



IP

- [clear ip nhrp \(2 ページ\)](#)
- [debug nhrp \(4 ページ\)](#)
- [fhrp delay \(6 ページ\)](#)
- [fhrp version vrrp v3 \(7 ページ\)](#)
- [ip address dhcp \(8 ページ\)](#)
- [ip address pool \(DHCP\) \(12 ページ\)](#)
- [ip address \(13 ページ\)](#)
- [ip nhrp map \(16 ページ\)](#)
- [ip nhrp map multicast \(18 ページ\)](#)
- [ip nhrp network-id \(20 ページ\)](#)
- [ip nhrp nhs \(21 ページ\)](#)
- [ipv6 nd cache expire \(23 ページ\)](#)
- [ipv6 nd na glean \(25 ページ\)](#)
- [ipv6 nd nud retry \(26 ページ\)](#)
- [key chain \(28 ページ\)](#)
- [key-string \(認証\) \(29 ページ\)](#)
- [key \(30 ページ\)](#)
- [show ip nhrp nhs \(32 ページ\)](#)
- [show ip ports all \(35 ページ\)](#)
- [show key chain \(37 ページ\)](#)
- [show track \(38 ページ\)](#)
- [track \(40 ページ\)](#)
- [vrrp \(42 ページ\)](#)
- [vrrp description \(43 ページ\)](#)
- [vrrp preempt \(44 ページ\)](#)
- [vrrp priority \(46 ページ\)](#)
- [vrrp timers advertise \(47 ページ\)](#)
- [vrrs leader \(49 ページ\)](#)

clear ip nhrp

Next Hop Resolution Protocol (NHRP) キャッシュ内のすべてのダイナミックエントリをクリアするには、ユーザ EXEC モードまたは特権 EXEC モードで **clear ip nhrp** コマンドを使用します。

```
clear ip nhrp[{vrf {vrf-name | global}}] [{dest-ip-address [{dest-mask}] | tunnel number | counters
[{interface tunnel number}] | stats [{tunnel number}{vrf {vrf-name | global}}]]}]
```

構文の説明

vrf	(任意) 指定された Virtual Routing and Forwarding (VRF) インスタンスの NHRP キャッシュからエントリを削除します。
<i>vrf-name</i>	(任意) コマンドが適用された VRF アドレス ファミリの名前。
global	(任意) グローバル VRF インスタンスを指定します。
<i>dest-ip-address</i>	(任意) 宛先 IP アドレス。この引数を指定すると、指定された宛先 IP アドレスの NHRP マッピングエントリがクリアされます。
<i>dest-mask</i>	(任意) 宛先ネットワークマスク。
counters	(任意) NHRP カウンタをクリアします。
interface	(任意) すべてのインターフェイスの NHRP マッピングエントリをクリアします。
<i>tunnel number</i>	(任意) NHRP キャッシュから指定されたインターフェイスを削除します。
stats	(任意) すべてのインターフェイスの IPv4 統計情報をすべてクリアします。

コマンドモード

ユーザ EXEC (>)

特権 EXEC (#)

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

clear ip nhrp コマンドでは、スタティックに設定された IP と NBMA のいずれのアドレスマッピングも NHRP キャッシュからクリアしません。

例

次に、インターフェイスの NHRP キャッシュ内のダイナミックエントリすべてをクリアする例を示します。

```
Switch# clear ip nhrp
```

関連コマンド

コマンド	説明
show ip nhrp	NHRP マッピング情報を表示します。

debug nhrp

Next Hop Resolution Protocol (NHRP) のデバッグを有効にするには、特権 EXEC モードで **debug nhrp** コマンドを使用します。デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
debug nhrp [{attribute | cache | condition {interface tunnel number | peer {nbma
{ipv4-nbma-address nbma-name ipv6-nbma-address} } | unmatched | vrf vrf-name } | detail | error
| extension | group | packet | rate}]
no debug nhrp [{attribute | cache | condition {interface tunnel number | peer {nbma
{ipv4-nbma-address nbma-name ipv6-nbma-address} } | unmatched | vrf vrf-name } | detail | error
| extension | group | packet | rate}]
```

構文の説明

attribute	(任意) NHRP 属性デバッグ操作を有効にします。
cache	(任意) NHRP キャッシュ デバッグ操作を有効にします。
condition	(任意) NHRP 条件デバッグ操作を有効にします。
interface tunnel number	(任意) トンネルインターフェイスのデバッグ操作を有効にします。
nbma	(任意) ノンブロードキャスト マルチプル アクセス (NBMA) ネットワークのデバッグ操作を有効にします。
<i>ipv4-nbma-address</i>	(任意) NBMA ネットワークの IPv4 アドレスに基づくデバッグ操作を有効にします。
<i>nbma-name</i>	(任意) NBMA ネットワーク名。
<i>IPv6-address</i>	(任意) NBMA ネットワークの IPv6 アドレスに基づくデバッグ操作を有効にします。 (注) <i>IPv6-address</i> 引数は、Cisco IOS XE Denali 16.3.1 ではサポートされていません。
vrf vrf-name	(任意) Virtual Routing and Forwarding インスタンスのデバッグ操作を有効にします。
detail	(任意) NHRP デバッグの詳細なログを表示します。
error	(任意) NHRP エラー デバッグ操作を有効にします。
extension	(任意) NHRP 拡張処理デバッグ操作を有効にします。
group	(任意) NHRP グループ デバッグ操作を有効にします。
packet	(任意) NHRP アクティビティ デバッグを有効にします。
rate	(任意) NHRP レート制限を有効にします。

routing	(任意) NHRP ルーティング デバッグ操作を有効にします。
---------	---------------------------------

コマンド デフォルト NHRP デバッグは有効になっていません。

コマンド モード 特権 EXEC (#)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン



(注) Cisco IOS XE Denali 16.3.1 では、このコマンドは IPv4 だけをサポートしています。
IPv6-nbma-address 引数は、スイッチでは使用可能ですが、設定しても機能しません。

NHRP 属性ログを表示するには、**debug nhrp detail** コマンドを使用します。

Virtual-Access number キーワードと引数のペアは、デバイスで仮想アクセスインターフェイスが使用可能な場合にのみ表示されます。

例

次に、**debug nhrp** コマンドの出力例と、IPv4 に関する NHRP デバッグ出力を表示する例を示します。

```
Switch# debug nhrp

Aug  9 13:13:41.486: NHRP: Attempting to send packet via DEST 10.1.1.99
Aug  9 13:13:41.486: NHRP: Encapsulation succeeded. Tunnel IP addr 10.11.11.99
Aug  9 13:13:41.486: NHRP: Send Registration Request via Tunnel0 vrf 0, packet size: 105
Aug  9 13:13:41.486:      src: 10.1.1.11, dst: 10.1.1.99
Aug  9 13:13:41.486: NHRP: 105 bytes out Tunnel0
Aug  9 13:13:41.486: NHRP: Receive Registration Reply via Tunnel0 vrf 0, packet size:
125
Aug  9 13:13:41.486: NHRP: netid_in = 0, to_us = 1
```

関連コマンド

コマンド	説明
show ip nhrp	NHRP マッピング情報を表示します。

fhrp delay

First Hop Redundancy Protocol (FHRP) クライアントの初期化の遅延時間を指定するには、インターフェイス コンフィギュレーション モードで **fhrp delay** コマンドを使用します。指定した時間を削除するには、このコマンドの **no** 形式を使用します。

```
fhrp delay {[minimum] [reload] seconds}
no fhrp delay {[minimum] [reload] seconds}
```

構文の説明

minimum	(任意) インターフェイスが使用可能になった後の遅延時間を設定します。
reload	(任意) デバイスのリロード後の遅延時間を設定します。
<i>seconds</i>	秒単位の遅延時間。範囲は 0 ~ 3600 です。

コマンド デフォルト なし

コマンド モード インターフェイス コンフィギュレーション (config-if)

例 次に、FHRP クライアントの初期化の遅延期間を指定する例を示します。

```
Device(config-if)# fhrp delay minimum 90
```

関連コマンド

コマンド	説明
show fhrp	ファーストホップ冗長性プロトコル (FHRP) の情報を表示します。

fhrp version vrrp v3

Virtual Router Redundancy Protocol バージョン 3 (VRRPv3) と Virtual Router Redundancy Service (VRRS) をデバイスで有効にするには、グローバル コンフィギュレーション モードで **fhrp version vrrp v3** コマンドを使用します。VRRPv3 と VRRS の設定機能をデバイスで無効にするには、このコマンドの **no** 形式を使用します。

fhrp version vrrp v3
no fhrp version vrrp v3

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

VRRPv3 と VRRS 設定はデバイスで有効になっていません。

コマンド モード

グローバル コンフィギュレーション (config)

使用上のガイドライン

VRRPv3 が使用中の場合、VRRP バージョン 2 (VRRPv2) は使用できません。

例

次の例では、トラッキングプロセスは、VRRPv3 グループを使用して IPv6 オブジェクトの状態を追跡するように設定されています。ギガビットイーサネットインターフェイス 0/0/0 の VRRP は、VRRPv3 グループで IPv6 オブジェクトに何らかの変更が生じた場合には通知されるように、トラッキングプロセスに登録します。シリアルインターフェイス VRRPv3 の IPv6 オブジェクトステータスがダウンになると、VRRP グループのプライオリティは 20 だけ引き下げられます。

```
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# vrrp 1 address-family ipv6
Device(config-if-vrrp)# track 1 decrement 20
```

関連コマンド

コマンド	説明
track (VRRP)	VRRPv3 グループを使用したオブジェクトの追跡を有効にします。

ip address dhcp

DHCP からインターフェイスの IP アドレスを取得するには、インターフェイス コンフィギュレーションモードで **ip address dhcp** コマンドを使用します。取得されたいずれかのアドレスを削除するには、このコマンドの **no** 形式を使用します。

ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]
no ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]

構文の説明

client-id	(任意) クライアント ID を指定します。デフォルトでは、クライアント識別子は ASCII 値です。 client-id interface-type number オプションは、クライアント識別子を、指定されたインターフェイスの 16 進数 MAC アドレスに設定します。
<i>interface-type</i>	(任意) インターフェイスタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用します。
<i>number</i>	(任意) インターフェイスまたはサブインターフェイスの番号です。ネットワークワーキングデバイスに対する番号付け構文の詳細については、疑問符 (?) のオンラインヘルプ機能を使用してください。
hostname	(任意) ホスト名を指定します。
<i>hostname</i>	(任意) ホスト名を DHCP オプション 12 フィールドに配置します。この名前は、グローバルコンフィギュレーションモードで入力されたホスト名と同じにする必要はありません。

コマンド デフォルト

ホスト名は、デバイスのグローバルコンフィギュレーションホスト名です。クライアント識別子は ASCII 値です。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンド履歴

リリース	変更内容
12.1(2)T	このコマンドが導入されました。
12.1(3)T	このコマンドが変更されました。 client-id キーワードと <i>interface-type number</i> 引数が追加されました。
12.2(3)	このコマンドが変更されました。 hostname キーワードと <i>hostname</i> 引数が追加されました。 client-id interface-type number オプションの動作は変更されています。詳細については、「使用上のガイドライン」セクションを参照してください。
12.2(8)T	このコマンドが変更されました。このコマンドは、ATM (PPPoA) インターフェイスおよび特定の ATM インターフェイスでの PPP の使用のために展開されました。

リリース	変更内容
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。
15.1(3)T	このコマンドが変更されました。トンネルインターフェイスでのサポートが提供されていました。

使用上のガイドライン



- (注) Cisco IOS リリース 12.2(8)T よりも前には、**ip address dhcp** コマンドはイーサネット インターフェイスのみで使用が可能でした。

ip address dhcp コマンドを使用すると、インターフェイスは DHCP プロトコルを使用して IP アドレスを動的に学習できます。これはインターネットサービスプロバイダー (ISP) に動的に接続するイーサネットインターフェイスで特に役立ちます。このインターフェイスにダイナミックアドレスを割り当てると、同インターフェイスを使用して、Cisco IOS ネットワークアドレス変換 (NAT) のポートアドレス変換 (PAT) で、デバイスに接続済みの個別に処理されたネットワークにインターネットアクセスを提供できます。

また **ip address dhcp** コマンドは、ATM ポイントツーポイント インターフェイスと連動し、どのカプセル化方式でも受け入れます。ただし、ATM マルチポイントインターフェイスの場合、**protocol ip inarp** インターフェイス コンフィギュレーションコマンドで Inverse ARP を指定し、**aa15snap** カプセル化タイプのみを使用する必要があります。

一部の ISP の場合、DHCPDISCOVER メッセージに、特定のホスト名と、インターフェイスの MAC アドレスであるクライアント識別子を含める必要があります。**ip address dhcp client-id interface-type number hostname hostname** コマンドは、*interface-type* が、このコマンドが設定されたイーサネット インターフェイスであり、*interface-type number* が ISP によって提供されたホスト名である場合に最も一般的に使用されます。

クライアント識別子 (DHCP オプション 61) には、16 進数または ASCII 値を使用できます。デフォルトでは、クライアント識別子は ASCII 値です。**client-id interface-type number** オプションは、デフォルトの値を上書きし、指定されたインターフェイスの 16 進数 MAC アドレスの使用を強制します。



- (注) Cisco IOS リリース 12.1(3)T から 12.2(3) までのリリースでは、**client-id** オプションキーワードは、クライアント識別子の ASCII 固定値の変更を許可します。リリース 12.2(3) 以降、**client-id** オプションキーワードは、クライアント識別子として指定されたインターフェイスの 16 進数 MAC アドレスの使用を強制します。

DHCP サーバから IP アドレスを取得するようシスコ デバイスが設定されている場合、デバイスは、ネットワークの DHCP サーバにデバイスに関する情報を提供する DHCPDISCOVER メッセージを送信します。

ip address dhcp コマンドを使用する場合、オプションキーワードの有無にかかわらず、DHCP オプション 12 フィールド（ホスト名オプション）が DISCOVER メッセージに含まれます。デフォルトでは、オプション 12 で指定されたホスト名は、デバイスのグローバルコンフィギュレーション ホスト名になります。ただし、**ip address dhcp hostname hostname** コマンドを使用して、デバイスのグローバルコンフィギュレーション ホスト名ではない別の名前を DHCP オプション 12 フィールドに入力することもできます。

no ip address dhcp コマンドは、取得済みの IP アドレスを削除して、DHCPRELEASE メッセージを送信します。

DHCP サーバで必要なものを判別するため、さまざまな設定を試行しなければならない場合があります。下の表に、使用可能なコンフィギュレーション方式と、各方式の DISCOVER メッセージに含まれる情報を示します。

表 1: コンフィギュレーション方式と生成される DISCOVER メッセージの内容

コンフィギュレーション方式	DISCOVER メッセージの内容
ip address dhcp	DISCOVER メッセージのクライアント ID フィールドには「cisco-mac-address-Eth1」が含まれます。 <i>mac-address</i> は、イーサネット 1 インターフェイスの MAC アドレスで、オプション 12 フィールドのデバイスのデフォルト ホスト名を含んでいます。
ip address dhcp hostname hostname	DISCOVER メッセージのクライアント ID フィールドには「cisco-mac-address-Eth1」が含まれます。 <i>mac-address</i> は、イーサネット 1 インターフェイスの MAC アドレスで、オプション 12 フィールドの <i>hostname</i> を含んでいます。
ip address dhcp client-id ethernet 1	DISCOVER メッセージは、クライアント ID フィールドにイーサネット 1 インターフェイスの MAC アドレスを含んでおり、オプション 12 フィールドにデバイスのデフォルト ホスト名を含んでいます。
ip address dhcp client-id ethernet 1 hostname hostname	DISCOVER メッセージは、クライアント ID フィールドにイーサネット 1 インターフェイスの MAC アドレスを含んでおり、オプション 12 フィールドに <i>hostname</i> を含んでいます。

例

次の例では、**ip address dhcp** コマンドがイーサネット インターフェイス 1 に入力されます。次の例のように設定されたデバイスによって送信された DISCOVER メッセージには、クライアント ID フィールドの「cisco-mac-address-Eth1」と、オプション 12 フィールドの値 abc が含まれます。

```
hostname abc
```

```
!
interface GigabitEthernet 1/0/1
 ip address dhcp
```

次の例のように設定されたデバイスによって送信された DISCOVER メッセージには、クライアント ID フィールドの「cisco- mac-address -Eth1」と、オプション 12 フィールドの値 def が含まれます。

```
hostname abc
!
interface GigabitEthernet 1/0/1
 ip address dhcp hostname def
```

次の例のように設定されたデバイスによって送信された DISCOVER メッセージには、クライアント ID フィールドのイーサネットインターフェイス 1 の MAC アドレスと、オプション 12 フィールドの値 abc が含まれます。

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id GigabitEthernet 1/0/1
```

次の例のように設定されたデバイスによって送信された DISCOVER メッセージには、クライアント ID フィールドのイーサネットインターフェイス 1 の MAC アドレスと、オプション 12 フィールドの値 def が含まれます。

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id GigabitEthernet 1/0/1 hostname def
```

関連コマンド

コマンド	説明
ip dhcp pool	Cisco IOS DHCP サーバに DHCP アドレス プールを設定し、DHCP プール コンフィギュレーション モードを開始します。

ip address pool (DHCP)

Dynamic Host Configuration Protocol (DHCP) に IP Control Protocol (IPCP) ネゴシエーションからサブネットが入力されるときに、インターフェイスの IP アドレスが自動設定されるようにするには、インターフェイス コンフィギュレーション モードで **ip address pool** コマンドを使用します。インターフェイスの IP アドレスの自動設定を無効にするには、このコマンドの **no** 形式を使用します。

ip address pool name
no ip address pool

構文の説明

<i>name</i>	DHCP プールの名前。インターフェイスの IP アドレスは、 <i>name</i> で指定された DHCP プールから自動設定されます。
-------------	--

コマンド デフォルト

IP アドレスのプーリングは無効になっています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(8)T	このコマンドが導入されました。

使用上のガイドライン

デバイスの DHCP プールによって処理する必要のある LAN に接続されている DHCP クライアントが存在する場合、このコマンドを使用して LAN インターフェイスの IP アドレスを自動設定します。DHCP プールは、IPCP サブネット ネゴシエーションによってサブネットを動的に取得します。

例

次の例では、GigabitEthernet インターフェイス 1/0/1 の IP アドレスが abc という名前のアドレス プールから自動設定されるように指定します。

```
ip dhcp pool abc
  import all
  origin ipcp
!
interface GigabitEthernet 1/0/1
  ip address pool abc
```

関連コマンド

コマンド	説明
show ip interface	IP 用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。

ip address

インターフェイスのプライマリまたはセカンダリ IP アドレスを設定するには、インターフェイス コンフィギュレーション モードで **ip address** コマンドを使用します。IP アドレスを削除するか、IP 処理を無効にするには、このコマンドの **no** 形式を使用します。

```
ip address ip-address mask [secondary [vrf vrf-name ]]
no ip address ip-address mask [secondary [vrf vrf-name ]]
```

構文の説明

<i>ip-address</i>	IP アドレス。
<i>mask</i>	関連する IP サブネットのマスク。
secondary	(任意) 設定されたアドレスをセカンダリ IP アドレスに指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。 (注) セカンダリ アドレスが vrf のキーワードでの VRF テーブルの設定に使用される場合には、 vrf キーワードも指定する必要があります。
vrf	(任意) VRF テーブルの名前 <i>vrf-name</i> 引数は、入力インターフェイスの VRF 名を指定します。

コマンドデフォルト IP アドレスはインターフェイスに定義されません。

コマンドモード インターフェイス コンフィギュレーション (config-if)

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン

インターフェイスには、1つのプライマリ IP アドレスと複数のセカンダリ IP アドレスを設定できます。Cisco IOS ソフトウェアにより生成されるパケットは、必ずプライマリ IP アドレスを使用します。そのため、セグメントのすべてのデバイスとアクセスサーバは、同じプライマリ ネットワーク番号を共有する必要があります。

ホストは、Internet Control Message Protocol (ICMP) マスク要求メッセージを使用して、サブネットマスクを判別できます。デバイスは、ICMP マスク応答メッセージでこの要求に応答できます。

no ip address コマンドを使用して IP アドレスを削除することにより、特定のインターフェイス上の IP 処理を無効にできます。ソフトウェアが、その IP アドレスのいずれかを使用する別のホストを検出すると、コンソールにエラーメッセージを出力します。

オプションの **secondary** キーワードを使用すると、セカンダリアドレスを無制限に指定できます。システムがセカンダリの送信元アドレスのルーティングの更新以外にデータグラムを生成

しないということを除けば、セカンダリ アドレスはプライマリ アドレスのように処理されます。IP ブロードキャストおよび Address Resolution Protocol (ARP) 要求は、IP ルーティング テーブルのインターフェイス ルートのように、正しく処理されます。

セカンダリ IP アドレスは、さまざまな状況で使用できます。次に、一般的な使用状況を示します。

- 特定のネットワーク セグメントに十分なホスト アドレスがない場合。たとえば、サブネット化により、論理サブネットあたり最大 254 のホストを使用できますが、1 つの物理サブネットでは、300 のホスト アドレスが必要になります。デバイスまたはアクセスサーバでセカンダリ IP アドレスを使用すると、2 つの論理サブネットで 1 つの物理サブネットを使用できます。
- レベル 2 ブリッジを使用して構築された旧式ネットワークがたくさんある場合。セカンダリ アドレスは、慎重に使用することで、サブネット化されたデバイスベース ネットワークへの移行に役立ちます。旧式のブリッジセグメントのデバイスでは、そのセグメントに複数のサブネットがあることを簡単に認識させることができます。
- 1 つのネットワークの 2 つのサブネットは、別の方法で、別のネットワークにより分離できる場合があります。サブネットが使用中の場合、この状況は許可されません。このような場合、最初のネットワークは、セカンダリ アドレスを使用している 2 番目のネットワークの上に拡張されます。つまり、上の階層となります。



(注)

- ネットワーク セグメント上のすべてのデバイスがセカンダリ アドレスを使用した場合、同一のセグメント上にある他のデバイスも、同一のネットワークまたはサブネットからセカンダリ アドレスを使用しなければなりません。ネットワーク セグメント上のセカンダリ アドレスの使用に矛盾があると、ただちにルーティング ループが引き起こされる可能性があります。
- Open Shortest Path First (OSPF) アルゴリズムを使用してルーティングする場合は、インターフェイスのすべてのセカンダリ アドレスがプライマリ アドレスと同じ OSPF エリアにあることを確認してください。
- セカンダリ IP アドレスを設定する場合は、CPU 使用率が高くないように、**no ip redirects** コマンドを入力して ICMP リダイレクトメッセージの送信を無効にする必要があります。

インターフェイスで IP を透過的にブリッジする前に、次の手順を実行する必要があります。

- IP ルーティングを無効にします (**no ip routing** コマンドを指定します)。
- インターフェイスをブリッジグループに追加して、**bridge-group** コマンドを参照してください。

インターフェイスで IP のルーティングと透過的なブリッジングを同時に実行するには、**bridge crb** コマンドを参照してください。

例

次の例では、192.108.1.27 がプライマリ アドレスで、192.31.7.17 が GigabitEthernet インターフェイス 1/0/1 のセカンダリ アドレスです。

```
Device# enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 192.108.1.27 255.255.255.0
Device(config-if)# ip address 192.31.7.17 255.255.255.0 secondary
```

関連コマンド

Command	Description
match ip route-source	送信元 IP アドレスを、VRF で接続されたルートに基づいて設定された必要なルート マップに一致するように指定します。
route-map	1 つのルーティング プロトコルから他のルーティング プロトコルへのルートを再配布するか、またはポリシー ルーティングを有効にするための条件を定義します。
set vrf	ポリシーベース ルーティング VRF の選択のために、ルート マップ内で VPN VRF 選択を有効にします。
show ip arp	SLIP アドレスが固定 ARP テーブル エントリとして表示される ARP キャッシュを表示します。
show ip interface	IP 用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。
show route-map	静的ルートマップと動的ルートマップを表示します。

ip nhrp map

ノンブロードキャストマルチアクセス (NBMA) ネットワークに接続された IP 宛先の IP と NBMA 間のアドレスマッピングをスタティックに設定するには、インターフェイス コンフィギュレーション モードで **ip nhrp map** コマンドを使用します。Next Hop Resolution Protocol (NHRP) キャッシュからスタティックエントリを削除するには、このコマンドの **no** 形式を使用します。

```
ip nhrp map ip-address {ip-nbma-address | destination-mask [{ip-nbma-address ipv6-nbma-address}]
ipv6-nbma-address}
no ip nhrp map ip-address {ip-nbma-address | destination-mask [{ip-nbma-address
ipv6-nbma-address}] ipv6-nbma-address}
```

構文の説明		
	<i>ip-address</i>	NBMA ネットワーク経由で到達可能な宛先の IP アドレス。このアドレスは、NBMA アドレスにマッピングされます。
	<i>ip-nbma-address</i>	NBMA ネットワーク経由で直接到達可能な NBMA アドレス。アドレス形式はメディアによって異なります。たとえば、ATM にはネットワーク サービスアクセスポイント (NSAP) アドレスがあり、イーサネットには MAC アドレスがあり、Switched Multimegabit Data Service (SMDS; スイッチドマルチメガビットデータ サービス) には E.164 アドレスがあります。このアドレスは、IP アドレスにマッピングされます。
	<i>destination-mask</i>	宛先アドレス マスク。
	<i>ipv6-nbma-address</i>	IPv6 NBMA アドレス。 (注) この引数は、Cisco IOS XE Denali 16.3.1 ではサポートされていません。

コマンド デフォルト スタティック IP-to-NBMA キャッシュは存在しません。

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン Cisco IOS XE Denali 16.3.1 では、NHRP はハブ/スポーク間通信のみをサポートし、スポーク間通信はサポートされていません。



(注) Cisco IOS XE Denali 16.3.1 では、このコマンドは IPv4 だけをサポートしています。
ipv6-nbma-address 引数は、スイッチでは使用可能ですが、設定しても機能しません。

ネクストホップサーバに到達するには、少なくとも1つのスタティック マッピングを設定します。統計的に複数のIP-to-NBMAアドレスマッピングを設定するには、このコマンドを複数回設定します。

ルーティングプロトコル、Open Shortest Path First (OSPF) または Enhanced Interior Gateway Routing Protocol (EIGRP) を使用している場合は、トラフィックを許可するトンネルで、**ip ospf network point-to-multipoint** コマンド (OSPF がハブ/スポーク通信に使用されている場合) および **ip split-horizon eigrp** コマンド (EIGRP が使用されている場合) を設定します。

例

次に、マルチポイントトンネルネットワーク内のこのステーションが2つのネクストホップサーバ 10.0.0.1 と 10.0.1.3 によってサービス提供されるようにスタティックに設定する例を示します。10.0.0.1 の NBMA アドレスは 192.0.2.1 としてスタティックに設定され、10.0.1.3 の NBMA アドレスは 198.51.100.1 です。

```
Switch(config)# interface tunnel 0
Switch(config-if)# ip nhrp nhs 10.0.0.1
Switch(config-if)# ip nhrp nhs 10.0.1.3
Switch(config-if)# ip nhrp map 10.0.0.1 192.0.2.1
Switch(config-if)# ip nhrp map 10.0.1.3 198.51.100.1
```

関連コマンド

Command	Description
clear ip nhrp	NHRP キャッシュからすべてのダイナミック エントリを削除します。
debug nhrp	NHRP デバッグをイネーブルにします。
interface	インターフェイスを設定し、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。
ip split-horizon eigrp	EIGRP スプリット ホライズンを有効にします。
ip ospf network point-to-multipoint	OSPF ネットワーク タイプをポイントツーマルチポイントに設定します。

ip nhrp map multicast

トンネルネットワーク経由で送信されるブロードキャストまたはマルチキャストパケットの宛先として使用されるノンブロードキャスト マルチアクセス (NBMA) アドレスを設定するには、インターフェイス コンフィギュレーション モードで **ip nhrp map multicast** コマンドを使用します。宛先を削除するには、このコマンドの **no** 形式を使用します。

ip nhrp map multicast {*ip-nbma-address* *ipv6-nbma-address* | **dynamic**}
no ip nhrp map multicast {*ip-nbma-address* *ipv6-nbma-address* | **dynamic**}

構文の説明	
<i>ip-nbma-address</i>	NBMA ネットワーク経由で直接到達可能な NBMA アドレス。アドレス形式は、使用しているメディアによって異なります。
<i>ipv6-nbma-address</i>	IPv6 NBMA アドレス。 (注) この引数は、Cisco IOS XE Denali 16.3.1 ではサポートされていません。
dynamic	ハブのクライアント登録から宛先をダイナミックに学習します。

コマンド デフォルト NBMA アドレスは、ブロードキャストまたはマルチキャスト パケットの宛先として設定されていません。

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

(注) Cisco IOS XE Denali 16.3.1 では、このコマンドは IPv4 だけをサポートしています。
ipv6-nbma-address 引数は、スイッチでは使用可能ですが、設定しても機能しません。

このコマンドは、トンネルインターフェイスだけに適用されます。このコマンドは、基盤となるネットワークが IP マルチキャストをサポートしていない場合に、トンネルネットワーク経由でブロードキャストをサポートするために役立ちます。基盤となるネットワークが IP マルチキャストをサポートしている場合は、**tunnel destination** コマンドを使用して、トンネルブロードキャストまたはマルチキャストを伝送するためのマルチキャスト宛先を設定する必要があります。

複数の NBMA アドレスが設定されている場合、システムはアドレスごとにブロードキャストパケットを複製します。

例

次に、パケットが 10.255.255.255 に送信される場合に、宛先 10.0.0.1 と 10.0.0.2 に対してパケットが複製される例を示します。

```
Switch(config)# interface tunnel 0
Switch(config-if)# ip address 10.0.0.3 255.0.0.0
Switch(config-if)# ip nhrp map multicast 10.0.0.1
Switch(config-if)# ip nhrp map multicast 10.0.0.2
```

関連コマンド

コマンド	説明
debug nhrp	NHRP デバッグをイネーブルにします。
interface	インターフェイスを設定し、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。
tunnel destination	トンネル インターフェイスの宛先を指定します。

ip nhrp network-id

インターフェイスの Next Hop Resolution Protocol (NHRP) を有効にするには、インターフェイス コンフィギュレーションモードで **ip nhrp network-id** コマンドを使用します。インターフェイスで NHRP を無効にするには、このコマンドの **no** 形式を使用します。

ip nhrp network-id *number*
no ip nhrp network-id [*{number}*]

構文の説明

<i>number</i>	ノンブロードキャスト マルチアクセス (NBMA) ネットワークからのグローバルに一意的な 32 ビット ネットワーク識別子。範囲は 1 ~ 4294967295 です。
---------------	---

コマンド デフォルト

NHRP はインターフェイスで無効になっています。

コマンド モード

インターフェイス コンフィギュレーション (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

一般に、論理 NBMA ネットワーク内のすべての NHRP ステーションは、同じネットワーク ID を使用して設定する必要があります。

例

次に、インターフェイスで NHRP を有効にする例を示します。

```
Switch(config-if)# ip nhrp network-id 1
```

関連コマンド

コマンド	説明
clear ip nhrp	NHRP キャッシュからすべてのダイナミック エントリを削除します。
debug nhrp	NHRP デバッグをイネーブルにします。
interface	インターフェイスを設定し、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。

ip nhrp nhs

1 つ以上の Next Hop Resolution Protocol (NHRP) サーバのアドレスを指定するには、インターフェイス コンフィギュレーション モードで **ip nhrp nhs** コマンドを使用します。アドレスを削除するには、このコマンドの **no** 形式を使用します。

```
ip nhrp nhs {nhs-address [nbma {nbma-address FQDN-string}] [multicast] [priority value]
[cluster value] | cluster value max-connections value | dynamic nbma {nbma-address
FQDN-string} [multicast] [priority value] [cluster value] | fallback seconds}
no ip nhrp nhs {nhs-address [nbma {nbma-address FQDN-string}] [multicast] [priority value]
[cluster value] | cluster value max-connections value | dynamic nbma {nbma-address
FQDN-string} [multicast] [priority value] [cluster value] | fallback seconds}
```

構文の説明

<i>nhs-address</i>	指定されているネクストホップ サーバのアドレス。
nbma	(任意) ノンブロードキャスト マルチアクセス (NBMA) アドレスまたは FQDN を指定します。
<i>nbma-address</i>	NBMA アドレス。
<i>FQDN-string</i>	ネクストホップ サーバ (NHS) の完全修飾ドメイン名 (FQDN) 文字列。
multicast	(任意) ブロードキャストおよびマルチキャストに NBMA マッピングを使用することを指定します。
priority value	(任意) ハブに優先順位を割り当てて、トンネルを確立するためにスポークがハブを選択する順序を制御します。指定できる範囲は 0 ~ 255 で、0 は最高の優先順位、255 は最低の優先順位です。
cluster value	(任意) NHS グループを指定します。範囲は 0 ~ 10 です。
max-connections value	アクティブにする必要がある各 NHS グループの NHS 要素の数を指定します。有効な範囲は 0 ~ 255 です。
dynamic	NHS プロトコル アドレスをダイナミックに学習するようにスポークを設定します。
fallback seconds	リカバリ時により優先順位の高い NHS にフォールバックする前にスポークが待機する必要がある期間を秒単位で指定します。

コマンド デフォルト

ネクストホップサーバは明示的に設定されていないため、通常のネットワーク層のルーティング決定が NHRP トラフィックの転送に使用されます。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

ネクストホップサーバのアドレスとそれがサービスを提供するネットワークを指定するには、**ip nhrp nhs** コマンドを使用します。通常、NHRP は、ネットワーク層転送テーブルを使用して、NHRP パケットの転送方法を決定します。ネクストホップサーバが設定されている場合は、これらのネクストホップアドレスの方が、通常 NHRP トラフィック向けに使用されている転送パスより優先されます。

設定されたネクストホップサーバに対して、同じ *nhs-address* 引数と異なる IP ネットワークアドレスを使用して **ip nhrp nhs** コマンドを繰り返すことで、複数のネットワークを指定できます。

例

次に、NBMA と FQDN を使用してハブをスポークに登録する例を示します。

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs 192.0.2.1 nbma examplehub.example1.com
```

次に、目的の **max-connections** 値を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs cluster 5 max-connections 100
```

次に、NHS フォールバック時間を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs fallback 25
```

次に、NHS 優先順位とグループ値を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs 192.0.2.1 priority 1 cluster 2
```

関連コマンド

コマンド	説明
ip nhrp map	NBMA ネットワークに接続された IP 宛先の IP-to-NBMA アドレス マッピングをスタティックに設定します。
show ip nhrp	NHRP マッピング情報を表示します。

ipv6 nd cache expire

IPv6 ネイバー探索のキャッシュエントリの有効期限が切れるまでの時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd cache expire** コマンドを使用します。この設定を削除するには、このコマンドの **no** 形式を使用します。

ipv6 nd cache expire *expire-time-in-seconds* [**refresh**]
no ipv6 nd cache expire *expire-time-in-seconds* [**refresh**]

構文の説明

構文の説明

expire-time-in-seconds 時間の範囲は 1 ～ 65,536 秒です。デフォルトは 14,400 秒、つまり 4 時間です。

refresh (任意) ネイバー探索キャッシュエントリを自動的に更新します。

コマンドモード

インターフェイス コンフィギュレーション (config-if)

コマンド履歴

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、14,400 秒間、つまり 4 時間にわたって STALE 状態が続いた場合は、ネイバー探索キャッシュエントリの有効期限が切れて削除されます。**ipv6 nd cache expire** コマンドを使用すると、有効期限を変更したり、エントリが削除される前に期限切れのエントリの自動更新をトリガーすることができます。

refresh キーワードを使用すると、ネイバー探索キャッシュエントリが自動更新されます。エントリは DELAY 状態に移行し、ネイバー到達不能検出プロセスが実行され、5 秒後にエントリは DELAY 状態から PROBE 状態に遷移します。エントリが PROBE 状態に到達すると、ネイバー送信要求が送信され、設定に従って再送信されます。

例

次に、ネイバー探索キャッシュエントリが 7,200 秒 (2 時間) で期限が切れるように設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd cache expire 7200
```

関連コマンド

コマンド	説明
ipv6 nd na glean	非送信要求ネイバー アドバタイズメントからエントリを収集するネイバー探索を設定します。

コマンド	説明
ipv6 nd nud retry	ネイバー到達不能検出でネイバー送信要求を再送信する回数を設定します。
show ipv6 interface	IPv6 用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。

ipv6 nd na glean

非送信要求ネイバーアドバタイズメントからエントリを収集するようにネイバー探索を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd na glean** コマンドを使用します。この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。

ipv6 nd na glean
no ipv6 nd na glean

コマンドモード インターフェイス コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン 重複アドレス検出 (DAD) が正常に完了すると、IPv6 ノードからマルチキャスト非送信要求ネイバー アドバタイズメント パケットが発行されることがあります。デフォルトでは、これらの非送信要求ネイバーアドバタイズメントパケットは他の IPv6 ノードから無視されます。**ipv6 nd na glean** コマンドは、非送信要求ネイバー アドバタイズメントパケットの受信時にルータでネイバー アドバタイズメント エントリを作成するように設定します (これらのエントリがまだ存在せず、ネイバーアドバタイズメントにリンク層アドレスオプションがある場合)。このコマンドを使用すると、データトラフィックをネイバーと交換する前に、デバイスのネイバーアドバタイズメントキャッシュにネイバーのエントリを読み込むことができます。

例

次に、非送信要求ネイバーアドバタイズメントからエントリを収集するようにネイバー探索を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd na glean
```

関連コマンド

コマンド	説明
ipv6 nd cache expire	IPv6 ネイバー探索キャッシュエントリの期限が切れるまでの時間を設定します。
ipv6 nd nud retry	ネイバー到達不能検出でネイバー送信要求を再送信する回数を設定します。
show ipv6 interface	IPv6 用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。

ipv6 nd nud retry

ネイバー到達不能検出プロセスでネイバー送信要求を再送信する回数を設定するには、インターフェイスコンフィギュレーションモードで **ipv6 nd nud retry** コマンドを使用します。この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。

```
ipv6 nd nud retry base interval max-attempts {final-wait-time}
no ipv6 nd nud retry base interval max-attempts {final-wait-time}
```

構文の説明

<i>base</i>	ネイバー到達不能検出プロセスのベース値。
<i>interval</i>	再試行の時間間隔（ミリ秒）。 有効な範囲は 1000 ～ 32000 です。
<i>max-attempts</i>	再試行の最大回数（ベース値に依存）。 有効な範囲は 1 ～ 128 です。
<i>final-wait-time</i>	最後のプローブの待機時間（ミリ秒）。 有効な範囲は 1000 ～ 32000 です。

コマンドモード

インターフェイス コンフィギュレーション (config-if)

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン

ネイバーのネイバー検出エントリを再度解決するためにデバイスでネイバー到達不能検出を実行する際、ネイバー送信要求パケットが 1 秒間隔で 3 回送信されます。スパニングツリーイベント、トラフィックの多いイベント、エンドホストのリロードなどの特定の状況においては、ネイバー送信要求が 1 秒間隔で 3 回送信されても十分でない場合があります。このような状況でネイバーキャッシュを維持するには、**ipv6 nd nud retry** コマンドを使用してネイバー送信要求の再送信の指数タイマーを設定します。

再試行の最大回数は、*max-attempts* 引数を使用して設定されます。再送信間隔は、次の式で計算されます。

$$tm^n$$

各値は次のとおりです。

- t = 時間間隔
- m = ベース (1、2、または 3)
- n = 現在のネイバー送信要求番号 (最初のネイバー送信要求が 0)

したがって、**ipv6 nd nud retry 3 1000 5** コマンドは、1、3、9、27、81 秒の間隔で再送信します。最終待機時間が設定されていない場合、エントリは 243 秒後に削除されます。

ipv6 nd nud retry コマンドはネイバー到達不能検出プロセスの再送信レートにのみ影響し、最初の解決には影響しません。最初の解決では、デフォルトに基づいてネイバー送信要求パケットが 1 秒間隔で 3 回送信されます。

例

次に、1 秒の固定間隔で 3 回再送信するように設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 1 1000 3
```

次に、再送信間隔を 1、2、4、8 に設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 2 1000 4
```

次に、再送信間隔を 1、3、9、27、81 に設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 3 1000 5
```

関連コマンド

コマンド	説明
ipv6 nd cache expire	IPv6 ネイバー探索 (ND) キャッシュエントリの期限が切れるまでの時間を設定します。
ipv6 nd na glean	非送信要求ネイバー アドバタイズメントからエントリを収集するネイバー探索を設定します。
show ipv6 interface	IPv6 用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。

key chain

ルーティングプロトコルの認証を有効にするために必要な認証キーチェーンを定義して、キーチェーン コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **key chain** コマンドを使用します。キーチェーンを削除するには、このコマンドの **no** 形式を使用します。

key chain *name-of-chain*

no key chain *name-of-chain*

構文の説明

<i>name-of-chain</i>	キーチェーンの名前。キーチェーンには、少なくとも1つのキーを含める必要がありますが、最大 2147483647 個のキーを含めることができます。
----------------------	--

コマンドデフォルト

キーチェーンは存在しません。

コマンドモード

グローバル コンフィギュレーション (config)

使用上のガイドライン

認証を有効にするには、キーでキーチェーンを設定する必要があります。

複数のキーチェーンの識別が可能ですが、ルーティングプロトコルごとのインターフェイスごとに1つのキーチェーンを使用することを推奨します。**key chain** コマンドを指定すると、キーチェーン コンフィギュレーション モードが開始されます。

例

次に、キーチェーンを指定する例を示します。

```
Device(config-keychain-key) # key-string chestnut
```

関連コマンド

Command	Description
accept-lifetime	キーチェーンの認証キーが有効として受信される期間を設定します。
key	キーチェーンの認証キーを識別します。
key-string (authentication)	キーの認証文字列を指定します。
send-lifetime	キーチェーンの認証キーが有効に送信される期間を設定します。
show key chain	認証キーの情報を表示します。

key-string (認証)

キーの認証文字列を指定するには、キーチェーン キー コンフィギュレーション モードで **key-string** (認証) コマンドを使用します。認証文字列を削除するには、このコマンドの **no** 形式を使用します。

key-string key-string text
no key-string text

構文の説明

<i>text</i>	認証されるルーティングプロトコルを使用してパケットで送信および受信される必要のある認証文字列。文字列には、大文字小文字の英数字 1 ~ 80 文字を含めることができます。
-------------	---

コマンドデフォルト

キーの認証文字列は存在しません。

コマンドモード

キー チェーン キー コンフィギュレーション (config-keychain-key)

例

次に、キーの認証文字列を指定する例を示します。

```
Device(config-keychain-key)# key-string key1
```

関連コマンド

Command	Description
accept-lifetime	キー チェーンの認証キーが有効として受信される期間を設定します。
key	キー チェーンの認証キーを識別します。
key chain	ルーティング プロトコルの認証をイネーブルにするために必要な認証キーチェーンを定義します。
send-lifetime	キー チェーンの認証キーが有効に送信される期間を設定します。
show key chain	認証キーの情報を表示します。

key

キーチェーンの認証キーを識別するには、キーチェーンコンフィギュレーションモードで **key** コマンドを使用します。キーチェーンからキーを削除するには、このコマンドの **no** 形式を使用します。

key *key-id*
no key *key-id*

構文の説明

<i>key-id</i>	キーチェーンの認証キーの識別番号。キーの範囲は 0 ~ 2147483647 です。キーの ID 番号は連続している必要はありません。
---------------	---

コマンドデフォルト

キーチェーンにキーは存在しません。

コマンドモード

キーチェーンコンフィギュレーション (config-keychain)

コマンド履歴

リリース	変更内容
11.1	このコマンドが導入されました。
12.4(6)T	IPv6 のサポートが追加されました。
12.2(33)SRB	このコマンドが、Cisco IOS Release 12.2(33)SRB に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィチャーセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。

使用上のガイドライン

キーチェーンに複数のキーを設定し、**accept-lifetime** および **send-lifetime** キーチェーンキーコマンド設定に基づいてキーが将来無効になるように、ソフトウェアでキーを配列できるようにすると便利です。

各キーには、ローカルに格納される独自のキー識別子があります。キー ID、およびメッセージに関連付けられたインターフェイスの組み合わせにより、使用中の認証アルゴリズムおよび Message Digest 5 (MD5) 認証キーが一意に識別されます。有効なキーの数にかかわらず、1 つの認証パケットのみが送信されます。ソフトウェアは、最小のキー識別番号の検索を開始し、最初の有効なキーを使用します。

最後のキーが期限切れになった場合、認証は続行されますが、エラーメッセージが生成されません。認証を無効にするには、手動で有効な最後のキーを削除する必要があります。

すべてのキーを削除するには、**no key chain** コマンドを使用してキーチェーンを削除します。

例

次に、キーを指定してキーチェーンでの認証を確認する例を示します。

```
Device(config-keychain)# key 1
```

関連コマンド

Command	Description
accept-lifetime	キーチェーンの認証キーが有効として受信される期間を設定します。
key chain	ルーティングプロトコルの認証をイネーブ爾にするために必要な認証キーチェーンを定義します。
key-string (authentication)	キーの認証文字列を指定します。
send-lifetime	キーチェーンの認証キーが有効に送信される期間を設定します。
show key chain	認証キーの情報を表示します。

show ip nhrp nhs

Next Hop Resolution Protocol (NHRP) ネクストホップサーバ (NHS) 情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip nhrp nhs** コマンドを使用します。

show ip nhrp nhs [{*interface*}] [**detail**] [{**redundancy** [{*cluster number* | **preempted** | **running** | **waiting**}]}]

構文の説明		
	<i>interface</i>	(任意) インターフェイスに現在設定されている NHS 情報を表示します。タイプ、番号範囲、説明については、下の表を参照してください。
	detail	(任意) 詳細な NHS 情報を表示します。
	redundancy	(任意) NHS 冗長スタックに関する情報を表示します。
	cluster number	(任意) 冗長クラスタ情報を表示します。
	preempted	(任意) アクティブになれず、プリエンプション処理された NHS に関する情報を表示します。
	running	(任意) 現在「Responding」または「Expecting replies」状態になっている NHS を表示します。
	waiting	(任意) スケジュール処理待ち状態の NHS を表示します。

コマンドモード ユーザ EXEC (>)
特権 EXEC (#)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン 次の表に、任意指定の *interface* 引数の有効なタイプ、番号の範囲、および説明を示します。



(注) 有効なタイプは、プラットフォームとプラットフォーム上のインターフェイスによって異なります。

表 2: 有効なタイプ、番号の範囲、およびインターフェイスの説明

有効なタイプ	番号の範囲	インターフェイスの説明
ANI	0 ~ 1000	自律型ネットワーク仮想インターフェイス

有効なタイプ	番号の範囲	インターフェイスの説明
Auto-Template	1 ~ 999	自動テンプレート インターフェイス
GMPLS	0 ~ 1000	マルチプロトコル ラベル スイッチング (MPLS) インターフェイス
GigabitEthernet	0 ~ 9	GigabitEthernet IEEE 802.3z
InternalInterface	0 ~ 9	内部インターフェイス
LISP	0 ~ 65520	Locator/ID Separation Protocol (LISP) 仮想インターフェイス
loopback	0 ~ 2,147,483,647	ループバック インターフェイス
Null	0 ~ 0	ヌル インターフェイス
PROTECTION_GROUP	0 ~ 0	保護グループ コントローラ
Port-channel	1 ~ 128	ポート チャネル インターフェイス
TenGigabitEthernet	0 ~ 9	TenGigabitEthernet インターフェイス
Tunnel	0 ~ 2,147,483,647	トンネル インターフェイス
Tunnel-tp	0 ~ 65535	MPLS トランスポート プロファイル インターフェイス
Vlan	1 ~ 4094	VLAN インターフェイス

例

次に、**show ip nhrp nhs detail** コマンドの出力例を示します。

```
Switch# show ip nhrp nhs detail
Legend:
  E=Expecting replies
  R=Responding
Tunnel1:
  10.1.1.1          E req-sent 128 req-failed 1 repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 1, Ret 64 NHS 10.1.1.1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 3: **show ip nhrp nhs** のフィールドの説明

フィールド	説明
Tunnel1	ターゲットネットワークに到達するために経由するインターフェイス。

関連コマンド

コマンド	説明
ip nhrp map	NBMA ネットワークに接続された IP 宛先の IP-to-NBMA アドレス マッピングをスタティックに設定します。
show ip nhrp	NHRP マッピング情報を表示します。

show ip ports all

デバイス上で開いているすべてのポートを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip ports all** を使用します。

show ip ports all

構文の説明

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ユーザ EXEC (>)

特権 EXEC (#)

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、Cisco ネットワーキング スタックを使用して開かれたポートを含むシステム上で開いているすべての TCP/IP ポートのリストを表示します。

開いているポートを閉じるには、次のいずれかの方法を使用します。

- アクセスコントロールリスト (ACL) を使用します。
- UDP 2228 ポートを閉じるには、**no l2 traceroute** コマンドを使用します。
- TCP 80、TCP 443、TCP 6970、TCP 8090 ポートを閉じるには、**no ip http server** および **no ip http secure-server** コマンドを使用します。

例

次に、**show ip ports all** コマンドの出力例を示します。

```
Device#
show ip ports all
Proto Local Address Foreign Address State PID/Program Name
TCB Local Address Foreign Address (state)
tcp *:4786 *:* LISTEN 224/[IOS]SMI IBC server process
tcp *:443 *:* LISTEN 286/[IOS]HTTP CORE
tcp *:443 *:* LISTEN 286/[IOS]HTTP CORE
tcp *:80 *:* LISTEN 286/[IOS]HTTP CORE
tcp *:80 *:* LISTEN 286/[IOS]HTTP CORE
udp *:10002 *:* 0/[IOS] Unknown
udp *:2228 10.0.0.0:0 318/[IOS]L2TRACE SERVER
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 4: *show ip ports all* のフィールドの説明

フィールド	説明
Protocol	使用されている転送プロトコル。
Local Address.	デバイスの IP アドレス。
Foreign Address	リモートまたはピア アドレス。
State	接続の状態。リッスン、確立済み、または接続済みを選択できます。
PID/Program Name	プロセス ID または名前。

関連コマンド

Command	Description
show tcp brief all	TCP 接続のエンドポイントに関する情報を表示します。
show ip sockets	IP ソケット情報を表示します。

show key chain

キーチェーンを表示するには、**show key chain** コマンドを使用します。

show key chain [*name-of-chain*]

構文の説明	<i>name-of-chain</i> (任意) キーチェーンコマンドで命名された表示対象のキーチェーン名。
-------	---

コマンドデフォルト パラメータを指定せずにコマンドを使用すると、すべてのキーチェーンのリストを表示します。

コマンドモード 特権 EXEC (#)

例

次に、**show key chain** コマンドの出力例を示します。

```

show key chain
Device# show key chain

Key-chain AuthenticationGLBP:
  key 1 -- text "Thisisasecretkey"
    accept lifetime (always valid) - (always valid) [valid now]
    send lifetime (always valid) - (always valid) [valid now]
Key-chain glbp2:
  key 100 -- text "abc123"
    accept lifetime (always valid) - (always valid) [valid now]
    send lifetime (always valid) - (always valid) [valid now]

```

関連コマンド	コマンド	説明
	key-string	キーの認証文字列を指定します。
	send-lifetime	キーチェーンの認証キーが有効に送信される期間を設定します。

show track

トラッキングプロセスが追跡したオブジェクトに関する情報を表示するには、特権 EXEC モードで **show track** コマンドを使用します。

```
show track [{object-number [brief] | application [brief] | interface [brief] | ip[route [brief] |
[sla [brief]] | ipv6 [route [brief]] | list [route [brief]] | resolution [ip | ipv6] | stub-object [brief]
| summary | timers}]
```

構文の説明

object-number	(任意) トラッキング対象オブジェクトを表すオブジェクト番号。範囲は1～1000です。
brief	(任意) 先行する引数やキーワードに関連する1行の情報を表示します。
application	(任意) トラッキング対象のアプリケーションオブジェクトを表示します。
interface	(任意) トラッキング対象のインターフェイスオブジェクトを表示します。
ip route	(任意) トラッキング対象のIPルートオブジェクトを表示します。
ip sla	(任意) トラッキング対象のIP SLAオブジェクトを表示します。
ipv6 route	(任意) トラッキング対象のIPv6ルートオブジェクトを表示します。
list	(任意) ブールオブジェクトを表示します。
resolution	(任意) トラッキング対象パラメータの解像度を表示します。
summary	(任意) 指定されたオブジェクトの概要を表示します。
timers	(任意) ポーリング間隔タイマーを表示します。

コマンドモード

特権 EXEC (#)

コマンド履歴

リリース	変更内容
XE 3.10S	このコマンドが変更されました。出力が拡張され、IPv6ルート情報が表示されるようになりました。

使用上のガイドライン

トラッキングプロセスによってトラッキングされているオブジェクトに関する情報を表示するには、このコマンドを使用します。引数やキーワードを指定しない場合は、すべてのオブジェクトの情報が表示されます。

最大1000のオブジェクトを追跡できます。トラッキング対象オブジェクトは1000個設定できますが、各トラッキング対象オブジェクトはCPUリソースを使用します。デバイスで使用可能なCPUリソースの合計は、トラフィック負荷などの変数や、他のプロトコルがどのように

設定され実行されているかに応じて異なります。1000個の追跡対象オブジェクトが使用できるかどうかは、使用可能なCPUによって異なります。特定のサイトトラフィック条件下でサービスが機能することを保証するには、サイト上でテストを実施する必要があります。

例

次に、インターフェイスでIPルーティングの状態をトラッキングした場合の例を示します。

```
Device# show track 1

Track 1
  Interface GigabitEthernet 1/0/1 ip routing
  IP routing is Down (no IP addr)
    1 change, last change 00:01:08
```

次の表で、この出力で表示される重要なフィールドについて説明します。

表 5: show track フィールドの説明

フィールド	説明
Track	トラッキング対象オブジェクトの数。
Interface GigabitEthernet 1/0/1 IP routing	インターフェイスタイプ、インターフェイス番号、およびトラッキング対象オブジェクト。
IP routing is	Up または Down で表示されるオブジェクトの状態の値。オブジェクトがダウンしている場合は、理由が示されます。
1 change、last change	トラッキング対象オブジェクトの状態が変更された回数と、最後の変更からの経過時間 (hh:mm:ss で表示)。

関連コマンド

Command	Description
show track resolution	追跡対象パラメータの解像度を表示します。
track interface	インターフェイスをトラッキングされるように設定し、トラッキング コンフィギュレーション モードを開始します。
track ip route	IP ルートの状態を追跡し、トラッキング コンフィギュレーション モードを開始します。

track

Gateway Load Balancing Protocol (GLBP) の重み付けがインターフェイスの状態に基づいて変更されている場合にトラッキング対象インターフェイスを設定するには、グローバルコンフィギュレーションモードで **track** コマンドを使用します。トラッキングを削除するには、このコマンドの **no** 形式を使用します。

```
track object-number interface type number {line-protocol | ip routing | ipv6 routing}
no track object-number interface type number {line-protocol | ip routing | ipv6 routing}
```

構文の説明

<i>object-number</i>	トラッキングされるインターフェイスを表すオブジェクト番号。値の範囲は 1 ~ 1000 です。
<i>interface type number</i>	トラッキングするインターフェイス タイプおよび番号。
line-protocol	インターフェイスがアップ状態かどうかをトラッキングします。
ip routing	インターフェイスがアップの状態であることを GLBP に報告する前に、IP ルーティングが有効かどうか、インターフェイスに IP アドレスが設定されているか、インターフェイスがアップの状態かどうかをトラッキングします。
ipv6 routing	インターフェイスがアップの状態であることを GLBP に報告する前に、IPv6 ルーティングが有効かどうか、インターフェイスに IP アドレスが設定されているか、インターフェイスがアップの状態かどうかをトラッキングします。

コマンド デフォルト

インターフェイスの状態はトラッキングされません。

コマンド モード

グローバル コンフィギュレーション (config)

使用上のガイドライン

トラッキング対象インターフェイスのパラメータを設定するには、**track** コマンドと併せて **glbp weighting** および **glbp weighting track** コマンドを使用します。GLBP デバイスのトラッキング対象インターフェイスがダウンすると、そのデバイスの重み値は減らされます。重み値が指定された最小値を下回った場合、デバイスは、アクティブ GLBP 仮想フォワーダとしての機能を失います。

最大 1000 のオブジェクトを追跡できます。トラッキング対象オブジェクトは 1000 個設定できますが、各トラッキング対象オブジェクトは CPU リソースを使用します。デバイスで使用可能な CPU リソースの合計は、トラフィック負荷などの変数や、他のプロトコルがどのように設定され実行されているかに応じて異なります。1000 個の追跡対象オブジェクトが使用できるかどうかは、使用可能な CPU によって異なります。特定のサイト トラフィック条件下でサービスが機能することを保証するには、サイト上でテストを実施する必要があります。

例

次に、TenGigabitEthernet インターフェイス 0/0/1 が、GigabitEthernet インターフェイス 1/0/1 および 1/0/3 がアップの状態にあるかどうかをトラッキングする例を示します。GigabitEthernet インターフェイスのいずれかがダウンすると、GLBP の重み値は、デフォルト値である 10 まで減らされます。両方の GigabitEthernet インターフェイスがダウンすると、GLBP の重み値は下限しきい値未満に下がり、デバイスはアクティブフォワーダではなくなります。アクティブフォワーダとしての役割を再開するには、デバイスは、両方のトラッキング対象インターフェイスをアップの状態に戻し、重み値を上限しきい値を超える値に上げる必要があります。

```
Device(config)# track 1 interface GigabitEthernet 1/0/1 line-protocol
Device(config-track)# exit
Device(config)# track 2 interface GigabitEthernet 1/0/3 line-protocol
Device(config-track)# exit
Device(config)# interface TenGigabitEthernet 0/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
Device(config-if)# glbp 10 weighting track 1
Device(config-if)# glbp 10 weighting track 2
```

関連コマンド

コマンド	説明
glbp weighting	GLBP ゲートウェイの初期重み値を指定します。
glbp weighting track	GLBP ゲートウェイの重み付けに影響する、追跡対象のオブジェクトを指定します。

vrrp

Virtual Router Redundancy Protocol バージョン 3 (VRRPv3) グループを作成し、VRRPv3 グループ コンフィギュレーションモードを開始するには、**vrrp** を使用します。VRRPv3 グループを削除するには、このコマンドの **no** 形式を使用します。

```
vrrp group-id address-family {ipv4 | ipv6}
no vrrp group-id address-family {ipv4 | ipv6}
```

構文の説明

<i>group-id</i>	仮想ルータ グループ番号。範囲は 1 ~ 255 です。
address-family	この VRRP グループのアドレスファミリを指定します。
ipv4	(任意) IPv4 アドレスを指定します。
ipv6	(任意) IPv6 アドレスを指定します。

コマンドデフォルト

なし

コマンドモード

インターフェイス コンフィギュレーション (config-if)

使用上のガイドライン

例

次の例は、VRRPv3 グループの作成方法と VRRP コンフィギュレーションモードの開始方法を示しています。

```
Device(config-if)# vrrp 3 address-family ipv4
```

関連コマンド

コマンド	説明
timers advertise	アドバタイズメントタイマーを設定します (ミリ秒単位)。

vrrp description

Virtual Router Redundancy Protocol (VRRP) に説明を割り当てるには、インターフェイス コンフィギュレーションモードで **vrrp description** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

description *text*

no description

構文の説明

<i>text</i>	グループの目的または用途を説明するテキスト（最大 80 文字）。
-------------	----------------------------------

コマンドデフォルト

VRRP グループの説明はありません。

コマンドモード

VRRP 設定 (config-if-vrrp)

コマンド履歴

リリース	変更内容
	このコマンドが導入されました。

例

次の例では、VRRP を有効にしています。VRRP グループ 1 は、「Building A – Marketing and Administration (ビルディング A : マーケティングおよび管理)」と説明されます。

```
Device(config-if-vrrp)# description Building A - Marketing and Administration
```

関連コマンド

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループ コンフィギュレーションモードを開始します。

vrrp preempt

デバイスに現在のマスター仮想ルータより高い優先順位が与えられている場合、そのデバイスが Virtual Router Redundancy Protocol (VRRP) グループのマスター仮想ルータの機能を引き継ぐように設定するには、VRRP コンフィギュレーションモードで **preempt** コマンドを使用します。この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。

preempt [**delay minimum** *seconds*]
no preempt

構文の説明	delay minimum <i>seconds</i>	(任意) マスターの所有権を要求するアドバタイズメントを発行するまでに、デバイスが待機する秒数。デフォルト遅延値は 0 秒です。
-------	-------------------------------------	--

コマンド デフォルト このコマンドは有効です。

コマンド モード VRRP 設定 (config-if-vrrp)

コマンド履歴	リリース	変更内容
		このコマンドが導入されました。

使用上のガイドライン デフォルトでは、このコマンドで設定されるデバイスは、現在のマスター仮想ルータよりも高い優先順位を持つ場合、マスター仮想ルータとしての機能を引き継ぎます。VRRP デバイスが、マスター所有権を要求するアドバタイズメントを発行するまで、指定された秒数待機するように遅延時間を設定できます。



(注) このコマンドの設定にかかわらず、IPアドレスの所有者であるデバイスがプリエンプション処理します。

例

次に、デバイスの 200 の優先順位が現在のマスター仮想ルータの優先順位よりも高い場合に、デバイスが現在のマスター仮想ルータをプリエンプション処理するように設定する例を示します。デバイスは、現在のマスター仮想ルータをプリエンプション処理する場合、マスター仮想ルータであることを要求するアドバタイズメントを発行するまでに 15 秒待機します。

```
Device(config-if-vrrp)#preempt delay minimum 15
```

関連コマンド

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループ コンフィギュレーション モードを開始します。
priority	VRRP グループ内のデバイスの優先度レベルを設定します。

vrrp priority

Virtual Router Redundancy Protocol (VRRP) 内のデバイスの優先度レベルを設定するには、インターフェイス コンフィギュレーション モードで **priority** コマンドを使用します。デバイスの優先度レベルを削除するには、このコマンドの **no** 形式を使用します。

priority *level*

no priority *level*

構文の説明

<i>level</i>	VRRP グループ内のデバイスの優先順位。有効な範囲は 1 ~ 254 です。デフォルトは 100 です。
--------------	---

コマンド デフォルト

優先度レベルはデフォルト値の 100 に設定されています。

コマンド モード

VRRP 設定 (config-if-vrrp)

コマンド履歴

リリース	変更内容
	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、どのデバイスをマスター仮想ルータにするかを制御できます。

例

次に、デバイスを 254 の優先順位に設定する例を示します。

```
Device(config-if-vrrp)# priority 254
```

関連コマンド

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループ コンフィギュレーション モードを開始します。
vrrp preempt	デバイスに現在のマスター仮想ルータより高い優先順位が与えられている場合、そのデバイスが VRRP グループのマスター仮想ルータの機能を引き継ぐように設定します。

vrrp timers advertise

Virtual Router Redundancy Protocol (VRRP) グループ内のマスター仮想ルータによる連続したアドバタイズメント間の間隔を設定するには、VRRP コンフィギュレーションモードで **timers advertise** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

timers advertise [*msec*] *interval*
no timers advertise [*msec*] *interval*

構文の説明

<i>group</i>	仮想ルータ グループ番号。グループ番号の範囲は 1 ～ 255 です。
<i>msec</i>	(任意) アドバタイズメント時間の単位を秒からミリ秒に変更します。このキーワードを付加しないと、アドバタイズメント間隔は秒単位になります。
<i>interval</i>	マスター仮想ルータによる連続したアドバタイズメント間の時間間隔。 msec キーワードを指定しなかった場合、間隔は秒単位になります。デフォルト値は 1 秒です。有効範囲は 1 ～ 255 秒です。 msec キーワードを指定した場合、有効な範囲は 50 ～ 999 ミリ秒です。

コマンドデフォルト

デフォルトの間隔である 1 秒に設定されています。

コマンドモード

VRRP 設定 (config-if-vrrp)

コマンド履歴

リリース	変更内容
	このコマンドが導入されました。

使用上のガイドライン

マスター仮想ルータから送信されるアドバタイズメントは、現在のマスター仮想ルータの状態と優先順位を伝えます。

vrrp timers advertise コマンドは、連続するアドバタイズメントパケットの間の時間間隔と、マスタールータがダウンしていると他のルータが宣言するまでの時間を設定します。タイマー値が設定されていないルータまたはアクセス サーバは、マスタールータからタイマー値を取得できます。マスタールータで設定されたタイマーは、他のすべてのタイマー設定を常に上書きします。VRRP グループ内のすべてのルータが同じタイマー値を使用する必要があります。同じタイマー値が設定されていないと、VRRP グループ内のデバイスが相互通信せず、正しく設定されていないデバイスのステータスがマスターに変わります。

例

次に、マスター仮想ルータがアドバタイズメントを 4 秒ごとに送信するように設定する例を示します。

```
Device(config-if-vrrp)# timers advertise 4
```

関連コマンド

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループ コンフィギュレーション モードを開始します。
timers learn	VRRP グループのバックアップ仮想ルータとして動作するときに、マスター仮想ルータが使用していたアドバタイズ間隔を学習するようにデバイスを設定します。

vrrs leader

リーダーの名前を Virtual Router Redundancy Service (VRRS) に登録されるように指定するには、**vrrs leader** コマンドを使用します。指定された VRRS リーダーを削除するには、このコマンドの **no** 形式を使用します。

vrrs leader *vrrs-leader-name*
no vrrs leader *vrrs-leader-name*

構文の説明

<i>vrrs-leader-name</i>	リードする VRRS タグの名前。
-------------------------	-------------------

コマンド デフォルト

登録済みの VRRS 名はデフォルトで使用不可になっています。

コマンド モード

VRRP 設定 (config-if-vrrp)

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。

例

次に、VRRS に登録されるリーダーの名前を指定する例を示します。

```
Device(config-if-vrrp)# vrrs leader leader-1
```

関連コマンド

コマンド	説明
vrrp	VRRP グループを作成し、VRRP コンフィギュレーションモードを開始します。

