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.24）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。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

- 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 Cisco 12000 シリーズでは、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、Cisco 12000 ルータの 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

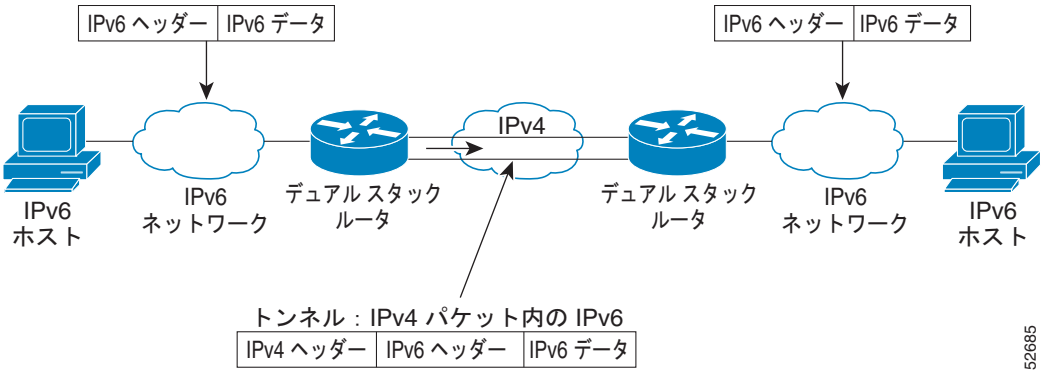
トンネリング for IPv6 を設定するには、次の概念を理解する必要があります。

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）

図 1　オーバーレイ トンネル



（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、現在推奨していません。
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、::*tunnel-source*/96 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 eui-64 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。

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。

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:*border-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 0:0:0:0:0:0: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。

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、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 に、ISATAP アドレス形式を示します。

表 3　　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 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 2001:0DB8:1234:5678::/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、この IPv4 アドレスは、16 進形式で 0AAD:8108 として表されます。たとえば、2001:0DB8:1234:5678:0000:5EFE:0AAD:8108 となります。

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、「*IPv6 セキュリティへの IPsec の実装*」を参照してください。

トンネリング for IPv6 の実装方法

ここでは、トンネリング for IPv6 を実装する方法について説明します。

- 「手動 IPv6 トンネルの設定」（P.7）
- 「GRE IPv6 トンネルの設定」（P.8）
- 「自動 6to4 トンネルの設定」（P.10）
- 「自動 IPv4 互換 IPv6 トンネル」（P.5）
- 「ISATAP トンネルの設定」（P.13）
- 「IPv6 トンネルの設定と動作の確認」（P.14）

手動 IPv6 トンネルの設定

ここでは、IPv6 オーバーレイ トンネルを手動で設定する方法について説明します。

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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **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	**configure terminal** **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	**interface tunnel** *tunnel-number* **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	**ipv6 address** *ipv6-prefix*/*prefix-length* [**eui-64**] **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	**tunnel source** {*ip-address* | *interface-type interface-number*} **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	**tunnel destination** *ip-address* **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	**tunnel mode ipv6ip** **例：** `Router(config-if)# tunnel mode ipv6ip`	手動 IPv6 トンネルを指定します。 **（注）** **tunnel mode ipv6ip** コマンドでは、IPv6 をパッセンジャ 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

ここでは、IPv6 ネットワーク上で GRE トンネルを設定する方法について説明します。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**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **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	**configure terminal** **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	**interface tunnel** *tunnel-number* **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	**ipv6 address** *ipv6-prefix*/*prefix-length* [**eui-64**] **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	**tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*} **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。

	コマンドまたはアクション	目的
ステップ 6	**tunnel destination** {*host-name* | *ip-address* | *ipv6-address*} **例：** `Router(config-if)# tunnel destination 2001:0DB8:1111:2222::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	**tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ipv6** | **ipip** [**decapsulate-any**] | **iptalk** | **ipv6** | **mpls** | **nos**} **例：** `Router(config-if)# tunnel mode gre ipv6`	GRE IPv6 トンネルを指定します。 **（注）** **tunnel mode gre ipv6** 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

ここでは、6to4 オーバーレイ トンネルの設定方法について説明します。

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。このため、IPv4 プロトコル タイプ 41 を含むパケットがインターフェイスに到着すると、そのパケットは、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*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **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	**configure terminal** **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	**interface tunnel** *tunnel-number* **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	**ipv6 address** *ipv6-prefix*/*prefix-length* [**eui-64**] **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。 • 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。
ステップ 5	**tunnel source** {*ip-address* | *interface-type interface-number*} **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） **tunnel source** 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	**tunnel mode ipv6ip 6to4** **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。

	コマンドまたはアクション	目的
ステップ 7	**exit** **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	**ipv6 route** *ipv6-prefix*/*prefix-length* **tunnel** *tunnel-number* **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。 **（注）** 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。 • **ipv6 route** コマンドで指定したトンネル番号は、**interface tunnel** 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。

IPv4 互換 IPv6 トンネルの設定

ここでは、IPv4 互換 IPv6 オーバーレイ トンネルの設定方法について説明します。

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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **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	**configure terminal** **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	**interface tunnel** *tunnel-number* **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	**tunnel source** {*ip-address* | *interface-type interface-number*} **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）** **tunnel source** 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	**tunnel mode ipv6ip auto-tunnel** **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。

ISATAP トンネルの設定

ここでは、ISATAP オーバーレイ トンネルを設定する方法について説明します。

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	**enable** **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	**configure terminal** **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	**interface tunnel** *tunnel-number* **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	**ipv6 address** *ipv6-prefix*/*prefix-length* [**eui-64**] **例：** `Router(config-if)# ipv6 address 2001:0DB8:6301::/64 eui-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。 **（注）** IPv6 アドレスの設定の詳細については、「*Configuring Basic Connectivity for IPv6*」の章を参照してください。
ステップ 5	**no ipv6 nd ra suppress** **例：** `Router(config-if)# no ipv6 nd ra suppress`	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。
ステップ 6	**tunnel source** {*ip-address* | *interface-type interface-number*} **例：** `Router(config-if)# tunnel source ethernet 1/0/1`	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）** **tunnel source** 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 7	**tunnel mode ipv6ip isatap** **例：** `Router(config-if)# tunnel mode ipv6ip isatap`	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。

IPv6 トンネルの設定と動作の確認

この任意の作業では、IPv6 トンネルの設定と動作を確認する方法について説明します。この作業手順に含まれているコマンドは、任意の順番で使用できます。また、繰り返す必要がある場合があります。

手順の概要

1. **enable**
2. **show interfaces tunnel** *number* [**accounting**]
3. **ping** [*protocol*] *destination*

4. **show ip route** [*address* [*mask*]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **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	**show interfaces tunnel** *number* [**accounting**] **例：** `Router# show interfaces tunnel 0`	（任意）トンネル インターフェイス情報を表示します。 • *number* 引数を使用して、指定したトンネルの情報を表示します。
ステップ 3	**ping** [*protocol*] *destination* **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	**show ip route** [*address* [*mask*]] **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

ここでは、次の出力例について説明します。

- 「show interfaces tunnel コマンドの出力例」
- 「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」

show interfaces tunnel コマンドの出力例

この例では、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ている、汎用的な例を使用します。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 2001:0DB8:1111:2222::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 2001:0DB8:1111:2222::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 2001:0DB8:1111:2222::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:0DB8:1111:2222::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

ここでは、次の設定例について説明します。

手動 IPv6 トンネルの設定：例

次の例では、ルータ A とルータ B 間に手動 IPv6 トンネルを設定します。この例では、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 が、グローバル IPv6 アドレスを使用して手動で設定されます。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
```

GRE トンネルの設定：例

ここでは、次の設定例について説明します。

IS-IS および IPv6 トラフィックを実行する GRE トンネル：例

次の例では、ルータ A とルータ B 間で IS-IS と IPv6 の両方のトラフィックを実行する GRE トラフィックを設定します。

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 2001:0DB8:1111:2222::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 2001:0DB8:1111:2222::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
```

IPv6 トンネルのトンネル宛先アドレス：例

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 2001:0DB8:1111:2222::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
```

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

次の例では、CLNS ネットワーク内のルータ A とルータ B 間で IS-IS と IPv6 トラフィックの両方を実行する GRE CTunnel を設定します。**ctunnel mode gre** コマンドによって、シスコのネットワーキング デバイスとサードパーティのネットワーキング 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 コマンドによって、RFC 3147 に準拠したトンネリング方法が提供され、シスコの装置とサードパーティのネットワーキング デバイス間のトンネリングが可能になります。

ルータ A

```
ipv6 unicast-routing

clns routing

interface ctunnel 102

 ipv6 address 2001:0DB8:1111:2222::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 2001:0DB8:1111:2222::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
```

GRE モードをオフにし、シスコの装置上のエンドポイント間だけのデフォルト シスコ カプセル化ルーティングに CTunnel を戻すには、**no ctunnel mode** コマンドまたは **ctunnel mode cisco** コマンドを使用します。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。

6to4 トンネルの設定：例

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 番めの 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
```

IPv4 互換 IPv6 トンネルの設定：例

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（0:0:0:0:0:0: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 アトリビュート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
```

ISATAP トンネルの設定：例

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 2001:0DB8::/64 eui-64
 no ipv6 nd ra suppress
 exit
```

関連情報

- 自動 6to4 トンネルを設定済みである場合は、IPv4 アドレスから作成した /48 6to4 プレフィクスの周囲に IPv6 ネットワークを設計できます。
- IPv6 ルーティング プロトコルを実装する場合は、「*Implementing RIP for IPv6*」、「*Implementing IS-IS for IPv6*」、「*Implementing OSPF for IPv6*」、または「*Implementing Multiprotocol BGP for IPv6*」の章を参照してください。
- IPv6 ネットワーク用のセキュリティ機能を実装する場合は、「*Implementing IPsec in IPv6 Security*」の章を参照してください。

その他の関連資料

ここでは、トンネリング for IPv6 機能の実装に関する関連資料について説明します。

関連資料

関連項目	参照先
IPsec VTI	「*Implementing IPsec in IPv6 Security*」
IPv6 のサポート機能リスト	「*Start Here: Cisco IOS Software Release Specifics for IPv6 Features*」
CLNS トンネル	『*Cisco IOS ISO CLNS Configuration Guide*』
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	『*Cisco IOS IPv6 Command Reference*』

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
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

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

シスコのテクニカル サポート

説明	リンク
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。 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。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • 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 • ツールおよびリソースへアクセスする • Product Alert の受信登録 • Field Notice の受信登録 • Bug Toolkit を使用した既知の問題の検索 • 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 • トレーニング リソースへアクセスする • 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 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。	http://www.cisco.com/en/US/support/index.html

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。この表には、Cisco IOS Release 12.2(2)T 以降のリリースで導入または変更された機能だけを示します。

ここに記載されていないこのテクノロジーの機能情報については、「*Start Here: Cisco IOS Software Release Specifies for IPv6 Features*」を参照してください。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

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 を使用すると、Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージがサポートする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確認できます。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 Cisco IOS 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 Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降の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
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[1] 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	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。 • 「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） • 「手動 IPv6 トンネルの設定」（P.7） • 「手動 IPv6 トンネルの設定：例」（P.17）
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	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。 • 「手動で設定された IPv6 トンネル」（P.4）
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	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。 • 「自動 6to4 トンネル」（P.5） • 「自動 6to4 トンネルの設定」（P.10）

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	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。 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。 • 「オーバーレイ トンネル for IPv6」（P.2） • 「自動 IPv4 互換 IPv6 トンネル」（P.5） • 「IPv4 互換 IPv6 トンネルの設定」（P.12） • 「IPv4 互換 IPv6 トンネルの設定：例」（P.20）
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[1] 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(17a)SX1 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T	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。 • 「トンネリング for IPv6 の実装の制約事項」（P.2） • 「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） • 「手動 IPv6 トンネルの設定」（P.7） • 「手動 IPv6 トンネルの設定：例」（P.17）
IPv6 トンネリング：IPv6 over IPv4 GRE トンネル	12.0(22)S[2] 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	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。 • 「オーバーレイ トンネル for IPv6」（P.2） • 「IPv6 トラフィック用の GRE/IPv4 トンネル サポート」（P.4） • 「GRE IPv6 トンネルの設定」（P.8） • 「GRE トンネルの設定：例」（P.17）
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[3]	12.0(23)S[1]	IPv6 は、この機能をサポートします。

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：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	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。 • 「オーバーレイ トンネル for IPv6」（P.2） • 「ISATAP トンネル」（P.6） • 「ISATAP トンネルの設定」（P.13） • 「ISATAP トンネルの設定：例」（P.21）
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	IPv6 では、この機能をサポートします。 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。 • 「手動で設定された IPv6 トンネル」（P.4） • 「手動 IPv6 トンネルの設定」（P.7）
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、この機能をサポートします。 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。 • 「手動で設定された IPv6 トンネル」（P.4） • 「手動 IPv6 トンネルの設定」（P.7）
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	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。 • 「オーバーレイ トンネル for IPv6」（P.2） • 「IPv6 トラフィック用の GRE/IPv4 トンネル サポート」（P.4） • 「GRE IPv6 トンネルの設定」（P.8）
IPv6 トンネリング：CLNS ネットワークでの 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	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 CTunnel 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。 この機能に関する詳細については、次の各項を参照してください。 • 「オーバーレイ トンネル for IPv6」（P.2） • 「IPv4 パケットと IPv6 パケットの GRE/CLNS トンネル サポート」（P.5） • 「CLNS で IPv6 パケットを伝送するように GRE モードで CTunnel を設定：例」（P.19）

1. Cisco IOS Release 12.0(23)S の場合、Cisco 12000 シリーズ インターネット ルータでは、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。
2. IPv6 over IPv4 GRE トンネルは、Cisco 12000 シリーズのインターネット ルータではサポートされていません。

3. 機能は、Cisco 12000 シリーズのインターネット ルータだけでサポートされています。