P コマンド

ここでは、[P] から始まる 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。

platform ip verify

IP パケット検証を設定するには、**platform ip verify** 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。

platform ip verify {**checksum** | **fragment** | **tcp tiny-frag** | **version**}

no platform ip verify {**checksum** | **fragment**}

シンタックスの説明

checksum	チェックサムが正しくない場合には、IPv4 または IPv6 パケットをドロップします。
fragment	パケット フラグメントのオフセットがゼロ以外で DF ビットがアクティブの場合には、IPv4 または IPv6 パケットをドロップします。
tcp tiny-frag	IP フラグメント オフセットが 1 の場合、または IP フラグメント オフセットが 0 で IP ペイロード長が 16 未満の場合には、IPv4 パケットをドロップします。
version	ethertype が 4（IPv4）にセットされていない場合には、IPv4 パケットをドロップします。

デフォルト

すべてのアドレス テストがイネーブルです。

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

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

チェックサムまたはフラグメントに基づいた IPv4 および IPv6 パケットのパケット検証テストを設定するには、**platform ip verify** 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

次に、フラグメントされた IPv4 または IPv6 パケットをドロップする例を示します。

```
switch(config)# platform ip verify fragment
```

関連コマンド

コマンド	説明
platform ip verify address	アドレスに基づいた IPv4 および IPv6 パケット検証チェックを設定します。
platform ip verify length	長さに基づいた IPv4 パケット検証チェックを設定します。
platform ipv6 verify	IPv6 パケット検証を設定します。
show hardware forwarding ip verify	IP パケット検証チェックに関する情報を表示します。

platform ip verify address

IP アドレスによるパケット検証を設定するには、**platform ip verify 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。

platform ip verify address {**destination zero** | **identical** | **reserved** | **source** {**broadcast** | **multicast**}}

no platform ip verify address {**destination zero** | **identical** | **reserved** | **source** {**broadcast** | **multicast**}}

シンタックスの説明

destination zero	IPv4 宛先アドレスが 0.0.0.0 または IPv6 宛先アドレスが ::... の場合には、IP パケットをドロップします。
identical	IPv4 または IPv6 発信元アドレスが IPv4 または IPv6 宛先アドレスと同じ場合には、IP パケットをドロップします。
reserved	IPv4 アドレスが 127.x.x.x の範囲にある場合、または IPv6 アドレスが ::1 の範囲にある場合には、IP パケットをドロップします。
source	IP 発信元アドレスに基づいて IP パケットをドロップします。
broadcast	IP 発信元アドレスが 255.255.255.255 の場合には、IP パケットをドロップします。
multicast	IPv4 発信元アドレスが 224.x.x.x の範囲にある場合、または IPv6 発信元アドレスが FF00::/8 の範囲にある場合には、IP パケットをドロップします。

デフォルト

すべてのアドレス テストがイネーブルです。

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

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

アドレスに基づいた IPv4 および IPv6 パケットのパケット検証テストを設定するには、**platform ip verify 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

次に、IPv4 または IPv6 ブロードキャスト パケットをドロップする例を示します。

```
switch(config)# platform ip verify address source broadcast
```

関連コマンド

コマンド	説明
platform ip verify	チェックサムまたはフラグメントに基づいた IPv4 および IPv6 パケット検証チェックを設定します。
platform ip verify length	長さに基づいた IPv4 パケット検証チェックを設定します。
platform ipv6 verify	IPv6 パケット検証を設定します。
show hardware forwarding ip verify	IP パケット検証チェックに関する情報を表示します。

platform ip verify length

パケット長に基づいた IPv4 パケット検証を設定するには、**platform ip verify length** 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。

platform ip verify length {**consistent** | **maximum** {**max-frag** | **max-tcp** | **udp**} | **minimum**}

no platform ip verify length {**consistent** | **maximum** {**max-frag** | **max-tcp** | **udp**} | **minimum**}

シンタックスの説明

consistent	イーサネット フレーム サイズが、IP パケット長にイーサネット ヘッダーを加えた値以上の場合には、IPv4 パケットをドロップします。
maximum {**max-frag** | **max-tcp** | **udp**}	次の条件に基づいて IPv4 パケットをドロップします。 • **max-frag —** 最大フラグメント オフセットが 65536 より大きい場合には、IP パケットをドロップします。 • **max-tcp —** TCP 長が IP ペイロード長より大きい場合には、IP パケットをドロップします • **udp —** IP ペイロード長が UDP パケット長を下回る場合には、IP パケットをドロップします。
minimum	イーサネット フレーム長が IP パケット長に 4 オクテット（CRC 長）を加えた値を下回る場合には、IP パケットをドロップします。

デフォルト

すべてのアドレス テストがイネーブルです。

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

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

パケット長に基づいた IPv4 および IPv6 パケットのパケット検証テストを設定するには、**platform ip verify length** 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

次に、最小長の IPv4 パケットをドロップする例を示します。

```
switch(config)# platform ip verify length minimum
```

関連コマンド

コマンド	説明
platform ip verify	チェックサムまたはフラグメントに基づいた IPv4 パケット検証チェックを設定します。
platform ip verify address	アドレスに基づいた IPv4 および IPv6 パケット検証チェックを設定します。
platform ipv6 verify	IPv6 パケット検証を設定します。
show hardware forwarding ip verify	IP パケット検証チェックに関する情報を表示します。

platform ipv6 verify

IPv6 パケット検証を設定するには、**platform ipv6 verify** 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。

platform ipv6 verify {**length** {**consistent** | **maximum** {**max-frag** | **max-tcp** | **udp**} | **tcp tiny-frag** | **version**}

no platform ip verify {**checksum** | **fragment**}

シンタックスの説明

length	長さに基づいて IPv6 パケットをドロップします。
consistent	イーサネット フレーム サイズが、IPv6 パケット長にイーサネット ヘッダーを加えた値以上の場合には、IPv6 パケットをドロップします。
maximum {**max-frag** | **max-tcp** | **udp**}	次の条件に基づいて IPv6 パケットをドロップします。 • **max-frag —** 計算式（IPv6 ペイロード長 – IPv6 拡張ヘッダー バイト数）+（フラグメント オフセット ÷ 8）の値が 65536 より大きい場合には、IPv6 パケットをドロップします。 • **max-tcp —** TCP 長が IP ペイロード長より大きい場合には、IPv6 パケットをドロップします • **udp —** IP ペイロード長が UDP パケット長を下回る場合には、IPv6 パケットをドロップします。
tcp tiny-frag	IP フラグメント オフセットが 1 の場合、または IPv6 フラグメント オフセットが 0 で IPv6 ペイロード長が 16 未満の場合には、IPv4 パケットをドロップします。
version	ethertype が 6（IPv6）にセットされていない場合には、IPv6 パケットをドロップします。

デフォルト

すべてのアドレス テストがイネーブルです。

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

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

IPv6 パケットによるパケット検証テストを設定するには、**platform ipv6 verify** 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

次に、すべての IPv4 パケットをドロップする例を示します。

```
switch(config)# platform ipv6 verify version
```

関連コマンド

コマンド	説明
platform ip verify address	アドレスに基づいた IPv4 および IPv6 パケット検証チェックを設定します。
platform ip verify length	長さに基づいた IPv4 パケット検証チェックを設定します。
show hardware forwarding ip verify	IP パケット検証チェックに関する情報を表示します。

policy statistics enable（OSPFv3）

OSPF バージョン 3（OSPFv3）ポリシー統計情報をイネーブルにするには、**policy statistics enable** コマンドを使用します。ポリシー統計情報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。

policy statistics enable

no policy statistics enable

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

ポリシー統計情報はディセーブルです。

コマンド モード

ルータ 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

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

この OSPFv3 インスタンスに適用されるルート ポリシーに基づいた統計情報の収集をイネーブルにするには、**policy statistics enable** 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、OSPFv3 2 に関して収集するポリシー統計情報をイネーブルにする例を示します。

```
switch(config)# ospfv3 2
switch(config-router)# policy statistics enable
```

関連コマンド

コマンド	説明
show ospfv3 policy statistics	ポリシー統計情報を表示します。

preempt（GLBP）

現在の Active Virtual Gateway（AVG; アクティブ バーチャル ゲートウェイ）よりプライオリティの高いゲートウェイがある場合、そのゲートウェイが Gateway Load Balancing Protocol（GLBP）グループの AVG を引き継ぐように設定するには、**glbp preempt** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

preempt [**delay minimum** *seconds* | ***sync*** *seconds*]

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

シンタックスの説明

delay minimum *seconds*	（任意）ゲートウェイが AVG の役割を引き継ぐ前の、ゲートウェイの最小遅延時間を秒数で指定します。範囲は 0 ～ 3600 秒です。デフォルトの遅延時間は 30 秒です。
sync *seconds*	（任意）ゲートウェイが同期の完了するのを待つ時間を秒数で指定します。有効範囲は 0 ～ 3600 秒です。

デフォルト

現在の AVG より高いプライオリティを持つ GLBP ゲートウェイが、AVG の役割を引き継ぐことができません。
デフォルトの遅延時間は 30 秒です。

コマンド モード

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

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにはライセンスは必要ありません。

例

次に、ルータのプライオリティが 254 で、現在の AVG より高い場合に、そのルータが現在の AVG に対してプリエンプションを行うように設定する例を示します。この場合、AVG の役割を引き継ぐ前に 60 秒間待ちます。

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

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を開始し、GLBP グループを作成します。
priority	GLBP グループ内のルータのプライオリティ レベルを設定します。

preempt（HSRP）

プリエンプション遅延を設定するには、**preempt** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

preempt [**delay** {**minimum** *min-delay* | ***reload*** *rel-delay* | **sync** *sync-delay*}]

no preempt [**delay** {**minimum** *min-delay* | ***reload*** *rel-delay* | **sync** *sync-delay*}]

シンタックスの説明

delay minimum *min-delay*	（任意）ルータがアクティブになる前にルーティング テーブルの更新が行われるよう、プリエンプションを遅らせる最小時間。デフォルトは 0 です。
reload *rel-delay*	（任意）ルータのリロード後の遅延時間。この時間は、ルータのリロード後の最初のインターフェイス起動イベントにのみ適用されます。デフォルトは 0 です。
sync *seconds*	（任意）IP 冗長性クライアントがプリエンプションを妨げることができる最小時間を秒数で指定します。この時間が経過すると、IP 冗長性クライアントの状態とは無関係にプリエンプションが発生します。デフォルトは 0 です。

デフォルト

デフォルトの遅延時間はどのオプションも 0 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または HSRP テンプレート 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

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにはライセンスは必要ありません。

ルータがアクティブになる前にルーティング テーブルの更新が行われるよう、最小遅延時間を指定します。ルータが最初に起動したとき、ルータのルーティング テーブルは完全ではありません。高いプライオリティのルータが低いプライオリティのアクティブ ルータから hello パケットを最初に受信した場合、高いプライオリティのルータはプリエンプションを遅らせるだけであることに注意してください。高いプライオリティのルータが起動したときに、低いプライオリティのアクティブ ルータから hello パケットを受信しなかった場合、グループのアクティブ ルータが存在していないとみなされて、高いプライオリティのルータはただちにアクティブになります。

例

次に、プライオリティが 110 のルータがアクティブになるときの遅延を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 0/1
switch(config-if)# ip address 10.0.0.1 255.255.255.0
switch(config-if)# hsrp 4
switch(config-if-hsrp)# priority 110
switch(config-if-hsrp)# preempt
switch(config-if-hsrp)# authentication text sanjose
switch(config-if-hsrp)# ip 10.0.0.3
switch(config-if-hsrp)# end
```

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。

preempt（VRRP）

高いプライオリティのバックアップ仮想ルータによる低いプライオリティのマスター仮想ルータに対するプリエンプションをイネーブルにするには、**preempt** コマンドを使用します。高いプライオリティのバックアップ仮想ルータによる低いプライオリティのマスター仮想ルータに対するプリエンプ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。

preempt

no preempt

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 イネーブル

コマンド モード VRRP 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 スーパーユーザ
VDC 管理者

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）を使用すると、故障した仮想ルータ マスターを引き継いだ仮想ルータ バックアップを、使用可能になった高いプライオリティの仮想ルータ バックアップでプリエンプションすることができます。

デフォルトでは、プリエンプション スキームがイネーブルです。使用可能になる高いプライオリティのバックアップ仮想ルータは、仮想ルータ マスターになるように選出されていたバックアップ仮想ルータを引き継ぎます。プリエンプションをディセーブルにした場合、仮想ルータ マスターになるように選出されているバックアップ仮想ルータは、元の仮想ルータ マスターが回復して再びマスターになるまでマスターであり続けます。

仮想 IP アドレスがインターフェイスの IP アドレスでもある場合には、プリエンプションが適用されます。

このコマンドの使用にはライセンスは必要ありません。

例

次に、高いプライオリティのバックアップ仮想ルータによる低いプライオリティのマスター仮想ルータに対するプリエンプションをイネーブルにする例を示します。

（注） このプリエンプションは、プライマリ IP アドレスには適用されません。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# vrrp 250
switch(config-if-vrrp)# preempt
```

関連コマンド

コマンド	説明
show vrrp	VRRP 設定情報を表示します。
clear vrrp	指定の仮想ルータの全ソフトウェア カウンタを消去します。

priority（GLBP）

Gateway Load Balancing Protocol（GLBP）グループ内のゲートウェイのプライオリティ レベルを設定するには、**priority** コマンドを使用します。ゲートウェイのプライオリティ レベルを削除するには、このコマンドの **no** 形式を使用します。

priority *level*

no priority

シンタックスの説明

level	GLBP グループ内のゲートウェイのプライオリティ。範囲は 1 ～ 255 で、デフォルトは 100 です。

デフォルト

level：100

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

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

Active Virtual Gateway（AVG; アクティブ バーチャル ゲートウェイ）になる仮想ゲートウェイを制御するには、**priority** コマンドを使用します。GLBP は、GLBP グループ内のすべての仮想ゲートウェイのプライオリティを比較し、数値的に最も高いプライオリティを持つゲートウェイを AVG として選択します。2 つの仮想ゲートウェイのプライオリティが等しい場合、GLBP は最も高い IP アドレスを持つゲートウェイを選択します。

このコマンドにはライセンスは必要ありません。

例

次に、仮想ゲートウェイをプライオリティ 254 に設定する例を示します。

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

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を開始し、GLBP グループを作成します。
preempt	現在の AVG よりプライオリティの高いゲートウェイがある場合、そのゲートウェイが GLBP グループの AVG を引き継ぐように設定します。

priority（HSRP）

Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）グループ内のプライオリティ レベルを設定するには、**priority** コマンドを使用します。プライオリティ レベルを削除するには、このコマンドの **no** 形式を使用します。

priority *level*

no priority

シンタックスの説明

level	仮想ルータのインターフェイス プライオリティ。値の範囲は 1 ～ 255 です。このルータが IP アドレスのオーナーである場合には、値は自動的に 255 に設定されます。デフォルトは 100 です。

デフォルト

level：100

コマンド モード

HSRP コンフィギュレーションまたは HSRP テンプレート 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

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

アクティブ ルータになる仮想ルータを制御するには、**priority** コマンドを使用します。HSRP は、HSRP グループ内のすべての仮想ルータのプライオリティを比較し、数値的に最も高いプライオリティを持つルータを選択します。2 つの仮想ルータのプライオリティが等しい場合、HSRP は最も高い IP アドレスを持つルータを選択します。

このコマンドにはライセンスは必要ありません。

例

次に、仮想ルータをプライオリティ 254 に設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 0/1
switch(config-if)# ip address 10.0.0.1 255.255.255.0
switch(config-if)# hsrp 4
switch(config-if-hsrp)# priority 254
```

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。

priority（VRRP）

Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）のプライオリティを設定するには、**priority** 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。

priority *value*

no priority

シンタックスの説明

value	仮想ルータのインターフェイス プライオリティ。値の範囲は 1 ～ 255 です。このルータが IP アドレスのオーナーである場合には、値は自動的に 255 に設定されます。

デフォルト

デフォルトの値は 100 です。スイッチのインターフェイスの IP アドレスがプライマリ仮想 IP アドレスと同じ場合、そのスイッチのデフォルト値は 255 です。

コマンド モード

VRRP 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

スーパーユーザ
VDC 管理者

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このプライオリティでは、VRRP ルータが仮想ルータ バックアップとして機能するかどうかや、仮想ルータ マスターの障害が発生した場合に VRRP ルータが仮想ルータ マスターになる優先順位、各 VRRP の役割、および仮想ルータ マスターの障害が発生した場合の動作が決定されます。

VRRP ルータが仮想ルータの IP アドレスと物理インターフェイスの IP アドレスのオーナーである場合には、このルータが仮想ルータ マスターとして機能します。

デフォルトでは、プリエンプション スキームがイネーブルです。使用可能になる高いプライオリティのバックアップ仮想ルータは、仮想ルータ マスターになるように選出されていたバックアップ仮想ルータを引き継ぎます。プリエンプションをディセーブルにした場合、仮想ルータ マスターになるように選出されているバックアップ仮想ルータは、元の仮想ルータ マスターが回復して再びマスターになるまでマスターであり続けます。

このコマンドの使用にはライセンスは必要ありません。

例

次に、仮想ルータのプライオリティを指定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# vrrp 250
switch(config-if-vrrp)# priority 2
```

関連コマンド

コマンド	説明
feature vrrp	VRRP をイネーブルにします。
show vrrp	VRRP 設定情報を表示します。

protocol shutdown（OSPF）

OSPF インスタンスをシャットダウンするには、**protocol shutdown** 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。

protocol shutdown

no protocol shutdown

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 インスタンスは、設定されるとデフォルトでイネーブルです。

コマンド モード

ルータ コンフィギュレーション
ルータ 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

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

設定を削除しないで OSPF のインスタンスをディセーブルに設定するには、**protocol 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

次に、OSPF 209 をディセーブルにする例を示します。

```
switch(config) router ospf 209
switch(config-router)# protocol shutdown
```

protocol shutdown（OSPFv3）

OSPF バージョン 3（OSPFv3）インスタンスをシャットダウンするには、**protocol shutdown** 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。

protocol shutdown

no protocol shutdown

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

OSPFv3 インスタンスは、設定されるとデフォルトでイネーブルです。

コマンド モード

ルータ コンフィギュレーション
ルータ 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

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

設定を削除しないで OSPFv3 のインスタンスをディセーブルに設定するには、**protocol 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

次に、OSPFv3 209 をディセーブルにする例を示します。

```
switch(config) router ospfv3 209
switch(config-router)# protocol shutdown
```