



I コマンド

この章では、I で始まる Cisco NX-OS ユニキャスト ルーティング コマンドについて説明します。

ip (GLBP)

グループに対して Gateway Load Balancing Protocol (GLBP) をアクティブにするには、**ip** コマンドを使用します。グループの GLBP 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 [*ip-address* [**secondary**]]

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

シンタックスの説明

<i>ip-address</i>	(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。

デフォルト

ディセーブル

コマンド モード

GLBP コンフィギュレーション

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

設定済みのインターフェイスに対して GLBP をアクティブにするには、**ip** コマンドを使用します。仮想 IP アドレスを設定する場合、そのアドレスは GLBP グループ全体の専用 IP アドレスになります。仮想 IP アドレスを設定しない場合、ゲートウェイは同じ GLBP グループ内の別のゲートウェイから仮想 IP アドレスを学習します。GLBP が Active Virtual Gateway (AVG; アクティブ仮想ゲートウェイ) を選択できるようにするには、その LAN 上の 1 つ以上のゲートウェイに仮想 IP アドレスを設定する必要があります。

AVG に仮想 IP アドレスを設定すると、現在使用されている仮想 IP アドレスが上書きされます。

インターフェイスに **ip** コマンドを設定すると、プロキシ Address Resolution Protocol (ARP; アドレス解決プロトコル) 要求の処理方法が変更されます (プロキシ ARP がディセーブルに設定されていない場合)。ホストは IP アドレスを MAC アドレスにマッピングするために ARP 要求を送信します。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 要求に応答します。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。

**(注)**

ip コマンドを使用して仮想 IP アドレスを指定し、GLBP グループをアクティブにする前に、すべての GLBP オプションを設定する必要があります。

このコマンドにはライセンスは必要ありません。

例

次に、イーサネット インターフェイス 1/1 上でグループ 10 用の GLBP をアクティブにする例を示します。GLBP グループで使用される仮想 IP アドレスは、192.0.2.10 に設定されます。

```
switch(config)# interface ethernet 1/1
switch(config-if)# ip address 192.0.2.32 255.255.255.0
switch(config-if)# glbp 10
switch(config-glbp)# ip 192.0.2.10
```

次に、イーサネット インターフェイス 2/1 上でグループ 10 用の GLBP をアクティブにする例を示します。GLBP グループで使用される仮想 IP アドレスは、同じ GLBP グループに属するように設定された別のゲートウェイから取得されます。

```
switch(config)# interface ethernet 2/1
switch(config-if)# glbp 10
switch(config-glbp)# ip
```

関連コマンド

コマンド	説明
glbp	GLBP コンフィギュレーション モードに入って、GLBP グループを作成します。
show glbp	GLBP の情報を表示します。

ip (HSRP)

HSRP グループに仮想アドレスを指定するには、**ip** コマンドを使用します。グループの HSRP 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 [**autoconfig** | *ip-address* [**secondary**]]

no ip [**autoconfig** | *ip-address* [**secondary**]]

シンタックスの説明

autoconfig	(任意) リンクローカル プレフィックスと修正 EUI-64 形式のインターフェイス 識別情報からリンクローカル アドレスを生成します。ここで、EUI-64 インターフェイス識別情報は関連する HSRP 仮想 MAC アドレスから作成されます。グローバルユニキャスト 仮想 IPv6 アドレスが設定されている場合は、このオプションを設定できません。
<i>ip-address</i>	(任意) 仮想ルータの仮想 IP アドレス (HSRP グループ)。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。その HSRP グループ内の 1 つ以上のルータに仮想 IP アドレスを設定する必要があります。グループ内の他のルータはこのアドレスを選択します。IP アドレスは、IPv4 または IPv6 アドレスにすることができます。
secondary	(任意) IPv4 アドレスがセカンダリ HSRP 仮想アドレスであることを示します。HSRP IPv6 グループにはセカンダリ アドレスがありません。

デフォルト

ディセーブル

コマンド モード

HSRP コンフィギュレーション

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
5.0(2)	IPv6 のサポートと autoconfig キーワードが追加されました。
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

設定済みのインターフェイスに対して HSRP をアクティブにするには、**ip** コマンドを使用します。仮想 IP アドレスを設定する場合、そのアドレスは HSRP グループ全体の専用 IP アドレスになります。IPv4 グループの場合は、仮想 IP アドレスが設定されていなければ、ゲートウェイは同じ HSRP グループ内の別のゲートウェイから仮想 IP アドレスを取得します。HSRP が Active Virtual Gateway (AVG; アクティブ仮想ゲートウェイ) を選択できるようにするには、その LAN 上の 1 つ以上のゲートウェイに仮想 IP アドレスを設定する必要があります。IPv6 グループの場合は、**autoconfig** キーワードを使用して仮想 IP アドレスを生成できます。

AVG に仮想 IP アドレスを設定すると、現在使用されている仮想 IP アドレスが上書きされます。

設定された IPv6 アドレスがリンクローカルアドレスの場合は、HSRP Ipv6 セカンダリ アドレスが存在しません。

インターフェイス上で IPv4 HSRP グループ用に **ip** コマンドを設定すると、プロキシ Address Resolution Protocol (ARP; アドレス解決プロトコル) 要求の処理方法が変更されます (プロキシ ARP がディセーブルに設定されていない場合)。ホストは IP アドレスを MAC アドレスにマッピングするために ARP 要求を送信します。HSRP 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 要求に応答します。HSRP 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。



(注)

ip コマンドを使用して仮想 IP アドレスを指定し、HSRP グループをアクティブにする前に、すべての HSRP オプションを設定する必要があります。このようにすれば、グループを初めてイネーブルにする際にコンフィギュレーションの作成が遅れても、他のルータに認証エラー メッセージや不測の状態変更が生じるのを避けることができます。常に IP アドレスを指定することを推奨します。

このコマンドにはライセンスは必要ありません。

例

次に、イーサネット インターフェイス 1/1 上でグループ 10 用の HSRP をアクティブにする例を示します。HSRP グループで使用される仮想 IP アドレスは、192.0.2.10 に設定されます。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# ip address 192.0.2.32 255.255.255.0
switch(config-if)# hsrp 10
switch(config-hsrp)# ip 192.0.2.10
```

次に、イーサネット インターフェイス 2/1 上でグループ 10 用の HSRP をアクティブにする例を示します。HSRP グループで使用される仮想 IP アドレスは、同じ HSRP グループに属するように設定された別のゲートウェイから取得されます。

```
switch(config)# interface ethernet 2/1
switch(config-if)# hsrp 10
switch(config-hsrp)# ip
```

次に、イーサネット インターフェイス 1/1 上でグループ 2 用の HSRP をアクティブにする例を示します。この例では、インターフェイス上にセカンダリ IP アドレスが作成されます。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# ip address 20.20.20.1 255.255.255.0 secondary
switch(config-if)# ip address 10.10.10.1 255.255.255.0
switch(config-if)# hsrp 2
switch(config-if-hsrp)# ip 10.10.10.2
switch(config-if-hsrp)# ip 20.20.20.2 secondary
```

関連コマンド

コマンド	説明
feature hsrp	HSRP コンフィギュレーションをイネーブルにします。
show hsrp	HSRP 情報を表示します。

ip arp

スタティック ARP エントリを設定するには、**ip arp** コマンドを使用します。スタティック ARP 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 arp ip-address mac-address

no ip arp ip-address

シンタックスの説明	ip-address	A.B.C.D 形式の IPv4 アドレス。
	mac-address	次の形式の MAC アドレス : <ul style="list-style-type: none"> • E.E.E • EE-EE-EE-EE-EE-EE • EE:EE:EE:EE:EE:EE • EEEE.EEEE.EEEE

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

サポートされるユーザ ロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。
4.2(1)	マルチキャスト スタティック MAC アドレスに対するサポートが追加されました。

使用上のガイドライン

このコマンドにはライセンスは必要ありません。

例

次に、インターフェイス イーサネット 2/1 上でスタティック ARP エントリを設定する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip arp 192.0.2.1 0150.5a03.efab
```

関連コマンド

コマンド	説明
show ip arp	ARP エントリを表示します。

ip arp gratuitous

無償 ARP をイネーブルにするには、**ip arp gratuitous** コマンドを使用します。無償 ARP 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 arp gratuitous {request | update}

no ip arp gratuitous {request | update}

シンタックスの説明

request	アドレス重複検出時の無償 ARP 要求の送信をイネーブルにします。
update	無償 ARP 用の ARP キャッシュのアップデートをイネーブルにします。

デフォルト

イネーブル

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(3)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにはライセンスは必要ありません。

例

インターフェイス Ethernet 2/1 上の gratuitous ARP 要求をディセーブルにする例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip arp request
```

関連コマンド

コマンド	説明
ip arp	スタティック ARP エントリを設定します。

ip as-path access-list

Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) Autonomous System (AS; 自律システム) 番号に対する access-list フィルタを設定するには、**ip as-path access-list** を使用します。フィルタを削除するには、このコマンドの **no** 形式を使用します。

```
ip as-path access-list name {deny | permit} regexp
```

```
no ip as-path access-list name {deny | permit} regexp
```

シンタックスの説明

name	AS パス アクセス リスト名。名前は、63 文字以下の任意の英数字文字列にできます。
deny	AS 番号が <i>regexp</i> 引数と一致するパケットを拒否します。
permit	AS 番号が <i>regexp</i> 引数と一致するパケットを許可します。
regexp	BGP AS パスと照合する正規表現。正規表現についての詳細は、次の URL で『Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 5.x』を参照してください。 http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/fundamentals/configuration/guide2/fun_nx-os_book.html

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

自律システム パス フィルタを設定するには、**ip as-path access-list** コマンドを使用します。着信と発信の両方の BGP パスに自律システム パス フィルタを適用できます。各フィルタは正規表現で定義されます。正規表現が、ルート of 自律システム パスの ASCII ストリング表現と一致した場合、許可または拒否の条件が適用されます。自律システム パスにはローカル自律システム番号を含めないでください。このコマンドにはライセンスは必要ありません。

例

AS 番号 55:33 および 20:01 を許可する AS パス フィルタを BGP に設定し、着信フィルタリングの BGP ピアにこのフィルタを適用する例を示します。

```
switch# configure terminal
switch(config)# ip as-path access-list filter1 permit 55:33,20:01
switch(config) router bgp 65536:20
switch(config-router)# neighbor 192.0.2.1/16 remote-as 65536:20
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# filter-list filter1 in
```

関連コマンド

コマンド	説明
filter-list	BGP ピアに対する AS パス フィルタを指定します。
show ip as-path access-list	IP AS パス アクセス リストに関する情報を表示します。

ip authentication key-chain eigrp

Enhanced Interior Gateway Routing Protocol (EIGRP) パケットの認証をイネーブルにして、インターフェイス上で使用可能なキー セットを指定するには、**ip authentication key-chain eigrp** コマンドを使用します。認証を禁止するには、このコマンドの **no** 形式を使用します。

ip authentication key-chain eigrp *instance-tag* *name-of-chain*

no ip authentication key-chain eigrp *instance-tag* *name-of-chain*

シンタックスの説明

<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
<i>name-of-chain</i>	有効なキー グループ

デフォルト

EIGRP パケットには認証は適用されません。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

インターフェイス コンフィギュレーション モードで **ip authentication mode eigrp** コマンドを使用して、認証モードを設定する必要があります。インターフェイスに対する認証設定を完了するには、**key-chain** コマンドを使用して、別途キー チェーンを設定する必要があります。

このコマンドには、Enterprise Services ライセンスが必要です。

例

キーチェーン ツリーに属しているキーの受け入れと送信をインターフェイスに設定する例を示します。

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 1/2
switch(config-if)# ip authentication key-chain eigrp 209 trees
```

関連コマンド

コマンド	説明
ip authentication mode eigrp	インターフェイスに EIGRP の認証モードを設定します。
key-chain	認証方式で使用可能なキー セットを作成します。

ip authentication mode eigrp

EIGRP パケット内で使用される認証タイプを指定するには、**ip authentication mode eigrp** コマンドを使用します。認証を削除するには、このコマンドの **no** 形式を使用します。

ip authentication mode eigrp *instance-tag* md5

no ip authentication mode eigrp *instance-tag* md5

シンタックスの説明

<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
md5	Message Digest 5 (MD5) 認証を指定します。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、Enterprise Services ライセンスが必要です。

例

インターフェイスに使用される認証方式を MD5 に設定する例を示します。

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 1/2
switch(config-if)# ip authentication mode eigrp 209 md5
```

関連コマンド

コマンド	説明
authentication mode (EIGRP)	VRF の EIGRP の認証モードを設定します。
ip authentication key-chain eigrp	EIGRP の認証をイネーブルにして、インターフェイスに使用可能なキーセットを指定します。
key chain	認証方式で使用可能なキーセットを作成します。

ip bandwidth eigrp

Enhanced Interior Gateway Routing Protocol (EIGRP) インターフェイスの帯域幅を設定するには、**ip bandwidth eigrp** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip bandwidth eigrp *instance-tag* *bandwidth*

no ip bandwidth eigrp

シンタックスの説明

<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
<i>bandwidth</i>	帯域幅値。範囲は 1 ~ 2,560,000,000 キロビットです。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、Enterprise Services ライセンスが必要です。

例

自律システム 209 で帯域幅 10000 が使用されるように EIGRP を設定する例を示します。

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip bandwidth eigrp 209 10000
```

関連コマンド

コマンド	説明
ip bandwidth-percent eigrp	インターフェイスの帯域幅のうち、EIGRP に使用できる割合をパーセントで設定します。

ip bandwidth-percent eigrp

インターフェイス上で Enhanced Interior Gateway Routing Protocol (EIGRP) に使用できる帯域幅のパーセンテージを設定するには、**ip bandwidth eigrp** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip bandwidth-percent eigrp *instance-tag percent*

no ip bandwidth-percent eigrp

シンタックスの説明

<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
<i>percent</i>	EIGRP に使用できる帯域幅のパーセンテージ

デフォルト

percent : 50

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

EIGRP が使用する帯域幅は、リンクの帯域幅の最大 50 % です。このパーセンテージは、**ip bandwidth** インターフェイス コンフィギュレーション コマンドで定義されます。このデフォルトのパーセンテージを変更するには、**ip bandwidth-percent** コマンドを使用します。

このコマンドには、Enterprise Services ライセンスが必要です。

例

自律システム 209 でインターフェイスの帯域幅の最大 75 % を使用するように EIGRP を設定する例を示します。

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip bandwidth-percent eigrp 209 75
```

関連コマンド

コマンド	説明
ip bandwidth eigrp	インターフェイスの EIGRP 帯域幅値を設定します。

ip community-list

コミュニティ リストのエントリを作成するには、**ip community-list** コマンドを使用します。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 community-list standard list-name {deny | permit} {aa:nn | internet | local-AS | no-advertise | no-export}
```

```
no ip community-list standard list-name
```

```
ip community-list expanded list-name {deny | permit} regex
```

```
no ip community-list expanded list-name
```

シンタックスの説明

standard <i>list-name</i>	標準コミュニティ リストを設定します。
permit	一致条件のアクセスを許可します。
deny	一致条件のアクセスを拒否します。
<i>aa:nn</i>	(任意) 4 バイトの新コミュニティ形式で入力する自律システム番号およびネットワーク番号。この値は、コロンで区切られた 2 バイトの数 2 つで設定されます。2 バイトの数ごとに 1 ~ 65535 の数を入力できます。1 つのコミュニティ、または複数のコミュニティをそれぞれスペースで区切って入力できます。 これらの任意のコミュニティ キーワードを複数選択できます。
internet	(任意) インターネット コミュニティを指定します。このコミュニティのルートは、すべてのピア (内部および外部) にアドバタイズされます。 これらの任意のコミュニティ キーワードを複数選択できます。
no-export	(任意) no-export コミュニティを指定します。このコミュニティのあるルートは、同じ AS 内のピアへのみ、または連合内の他のサブ AS へのみアドバタイズされます。これらのルートは外部ピアにはアドバタイズされません。 これらの任意のコミュニティ キーワードを複数選択できます。
local-AS	(任意) local-as コミュニティを指定します。コミュニティのあるルートは、ローカル AS の一部であるピアへのみ、または連合のサブ AS 内のピアへのみアドバタイズされます。これらのルートは、外部ピア、または連合内の別のサブ AS にアドバタイズされません。 これらの任意のコミュニティ キーワードを複数選択できます。
no-advertise	(任意) no-advertise コミュニティを指定します。このコミュニティのあるルートはピア (内部または外部) にはアドバタイズされません。 これらの任意のコミュニティ キーワードを複数選択できます。

expanded list-name	拡張コミュニティ リストを設定します。
regex	入力ストリングとの照合パターンの指定に使用される正規表現。正規表現についての詳細は、次の URL で『Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 5.x』を参照してください。 http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/fundamentals/configuration/guide2/fun_nx-os_book.html



(注) 正規表現を使用できるのは拡張コミュニティ リストだけです。

デフォルト

コミュニティの交換はデフォルトではイネーブルになりません。

コマンド モード

グローバル コンフィギュレーション (config)

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

BGP コミュニティ フィルタリングを設定するには、**ip community-list** コマンドを使用します。BGP コミュニティ値は 4 バイトの数値で設定されます。先頭の 2 バイトは自律システム番号を表し、末尾の 2 バイトはユーザ定義のネットワーク番号を表します。BGP ピア間の BGP コミュニティ アトリビュート交換は、**send-community** コマンドが、指定されたネイバー用に設定されている場合にイネーブルになります。BGP コミュニティ アトリビュートは、RFC 1997 および RFC 1998 に定義されています。

BGP コミュニティの交換はデフォルトではイネーブルになりません。**send-community** コマンドは、BGP ネイバー アドレスファミリ コンフィギュレーション モードで、BGP ピア間の BGP コミュニティ アトリビュート交換をイネーブルにするために使用します。

このコマンドまたは **set community** コマンドで他のコミュニティ値が設定されるまで、デフォルトではすべてのルータまたはプレフィクスにインターネット コミュニティが適用されます。

特定のコミュニティ セットと照合するように許容値が設定されている場合は、デフォルトで、コミュニティ リストが他のすべてのコミュニティ値に対して暗黙拒否に設定されます。**internet** コミュニティは、コミュニティ リストに暗黙許可を適用するために使用します。

標準コミュニティ リスト

標準コミュニティ リストは、既知のコミュニティや特定のコミュニティ番号の設定に使用されます。任意のコミュニティ キーワードを複数選択できます。各標準コミュニティ リストには最大 16 のコミュニティを設定できます。16 を超えるコミュニティを設定しようとする、制限数を越えた後続のコミュニティは処理されないか、または実行コンフィギュレーション ファイルに保存されます。

設定できる最大コミュニティ数は 32 です。

拡張コミュニティ リスト

拡張コミュニティ リストは正規表現によるフィルタ コミュニティに使用されます。正規表現は、コミュニティ アトリビュートの照合パターンを設定に使用されます。* または + の文字を使用した照合の順序は、最長のコンストラクトが最初になります。入れ子式のコンストラクトは外側から内側へ照合されます。連結コンストラクトは左側から順に照合されます。ある正規表現が、1 つの入力ストリングの異なる 2 つの部分と一致する可能性がある場合、早く入力された部分が最初に一致します。

コミュニティ リストの処理

同じコミュニティ リスト文に複数の値を設定すると、論理 AND 条件が作成されます。AND 条件を満たすためにはすべてのコミュニティ値が一致しなければなりません。別のコミュニティ リスト文に複数の値を設定すると、論理 OR 条件が作成されます。条件に一致する最初のリストが処理されます。

このコマンドにはライセンスは必要ありません。

例

指定コミュニティのルートがすべてのピア（内部と外部の両方）にアダプタイズされるような標準コミュニティ リストの設定例を示します。

```
switch(config)# ip community-list standard test1 permit internet
switch(config)#
```

次に、以下の場所からのルートを許容するような標準コミュニティ リストの設定例を示します。

- 自律システム 65534 のネットワーク 40、および自律システム 65412 のネットワーク 60
- 同じ自律システム内のピア、または同じコンフェデレーション内のサブ自律システムのピア

この例では、論理 AND 条件が使用されているので、すべてのコミュニティ値が一致しないとリストは処理されません。

```
switch(config)# ip community-list standard test1 permit 65534:40 65412:60 no-export
switch(config)#
```

次の例では、標準コミュニティ リストが、自律システム 65534 内のネットワーク 40 からのコミュニティと自律システム 65412 内のネットワーク 60 からのコミュニティを搬送するルートを拒否するように設定されます。この例は、論理 AND 条件を示しています。すべてのコミュニティ値が一致しないとリストが処理されません。

```
switch(config)# ip community-list standard test2 deny 65534:40 65412:60
```

次の例では、名前付き標準コミュニティ リストが、ローカル自律システム内のすべてのルートを許可する、または、自律システム 40000 内のネットワーク 20 からのルートを許可するように設定されます。この例は、論理 OR 条件を示しています。最初の一致が処理されます。

```
switch(config)# ip community-list standard RED permit local-AS
```

```
switch(config)# ip community-list standard RED permit 40000:20
switch(config)#
```

次の例では、プライベート自律システムからのコミュニティを持つルートを拒否するような拡張コミュニティ リストが設定されます。

```
switch(config)# ip community-list expanded 500 deny
_64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_
switch(config)#
```

次の例では、自律システム 50000 のネットワーク 1 から 99 からのルートを拒否するような名前方式の拡張コミュニティ リストが設定されます。

```
switch(config)# ip community-list list expanded BLUE deny 50000:[0-9][0-9]_
switch(config)#
```

関連コマンド

コマンド	説明
feature bgp	BGP をイネーブルにします。
match community	ルート マップ内のコミュニティを照合します。
send-community	コミュニティアトリビュートを BGP ピアに伝搬するように BGP を設定します。
set community	ルート マップ内のコミュニティを設定します。

ip delay eigrp

インターフェイスでの Enhanced Interior Gateway Routing Protocol (EIGRP) のスルーput 遅延を設定するには、**ip delay eigrp** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip delay eigrp *instance-tag* *seconds*

no ip delay eigrp *instance-tag*

シンタックスの説明

<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
<i>seconds</i>	スルーput 遅延 (10 マイクロ秒)。範囲は 1 ~ 16777215 です。

デフォルト

100 (10 マイクロ秒単位)

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

10 マイクロ秒単位でインターフェイスにスルーput 遅延を設定します。たとえば、**ip delay eigrp** コマンドを 100 に設定すると、スルーput 遅延は 1000 マイクロ秒になります。

このコマンドには、Enterprise Services ライセンスが必要です。

例

インターフェイスの遅延を 400 マイクロ秒に設定する例を示します。

```
switch(config)# router eigrp 1
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip delay eigrp 1 40
```

関連コマンド

コマンド	説明
ip hello-interval eigrp	自律システム番号で指定される EIGRP ルーティングプロセスに対するインターフェイスの hello インターバルを設定します。

ip directed-broadcast

ダイレクトブロードキャストから物理ブロードキャストへの変換をイネーブルにするには、**ip directed-broadcast** 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。

ip directed-broadcast

no ip directed-broadcast

シンタックスの説明 このコマンドには、キーワードと引数はありません。

デフォルト 無効。すべての IP ダイレクトブロードキャストが破棄されます。

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

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン IP ダイレクトブロードキャストとは、宛先アドレスは特定の IP サブネットの有効なブロードキャストアドレスだが、その宛先サブネット上に存在しないノードから送信された IP パケットのことです。

宛先サブネットに直接接続されていないデバイスは、ユニキャスト IP パケットをそのサブネット上のホストに転送するのと同じ方法で、IP ダイレクトブロードキャストを転送します。ダイレクトブロードキャストパケットが、宛先サブネットに直接接続されたデバイスに到着すると、宛先サブネット上のブロードキャストとして「展開」されます。パケットの IP ヘッダーに含まれる宛先アドレスがサブネット用に設定された IP ブロードキャストアドレスに書き換えられ、パケットがリンクレイヤブロードキャストとして送信されます。

ダイレクトブロードキャストがインターフェイスに対して有効になっている場合は、アドレスからそのインターフェイスが接続されたサブネット行きのダイレクトブロードキャストとして識別される着信 IP パケットがそのサブネット上のブロードキャストとして展開されます。

no ip directed-broadcast コマンドがインターフェイスに対して設定されている場合は、そのインターフェイスが接続されたサブネット行きのダイレクトブロードキャストが展開されずに破棄されます。



(注) ダイレクトブロードキャストの中でも、特に、Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) ダイレクトブロードキャストが悪意のある人物によって不正使用されたことがあるため、セキュリティ意識の高いユーザが、ダイレクトブロードキャストを必要としないインターフェイスやアクセスリストを使用して展開パケットの数が制限されているインターフェイス上では **ip directed-broadcast** コマンドを無効にすることを推奨します。

このコマンドにはライセンスは必要ありません。

例

次に、イーサネット インターフェイス 2/1 上で IP ダイレクト ブロードキャストの転送をイネーブルにする例を示します。

```
switch(config)# interface ethernet 2/1  
switch(config-if)# ip directed-broadcast
```

ip distribute-list eigrp

インターフェイスでの Enhanced Interior Gateway Routing Protocol (EIGRP) の配布リストを設定するには、**ip distribute-list eigrp** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

```
ip distribute-list eigrp instance-tag {prefix-list list-name | route-map map-name} {in | out}
```

```
no ip distribute-list eigrp instance-tag {prefix-list list-name | route-map map-name} {in | out}
```

シンタックスの説明

instance-tag	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
prefix-list <i>list-name</i>	EIGRP ルートのフィルタリングに使用する IP プレフィクス リストの名前を指定します。
route-map <i>map-name</i>	EIGRP ルートのフィルタリングに使用するルート マップの名前を指定します。
in	着信ルートにルート ポリシーを適用します。
out	発信ルートにルート ポリシーを適用します。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

インターフェイスに対するルート フィルタ ポリシーを設定するには、**ip distribute-list eigrp** コマンドを使用します。この設定を完了するためには、ルート マップまたはプレフィクス リストの名前を設定する必要があります。

このコマンドには、Enterprise Services ライセンスが必要です。

例

インターフェイスに着信するすべての EIGRP ルートのルート マップを設定する例を示します。

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip distribute-list eigrp 209 route-map InputFilter in
```

関連コマンド

コマンド	説明
prefix-list	プレフィクス リストを設定します。
route-map	ルート マップを設定します。

ip domain-list

IP ドメイン リストを設定するには、**ip domain-list** コマンドを使用します。IP ドメイン リスト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 domain-list *domain-name* [**use-vrf** *name*]

no ip domain-list *domain-name* [**use-vrf** *name*]

シンタックスの説明	domain-list	IP ドメイン リストのドメイン名を指定します。名前は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
	use-vrf <i>name</i>	(任意)IP ドメイン リストのドメイン名の解決に使用する Virtual Routing and Forwarding (VRF; 仮想ルーティング/転送) を指定します。名前は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。

デフォルト なし

コマンドモード グローバル コンフィギュレーション
VRF コンテキスト コンフィギュレーション

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン **ip domain-list** コマンドは、デバイス用の追加のドメイン名を設定するために使用します。**vrf context** コマンドは、VRF コンテキスト モードに入って、特定の VRF 用の追加のドメイン名を設定するために使用します。

このコマンドにはライセンスは必要ありません。

例 次に、デフォルト VRF 用の IP ドメイン リストを設定する例を示します。

```
switch# config terminal
switch(config)# ip domain-list Mysite.com
```

次に、管理 VRF 用の IP ドメイン リストを設定する例を示します。

```
switch# config terminal
switch(config)# vrf context management
switch(config-vrf)# ip domain-list Mysite.com
```

次に、デフォルト VRF を通してドメイン名を解決できない場合に管理 VRF をバックアップとして使用するように、デフォルト VRF 用の IP ドメイン リストを設定する例を示します。

```
switch# config terminal
switch(config)# ip domain-list Mysite.com use-vrf management
```

関連コマンド

コマンド	説明
show hosts	IP ドメイン名の設定に関する情報を表示します。

ip domain-lookup

Domain Name Server (DNS; ドメイン ネーム サーバ) の検索機能をイネーブルにするには、**ip domain-lookup** 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。

ip domain-lookup

no ip domain-lookup

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード グローバル コンフィギュレーション モード

サポートされるユーザロール ネットワーク 管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン **ip domain-lookup** コマンドは、DNS をイネーブルにするために使用します。このコマンドにはライセンスは必要ありません。

例 次に、DNS サーバの検索機能を設定する例を示します。

```
switch# config terminal
switch(config)# ip domain-lookup
```

関連コマンド	コマンド	説明
	show hosts	DNS に関する情報を表示します。

ip domain-name

ドメイン名を設定するには、**ip domain-name** コマンドを使用します。ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

ip domain-name *domain-name* [**use-vrf** *name*]

no ip domain-name *domain-name* [**use-vrf** *name*]

シンタックスの説明

domain-name	ドメイン名を指定します。名前は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
use-vrf name	(任意) ドメイン名の解決に使用される VRF を指定します。名前は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。

デフォルト

なし

コマンドモード

グローバル コンフィギュレーション
VRF コンテキスト コンフィギュレーション

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

ip domain-name コマンドは、デバイス用のドメイン名を設定するために使用します。**vrf context** コマンドは、VRF コンテキスト モードを開始して、特定の VRF 用のドメイン モナステリを設定するために使用します。

このコマンドにはライセンスは必要ありません。

例

次に、デフォルト VRF 用の IP ドメイン名を設定する例を示します。

```
switch# config terminal
switch(config)# ip domain-name Mysite.com
```

次に、管理 VRF 用の IP ドメイン名を設定する例を示します。

```
switch# config terminal
switch(config)# vrf context management
switch(config-vrf)# ip domain-name Mysite.com
```

次に、デフォルト VRF を通してドメイン名を解決できない場合に管理 VRF をバックアップとして使用するように、デフォルト VRF 用の IP ドメイン名を設定する例を示します。

■ ip domain-name

```
switch# config terminal
switch(config)# ip domain-name Mysite.com use-vrf management
```

関連コマンド

コマンド	説明
show hosts	IP ドメイン名の設定に関する情報を表示します。

ip eigrp shutdown

インターフェイスの Enhanced Interior Gateway Routing Protocol (EIGRP) をシャットダウンするには、**ip eigrp shutdown** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip eigrp *instance-tag* shutdown

no ip eigrp *instance-tag* shutdown

シンタックスの説明

<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
---------------------	--

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

ip eigrp shutdown コマンドは、保守のために、EIGRP 用のインターフェイスをシャットダウンして、インターフェイスに対する EIGRP 隣接関係を禁止します。このインターフェイスのネットワーク アドレスが EIGRP トポロジ テーブルに表示されなくなります。

ip passive-interface eigrp コマンドは、EIGRP の隣接関係を禁止しますが、トポロジ テーブル内のネットワーク アドレスを維持するために使用します。

このコマンドには、Enterprise Services ライセンスが必要です。

例

インターフェイスの EIGRP を ディセーブルにする例を示します。

```
switch(config)# router eigrp 201
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip eigrp 201 shutdown
```

関連コマンド

コマンド	説明
ip passive-interface eigrp	EIGRP のインスタンスを設定します。
router eigrp	EIGRP のインスタンスを設定します。

ip extcommunity-list

拡張コミュニティ リスト エントリを作成するには、**ip extcommunity-list** コマンドを使用します。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 extcommunity-list standard list-name {deny | permit} generic {transitive | nontransitive} aa4:nn
```

```
no ip extcommunity-list standard generic {transitive | nontransitive} list-name
```

```
ip extcommunity-list expanded list-name {deny | permit} generic {transitive | nontransitive} regexp
```

```
no ip extcommunity-list expanded generic {transitive | nontransitive} list-name
```

シンタックスの説明

standard <i>list-name</i>	名前付き標準拡張コミュニティ リストを設定します。
deny	一致条件のアクセスを拒否します。
permit	一致条件のアクセスを許可します。
generic	汎用特定拡張コミュニティ タイプを指定します。
transitive	拡張コミュニティ アトリビュートを他の自律システムに伝搬するように BGP を設定します。
nontransitive	拡張コミュニティ アトリビュートを他の自律システムに伝搬するように BGP を設定します。
<i>aa4:nn</i>	(任意) 自律システム番号とネットワーク番号。この値は、コロンで区切られた 4 バイトの AS 番号と 2 バイトのネットワーク番号を使用して設定されます。4 バイトの AS 番号の範囲は 1 ~ 4294967295 (プレーンテキスト表記) または 1.0 ~ 56636.65535 (AS.dot 表記) です。単一のコミュニティまたはスペースで区切られた複数のコミュニティを入力できます。
expanded <i>list-name</i>	名前付き詳細拡張コミュニティ リストを設定します。
<i>regexp</i>	入力ストリングとの照合パターンの指定に使用される正規表現。正規表現についての詳細は、次の URL で『Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 5.x』を参照してください。 http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/fundamentals/configuration/guide2/fun_nx-os_book.html
	
(注)	正規表現を使用できるのは詳細拡張コミュニティ リストだけです。

デフォルト

コミュニティの交換はデフォルトではイネーブルになりません。

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.2(1)	このコマンドが追加されました。

使用上のガイドライン

ip extcommunity-list コマンドは、BGP 用の拡張コミュニティ フィルタリングを設定するために使用します。拡張コミュニティ値は 6 バイトの数値として設定されます。先頭の 4 バイトは自律システム番号を表し、末尾の 2 バイトはユーザ定義のネットワーク番号を表します。BGP 汎用特定コミュニティ アトリビュートは、draft-ietf-idr-as4octet-extcomm-generic-subtype-00.txt 内で定義されます。

BGP 拡張コミュニティ交換はデフォルトでイネーブルになっていません。**send-extcommunity** コマンドは、BGP ネイバー アドレスファミリ コンフィギュレーション モードで BGP ピア間の拡張コミュニティ アトリビュート交換をイネーブルにするために使用します。

特定の拡張コミュニティ セットと一致するように許容値が設定されている場合は、デフォルトで、拡張コミュニティ リストが他のすべての拡張コミュニティ値に対して暗黙拒否に設定されます。

標準拡張コミュニティ リスト

標準拡張コミュニティ リストは、特定の拡張コミュニティ番号を設定するために使用します。標準拡張コミュニティ リストでは、最大 16 個の拡張コミュニティを設定できます。

詳細拡張コミュニティ リスト

詳細拡張コミュニティ リストは、正規表現を使用してコミュニティをフィルタするために使用します。正規表現は、コミュニティ アトリビュートと一致するパターンを設定するために使用します。* または + の文字を使用した照合の順序は、最長のコンストラクトが最初になります。入れ子式のコンストラクトは外側から内側へ照合されます。連結コンストラクトは左側から順に照合されます。ある正規表現が、1 つの入カストリングの異なる 2 つの部分と一致する可能性がある場合、早く入力された部分が最初に一致します。

コミュニティ リストの処理

1 つの拡張コミュニティ リスト文で複数の値を設定すると、論理 AND 条件が生成されます。AND 条件を満たすためにはすべての拡張コミュニティ値が一致する必要があります。別々のコミュニティ リスト文で複数の値を設定すると、論理 OR 条件が生成されます。条件に一致する最初のリストが処理されます。

このコマンドにはライセンスは必要ありません。

例

次に、自律システム 1.65534 内のネットワーク 40 からのルートと、自律システム 1.65412 内のネットワーク 60 からのルートを許可する標準汎用特定拡張コミュニティ リストを設定する例を示します。

次の例は、論理 AND 条件を示しています。

```
switch(config)# ip extcommunity-list standard test1 permit generic transitive 1.65534:40
1.65412:60
switch(config)#
```

すべてのコミュニティ値が一致しないとリストは処理されません。

関連コマンド

コマンド	説明
feature bgp	BGP をイネーブルにします。
match extcommunity	ルートマップ内の拡張コミュニティを照合します。
send-community	コミュニティアトリビュートを BGP ピアに伝搬するように BGP を設定します。
set extcommunity	ルートマップ内の拡張コミュニティを設定します。

ip hello-interval eigrp

インターフェイスの EIGRP hello インターバルを設定するには、**ip hello-interval eigrp** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip hello-interval eigrp *instance-tag* *seconds*

no ip hello-interval eigrp *instance-tag*

シンタックスの説明	説明
<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
<i>seconds</i>	hello インターバル (秒単位)。有効範囲は 1 ~ 65535 です。

デフォルト 5 秒

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

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン このコマンドには、Enterprise Services ライセンスが必要です。

例 インターフェイスの hello インターバルを 10 秒に設定する例を示します。

```
switch(config)# router eigrp 1
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip hello-interval eigrp 1 10
```

ip hold-time eigrp

EIGRP インターフェイスのホールド時間を設定するには、**ip hold-time eigrp** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip hold-time eigrp *instance-tag* *seconds*

no ip hold-time eigrp *instance-tag*

シンタックスの説明	
<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
<i>seconds</i>	ホールド時間 (秒単位)。有効範囲は 1 ~ 65535 です。

デフォルト 15 秒

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

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン **ip hold-time eigrp** コマンドは、非常に輻輳した大規模ネットワーク上のデフォルト ホールド時間を増加するために使用します。

ホールド時間は、**hello** インターバルの 3 倍以上の値に設定することを推奨します。指定されたホールド時間内にルータが **hello** パケットを受信しなかった場合は、そのルータ経由のルートが使用できないと判断されます。

ホールド時間を長くすると、ネットワーク全体のルート コンバージェンスが遅延します。

このコマンドには、Enterprise Services ライセンスが必要です。

例 次に、インターフェイスのホールド時間を 40 秒に設定する例を示します。

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip hold-time eigrp 209 40
```

関連コマンド	コマンド	説明
	ip hello-interval eigrp	自律システム番号で指定された EIGRP ルーティング プロセス用のインターフェイス上の hello インターバルを設定します。

ip host

DNS ホスト キャッシュ内で静的なホスト名/アドレス マッピングを定義するには、**ip host** コマンドを使用します。ホスト名/アドレス マッピ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。

ip host name address1 [address2... address6]

no ip host name address1 [address2... address6]

シンタックスの説明

<i>name</i>	ホスト名。 <i>name</i> は、大文字と小文字が区別される 80 文字以下の任意の英数字文字列にできます。
<i>address1</i>	x.x.x.x 形式の IPv4 アドレス。
<i>address2 ...address6</i>	(任意) x.x.x.x 形式の追加の IPv4 アドレス (最大 5 個)。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

ip host コマンドは、スタティック ホスト名を DNS に追加するために使用します。このコマンドにはライセンスは必要ありません。

例

次に、スタティック ホスト名を設定する例を示します。

```
switch(config)# ip host mycompany.com 192.0.2.1
```

関連コマンド

コマンド	説明
ipv6 host	DNS データベース内のスタティック ホスト名を設定します。

ip load-sharing address

ユニキャスト FIB で使用される負荷分散アルゴリズムを設定するには、**ip load-sharing address** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip load-sharing address {destination port destination | source-destination [port source-destination]} [universal-id seed]

no ip load-sharing address {destination port destination | source-destination [port source-destination]} [universal-id seed]

シンタックスの説明	
destination port destination	宛先のアドレスおよびポートに基づく負荷分散アルゴリズムを設定します。
source-destination	送信元と宛先のアドレスに基づく負荷分散アルゴリズムを設定します。
port source-destination	(任意) 送信元と宛先のアドレスおよびポート アドレスに基づく負荷分散アルゴリズムを設定します。
universal-id seed	(任意) 負荷分散ハッシュ アルゴリズムのランダム シードを設定します。範囲は 1 ~ 4294967295 です。

デフォルト 宛先アドレスおよびポート アドレス

コマンド モード グローバル コンフィギュレーション

サポートされるユーザ ロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン **ip load-sharing address** コマンドは、ユニキャスト FIB で RIB 内の等価コスト パスからパスを選択するときに使用される負荷分散アルゴリズムを設定するために使用します。

このコマンドにはライセンスは必要ありません。

例 送信元および宛先のアドレスを使用する負荷分散型アルゴリズムの設定例を示します。

```
switch(config)# ip load-sharing address source-destination
```

関連コマンド

コマンド	説明
show ip load-sharing	負荷分散型アルゴリズムを表示します。
show routing hash	RIB と FIB でソース/宛先ペアに対して選択されたパスを表示します。

ip load-sharing per-packet

インターフェイス上でパケット単位負荷分散を設定するには、**ip load-sharing per-packet** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip load-sharing per-packet

no load-sharing per-packet

シンタックスの説明 このコマンドには、キーワードと引数はありません。

デフォルト ディセーブル

コマンドモード グローバル コンフィギュレーション

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.1(2)	このコマンドが追加されました。

使用上のガイドライン **ip load-sharing per-packet** コマンドは、インターフェイス上で負荷分散アルゴリズムを設定するために使用します。このコマンドは、**ip load-sharing address** コマンドよりも優先されます。



(注)

パケット単位負荷分散を使用すると、不連続パケットが発生する可能性があります。特定のソース/宛先ホスト ペア宛でのパケットが、別のパスをたどったり、順序どおりに宛先に届かなかったりする場合があります。ネットワークやアプリケーションに対する不連続パケットの意味を理解しておいてください。パケット単位負荷分散はすべてのネットワークに適しているわけではありません。フロー単位負荷分散は、パケットが必ず送信順に届くことを保証します。

入力インターフェイス上でパケット単位負荷分散を設定します。この設定によって、Cisco NX-OS でパケットに対して選択される出力インターフェイスが決まります。

たとえば、2 つの出力インターフェイス上に ECMP パスを設定した場合は、Cisco NX-OS でイーサネット 1/1 上の入力パケットに対して次の負荷分散方式が使用されます。

- イーサネット 1/1 上でパケット単位負荷分散を設定した場合はパケット単位負荷分散
- フロー単位負荷分散

他のインターフェイスの設定が、この例のイーサネット 1/1 に使用されている負荷分散方式に影響することはありません。

このコマンドにはライセンスは必要ありません。

例

次に、インターフェイスのイーサネット 1/2 上でパケット単位負荷分散をイネーブルにする例を示します。

```
switch(config)# interface ethernet 1/2  
switch(config-if)# ip load-sharing per-packet
```

関連コマンド

コマンド	説明
ip load-sharing	フロー単位負荷分散アルゴリズムを設定します。
show ip load-sharing	負荷分散型アルゴリズムを表示します。

ip name-server

ネームサーバを設定するには、**ip name-server** 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。

ip name-server *ip-address* [**use-vrf** *name*]

no ip name-server *ip-address* [**use-vrf** *name*]

シンタックスの説明	
ip-address	ネームサーバの IP アドレスを指定します。
use-vrf name	(任意) ネームサーバに到達するために使用する VRF を指定します。名前は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。

デフォルト なし

コマンドモード グローバル コンフィギュレーション
VRF コンテキスト コンフィギュレーション

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン **ip name-server** コマンドは、ネームサーバをデバイス用に設定するために使用します。**vrf context** コマンドは、VRF コンテキスト モードに入って、特定の VRF 用のドメイン名を設定するために使用します。

このコマンドにはライセンスは必要ありません。

例 次に、デフォルト VRF 用の IP ネームサーバを設定する例を示します。

```
switch# config terminal
switch(config)# ip name-server 192.0.2.1
```

次に、管理 VRF 用の IP ネームサーバを設定する例を示します。

```
switch# config terminal
switch(config)# vrf context management
switch(config-vrf)# ip name-server 192.0.2.1
```

次に、IP ネームサーバがデフォルト VRF 経由で到達できなかった場合に管理 VRF をバックアップとして使用するよう、デフォルト VRF 用の IP ネームサーバを設定する例を示します。

```
switch# config terminal  
switch(config)# ip name-server 192.0.2.1 use-vrf management
```

関連コマンド

コマンド	説明
show hosts	IP ドメイン名の設定に関する情報を表示します。

ip next-hop-self eigrp

ルートのアドバタイズ時にネクストホップアドレスとしてローカル IP アドレスを使用するように Enhanced Interior Gateway Routing Protocol (EIGRP) プロセスに指示するには、**next-hop-self eigrp** コマンドを使用します。受信したネクストホップ値を使用するには、このコマンドの **no** 形式を使用します。

ip next-hop-self eigrp *instance-tag*

no ip next-hop-self eigrp *instance-tag*

シンタックスの説明

<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
---------------------	--

デフォルト

EIGRP は常に、IP ネクストホップ値を自身に設定します。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトの設定では、EIGRP は、ルータがルートを学習したインターフェイスと同じインターフェイス上でルートをアドバタイズする場合も、アドバタイズするルートの IP ネクストホップ値としてそれ自身を設定します。このデフォルト設定を変更するには、**no ip next-hop-self eigrp** インターフェイス コンフィギュレーション コマンドを使用して、ルートのアドバタイズ時に受信したネクストホップ値を使用するように EIGRP に指示する必要があります。

例

デフォルトの IP ネクストホップ値を変更し、受信したネクストホップ値を使用するように EIGRP に指示する例を示します。

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-eigrp-af-if)# no ip next-hop-self eigrp 209
```


ip offset-list eigrp

インターフェイスでの Enhanced Interior Gateway Routing Protocol (EIGRP) のオフセットリストを設定するには、**ip offset-list eigrp** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

```
ip offset-list eigrp instance-tag {prefix-list list-name | route-map map-name} {in | out}
offset
```

```
no ip offset-list eigrp instance-tag {prefix-list list-name | route-map map-name} {in | out}
offset
```

シンタックスの説明

<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
prefix-list <i>list-name</i>	EIGRP ルートのフィルタリングに使用する IP プレフィクス リストの名前を指定します。
route-map <i>map-name</i>	EIGRP ルートのフィルタリングに使用するルート マップの名前を指定します。
in	着信ルートにルート ポリシーを適用します。
out	発信ルートにルート ポリシーを適用します。
<i>offset</i>	EIGRP メトリックに追加する値

デフォルト

このコマンドには、デフォルトはありません。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

ip offset-list eigrp コマンドは、インターフェイス上でアダプタイズするルートに影響を与えるために使用します。Cisco NX-OS は、指定されたプレフィクス リストまたはルート マップと一致するすべてのルートに、設定されたオフセット値を追加します。この設定を完了するためには、ルート マップまたはプレフィクス リストの名前を設定する必要があります。

このコマンドには、Enterprise Services ライセンスが必要です。

■ ip offset-list eigrp

例

次の例では、ルート マップ `OffsetFilter` と一致するインターフェイスに着信する EIGRP ルートのメトリックに `20` を追加するように、オフセット リスト フィルタを設定します。

```
switch(config)# router eigrp 209  
switch(config-router)# interface ethernet 2/1  
switch(config-if)# ip offset-list eigrp 209 route-map OffsetFilter in 20
```

関連コマンド

コマンド	説明
<code>prefix-list</code>	プレフィクス リストを設定します。
<code>route-map</code>	ルート マップを設定します。

ip ospf authentication

Open Shortest Path First (OSPF) インターフェイスの認証タイプを指定するには、**ip ospf authentication** コマンドを使用します。インターフェイスの認証タイプを削除するには、このコマンドの **no** 形式を使用します。

ip ospf authentication [**key-chain** *key-name* | **message-digest** | **null**]

no ip ospf authentication

シンタックスの説明

key-chain <i>key-name</i>	(任意) 認証に使用するキー チェーンを指定します。 <i>key-name</i> 引数には、任意の英数字を使用できます。
message-digest	(任意) message-digest 認証を使用するように指定します。
null	(任意) 認証が使用されないように指定します。このキーワードを使用すると、そのエリアに設定されている他の認証すべてが変更されます。

デフォルト

認証は使用されません。

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

サポートされるユーザ ロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

OSPF インターフェイスの認証モードを設定するには、**ip ospf authentication** コマンドを使用します。キーワードを指定せずにこのコマンドを使用する場合は、**ip ospf authentication-key** コマンドでパスワードを設定します。**message-digest** キーワードを使用する場合は、**ip ospf message-digest-key** コマンドでインターフェイスの **message-digest** キーを設定します。

インターフェイスに認証を設定すると、そのエリアに設定した認証が変更されます。

このコマンドには、Enterprise Services ライセンスが必要です。

例

message-digest 認証の設定例を示します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# ip ospf authentication message-digest
switch(config-if)# ip ospf message-digest-key 33 md5 0 mypassword
```

関連コマンド

コマンド	説明
area authentication	OSPF エリアの認証をイネーブルにします。
ip ospf authentication-key	OSPF のパスワード認証を使用しているネイバー ルート用のパスワードを指定します。
ip ospf message-digest-key	OSPF MD5 message-digest キーを設定します。

ip ospf authentication-key

ネイバー Open Shortest Path First (OSPF) ルータに使用される簡易パスワード認証用のパスワードを指定するには、**ip ospf authentication-key** コマンドを使用します。過去に割り当てられた OSPF パスワードを削除するには、このコマンドの **no** 形式を使用します。

ip ospf authentication-key [0 | 3] password

no ip ospf authentication-key

シンタックスの説明

0	非暗号化パスワードを設定します。
3	3DES 暗号化パスワード スtring を設定します。
<i>password</i>	キーボードから入力可能な文字による最大 8 バイトの連続したストリング

デフォルト

非暗号化パスワード

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

サポートされるユーザ ロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

簡易パスワード認証のパスワードを設定するには、**ip ospf authentication-key** コマンドを使用します。このコマンドで作成されたパスワードは、Cisco NX-OS がルーティング プロトコル パケットを開始するときに、OSPF ヘッダーに直接挿入されるキーとして使用されます。インターフェイス単位で各ネットワークに個別のパスワードを指定できます。OSPF 情報を交換できるように、同一ネットワーク上のすべてのネイバー ルータに、同じパスワードを与える必要があります。



(注)

Cisco NX-OS は、**ip ospf authentication** インターフェイス コンフィギュレーション コマンドでインターフェイスの認証をイネーブルにする場合、またはルータ コンフィギュレーション モードの **area authentication** コマンドで認証エリアを設定する場合にこのキーを使用します。

このコマンドには、Enterprise Services ライセンスが必要です。

例

ストリング `yourpass` を使用して非暗号化認証キーを設定する例を示します。

```
switch(config-if)# ip ospf authentication-key yourpass
```

関連コマンド

コマンド	説明
area authentication	OSPF エリアの認証タイプを指定します。
ip ospf authentication	インターフェイスの認証タイプを指定します。

ip ospf cost

インターフェイス上のパケット送信コストを指定するには、**ip ospf cost** コマンドを使用します。パスコストをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

ip ospf cost interface-cost

no ip ospf cost interface-cost

シンタックスの説明

<i>interface-cost</i>	リンクステート メトリックとして表される符号なし整数値。有効範囲は 1 ~ 65535 です。
-----------------------	---

デフォルト

基準帯域幅をインターフェイスの設定帯域幅で除算した値に基づいてコストを計算します。基準帯域幅は設定できますが、デフォルトは 40 Gb/s 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

サポートされるユーザ ロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

各インターフェイスのコスト メトリックを手動で設定するには、**ip ospf cost** コマンドを使用します。このコマンドによって、ルータ コンフィギュレーション モードの **reference-bandwidth** コマンドで設定した参照帯域幅の設定値は無効となります。

このコマンドを使用しない場合、リンク コストは次の式で計算されます。

$$\text{リンク コスト} = \text{基準帯域幅} \div \text{インターフェイス帯域幅}$$

このコマンドには、Enterprise Services ライセンスが必要です。

例

インターフェイス コスト値を 65 に設定する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf cost 65
```

関連コマンド

コマンド	説明
reference-bandwidth	OSPF がリンク コストの算出に使用する参照帯域幅を指定します。

ip ospf dead-interval

ネイバーから少なくとも 1 回 **hello** パケットを受信する必要があるインターバル（このインターバルの間に一度も受信しなかった場合、ルータはそのネイバーがダウン状態であると宣言します）を設定するには、**ip ospf dead-interval** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip ospf dead-interval seconds

no ip ospf dead-interval

シンタックスの説明	<i>seconds</i>	ルータがネイバーから少なくとも 1 つの hello パケットを受信する必要があるインターバル（秒単位）。受信しない場合には、そのネイバールータとの隣接関係がローカル ルータから削除され、ルーティングから除外されます。有効範囲は 1 ~ 65535 です。この値は、ネットワーク上のすべてのノードで一致させる必要があります。
------------------	----------------	---

デフォルト *seconds* のデフォルト値は、**ip ospf hello-interval** コマンドで設定されたインターバルの 4 倍です。

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

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン OSPF を通して **hello** パケットでアドバタイズされるデッド インターバルを設定するには、**ip ospf dead-interval** コマンドを使用します。この値は、特定のネットワーク上の全ネットワークング デバイスに対して同じにする必要があります。

ネイバーのダウンを迅速に検出して、コンバージェンスを向上させるには、デッド インターバルを短くします。デッド インターバルを極端に短くすると、ルーティングが不安定になることがあります。

デッド インターバルと **hello** インターバルを確認するには、**show ip ospf interface** コマンドを使用します。

このコマンドには、Enterprise Services ライセンスが必要です。

例 OSPF デッド インターバルを 20 秒に設定する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf dead-interval 20
```


関連コマンド

コマンド	説明
ip ospf hello-interval	OSPF がインターフェイス上で送信する hello パケットのインターバル
show ip ospf interface	OSPF 関連情報を表示します。

ip ospf hello-interval

OSPF を通してインターフェイス上で送信される hello パケットのインターバルを指定するには、**ip ospf hello-interval** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip ospf hello-interval seconds

no ip ospf hello-interval

シンタックスの説明

seconds インターバルを指定します（秒単位）。この値は、特定のネットワーク上の全デバイスに対して同じにする必要があります。有効範囲は 1 ~ 65535 です。

デフォルト

10 秒

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

OSPF が hello パケットをアドバタイズするレートを設定するには、**ip ospf hello-interval** コマンドを使用します。hello インターバルを短くするほど、OSPF はトポロジの変更を短時間で検出できます。この値は、特定のネットワーク上の全ルータと全アクセス サーバに対して同じにする必要があります。このコマンドには、Enterprise Services ライセンスが必要です。

例

hello パケット間のインターバルを 15 秒に設定する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf hello-interval 15
```

関連コマンド

コマンド	説明
ip ospf dead-interval	ネイバーがルータをダウンしているとして宣言するまでに、hello パケットを 1 つも受信しない時間を設定します。

ip ospf message-digest-key

Open Shortest Path First (OSPF) Message Digest 5 (MD5) 認証をイネーブルにするには、**ip ospf message-digest-key** コマンドを使用します。古い MD5 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。

```
ip ospf message-digest-key key-id md5 [0 | 3] key
```

```
no ip ospf message-digest-key key-id
```

シンタックスの説明

<i>key-id</i>	1 ~ 255 の範囲の識別子
0	(任意) md5 キーを生成するための非暗号化パスワードを指定します。
3	(任意) md5 キーを生成するための暗号化 3DES パスワードを指定します。
キー	最大 16 バイトの英数字パスワード

デフォルト

非暗号化

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

MD5 digest 認証モードを設定する場合は **ip ospf message-digest-key** コマンドを使用します。ネットワーク上のすべてのネイバー ルータで *key* 値を同一にする必要があります。

このコマンドには、Enterprise Services ライセンスが必要です。

例

キー 19、パスワード 8ry4222 を設定する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf message-digest-key 19 md5 8ry4222
```

関連コマンド

コマンド	説明
area authentication	OSPF エリアの認証をイネーブルにします。
ip ospf authentication	インターフェイスの認証タイプを指定します。

ip ospf mtu-ignore

受信 Database Descriptor (DBD) パケットに対する Open Shortest Path First (OSPF) 最大伝送ユニット (maximum transmission unit; MTU) 不一致検出をディセーブルにするには、**ip ospf mtu-ignore** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip ospf mtu-ignore

no ip ospf mtu-ignore

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

OSPF MTU 不一致検出はイネーブルです。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

インターフェイスの MTU 不一致検出をディセーブルにするには、**ip ospf mtu-ignore** コマンドを使用します。デフォルトでは、OSPF は、共通のインターフェイス上でネイバーが同一の MTU を使用しているかどうかをチェックします。着信インターフェイスに設定されている IP MTU よりも受信 MTU が大きい場合、OSPF は隣接関係を確立しません。このチェックをディセーブルにして、OSPF ネイバー間で MTU 値が異なる場合に隣接関係を許可するには、**ip ospf mtu-ignore** コマンドを使用します。

このコマンドには、Enterprise Services ライセンスが必要です。

例

受信 DBD パケットに対する MTU 不一致検出をディセーブルにする例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf mtu-ignore
```

ip ospf network

Open Shortest Path First (OSPF) ネットワーク タイプをインターフェイスのデフォルト以外に設定するには、**ip ospf network** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip ospf network {broadcast | point-to-point}

no ip ospf network

シンタックスの説明

broadcast	ネットワーク タイプをブロードキャストに設定します。
point-to-point	ネットワーク タイプをポイントツーポイントに設定します。

デフォルト

ネットワーク タイプに依存します。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

ネットワーク タイプは OSPF インターフェイスの動作に影響します。通常、OSPF ネットワーク タイプはブロードキャストであり、OSPF マルチキャスト機能を使用します。このネットワーク タイプを使用した場合、代表ルータとバックアップ代表ルータが選出されます。ポイントツーポイント ネットワークの場合、2 つのネイバーしか存在しないのでマルチキャストは不要です。インターフェイス上のルータがネイバーになるには、すべてのネットワーク タイプが一致する必要があります。

このコマンドは、インターフェイス コンフィギュレーション モードの **medium {broadcast | p2p}** コマンドよりも優先されます。

このコマンドには、Enterprise Services ライセンスが必要です。

例

OSPF ネットワークをブロードキャスト ネットワークに設定する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip address 192.0.2.33 255.255.255.0
switch(config-if)# ip ospf network broadcast
```

ip ospf passive-interface

インターフェイスの Open Shortest Path First (OSPF) ルーティング アップデートを停止するには、**ip ospf passive-interface** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip ospf passive-interface

no ip ospf passive-interface

シンタックスの説明 このコマンドには、キーワードと引数はありません。

デフォルト ディセーブル

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

サポートされるユーザロール ネットワーク 管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン インターフェイスが受動インターフェイスとして設定されると、OSPF プロトコルには参加せず、隣接関係の確立もルーティング アップデートの送信も行いません。ただし、インターフェイスはルーティング ネットワークの一部としてアナウンスされます。

このコマンドには、Enterprise Services ライセンスが必要です。

例 インターフェイスを受動に設定する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf passive-interface
```

ip ospf priority

Open Shortest Path First (OSPF) インターフェイスのルータ プライオリティを設定するには、**ip ospf priority** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip ospf priority *number-value*

no ip ospf priority *number-value*

シンタックスの説明	<i>number-value</i>	ルータのプライオリティを指定する数値。指定できる範囲は 0 ~ 255 です。
-----------	---------------------	---

デフォルト	プライオリティ 1
-------	-----------

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
----------	----------------------

サポートされるユーザロール	ネットワーク管理者 VDC 管理者
---------------	----------------------

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン	<p>ルータ プライオリティの設定には、ip ospf priority コマンドを使用します。ルータ プライオリティによって、ネットワークの代表ルータが決まります。ネットワークに 2 台のルータが接続されている場合は、両方が代表ルータになるとうとします。ルータ プライオリティの高いルータが優先します。両方も同じプライオリティの場合、ルータ ID の高いルータが優先します。ルータ プライオリティがゼロに設定されているルータは、代表ルータにもバックアップ代表ルータにもなれません。</p>
------------	--

Cisco NX-OS は、ルータ コンフィギュレーション モードの **neighbor** を使用して、OSPF がブロードキャスト ネットワーク用に設定された場合に、このプライオリティ値を使用します。

このコマンドには、Enterprise Services ライセンスが必要です。

例	ルータ プライオリティ値を 4 に設定する例を示します。
---	------------------------------

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf priority 4
```

■ ip ospf priority

関連コマンド

コマンド	説明
ip ospf network	OSPF ネットワーク タイプをそのメディアのデフォルト以外のタイプに設定します。

ip ospf retransmit-interval

インターフェイスに属している隣接関係の OSPF Link-State Advertisement (LSA; リンクステートアドバタイズメント) の再送信インターバルを指定するには、**ip ospf retransmit-interval** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip ospf retransmit-interval *seconds*

no ip ospf retransmit-interval

シンタックスの説明	<i>seconds</i>	再送信間の時間 (秒単位)。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな値にする必要があります。値の範囲は 1 ~ 65,535 秒です。デフォルトは 5 秒です。
------------------	----------------	---

デフォルト	5 秒
--------------	-----

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
-----------------	----------------------

サポートされるユーザロール	ネットワーク管理者 VDC 管理者
----------------------	----------------------

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン LSA 再送信インターバルを設定するには、**ip ospf retransmit-interval** コマンドを使用します。ルータがネイバーに LSA を送信する場合、ネイバーから Acknowledgement (ACK; 確認応答) メッセージを受信するまでは送信した LSA を保持しています。再送信インターバル以内に ACK を受信しないと、ローカルルータは LSA を再送信します。

このコマンドには、Enterprise Services ライセンスが必要です。

例 次に、再送信インターバルの値を 8 秒に設定する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf retransmit-interval 8
```

ip ospf shutdown

Open Shortest Path First (OSPF) インターフェイスをシャットダウンするには、**ip ospf shutdown** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip ospf shutdown

no ip ospf shutdown

シンタックスの説明 このコマンドには、キーワードと引数はありません。

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

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン インターフェイスの OSPF をシャットダウンするには、**ip ospf shutdown** コマンドを使用します。このコマンドには、Enterprise Services ライセンスが必要です。

例 インターフェイスの OSPF をシャットダウンする例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf shutdown
```

ip ospf transmit-delay

インターフェイスで Open Shortest Path First (OSPF) リンクステート アップデート パケットを送信するために必要と予測される時間を設定するには、**ip ospf transmit-delay** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip ospf transmit-delay *seconds*

no ip ospf transmit-delay

シンタックスの説明	<i>seconds</i>	リンクステート アップデートの送信に必要な時間 (秒)。範囲は 1 ~ 450 秒です。
------------------	----------------	--

デフォルト	1 秒
--------------	-----

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
-----------------	----------------------

サポートされるユーザ ロール	ネットワーク管理者 VDC 管理者
-----------------------	----------------------

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン	LSA アップデート パケットの送信に必要なと予測される時間を設定するには、 ip ospf transmit-delay コマンドを使用します。OSPF は、LSA アップデートを送信する前に遅延時間を送信することによって LSA 経過時間を増分します。この値を設定する場合は、インターフェイスの送信遅延と伝搬遅延を考慮するようにしてください。
-------------------	--

このコマンドには、Enterprise Services ライセンスが必要です。

例	送信遅延値を 8 秒に設定する例を示します。
----------	------------------------

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip ospf transmit-delay 8
```

ip passive-interface eigrp

Enhanced Interior Gateway Routing Protocol (EIGRP) インターフェイスのすべてのルーティングアップデートを停止するには、**ip passive-interface eigrp** コマンドを使用します。ルーティングアップデートの送信を再度イネーブルにするには、このコマンドの **no** 形式を使用します。

ip passive-interface eigrp *instance-tag*

no ip passive-interface eigrp *instance-tag*

シンタックスの説明

instance-tag EIGRP インスタンスの名前。*instance-tag* は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。

デフォルト

インターフェイス上でルーティング アップデートが送信されます。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

ip passive-interface eigrp コマンドは、インターフェイス上のすべてのルーティング更新を停止し、EIGRP 隣接関係の形成を抑制するために使用します。インターフェイスのネットワーク アドレスは、EIGRP トポロジテーブル内に残ります。

このコマンドには、Enterprise Services ライセンスが必要です。

例

次に、インターフェイス Ethernet 2/1 上の EIGRP ルーティング アップデートを停止する例を示します。

```
switch(config)# router eigrp 201
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip passive-interface eigrp 201
```

ip policy route-map

インターフェイスでのポリシー ルーティングに使用するルート マップを特定するには、**ip policy route-map** コマンドを使用します。ルート マップを削除するには、このコマンドの **no** 形式を使用します。

ip policy route-map *name*

no ip policy route-map [*name*]

シンタックスの説明

name ルート マップ名。名前は、63 文字以下の任意の英数字文字列にできます。

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

サポートされるユーザ ロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

ポリシー ルーティングに使用するルート マップを特定するには、**ip policy route-map** コマンドを使用します。ルート マップを作成するには、**route-map** コマンドを使用します。**route-map** コマンドごとに、それに関連した **match** および **set** コマンドのリストがあります。**match** コマンドでは、パケットの宛先 IP アドレスに基づいて、一致基準（そのインターフェイスにポリシー ルーティングが許可される条件）を指定します。**set** コマンドでは、**set** 処理（**match** コマンドによる基準が満たされた場合に実行する特定のポリシー ルーティング処理）を指定します。**no ip policy route-map** コマンドは、ルート マップへのポインタを削除します。

match ip address コマンドを使用し、拡張 IP アクセス リストを参照する場合、拡張 IP アクセス リストに定義可能なあらゆる一致基準でポリシーベース ルーティングを実行できます。

ip policy route-map コマンドを使用する前に、**feature pbr** コマンドでポリシーベース ルーティングをイネーブルにする必要があります。

このコマンドには、Enterprise Services ライセンスが必要です。

例

次に、インターフェイスにポリシーベース ルート マップを設定する例を示します。

```
switch# configure terminal
switch(config)# feature pbr
switch(config)# interface ethernet 2/1
switch(config-if)# ip policy route-map policymap
```

関連コマンド

コマンド	説明
feature pbr	ポリシーベース ルーティング機能をイネーブルにします。
route-map	ルート マップを作成します。
show route-map pbr-statistics	ポリシーベース ルート マップについての統計情報を表示します。

ip port-unreachable

ICMP ポート到達不能メッセージの生成をイネーブルにするには、**ip port-unreachable** 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。

ip port-unreachable

no ip port-unreachable

シンタックスの説明 このコマンドには、キーワードと引数はありません。

デフォルト イネーブル

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

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン このコマンドにはライセンスは必要ありません。

例 次に、必要に応じて、インターフェイス上の ICMP ポート到達不能メッセージの生成をイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# ip port-unreachable
```

関連コマンド	コマンド	説明
	ip unreachable	ICMP 到達不能メッセージを送信します。

ip prefix-list

IP パケットまたはルートを照合するプレフィクス リストを作成するには、**ip prefix-list** コマンドを使用します。プレフィクス リストを削除するには、このコマンドの **no** 形式を使用します。

ip prefix-list name [seq number] {permit | deny} prefix [eq length | [ge length] [le length]]

no prefix-list name [seq number] {permit | deny} prefix [eq length | [ge length] [le length]]

シンタックスの説明

<i>name</i>	IP プレフィクス リストの名前。名前は、63 文字以下の任意の英数字文字列にできます。
<i>seq number</i>	(任意) プレフィクス リストのエントリの順序を示すシーケンス番号。範囲は 1 ~ 4294967294 です。
permit	プレフィクス リストと一致するルートまたは IP パケットを許可します。
deny	プレフィクス リストと一致するルートまたは IP パケットを拒否します。
<i>prefix</i>	A.B.C.D/length の形式の IP プレフィクス
<i>eq length</i>	(任意) 照合するプレフィクスの長さ (完全一致)。範囲は 1 ~ 32 です。
<i>ge length</i>	(任意) 照合するプレフィクス長の最大値。範囲は 1 ~ 32 です。
<i>le length</i>	(任意) 照合するプレフィクス長の最小値。範囲は 1 ~ 32 です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

IP プレフィクス フィルタリングを設定するには、**ip prefix-list** コマンドを使用します。**permit** または **deny** のキーワードを指定してプレフィクス リストを設定し、一致条件に基づいてプレフィクスを許可または拒否します。プレフィクス リストは、IP アドレスとビット マスクで構成されています。ビット マスクは、1 ~ 32 の数値として入力されます。どのプレフィクス リストのエントリとも一致しないトラフィックに暗黙拒否が適用されます。

プレフィクス リストは、完全一致方式で指定のプレフィクス長と照合するように設定することも、またプレフィクス範囲と照合するように設定することもできます。**ge** と **le** のキーワードを使用して照合するプレフィクス長の範囲を指定することにより、**network/length** 引数だけを指定するよりも柔軟な設定が可能となります。**ge** と **le** のいずれのキーワードも設定しない場合、Cisco NX-OS は完全一致方式

でプレフィクス リストを処理します。 **ge ge-length** と **le le-length** の両方のキーワードと引数を設定した場合、許可されるプレフィクス長の範囲は **ge-length** 引数と **le-length** 引数の間になります。この動作は、次の式で表すことができます。

$$\text{ネットワーク/長さ} < \text{ge ge-length} < \text{le le-length} \leq 32$$

シーケンス番号を設定しないと、Cisco NX-OS によって、プレフィクス リスト エントリにデフォルトのシーケンス番号である 5 が適用され、後続のプレフィクス リスト エントリのシーケンス番号は 5 ずつ増分されます (5、10、15 など)。最初のプレフィクス リスト エントリのシーケンス番号を設定し、後続のエントリにシーケンス番号を設定しないと、Cisco NX-OS によって、後続のエントリのシーケンス番号は 5 ずつ増分されます (たとえば、最初に設定したシーケンス番号が 3 の場合、後続のエントリは、8、13、18 のように増分されます)。デフォルトのシーケンス番号の適用を停止するには、**seq** キーワードを指定して、このコマンドの **no** 形式を使用します。

Cisco NX-OS は、シーケンス番号が最も小さいエントリからプレフィクス リストの評価を開始し、一致するものが見つかるまで順番に評価していきます。ネットワークに該当するような一致が見つかったら、そのネットワークに **permit** または **deny** 文が適用され、リストの残りは評価されません。



最も処理される頻度の高いプレフィクス リスト文のシーケンス番号を最小にすれば、最良のパフォーマンスを得ることができます。 **seq number** のキーワードと引数はリシーケンスに使用できます。

ネイバー アドレスファミリ モードで **prefix-list** コマンドを入力すると、特定のピアのインバウンドまたはアウトバウンドのアップデートにプレフィクス リストを適用できます。プレフィクス リストの情報とカウンタは、**show ip prefix-list** コマンドの出力に表示されます。 **prefix-list** カウンタをリセットするには、**clear ip prefix-list** コマンドを入力します。

このコマンドにはライセンスは必要ありません。

例

プレフィクス リストを設定し、BGP ピアに適用する例を示します。

```
switch# config t
switch(config)# ip prefix-list allowprefix 10 permit 192.0.2.0 eq 24
switch(config)# ip prefix-list allowprefix 20 permit 209.165.201.0 eq 27
switch(config) router bgp 65536:20
switch(config-router)# neighbor 192.0.2.1/16 remote-as 65536:20
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# prefix-list allowprefix in
```

関連コマンド

コマンド	説明
clear ip prefix-list	IP プレフィクス リストのカウンタをクリアします。
prefix-list	BGP ピアにプレフィクス リストを適用します。
show ip prefix-list	IP プレフィクス リストについての情報を表示します。

ip prefix-list description

IP プレフィクス リストを説明する文字列を設定するには、**ip prefix-list description** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip prefix-list name description string

no ip prefix-list name description

シンタックスの説明	パラメータ	説明
	<i>name</i>	プレフィクス リストの名前。名前は、63 文字以下の任意の英数字文字列にできます。
	<i>string</i>	プレフィクス リストを説明する文字列。最大 90 文字の英数字を使用できます。

デフォルト なし

コマンド モード グローバル コンフィギュレーション

サポートされるユーザ ロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン このコマンドにはライセンスは必要ありません。

例 IP プレフィクス リストの説明の設定例を示します。

```
switch# configure terminal
switch(config)# ip prefix-list test1 description "this is a test"
```

関連コマンド	コマンド	説明
	ip prefix-list	IPv6 プレフィクス リストを作成します。
	show ip prefix-list	IPv6 プレフィクス リストについての情報を表示します。

ip proxy-arp

インターフェイス上でプロキシ ARP をイネーブルにするには、**ip proxy-arp** コマンドを使用します。インターフェイス上でプロキシ ARP 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 proxy-arp

no ip proxy-arp

シンタックスの説明 このコマンドには、キーワードと引数はありません。

デフォルト イネーブル

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

サポートされるユーザ ロール ネットワーク 管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン このコマンドにはライセンスは必要ありません。

例 次に、プロキシ ARPt をイネーブルにする例を示します。

```
RIP Version 2 パケットの認証をイネーブルにして、インターフェイス上で使用可能なキー セットを指定するには、インターフェイス コンフィギュレーション モードで switch(config)# interface ethernet 2/1  
switch(config-if)# ip proxy-arp
```

ip rip authentication key-chain

ip rip authentication key-chain コマンドを使用します。認証を禁止するには、このコマンドの **no** 形式を使用します。

ip rip authentication key-chain *name-of-chain*

no ip rip authentication key-chain [*name-of-chain*]

シンタックスの説明

name-of-chain 有効なキー グループを指定します。

デフォルト

RIP パケットには認証は適用されません。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

インターフェイスに対する認証設定を完了するには、**key-chain** コマンドを使用して、別途キー チェーンを設定する必要があります。

このコマンドにはライセンスは必要ありません。

例

キーチェーン ツリーに属しているキーの受け入れと送信をインターフェイスに設定する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip rip authentication key-chain trees
```

関連コマンド

コマンド	説明
key-chain	認証方式で使用可能なキー セットを作成します。

ip rip authentication mode

Routing Information Protocol (RIP) Version 2 パケットに使用される認証タイプを指定するには、インターフェイス コンフィギュレーション モードで、**ip rip authentication mode** コマンドを使用します。クリア テキスト認証に戻すには、このコマンドの **no** 形式を使用します。

ip rip authentication mode {text | md5}

no ip rip authentication mode

シンタックスの説明

text	クリア テキスト認証を指定します。
md5	Message Digest 5 (MD5) 認証を指定します。

デフォルト

キー チェーンを設定した場合、RIP パケットにクリア テキスト認証が適用されます。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

RIPng for IPv6 には、IPv6 に組み込まれた認証が使用されます。
このコマンドにはライセンスは必要ありません。

例

インターフェイスに使用される認証方式を MD5 に設定する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip rip authentication mode md5
```

関連コマンド

コマンド	説明
ip rip authentication key-chain	RIP Version 2 パケットの認証をイネーブルにして、インターフェイスに使用可能なキー セットを指定します。
key chain	ルーティング プロトコルの認証をイネーブルにします。

ip rip metric-offset

インターフェイスの着信 IP Routing Information Protocol (RIP) ルート メトリックに追加値を設定するには、インターフェイス コンフィギュレーション モードで **ip rip metric-offset** コマンドを使用します。メトリック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。

ip rip metric-offset value

no ip rip metric-offset

シンタックスの説明

<i>value</i>	インターフェイスの着信ルート メトリックに追加する値。範囲は 1 ~ 15 です。デフォルトは 1 です。
--------------	---

デフォルト

value : 1

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

ip route metric-offset コマンドは、Cisco NX-OS が使用するルートに影響を与えます。このコマンドを使用すると、インターフェイス上の全着信ルートのルート メトリックに固定オフセットを追加できます。あるインターフェイスの **metric-offset** を 5 に設定し、着信ルート メトリックが 5 の場合、Cisco NX-OS はそのルート テーブルにメトリック 10 のルートを追加します。

このコマンドにはライセンスは必要ありません。

例

インターフェイス Ethernet 2/1 のすべての着信 RIP ルートにメトリック オフセット 10 を設定する例を示します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# ip rip metric-offset 10
```

関連コマンド

コマンド	説明
ip rip offset-list	着信 RIP ルート メトリックにオフセット値を追加します。

ip rip offset-list

Routing Information Protocol (RIP) を通じて学習されたルートの着信および発信メトリックにオフセットを追加するには、インターフェイス コンフィギュレーション モードで **ip rip offset-list** コマンドを使用します。オフセットリストを削除するには、このコマンドの **no** 形式を使用します。

ip rip offset-list value

no ip rip offset-list

シンタックスの説明

<i>value</i>	インターフェイスの着信ルートメトリックに追加する値。範囲は 1 ~ 15 です。デフォルトは 1 です。
--------------	--

デフォルト

value : 1

コマンドモード

ルータ アドレスファミリ コンフィギュレーション

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにはライセンスは必要ありません。

例

インターフェイス Ethernet 2/1 のすべての着信 RIP ルートにオフセット 10 を設定する例を示します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# ip rip offset-list 10
```

関連コマンド

コマンド	説明
ip rip metric-offset	着信 RIP ルートメトリックにオフセット値を追加します。

ip rip passive-interface

インターフェイスでの Routing Information Protocol (RIP) アップデートの送信を停止するには、インターフェイス コンフィギュレーション モードで **ip rip passive-interface** コマンドを使用します。アップデートの停止を解除するには、このコマンドの **no** 形式を使用します。

ip rip passive-interface

no ip rip passive-interface

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト インターフェイス上で RIP アップデートが送信されます。

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

サポートされるユーザロール ネットワーク 管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン RIP によって、受動インターフェイス上のマルチキャスト（またはブロードキャスト）アドレスに対するルーティング アップデートの送信は停止されますが、そのインターフェイス上のネイバーからのルーティング アップデートの受信および処理は続行されます。

このコマンドにはライセンスは必要ありません。

例 イーサネット 1/2 を受動インターフェイスとして設定する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip rip passive-interface
```


ip rip poison-reverse

Routing Information Protocol (RIP) ルータ アップデートのポイズン リバースをイネーブルにするには、インターフェイス コンフィギュレーション モードで **ip rip poison-reverse** コマンドを使用します。RIP アップデートのポイズン リバース処理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 rip poison-reverse

no ip rip poison-reverse

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

スプリット ホライズンは常にイネーブルです。ポイズン リバース処理はディセーブルです。

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

サポートされるユーザ ロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

RIP ルータ アップデートのポイズン リバース処理をイネーブルにするには、**ip rip poison-reverse** コマンドを使用します。デフォルトでは、Cisco NX-OS は、RIP ルートを学習したインターフェイスからの RIP ルートのアドバタイズは行いません (スプリット ホライズン)。ポイズン リバースとスプリット ホライズンを両方とも設定した場合、Cisco NX-OS はルートを学習したインターフェイスを通じて、その学習ルートは到達不能であるとアドバタイズします。

このコマンドにはライセンスは必要ありません。

例

RIP を実行するインターフェイスのポイズン リバース処理をイネーブルにする例を示します。

```
switch(config)# interface ethernet 1/2  
switch(config-if)# ip rip poison-reverse
```

ip rip route-filter

インターフェイスの着信または発信 Routing Information Protocol (RIP) ルートをフィルタリングするには、インターフェイス コンフィギュレーション モードで **route-filter** コマンドを使用します。インターフェイスからフィルタリ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。

ip rip route filter {**prefix-list** *list-name* | **route-map** *map-name*} {**in** | **out**}

シンタックスの説明

prefix-list <i>list-name</i>	RIP パケット フィルタリング用のプレフィクス リストを関連付けます。
route-map <i>map-name</i>	ルート マップを関連付けて RIP の再配布ポリシーを設定します。
in	着信ルートをフィルタリングします。
out	発信ルートをフィルタリングします。

デフォルト

ルート フィルタリングはディセーブルです。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

インターフェイスの着信ルートまたは発信ルートをフィルタリングするには、**ip rip route-filter** コマンドを使用します。

このコマンドにはライセンスは必要ありません。

例

RIP インターフェイスのルート フィルタリングにルート マップを使用する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip rip route-filter route-map InRipFilter in
```

関連コマンド

コマンド	説明
route-map	ルート マップを作成します。
prefix-list	プレフィクス リストを作成します。

ip rip summary-address

Routing Information Protocol (RIP) インターフェイスにおけるサマリー集約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 rip summary-address** コマンドを使用します。特定のアドレスまたはサブネットの集約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 rip summary-address ip-prefix/mask
```

```
no ip rip summary-address ip-prefix/mask
```

シンタックスの説明

<i>ip-prefix/length</i>	集約する IP プレフィクスおよびプレフィクス長
-------------------------	--------------------------

デフォルト

デフォルトでは、ディセーブルです。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

特定のインターフェイスのアドレスまたはサブネットを集約するには、**ip rip summary-address** コマンドを使用します。

このコマンドにはライセンスは必要ありません。

例

次の例では、サマリー アドレス 192.0.2.0 がインターフェイス Ethernet 1/2 からアドバタイズされます。

```
switch(config)# interface ethernet 1/2  
switch(config-if)# ip summary-address rip 192.0.2.0/24
```

ip route

スタティック ルートを設定するには、**ip route** コマンドを使用します。スタティック ルートを削除するには、このコマンドの **no** 形式を使用します。

```
ip route ip-prefix/mask {[interface] next-hop} [preference] [tag id]
```

```
no ip route ip-prefix/mask {[interface] next-hop}} [preference] [tag id]
```

シンタックスの説明

<i>ip-prefix/length</i>	IP プレフィックスとプレフィックス長。形式は <i>x.x.x.x/length</i> です。length は 1 ~ 32 です。
<i>interface</i>	(任意) このルートに到達するためにすべてのパケットが送信されるインターフェイス。? を使用して サポートされているインターフェイスのリストを表示します。
<i>next-hop</i>	ネットワークに到達するために使用可能なネクストホップの IP アドレス。IP アドレス、インターフェイス タイプ、およびインターフェイス番号を指定できます。形式は <i>x.x.x.x/length</i> です。length は 1 ~ 32 です。
<i>preference</i>	(任意) このルートまでの管理ディスタンスとして使用されるルートプリファレンスを設定します。範囲は 1 ~ 255 です。デフォルトは 1 です。
tag id	(任意) ルート マップ内の照合に使用可能なルート タグを割り当てます。範囲は 0 ~ 4294967295 です。デフォルトは 0 です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

スタティック ルートのデフォルト管理ディスタンスは 1 です。ダイナミック ルーティング プロトコルをスタティック ルートよりも優先させたい場合は、スタティック ルート プリファレンス引数をダイナミック ルーティング プロトコルの管理ディスタンスよりも大きい値に設定する必要があります。たとえば、EIGRP を使用して抽出されたルートのデフォルト管理ディスタンスが 100 とします。スタティック ルートよりも EIGRP ダイナミック ルートを優先する場合は、100 を超える管理ディスタンスを指定します。

このコマンドにはライセンスは必要ありません。

例

次に、ネクストホップ アドレス 10.0.0.2 を通して到達可能な IP アドレス プレフィックスが 192.168.1.1/32 の宛先用のスタティック ルートを作成する例を示します。

```
switch(config)# ip route 192.168.1.1/32 10.0.0.2
```

この例では、以前の例にタグを割り当てて、このスタティック ルート上で照合可能なルート マップを設定できるようにします。

```
switch(config)# ip route 192.168.1.1/32 10.0.0.2 tag 5
```

この例では、110 のプリファレンスを選択します。この場合は、管理ディスタンスが 110 未満のダイナミック ルート情報が入手できなければ、プレフィックスが 10.0.0.0 のパケットが 172.31.3.4 にあるルータに転送されます。

```
ip route 10.0.0.0/8 172.31.3.4 110
```

関連コマンド

コマンド	説明
ipv6 route	IPv6 スタティック ルートを設定します。
match tag	ルートに関連付けられたタグ値を照合します。

ip router eigrp

インターフェイス用の EIGRP インスタンスを指定するには、**ip router eigrp** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip router eigrp *instance-tag*

no ip router eigrp *instance-tag*

シンタックスの説明

<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
---------------------	--

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

ip router eigrp コマンドは、インターフェイス用の EIGRP インスタンスを指定するために使用します。このコマンドには、Enterprise Services ライセンスが必要です。

例

次に、インターフェイス用の EIGRP インスタンスを設定する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip router eigrp Base
```

ip router ospf area

インターフェイスの Open Shortest Path First (OSPF) インスタンスとエリアを設定するには、**ip router ospf area** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip router ospf instance-tag area area-id [secondaries none]

no ip router ospf instance-tag area area-id [secondaries none]

シンタックスの説明	
<i>instance-tag</i>	インスタンス タグ。英数字文字列で指定します。
<i>area-id</i>	認証をイネーブルにする OSPF エリアの識別子。正の整数値または IP アドレスを指定します。
secondaries none	(任意) セカンダリ IP アドレスを除外します。

デフォルト 10 秒

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

サポートされるユーザ ロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン インターフェイスのエリアおよび OSPF インスタンスを指定するには、**ip router ospf area** コマンドを使用します。

このコマンドには、Enterprise Services ライセンスが必要です。

例 次に、OSPF 用のインターフェイスを設定する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip router ospf Base area 33
```

ip router ospf multi-area

OSPF インターフェイス上で複数エリア隣接関係を設定するには、**ip router ospf multi-area** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ip router ospf instance-tag multi-area area-id

no ip router ospf instance-tag multi-area area-id

シンタックスの説明

<i>instance-tag</i>	インスタンス タグ。大文字と小文字が区別される 63 文字以下の英数字文字列として指定します。
<i>area-id</i>	プライマリ インターフェイスに別のエリアとして追加する OSPF エリアに関する識別情報。正の整数値または IP アドレスを指定します。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.2(1)	このコマンドが追加されました。

使用上のガイドライン

ip router ospf multi-area コマンドは、OSPF インターフェイス上の追加エリアを指定するために使用します。

このコマンドには、Enterprise Services ライセンスが必要です。

例

次に、複数エリア隣接関係を設定する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip router ospf Base area 33
switch(config-if)# ip router ospf Base multi-area 99
```


ip source-route

送信元ルーティング ヘッダー オプションを使用して IP データグラムを処理するには、**ip source-route** コマンドを使用します。source-route オプションを含む IP データグラムをソフトウェアで破棄させるには、このコマンドの **no** 形式を使用します。

ip source-route

no ip source-route

シンタックスの説明 このコマンドには、キーワードと引数はありません。

デフォルト イネーブル

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

サポートされるユーザ ロール ネットワーク 管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン このコマンドにはライセンスは必要ありません。

例 次に、送信元ルーティング ヘッダー オプションを使用した IP データグラム処理をイネーブルにする例を示します。

```
switch# config t  
switch(config)# interface ethernet 2/1  
switch(config-if)# ip source-route
```

ip split-horizon eigrp

Enhanced Interior Gateway Routing Protocol (EIGRP) プロセスのスプリット ホライズンをイネーブルにするには、**ip split-horizon eigrp** コマンドを使用します。スプリット ホライズン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 split-horizon eigrp *instance-tag*

no ip split-horizon eigrp *instance-tag*

シンタックスの説明

<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
---------------------	--

デフォルト

イネーブル

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

インターフェイスのスプリット ホライズンをディセーブルにするには、**no ip split-horizon eigrp** コマンドを使用します。

このコマンドには、Enterprise Services ライセンスが必要です。

例

イーサネットリンクのスプリット ホライズンをディセーブルにする例を示します。

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-eigrp-af-if)# no ip split-horizon eigrp 209
```

ip summary-address eigrp

指定の Enhanced Interior Gateway Routing Protocol (EIGRP) インターフェイスのサマリー集約アドレスを設定するには、**ip summary-address eigrp** コマンドを使用します。設定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 summary-address eigrp instance-tag {ip-address /length | ip-address mask}
[admin-distance]
```

```
no ip summary-address eigrp instance-tag {ip-address /length | ip-address mask}
```

シンタックスの説明

<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
<i>ip-address/length</i>	インターフェイスに適用するサマリー IP プレフィクスとプレフィクス長 (4 分割ドット付き 10 進表記)。たとえば、/8 は、IP プレフィクスの最初の 8 ビットがネットワーク ビットであることを示します。 <i>length</i> を使用する場合、スラッシュが必要です。
<i>ip-address</i>	インターフェイスに適用するサマリー IP アドレス (4 分割ドット付き 10 進表記)。
<i>mask</i>	IP アドレス マスク
<i>admin-distance</i>	(任意) 管理ディスタンス。範囲は 1 ~ 255 です。

デフォルト

EIGRP サマリー ルートには、管理ディスタンス 5 が適用されます。事前設定されるサマリー アドレスはありません。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

インターフェイス レベルのアドレス集約を設定するには、**ip summary-address eigrp** コマンドを使用します。EIGRP サマリー ルートの管理ディスタンスは 5 です。このコマンドには、Enterprise Services ライセンスが必要です。

例

EIGRP インターフェイスの 192.168.0.0/16 サマリー アドレスに管理ディスタンス 95 を設定する例を示します。

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ip summary-address eigrp 209 192.168.0.0/16 95
```

ip tcp path-mtu-discovery

IPv4 または IPv6 インターフェイス上のパス MTU ディスカバリをイネーブルにするには、**ip tcp path-mtu discovery** 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。

ip ip tcp path-mtu discovery

no ip tcp path-mtu discovery

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト ディセーブル

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

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。
	5.0(2)	IPv6 パス MTU ディスカバリのサポートが追加されました。

使用上のガイドライン このコマンドにはライセンスは必要ありません。

例 次に、IPv4 と IPv6 の両方に対してパス MTU ディスカバリをイネーブルにする例を示します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# ip tcp path-mtu-discovery
```

ip wccp

サービス グループ内の Web Cache Communication Protocol (WCCP) サービスをイネーブルにするには、**ip wccp** コマンドを使用します。サービス グループ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 wccp {service-number | web-cache} [mode {open [redirect-list access-list] | closed
service-list service-access-list}] [password [0-7] password]
```

```
no ip wccp {service-number | web-cache} [mode {open [redirect-list access-list] | closed
service-list service-access-list}] [password [0-7] password]
```

シンタックスの説明

<i>service-number</i>	ダイナミック サービス識別情報。 <i>service-number</i> の範囲は 1 ~ 255 です。
web-cache	既知の Web キャッシュ サービスを指定します。
mode	(任意) ローカルルートまたは直接ルートのルート タグ値を設定します。
新しいウィンドウで	サービスを開いていると見なします。
closed service-list <i>service-access-list</i>	サービスを閉じていると見なします。サービス リストは、サービスと一致するパケットが定義された名前付き IP アクセス リストを示します。 <i>service-access-list</i> は、大文字と小文字が区別される 64 文字以下の任意の英数字文字列にできます。
redirect-list <i>access-list</i>	(任意) このサービス グループにリダイレクトされるトラフィックを制御するアクセス リストを指定します。 <i>access-list</i> は、大文字と小文字が区別される 64 文字以下の任意の英数字文字列にできます。
password [0-7]	(任意) サービス グループから受信されたメッセージに対する MD5 認証を設定します。WCCP は、認証で受け入れられなかったメッセージを破棄します。暗号化タイプは 0 ~ 7 の任意の値 (包含的) にできます。ここで、0 は暗号化されないことを、7 は独自の暗号化を示します。
<i>password</i>	MD5 パスワード。 <i>password</i> は、大文字と小文字が区別される 8 文字以下の任意の英数字文字列にできます。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション
VRF コンフィギュレーション

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.2(1)	このコマンドが追加されました。

使用上のガイドライン

redirect-list キーワードは、サービス グループのキャッシュ エンジンにリダイレクトされるトラフィックを制御するアクセス リストを使用するようにルータに指示します。*access list* は、リダイレクトが許可されたトラフィックを識別します。デフォルトは TCP トラフィックのリダイレクトです。

service-list キーワードは閉じられたモード サービスにのみ使用します。WCCP サービスが閉じられている場合は、WCCP が、トラフィックを受信するためのクライアント アプリケーションが登録されていないパケットを破棄します。**service-list** キーワードと *service-access-list* 引数は、アプリケーション プロトコル タイプまたはポート番号を登録するために使用します。

パスワードは 7 文字以下の文字列にできます。パスワードを指定した場合は、認証で受け入れられなかったメッセージが破棄されます。パスワード名と HMAC MD5 値を組み合わせて、ルータとキャッシュ エンジン間の安全な接続が構築されます。

password 0 *pwstring* は、パスワードをクリア テキストで保存するために使用します。**password 7** *pwstring* は、パスワードを暗号化形式で保存するために使用します。すでに暗号化されたパスワードに対して **password 7** キーワードを使用できます。



(注)

ip wccp コマンドには必要なすべてのパラメータを指定する必要があります。**ip wccp** コマンドの入力によって、過去の設定が上書きされます。

このコマンドにはライセンスは必要ありません。

例

次に、宛先が 10.168.196.51 以外の Web 関連パケットを Web キャッシュにリダイレクトするようにルータを設定する例を示します。

```
switch(config)# access-list 100
switch(config-acl)# permit ip any any
switch(config-acl)# exit
switch(config)# ip wccp web-cache redirect-list 100
switch(config)# interface ethernet 2/1
switch(config-if)# ip wccp web-cache redirect out
```

次に、閉じられた WCCP サービスを設定する例を示します。

```
switch(config)# ip wccp 99 service-list access1 mode closed
```

関連コマンド

コマンド	説明
feature wccp	WCCP 機能をイネーブルにします。
show ip wccp	WCCP サービス グループのステータスを表示します。

ip wccp redirect

WCCP を使用してアウトバウンドまたはインバウンド インターフェイス上でパケットをリダイレクトするには、**ip wccp redirect** コマンドを使用します。WCCP リダイレクション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 wccp {service-number | web-cache} redirect {in | out}
```

```
no ip wccp {service-number | web-cache} redirect {in | out}
```

シンタックスの説明

service-number	ダイナミック サービス識別情報。 <i>service-number</i> の範囲は 1 ~ 255 です。
web-cache	既知の Web キャッシュ サービスを指定します。
in	インバウンド インターフェイス上でパケットをリダイレクトします。
out	アウトバウンド インターフェイス上でパケットをリダイレクトします。

デフォルト

ディセーブル

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.2(1)	このコマンドが追加されました。

使用上のガイドライン

WCCPv2 は、レイヤ 3 サブインターフェイス、VLAN インターフェイス、レイヤ 3、およびポートチャネルを含むレイヤ 3 インターフェイス上でのみサポートされます。

ip wccp redirect in コマンドは、インバウンド ネットワーク トラフィックを受信するインターフェイス上の WCCP リダイレクションを設定するために使用します。インターフェイス上でコマンドを設定すると、そのインターフェイスに到着したすべてのパケットが、指定された WCCP サービスで定義された基準に照らして比較されます。パケットが基準を満たしていれば、リダイレクトされます。

ip wccp redirect out コマンドは、アウトバウンド インターフェイス上の WCCP リダイレクションチェックを設定するために使用します。

サービス グループを設定するときにリダイレクト リストを含めることもできます。リダイレクト リストを使用すれば、NAT (送信元) IP アドレスを含むパケットを拒否して、リダイレクションを阻止できます。リダイレクト リストとサービス グループの設定方法については、**ip wccp** コマンドを参照してください。

キャッシュ エンジンからのすべてのパケットのリダイレクションを阻止するには、キャッシュ エンジンに相対するルータ インターフェイス上で **ip wccp redirect exclude in** コマンドを使用します。



(注)

同じインターフェイス上で **ip wccp redirect {in | out}** コマンドと **ip wccp redirect exclude in** コマンドを使用しないでください。**ip wccp redirect exclude in** コマンドは、**ip wccp redirect {in | out}** コマンドよりも優先されます。

このコマンドにはライセンスは必要ありません。

例

次に、WCCP がイーサネット インターフェイス 2/2 上で発信パケットをキャッシュ エンジンにリダイレクトするセッションを設定する例を示します。

```
switch(config)# ip wccp 99
switch(config)# interface ethernet 2/2
switch(config-if)# ip wccp 99 redirect out
```

次に、イーサネット インターフェイス 2/1 上に到着した HTTP トラフィックがキャッシュ エンジンにリダイレクトされるセッションを設定する例を示します。

```
switch(config)# ip wccp web-cache
switch(config)# interface ethernet 0/1
switch(config-if)# ip wccp web-cache redirect in
```

関連コマンド

コマンド	説明
feature wccp	WCCP 機能をイネーブルにします。
ip wccp redirect exclude in	インターフェイス上の WCCP リダイレクションを除外します。
show ip wccp	WCCP サービス グループのステータスを表示します。

ip wccp redirect exclude in

WCCP リダイレクション チェックからインターフェイス上のインバウンド パケットを除外するには、**ip wccp redirect exclude in** コマンドを使用します。リダイレクション チェックからパケットを除外するためのルータ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。

ip wccp redirect exclude in

no ip wccp redirect exclude in

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

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

サポートされるユーザ ロール

ネットワーク 管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.2(1)	このコマンドが追加されました。

使用上のガイドライン

ip wccp redirect exclude in コマンドは、アウトバウンド インターフェイスで発生する可能性のある任意のリダイレクション チェックからインターフェイス上のインバウンド パケットを除外するために使用します。このコマンドは、すべてのサービスに影響を与えるため、リダイレクションから除外するインバウンド インターフェイスにのみ適用する必要があります。



(注)

同じインターフェイス上で **ip wccp redirect {in | out}** コマンドと **ip wccp redirect exclude in** コマンドを使用しないでください。**ip wccp redirect exclude in** コマンドは、**ip wccp redirect {in | out}** コマンドよりも優先されます。

このコマンドにはライセンスは必要ありません。

例

次に、すべての WCCP リダイレクション チェックからイーサネット インターフェイス 2/1 に到着したパケットを除外する例を示します。

```
switch(config)# interface ethernet 2/2  
switch(config-if)# ip wccp redirect exclude in
```

関連コマンド

コマンド	説明
feature wccp	WCCP 機能をイネーブルにします。
ip wccp redirect	インターフェイス上の WCCP リダイレクションを設定します。
show ip wccp	WCCP サービス グループのステータスを表示します。

ip unreachable

ICMP 到達不能メッセージの生成をイネーブルにするには、**ip unreachable** 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。

ip unreachable

no ip unreachable

シンタックスの説明

このコマンドには、キーワードと引数はありません。

デフォルト

イネーブル

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにはライセンスは必要ありません。

例

次に、必要に応じて、インターフェイス上の ICMP 到達不能メッセージの生成をイネーブルにする例を示します。

```
switch# config t  
switch(config)# interface ethernet 2/1  
switch(config-if)# ip unreachable
```

関連コマンド

コマンド	説明
ip port-unreachable	ICMP ポート到達不能メッセージを送信します。

ipv6 address

インターフェイスに IPv6 アドレスを設定するには、**ipv6 address** 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。

```
ipv6 address {addr [eui64] [route-preference preference] [secondary] tag tag-id] |
use-link-local-only}
```

```
no ipv6 address {addr [eui64] [route-preference preference] [secondary] [tag tag-id] |
use-link-local-only}
```

シンタックスの説明	addr	IPv6 アドレス。形式は A:B::C:D/length です。length の範囲は 1 ~ 128 です。
	eui64	(任意) アドレスの下位 64 ビットに Extended Unique Identifier (EUI64) を設定します。
	route-preference preference	(任意) ローカル ルートまたは直接ルートのルート プリファレンスを設定します。指定できる範囲は 0 ~ 255 です。
	secondary	(任意) セカンダリ IPv6 アドレスを作成します。
	tag tag-id	(任意) ローカル ルートまたは直接ルートのルート タグ値を設定します。

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

サポートされるユーザ ロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。
	4.0(3)	tag キーワードが追加されました。

使用上のガイドライン インターフェイスに IPv6 のアドレスまたはセカンダリ アドレスを設定するには、**ipv6 address** コマンドを使用します。

このコマンドにはライセンスは必要ありません。

例 IPv6 アドレスの設定例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 address 2001:0DB8::3/48
```

関連コマンド

コマンド	説明
<code>ip address</code>	インターフェイスに IPv4 アドレスを設定します。

ipv6 authentication key-chain eigrp

EIGRP for IPv6 パケットの認証をイネーブルにして、インターフェイス上で使用可能なキー セットを指定するには、**ipv6 authentication key-chain eigrp** コマンドを使用します。認証を禁止するには、このコマンドの **no** 形式を使用します。

ipv6 authentication key-chain eigrp *instance-tag* *name-of-chain*

no ipv6 authentication key-chain eigrp *instance-tag* *name-of-chain*

シンタックスの説明

<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
<i>name-of-chain</i>	キー チェーンの名前。キー チェーン名は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。

デフォルト

EIGRP パケットには認証は適用されません。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

インターフェイス コンフィギュレーション モードで **ipv6 authentication mode eigrp** コマンドを使用して、認証モードを設定する必要があります。インターフェイスに対する認証設定を完了するには、**key-chain** コマンドを使用して、別途キー チェーンを設定する必要があります。

このコマンドには、Enterprise Services ライセンスが必要です。

例

キーチェーン ツリーに属しているキーの受け入れと送信をインターフェイスに設定する例を示します。

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 1/2
switch(config-if)# ipv6 authentication key-chain eigrp 209 trees
```

関連コマンド

コマンド	説明
ipv6 authentication mode eigrp	EIGRP for IPv6 インターフェイス用の認証モードを設定します。
key-chain	認証方式で使用可能なキー セットを作成します。

ipv6 authentication mode eigrp

EIGRP for IPv6 パケットに使用される認証タイプを指定するには、**ipv6 authentication mode eigrp** コマンドを使用します。認証を削除するには、このコマンドの **no** 形式を使用します。

ipv6 authentication mode eigrp *instance-tag* md5

no ipv6 authentication mode eigrp *instance-tag* md5

シンタックスの説明	説明
<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
md5	Message Digest 5 (MD5) 認証を指定します。

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

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.1(2)	このコマンドが追加されました。

使用上のガイドライン このコマンドには、Enterprise Services ライセンスが必要です。

例 インターフェイスに使用される認証方式を MD5 に設定する例を示します。

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 1/2
switch(config-if)# ipv6 authentication mode eigrp 209 md5
```

関連コマンド	コマンド	説明
	authentication mode (EIGRP)	アドレスファミリ モードで EIGRP 用の認証モードを設定します。
	iv6p authentication key-chain eigrp	EIGRP の認証をイネーブルにして、インターフェイスに使用可能なキー セットを指定します。
	key chain	認証方式で使用可能なキー セットを作成します。

ipv6 bandwidth eigrp

EIGRP for IPv6 インターフェイスで帯域幅メトリックを設定するには、**ipv6 bandwidth eigrp** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 bandwidth eigrp *instance-tag* *bandwidth*

no ipv6 bandwidth eigrp

シンタックスの説明		
<i>instance-tag</i>		EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
<i>bandwidth</i>		帯域幅値。範囲は 1 ~ 2,560,000,000 キロビットです。

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

サポートされるユーザ ロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.1(2)	このコマンドが追加されました。

使用上のガイドライン このコマンドには、Enterprise Services ライセンスが必要です。

例 自律システム 209 で帯域幅 10000 が使用されるように EIGRP を設定する例を示します。

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 bandwidth eigrp 209 10000
```

関連コマンド	コマンド	説明
	ipv6 bandwidth-percent eigrp	インターフェイスの帯域幅のうち、EIGRP に使用できる割合をパーセントで設定します。

ipv6 bandwidth-percent eigrp

EIGRP for IPv6 インターフェイスで使用可能な帯域幅のパーセンテージを設定するには、**ipv6 bandwidth-percent eigrp** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 bandwidth-percent eigrp *instance-tag percent*

no ipv6 bandwidth-percent eigrp

シンタックスの説明

<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
<i>percent</i>	EIGRP に使用できる帯域幅のパーセンテージ

デフォルト

percent : 50

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

EIGRP が使用する帯域幅は、リンクの帯域幅の最大 50 % です。このパーセンテージは、**ip bandwidth** インターフェイス コンフィギュレーション コマンドで定義されます。このデフォルトのパーセンテージを変更するには、**ip bandwidth-percent** コマンドを使用します。

このコマンドには、Enterprise Services ライセンスが必要です。

例

自律システム 209 でインターフェイスの帯域幅の最大 75 % を使用するように EIGRP を設定する例を示します。

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 bandwidth-percent eigrp 209 75
```

関連コマンド

コマンド	説明
ipv6 bandwidth eigrp	インターフェイスの EIGRP 帯域幅値を設定します。

ipv6 delay eigrp

EIGRP for IPv6 インターフェイスのスループット遅延を設定するには、**ipv6 delay eigrp** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 delay eigrp *instance-tag* *seconds*

no ipv6 delay eigrp *instance-tag*

シンタックスの説明	説明
<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
<i>seconds</i>	スループット遅延 (10 マイクロ秒)。範囲は 1 ~ 16777215 です。

デフォルト 100 (10 マイクロ秒単位)

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

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.1(2)	このコマンドが追加されました。

使用上のガイドライン 10 マイクロ秒単位でインターフェイスにスループット遅延を設定します。たとえば、**ipv6 delay eigrp** コマンドを 100 に設定すると、スループット遅延は 1000 マイクロ秒になります。
このコマンドには、Enterprise Services ライセンスが必要です。

例 インターフェイスの遅延を 400 マイクロ秒に設定する例を示します。

```
switch(config)# router eigrp 1
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 delay eigrp 1 40
```

関連コマンド	コマンド	説明
	ipv6 hello-interval eigrp	自律システム番号で指定される EIGRP ルーティングプロセスに対するインターフェイスの hello インターバルを設定します。

ipv6 distribute-list eigrp

EIGRP for IPv6 インターフェイス用の配布リストを設定するには、**ipv6 distribute-list eigrp** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

```
ipv6 distribute-list eigrp instance-tag {prefix-list list-name | route-map map-name} {in | out}
```

```
no ipv6 distribute-list eigrp instance-tag {prefix-list list-name | route-map map-name} {in | out}
```

シンタックスの説明

instance-tag	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
prefix-list <i>list-name</i>	EIGRP ルートをフィルタするための IPv6 プレフィクス リストの名前を指定します。
route-map <i>map-name</i>	EIGRP ルートのフィルタリングに使用するルート マップの名前を指定します。
in	着信ルートにルート ポリシーを適用します。
out	発信ルートにルート ポリシーを適用します。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

ipv6 distribute-list eigrp コマンドは、インターフェイス上のルート フィルタ ポリシーを設定するために使用します。この設定を完了するためには、ルート マップまたはプレフィクス リストの名前を設定する必要があります。

このコマンドには、Enterprise Services ライセンスが必要です。

例

インターフェイスに着信するすべての EIGRP ルートのルート マップを設定する例を示します。

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 distribute-list eigrp 209 route-map InputFilter in
```

関連コマンド

コマンド	説明
prefix-list	プレフィクス リストを設定します。
route-map	ルート マップを設定します。

ipv6 eigrp shutdown

EIGRP for IPv6 インターフェイスをシャットダウンするには、**ipv6 eigrp shutdown** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 eigrp *instance-tag* shutdown

no ipv6 eigrp *instance-tag* shutdown

シンタックスの説明	<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
-----------	---------------------	--

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
----------	----------------------

サポートされるユーザロール	ネットワーク管理者 VDC 管理者
---------------	----------------------

コマンドの履歴	リリース	変更内容
	4.1(2)	このコマンドが追加されました。

使用上のガイドライン	このコマンドには、Enterprise Services ライセンスが必要です。
------------	--

例	インターフェイスの EIGRP をディセーブルにする例を示します。
---	-----------------------------------

```
switch(config)# router eigrp 201
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 eigrp 201 shutdown
```

関連コマンド	コマンド	説明
	router eigrp	EIGRP のインスタンスを設定します。

ipv6 hello-interval eigrp

インターフェイスの EIGRP for IPv6 hello インターバルを設定するには、**ipv6 hello-interval eigrp** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 hello-interval eigrp *instance-tag seconds*

no ipv6 hello-interval eigrp *instance-tag*

シンタックスの説明

<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
<i>seconds</i>	hello インターバル (秒単位)。有効範囲は 1 ~ 65535 です。

デフォルト

5 秒

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、Enterprise Services ライセンスが必要です。

例

インターフェイスの hello インターバルを 10 秒に設定する例を示します。

```
switch(config)# router eigrp 1
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 hello-interval eigrp 1 10
```

ipv6 hold-time eigrp

EIGRP for IPv6 インターフェイスのホールド時間を設定するには、**ipv6 hold-time eigrp** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 hold-time eigrp *instance-tag* *seconds*

no ipv6 hold-time eigrp *instance-tag*

シンタックスの説明	
<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
<i>seconds</i>	ホールド時間 (秒単位)。有効範囲は 1 ~ 65535 です。

デフォルト 15 秒

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

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.1(2)	このコマンドが追加されました。

使用上のガイドライン **ipv6 hold-time eigrp** コマンドは、非常に輻輳した大規模ネットワーク上のデフォルト ホールド時間を増加するために使用します。

ホールド時間は、**hello** インターバルの 3 倍以上の値に設定することを推奨します。指定されたホールド時間内にルータが **hello** パケットを受信しなかった場合は、そのルータ経由のルートが使用できないと判断されます。

ホールド時間を長くすると、ネットワーク全体のルート コンバージェンスが遅延します。

このコマンドには、Enterprise Services ライセンスが必要です。

例 次に、インターフェイスのホールド時間を 40 秒に設定する例を示します。

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 hold-time eigrp 209 40
```

関連コマンド	コマンド	説明
	ipv6 hello-interval eigrp	自律システム番号で指定された EIGRP ルーティング プロセス用のインターフェイス上の hello インターバルを設定します。

ipv6 host

DNS ホスト キャッシュ内でスタティック ホスト名/アドレス マッピングを定義するには、**ipv6 host** コマンドを使用します。ホスト名/アドレス マッピ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。

```
ipv6 host name address1 [address2... address6]
```

```
no ipv6 host name address1 [address2... address6]
```

シンタックスの説明

<i>name</i>	ホスト名。 <i>name</i> は、大文字と小文字が区別される 80 文字以下の任意の英数字文字列にできます。
<i>address1</i>	A::B::C:D 形式の IPv6 アドレス。
<i>address2 ...address6</i>	(任意) A::B::C:D 形式の追加の IPv6 アドレス (最大 5 個)。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

ipv6 host コマンドは、スタティック ホスト名を DNS に追加するために使用します。このコマンドにはライセンスは必要ありません。

例

次に、スタティック ホスト名を設定する例を示します。

```
switch(config)# ipv6 host mycompany.com 2001:0DB8::4
```

関連コマンド

コマンド	説明
ip host	スタティック ホスト名を設定します。

ipv6 nd hop-limit

IPv6 ネイバー探索パケット内のホップ リミットをアダプタイズするには、**ipv6 nd hop-limit** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd hop-limit *hop-limit*

no ipv6 nd hop-limit [*hop-limit*]

シNTAXの説明	<i>hop-limit</i>	IPv6 ヘッダー内のホップ リミット。指定できる範囲は 0 ~ 255 です。
デフォルト	64	
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	
サポートされるユーザロール	ネットワーク管理者 VDC 管理者	
コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。
使用上のガイドライン	このコマンドにはライセンスは必要ありません。	
例	次に、IPv6 ホップ リミットを設定する例を示します。 <pre>switch(config)# interface ethernet 2/1 switch(config-if)# ipv6 nd hop-limit 55</pre>	
関連コマンド	コマンド	説明
	show ipv6 nd interface	インターフェイスの IPv6 ネイバー探索情報を表示します。

ipv6 nd managed-config-flag

ステートフルアドレス自動設定を使用してアドレス情報を取得するように ICMPv6 Router-Advertisement メッセージ内でアドバタイズするには、**ipv6 nd managed-config-flag** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

シンタックスの説明 このコマンドには、キーワードと引数はありません。

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

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン このコマンドにはライセンスは必要ありません。

例 次に、ステートフルアドレス自動設定を使用してアドレス情報を取得するように ICMPv6 Router-Advertisement メッセージ内でアドバタイズする例を示します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd managed-config-flag
```

関連コマンド	コマンド	説明
	show ipv6 nd interface	インターフェイスの IPv6 ネイバー探索情報を表示します。

ipv6 nd mtu

このリンク上で ICMPv6 Router-Advertisement メッセージ内の MTU をアダバタイズするには、**ipv6 nd mtu** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd mtu *mtu*

no ipv6 nd mtu [*mtu*]

シンタックスの説明

mtu バイト単位の MTU。範囲は 1280 ~ 65535 です。

デフォルト

1500

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにはライセンスは必要ありません。

例

次に、リンク上でアダバタイズする MTU 値を設定する例を示します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd mtu 1280
```

関連コマンド

コマンド	説明
show ipv6 nd interface	インターフェイスの IPv6 ネイバー探索情報を表示します。

ipv6 nd ns-interval

IPv6 Neighbor Solicitation (NS; ネイバー送信要求) メッセージ間の再送信インターバルを設定するには、**ipv6 nd ns-interval** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6nd ns-interval *interval*

no ipv6 nd ns-interval [*interval*]

シンタックスの説明

interval ミリ秒単位のインターバル。範囲は 1000 ~ 3600000 です。

デフォルト

1000

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにはライセンスは必要ありません。

例

次に、ネイバー再送信要求インターバルを設定する例を示します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd ns-interval 1280
```

関連コマンド

コマンド	説明
show ipv6 nd interface	インターフェイスの IPv6 ネイバー探索情報を表示します。

ipv6 nd other-config-flag

ホストがステートフル自動設定を使用して非アドレス関連情報を取得するように ICMPv6 ルータ アドバタイズメント メッセージ内で指定するには、**ipv6 nd other-config-flag** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

シンタックスの説明 このコマンドには、キーワードと引数はありません。

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

サポートされるユーザロール ネットワーク 管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン このコマンドにはライセンスは必要ありません。

例 次に、ICMPv6 ルータ アドバタイズメント メッセージ内でステートフル自動設定を設定する例を示します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd other-config-flag
```

関連コマンド	コマンド	説明
	show ipv6 nd interface	インターフェイスの IPv6 ネイバー探索情報を表示します。

ipv6 nd ra-interval

ICMPv6 ルータ アドバタイズメント メッセージの送信間のインターバルを設定するには、**ipv6 nd ra-interval** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ra-interval *interval*

no ipv6 nd ra-interval [*interval*]

シンタックスの説明	<i>interval</i>	ルータ アドバタイズメント メッセージの送信間のインターバル (秒単位)。範囲は 4 ~ 1800 です。
------------------	-----------------	---

デフォルト	600
--------------	-----

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
-----------------	----------------------

サポートされるユーザロール	ネットワーク管理者 VDC 管理者
----------------------	----------------------

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン	このコマンドにはライセンスは必要ありません。
-------------------	------------------------

例	次に、ICMPv6 ルータ アドバタイズメント メッセージ インターバルを設定する例を示します。
----------	--

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd ra-interval 500
```

関連コマンド	コマンド	説明
	show ipv6 nd interface	インターフェイスの IPv6 ネイバー探索情報を表示します。

ipv6 nd ra-lifetime

ICMPv6 ルータ アドバタイズメント メッセージ内でデフォルト ルータのライフタイムをアドバタイズするには、**ipv6 nd ra-lifetime** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ra-lifetime *lifetime*

no ipv6 nd ra-lifetime [*lifetime*]

シンタックスの説明

<i>lifetime</i>	秒単位のライフタイム。範囲は 0 ～ 9000 です。0 の場合は、このルータがデフォルトルータになりません。
-----------------	---

デフォルト

ルータ アドバタイズメント インターバルの 3 倍。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにはライセンスは必要ありません。

例

次に、ICMPv6 ルータ アドバタイズメント メッセージ ライフタイムを設定する例を示します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd ra-lifetime 1500
```

関連コマンド

コマンド	説明
show ipv6 nd interface	インターフェイスの IPv6 ネイバー探索情報を表示します。

ipv6 nd reachable-time

ICMPv6 ルータ アドバタイズメント メッセージ内の到達可能性確認の受信後にノードでネイバーがアップしたことを認識した時間をアドバタイズするには、**ipv6 nd reachable-time** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd reachable-time *time*

no ipv6 nd reachable-time [*time*]

シンタックスの説明

time ミリ秒単位の時間。範囲は 0 ~ 3600000 です。

デフォルト

0

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにはライセンスは必要ありません。

例

次に、ICMPv6 ルータ アドバタイズメント到達可能性時間を設定する例を示します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd reachable-time 1500
```

関連コマンド

コマンド	説明
show ipv6 nd interface	インターフェイスの IPv6 ネイバー探索情報を表示します。

ipv6 nd redirects

ICMPv6 リダイレクト メッセージの送信をイネーブルにするには、**ipv6 redirects** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd redirects

no ipv6 nd redirects

シンタックスの説明 このコマンドには、キーワードと引数はありません。

デフォルト ディセーブル

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

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン このコマンドにはライセンスは必要ありません。

例 次に、ICMPv6 ルータ アドバタイズメント メッセージをディセーブルにする例を示します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd suppress-ra
```

関連コマンド	コマンド	説明
	show ipv6 nd interface	インターフェイスの IPv6 ネイバー探索情報を表示します。

ipv6 nd retrans-timer

ICMPv6 ルータ アドバタイズメント メッセージ内でネイバー再送信要求間の時間をアドバタイズするには、**ipv6 nd retrans-timer** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd retrans-timer *time*

no ipv6 nd retrans-timer [*time*]

シンタックスの説明

time ミリ秒単位の時間。範囲は 0 ~ 4294967295 です。

デフォルト

0

コマンドモード

if-igmp configuration (config-xxx)

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにはライセンスは必要ありません。

例

次に、ICMPv6 ルータ アドバタイズメント到達可能性時間を設定する例を示します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd reachable-time 1500
```

関連コマンド

コマンド	説明
show ipv6 nd interface	インターフェイスの IPv6 ネイバー探索情報を表示します。

ipv6 nd suppress-ra

ICMPv6 ルータ アドバタイズメント メッセージの送信をディセーブルにするには、**ipv6 nd suppress-ra** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

シンタックスの説明 このコマンドには、キーワードと引数はありません。

デフォルト イネーブル

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

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン このコマンドにはライセンスは必要ありません。

例 次に、ICMPv6 ルータ アドバタイズメント メッセージをディセーブルにする例を示します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 nd suppress-ra
```

関連コマンド	コマンド	説明
	show ipv6 nd interface	インターフェイスの IPv6 ネイバー探索情報を表示します。

ipv6 neighbor

IPv6 ネイバー探索キャッシュ内のスタティック エントリを設定するには、**ipv6 neighbor** コマンドを使用します。IPv6 ネイバー探索キャッシュからスタティック IPv6 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。

ipv6 neighbor *pv6-address interface-type interface-number hardware-address*

no ipv6 neighbor *ipv6-address interface-type interface-number hardware-address*

シンタックスの説明

<i>ipv6-address</i>	ローカル データリンク アドレスに対応する IPv6 アドレス。 この引数には RFC2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
<i>interface-type</i>	指定されたインターフェイス タイプ。サポートされているインターフェイス タイプについては、疑問符 (?) オンライン ヘルプ機能を使用してください。
<i>interface-number</i>	指定されたインターフェイス番号。
<i>hardware-address</i>	ローカル データリンク アドレス (48 ビットアドレス)。

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

サポートされるユーザ ロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

ipv6 neighbor コマンドは、スタティック エントリを作成するために使用します。指定した IPv6 アドレスのエントリがすでにネイバー検出キャッシュにある場合 (IPv6 ネイバー検出プロセスで学習した場合)、エントリは自動的にスタティック エントリに変換されます。

show ipv6 neighbors コマンドは、IPv6 ネイバー探索キャッシュ内のスタティック エントリを表示するために使用します。IPv6 ネイバー探索キャッシュ内のスタティック エントリは次のいずれかの状態になります。

- INCMP (不完全) : このエントリのインターフェイスがダウンしています。
- REACH (到達可能) : このエントリのインターフェイスがアップしています。



(注) 到達可能性検出は、IPv6 ネイバー探索キャッシュ内のスタティック エントリに適用されません。そのため、INCMP および REACH 状態に関する説明とダイナミックおよびスタティック キャッシュ エントリに関する説明は一致しません。ダイナミック キャッシュ エントリの INCMP および REACH 状態の説明については、`show ipv6 neighbors` コマンドを参照してください。

clear ipv6 neighbors コマンドは、スタティック エントリを除いて、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除します。**no ipv6 neighbor** コマンドは、指定されたスタティック エントリを近隣探索キャッシュから削除します。このコマンドは、IPv6 ネイバー探索プロセスから取得されたダイナミック エントリをキャッシュから削除しません。**no ipv6 enable** コマンドまたは **no ipv6 unnumbered** コマンドを使用してインターフェイス上の IPv6 をディセーブルにすると、スタティック エントリ (INCMP に対するエントリ変更のステート) を除いて、そのインターフェイスに設定されたすべての IPv6 ネイバー探索キャッシュ エントリが削除されます。

IPv6 ネイバー検出キャッシュ内のスタティック エントリは、ネイバー検出プロセスでは変更されません。

例

次の例では、イーサネット インターフェイス 2/1 上の IPv6 アドレスが 2001:0DB8::45A で、リンクレイアアドレスが 0002.7D1A.9472 のネイバーに関する IPv6 ネイバー探索キャッシュ内のスタティック エントリを設定します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 neighbor 2001:0DB8::45A ethernet 2/10002.7D1A.9472
```

ipv6 next-hop-self eigrp

これらのルートのアドバタイズ時にネクストホップ アドレスとしてローカル IPv6 アドレスを使用するように EIGRP for IPv6 プロセスに指示するには、**next-hop-self eigrp** コマンドを使用します。受信したネクストホップ値を使用するには、このコマンドの **no** 形式を使用します。

ipv6 next-hop-self eigrp *instance-tag*

no ipv6 next-hop-self eigrp *instance-tag*

シンタックスの説明

instance-tag

EIGRP インスタンスの名前。*instance-tag* は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。

デフォルト

EIGRP は、常に、IPv6 ネクストホップ値を自己設定します。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

デフォルトで、EIGRP は、ルータがルートを取得したインターフェイスと同じインターフェイス上でルートをアドバタイズする場合でも、アドバタイズするルートの IPv6 ネクストホップ値を自己設定します。このデフォルトを変更するには、**no ipv6 next-hop-self eigrp** インターフェイス コンフィギュレーション コマンドを使用して、これらのルートのアドバタイズ時に受信したネクストホップ値を使用するように EIGRP に指示する必要があります。

例

デフォルトの IPv6 ネクストホップ値を変更し、受信したネクストホップ値を使用するように EIGRP に指示する例を示します。

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-eigrp-af-if)# no ipv6 next-hop-self eigrp 209
```

ipv6 offset-list eigrp

EIGRP for IPv6 インターフェイスのオフセット リストを設定するには、**ipv6 offset-list eigrp** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

```
ipv6 offset-list eigrp instance-tag {prefix-list list-name | route-map map-name} {in | out} offset
```

```
no ipv6 offset-list eigrp instance-tag {prefix-list list-name | route-map map-name} {in | out} offset
```

シンタックスの説明

<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
prefix-list <i>list-name</i>	EIGRP ルートをフィルタするための IPv6 プレフィクス リストの名前を指定します。
route-map <i>map-name</i>	EIGRP ルートのフィルタリングに使用するルート マップの名前を指定します。
in	着信ルートにルート ポリシーを適用します。
out	発信ルートにルート ポリシーを適用します。
<i>offset</i>	EIGRP メトリックに追加する値

デフォルト

このコマンドには、デフォルトはありません。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

ipv6 offset-list eigrp コマンドは、インターフェイス上でアドバタイズされるルートに影響を与えます。Cisco NX-OS は、指定されたプレフィクス リストまたはルート マップと一致するすべてのルートに、設定されたオフセット値を追加します。この設定を完了するためには、ルート マップまたはプレフィクス リストの名前を設定する必要があります。

このコマンドには、Enterprise Services ライセンスが必要です。

例

次の例では、ルート マップ OffsetFilter と一致するインターフェイスに着信する EIGRP ルートのメトリックに 20 を追加するように、オフセット リスト フィルタを設定します。

```
switch(config)# router eigrp 209
```



```
switch(config-router)# interface ethernet 2/1  
switch(config-if)# ipv6 offset-list eigrp 209 route-map OffsetFilter in 20
```

関連コマンド

コマンド	説明
prefix-list	プレフィクス リストを設定します。
route-map	ルート マップを設定します。

ipv6 passive-interface eigrp

EIGRP for IPv6 インターフェイス上のすべてのルーティング アップデートを抑制するには、**ipv6 passive-interface eigrp** コマンドを使用します。ルーティング アップデートの送信を再度イネーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 passive-interface eigrp *instance-tag*

no ipv6 passive-interface eigrp *instance-tag*

シンタックスの説明

<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
---------------------	--

デフォルト

インターフェイス上でルーティング アップデートが送信されます。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

ipv6 passive-interface eigrp コマンドは、インターフェイス上のすべてのルーティング アップデートを停止し、EIGRP 隣接関係の形成を抑制するために使用します。

このコマンドには、Enterprise Services ライセンスが必要です。

例

次に、インターフェイス Ethernet 2/1 上の EIGRP ルーティング アップデートを停止する例を示します。

```
switch(config)# router eigrp 201
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 passive-interface eigrp 201
```

ipv6 policy route-map

インターフェイス上のポリシー ルーティングに使用されるルート マップを特定するには、**ipv6 policy route-map** コマンドを使用します。ルート マップを削除するには、このコマンドの **no** 形式を使用します。

ipv6 policy route-map *name*

no ipv6 policy route-map [*name*]

シンタックスの説明

<i>name</i>	ルート マップ名。名前は、63 文字以下の任意の英数字文字列にできます。
-------------	--------------------------------------

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

サポートされるユーザ ロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.2(1)	このコマンドが追加されました。

使用上のガイドライン

ipv6 policy route-map コマンドは、IPv6 インターフェイス上でポリシー ルーティングを使用するためのルート マップを特定するために使用します。ルート マップを作成するには、**route-map** コマンドを使用します。**route-map** コマンドごとに、それに関連した **match** および **set** コマンドのリストがあります。**match** コマンドは、パケットの宛先 IPv6 アドレスに基づいて、一致基準（インターフェイスに対してポリシー ルーティングが許可される条件）を指定します。**set** コマンドでは、set 処理（**match** コマンドによる基準が満たされた場合に実行する特定のポリシー ルーティング処理）を指定します。**no ipv6 policy route-map** コマンドは、ルート マップへのポインタを削除します。

match ipv6 address コマンドを使用し、IPv6 アクセス リストを参照している場合は、IPv6 アクセス リスト内で定義可能な任意の一致基準でポリシーベース ルーティングを実行できます。

ipv6 policy route-map コマンドを使用する前に、**feature pbr** コマンドでポリシーベース ルーティングをイネーブルにする必要があります。

このコマンドには、Enterprise Services ライセンスが必要です。

例

次に、インターフェイスにポリシーベース ルート マップを設定する例を示します。

```
switch# configure terminal
switch(config)# feature pbr
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 policy route-map policymap
```

関連コマンド

コマンド	説明
feature pbr	ポリシーベース ルーティング機能をイネーブルにします。
route-map	ルート マップを作成します。
show route-map pbr-statistics	ポリシーベース ルート マップについての統計情報を表示します。
show ipv6 policy	IPv6 ポリシーに関する情報を表示します。

ipv6 prefix-list

ipv6 prefix-list コマンドは、IPv6 パケットまたはルートを照合するプレフィクス リストを作成するために使用します。プレフィクス リストを削除するには、このコマンドの **no** 形式を使用します。

```
ipv6 prefix-list name [seq number] {permit | deny} prefix [eq length | [ge length] [le length]]
```

```
no ipv6 prefix-list name [seq number] {permit | deny} prefix [eq length | [ge length] [le length]]
```

シンタックスの説明

name	IPv6 プレフィクス リストの名前。名前は、63 文字以下の任意の英数字文字列にできます。
seq number	(任意) プレフィクス リストのエントリの順序を示すシーケンス番号。範囲は 1 ~ 4294967294 です。
permit	プレフィクス リストと一致するルートまたは IP パケットを許可します。
deny	プレフィクス リストと一致するルートまたは IP パケットを拒否します。
prefix	A:B::C:D/length 形式の IP プレフィクス
eq length	(任意) 照合するプレフィクスの長さ (完全一致)。範囲は 1 ~ 128 です。
ge length	(任意) 照合するプレフィクス長の最大値。範囲は 1 ~ 128 です。
le length	(任意) 照合するプレフィクス長の最小値。範囲は 1 ~ 128 です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

IPv6 プレフィクス フィルタリングを設定するには、**ipv6 prefix-list** コマンドを使用します。**permit** または **deny** のキーワードを指定してプレフィクス リストを設定し、一致条件に基づいてプレフィクスを許可または拒否します。プレフィクス リストは、IPv6 アドレスとビット マスクで構成されています。ビット マスクは、1 ~ 128 の数値として入力されます。どのプレフィクス リストのエントリとも一致しないトラフィックに暗黙拒否が適用されます。

プレフィクス リストは、完全一致方式で指定のプレフィクス長と照合するように設定することも、またプレフィクス範囲と照合するように設定することもできます。**ge** と **le** のキーワードを使用して照合するプレフィクス長の範囲を指定することにより、**network/length** 引数だけを指定するよりも柔軟な設定が可能となります。**ge** と **le** のいずれのキーワードも設定しない場合、Cisco NX-OS は完全一致方式

でプレフィクス リストを処理します。**ge ge-length** と **le le-length** の両方のキーワードと引数を設定した場合、許可されるプレフィクス長の範囲は **ge-length** 引数と **le-length** 引数の間になります。この動作は、次の式で表すことができます。

$$\text{ネットワーク/長さ} < \text{ge ge-length} < \text{le le-length} \leq 32$$

シーケンス番号を設定しないと、Cisco NX-OS によって、プレフィクス リスト エントリにデフォルトのシーケンス番号である 5 が適用され、後続のプレフィクス リスト エントリのシーケンス番号は 5 ずつ増分されます (5、10、15 など)。最初のプレフィクス リスト エントリのシーケンス番号を設定し、後続のエントリにシーケンス番号を設定しないと、Cisco NX-OS によって、後続のエントリのシーケンス番号は 5 ずつ増分されます (たとえば、最初に設定したシーケンス番号が 3 の場合、後続のエントリは、8、13、18 のように増分されます)。デフォルトのシーケンス番号の適用を停止するには、**seq** キーワードを指定して、このコマンドの **no** 形式を使用します。

Cisco NX-OS は、シーケンス番号が最も小さいエントリからプレフィクス リストの評価を開始し、一致するものが見つかるまで順番に評価していきます。ネットワークに該当するよう一致が見つかったら、そのネットワークに **permit** または **deny** 文が適用され、リストの残りは評価されません。



ヒント

最も処理される頻度の高いプレフィクス リスト文のシーケンス番号を最小にすれば、最良のパフォーマンスを得ることができます。**seq number** のキーワードと引数はリシーケンスに使用できます。

ネイバー アドレスファミリ モードで **prefix-list** コマンドを入力すると、特定のピアのインバウンドまたはアウトバウンドのアップデートにプレフィクス リストを適用できます。プレフィクス リストの情報とカウンタは、**show ipv6 prefix-list** コマンドの出力に表示されます。**prefix-list** カウンタをリセットするには、**clear ipv6 prefix-list** コマンドを入力します。

このコマンドにはライセンスは必要ありません。

例

次に、IPv6 プレフィクス リストを設定し、BGP ピアに適用する例を示します。

```
switch# config t
switch(config)# ipv6 prefix-list allowprefix 10 permit 2001:0DB8::/48 eq 24
switch(config) router bgp 65536:20
switch(config-router)# neighbor 2001:0DB8::1/64 remote-as 65536:20
switch(config-router-neighbor)# address-family ipv6 unicast
switch(config-router-neighbor-af)# prefix-list allowprefix in
```

関連コマンド

コマンド	説明
clear ip prefix-list	IP プレフィクス リストのカウンタをクリアします。
prefix-list	BGP ピアにプレフィクス リストを適用します。
show ip prefix-list	IP プレフィクス リストについての情報を表示します。

ipv6 prefix-list description

IPv6 プレフィクス リストを説明する文字列を設定するには、**ipv6 prefix-list description** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 prefix-list name description string

no ipv6 prefix-list name description

シンタックスの説明	name	プレフィクス リストの名前。名前は、63 文字以下の任意の英数字文字列にできます。
	string	プレフィクス リストを説明する文字列。最大 90 文字の英数字を使用できます。

デフォルト なし

コマンド モード グローバル コンフィギュレーション

サポートされるユーザロール ネットワーク管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン このコマンドにはライセンスは必要ありません。

例 次に、IPv6 プレフィクス リストの説明の設定例を示します。

```
switch# configure terminal
switch(config)# ipv6 prefix-list test1 description "this is a test"
```

関連コマンド	コマンド	説明
	ipv6 prefix-list	IPv6 プレフィクス リストを作成します。
	show ipv6 prefix-list	IPv6 プレフィクス リストについての情報を表示します。

ipv6 route

スタティック IPv6 ルートを設定するには、**ipv6 route** コマンドを使用します。スタティック ルートを削除するには、このコマンドの **no** 形式を使用します。

```
ipv6 route ipv6-prefix/length { next-hop-addr | next-hop-prefix } | interface |
link-local-addr } [preference] [tag tag-id]
```

```
no ipv6 route ipv6-prefix/length
```

シンタックスの説明

<i>ipv6-prefix/length</i>	IPv6 prefix and prefix length. 形式は A:B::C:D/length です。length の範囲は 1 ~ 128 です。
<i>next-hop</i>	ネクストホップ アドレス。形式は A:B::C:D です。
<i>next-hop-prefix</i>	ネクストホップのプレフィクスと長さ。形式は A:B::C:D/length です。length の範囲は 1 ~ 128 です。
<i>interface</i>	このルートに到達するためのインターフェイス。? を使用して サポートされているインターフェイスのリストを表示します。
<i>link-local-addr</i>	IPv6 リンクローカル アドレス。形式は A:B::C:D です。
<i>preference</i>	(任意) このルートまでの管理ディスタンスとして使用されるルートプリファレンスを設定します。範囲は 1 ~ 255 です。デフォルトは 1 です。
tag id	(任意) ルート マップ内の照合に使用可能なルート タグを割り当てます。範囲は 0 ~ 4294967295 です。デフォルトは 0 です。

デフォルト

デフォルトでは、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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにはライセンスは必要ありません。

例

この例では、IPv6 スタティック ルートを作成します。

```
switch(config)# ipv6 route 2001:0DB8::/48 2b11::2f01:4c
```


関連コマンド

コマンド	説明
ip route	IPv4 スタティック ルートを設定します。

ipv6 router eigrp

EIGRP for IPv6 インターフェイスを指定するには、**ipv6 router eigrp** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 router eigrp *instance-tag*

no ipv6 router eigrp *instance-tag*

シンタックスの説明	<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
-----------	---------------------	--

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
----------	----------------------

サポートされるユーザロール	ネットワーク管理者 VDC 管理者
---------------	----------------------

コマンドの履歴	リリース	変更内容
	4.1(2)	このコマンドが追加されました。

使用上のガイドライン **ipv6 router eigrp** コマンドは、インターフェイス用の EIGRP インスタンスを指定するために使用します。このコマンドには、Enterprise Services ライセンスが必要です。

例 次に、インターフェイス用の EIGRP インスタンスを設定する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ipv6 router eigrp Base
```

ipv6 router ospfv3 area

インターフェイス用の Open Shortest Path First version 3 (OSPFv3) インスタンスとエリアを指定するには、**ipv6 router ospfv3 area** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 router ospfv3 instance-tag area area-id [secondaries none]

no ipv6 router ospfv3 instance-tag area area-id [secondaries none]

シンタックスの説明

<i>instance-tag</i>	インスタンス タグ。英数字文字列で指定します。
<i>area-id</i>	認証をイネーブルにする OSPFv3 エリアの識別情報。正の整数値または IP アドレスを指定します。
secondaries none	(任意) セカンダリ IP アドレスを除外します。

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

サポートされるユーザ ロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

ipv6 router ospfv3f area コマンドは、インターフェイス用のエリアと OSPFv3 インスタンスを指定するために使用します。

このコマンドには、Enterprise Services ライセンスが必要です。

例

次に、インターフェイスを OSPFv3 用に設定する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ipv6 router ospfv3 Base area 33
```

ipv6 router ospfv3 multi-area

OSPFv3 インターフェイス上で複数エリア隣接関係を設定するには、**ipv6 router ospfv3 multi-area** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 router ospfv3 instance-tag multi-area area-id

no ipv6 router ospfv3 instance-tag multi-area area-id

シンタックスの説明

<i>instance-tag</i>	インスタンス タグ。大文字と小文字が区別される 63 文字以下の英数字文字列として指定します。
<i>area-id</i>	プライマリ インターフェイスに別のエリアとして追加する OSPF エリアに関する識別情報。正の整数値または IP アドレスを指定します。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.2(1)	このコマンドが追加されました。

使用上のガイドライン

ipv6 router ospfv3 multi-area コマンドは、OSPFv3 インターフェイス上で追加のエリアを指定するために使用します。

このコマンドには、Enterprise Services ライセンスが必要です。

例

次に、複数エリア隣接関係を設定する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ipv6 router ospfv3 Base area 33
switch(config-if)# ipv6 router ospfv3 Base multi-area 99
```

ipv6 split-horizon eigrp

EIGRP for IPv6 プロセスのスプリット ホライズンをイネーブルにするには、**ipv6 split-horizon eigrp** コマンドを使用します。スプリット ホライズン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。

ipv6 split-horizon eigrp *instance-tag*

no ipv6 split-horizon eigrp *instance-tag*

シンタックスの説明

<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
---------------------	--

デフォルト

イネーブル

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

no ipv6 split-horizon eigrp コマンドは、インターフェイス上のスプリット ホライズンをディセーブルにするために使用します。

このコマンドには、Enterprise Services ライセンスが必要です。

例

イーサネット リンクのスプリット ホライズンをディセーブルにする例を示します。

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-eigrp-af-if)# no ipv6 split-horizon eigrp 209
```

ipv6 summary-address eigrp

指定された EIGRP for IPv6 インターフェイスのサマリー集約アドレスを設定するには、**ipv6 summary-address eigrp** コマンドを使用します。設定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。

```
ipv6 summary-address eigrp instance-tag {ipv6-address /length} [admin-distance]
```

```
no ipv6 summary-address eigrp instance-tag {ipv6-address /length}
```

シンタックスの説明

<i>instance-tag</i>	EIGRP インスタンスの名前。 <i>instance-tag</i> は、大文字と小文字が区別される 63 文字以下の任意の英数字文字列にできます。
<i>ipv6-address/length</i>	インターフェイスに A:B::C:D/length 形式で適用されるサマリー IPv6 プレフィクスとプレフィクス長。length の範囲は 1 ~ 128 です。
<i>admin-distance</i>	(任意) 管理ディスタンス。範囲は 1 ~ 255 です。

デフォルト

EIGRP サマリー ルートには、管理ディスタンス 5 が適用されます。事前設定されるサマリー アドレスはありません。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

ipv6 summary-address eigrp コマンドは、インターフェイス レベルのサマリー アドレスを設定するために使用します。EIGRP サマリー ルートの管理ディスタンスは 5 です。

このコマンドには、Enterprise Services ライセンスが必要です。

例

次に、2001:0DB8::/48 サマリー アドレス用の EIGRP インターフェイス上で 95 の管理ディスタンスを設定する例を示します。

```
switch(config)# router eigrp 209
switch(config-router)# interface ethernet 2/1
switch(config-if)# ipv6 summary-address eigrp 209 2001:0DB8::/48 95
```

ipv6 unreachableables

ICMPv6 到達不能メッセージの送信をイネーブルにするには、**ipv6 unreachableables** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 [icmp] unreachableables

no ipv6 [icmp] unreachableables

シンタックスの説明

icmp (任意) ICMPv6 コマンド。

デフォルト

ディセーブル

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

ポート到達不能メッセージは、常に、レート リミットがイネーブルになっています。このコマンドにはライセンスは必要ありません。

例

次に、ICMPv6 到達不能メッセージをイネーブルにする例を示します。

```
switch(config)# interface ethernet 2/1  
switch(config-if)# ipv6 unreachableables
```

関連コマンド

コマンド	説明
show ipv6 nd interface	インターフェイスの IPv6 ネイバー探索情報を表示します。

is-type

Intermediate System-to-Intermediate System (IS-IS) ルーティング プロセスのインスタンスのルーティング レベルを設定するには、**is-type** コマンドを使用します。デフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

is-type {level-1 | level-1-2 | level-2}

no is-type {level-1 | level-1-2 | level-2}

シンタックスの説明

level-1	ルータがレベル 1 (エリア内) ルーティングのみを実行するように指定します。
level-1-2	ルータがレベル 1 とレベル 2 のルーティングを両方実行するように指定します。
level-2	ルーティング プロセスがレベル 2 (エリア間) ルータのみとして機能するように指定します。

コマンドのデフォルト

通常、ルータはデフォルトの設定でレベル 1 (エリア内) およびレベル 2 (エリア間) のルータとして機能します。マルチエリア IS-IS 設定では、設定されている IS-IS ルーティング プロセスの最初のインスタンスはデフォルトでレベル 1-2 (エリア内およびエリア間) ルータになります。設定されている IS-IS プロセスの残りのインスタンスはデフォルトでレベル 1 ルータになります。

コマンド モード

ルータ コンフィギュレーション
VRF コンフィギュレーション

サポートされるユーザ ロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

IS-IS ルーティング プロセスのルーティング レベルは次のように定義されています。

- **level-1** : ルータがレベル 1 (エリア内) ルーティングのみを実行するように指定します。このルータが学習するのはそのエリア内の宛先だけです。レベル 2 (エリア間) ルーティングは、最も近いレベル 1-2 ルータで実行されます。
- **level-1-2** : ルータがレベル 1 とレベル 2 のルーティングを両方実行するように指定します。このルータは、ルーティング プロセスのインスタンスを 2 つ実行します。このルータにはエリア内 (レベル 1 ルーティング) の宛先に関する Link-State Packet Database (LSDB) があり、最短パス優先 (SPF) 計算によってエリア トポロジが検出されます。このルータには、その他すべてのバックボーン (レベル 2) ルータの Link-State Packet (LSP; リンクステート パケット) が保存された別の LSDB もあり、別の SPF 計算によって、バックボーンのトポロジやその他すべてのエリアに存在するものが検出されます。
- **level-2** : ルーティング プロセスがレベル 2 (エリア間) ルータのみとして機能するように指定します。このルータはバックボーンの一部であり、そのエリア内のレベル 1 専用ルータとは通信しません。

IS-IS ルーティング プロセスのタイプを設定することを推奨します。マルチエリア IS-IS を設定している場合は、ルータのタイプを設定するか、またはデフォルト設定のままにしておく必要があります。デフォルトで、`router isis` コマンドで設定した IS-IS ルーティング プロセスの最初のインスタンスは、レベル 1-2 ルータになります。

ネットワークにエリアが 1 つだけしかない場合は、必ずしもレベル 1 とレベル 2 の両方のルーティング アルゴリズムを実行する必要はありません。IS-IS が IP ルーティングのみに使用され、エリアが 1 つしかない場合は、常にレベル 2 だけを実行できます。すでにレベル 1-2 エリアがある場合、その後追加されたエリアは、デフォルトでレベル 1 エリアになります。

ルータ インスタンスがレベル 1-2 (シスコ デバイスにおける IS-IS ルーティング プロセスの最初のインスタンスのデフォルト) に設定されている場合、`is-type` コマンドを使用して、そのエリアのレベル 2 (エリア間) ルーティングを削除できます。`is-type` コマンドを使用してエリアに レベル 2 ルーティングを設定できるのは、シスコ デバイスでレベル 2 に設定されている唯一の IS-IS ルーティング プロセス インスタンスの場合だけです。

このコマンドには、Enterprise Services ライセンスが必要です。

例

エリア ルータの指定例を示します。

```
switch(config)# router isis
switch(config-router)# is-type level-2-only
```

関連コマンド

コマンド	説明
<code>feature isis</code>	ルータ上の IS-IS をイネーブルにします。
<code>router isis</code>	IS-IS をイネーブルにします。

isis authentication key-chain

個々の IS-IS インターフェイスに対して IS-IS 認証をイネーブルにするには、**isis authentication key-chain** コマンドを使用します。このような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。

isis authentication key-chain auth-key {level-1 | level-2}

no isis authentication key-chain auth-key {level-1 | level-2}

シンタックスの説明

<i>auth-key</i>	認証キー チェーン
level-1	レベル 1 の Link State Packets (LSP; リンクステート パケット)、Complete Sequence Number Packet (CSNP)、および Partial Sequence Number Packet (PSNP) のみに認証キーを指定します。
level-2	レベル 2 の LSP、CSNP、および PSNP パケットのみに認証キーを指定します。

コマンドのデフォルト

ルータ レベルでは、IS-IS パケットにキー チェーン認証は適用されません。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

isis authentication key-chain コマンドでキー チェーンを設定しないと、キー チェーン認証は実行されません。

キー チェーン認証は、クリア テキスト認証または MD5 認証に適用できます。モードは **authentication mode** コマンドで設定されます。

IS-IS に一度に適用できる認証キー チェーンは 1 つだけです。別の **isis authentication key-chain** コマンドを設定すると、最初の認証キー チェーンは無効になります。

authentication key-chain コンフィギュレーション コマンドを使用すると、IS-IS インスタンスごとにキー チェーン認証を設定できます。

このコマンドには、Enterprise Services ライセンスが必要です。

例

次の例では、特定のインターフェイスに対して、site1 という名前のキーチェーンに属しているすべてのキーの受け入れと送信を実行するように IS-IS が設定されます。

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/5
switch(config-if)# isis authentication key-chain site1 level-1
switch(config-if)#
```

関連コマンド

コマンド	説明
authentication key-chain	IS-IS インスタンス単位で認証をイネーブルにします。
feature isis	ルータ上の IS-IS をイネーブルにします。
router isis	IS-IS をイネーブルにします。

isis authentication-check

インターフェイスから送信される IS-IS パケットのみ（受信パケットは含まれない）に対して認証が実行されるように IS-IS インスタンスを指定するには、**isis authentication-check** コマンドを使用します。ルータ レベルで認証が設定されている場合に、その認証が送信と受信のパケットに実行されるように IS-IS インスタンスを設定するには、このコマンドの **no** 形式を使用します。

authentication-check {level-1 | level-2}

no authentication-check

シンタックスの説明	level-1	level-2
	レベル 1 の送信パケットのみ（受信パケットは含まれない）に認証が実行されるように指定します。	レベル 2 の送信パケットのみ（受信パケットは含まれない）に認証が実行されるように指定します。

コマンドのデフォルト 認証がルータ レベルで設定されている場合、その認証が送信と受信の IS-IS パケットに適用されます。

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

使用上のガイドライン **isis authentication-check** コマンドは、認証モードと認証キー チェーンを設定する前に入力してください。**isis authentication-check** コマンドを入力すると、送信パケットのみに認証が挿入され、受信パケットはチェックされないため、各ルータに許容されるキー設定時間が長くなります。通信しているすべてのルータに **authentication-check** コマンドを入力してから、各ルータに対する認証モードとキーチェーンをイネーブルにします。その後、このコマンドをディセーブルにする場合は、**no isis authentication-check** コマンドを入力します。

このコマンドは、クリア テキスト認証または Message Digest 5 (MD5) 認証に適用できます。モードは **authentication mode** コマンドで設定されます。

authentication-check コンフィギュレーション モード コマンドを使用して、IS-IS インスタンスごとに認証チェックを指定できます。

このコマンドには、Enterprise Services ライセンスが必要です。

例 送信パケットに（受信パケットは含まれない）クリア テキスト認証を使用するように、特定のインターフェイス上の IS-IS レベル 1 パケットを設定する例を示します。

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/5
switch(config-if)# isis authentication-check level-1
switch(config-if)# isis authentication key-chain sitel level-1
switch(config-if)#
```

関連コマンド

コマンド	説明
authentication-check	送信される IS-IS パケットのみ（受信パケットは含まれない）に認証が実行されるように指定します。
feature isis	ルータ上の IS-IS をイネーブルにします。
router isis	IS-IS をイネーブルにします。

isis authentication-type

特定のインターフェイス上の IS-IS パケットで使用される認証タイプを指定するには、**isis authentication-type** コマンドを使用します。クリア テキスト認証に戻すには、このコマンドの **no** 形式を使用します。

isis authentication-type {cleartext | md5} [level-1 | level-2]

no isis authentication-type

シンタックスの説明

cleartext	クリア テキスト認証を指定します。
md5	Message Digest 5 (MD5) 認証を指定します。
level-1	レベル 1 の Link State Packets (LSP; リンクステート パケット)、Complete Sequence Number Packet (CSNP)、および Partial Sequence Number Packet (PSNP) パケットのみに対して、指定された認証をイネーブルにします。
level-2	レベル 2 の LSP、CSNP、および PSNP パケットのみに対して、指定された認証をイネーブルにします。

コマンドのデフォルト

このコマンドを使用しても、ルータ レベルでは、IS-IS パケットに認証は適用されません。

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

サポートされるユーザ ロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

level-1 と **level-2** のいずれのキーワードも入力しないと、そのモードが両方のレベルに適用されます。
authentication-type コンフィギュレーション モード コマンドを使用すると、IS-IS インスタンスごとに認証タイプを設定できます。

このコマンドには、Enterprise Services ライセンスが必要です。

例

特定のインターフェイス上のレベル 1 パケットに対して Message Digest 5 (MD5) 認証が実行されるように、IS-IS インスタンスを設定する例を示します。

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/5
switch(config-if)# isis authentication-type md5 level-1
switch(config-router)#
```

関連コマンド

コマンド	説明
authentication-type	IS-IS インスタンス単位で認証タイプを指定します。
feature isis	ルータ上の IS-IS をイネーブルにします。
router isis	IS-IS をイネーブルにします。

isis circuit-type

隣接関係のタイプを設定するには、**isis circuit-type** コマンドを使用します。回線タイプをレベル 1 とレベル 2 にリセットするには、このコマンドの **no** 形式を使用します。

isis circuit-type {level-1 | level-1-2 | level-2-only}

no isis circuit-type

シンタックスの説明

level-1	レベル 1 隣接関係専用ルータを設定します。
level-1-2	レベル 1 とレベル 2 の隣接関係専用ルータを設定します。
level-2-only	レベル 2 隣接関係専用ルータを設定します。

コマンドのデフォルト

レベル 1 と レベル 2 の隣接関係が確立されます。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドの設定は必須ではありません。level-1-only、level 1-2、または level 2-only のシステムとしてルータを設定することを推奨します。使用されないレベル 1 hello パケットの送出による帯域幅の浪費を避けるために一部のインターフェイスを level-2-only に設定するのは、エリア間ルータ（レベル 1-2 ルータ）だけにしてください。ポイントツーポイント インターフェイスでは、レベル 1 とレベル 2 の hello は同じパケットである点に留意してください。

レベル 1 隣接関係を確立できるのは、このシステムとそのネイバーの間に共通のエリア アドレスが 1 つ以上ある場合です。このインターフェイス上では、レベル 2 隣接関係は確立されません。

レベル 1 とレベル 2 の隣接関係が確立されるのは、ネイバーもレベル 1-2 として設定され、共通のエリアが 1 つ以上ある場合です。共通のエリアがない場合は、レベル 2 隣接関係が確立されます。これはデフォルトです。

他のルータがレベル 2 またはレベル 1-2 ルータで、そのインターフェイスがレベル 1-2 またはレベル 2 に設定されている場合に、レベル 2 隣接関係が確立されます。このインターフェイス上では、レベル 1 隣接関係が確立されません。

このコマンドには、Enterprise Services ライセンスが必要です。

例

次の例では、イーサネット インターフェイス 2/5 上の他のルータが同じエリアにあり、イーサネット インターフェイス 1 上の他のルータは別のエリアにあるため、ルータはレベル 1 hello の送信を停止します。

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/5
switch(config-if)# isis circuit-type level-2-only
switch(config-if)#
```

isis csnp-interval

IS-IS Complete Sequence Number (CSNP) インターバルを設定するには、**isis csnp-interval** 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。

isis csnp-interval seconds {level-1 | level-2}

no isis csnp-interval [level-1 | level-2]

シンタックスの説明

<i>seconds</i>	マルチアクセス ネットワークにおける CSNP の送信インターバル (秒単位)。このインターバルは代表ルータだけに適用されます。範囲は 0 ~ 65535 です。デフォルトは 10 です。
level-1	レベル 1 CSNP 専用の送信インターバルを設定します。
level-2	レベル 2 CSNP 専用の送信インターバルを設定します。

コマンドのデフォルト

デフォルトの設定値は次のとおりです。

- 10 秒
- レベル 1 とレベル 2

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

通常は、このコマンドのデフォルト値を変更する必要はありません。

このコマンドは、代表ルータまたは指定インターフェイスのみに適用されます。データベースの同期を維持するため、代表ルータのみが CSNP パケットを送信します。CSNP インターバルはレベル 1 とレベル 2 で別々に設定できます。

ポイントツーポイント サブインターフェイスに対して **isis csnp-interval** コマンドを使用する場合は、IS-IS mesh-group 機能も使用する必要があります。

このコマンドには、Enterprise Services ライセンスが必要です。

例

30 秒ごとに CSNP を送信するようにインターフェイス Ethernet 2/5 を設定する例を示します。

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/5
switch(config-if)# isis csnp-interval 30 level-1
switch(config-if)#
```

関連コマンド

show isis interface IS-IS 情報を表示します。

isis hello padding

インターフェイス レベルで IS-IS hello パディングを再度イネーブルにするには、**isis hello padding** コマンドを入力します。IS-IS hello パディング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。

isis hello padding

no isis hello padding

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト IS-IS hello パディングはイネーブルです。

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

サポートされるユーザロール ネットワーク 管理者
VDC 管理者

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン IS-IS hello は最大伝送ユニット (maximum transmission unit; MTU) にフル サイズまで埋め込まれます。IS-IS hello をフル MTU に埋め込む利点は、大きなフレームに関連した送信問題によるエラーや隣接インターフェイスの MTU 不一致によるエラーを検出できることです。

両方のインターフェイスの MTU が同じである場合やトランスレーショナルブリッジングの場合には、ネットワーク帯域幅の無駄を省くため、**hello** パディングをディセーブルにできます。**hello** パディングがディセーブルになっても、Cisco ルータは、MTU 不一致検出の利点を維持するため、最初の 5 回の IS-IS hello をフルサイズの MTU に埋め込みます。

特定のインターフェイスの **hello** パディングを選択的にディセーブルにするには、インターフェイス コンフィギュレーション モードで **no isis hello padding** コマンドを入力します。IS-IS ルーティング プロセスに関して、ルータ上のすべてのインターフェイスの **hello** パディングをディセーブルにするには、ルータ コンフィギュレーション モードで **no hello padding** コマンドを入力します。

このコマンドには、Enterprise Services ライセンスが必要です。

例

インターフェイス Ethernet 0/0 に関して、インターフェイス レベルの hello パディングをオフにするには、次のように、インターフェイス コンフィギュレーション モードで **no isis hello padding** コマンドを入力します。

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 0/0
switch(config-if)# no isis hello padding
switch(config-if)#
```

関連コマンド

コマンド	説明
hello padding	ルータ レベルの IS-IS hello パディングを再度イネーブルにします。

isis hello-interval

Cisco NX-OS ソフトウェアから送信される hello パケット間の時間を指定するには、**isis hello-interval** 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。

isis hello-interval seconds {level-1 | level-2}

no isis hello-interval {level-1 | level-2}

シンタックスの説明

seconds hello パケット間の時間長（秒単位）。デフォルトでは、送信される hello パケットで、hello インターバル（*seconds*）の 3 倍の値がホールド時間としてアドバタイズされます（3 の乗数を変更するには、**isis hello-multiplier** コマンドで指定します）。hello インターバルを短くすると、トポロジの変更は迅速に検出されますが、ルーティングトラフィックが増大します。範囲は 0 ～ 65535 です。デフォルトは 10 です。



(注) Designated Intermediate System (DIS) インターフェイスでは、設定値の 3 分の 1 だけしか使用されません。設定された hello インターバルの全体的値が使用されるのは、DIS 以外のインターフェイスだけです。

level-1 レベル 1 専用の hello インターバルを設定します。X.25、Switched Multimegabit Data Service (SMDS)、フレーム リレー マルチアクセス ネットワークでは、これを使用します。

level-2 レベル 2 専用の hello インターバルを設定します。X.25、SMDS、フレーム リレー マルチアクセス ネットワークでは、これを使用します。

コマンドのデフォルト

デフォルトの設定値は次のとおりです。

- 10 秒
- レベル 1 とレベル 2

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

ホールド時間は、hello インターバル × hello 乗数になります。

hello インターバルは、レベル 1 とレベル 2 で別々に設定できます。**level-1** および **level-2** キーワードは、LAN インターフェイス上で使用されます。

hello インターバルを短くすると、コンバージェンスが迅速に実行されますが、帯域幅と CPU 使用率が増大します。また、ネットワークが不安定になることもあります。**hello** インターバルを長くすると、帯域幅と CPU 使用率を節約できます。特に、**hello** インターバルを長くしたうえに、**hello** 乗数を大きくすると、ネットワーク全体の安定性が増します。**DIS** インターフェイスに **hello** インターバルを設定する場合、インターバル値の 3 分の 1 だけしか使用されません。したがって、**DIS** インターフェイスのホールド時間 (**hello** インターバル × **hello** 乗数) も、**DIS** 以外のインターフェイスの 3 分の 1 になります。

ポイントツーポイントインターフェイスの場合は、LAN インターフェイスの場合よりも **hello** インターバルと **hello** 乗数による調整効果があります。

このコマンドには、Enterprise Services ライセンスが必要です。

例

次の例では、5 秒ごとに **hello** パケットをアドバタイズするようにインターフェイス Ethernet 2/3 を設定します。ルータはステーションルータとして動作するように設定されています。この設定では、インターバルを大きい値に設定した場合よりも生成されるトラフィック量は多くなりますが、トポロジの変更は短時間で検出されます。

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/3
switch(config-if)# isis hello-interval 5 level-1
switch(config-if)#
```

関連コマンド

コマンド	説明
isis hello-multiplier	ネイバーで受信されなかったために、ルータで隣接関係のダウンが宣言される IS-IS hello パケット数を指定します。

isis hello-multiplier

ネイバーで受信されなかったために、ルータで隣接関係のダウンが宣言される IS-IS hello パケット数を指定するには、**isis hello-multiplier** 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。

isis hello-multiplier multiplier {level-1 | level-2}

no isis hello-multiplier {level-1 | level-2}

シンタックスの説明

<i>multiplier</i>	整数値。範囲は 3 ~ 1000 です。デフォルトは 3 です。
level-1	レベル 1 隣接関係専用の hello 乗数を設定します。
level-2	レベル 2 隣接関係専用の hello 乗数を設定します。

コマンドのデフォルト

デフォルトの設定値は次のとおりです。

- *multiplier* : 3
- レベル 1 とレベル 2

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

IS-IS hello パケットで伝送される「保持時間」によって、ネイバーがダウンとして宣言される前に次の hello パケットを待機する時間が決定されます。この値によって、障害状態のリンクやネイバーの検出とルート再計算にかかる時間が決まります。IS-IS hello パケットでアドバタイズされるホールド時間は、hello インターバルに hello 乗数を掛けた値に設定されます。アドバタイズされたホールド時間中に IS-IS hello パケットが受信されなかった場合は、ネイバーがこのルータとの隣接関係がダウンしていると宣言します。ホールド時間（つまり、hello 乗数と hello インターバル）はインターフェイス単位で設定できます。また、1 つのエリア内のルータごとに別々のホールド時間を設定できます。

hello 乗数を小さくすると、コンバージェンスが高速になりますが、ルーティングが不安定になる可能性があります。必要に応じて、ネットワークの安定性を高めるために hello 乗数の値を大きくしてください。hello 乗数をデフォルトの 3 未満の値に設定しないでください。

hello パケットが頻繁に失われ、IS-IS の隣接関係が不必要に障害状態になる場合は、**isis hello-multiplier** コマンドを使用してください。hello 乗数を大きくして、hello インターバルを短くすると (**isis hello-interval** コマンド)、リンク障害検出の所要時間を伸ばすことなく、hello プロトコルの信頼性を高めることができます。

ポイントツーポイントリンクでは1つのhelloだけでレベル1とレベル2の両方に対応できるため、異なるhello乗数を設定できるのはイーサネットやFDDIのようなマルチアクセスネットワークの場合だけです。X.25、Frame Relay、ATMなどのマルチポイントモードのNonbroadcast Multizccess (NBMA) ネットワークでは、レベル1とレベル2に別々のhelloパケットも送信されます。ただし、IS-ISはWAN NBMAメディアを通じたポイントツーポイントサブインターフェイスで実行することを推奨します。

このコマンドには、Enterprise Services ライセンスが必要です。

例

次の例では、ネットワーク管理者は、隣接関係がダウンするのは、多数（10）のhelloパケットが非受信になった場合だけにして、ネットワークの安定性を高めたいと考えています。リンク障害の検出にかかる総時間は60秒です。この設定では、ネットワークは安定した状態になりますが、リンクは完全に輻輳します。

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 2/3
switch(config-if)# ip router isis
switch(config-if)# isis hello-interval 6 level-1
switch(config-if)# isis hello-multiplier 10 level-1
```

関連コマンド

コマンド	説明
isis hello-interval	Cisco NX-OS ソフトウェアによる hello パケットの送信インターバルを指定します。

isis lsp-interval

連続する IS-IS LSP 間の時間遅延を設定するには、**isis lsp-interval** 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。

isis lsp-interval *milliseconds*

no isis lsp-interval

シンタックスの説明	<i>milliseconds</i> 後続の LSP（ミリ秒）との間の遅延時間。範囲は 10 ～ 65535 です。
------------------	---

コマンドのデフォルト	デフォルトの遅延時間は 33 ミリ秒です。
-------------------	-----------------------

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
----------------	----------------------

サポートされるユーザロール	ネットワーク管理者 VDC 管理者
----------------------	----------------------

コマンドの履歴	リリース	変更内容
	4.0(1)	このコマンドが追加されました。

使用上のガイドライン	IS-IS ネイバーやインターフェイスの数が多いたポロジでは、LSP の送受信による CPU 負荷によってルータに問題が生じることがあります。このコマンドを使用すると、LSP の送信レート（および他のシステムの受信レート）を削減できます。
-------------------	---

このコマンドには、Enterprise Services ライセンスが必要です。

例	次の例では、システムがインターフェイス Ethernet 0/0 で LSP を 100 ミリ秒ごとに送信するように（1 秒あたり 10 パケット）設定します。
----------	--

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 0/0
switch(config-if)# isis lsp-interval 100
```

関連コマンド	コマンド	説明
	isis retransmit-interval	ポイントツーポイントリンクでの各 LSP（IS-IS リンクステート PDU）の再送信間隔を設定します。

isis mesh-group

高メッシュのポイントツーポイント トポロジを伴う NonBroadcast Multiaccess (NBMA) ネットワークで LSP フラッドイングを最適化するには、**isis mesh-group** コマンドを使用します。メッシュグループからサブインターフェイスを削除するには、このコマンドの **no** 形式を使用します。

isis mesh-group {*number* | **blocked**}

no isis mesh-group {*number* | **blocked**}

シンタックスの説明

number	このインターフェイスがメンバーとして属しているメッシュグループの識別番号。範囲は 1 ~ 4294967295 です。
blocked	このサブインターフェイスでは LSP フラッドイングが実行されないように指定します。

コマンドのデフォルト

インターフェイスは通常のフラッドイングを実行します。

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

メッシュグループに属していないサブインターフェイスで最初に受信された LSP は通常、他のすべてのサブインターフェイスにフラッドイングされます。

メッシュグループに属しているサブインターフェイスで最初に受信された LSP は同じメッシュグループ内のインターフェイスを除くすべてのインターフェイスにフラッドイングされます。サブインターフェイスに **blocked** キーワードを入力すると、新しく受信された LSP は、そのインターフェイスからフラッドイングされません。

不完全なフラッドイングの可能性を最小限に抑えるためには、無制限のフラッドイングを許可するのはメッシュ内の最小限のリンクだけにする必要があります。すべての物理パスをカバーするような論理リンクの最小セットを選択すると、フラッドイングは非常に少なくなります。ロバストネスが低下しませんが、LSP フラッドイングによってスケーリング パフォーマンスが阻害されず、しかも最大の障害時にも、ネットワークの他の部分から論理的に切断されるルータがないように、必要十分なリンクだけを選択できれば理想的です。つまり、すべてのリンクのフラッドイングをブロックすれば、スケーリング パフォーマンスは最高になりますが、フラッドイングはまったく生じなくなります。すべてのリンクでフラッドイングを許可すると、スケーリング パフォーマンスが大きく低下します。

このコマンドには、Enterprise Services ライセンスが必要です。

例

3つのメッシュグループ内の6つのインターフェイスを設定する例を示します。受信されたLSPは次のように処理されます。

- 最初に Ethernet 1/0.1 を通じて受信された LSP は、Ethernet 1/0.2 (同じメッシュグループ内) と Ethernet 1/2.1 (ブロックされている) を除くすべてのインターフェイスにフラッドイングされます。
- 最初に Ethernet 1/1.2 を通じて受信された LSP は、Ethernet 1/1.1 (同じメッシュグループ内) と Ethernet 1/2.1 (ブロックされている) を除くすべてのインターフェイスにフラッドイングされます。
- 最初に Ethernet 1/2.1 を通じて受信された LSP は無視されず、通常どおりすべてのインターフェイスにフラッドイングされます。最初に Ethernet 1/2.2 を通じて受信された LSP は、Ethernet 1/2.1 (ブロックされている) を除くすべてのインターフェイスにフラッドイングされます。

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 1/0.1
switch(config-if)# isis mesh-group 10
```

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 1/0.2
switch(config-if)# isis mesh-group 10
```

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 1/1.1
switch(config-if)# isis mesh-group 11
```

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 1/1.2
switch(config-if)# isis mesh-group 11
```

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 1/2.1
switch(config-if)# isis mesh-group blocked
```

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 1/2.2
switch(config-if)# isis mesh-group 12
```

関連コマンド

コマンド	説明
router isis	IS-IS ルーティング プロトコルをイネーブルにして、IS-IS プロセスを指定します。

isis metric

IS-IS メトリックの値を設定するには、**isis metric** 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。

```
isis metric metric-value {level-1 | level-2}
```

```
no isis metric metric-value {level-1 | level-2}
```

シンタックスの説明

<i>metric-value</i>	リンクに指定されたメトリック。このメトリックは、このリンクを通じてネットワーク内の他の各ルータからその他の宛先へのコストの計算に使用されます。レベル 1 またはレベル 2 のルーティングに対してこのメトリックを設定できます。範囲は 1 ~ 16777215 です。デフォルトは 10 です。
<i>maximum</i>	SPF 計算からリンクまたは隣接関係を除外します。
level-1	レベル 1 (エリア内) ルーティングの SPF 計算のみにこのメトリックが使用されるように指定します。オプションのキーワードを指定しないと、レベル 1 とレベル 2 のルーティングに対してメトリックがイネーブルになります。
level-2	レベル 2 (エリア間) ルーティングの SPF 計算のみにこのメトリックが使用されるように指定します。レベルを指定しないと、レベル 1 とレベル 2 のルーティングに対してメトリックがイネーブルになります。

コマンドのデフォルト

デフォルトのメトリック値は 10 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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

level-1 または **level-2** のキーワードを指定すると、レベル 1 またはレベル 2 のそれぞれのルーティングに対してだけメトリックがリセットされます。

すべてのインターフェイスにメトリックを設定することを推奨します。メトリックを設定しないインターフェイスがあると、IS-IS メトリックはホップカウント メトリックと同様になります。

Link-State Packet (LSP) での IPv4 情報のアドバタイズに使用される TLV は拡張メトリックのみを使用するように定義されるので、**metric-style wide** コマンドを使用して、IS-IS が新形式の Type-Length-Value (TLV) を使用するように設定することを推奨します。Cisco NX-OS ソフトウェアは、24 ビットメトリック フィールドをサポートしています。24 ビットメトリック フィールドは **ワイドメトリック** と呼ばれています。新しいメトリック形式を使用すると、リンク メトリックの最大値は 16777215、総パスメトリックは 4261412864 になります。

このコマンドには、Enterprise Services ライセンスが必要です。

例

インターフェイス Ethernet 3/2 に対して、level 1 のリンクステート メトリック コストを 15 に設定する例を示します。

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 3/2
switch(config-if)# isis metric 15 level-1
```

関連コマンド

コマンド	説明
metric-style wide	IS-IS を実行中のルータが新形式の TLV のみを生成、受信するように設定します。

isis passive

インターフェイス上の隣接関係の形成を抑制しながら、インターフェイスに関連付けられたプレフィクスをアドバタイズするには、**isis passive** コマンドを使用します。抑制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。

isis passive {level-1 | level-1-2 | level-2-only}

no isis passive {level-1 | level-1-2 | level-2-only}

シンタックスの説明

level-1	レベル 1 PDU のみを抑制します。
level-1-2	レベル 1 とレベル 2 の PDU を抑制します。
level-2-only	レベル 2 PDU のみを抑制します。

デフォルト

デフォルトの設定値は次のとおりです。

- このコマンドは、デフォルトではディセーブルです。
- イネーブルにした場合のデフォルトは **level-1-2** 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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ループバック インターフェイス上では必要ありません。 **ip router isis** コマンドは、ループバック インターフェイス上のインターフェイス コンフィギュレーション モードで、そのインターフェイスと IS-IS インスタンスを関連付けるために使用します。

このコマンドには、Enterprise Services ライセンスが必要です。

例

レベル 1 でイーサネット インターフェイス 3/2 の隣接関係を抑制する例を示します。

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 3/2
switch(config-if)# isis passive level-1
```

isis priority

代表ルータのプライオリティを設定するには、インターフェイス コンフィギュレーション モードで **isis priority** コマンドを使用します。デフォルトのプライオリティにリセットするには、このコマンドの **no** 形式を使用します。

isis priority *number-value* [**level-1** | **level-2**]

no isis priority [**level-1** | **level-2**]

シンタックスの説明

<i>number-value</i>	ルータのプライオリティを 0 ～ 127 の数値で設定します。デフォルト値は 64 です。
level-1	(任意) レベル 1 専用のプライオリティを設定します。
level-2	(任意) レベル 2 専用のプライオリティを設定します。

デフォルト

64 のプライオリティ
レベル 1 とレベル 2

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

サポートされるユーザロール

ネットワーク管理者
VDC 管理者

コマンドの履歴

リリース	変更内容
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

プライオリティはレベル 1 とレベル 2 で別々に設定できます。**level-1** または **level-2** キーワードを指定すると、レベル 1 またはレベル 2 のそれぞれのルーティングのプライオリティだけがリセットされます。

プライオリティ値は、LAN 上の代表ルータまたは Designated Intermediate System (DIS) を決める際に使用されます。プライオリティは hello パケットでアドバタイズされます。プライオリティが最高のルータが DIS になります。

Intermediate System-to-Intermediate System (IS-IS) では、バックアップ代表ルータはありません。プライオリティを 0 に設定すると、そのシステムが DIS になる可能性は低くなりますが、完全には回避できません。プライオリティの高いルータがオンラインになると、現在の DIS からその役割を引継ぎます。プライオリティ値が同一の場合は、MAC アドレス値が高いルータが優先されます。

このコマンドには、Enterprise Services ライセンスが必要です。

例

次に、プライオリティ レベルを 80 に設定することによって、レベル 1 ルーティングにプライオリティを設定する例を示します。このルータは、DIS になっている可能性があります。

```
switch(config)# router isis test1
switch(config-router)# interface ethernet 3/2
switch(config-if)# isis priority 80 level-1
```