスおよび (1 つまたは複数の) プレフィクスは、ネイティブ IPv6 インターフェイス用として設定されます。IPv6 トンネル インターフェイスは、インターフェイス ID 内の最後の 32 ビットが IPv4 トンネル送信元アドレスを使用して作成されているため、変更された EUI-64 アドレスを使用して設定されている必要があります。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel tunnel-number**
4. **ipv6 address ipv6-prefix/prefix-length [eui-64]**
5. **no ipv6 nd ra suppress**
6. **tunnel source {ip-address | interface-type interface-number}**
7. **tunnel mode ipv6ip isatap**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<pre>enable</pre> <p>例:</p> <pre>Router&gt; enable</pre>	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> <li>• 必要に応じてパスワードを入力します。</li> </ul>
ステップ2	<pre>configure terminal</pre> <p>例:</p> <pre>Router# configure terminal</pre>	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	<pre>interface tunnel tunnel-number</pre> <p>例:</p> <pre>Router(config)# interface tunnel 1</pre>	トンネル インターフェイスおよび番号を指定し、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。

	コマンドまたはアクション	目的
ステップ4	<pre>ipv6 address ipv6-prefix/prefix-length [eui-64]</pre> <p>例： Router(config-if)# ipv6 address 2001:DB8:6301::/64 eui-64</p>	<p>インターフェイスに割り当てられた IPv6 アドレスを指定し、インターフェイスでの IPv6 処理をイネーブルにします。</p> <p>(注) IPv6 アドレスの設定の詳細については、「<i>Configuring Basic Connectivity for IPv6</i>」の章を参照してください。</p>
ステップ5	<pre>no ipv6 nd ra suppress</pre> <p>例： Router(config-if)# no ipv6 nd ra suppress</p>	<p>IPv6 ルータ アドバタイズメントの送信は、トンネルインターフェイス上ではデフォルトでディセーブルになっています。このコマンドによって、IPv6 ルータ アドバタイズメントの送信が再度イネーブルになり、クライアントの自動設定が可能になります。</p>
ステップ6	<pre>tunnel source {ip-address   interface-type interface-number}</pre> <p>例： Router(config-if)# tunnel source ethernet 1/0/1</p>	<p>トンネルインターフェイスの送信元インターフェイスのタイプおよび番号を指定します。</p> <p>(注) <b>tunnel source</b> コマンドで指定したインターフェイスのタイプおよび番号は、IPv4 アドレスを使用して設定する必要があります。</p>
ステップ7	<pre>tunnel mode ipv6ip isatap</pre> <p>例： Router(config-if)# tunnel mode ipv6ip isatap</p>	<p>ISATAP アドレスを使用する IPv6 オーバーレイ トンネルを指定します。</p>

## IPv6 トンネルの設定と動作の確認

IPv6 トンネルの設定と動作を確認するには、次の作業を実行します。

### 手順の概要

1. **enable**
2. **show interfaces tunnel number [accounting]**
3. **ping [protocol] destination**
4. **show ip route [address [mask]]**
5. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<pre>enable</pre> <p>例： Router&gt; enable</p>	<p>特権 EXEC モードをイネーブルにします。</p> <ul style="list-style-type: none"> <li>• 必要に応じてパスワードを入力します。</li> </ul>
ステップ2	<pre>show interfaces tunnel number [accounting]</pre> <p>例： Router# show interfaces tunnel 0</p>	<p>(任意) トンネルインターフェイス情報を表示します。</p> <ul style="list-style-type: none"> <li>• <i>number</i> 引数を使用して、指定したトンネルの情報を表示します。</li> </ul>



	コマンドまたはアクション	目的
ステップ3	<code>ping [protocol] destination</code>  例： Router# ping 10.0.0.1	(任意) 基本的なネットワーク接続を診断します。
ステップ4	<code>show ip route [address [mask]]</code>  例： Router# show ip route 10.0.0.2	(任意) ルーティング テーブルの現在の状態を表示します。  (注) この作業に関係のある構文だけを示しています。

## 例

- [Sample Output from the show interfaces tunnel Command](#)
- 「ping コマンドの出力例」
- 「show ip route コマンドの出力例」
- 「ping コマンドの出力例」

### ping コマンドからリモート エンドポイント アドレスを確認するための出力例

この例は、手動で設定された IPv6 トンネルと IPv6 over IPv4 GRE トンネルの両方に適した一般的な例です。この例では、2 台のルータがトンネルのエンドポイントとして設定されています。ルータ A は、IPv4 アドレス 10.0.0.1 および IPv6 プレフィクス 2001:DB8:1111:2222::1/64 を含むトンネル インターフェイス 0 として設定されたイーサネット インターフェイス 0/0 を持ちます。ルータ B は、IPv4 アドレス 10.0.0.2 および IPv6 プレフィクス 2001:DB8:1111:2222::2/64 を含むトンネル インターフェイス 1 として設定されたイーサネット インターフェイス 0/0 を持ちます。トンネル送信元およびトンネル宛先のアドレスが設定されていることを確認するには、**show interfaces tunnel** コマンドをルータ A で使用します。

```
RouterA# show interfaces tunnel 0

Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.0.0.1 (Ethernet0/0), destination 10.0.0.2, fastswitch TTL 255
  Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
  Tunnel TTL 255
  Checksumming of packets disabled, fast tunneling enabled
  Last input 00:00:14, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    4 packets input, 352 bytes, 0 no buffer
      Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    8 packets output, 704 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

### ping コマンドの出力例

ローカル エンドポイントが設定され、機能していることを確認するには、**ping** コマンドをルータ A で使用します。

```
RouterA# ping 2001:DB8:1111:2222::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1111:2222::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms
```

### show ip route コマンドの出力例

リモート エンドポイント アドレスへのルートが存在することを確認するには、**show ip route** コマンドを次のように使用します。

```
RouterA# show ip route 10.0.0.2

Routing entry for 10.0.0.0/24
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
    * directly connected, via Ethernet0/0
      Route metric is 0, traffic share count is 1
```

### ping コマンドの出力例

リモート エンドポイント アドレスに到着できることを確認するには、**ping** コマンドをルータ A で使用します。



(注)

---

フィルタリングが原因で、**ping** コマンドを使用してリモート エンドポイント アドレスに到着できない場合がありますが、トンネル トラフィックは依然としてその宛先に到着している場合があります。

---

```
RouterA# ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/28 ms
```

リモート IPv6 トンネル エンドポイントが到着可能であることを確認するには、ルータ A で **ping** コマンドを再び使用します。フィルタリングに関する同じ注意事項がこの例にも当てはまります。

```
RouterA# ping 1::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms
```

これらの手順は、トンネルのもう一方のエンドポイントで繰り返すことができます。

## トンネリング for IPv6 の実装の設定例

- 「例：手動 IPv6 トンネルの設定」(P.19)
- 「例：GRE トンネルの設定」(P.19)
- 「例：CLNS で IPv6 パケットを伝送するように GRE モードで CTunnel を設定」(P.20)

- 「例：6to4 トンネルの設定」(P.21)
- 「例：IPv4 互換 IPv6 トンネルの設定」(P.22)
- 「例：6RD トンネルの設定」(P.23)
- 「例：ISATAP トンネルの設定」(P.23)

## 例：手動 IPv6 トンネルの設定

ルータ A とルータ B 間で手動 IPv6 トンネルを設定する例を次に示します。例では、ルータ A とルータ B の両方のトンネル インターフェイス 0 は、グローバル IPv6 アドレスを使用して手動で設定されています。トンネル送信元およびトンネル宛先のアドレスについても、手動で設定されます。

### ルータ A の設定

```
interface ethernet 0
 ip address 192.168.99.1 255.255.255.0

interface tunnel 0
 ipv6 address 3ffe:b00:c18:1::3/127
 tunnel source ethernet 0
 tunnel destination 192.168.30.1
 tunnel mode ipv6ip
```

### ルータ B の設定

```
interface ethernet 0
 ip address 192.168.30.1 255.255.255.0

interface tunnel 0
 ipv6 address 3ffe:b00:c18:1::2/127
 tunnel source ethernet 0
 tunnel destination 192.168.99.1
 tunnel mode ipv6ip
```

## 例：GRE トンネルの設定

- 「例：IS-IS および IPv6 トラフィックを実行する GRE トンネル」(P.19)
- 「例：IPv6 トンネルのトンネル宛先アドレス」(P.20)

## 例：IS-IS および IPv6 トラフィックを実行する GRE トンネル

次に、ルータ A とルータ B との間で IS-IS および IPv6 トラフィックをともに送出する GRE トンネルを設定する例を示します。

### ルータ A の設定

```
ipv6 unicast-routing
 clns routing
 !
interface tunnel 0
 no ip address
 ipv6 address 3ffe:b00:c18:1::3/127
 ipv6 router isis
 tunnel source Ethernet 0/0
 tunnel destination 2001:DB8:1111:2222::1/64
 tunnel mode gre ipv6
```

```
!
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0
!
router isis
 net 49.0000.0000.000a.00
```

### ルータ B の設定

```
ipv6 unicast-routing
clns routing
!
interface tunnel 0
 no ip address
 ipv6 address 3ffe:b00:c18:1::2/127
 ipv6 router isis
 tunnel source Ethernet 0/0
 tunnel destination 2001:DB8:1111:2222::2/64
 tunnel mode gre ipv6
!
interface Ethernet0/0
 ip address 10.0.0.2 255.255.255.0
!
router isis
 net 49.0000.0000.000b.00
 address-family ipv6
 redistribute static
 exit-address-family
```

## 例 : IPv6 トンネルのトンネル宛先アドレス

次の例では、IPv6 パケットの GRE トンネリングのトンネル宛先アドレスを設定する方法について説明します。

```
Router(config)# interface Tunnel0
Router(config-if)# no ip address
Router(config-if)# ipv6 router isis
Router(config-if)# tunnel source Ethernet 0/0
Router(config-if)# tunnel destination 2001:DB8:1111:2222::1/64
Router(config-if)# tunnel mode gre ipv6
Router(config-if)# exit
!
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# exit
!
Router(config)# ipv6 unicast-routing

Router(config)# router isis
Router(config)# net 49.0000.0000.000a.00
```

## 例 : CLNS で IPv6 パケットを伝送するように GRE モードで CTunnel を設定

CLNS ネットワーク内のルータ A とルータ B 間で IS-IS および IPv6 トラフィックをともに送受する GRE CTunnel を設定する例を次に示します。 **ctunnel mode gre** コマンドによって、シスコのネットワーク デバイスとサードパーティのネットワーク デバイス間のトンネリングが可能になり、IPv4 と IPv6 の両方のトラフィックを伝送できます。

**ctunnel mode gre** コマンドにより、RFC 3147 に準拠したトンネリング方法が提供され、シスコの機器とサードパーティ製ネットワークング デバイス間のトンネリングが許可されます。

### ルータ A

```
ipv6 unicast-routing

clns routing

interface ctunnel 102

    ipv6 address 2001:DB8:1111:2222::1/64
    ctunnel destination 49.0001.2222.2222.2222.00
    ctunnel mode gre

interface Ethernet0/1
    clns router isis

router isis
    net 49.0001.1111.1111.1111.00
```

### ルータ B

```
ipv6 unicast-routing

clns routing

interface ctunnel 201
    ipv6 address 2001:DB8:1111:2222::2/64
    ctunnel destination 49.0001.1111.1111.1111.00
    ctunnel mode gre

interface Ethernet0/1
    clns router isis

router isis
    net 49.0001.2222.2222.2222.00
```

シスコ機器のエンドポイント間で GRE モードをオフにして、CTunnel をデフォルトのシスコ カプセル化ルーティングのみに戻すには、**no ctunnel mode** コマンドまたは **ctunnel mode cisco** コマンドのいずれかを使用します。次の例では、IPv4 トラフィックだけを転送するように変更された同じ設定を示します。

## 例 : 6to4 トンネルの設定

次の例では、孤立した IPv6 ネットワーク内の境界ルータ上に 6to4 トンネルを設定します。IPv4 アドレスは 192.168.99.1 であり、IPv6 プレフィクス 2002:c0a8:6301::/48 に変換されます。IPv6 プレフィクスは、トンネルインターフェイス用として 2002:c0a8:6301::/64 にサブネット化されます。つまり、最初の IPv6 ネットワークは 2002:c0a8:6301:1::/64、2 番目の IPv6 ネットワークは 2002:c0a8:6301:2::/64 になります。スタティック ルートによって、IPv6 プレフィクス 2002::/16 のその他のすべてのトラフィックは、自動トンネリングのためにトンネルインターフェイス 0 に送信されます。

```
interface Ethernet0
    description IPv4 uplink
    ip address 192.168.99.1 255.255.255.0
    !
interface Ethernet1
```

```

description IPv6 local network 1
ipv6 address 2002:c0a8:6301:1::1/64
!
interface Ethernet2
description IPv6 local network 2
ipv6 address 2002:c0a8:6301:2::1/64
!
interface Tunnel0
description IPv6 uplink
no ip address
ipv6 address 2002:c0a8:6301::1/64
tunnel source Ethernet 0
tunnel mode ipv6ip 6to4
!
ipv6 route 2002::/16 tunnel 0

```

## 例：IPv4 互換 IPv6 トンネルの設定

次の例では、手動トンネルのメッシュを設定することなく、複数のルータ間で **Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル)** を実行できるようにする **IPv4 互換 IPv6 トンネル** を設定します。各ルータには単一の **IPv4 互換トンネル** があり、複数の **BGP セッション** を（各ネイバーへの）各トンネル上で実行できます。イーサネット インターフェイス **0** は、トンネル送信元として使用されます。トンネル宛先は、**IPv4 互換 IPv6 アドレス** の下位 **32 ビット** 内の **IPv4 アドレス** によって自動的に決定されます。特に、**IPv6 プレフィクス 0:0:0:0:0:0** は、**IPv4 アドレス (0:0:0:0:0:A.B.C.D または ::A.B.C.D の形式)** に連結されて、**IPv4 互換 IPv6 アドレス** が作成されます。イーサネット インターフェイス **0** は、**グローバル IPv6 アドレス** および **IPv4 アドレス** を使用して設定されています（このインターフェイスでは、**IPv6 プロトコル スタック** と **IPv4 プロトコル スタック** の両方がサポートされています）。

この例ではマルチプロトコル **BGP** を使用して、**IPv6 到着可能情報** をピア **10.67.0.2** と交換しています。イーサネット インターフェイス **0** の **IPv4 アドレス** は、**IPv4 互換 IPv6 アドレス** の下位 **32 ビット** で使用されており、**ネクストホップ属性** としても使用されています。**BGP ネイバーの IPv4 互換 IPv6 アドレス** を使用すると、**IPv4 互換トンネル** を介して **IPv6 BGP セッション** を自動的に転送できます。

```

interface tunnel 0
tunnel source Ethernet 0
tunnel mode ipv6ip auto-tunnel

interface ethernet 0
ip address 10.27.0.1 255.255.255.0
ipv6 address 3000:2222::1/64

router bgp 65000
no synchronization
no bgp default ipv4-unicast
neighbor ::10.67.0.2 remote-as 65002

address-family ipv6
neighbor ::10.67.0.2 activate
neighbor ::10.67.0.2 next-hop-self
network 2001:2222:d00d:b10b::/64

```

## 例：6RD トンネルの設定

次の例では、6RD トンネルの実行コンフィギュレーションとそれに対応する **show tunnel 6rd** コマンドの出力を示します。

```
interface Tunnell
  ipv6 address 2001:B000:100::1/32
  tunnel source Ethernet2/1
  tunnel mode ipv6ip 6rd
  tunnel 6rd prefix 2001:B000::/32
  tunnel 6rd ipv4 prefix-len 16 suffix-len 8
end

Router# show tunnel 6rd tunnel 1

Interface Tunnell:
  Tunnel Source: 10.1.1.1
  6RD: Operational, V6 Prefix: 2001:B000::/32
      V4 Common Prefix Length: 16, Value: 10.1.0.0
      V4 Common Suffix Length: 8, Value: 0.0.0.1
```

## 例：ISATAP トンネルの設定

次の例では、イーサネット 0 で定義されたトンネル送信元、および ISATAP トンネルの設定に使用する **tunnel mode** コマンドを示します。クライアントの自動設定を可能にするために、ルータ アドバタ イズメントがイネーブルになっています。

```
ipv6 unicast-routing
interface tunnel 1
  tunnel source ethernet 0
  tunnel mode ipv6ip isatap
  ipv6 address 2001:DB8::/64 eui-64
  no ipv6 nd ra suppress
exit
```

## その他の関連資料

### 関連資料

関連項目	参照先
IPsec VTI	<a href="#">「Implementing IPsec in IPv6 Security」</a>
IPv6 のサポート機能リスト	<a href="#">「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」</a>
CLNS トンネル	<a href="#">『Cisco IOS ISO CLNS Configuration Guide』</a>
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	<a href="#">『Cisco IOS IPv6 Command Reference』</a>

## 規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

## MIB

MIB	MIB リンク
なし	<p>選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索し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。</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFC

RFC	タイトル
RFC 2473	『 <i>Generic Packet Tunneling in IPv6 Specification</i> 』
RFC 2893	『 <i>Transition Mechanisms for IPv6 Hosts and Routers</i> 』
RFC 3056	『 <i>Connection of IPv6 Domains via IPv4 Clouds</i> 』
RFC 4214	『 <i>Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)</i> 』



## シスコのテクニカル サポート

説明	リンク
<p>右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。</p> <p>以下を含むさまざまな作業にこの Web サイトが役立ちます。</p> <ul style="list-style-type: none"><li>・テクニカル サポートを受ける</li><li>・ソフトウェアをダウンロードする</li><li>・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける</li><li>・ツールおよびリソースへアクセスする<ul style="list-style-type: none"><li>- Product Alert の受信登録</li><li>- Field Notice の受信登録</li><li>- Bug Toolkit を使用した既知の問題の検索</li></ul></li><li>・Networking Professionals (NetPro) コミュニティで、技術関連のディスカッションに参加する</li><li>・トレーニング リソースへアクセスする</li><li>・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する</li></ul> <p>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。</p>	<p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p>

# トンネリング for IPv6 の実装の機能情報

表 4 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア 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 により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。



(注) 表 4 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。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。

表 4 トンネリング for IPv6 の実装の機能情報

機能名	リリース	機能情報
6to4 トンネルの CEFv6 スイッチング	12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(18)SXE 12.2(12)T 12.4 15.0(1)S	シスコ エクスプレス フォワーディング スイッチングは、手動で設定された IPv6 トンネルに使用できます。 この機能に関する詳細については、次の各項を参照してください。 <ul style="list-style-type: none"> <li>「手動で設定された IPv6 トンネル」 (P.4)</li> </ul>
IPv6 トンネリング : 6RD IPv6 Rapid Deployment	15.1(3)T	6RD 機能により、サービス プロバイダーは、IPv4 による IPv6 のカプセル化を使用して、自身の IPv4 ネットワーク上でユニキャスト IPv6 サービスをお客様に提供できます。 この機能に関する詳細については、次の各項を参照してください。 <ul style="list-style-type: none"> <li>「IPv6 Rapid Deployment トンネル」 (P.6)</li> <li>「6RD トンネルの設定」 (P.14)</li> <li>「例 : 6RD トンネルの設定」 (P.23)</li> </ul>
IPv6 トンネリング : 自動 6to4 トンネル	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(33)SRA1 2.2(18)SXE 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	自動 6to4 トンネルを使用すると、孤立した IPv6 ドメインを、IPv4 ネットワークを介してリモート IPv6 ネットワークに接続できます。 この機能に関する詳細については、次の各項を参照してください。 <ul style="list-style-type: none"> <li>「自動 6to4 トンネル」 (P.5)</li> <li>「自動 6to4 トンネルの設定」 (P.11)</li> </ul>

表 4 トンネリング for IPv6 の実装の機能情報 (続き)

機能名	リリース	機能情報
IPv6 トンネリング : 自動 IPv4 互換トンネル	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(18)SXE 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	<p>自動 IPv4 互換トンネルでは、IPv4 互換 IPv6 アドレスを使用します。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> <li>• 「オーバーレイ トンネル for IPv6」 (P.2)</li> <li>• 「自動 IPv4 互換 IPv6 トンネル」 (P.6)</li> <li>• 「IPv4 互換 IPv6 トンネルの設定」 (P.13)</li> <li>• 「例 : IPv4 互換 IPv6 トンネルの設定」 (P.22)</li> </ul>
IPv6 トンネリング : CLNS ネットワーク内の IPv6 GRE トンネル	12.2(25)S 12.2(28)SB 12.2(33)SRA 12.3(7)T 12.4 12.4(2)T	<p>CLNS ネットワーク経由の IPv4 および IPv6 パケットの GRE トンネリングにより、Cisco CTunnels を他のベンダー製のネットワーキング機器と相互運用できます。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> <li>• 「オーバーレイ トンネル for IPv6」 (P.2)</li> <li>• 「IPv4 パケットと IPv6 パケットの GRE/CLNS トンネル サポート」 (P.5)</li> <li>• 「例 : CLNS で IPv6 パケットを伝送するように GRE モードで CTunnel を設定」 (P.20)</li> </ul>
IPv6 トンネリング : IP over IPv6 GRE トンネル	12.2(30)S 12.3(7)T 12.4 12.4(2)T	<p>GRE トンネルは、2 つのポイント間のリンクであり、リンクごとに個別のトンネルがあります。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> <li>• 「オーバーレイ トンネル for IPv6」 (P.2)</li> <li>• 「IPv6 トラフィック用の GRE/IPv4 トンネル サポート」 (P.4)</li> <li>• 「GRE IPv6 トンネルの設定」 (P.9)</li> </ul>
IPv6 トンネリング : IPv4 over IPv6 トンネル	12.2(30)S 12.2(33)SRA 12.3(7)T 12.4 12.4(2)T 15.0(1)S	<p>IPv6 ではこの機能がサポートされます。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> <li>• 「手動で設定された IPv6 トンネル」 (P.4)</li> <li>• 「手動 IPv6 トンネルの設定」 (P.8)</li> </ul>

表 4 トンネリング for IPv6 の実装の機能情報 (続き)

機能名	リリース	機能情報
IPv6 トンネリング : IPv6 over IPv4 GRE トンネル	12.0(22)S <sup>1</sup> 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(17a)SX1 12.2(4)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	GRE トンネルは、2つのポイント間のリンクであり、リンクごとに個別のトンネルがあります。これらのトンネルは、特定のパッセンジャまたはトランスポートプロトコルに結合されていませんが、この場合、GRE を使用するパッセンジャプロトコルとして IPv6 を伝送し、トランスポートプロトコルとして IPv4 または IPv6 を伝送します。  この機能に関する詳細については、次の各項を参照してください。 <ul style="list-style-type: none"> <li>• 「オーバーレイ トンネル for IPv6」 (P.2)</li> <li>• 「IPv6 トラフィック用の GRE/IPv4 トンネルサポート」 (P.4)</li> <li>• 「GRE IPv6 トンネルの設定」 (P.9)</li> <li>• 「例 : GRE トンネルの設定」 (P.19)</li> </ul>
IPv6 トンネリング : IPv6 over IPv6 トンネル	12.2(30)S 12.3(7)T 12.4 12.4(2)T	IPv6 ではこの機能がサポートされます。  この機能に関する詳細については、次の各項を参照してください。 <ul style="list-style-type: none"> <li>• 「手動で設定された IPv6 トンネル」 (P.4)</li> <li>• 「手動 IPv6 トンネルの設定」 (P.8)</li> </ul>
IPv6 トンネリング : トンネル ラインカードを使用する IPv6 over UTI <sup>2</sup>	12.0(23)S <sup>3</sup>	IPv6 は、この機能をサポートします。
IPv6 トンネリング : ISATAP トンネルサポート	12.2(14)S 12.2(28)SB 12.2(33)SRA1 2.2(17a)SX11 2.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	ISATAP は、基礎となる IPv4 ネットワークを IPv6 の NBMA リンク レイヤとして使用する、自動オーバーレイ トンネリング メカニズムです。  この機能に関する詳細については、次の各項を参照してください。 <ul style="list-style-type: none"> <li>• 「オーバーレイ トンネル for IPv6」 (P.2)</li> <li>• 「ISATAP トンネル」 (P.6)</li> <li>• 「ISATAP トンネルの設定」 (P.15)</li> <li>• 「例 : ISATAP トンネルの設定」 (P.23)</li> </ul>

表 4 トンネリング for IPv6 の実装の機能情報 (続き)

機能名	リリース	機能情報
IPv6 トンネリング：手動で設定された IPv6 over IPv4 トンネル	12.0(23)S <sup>3</sup> 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	手動で設定されたトンネルは、IPv4 バックボーンを介した 2 つの IPv6 ドメイン間の固定リンクに相当します。  この機能に関する詳細については、次の各項を参照してください。 <ul style="list-style-type: none"> <li>「オーバーレイ トンネル for IPv6」(P.2)</li> <li>「手動で設定された IPv6 トンネル」(P.4)</li> <li>「手動 IPv6 トンネルの設定」(P.8)</li> <li>「例：手動 IPv6 トンネルの設定」(P.19)</li> </ul>
IPv6 を介した mGRE トンネル	15.2(1)T	mGRE トンネルは、サービス プロバイダーがコア インフラストラクチャに IPv6 を導入できるように設定されます。  この機能に関する詳細については、次の各項を参照してください。 <ul style="list-style-type: none"> <li>「IPv6 を介した mGRE トンネル サポート」(P.5)</li> </ul>

1. IPv6 over IPv4 GRE トンネルは、GSR ではサポートされていません。
2. 機能は、GSR だけでサポートされています。
3. Cisco IOS Release 12.0(23)S の場合、GSR では、トラフィックをラインカード上で処理することで、手動で設定された IPv6 トンネルのパフォーマンスを強化しています。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2001–2011 Cisco Systems, Inc.  
All rights reserved.

Copyright © 2001–2011, シスコシステムズ合同会社.  
All rights reserved.

