IP トンネルの設定

IP トンネルについて

IP トンネルを使うと、同じレイヤまたは上位層プロトコルをカプセル化して、2 台のデバイス間で作成されたトンネルを通じて IP に結果を転送できます。

IP トンネルの概要

IP トンネルは次の 3 つの主要コンポーネントで構成されています。

- パッセンジャ プロトコル：カプセル化する必要があるプロトコル。パッセンジャ プロトコルの例には IPv4 があります。
- キャリア プロトコル：パッセンジャ プロトコルをカプセル化するために使用するプロトコル。Cisco NX-OS はキャリア プロトコルとして GRE をサポートします。
- トランスポート プロトコル：カプセル化したプロトコルを伝送するために使用するプロトコル。トランスポート プロトコルの例には IPv4 があります。IP トンネルは IPv4 などのパッセンジャ プロトコルを使用し、このプロトコルを GRE などのキャリア プロトコル内にカプセル化します。次に、このキャリア プロトコルは IPv4 などのトランスポート プロトコルを通じてデバイスから送信されます。

対応する特性を持つトンネル インターフェイスをトンネルの両端にそれぞれ設定します。

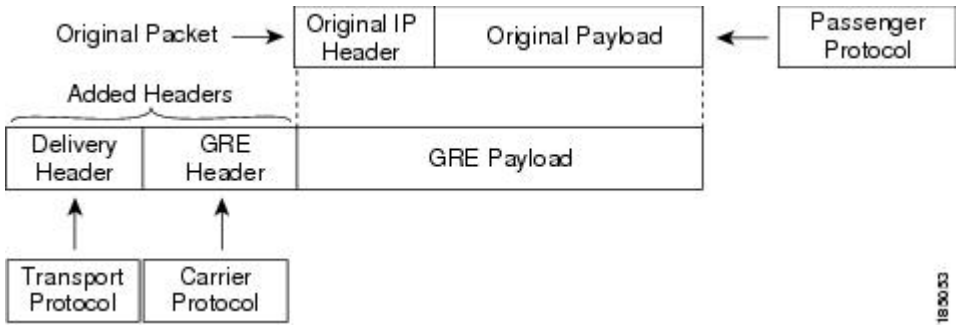
設定の前にトンネル機能をイネーブルにする必要があります。システムはこの機能をディセーブルにする前のチェックポイントを自動的に取得するため、このチェックポイントにロールバックできます。ロールバックおよびチェックポイントについては、『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』を参照してください。

GRE トンネル

Generic Routing Encapsulation（GRE）をさまざまなパッセンジャ プロトコルのキャリア プロトコルとして使用できます。

この次図は、GRE トンネルの IP トンネルのコンポーネントを示しています。オリジナルのパッセンジャ プロトコル パケットは GRE ペイロードとなり、デバイスはパケットに GRE ヘッダーを追加します。次にデバイスはトランスポート プロトコル ヘッダーをパケットに追加して送信します。

図 *1 : GRE PDU*



ポイントツーポイント IP-in-IP トンネルのカプセル化およびカプセル化解除

ポイントツーポイント IP-in-IP のカプセル化およびカプセル化解除は、送信元トンネル インターフェイスから宛先トンネルインターフェイスにカプセル化されたパケットを送信するために作成できる一種のトンネルです。このタイプのトンネルは、着信トラフィックと発信トラフィックの両方を伝送します。

（注） PBR ポリシーに基づく GRE または IP-in-IP トンネル接続先の選択は、サポートされません。

（注） IP-in-IP トンネル カプセル化とカプセル化解除は、N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチではサポートされません。

（注） IP-in-IP トンネルのカプセル化とカプセル化解除は、Cisco Nexus 9300-EX、9300-FX、 9300-GX および Nexus 9500 プラットフォーム スイッチの vPC 設定ではサポートされません。

マルチポイント IP-in-IP トンネルのカプセル化解除

マルチポイント IP-in-IP の decapsulate-any は、任意の数の IP-in-IP トンネルから 1 つのトンネルインターフェイスにパケットのカプセル化を解除するために作成できるトンネルのタイプです。このトンネルは発信トラフィックを伝送しません。ただし、任意の数のリモート トンネル エンドポイントが、このように設定されたトンネルを宛先として使用することができます。

パス MTU ディスカバリ

パス最大伝送単位（MTU）ディスカバリ（PMTUD）は、パケットの発信元から宛先へのパスに沿って最小MTUを動的に決定することで、2つのエンドポイント間のパスのフラグメンテーションを防ぎます。PMTUD は、パケットにフラグメンテーションが必要であるという情報がインターフェイスに届くと、接続に対する送信 MTU 値を減らします。

PMTUD をイネーブルにすると、インターフェイスはトンネルを通過するすべてのパケットにDon't Fragment（DF）ビットを設定します。トンネルに入ったパケットがそのパケットのMTU値よりも小さいMTU値を持つリンクを検出すると、リモート リンクはそのパケットをドロップし、パケットの送信元にインターネット制御メッセージ プロトコル（ICMP）メッセージを返します。このメッセージには、フラグメンテーションが要求されたこと（しかし許可されなかったこと）と、パケットをドロップしたリンクの MTU が含まれています。

（注） トンネル インターフェイスの PMTUD は、トンネル エンドポイントがトンネルのパスでデバイスによって生成されるICMPメッセージを受信することを要求します。ファイアウォール接続を通じてPMTUDを使用する前に、ICMPメッセージが受信できることを確認してください。

高可用性

IP トンネルはステートフル再起動をサポートします。ステートフル再起動はスーパーバイザ切り替え時に発生します。切り替え後、Cisco NX-OS は実行時の設定を適用します。

IP トンネルの前提条件

IP トンネルには次の前提条件があります。

- IP トンネルを設定するための TCP/IP に関する基礎知識があること。
- スイッチにログインしている。

- IP トンネルを設定してイネーブルにする前にデバイスのトンネリング機能をイネーブルにしておくこと。

注意事項と制約事項

IP トンネルの設定に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS リリース 9.3(3) 以降：
  - Cisco Nexus N92xx、N93xx-EX/FX/FX2、N9500 ライン カード、N9700-EX、および N9700-FX プラットフォームでは、全部で 16 の GRE/IPIP トンネルがサポートされています。
  - 同じ Cisco Nexus デバイス上の複数の IP-in-IP/GRE トンネル インターフェイスは、異なる VRF 間で、同じ IP アドレスを送信元とすること、または同じ IP アドレスを宛先とすることができます。これは、Cisco Nexus N92xx および N93xx-EX/FX/FX2 プラットフォームでサポートされています。これは、Cisco Nexus 9300-GX および N9500 プラットフォームではサポートされていません。
  - 複数の、最大で 16 の IPIP Decap-any トンネルがサポートされています。VRF ごとに 1 つの decap-any トンネルです。これは、Cisco Nexus N92xx および M93xx-EX/FX/FX2 プラットフォームでサポートされています。
  - IPIP/GRE カプセル化パケットが終端ノードで入力されるインターフェイスの VRF メンバーシップは、トンネルのパケットを正しく終端するために、トンネル転送 VRF と一致している必要があります。
  - パケットの外部ヘッダーがトンネルの送信元およびトンネルの宛先と一致する場合、デフォルト以外の VRF に着信する IPIP/GRE パケットは、デフォルトの VRF トンネルによって終端されることがあります。
- Cisco NX-OS リリース 9.3(5) 以降では、次の機能が N9K-C9316D-GX、N9K-C93600CD-GX、および N9K-C9364C-GX スイッチでサポートされています。
  - 合計 16 の GRE/IPIP トンネル。
  - 同じ Cisco Nexus デバイス上の複数の IP-in-IP/GRE トンネル インターフェイスは、異なる VRF 間で、同じ IP アドレスを送信元とすること、または同じ IP アドレスを宛先とすることができます。
  - 複数の、最大で 16 の IPIP Decap-any トンネルがサポートされています。VRF ごとに 1 つの decap-any トンネルです。
- トンネルの **source-direct** および **ipv6ipv6-decapsulate-any** オプションについてのガイドラインは、以下のとおりです：

- **source-direct** コマンドは、Application Spine Engine（ASE）および Leaf Spine Engine（LSE）を搭載した Cisco Nexus 9500 プラットフォーム スイッチでサポートされます。

  Network Forwarding Engine（NFE）を搭載した Cisco Nexus 9500 プラットフォームスイッチは、 **tunnel source direct** コマンドをサポートしていません。

  Cisco Nexus 9500 プラットフォーム スイッチでの **tunnel source direct** コマンドと **tunnel mode ipv6ipv6 decapsulate-any** コマンドは、MPLS ヘビー ルーティング テンプレートでのみサポートされます。

- IP トンネルは、インターフェイス、IPv4 アドレス、IPv6 アドレス、または IPv4 プレフィックスを使用した **tunnel source** CLI コマンドをサポートします。新しい **tunnel source direct** CLI コマンドを使用すれば、直接接続された IP アドレス（物理インターフェイス、ポートチャネル、ループバック、SVIなど）で IP-in-IP トンネルのカプセル化解除を設定できます。2 つのスイッチ間に複数の IP リンクがある場合は、IP ECMP リンクを選択できます。単一のトンネルインターフェイスは、外部宛先 IP がローカルで設定された IPv4 または IPv6 アドレスのいずれかであり、スイッチで動作的にアップ状態になっているようなトンネル パケットを、カプセル化解除できます。

- 現在、 **tunnel mode ipip decapsulate-any** は、IPv4 トランスポート（IPv4inIPv4 パケット）を介して IPv4 ペイロードをカプセル化解除するためにサポートされています。**tunnel mode ipv6ipv6 decapsulate-any** コマンドは、IPv6 トランスポートを介した IPv6 ペイロード（IPv6inIPv6 パケット）をサポートするために導入されました。

- ネットワーク形成エンジン（NFE）を搭載した Cisco Nexus 9500 プラットフォーム スイッチでは、 **tunnel source direct** および **tunnel mode ipv6ipv6 decapsulate-any** CLI コマンドはサポートされていません。

- **tunnel source direct** CLI コマンドがサポートされるのは、管理者が IP-in-IP カプセル化解除を使用して、パケットをネットワーク経由でソース ルーティングする場合だけです。source-direct トンネルは、管理上シャットダウンされない限り、常に動作的にアップ状態です。直接接続されたインターフェイスは、 **show ip route direct** CLI コマンドを使用して識別されます。

- CLIコマンドは、カプセル化解除トンネルモード（andなど）でのみサポートされます。 **tunnel source direct tunnel mode ipip decapsulate-any tunnel mode ipv6ipv6 decapsulate-any**

- source-direct の自動回復はサポートされていません。

- ipv6ipv6 decapsulate-any の場合、inter-VRF はサポートされません。トンネル インターフェイス VRF（iVRF）と、トンネル トランスポートまたはフォワーディング VRF（fVRF）は、同じである必要があります。Cisco Nexus 9200、9300-EX、および 9300-FX プラットフォーム スイッチと、EX および FX ラインカードを備えた Cisco Nexus 9500 プラットフォーム モジュラ スイッチには、VRF に関係なくカプセル化解除トンネルが 1 つだけ存在します。

- ipv6ipv6 decap-any トンネル インターフェイスで IPv6 を有効にするには、有効な IPv6 アドレスを設定するか、トンネル インターフェイスで **ipv6 address use-link-local-only** を設定します。

- 送信元ダイレクト トンネルで対応可能な送信元の最大数と関連動作については、次のハードウェア制限を参照してください。
  - 送信元直接トンネルは、ネットワーク転送エンジン（NFE）、アプリケーション スパイン エンジン（ASE）、およびリーフ スパイン エンジン（LSE）を搭載した Cisco Nexus 9000 シリーズ スイッチでサポートされるようになりましたほとんどの制限は、スケーリングされた SIP の場合に限り、インターフェイス上の IP/IPv6 アドレスの合計数にのみ適用されます。この場合のインターフェイスとは、L3、サブインターフェイス、PC、PC-サブ インターフェイス、ループバック、SVI、および任意のセカンダリ IP/IPv6 アドレスを指します。

    次の使用例を参照してください。

    - 使用例 1：IP / IPv6インターフェイス スケールの数がより多い場合に SIP がインストールされたときの非決定的動作への対応。

      両方のスイッチにトンネル SIP が 512 エントリがあります。トンネル送信元を使用する場合は、任意の IP または IPv6 アドレスを、 **ipip or ipv6ipv6 decap any** により、上記のテーブルにインストールされたトンネル送信元にダイレクトします。

      これらのエントリの挿入は、どのインターフェイス IP アドレスをインストールするかを制御する CLI コマンドを使用せずに、先着順に行われますシステムにインストールする IP/IPv6 インターフェイスの数が多い場合、動作は非決定的です（動作はインターフェイス フラップを使用して変更できます）。

    - 使用例 2：両方のスイッチでスケール数が異なる場合。それぞれに長所と短所があります。

      NFE を備えたスイッチの場合、IPv4 の個別のスケールはより大きくすることができますが（最大512）、IPv6と共有されます。ASE および LSE を備えたするスイッチでは、IPv4 の個別のスケールは 256 までですが、IPv6 とは共有されません。

      トンネル decap テーブルがいっぱいになると、TABLE_FULL エラーが表示されます。テーブルがいっぱいになった後でも、一部のエントリが削除されると、テーブルフル エラーはクリアされます。

表 *1*: スケール番号

コマンド	NFE を使用したスイッチ：テーブルサイズ 512、v4 は 1 エントリ、v6 は 4 エントリ	ASE および LSE を使用したスイッチ：テーブルサイズ 512、v4 は 1 エントリ、v6 は 2 エントリ（ペアインデックス）
トンネル ソース ダイレクトによる IPIP カプセル化解除	v4 と v6 の間で共有、v6 は 4 エントリを取得 v4 + 4 * v6 = 512 最大エントリ数は 512 で、v6 エントリなし	専用で 256
トンネル ソース ダイレクトによる IPv6IPv6 カプセル化解除	v4 と v6 の間で共有、v6 は 4 エントリを取得 v4 + 4 * v6 = 512 最大エントリ数は 128 で、v4 エントリなし	専用で 128

- 使用例 3：自動リカバリはサポートされていません。

  上記のテーブルが使い果たされたためにハードウェアにエントリがインストールされない場合、すでにインストールされている IP/IPv6 をインターフェイスから削除すると、テーブルにスペースが生じますが、前に失敗した SIP がテーブルに自動的に追加されることはありません。トンネル インターフェイスまたは IP インターフェイスをフラップしてインストールする必要があります。

  ただし、エントリが重複しているためにエントリがハードウェアにインストールされない場合（すでに 1 つのソースで **decap-any** が存在していて、 **source direct tunnel** CLI コマンドを設定した場合、以前に設定されたソースのエントリは重複します）両方のトンネルが削除された場合にのみエントリを削除するように注意してください。

- Network Forwarding Engine（NFE）とApplication Spine Engine（ASE）を備えた Cisco Nexus 9000 シリーズスイッチでは、専用の IPv4 および IPv6 のカプセル化解除がsyslog に記録されるため、syslog は異なります。**tunnel-decap-table** がいっぱいの場合、ユーザは次のように syslog を取得します。

```
2017 Apr 6 12:18:04 switch %$ VDC-1 %$
%IPFIB-2-FIB_HW_IPV4_TUNNEL_DECAP_TABLE_FULL: IPv4 tunnel decap hardware table
full.
IP tunnel decapsulation may not work for some GRE/IPinIP traffic

2017 Apr 6 12:18:11 switch %$ VDC-1 %$
%IPFIB-2-FIB_HW_IPV6_TUNNEL_DECAP_TABLE_FULL: IPv6 tunnel decap hardware table
full.
IP tunnel decapsulation may not work for some GRE/IPinIP traffic
```

テーブルがいっぱいで、一部のエントリがテーブルから削除されるようになった場合（インターフェイスが動作上ダウンしているか、IPアドレスが削除されているため）、テーブルがクリアされたとのsyslogが表示されます。トンネルを削除すると、そのトンネルの一部として追加されたすべてのエントリが削除されることに注意してください。

```
2017 Apr 5 13:29:25 switch %$ VDC-1 %$
%IPFIB-2-FIB_HW_IPV4_TUNNEL_DECAP_TABLE_FULL_CLRD: IPv4 tunnel decap hardware
table full exception cleared

2017 Apr 4 19:41:22 switch %$ VDC-1 %$
%IPFIB-2-FIB_HW_IPV6_TUNNEL_DECAP_TABLE_FULL_CLRD: IPv6 tunnel decap hardware
table full exception cleared
```

- IP-in-IP トンネルのカプセル化解除は、IPv6 対応ネットワークでサポートされます。

```
!
interface tunnel 1
  ipv6 address use-link-local-only             <<< enable IPv6
  tunnel mode ipv6ipv6 decapsulate-any
  tunnel source direct
  description IPinIP Decapsulation Interface
  mtu 1476
  no shutdown
```

- **internal** キーワードが付いているコ **show** マンドはサポートされていません。
- Cisco NX-OS は、次のプロトコルだけをサポートします。
  - IPv4 パッセンジャー プロトコル
  - GRE キャリア プロトコル
- Cisco NX-OS は、Cisco NX-OS リリース 9.3(3) よりも前のトンネルについては、次の最大数をサポートします。
  - IP トンネル：8 トンネル
  - GRE および IP-in-IP 標準トンネル：8 トンネル
- Cisco NX-OS リリース9.3(3) 以降、サポートされる GRE および IP-in-IP の通常トンネルの最大数は 16 です。
- アクセス コントロール リスト（ACL）またはQoS ポリシーはIP トンネルでサポートされません。
- Cisco NX-OS は、IETF RFC 2784 に定義されている GRE ヘッダーをサポートします。Cisco NX-OS は、トンネル キーと IETF RFC 1701 のその他のオプションをサポートしません。
- Cisco NX-OS は、GRE トンネル キープアライブをサポートしません。
- すべてのユニキャスト ルーティング プロトコルが IP トンネルでサポートされます。
- IP トンネル インターフェイスは、SPAN 送信元または宛先には設定できません。

- IP トンネルは、PIM またはその他のマルチキャスト機能およびプロトコルをサポートしません
- PBR ポリシーに基づく GRE または IP-in-IP トンネル接続先の選択は、サポートされません。
- IP トンネルは、デフォルトの **system routing** モードでのみサポートされ、その他のモードではサポートされません
- トンネルインターフェイスを **ipip mode** に設定する場合、最大の mtu 値は 9196 です。

  NX-OS 9.2(1) 以降のリリースから以前のリリースにダウングレードする場合、MTU 値が 9196 の **ipip mode** のトンネル インターフェイスを使用していると、ダウングレード操作の結果として MTU 設定が失われます。ベスト プラクティスとしては、MTU 設定が失われることを回避するために、ダウングレードを開始する前に MTU 値を 9192 に調整します。
- トンネルインターフェイスを **ipip mode** に設定する場合、デフォルトの mtu 値は 1480 です。

  NX-OS 9.2(1) 以降のリリース から以前のリリースにダウングレードする場合、明示的な MTU 設定のない **ipip mode** のトンネル インターフェイスを使用していると、ダウングレード操作の結果として MTU 値が 1480 から 1476 に変更されます。ベスト プラクティスとしては、MTU 値が変更されることを回避するために、ダウングレードを開始する前に MTU 値を 1476 に調整します。

  から NX-OS 9.2(1) 以降のリリースにアップグレードする場合、 で、明示的な mtu 設定のない **ipip mode** のトンネル インターフェイスがあると、アップグレード操作の結果として MTU 値が 1476 から 1480 に変更されます。ベスト プラクティスとしては、MTU 値が変更されることを回避するために、アップグレードを開始する前に MTU 値を 1480 に調整します。
- Cisco Nexus 9200 シリーズ スイッチでは、IP-in-IP トンネルで受信される GRE パケットが予想通りにドロップされず、パケット宛先に転送されます。
- スイッチから送信される Tx パケット（制御パケットなど）は、Tx 統計には含まれません。
- 別のトンネル経由で到達可能なトンネル宛先は、サポートされません。
- トンネル経由のルートについては整合性チェッカがサポートされません。
- 非 IP ルーティング プロトコル（isis など）は、IP-in-IP トンネル経由ではサポートされません。
- RFC5549 は、トンネル経由ではサポートされません。
- トンネル経由の BGP 隣接関係は、トンネル インターフェイスとトンネル入口が同じ VRF にあり（例：VRF-A）、トンネル出口が反対側からのルートリーク（例：VRF-B経由）で到達可能なシナリオでは、サポートされません。

- Cisco Nexus N9K-C9300-GX プラットフォームでは、GRE/IPinIP トンネル インターフェイスは、Dot1Q タグ付き L2 bcast または 1Q タグ付き L2/L3 mcast 中継トラフィックと共存できません。Cisco Nexus N9300-GX プラットフォームで**feature tunnel**を設定すると、次の警告が表示され、syslog メッセージにも警告が記録されます。デバイスに Dot1Q タグ付き L2 bcast または 1Q タグ付き L2/L3 mcast 中継トラフィックがある場合は、**feature tunnel** を設定しないでください。

```
N9300-GX(config)# feature tunnel
WARN:GRE/IPinIP cannot coexist with 1Q tagged L2 bcast or 1Q tagged L2/L3 mcast
transit packets on this
platform
N9300-GX(config)#
N9300-GX(config)# show logging logfile
2019 Dec 12 00:41:08 N9300-GX %TUNNEL-2-TRAFFIC_WARNING: GRE/IPinIP cannot coexist
with 1Q
tagged L2 bcast or 1Q tagged L2/L3 mcast transit packets on this platform
N9300-GX(config)#
```

- Cisco Nexus 9000 スイッチの**機能トンネル**機能は、VXLAN 機能である**機能 nv オーバーレイ**と共存できません。
- Cisco Nexus 9200、9300-EX、9300-FX、9300-FX2 シリーズ スイッチ、および 9700-EX/FX ライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチでは、複数のトンネル インターフェイスを、同じ IP アドレスを送信元または宛先とする単一の VRFに含めることはできません。たとえば、デバイスは、トンネル 0 およびトンネル 1 のインターフェイスを、同じ IP アドレスまたはインターフェイスを送信元とするデフォルト VRF に含めることはできません。
- vPC の Cisco Nexus 9300-EX、9300-FX、9300-GX、および Nexus 9500 プラットフォーム スイッチは、それぞれのトンネルの GRE トンネル エンドポイントとして機能できます。ただし、トンネルの宛先を vPC 経由にすることはできません。

デフォルト設定

次の表に、IP トンネル パラメータのデフォルト設定を示します。

表 *2:* デフォルトの *IP* トンネル パラメータ

パラメータ	デフォルト
パス MTU ディスカバリ経過時間タイマー	10 分
パス MTU ディスカバリの最小 MTU	64
トンネル機能	ディセーブル

IP トンネルの設定

IP トンネルの設定

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

トンネリングのイネーブル化

IP トンネルを設定する前にトンネリング機能をイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **feature tunnel**
3. **exit**
4. **show feature**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**feature tunnel**
	例：
	`switch(config)# feature tunnel`
	`switch(config-if)#`
		新しいトンネルインターフェイスを作成できます。
		トンネルインターフェイス機能を無効にするには、このコマンドの **no** 形式を使用します。
		（注） マルチキャストの重いテンプレートが適用されている場合、**feature tunnel** コマンドはマルチキャスト機能を中断する可能性があります。

ステップ 3	**exit**
	例：
	`switch(config-if)# exit`
	`switch#`
		インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。

ステップ 4	**show feature** 例：	（任意）デバイス上でイネーブルされている機能に関する情報を表示します。

	コマンドまたはアクション	目的
	`switch(config-if)# show feature`	
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

トンネル インターフェイスの作成

トンネル インターフェイスを作成して、この論理インターフェイスを IP トンネルに設定できます。

（注） Cisco NX-OS は、最大 8 つの IP トンネルをサポートしています。

（注） トンネル インターフェイスおよび関連するすべての設定を削除するには、**no interface tunnel** コマンドを使用します。

コマンド	目的
no interface tunnel *number* 例： `switch(config)# no interface tunnel 1`	トンネル インターフェイスおよび関連する設定を削除します。
description *string* 例： `switch(config-if)# description GRE tunnel`	トンネルの説明を設定します。
mtu *value* 例： `switch(config-if)# mtu 1400`	インターフェイスで送信される IP パケットの MTU を設定します。
tunnel ttl *value* 例： `switch(config-if)# tunnel ttl 100`	トンネルの存続可能時間を設定します。範囲は 1 ～ 255 です。

（注） トンネルの宛先の **use-vrf** とは異なるトンネル インターフェイス VRF を使用する GREv6 トンネルまたは IP-in-IP トンネルを設定することは、サポートされていません。トンネル インターフェイスとトンネルの宛先で同じ VRF を使用する必要があります。GREv4 では、トンネルの use-vrf とは異なるトンネルインターフェイス VRF の設定がサポートされています。

始める前に

異なる VRF でトンネル送信元およびトンネル宛先を設定できます。トンネリング機能がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface tunnel** *number*
3. **tunnel mode** {**gre ip** | **ipip** {**ip** | **decapsulate-any**}}
4. **tunnel source** {*ip-address* |*interface-name*}
5. **tunnel destination** *ip{address | hostname}*
6. **tunnel use-vrf** *vrf-name*
7. **show interfaces tunnel** *number*
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface tunnel** *number*
	例：
	`switch(config)# interface tunnel 1`
	`switch(config-if)#`
		新しいトンネル インターフェイスを作成します。

ステップ 3	**tunnel mode** {**gre ip**	**ipip** {**ip**	**decapsulate-any**}}	このトンネルモードを GRE、ipip、または ipip decapsulate-only に設定します。 IP での GRE カプセル化の使用を指定するには、**gre** キーワードおよび **ip** キーワードを指定します。 **ipip** キーワードは、IP-in-IP カプセル化の使用を指定します。オプションの **decapsulate-any** キーワードは、トンネル インターフェイスの IP-in-IP トンネルを終了させます。このキーワードは、発信トラフィックを伝送しないトンネルを作成します。ただし、リ

	コマンドまたはアクション	目的
		モート トンネル エンド ポイントは、宛先として設定されたトンネルを使用できます。
ステップ 4	**tunnel source** {*ip-address* |*interface-name*} 例： `switch(config-if)# tunnel source ethernet 1/2`	このIPトンネルの送信元アドレスを設定します。送信元は、IPアドレスまたは論理インターフェイス名によって指定できます。
ステップ 5	**tunnel destination** *ip{address | hostname}* 例： `switch(config-if)# tunnel destination 192.0.2.1`	このIPトンネルの宛先アドレスを設定します。宛先は、IPアドレスまたは論理ホスト名によって指定できます。
ステップ 6	**tunnel use-vrf** *vrf-name* 例： `switch(config-if)# tunnel use-vrf blue`	（任意）設定された VRF をトンネルの IP 宛先アドレスの検索に使用します。
ステップ 7	**show interfaces tunnel** *number* 例： `switch# show interfaces tunnel 1`	（任意）トンネルインターフェイス統計情報を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

例

次に、トンネル インターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# interface tunnel 1
switch(config-if)# tunnel source ethenet 1/2
switch(config-if)# tunnel destination 192.0.2.1
switch(config-if)# copy running-config startup-config
```

ネットマスクを使用した IP-in-IP トンネルの作成

ネットマスクを使用して IP-in-IP トンネルを作成すると、トンネル送信元サブネットおよびトンネル宛先サブネットを指定することと、一致するパケットのカプセル化を解除することが可能になります。

- IP-in-IP decap-any トンネルは、任意の数の IP-in-IP トンネルからカプセル化されたパケットを受信します。

- ネットマスク機能により、スイッチは、ネットマスクに適合するIPアドレスからのパケットを受信します。

ネットマスク機能に関する注意事項

- ルーティング プロトコルは、ネットマスクを使用して作成された IP-in-IP トンネルではサポートされません。
- カプセル化はネットマスク機能ではサポートされていません。同じサブネットの一連の送信元からのカプセル化解除だけがサポートされています。

手順の概要

1. **configure terminal**
2. **interface tunnel** *number*
3. **tunnel mode ipip** [**ip**]
4. **tunnel source** *ip-address* / *mask_length*
5. **tunnel destination** *ip-address* / *mask_length*
6. （任意） **no shut**
7. **ip address** *ip-prefix*/*length*

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface tunnel** *number*
	例：
	`switch(config)# interface tunnel 5`
	`switch(config-if)#`
		新しいトンネル インターフェイスを作成します。

ステップ 3	**tunnel mode ipip** [**ip**]	このトンネル モードを ipip に設定します。 **ipip** キーワードは、IP-in-IP カプセル化の使用を指定します。
ステップ 4	**tunnel source** *ip-address* / *mask_length* 例： `switch(config-if)# tunnel source 33.1.1.1 255.255.255.0`	このIPトンネルの送信元アドレスを設定します。送信元は、IPアドレスとマスクの長さによって指定されます。
ステップ 5	**tunnel destination** *ip-address* / *mask_length* 例： `switch(config-if)# tunnel destination 33.1.1.2 255.255.255.0`	このIPトンネルの宛先アドレスを設定します。宛先は、IPアドレスとマスクの長さによって指定されます。

	コマンドまたはアクション	目的
ステップ 6	（任意） **no shut**	インターフェイスを消去します。
ステップ 7	**ip address** *ip-prefix/length* 例： `switch(config-if)# ip address 50.1.1.1/24`	このインターフェイスの IP アドレスを設定します。

例

次に、ネットマスクを使用して IP-in-IP トンネルを作成する例を示します。

```
switch(config)# interface tunnel 10
switch(config-if)# tunnel mode ipip
switch(config-if)# tunnel source 33.1.1.2/24
switch(config-if)# tunnel destination 33.1.1.1/24
switch(config-if)# no shut
switch(config-if)# ip address 10.10.10.10/24
switch(config-if)# end
switch# show interface tunnel 10
Tunnel10 is up
    Admin State: up
    Internet address is 10.10.10.10/24
    MTU 1476 bytes, BW 9 Kbit
    Tunnel protocol/transport IPIP/IP
    Tunnel source 33.1.1.2, destination 33.1.1.1
    Transport protocol is in VRF "default"
    Last clearing of "show interface" counters never
    Tx
    0 packets output, 0 bytes
    Rx
    0 packets input, 0 bytes

switch# show run interface tunnel 10

!Command: show running-config interface Tunnel10
!Time: Wed Aug 26 13:50:01 2015

version 7.0(3)I2(1)

interface Tunnel10
  ip address 10.10.10.10/24
  tunnel mode ipip ip
  tunnel source 33.1.1.2 255.255.255.0
  tunnel destination 33.1.1.1 255.255.255.0
  no shutdown
```

トンネル インターフェイスの設定

トンネル インターフェイスを GRE トンネル モード、ipip モード、または ipip カプセル化解除モードに設定できます。GRE モードはデフォルトのトンネル モードです。.

Cisco NX-OS Release 7.0(3)I6(1) 以降、**tunnel source direct** および **tunnel mode ipv6ipv6 decapsulate-any** CLI コマンドが Cisco Nexus 9000 シリーズ スイッチでサポートされています。

tunnel source direct および **tunnel mode ipv6ipv6 decapsulate-any** CLI コマンドは、Cisco Nexus 9000 シリーズ スイッチでサポートされています。

（注） Network Forwarding Engine（NFE）を搭載した Cisco Nexus 9500 プラットフォーム スイッチでは、**tunnel source direct**および **tunnel mode ipv6ipv6 decapsulate-any** CLI コマンドはサポートされていません。

IPv6 トランスポート（IPv6inIPv6 パケット）を介した IPv6 ペイロードをサポートするために、新しい CLI **tunnel mode ipv6ipv6 decapsulate-any** コマンドが導入されました。新しい CLI **tunnel source direct** コマンドを使用すれば、直接接続された IP アドレス（物理インターフェイス、ポートチャネル、ループバック、SVI など）で IP-in-IP トンネルのカプセル化解除を設定できます。

始める前に

トンネリング機能がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface tunnel** *number*
3. **tunnel mode** {**gre ip** | **ipip** | {**ip** | **decapsulate-any**}}
4. （任意） **tunnel mode ipv6ipv6 decapsulate-any**
5. **tunnel source direct**
6. **show interfaces tunnel** *number*
7. **mtu** *value*
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface tunnel** *number*
	例：
	`switch(config)# interface tunnel 1`
	`switch(config-if)#`
		新しいトンネル インターフェイスを作成します。

ステップ 3	**tunnel mode** {**gre ip**	**ipip**	{**ip**	**decapsulate-any**}}	このトンネルモードを GRE、ipip、または ipip decapsulate-only に設定します。

	コマンドまたはアクション	目的
		IP での GRE カプセル化の使用を指定するには、**gre** キーワードおよび **ip** キーワードを指定します。 ipip キーワードは、IP-in-IP カプセル化の使用を指定します。オプションの **decapsulate-any** キーワードは、トンネル インターフェイスの IP-in-IP トンネルを終了させます。このキーワードは、発信トラフィックを伝送しないトンネルを作成します。ただし、リモート トンネル エンド ポイントは、宛先として設定されたトンネルを使用できます。
ステップ 4	（任意） **tunnel mode ipv6ipv6 decapsulate-any**	IPv6 トランスポートを介した IPv6 ペイロード（IPv6 パケット）をサポートします（7.0(3)I6(1) 以降）。この手順は、IPv6 ネットワークにのみ適用されます。 （注） このコマンドは、Cisco Nexus 9500-GX プラットフォーム スイッチではサポートされていません。
ステップ 5	**tunnel source direct**	直接接続されている IP アドレスで IP-in-IP トンネルのカプセル化解除を設定します。このオプションは、IP-in-IP カプセル化解除を使用してネットワーク経由でパケットを送信する場合にのみサポートされるようになりました。 （注） このコマンドは、Network Forwarding Engine（NFE）を備えた Cisco Nexus 9500 プラットフォームスイッチではサポートされません。
ステップ 6	**show interfaces tunnel** *number* 例： `switch(config-if)# show interfaces tunnel 1`	（任意）トンネルインターフェイス統計情報を表示します。
ステップ 7	**mtu** *value*	インターフェイスで送信される IP パケットの Maximum Transmission Unit（MTU; 最大伝送単位）を設定します。 有効な範囲は 64 ～ 9192 ユニットです。

	コマンドまたはアクション	目的
		（注） **tunnel mode ipip** を設定する場合、その範囲は NX-OS のリリースによって異なります。 • 64 ~ 9192 ユニット • 64 ~ 9196 ユニット
ステップ 8	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

例

次に、GRE へのトンネル インターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# interface tunnel 1
switch(config-if)# tunnel mode gre ip
switch(config-if)# copy running-config startup-config
```

次に、ipip トンネルを作成する例を示します。

```
switch# configure terminal
switch(config)# interface tunnel 1
switch(config-if)# tunnel mode ipip
switch(config-if)# mtu 1400
switch(config-if)# copy running-config startup-config
switch(config-if)# no shut
```

次に、直接接続された IP アドレスで IP-in-IP トンネルのカプセル化解除を設定する例を示します。

```
switch# configure terminal
switch(config)# interface tunnel 0
switch(config-if)# tunnel mode ipip ip
switch(config-if)# tunnel source direct
switch(config-if)# description IPinIP Decapsulation Interface
switch(config-if)# no shut
```

次に、IPv6 対応ネットワークで IP-in-IP トンネルのカプセル化解除を設定する例を示します。

```
!
interface tunnel 1
  ipv6 address use-link-local-only             <<< enable IPv6
  tunnel mode ipv6ipv6 decapsulate-any
  tunnel source direct
  description IPinIP Decapsulation Interface
  mtu 1476
  no shutdown

show running-config interface tunnel 1
```

```
interface Tunnel1
  tunnel mode ipv6ipv6 decapsulate-any
  tunnel source direct
  no shutdown

show interface tunnel 1
Tunnel1 is up    Admin State: up
MTU 1460 bytes, BW 9 Kbit
Tunnel protocol/transport IPv6/DECAPANY/IPv6
Tunnel source - direct
Transport protocol is in VRF "default"
Tunnel interface is in VRF "default"
Last clearing of "show interface" counters never
Tx    0 packets output, 0 bytes    Rx    0 packets input, 0 bytes
```

GRE トンネルの設定

トンネル インターフェイスを GRE トンネル モードに設定できます。

（注） Cisco NX-OSは、IPV4 over IPV4のGREプロトコルのみをサポートします。

始める前に

トンネリング機能がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface tunnel** *number*
3. **tunnel mode gre ip**
4. **show interfaces tunnel** *number*
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface tunnel** *number*
	例：
	`switch(config)# interface tunnel 1`
	`switch(config-if)#`
		新しいトンネル インターフェイスを作成します。

	コマンドまたはアクション	目的
ステップ 3	**tunnel mode gre ip** 例： `switch(config-if)# tunnel mode gre ip`	このトンネル モードを GRE に設定します。
ステップ 4	**show interfaces tunnel** *number* 例： `switch(config-if)# show interfaces tunnel 1`	（任意）トンネルインターフェイス統計情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

Path MTU Discovery のイネーブル化

tunnel path-mtu discovery コマンドを使用し、トンネルのパスMTUディスカバリをイネーブルにします。

手順の概要

1. **tunnel path-mtu-discovery age-timer** *min*
2. **tunnel path-mtu-discovery min-mtu** *bytes*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**tunnel path-mtu-discovery age-timer** *min* 例： `switch(config-if)# tunnel path-mtu-discovery age-timer 25`	トンネル インターフェイスで Path MTU Discovery（PMTUD）をイネーブルにします。 • min：分数。指定できる範囲は 10 ～ 30 です。デフォルトは 10 です。
ステップ 2	**tunnel path-mtu-discovery min-mtu** *bytes* 例： `switch(config-if)# tunnel path-mtu-discovery min-mtu 1500`	トンネル インターフェイスで Path MTU Discovery（PMTUD）をイネーブルにします。 • bytes：認識された最小 MTU。 範囲は64ー9192です。デフォルトは 64 です。

トンネル インターフェイスへの VRF メンバーシップの割り当て

VRF にトンネル インターフェイスを追加できます。

始める前に

トンネリング機能がイネーブルになっていることを確認します。

VRF 用のインターフェイスを設定した後で、トンネル インターフェイスに IP アドレスを割り当てます。

手順の概要

1. **configure terminal**
2. **interface tunnel** *number*
3. **vrf member** *vrf-name*
4. **ip address** *ip-prefix/length*
5. **show vrf** [*vrf-name*] **interface** *interface-type number*
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface tunnel** *number*
	例：
	`switch(config)# interface tunnel 0`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	**vrf member** *vrf-name* 例： `switch(config-if)# vrf member RemoteOfficeVRF`	このインターフェイスを VRF に追加します。
ステップ 4	**ip address** *ip-prefix/length* 例： `switch(config-if)# ip address 192.0.2.1/16`	このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。
ステップ 5	**show vrf** [*vrf-name*] **interface** *interface-type number* 例： `switch(config-vrf)# show vrf Enterprise interface tunnel 0`	（任意）VRF 情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意）この設定の変更を保存します。

例

次に、VRF にトンネル インターフェイスを追加する例を示します。

```
switch# configure terminal
switch(config)# interface tunnel 0
switch(config-if)# vrf member RemoteOfficeVRF
switch(config-if)# ip address 209.0.2.1/16
switch(config-if)# copy running-config startup-config
```

IP トンネル設定の確認

IP トンネルの設定情報を確認するには、次のいずれかの作業を行います。

コマンド	目的
show interface tunnel *number*	トンネル インターフェイスの設定を表示します（MTU、プロトコル、転送、および VRF）。入力および出力パケット、バイト、およびパケット レートを表示します。
show interface tunnel *number* **brief**	トンネル インターフェイスの動作状態、IP アドレス、カプセル化のタイプ、MTU を表示します。
show interface tunnel *number* **counters**	入出力パケットのインターフェイス カウンタを表示します。 （注） インターフェイス カウンタとともに表示されるバイト カウントには、内部ヘッダー サイズが含まれます。
show interface tunnel *number* **description**	トンネル インターフェイスに設定された説明を表示します。
show interface tunnel *number* **status**	トンネル インターフェイスの動作ステータスを表示します。
show interface tunnel *number* **status err-disabled**	トンネル インターフェイスの errdisable 状態を表示します。

IP トンネリングの設定例

次の例では、簡易 GRE トンネルを示します。イーサネット 1/2 は、ルータ A のトンネル送信元であり、ルータ B のトンネル宛先です。イーサネット インターフェイス 2/1 は、ルータ B のトンネル送信元であり、ルータ A のトンネル宛先です。

ルータ A：

```
feature tunnel
interface tunnel 0
ip address 209.165.20.2/8
tunnel source ethernet 1/2
tunnel destination 192.0.2.2
tunnel mode gre ip
tunnel path-mtu-discovery 25 1500

interface ethernet 1/2
ip address 192.0.2.55/8
```

ルータ B：

```
feature tunnel
interface tunnel 0
ip address 209.165.20.1/8
tunnel source ethernet 2/1
tunnel destination 192.0.2.55
tunnel mode gre ip

interface ethernet 2/1
ip address 192.0.2.2/8
```

関連資料

関連項目	マニュアル タイトル
IP トンネル コマンド	『*Cisco Nexus 9000 Series NX-OS Interfaces Command Reference*』