IP

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。
vrf-name	（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。
dest-ip-address	（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。
dest-mask	（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。
tunnel *number*	（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*} } |**umatched** |**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。
ipv4-nbma-address	（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。
nbma-name	（任意）NBMA ネットワーク名。
IPv6-address	（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） *IPv6-address* 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
showipnhrp	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。
seconds	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 **fhrpversionvrrpv3** 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 ステートがダウンになると、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。

glbp authentication

Gateway Load Balancing Protocol（GLBP）の認証文字列を設定するには、インターフェイス コンフィギュレーション モードで **glbpauthentication** コマンドを使用します。認証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。

glbp *group-number***authentication** {**text** *string*|**md5** {**key-string** [{**0**|**7**}] キー|**key-chain** *name-of-chain*}}
no glbp *group-number* **authentication** {**text** *string*|**md5** {**key-string** [{**0**|**7**}] キー|**key-chain** *name-of-chain*}}

構文の説明

group-number	0 ～ 1023 の範囲の GLBP グループ番号。
text *string*	認証ストリングを指定します。コマンドとテキストを合わせた文字数が 255 文字を超えないようにします。
md5	Message Digest 5（MD5）認証。
key-string キー	MD5 認証の秘密キーを指定します。キー ストリングは、100 文字の長さを超えることはできません。少なくとも 16 文字使用することを推奨します。
0	（任意）非暗号化キー。プレフィックスが指定されていない場合、キーは暗号化されません。
7	（任意）暗号化キー。
key-chain *name-of-chain*	認証キーのグループを指定します。

コマンド デフォルト

GLBP メッセージの認証は発生しません。

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）

使用上のガイドライン

同じGLBPグループのメンバーとして設定されているすべてのデバイスで同じ認証方式を設定し、確実に相互運用できるようにする必要があります。デバイスは、誤った認証情報を含むすべての GLBP メッセージを無視します。

パスワード暗号化が **servicepassword-encryption** コマンドで設定されると、ソフトウェアは、キー文字列を暗号化されたテキストとして設定に保存します。

例

次に、グループ 10 の GLBP デバイスの相互運用を許可するために必要な認証文字列として stringxyz を設定する例を示します。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# glbp 10 authentication text stringxyz
```

次に、GLBPがキーチェーン「AuthenticateGLBP」を照会して、指定されたキーチェーンの現在アクティブなキーとキーIDを取得する例を示します。

```
Device(config)# key chain AuthenticateGLBP
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string ThisIsASecretKey
Device(config-keychain-key)# exit
Device(config-keychain)# exit
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# glbp 2 authentication md5 key-chain AuthenticateGLBP
```

関連コマンド

Command	Description
glbpip	GLBPをイネーブルにします。

glbp forwarder preempt

現在のアクティブ仮想フォワーダ（AVF）がその低い重み付けしきい値を下回った場合に、デバイスが Gateway Load Balancing Protocol（GLBP）グループの AVF として引き継がれるように設定するには、インターフェイス コンフィギュレーション モードで **glbpforwarderpreempt** コマンドを使用します。この機能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。

glbp *group* **forwarder preempt** [**delay minimum** *seconds*]
no glbp *group* **forwarder preempt** [**delay minimum**]

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
delayminimum *seconds*	（任意）デバイスが AVF のロールを引き継ぐ前に遅延する最小秒数を指定します。範囲は 0 ～ 3600 秒です。デフォルトの遅延時間は 30 秒です。

コマンド デフォルト

フォワーダ強制排除は、30 秒のデフォルト遅延でイネーブルになります。

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 Release 2.1	このコマンドが導入されました。

例

次に、現在の AVF がその低い重み付けしきい値を下回った場合に、デバイスが現在の AVF 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。デバイスが現在の AVF をプリエンプション処理した場合、デバイスは AVF の役割を引き継ぐ前に 60 秒間待ちます。

```
Device(config-if)# glbp 10 forwarder preempt delay minimum 60
```

関連コマンド

コマンド	説明
glbpip	GLBP をイネーブルにします。

glbp ip

Gateway Load Balancing Protocol（GLBP）を有効化するには、インターフェイス コンフィギュレーション モードで **glbpip** コマンドを使用します。GLBP を無効にするには、このコマンドの **no** 形式を使用します。

glbp *group* **ip** [*ip-address* **[secondary]**]
no glbp *group* **ip** [*ip-address* **[secondary]**]

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
ip-address	（任意）GLBP グループの仮想 IP アドレス。この IP アドレスはインターフェイス IP アドレスと同じサブネット内になければなりません。
secondary	（任意）IP アドレスがセカンダリ GLBP 仮想アドレスであることを示します。

コマンド デフォルト

GLBP はデフォルトで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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが導入されました。

使用上のガイドライン

glbpip コマンドを実行すると、設定されたインターフェイスで GLBP が有効になります。指定されている IP アドレスがある場合、そのアドレスが GLBP グループの指定仮想 IP アドレスとして使用されます。指定されている IP アドレスがない場合、指定アドレスは、同じ GLBP グループに属するよう設定された別のデバイスから取得されます。GLBP がアクティブ仮想ゲートウェイ（AVG）を選択する場合、ケーブル上の少なくとも 1 つのデバイスが指定アドレスで設定されている必要があります。デバイスは、GLBP ゲートウェイまたはフォワーダの権限を引き受ける前に、GLBP グループの仮想 IP アドレスで設定されているか、そのアドレスを取得している必要があります。AVG の指定アドレスを設定すると、常に使用されている指定アドレスが上書きされます。

glbpip コマンドがインターフェイスで有効になっている場合、プロキシの Address Resolution Protocol（ARP）要求の処理方法が変更されます（プロキシ ARP が無効になっていない場合）。ARP 要求はホストにより送信され、IP アドレスが MAC アドレスにマッピングされます。GLBP ゲートウェイは、ARP 要求を代行受信し、接続先ノードの代わりに ARP に応答します。GLBP グループのフォワーダがアクティブである場合、プロキシ ARP 要求への応答には、グループ内の最初のアクティブ フォワーダの MAC アドレスが使用されます。アクティブなフォワーダがない場合、プロキシ ARP 要求は停止されます。

例

次の例では、GigabitEthernet インターフェイス 1/0/1 上の グループ 10 の GLBP を有効にします。GLBP グループで使用される仮想 IP アドレスは、10.21.8.10 に設定されます。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 ip 10.21.8.10
```

関連コマンド

Command	Description
showglbp	GLBPの情報を表示します。

glbp load-balancing

Gateway Load Balancing Protocol（GLBP）のアクティブ仮想ゲートウェイ（AVG）で使用されるロード バランシング方式を指定するには、インターフェイス コンフィギュレーション モードで **glbpload-balancing** コマンドを使用します。ロード バランシングを無効にするには、このコマンドの **no** 形式を使用します。

glbp *group* **load-balancing** [{**host-dependent**|**round-robin**|**weighted**}]
no glbp *group* **load-balancing**

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
host-dependent	（任意）ホストの MAC アドレスに基づくロード バランシング方式（GLBP グループ メンバーの数を一定に保ったまま、特定のホストに常に同じフォワーダが使用される）を指定します。
round-robin	（任意）各仮想フォワーダが仮想 IP アドレスのアドレス解決応答に含まれるようなロード バランシング方式を指定します。この方式がデフォルトです。
weighted	（任意）ゲートウェイによってアドバタイズされる重み値に基づくロード バランシング方式を指定します。

コマンド デフォルト

ラウンドロビン方式がデフォルトです。

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 Release 2.1	このコマンドが導入されました。

使用上のガイドライン

各ホストが常に同じデバイスを使用する必要がある場合は、ホスト依存方式の GLBP ロード バランシングを使用します。GLBP グループ内のデバイスの転送能力が異なるために不均等なロード バランシングを必要とする場合は、重み値方式の GLBP ロード バランシングを使用します。

例

次に、GLBP グループ 10 の AVG に設定されたホスト依存的な GLBP ロード バランシングの例を示します。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# glbp 10 ip 10.21.8.10
Device(config-if)# glbp 10 load-balancing host-dependent
```

関連コマンド

コマンド	説明
showglbp	GLBPの情報を表示します。

glbp name

Gateway Load Balancing Protocol（GLBP）グループに名前を割り当てて IP 冗長性を有効にするには、インターフェイス コンフィギュレーション モードで**glbpname** コマンドを使用します。グループの IP 冗長性を無効にするには、このコマンドの **no** 形式を使用します。

glbp *group-number* **name** *group-name*
no glbp *group-number* **name** *group-name*

構文の説明

group-number	GLBP グループ番号。指定できる値の範囲は 0 ～ 1023 です。
group-name	文字列で指定された GLBP グループ名。文字数は最大で 255 です。

コマンド デフォルト

グループの IP 冗長性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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが導入されました。

使用上のガイドライン

冗長クライアントと GLBP グループを接続できるように、GLBP 冗長クライアントに同じ GLBP グループ名を設定する必要があります。

例

次に、GLBP グループ 10 に abccomp 名を割り当てる例を示します。

```
Device(config-if)# glbp 10 name abccomp
```

関連コマンド

コマンド	説明
glbpauthentication	GLBP に認証ストリングを設定します。
glbpforwarderpreempt	デバイスの優先順位が現在の AVF より高い場合、デバイスが GLBP グループの AVF として引き継がれるように設定します。
glbpip	GLBP を有効にします。
glbpload-balancing	GLBP のアクティブ仮想ゲートウェイ（AVG）によって使用されるロード バランシング方式を指定します。
glbppreempt	ゲートウェイの優先順位が現在の AVG より高い場合、ゲートウェイが GLBP グループの AVG として引き継がれるように設定します。

コマンド	説明
glbppriority	GLBP グループ内のゲートウェイのプライオリティ レベルを設定します。
glbptimers	GLBP ゲートウェイによって送信される hello パケット間の時間、および仮想ゲートウェイと仮想フォワーダの情報が有効と見なされる時間を設定します。
glbptimersredirect	GLBP グループの AVG がセカンダリ AVF にクライアントをリダイレクトし続ける時間を設定します。
glbpweighting	GLBP ゲートウェイの最初の重み値を指定します。
glbpweightingtrack	GLBP の重み値の変更がトラッキングされるオブジェクトの可用性に基づいているトラッキング オブジェクトを指定します。
showglbp	GLBP の情報を表示します。
track	GLBP重み付けの変更がインターフェイスの状態に基づいている場合、インターフェイスをトラッキングするように設定します。

glbp preempt

現在のアクティブ仮想ゲートウェイ（AVG）よりも優先順位の高いゲートウェイがある場合、そのゲートウェイが Gateway Load Balancing Protocol（GLBP）グループの AVG を引き継ぐように設定するには、インターフェイス コンフィギュレーション モードで **glbppreempt** コマンドを使用します。この機能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。

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

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
delayminimum *seconds*	（任意）デバイスが AVG の役割を引き継ぐ前に遅延する最小秒数を指定します。範囲は 0 ～ 3600 秒です。デフォルトの遅延時間は 30 秒です。

コマンド デフォルト

現在の AVG よりも優先順位の高い GLBP ゲートウェイが、AVG の役割を引き継ぐことはできません。デフォルトの遅延時間は 30 秒です。

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 Release 2.1	このコマンドが導入されました。

例

次に、デバイスの優先順位が 254 で、現在の AVG よりも優先順位が高い場合に、そのデバイスが現在の AVG 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。デバイスが現在の AVG をプリエンプション処理する場合、デバイスは、AVG の役割を引き継ぐ前に 60 秒間待ちます。

```
Device(config-if)# glbp 10 preempt delay minimum 60
Device(config-if)# glbp 10 priority 254
```

関連コマンド

コマンド	説明
glbpip	GLBP をイネーブルにします。
glbppriority	GLBP グループ内のデバイスの優先度レベルを設定します。

glbp priority

Gateway Load Balancing Protocol（GLBP）グループ内のゲートウェイ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**glbppriority** コマンドを使用します。ゲートウェイ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。

glbp *group* **priority** *level*
no glbp *group* **priority** *level*

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
level	GLBP グループ内のゲートウェイのプライオリティ。範囲は 1 ～ 255 です。デフォルトは 100 です。

コマンド デフォルト

GLBP 仮想ゲートウェイのプリエンプション スキーム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（config-if）

使用上のガイドライン

アクティブ仮想ゲートウェイ（AVG）になる仮想ゲートウェイを制御するには、このコマンドを使用します。異なる複数の仮想ゲートウェイの優先順位を比較した後、優先順位の数値が高いゲートウェイが AVG として選択されます。2 つの仮想ゲートウェイの優先順位が等しい場合、優先順位の高い IP アドレスが選択されます。

例

次に、仮想ゲートウェイを 254 の優先順位に設定する例を示します。

```
Device(config-if)# glbp 10 priority 254
```

関連コマンド

コマンド	説明
glbpip	GLBP をイネーブルにします。
glbppreempt	現在の AVG よりも優先順位の高いデバイスがある場合、そのデバイスが GLBP グループの AVG を引き継ぐように設定します。

glbp timers

Gateway Load Balancing Protocol（GLBP）ゲートウェイにより送信される hello パケットの時間間隔、および仮想ゲートウェイと仮想フォワーダ情報が有効と見なされる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 **glbptimers** コマンドを使用します。タイマーを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。

glbp *group* **timers** {*hellotime*{*holdtime* | **msec** *holdtime*} | **msec** { *holdtime* | **msec** *holdtime*} | **redirect** *time-interval-to-redirect* | *timeout*}
no glbp *group* **timers** {*hellotime*{*holdtime* | **msec** *holdtime*} | **msec** { *holdtime* | **msec** *holdtime*} | **redirect** *time-interval-to-redirect* | *timeout*}

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
msec	（任意）下記の（*hellotime* または *holdtime*）引数値をミリ秒で表すように指定します。
hellotime	hello 間隔デフォルトは 3 秒（3000 ミリ秒）です。
holdtime	hello パケットに含まれる仮想ゲートウェイおよび仮想フォワーダの情報が無効と見なされるまでの時間。デフォルトは 10 秒（10,000 ミリ秒）です。
redirect	Gateway Load Balancing Protocol（GLBP）グループのアクティブ仮想ゲートウェイ（AVG）が継続してクライアントをセカンダリ アクティブ仮想フォワーダ（AVF）にリダイレクトする時間間隔を指定します。
time-interval-to-redirect	リダイレクト タイマーの間隔は、0 ～ 3600 秒の範囲内です。デフォルトは 600 秒（10 分）です。 （注） *time-interval-to-redirect* 引数のゼロ（0）値は、指定できる値の範囲から除外することはできません。Cisco IOS ソフトウェアの事前設定でゼロ（0）値を使用しているため、アップグレードに悪影響を及ぼすことになります。ただし、ゼロ（0）値に設定することは推奨しません。*time-interval-to-redirect* にこの値を使用すると、リダイレクト タイマーが期限切れになりません。リダイレクト タイマーが期限切れにならず、デバイスに障害が発生すると、新しいホストがバックアップへリダイレクトされずに、障害が発生したデバイスに引き続き割り当てられます。
timeout	セカンダリ仮想フォワーダが使用できなくなるまでの 600 秒から 64,800 秒の範囲の時間間隔。デフォルトは 14,400 秒（4 時間）です。

コマンド デフォルト

GLBP タイマーはデフォルト値に設定されています。

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-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが導入されました。

使用上のガイドライン

タイマー値が設定されていないデバイスは、アクティブ仮想ゲートウェイ（AVG）からタイマー値を取得できます。AVG 上に設定されているタイマーは、他のすべてのタイマー設定を常に上書きします。GLBP グループ内のすべてのデバイスが同じタイマー値を使用するようにしてください。GLBP ゲートウェイが hello メッセージを送信した場合、その情報は 1 ホールドタイムの間有効と見なされます。通常、保留時間は hello タイムの値の 3 倍より大きくします（*holdtime* > 3 * *hellotime*）。保留時間の値の範囲によって、hello タイムより大きい保留時間が強制されます。

例

次に、GigabitEthernet インターフェイス 1/0/1 の GLBP グループ 10 の hello パケットの間隔を 5 秒に設定し、仮想ゲートウェイとバーチャル フォワーダの情報が無効と見なされる時間を 18 秒に設定する例を示します。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# glbp 10 ip
Device(config-if)# glbp 10 timers 5 18
```

関連コマンド

コマンド	説明
glbpip	GLBP を有効にします。
showglbp	GLBPの情報を表示します。

glbp weighting

Gateway Load Balancing Protocol（GLBP）ゲートウェイの初期重み値を指定するには、インターフェイス コンフィギュレーション モードで**glbpweighting** 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。

glbp *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*]
no glbp *group* **weighting**

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
maximum	1 ～ 254 の範囲の最大重み値。デフォルト値は 100 です。
lower *lower*	（任意）1 から指定された最大重み値までの範囲で重み値の下限を指定します。デフォルト値は 1 です。
upper *upper*	（任意）重み値の下限から最大重み値までの範囲で重み値の上限を指定します。デフォルト値は指定された最大重み値です。

コマンド デフォルト

デフォルトのゲートウェイ重み値は 100 で、デフォルトの下限重み値は 1 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 Release 2.1	このコマンドが導入されました。

使用上のガイドライン

仮想ゲートウェイの重み値は、ゲートウェイの転送能力の指標です。デバイス上の追跡対象インターフェイスに障害が発生し、そのデバイスの重み値が最大値から下限しきい値を下回るまで減ると、デバイスは仮想フォワーダとしての役割を放棄します。デバイスの重み値が上限しきい値を上回るまで増えると、デバイスは仮想フォワーダのアクティブな役割を再開できます。

追跡対象となるインターフェイスのパラメータを設定するには、**glbpweightingtrack** and **track** コマンドを使用します。デバイスのインターフェイスがダウンすると、デバイスの重み値が指定された値まで減少する場合があります。

例

次に、GLBP グループ 10 のゲートウェイの重み値を、重み値の下限を 95 に、重み値の上限を105 に、最大値を 110 に設定する例を示します。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
```

関連コマンド

Command	Description
glbpweightingtrack	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。
track	追跡対象インターフェイスを設定します。

glbp weighting track

トラッキング対象オブジェクトの可用性に基づいてGateway Load Balancing Protocol（GLBP）の重み値が増減するようにトラッキング対象オブジェクトを指定するには、インターフェイスコンフィギュレーションモードで**glbpweightingtrack**コマンドを指定します。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。

glbp *group* **weighting track** *object-number* [**decrement** *value*]
no glbp *group* **weighting track** *object-number* [**decrement** *value*]

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
object-number	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。有効な範囲は 1 ～ 1000 です。トラッキング対象オブジェクトを設定するには、**track** コマンドを使用します。
decrement *value*	（任意）インターフェイスがダウン（または復旧）したときにデバイスの GLBP の重み値を減らす（または増やす）量を指定します。値の範囲は 1 ～ 254 です。デフォルト値は 10 です。

コマンド デフォルト

GLBP の重み値の変更時に、オブジェクトはトラッキングされません。

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 Release 2.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、GLBPゲートウェイの重み値とゲートウェイインターフェイスの可用性を関連付けます。これは、GLBP に設定されてないインターフェイスをトラッキングする場合に便利です。

トラッキング対象のインターフェイスがダウンすると、GLBP ゲートウェイの重み値は 10 減少します。インターフェイスがトラッキングされない場合、インターフェイスの状態の変化は GLBP ゲートウェイの重み値に影響しません。GLBP グループごとに、トラッキング対象インターフェイスの個別のリストを設定できます。

オプションの *value* 引数は、トラッキング対象のインターフェイスがダウンした場合に GLBP ゲートウェイの重み値をどれだけデクリメントするかを指定します。トラッキング対象インターフェイスが稼働状態に戻ると、重み値は同じ分だけ増加します。

複数の追跡対象インターフェイスがダウンすると、それぞれに設定されている重みの減分値が累計されます。

各インターフェイスをトラッキング対象に設定するには、**track** コマンドを使用します。

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

この例では、GigabitEthernet インターフェイス 1/0/1 で、番号の 1 と 2 で表される 2 つのインターフェイスがトラッキングされることを示します。インターフェイス 1 がダウンすると、GLBP ゲートウェイ重み付けがデフォルト値の 10 だけ減算されます。インターフェイス 2 がダウンすると、GLBP ゲートウェイ重み付けが 5 だけ減算されます。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting track 1
Device(config-if)# glbp 10 weighting track 2 decrement 5
```

関連コマンド

Command	Description
glbpweighting	GLBP ゲートウェイの初期重み値を指定します。
track	追跡対象インターフェイスを設定します。

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 **ipaddressdhcp** 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。
interface-type	（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。
number	（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。
hostname	（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 *interface-type number* 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 *hostname* 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、**ipaddressdhcp** 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。

ipaddressdhcp 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 **ipaddressdhcp** 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、**protocolipinarp** 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。**ipaddressdhcp 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。

ipaddressdhcp 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 メッセージに含められます。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、**ipaddressdhcphostname** *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。

noipaddressdhcp 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
ipaddressdhcp	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。*mac-address* 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。
ipaddressdhcphostname *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。*mac-address* 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 *hostname* を含んでいます。
ipaddressdhcpclient-idethernet1	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。
ipaddressdhcpclient-idethernet1hostname *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 *hostname* を含んでいます。

例

次の例では、**ipaddressdhcp** 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
ipdhcppool	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 **ipaddresspool** 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

name	DHCP プールの名前。インターフェイスの IP アドレスは、*name* 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
showipinterface	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**ipaddress** 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

ip-address	[IP Address]。
mask	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**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*vrf-name* 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 Release 2.1	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。

noipaddress 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。

（注） 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。

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（**noiprouting** 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、**bridgecrb** 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 と 192.31.8.17 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。

```
interface GigabitEthernet 1/0/1
 ip address 192.108.1.27 255.255.255.0
 ip address 192.31.7.17 255.255.255.0 secondary
```

関連コマンド

Command	Description
matchiproute-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。
setvrf	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。
showiparp	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。
showipinterface	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。
showroute-map	静的ルート マップとダイナミック ルート マップを表示します。

ip http server

Cisco Web ブラウザのユーザ インターフェイスを含む、IP または IPv6 システム上で HTTP サーバを有効にするには、グローバル コンフィギュレーション モードで **ip http server** コマンドを入力します。HTTP サーバ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。

ip http server
no ip http server

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

HTTP サーバは、デフォルトにより標準のポート 80 を使用します。

HTTP/TCP ポート 8090 はデフォルトにより開いています。

コマンド モード

グローバル 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 3.2SE	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、HTTP サーバへの IPv4 と IPv6 の両方のアクセスを有効にします。ただし、**ip http access-class** コマンドで設定されたアクセス リストは、IPv4 トラフィックにのみ適用されます。IPv6 トラフィック フィルタリングはサポートされていません。

⚠

注意 標準 HTTP サーバとセキュア HTTP（HTTPS）サーバは、同時にシステム上で実行できます。**ip http secure-server** コマンドを使用して HTTPS サーバを有効にする場合は、**no ip http server** コマンドを使用して標準 HTTP サーバを無効にし、標準 HTTP 接続を介してセキュア データにアクセスできないようにします。

HTTP/TCP ポート 8090 を閉じるには、HTTP と HTTPS の両方のサーバを無効にする必要があります。**no http server** コマンドと **no http secure-server** コマンドをそれぞれ入力します。

例

次に、IPv4 と IPV6 の両方のシステムで HTTP サーバをイネーブルにする例を示します。

HTTP サーバを有効にした後は、使用する HTML ファイルの場所を指定して基本パスを設定できます。通常、HTTP Web サーバで使用される HTML ファイルは、システムのフラッシュ メモリに格納されます。リモート URL はこのコマンドを使用して指定できますが、リモート パス名（たとえば、HTML ファイルがリモート TFTP サーバ上にある場合など）の使用は推奨されません。

```
Device(config)#ip http server
Device(config)#ip http path flash:
```

関連コマンド

コマンド	説明
ip http access-class	HTTP サーバへのアクセスを制限する際に使用するアクセス リストを指定します。
ip http path	HTTP サーバが使用するファイルを見つけるために使用する基本パスを指定します。
ip http secure-server	HTTPS サーバをイネーブルにします。

ip http secure-server

セキュアHTTP（HTTPS）サーバを有効にするには、グローバルコンフィギュレーションモードで **ip http secure-server** コマンドを入力します。HTTPS サーバ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。

ip http secure-server
no ip http secure-server

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

HTTPS サーバはディセーブルです。

コマンド モード

グローバル 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 3.2SE	このコマンドが導入されました。

使用上のガイドライン

HTTPS サーバは、セキュア ソケット レイヤ（SSL）バージョン3.0プロトコルを使用します。

⚠

注意 HTTPS サーバをイネーブルにする場合は、同じサービスに対するセキュリティ保護されていない接続を防ぐため、常に標準HTTPサーバをディセーブルにする必要があります。グローバル コンフィギュレーション モードで **no ip http server** コマンドを使用して標準 HTTP サーバを無効にします（この手順は予防手段であり、通常、HTTP サーバはデフォルトで無効になっています）。

認証に認証局（CA）が使用されている場合は、HTTPSサーバをイネーブルにする前にルーティング デバイスで CA トラストポイントを宣言する必要があります。

HTTP/TCP ポート 8090 を閉じるには、HTTP と HTTPS の両方のサーバを無効にする必要があります。**no http server** コマンドと **no http secure-server** コマンドをそれぞれ入力します。

例

次の例では、HTTPS サーバが有効で、（以前に設定された）CA トラストポイント CA-trust-local が指定されています。

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ip http secure-server
Device(config)#ip http secure-trustpoint CA-trust-local
Device(config)#end

Device#show ip http server secure status
HTTP secure server status: Enabled
HTTP secure server port: 443
```

```
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: CA-trust-local
```

関連コマンド

コマンド	説明
ip http secure-trustpoint	HTTPS サーバの署名付き証明書を取得するために使用する CA トラストポイントを指定します。
ip http server	シスコの Web ブラウザ ユーザ インターフェイスを含む IP または IPv6 システムで HTTP サーバを有効にします。
show ip http server secure status	HTTPS サーバの設定ステータスを表示します。

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 **ipnhrpmap** 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

ip-address	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。
ip-nbma-address	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。
destination-mask	宛先アドレス マスク。
ipv6-nbma-address	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 のみをサポートします。*ipv6-nbma-address* 引数はスイッチで使用できますが、設定しても無効です。

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、**ipospfnetworkpoint-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 **ipsplit-horizoneigrp** 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
clearipnhrp	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。
ipsplit-horizoneigrp	EIGRP スプリット ホライズンを有効にします。
ipospfnetworkpoint-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 **ipnhrpmapmulticast** 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

ip-nbma-address	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。
ipv6-nbma-address	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 のみをサポートします。*ipv6-nbma-address* 引数はスイッチで使用できますが、設定しても無効です。

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、**tunneldestination** 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。
tunneldestination	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 **ipnhrpnetwork-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

number	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
clearipnhrp	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 **ipnhrpnhs** 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

nhs-address	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。
nbma-address	NBMA アドレス。
FQDN-string	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の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、**ipnhrpnhs**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* 引数を指定して **ipnhrpnhs** 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
ipnhrpmap	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。
showipnhrp	NHRP マッピング情報を表示します。

key chain

ルーティング プロトコルの認証を有効にし、キー チェーン コンフィギュレーション モードを開始するのに必要な認証キー チェーンを定義するには、グローバル コンフィギュレーション モードで **keychain** 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

name-of-chain	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。**keychain** 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。
showkeychain	認証キーの情報を表示します。

key-string（認証）

キーに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

text	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。
keychain	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。
showkeychain	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

key-id	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。

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、ソフトウェアが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す。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 keychain** 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。
keychain	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。
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。
showkeychain	認証キーの情報を表示します。

show glbp

Gateway Load Balancing Protocol（GLBP）情報を表示するには、特権 EXEC モードで **showglbp** コマンドを使用します。

capability [*interface-type interface-number*]
interface-type interface-number [*group-number*] [*state*] **[brief]**

構文の説明

capability	（任意）GLBP 機能インターフェイスを表示します。
interface-type interface-number	（任意）出力を表示するインターフェイスのタイプおよび番号
group-number	（任意）0 ～ 1023 の範囲の GLBP グループ番号
state	（任意）次のいずれかの GLBP デバイスの状態：**active**、**disabled**、**init**、**listen**、**standby**
brief	（任意）1 行の出力で各仮想ゲートウェイまたは仮想フォワーダの要約を示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが導入されました。

使用上のガイドライン

デバイスの GLBP グループに関する情報を表示するには、**showglbp** コマンドを使用します。**brief** キーワードは、各仮想ゲートウェイまたは仮想フォワーダに関する情報を 1 行で表示します。**capability** キーワードは、すべての GLBP 対応インターフェイスを表示します。

例

次に、GLBP グループ 10 を表示する **showglbp** コマンドからの出力例を示します。

```
Device# show glbp GigabitEthernet 1/0/1 10
GigabitEthernet1/0/1 - Group 10
  State is Active
    1 state change, last state change 00:04:52
  Virtual IP address is 10.21.8.10
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.608 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption disabled
  Active is local
  Standby is unknown
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  Group members:
```

```
  ac7e.8a35.6364 (10.21.8.32) local
There is 1 forwarder (1 active)
Forwarder 1
  State is Active
    1 state change, last state change 00:04:41
  MAC address is 0007.b400.0a01 (default)
  Owner ID is ac7e.8a35.6364
  Redirection enabled
  Preemption enabled, min delay 30 sec
  Active is local, weighting 100
```

下の表で、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 *2 : show glbp* フィールドの説明

フィールド	説明
GigabitEthernet 1/0/1 Group	インターフェイス タイプおよびインターフェイスの GLBP グループ番号。
State is	仮想ゲートウェイまたは仮想フォワーダのステート。仮想ゲートウェイの場合、ステートは次のいずれかになります。 • Active：ゲートウェイはアクティブ仮想ゲートウェイ（AVG）で、仮想 IP アドレスの Address Resolution Protocol（ARP）要求に応答します。 • Disabled：仮想 IP アドレスはまだ設定されていない、または学習されていませんが、別の GLBP 設定が存在します。 • Initial：仮想 IP アドレスは設定されている、または学習されていますが、仮想ゲートウェイの設定が完全ではありません。インターフェイスはアップ状態で、ルート IP に設定されている必要があります。インターフェイス IP アドレスが設定されている必要があります。 • Listen：仮想ゲートウェイは hello パケットを受信し、アクティブまたはスタンバイ仮想ゲートウェイが使用できなくなった場合に Speak ステートに変更できます。 • Speak：仮想ゲートウェイはアクティブまたはスタンバイ仮想ゲートウェイになろうとしています。 • Standby：ゲートウェイは次に AVG になる位置にいます。
Virtual IP address is	GLBP グループの仮想 IP アドレス。すべてのセカンダリ仮想 IP アドレスは、1 行ごとに表示されます。仮想 IP アドレスの 1 つが別のデバイスに設定されたアドレスと重複している場合、「duplicate」としてマークされます。重複アドレスは、デバイスが ARP キャッシュ エントリの保護に失敗したことを示します。

フィールド	説明
Hello time, hold time	Hello timeとは、hello パケット間の時間のことです（秒またはミリ秒単位）。Hold timeとは、他のデバイスがアクティブ ルータのダウンを宣言するまでの時間です（秒またはミリ秒単位）。GLBP グループのすべてのデバイスは、現在の AVG の hello 時間値と保留時間値を使用します。ローカルに設定された値が異なる場合、設定された値が hello 時間値と保留時間値の後ろのカッコ内に表示されます。
Next hello sent in	GLBPが次のhelloパケットを送信するまでの時間（秒またはミリ秒単位）。
プリエンプション	GLBP ゲートウェイのプリエンプションがイネーブルであるかどうか。有効な場合、最小遅延は、優先順位の低いアクティブデバイスをプリエンプトするまで、優先順位の高いの非アクティブデバイスが待つ時間です（秒単位）。 このフィールドも、GLBP フォワーダのプリエンプションを示すフォワーダ セクションの下に表示されます。
Active is	仮想ゲートウェイのアクティブ状態。値は「local」、「unknown」、または IP アドレスです。アドレス（およびアドレスの有効期限）は、現在の AVG のアドレスです。 このフィールドも、現在の AVF のアドレスを示すフォワーダ セクションの下に表示されます。
Standby is	仮想ゲートウェイのスタンバイ状態。値は「local」、「unknown」、または IP アドレスです。アドレス（およびアドレスの有効期限）は、スタンバイ ゲートウェイのアドレスです（ゲートウェイは次に AVG になります）。
重み付け	下限しきい値と上限しきい値のある初期重み値。
Track object	追跡対象オブジェクトのリストとそれらに対応する状態。
IP redundancy name is	GLBP グループの名前。

関連コマンド

Command	Description
glbpip	GLBP をイネーブルにします。
glbptimers	helloメッセージの間隔と、他のデバイスによってアクティブGLBPデバイスのダウンが宣言されるまでの時間を設定します。
glbpweightingtrack	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。

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

interface	（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 *3:* 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
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 *4 : 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
ipnhrpmap	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。
showipnhrp	NHRP マッピング情報を表示します。

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

name-of-chain	（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、**showkeychain** 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 **showtrack** 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
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。
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
```

下の表で、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	[アップ（Up）]または[ダウン（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。
trackinterface	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。
trackiproute	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

object-number	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。
interface *type number*	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。
iprouting	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。
ipv6routing	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** と併せて **glbpweighting** 及び **glbpweightingtrack** 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
glbpweighting	GLBP ゲートウェイの初期重み値を指定します。
glbpweightingtrack	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

group-id	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
timersadvertise	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 **vrrpdescription** 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

text	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
Cisco IOS XE Release 2.1	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。

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

構文の説明

delayminimum *seconds*	（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
Cisco IOS XE Release 2.1	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、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

level	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
Cisco IOS XE Release 2.1	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。
vrrppreempt	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 **timersadvertise** 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] 間隔
no timers advertise [msec] 間隔

構文の説明

group	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。
msec	（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。
間隔	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
Cisco IOS XE Release 2.1	このコマンドが導入されました。

使用上のガイドライン

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。

vrrptimersadvertise 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ト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。
timerslearn	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

vrrs-leader-name	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。