



## I コマンド

---

この章では、I で始まる Cisco Nexus 1000V コマンドについて説明します。

# id

テナント ID にネットワーク セグメンテーション ポリシーを関連付けるには、**id** コマンドを使用します。

**id** *isolation\_id*

## 構文の説明

*isolation\_id* ネットワーク セグメンテーション ポリシーのテナント ID。

## デフォルト

なし

## コマンドモード

ネットワーク セグメント ポリシー コンフィギュレーション (config-network-segment-policy)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.2(1)SV1(5.1)	このコマンドが追加されました。

## 使用上のガイドライン

テナント ID は vCloud Director の Organization UUID と相互に関連付けられ、いったん設定されると変更できません。

## 例

次に、ネットワーク セグメンテーション ポリシーをテナント ID と関連付ける例を示します。

```
n1000v# configure terminal
n1000v(config)# network-segment policy abc-policy-vxlan
n1000v(config-network-segment-policy) #id f5dcf127-cdb0-4bdd-8df5-9515d6dc8170
```

## 関連コマンド

コマンド	説明
<b>network-segment policy</b>	ネットワーク セグメンテーション ポリシーを作成します。
<b>show run network-segment policy</b>	ネットワーク セグメンテーション ポリシー設定を表示します。

# inherit port-profile

デフォルトの設定として新しいポート プロファイルに継承される設定を追加するには、**inherit port-profile** コマンドを使用します。継承されるポリシーを削除するには、このコマンドの **no** 形式を使用します。

**inherit port-profile** *name*

**no inherit port-profile**

## 構文の説明

<i>name</i>	ポリシーが継承されるポート プロファイルの名前。ポート プロファイルには最大 80 文字の名前を設定できます。ポート プロファイル名は、Cisco Nexus 1000V 上の各ポート プロファイルに対して一意である必要があります。
-------------	--

## デフォルト

なし

## コマンド モード

ポート プロファイル コンフィギュレーション (config-port-prof)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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

継承される設定は、ポート プロファイル タイプを除き、いずれも CLI を使用して変更できます。このコマンドの **no** 形式を使用すると、ポート プロファイルの設定は、ポート プロファイル タイプと継承される設定から明示的に独立して設定された設定を除き、デフォルトに戻ります。

## 例

次に、ポリシーが継承されるポート プロファイルとして *AllAccess1* を指定する例を示します。

```
n1000v# config t
n1000v(config)# port-profile type vethernet AllAccess2
n1000v(config-port-prof)# inherit port-profile AllAccess1
```

次に、継承されるポリシーを削除する例を示します。

```
n1000v# config t
n1000v(config)# port-profile type vethernet AllAccess2
n1000v(config-port-prof)# no port-profile inherit
```

## 関連コマンド

コマンド	説明
<b>show port-profile</b>	現在のポート プロファイルによって継承されるポート プロファイルを表示します。
<b>port-profile</b>	ポート プロファイル コンフィギュレーション モードを開始して、ポート プロファイルを定義します。

# install certificate

証明書をインストールするには、**install certificate** コマンドを使用します。証明書を削除するには、このコマンドの **no** 形式を使用します。

```
install certificate {bootflash: | default}
```

```
no install certificate
```

## 構文の説明

<b>bootflash:</b>	パスを指定します。
<b>default</b>	デフォルトの証明書を指定します。

## デフォルト

証明書はインストールされていません。

## コマンドモード

SVS 接続コンフィギュレーション (config-svs-conn)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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

作成できる SVS 接続は 1 つだけです。

## 例

次に、証明書をインストールする例を示します。

```
n1000v# configure terminal
n1000v(config)# svcs connect s1
n1000v(config-svs-conn)# install certificate default
n1000v(config-svs-conn)#
```

次に、証明書を削除する例を示します。

```
n1000v# configure terminal
n1000v(config)# svcs connect s1
n1000v(config-svs-conn)# no install certificate default
n1000v(config-svs-conn)#
```

## 関連コマンド

コマンド	説明
<b>show svcs</b>	SVS 情報を表示します。

# install license bootflash:

VSM にライセンス ファイルをインストールするには、**install license bootflash:** コマンドを使用します。

**install license bootflash:** *filename*

## 構文の説明

*filename* (任意) ライセンス ファイルの名前を指定します。名前を指定しないと、ライセンスはデフォルトの名前を使用してインストールされます。

## デフォルト

なし

## コマンドモード

任意

## サポートされるユーザロール

ネットワーク管理者  
ネットワーク オペレータ

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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

- 評価ライセンスが VSM にインストールされている場合は、最初にそれをアンインストールする必要があります。詳細については、『*Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。
- アクティブな VSM コンソール ポートにログインする必要があります。
- このコマンドでは、**license\_file.lic** という名前を使用してライセンス ファイルがインストールされます。異なる名前を指定することもできます。
- 同じ VSM に複数のライセンスをインストールする場合は (ライセンス スタッキングとも呼ばれます)、各ライセンス キー ファイルの名前が一意であることを確認してください。
- VSM にインストールする (スタックする) 追加のライセンス ファイルごとに、この手順を繰り返します。

## 例

次に、ライセンスを VSM のブートフラッシュにインストールした後、インストールされているファイルを表示する例を示します。

```
n1000v# install license bootflash:license_file.lic
Installing license ..done
n1000v# show license file license.lic
SERVER this_host ANY
VENDOR cisco
INCREMENT NEXUS1000V_LAN_SERVICES_PKG cisco 1.0 permanent 1 \
  HOSTID=VDH=1575337335122974806 \
  NOTICE="<LicFileID>license.lic</LicFileID><LicLineID>0</LicLineID> \
```

```
<PAK>PAK12345678</PAK>" SIGN=3AF5C2D26E1A
n1000v#
```

---

**関連コマンド**

コマンド	説明
<b>show license file</b>	VSM に設定されたライセンスを表示して、ライセンスのインストールを確認します。
<b>clear license</b>	ライセンスをアンインストールし（つまり、ライセンスを VSM から削除し）、そのライセンスの対象になっていた VEM へのイーサネット インターフェイスをシャットダウンします。
<b>logging level license</b>	ライセンス メッセージをログに記録する重大度のレベルを指定します。
<b>install license</b>	VSM にライセンス ファイルをインストールします。
<b>svs license transfer src-vem</b>	ソース VEM から別の VEM に、または使用可能なライセンスの VSM プールに、ライセンスを転送します。

# interface control

制御インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始するには、**interface control** コマンドを使用します。

## interface control0

### 構文の説明

このコマンドには、引数またはキーワードはありません。

### 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 (config)  
インターフェイス コンフィギュレーション (config-if)

### サポートされるユーザロール

ネットワーク管理者

### コマンド履歴

リリース	変更内容
4.0(4)SV1(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

### 例

次に、インターフェイス コンフィギュレーション モードを開始して制御インターフェイスを設定する例を示します。

```
n1000v(config)# interface control0
n1000v(config-if)#
```

### 関連コマンド

コマンド	説明
<b>show interface control0</b>	制御インターフェイスのトラフィックに関する情報を表示します。



# interface ethernet

イーサネット インターフェイスを設定するには、**interface ethernet** コマンドを使用します。

**interface ethernet** *slot/port*

<b>構文の説明</b>	<i>slot/port</i>	イーサネット インターフェイスのスロット番号およびポート番号を指定します。
--------------	------------------	---------------------------------------

<b>デフォルト</b>	なし
--------------	----

<b>コマンド モード</b>	グローバル コンフィギュレーション (config) インターフェイス コンフィギュレーション (config-if)
-----------------	--

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

コマンド履歴	リリース	変更内容
	4.0(4)SV1(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

**例** 次に、スロット 2、ポート 1 のイーサネット インターフェイスを設定するためにインターフェイス コマンド モードを開始する例を示します。

```
n1000v# config t
n1000v(config)# interface ethernet 2/1
n1000v(config-if)#
```

関連コマンド	コマンド	説明
	<b>show interface ethernet</b> <i>slot/port</i>	イーサネット インターフェイスの情報を表示します。

# interface loopback

ループバック インターフェイスを作成して設定するには、**interface loopback** コマンドを使用します。ループバック 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。

**interface loopback** *number*

**no interface loopback** *number*

## 構文の説明

*number*                      インターフェイス番号を指定します。有効な値は 0 ～ 1023 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 (config)  
インターフェイス コンフィギュレーション (config-if)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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

### 例

次に、ループバック インターフェイスを作成する例を示します。

```
n1000v(config)# interface loopback 50
n1000v(config-if)#
```

## 関連コマンド

コマンド	説明
<b>show interface loopback</b>	指定されたループバック インターフェイスのトラフィックに関する情報を表示します。

# interface mgmt

管理インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始するには、**interface management** コマンドを使用します。

## interface mgmt0

### 構文の説明

このコマンドには、引数またはキーワードはありません。

### 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 (config)  
インターフェイス コンフィギュレーション (config-if)

### サポートされるユーザロール

ネットワーク管理者

### コマンド履歴

リリース	変更内容
4.0(4)SV1(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

### 例

次に、インターフェイス コンフィギュレーション モードを開始して管理インターフェイスを設定する例を示します。

```
n1000v(config)# interface mgmt0
n1000v(config-if)#
```

### 関連コマンド

コマンド	説明
<b>show interface mgmt0</b>	管理インターフェイスのトラフィックに関する情報を表示します。

# interface port-channel

ポート チャネル インターフェイスを作成して、インターフェイス コンフィギュレーション モードを開始するには、**interface port-channel** コマンドを使用します。論理ポート チャネル インターフェイスまたは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。

**interface port-channel** *channel-number*

**no interface port-channel** *channel-number*

## 構文の説明

*channel-number* 論理ポート チャネル インターフェイスに割り当てられているチャンネル番号。有効値の範囲は、1 ~ 4096 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 (config)  
インターフェイス コンフィギュレーション (config-if)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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 チャネル グループの作成や削除、およびポート チャネルのインターフェイス コンフィギュレーション モードを開始するには、**interface port-channel** コマンドを使用します。

ポートは、1 つのチャンネル グループだけに属することができます。

**interface port-channel** コマンドを使用する際には、次の注意事項に従ってください。

- CDP を使用する場合は、ポート チャネル インターフェイスではなく物理インターフェイスでだけ設定を行う必要があります。
- ポート チャネル インターフェイスにスタティック MAC アドレスを割り当てなかった場合は、自動的に MAC アドレスが割り当てられます。スタティック MAC アドレスを割り当て、後で削除した場合は、MAC アドレスが自動的に割り当てられます。
- ポート チャネルの MAC アドレスは、チャンネル グループに最初に追加された稼働ポートのアドレスです。この最初に追加されたポートがチャンネルから削除されると、次に追加された動作ポート (存在する場合) の MAC アドレスになります。

## 例

次に、チャンネル グループ番号が 50 のポート チャネル グループ インターフェイスを作成する例を示します。

```
n1000v(config)# interface port-channel 50
n1000v(config-if)#
```

## 関連コマンド

コマンド	説明
<b>show interface port-channel</b>	指定されたポート チャネル インターフェイスのトラフィックに関する情報を表示します。
<b>show port-channel summary</b>	ポート チャネルに関する情報を表示します。

# interface vethernet

仮想イーサネット インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始するには、**interface vethernet** コマンドを使用します。仮想イーサネット 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。

**interface vethernet** *number*

**no interface vethernet** *number*

## 構文の説明

*number* インターフェイス番号を指定します。有効な値は、1 ~ 1048575 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 (config)  
インターフェイス コンフィギュレーション (config-if)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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

仮想イーサネット インターフェイスを作成するには、**interface vethernet** コマンドを使用します。

## 例

次に、仮想イーサネット インターフェイスを作成する例を示します。

```
n1000v(config)# interface vethernet 50
n1000v(config-if)#
```

## 関連コマンド

コマンド	説明
<b>show interface vethernet</b> <i>number</i>	指定した仮想イーサネット インターフェイスのトラフィックに関する情報を表示します。

# ip access-group

mgmt0 インターフェイスの IP アクセス グループを作成するには、**ip access-group** コマンドを使用します。アクセス グループを削除するには、このコマンドの **no** 形式を使用します。

```
ip access-group name {in | out}
```

```
no ip access-group name {in | out}
```

## 構文の説明

<i>name</i>	リスト名です。
<b>in</b>	着信（入力）トラフィックの方向を指定します。
<b>out</b>	発信（出力）トラフィックの方向を指定します。

## 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 (config-if)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.2(1)SV1(4)	このコマンドが追加されました。

## 使用上のガイドライン

### 例

次に、mgmt0 インターフェイスへの着信トラフィックに対する Telnet という名前の IP アクセス グループを設定する例を示します。

```
n1000v# config t
n1000v(config)# interface mgmt0
n1000v(config-if)# ip access-group telnet in
n1000v(config-if)#
```

## 関連コマンド

コマンド	説明
<b>show ip access-lists</b>	ACL の設定を表示します。

# ip access-list

アクセス リストを作成するには、**ip access-list** コマンドを使用します。アクセス 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 access-list {name | match-local-traffic}
```

```
no ip access-list {name | match-local-traffic}
```

## 構文の説明

<i>name</i>	リスト名です。
<b>match-local-traffic</b>	ローカルに生成されたトラフィックに対するアクセス リストの照合をイネーブルにします。

## デフォルト

アクセス リストは作成されていません。

## コマンドモード

グローバル コンフィギュレーション (config)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(1)	このコマンドが追加されました。

## 例

次に、アクセス リストを作成する例を示します。

```
n1000v# configure terminal
n1000v(config)# ip access-list acl1
n1000v(config)#
```

## 関連コマンド

コマンド	説明
<b>show access-lists</b>	アクセス リストを表示します。



# ip address

IP ルートを作成するには、**ip address** コマンドを使用します。IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

```
ip address {address mask | prefix} {next-hop | next-hop-prefix | interface-type
interface-number} [tag tag-value | preference]
```

```
no ip address {address mask | prefix} {next-hop | next-hop-prefix | interface-type
interface-number} [secondary | tag tag-value | preference]
```

## 構文の説明

<i>address</i>	A.B.C.D の形式で IP アドレスを指定します。
<i>mask</i>	A.B.C.D の形式で IP ネットワーク マスクを指定します。
<i>prefix</i>	A.B.C.D/LEN の形式で IP プレフィックスとネットワーク マスクの長さを指定します。
<i>next-hop</i>	A.B.C.D の形式で IP ネクストホップ アドレスを指定します。
<i>next-hop-prefix</i>	A.B.C.D/LEN の形式で IP ネクストホップ プレフィックスを指定します。
<i>interface-type</i>	インターフェイス タイプ。
<i>interface-number</i>	インターフェイスまたはサブインターフェイスの番号です。
<b>secondary</b>	(任意) インターフェイスに追加の IP アドレスを設定します。
<b>tag</b>	(任意) タグを指定します。
<i>tag-value</i>	タグの値を指定します。有効な値の範囲は 0 ~ 4294967295 です。デフォルトは 0 です。
<i>preference</i>	(任意) ルート プリファレンスです。

## 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 (config)

## サポートされるユーザ ロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(1)	このコマンドが追加されました。

## 例

次は、IP アドレスを作成する例を示します。

```
n1000v# configure terminal
n1000v(config)# ip address 209.165.200.225 255.255.255.224 x
n1000v(config)#
```

## 関連コマンド

コマンド	説明
<code>show ip interface A.B.C.D.</code>	ローカル IP アドレスのインターフェイスを表示します。

# ip arp inspection limit

ARP の要求と応答のレート制限を設定するには、**ip arp inspection limit** コマンドを使用します。この設定を削除するには、このコマンドの **no** 形式を使用します。レート制限をデフォルトに設定するには、このコマンドの **default** 形式を使用します。

```
ip arp inspection limit {rate pps [burst interval bint] | none}
```

```
no ip arp inspection limit {rate pps [burst interval bint] | none}
```

```
default ip arp inspection limit {rate pps [burst interval bint] | none}
```

## 構文の説明

<b>rate pps</b>	1 秒間のパケット数でレート制限を指定します。
<b>burst interval</b>	(任意) バースト間隔を指定します。
<b>bint</b>	(任意) バースト間隔を秒単位で指定します。
<b>none</b>	制限がないことを指定します。

## 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 (config-if)  
ポート プロファイル コンフィギュレーション (config-port-prof)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(2)	このコマンドが追加されました。

## 例

次に、ARP 要求のレート制限を 20 pps に設定する例を示します。

```
n1000v(config)# ip arp inspection limit rate 20
```

次に、設定を削除する例を示します。

```
n1000v(config)# no arp inspection limit rate 20
```

## 関連コマンド

コマンド	説明
<b>show ip arp inspection interface interface</b>	指定されたインターフェイスの信頼状態および ARP パケット レートを表示します。

# ip arp inspection trust

レイヤ 2 インターフェイスを信頼できる ARP インターフェイスとして設定するには、**ip arp inspection trust** コマンドを使用します。レイヤ 2 インターフェイスを信頼できない ARP インターフェイスとして設定するには、このコマンドの **no** 形式を使用します。レイヤ 2 インターフェイスをデフォルトに戻すには、このコマンドの **default** 形式を使用します。

**ip arp inspection trust**

**no ip arp inspection trust**

**default ip arp inspection trust**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

デフォルトでは、すべてのインターフェイスが信頼できない ARP インターフェイスです。

## コマンドモード

インターフェイス コンフィギュレーション (config-if)  
ポート プロファイル コンフィギュレーション (config-port-prof)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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

信頼できる ARP インターフェイスとして設定できるのは、レイヤ 2 仮想イーサネット インターフェイスだけです。

## 例

次に、レイヤ 2 インターフェイスを信頼できる ARP インターフェイスとして設定する例を示します。

```
n1000v# configure terminal
n1000v(config)# interface vethernet 2
n1000v(config-if)# ip arp inspection trust
n1000v(config-if)#
```

## 関連コマンド

コマンド	説明
<b>show ip arp inspection interface</b>	指定されたインターフェイスの信頼状態および ARP パケット レートを表 示します。

# ip arp inspection validate

追加の Dynamic ARP Inspection (DAI) 検証をイネーブルにするには、**ip arp inspection validate** コマンドを使用します。追加の DAI 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 inspection validate {dst-mac [ip] [src-mac] | ip [dst-mac] [src-mac] | src-mac [dst-mac] [ip]}
```

```
no ip arp inspection validate {dst-mac [ip] [src-mac] | ip [dst-mac] [src-mac] | src-mac [dst-mac] [ip]}
```

## 構文の説明

<b>dst-mac</b>	(任意) イーサネット ヘッダーの宛先 MAC アドレスを、ARP 応答の ARP 本文にあるターゲット MAC アドレスと照合します。MAC アドレスが一致していないパケットは無効として分類され、ドロップされます。
<b>ip</b>	(任意) ARP 本文が有効で、予期された IP アドレスかどうかを検証します。アドレスには 0.0.0.0、255.255.255.255、およびすべての IP マルチキャストアドレスが含まれます。すべての ARP 要求と ARP 応答で送信者 IP アドレスを検査し、ARP 応答でターゲット IP アドレスのみを検査します。
<b>src-mac</b>	(任意) イーサネット ヘッダーの送信元 MAC アドレスを、ARP 要求および応答の ARP 本文にある送信側 MAC アドレスと照合します。MAC アドレスが一致していないパケットは無効として分類され、ドロップされます。

## 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 (config)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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

最小限、1 つのキーワードを指定する必要があります。複数のキーワードを指定する場合、順序は影響しません。

## 例

次に、追加の DAI 検証をイネーブルにする例を示します。

```
n1000v# configure terminal
n1000v(config)# ip arp inspection validate src-mac dst-mac ip
n1000v(config)#
```

## 関連コマンド

コマンド	説明
<code>show ip arp inspection</code>	DAI 設定ステータスを表示します。

# ip arp inspection vlan

VLAN リストに対して Dynamic ARP Inspection (DAI) をイネーブルにするには、**ip arp inspection vlan** コマンドを使用します。VLAN リストの DAI 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 inspection vlan** *vlan-list*

**no ip arp inspection vlan** *vlan-list*

## 構文の説明

<i>vlan-list</i>	DAI をアクティブにする VLAN。 <i>vlan-list</i> 引数を使用すると、単一の VLAN ID、VLAN ID の範囲、またはカンマで区切られた ID および範囲を指定できます（「例」の項を参照）。有効な VLAN ID は、1 ~ 4096 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 (config)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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

デフォルトでは、DAI によって検査されたパケットはロギングされません。

## 例

次に、VLAN 13、15、および 17 ~ 23 で DAI をイネーブルにする例を示します。

```
n1000v# configure terminal
n1000v(config)# ip arp inspection vlan 13,15,17-23
n1000v(config)#
```

## 関連コマンド

コマンド	説明
<b>ip arp inspection validate</b>	追加の DAI 検証をイネーブルにします。
<b>show ip arp inspection vlan</b>	指定した VLAN のリストの DAI ステータスを表示します。

# ip dhcp snooping

デバイス上で DHCP スヌーピングをグローバルでイネーブルにするには、**ip dhcp snooping** コマンドを使用します。DHCP スヌーピングをグローバルで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 dhcp snooping**

**no ip dhcp snooping**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

デフォルトでは、DHCP スヌーピングはグローバルにディセーブルです。

## コマンド モード

グローバル コンフィギュレーション (config)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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

このコマンドを使用するには、DHCP スヌーピング機能をイネーブルにする必要があります (**feature dhcp** コマンドを参照)。

**no ip dhcp snooping** コマンドを使用して DHCP スヌーピングをディセーブルにすると、デバイスの DHCP スヌーピング設定が保持されます。

## 例

次に、DHCP スヌーピングをグローバルにイネーブルにする例を示します。

```
n1000v# configure terminal
n1000v(config)# ip dhcp snooping
n1000v(config)#
```

## 関連コマンド

コマンド	説明
<b>feature dhcp</b>	デバイスの DHCP スヌーピング機能をイネーブルにします。
<b>ip dhcp snooping trust</b>	インターフェイスを、DHCP メッセージの信頼できる送信元として設定します。
<b>ip dhcp snooping vlan</b>	特定の VLAN 上で DHCP スヌーピングをイネーブルにします。
<b>show ip dhcp snooping</b>	DHCP スヌーピングに関する一般的な情報を表示します。



# ip dhcp snooping information option

DHCP パケットの VSM MAC アドレスと vEthernet ポート情報をリレーするには、**ip dhcp snooping information option** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

**ip dhcp snooping information option**

**no ip dhcp snooping information option**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## 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 (config)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.2(1)SV1(4)	このコマンドが追加されました。

## 使用上のガイドライン

## 例

次に、DHCP パケットの VSM MAC アドレスと vEthernet ポート情報をグローバルにリレーする例を示します。

```
n1000v# configure terminal
n1000v(config)# ip dhcp snooping information option
n1000v(config)#
```

次に、DHCP パケットの VSM MAC アドレスと vEthernet ポート情報のグローバルなリレーを削除する例を示します。

```
n1000v# configure terminal
n1000v(config)# no ip dhcp snooping information option
n1000v(config)#
```

## 関連コマンド

コマンド	説明
<b>feature dhcp</b>	デバイスの DHCP スヌーピング機能をイネーブルにします。
<b>ip dhcp snooping trust</b>	インターフェイスを、DHCP メッセージの信頼できる送信元として設定します。
<b>ip dhcp snooping vlan</b>	特定の VLAN 上で DHCP スヌーピングをイネーブルにします。

コマンド	説明
<b>show ip dhcp snooping</b>	DHCP スヌーピングに関する一般的な情報を表示します。

# ip dhcp snooping limit rate

ポートで受信される DHCP パケットに対するレート制限を設定するには、**ip dhcp snooping limit rate** コマンドを使用します。各ポートで受信される DHCP パケットに対するレート制限を削除するには、このコマンドの **no** 形式を使用します。デフォルトの設定を復元するには、このコマンドの **default** 形式を使用します。

**ip dhcp snooping limit rate rate**

**no ip dhcp snooping limit rate**

**default ip dhcp snooping limit rate**

<b>構文の説明</b>	<i>rate</i> 1 秒あたりの DHCP パケットの数。指定できる範囲は 1 ~ 2048 です。
--------------	---

<b>デフォルト</b>	なし
--------------	----

<b>コマンドモード</b>	インターフェイス コンフィギュレーション (config-if) ポート プロファイル コンフィギュレーション (config-port-prof)
----------------	---

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

コマンド履歴	リリース	変更内容
	4.0(4)SV1(2)	このコマンドが追加されました。

<b>例</b>	次に、vEthernet インターフェイス 3 で DHCP パケットのレートを 30 pps に制限する例を示します。 <pre>n1000v# configure terminal n1000v(config)# interface vethernet 3 n1000v(config-if)# ip dhcp snooping limit rate 30</pre>
----------	---

関連コマンド	コマンド	説明
	<b>feature dhcp</b>	デバイスの DHCP スヌーピング機能をイネーブルにします。
	<b>ip dhcp snooping trust</b>	インターフェイスを、DHCP メッセージの信頼できる送信元として設定します。
	<b>ip dhcp snooping vlan</b>	特定の VLAN 上で DHCP スヌーピングをイネーブルにします。
	<b>show ip dhcp snooping</b>	DHCP スヌーピングに関する一般的な情報を表示します。

# ip dhcp snooping trust

インターフェイスを DHCP メッセージの信頼できる送信元として設定するには、**ip dhcp snooping trust** コマンドを使用します。インターフェイスを DHCP メッセージの信頼できない送信元として設定するには、このコマンドの **no** 形式を使用します。デフォルトの設定を復元するには、このコマンドの **default** 形式を使用します。

**ip dhcp snooping trust**

**no ip dhcp snooping trust**

**default ip dhcp snooping trust**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

デフォルトでは、DHCP メッセージの信頼できる送信元として設定されるインターフェイスはありません。

## 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 (config-if)  
ポート プロファイル コンフィギュレーション (config-port-prof)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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

DHCP の信頼状態は、次のタイプのインターフェイスに設定できます。

- レイヤ 2 vEthernet インターフェイス
- プライベート VLAN インターフェイス

## 例

次に、インターフェイスを DHCP メッセージの信頼できる送信元として設定する例を示します。

```
n1000v# configure terminal
n1000v(config)# interface vethernet 2
n1000v(config-if)# ip dhcp snooping trust
n1000v(config-if)#
```

## 関連コマンド

コマンド	説明
<b>feature dhcp</b>	デバイスの DHCP スヌーピング機能をイネーブルにします。
<b>ip dhcp snooping</b>	デバイスの DHCP スヌーピングをグローバルにイネーブルにします。

コマンド	説明
<b>ip dhcp snooping verify mac-address</b>	MAC アドレス検証を、DHCP スヌーピングの一部としてイネーブルにします。
<b>ip dhcp snooping vlan</b>	特定の VLAN 上で DHCP スヌーピングをイネーブルにします。
<b>show ip dhcp snooping</b>	DHCP スヌーピングに関する一般的な情報を表示します。

# ip dhcp snooping verify mac-address

DHCP スヌーピングの MAC アドレス検証をイネーブルにするには、**ip dhcp snooping verify mac-address** コマンドを使用します。MAC アドレス検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。

**ip dhcp snooping verify mac-address**

**no ip dhcp snooping verify mac-address**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## 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 (config)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(1)	このコマンドが追加されました。

## 例

次に、DHCP スヌーピングの MAC アドレス検証をイネーブルにする例を示します。

```
n1000v(config)# config t
n1000v(config)# ip dhcp snooping verify mac-address
n1000v(config)#
```

次に、DHCP スヌーピングの MAC アドレス検証をディセーブルにする例を示します。

```
n1000v(config)# config t
n1000v(config)# no ip dhcp snooping verify mac-address
n1000v(config)#
```

## 関連コマンド

コマンド	説明
<b>feature dhcp</b>	デバイスの DHCP スヌーピング機能をイネーブルにします。
<b>show running-config dhcp</b>	DHCP スヌーピング設定を表示します。
<b>ip dhcp snooping</b>	DHCP スヌーピングをグローバルにイネーブルにします。
<b>ip dhcp snooping vlan</b>	<i>vlan-list</i> で指定する VLAN の DHCP スヌーピングをイネーブルにします。
<b>clear ip dhcp snooping binding</b>	DHCP スヌーピング バインディング データベースに動的に追加されたエントリを消去します。

コマンド	説明
<b>ip dhcp snooping trust</b>	DHCP スヌーピングに関してインターフェイスを信頼できるインターフェイスとして設定します。
<b>ip dhcp snooping limit rate</b>	DHCP 制限レートを設定します。

# ip dhcp snooping vlan

1 つまたは複数の VLAN で DHCP スヌーピングをイネーブルにするには、**ip dhcp snooping vlan** コマンドを使用します。1 つまたは複数の VLAN 上で DHCP スヌーピ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。

**ip dhcp snooping vlan *vlan-list***

**no ip dhcp snooping vlan *vlan-list***

## 構文の説明

*vlan-list* DHCP スヌーピングをイネーブルにする VLAN 範囲。*vlan-list* 引数を使用すると、単一の VLAN ID、VLAN ID の範囲、またはカンマで区切られた ID および範囲を指定できます（「例」の項を参照）。有効な VLAN ID は、1 ～ 4096 です。

## デフォルト

デフォルトでは、すべての VLAN 上で DHCP スヌーピングはディセーブルです。

## コマンドモード

グローバル コンフィギュレーション (config)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(2)	このコマンドが追加されました。

## 例

次に、VLAN 100、200、および 250 ～ 252 で DHCP スヌーピングをイネーブルにする例を示します。

```
n1000v# configure terminal
n1000v(config)# ip dhcp snooping vlan 100,200,250-252
n1000v(config)#
```

## 関連コマンド

コマンド	説明
<b>feature dhcp</b>	デバイスの DHCP スヌーピング機能をイネーブルにします。
<b>ip dhcp snooping</b>	デバイスの DHCP スヌーピングをグローバルにイネーブルにします。
<b>ip dhcp snooping trust</b>	インターフェイスを、DHCP メッセージの信頼できる送信元として設定します。
<b>show ip dhcp snooping</b>	DHCP スヌーピングに関する一般的な情報を表示します。



# ip directed-broadcast

IP ダイレクトブロードキャストをイネーブルにするには、**ip directed-broadcast** コマンドを使用します。IP ダイレクトブロードキャ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 directed-broadcast**

**no ip directed-broadcast**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

なし

## コマンドモード

インターフェイス コンフィギュレーション (config-if)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(1)	このコマンドが追加されました。

## 例

次に、IP ダイレクトブロードキャストをイネーブルにする例を示します。

```
n1000v# configure terminal
n1000v(config)# interface mgmt 0
n1000v(config-if)# ip directed-broadcast
n1000v(config-if)#
```

## 関連コマンド

コマンド	説明
<b>show ip interface</b>	IP インターフェイス情報を表示します。

# ip dscp

ERSPAN トラフィックのパケットの IP DSCP 値を指定し、実行コンフィギュレーションで保存するには、**ip dscp** コマンドを保存します。

**ip dscp** *dscp\_value*

## 構文の説明

*dscp\_value*      ERSPAN トラフィック パケットの DSCP 値 (秒)。値は 0 ~ 63 の範囲で指定します。

## デフォルト

デフォルトの DSCP 値は、0 です。

## コマンドモード

CLI ERSPAN 送信元コンフィギュレーション (config-erspan-src)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(1)	このコマンドが追加されました。

## 例

次に、ERSPAN トラフィックのパケットの DSCP 値として 25 を指定する例を示します。

```
n1000v# config t
n1000v(config)# monitor session 3 type erspa
n1000v(config-erspan-src)# ip dscp 25
n1000v(config-erspan-src)#
```

## 関連コマンド

コマンド	説明
<b>monitor session type erspan-source</b>	任意のセッション番号でセッションを作成し、CLI ERSPAN 送信元コンフィギュレーション モードに切り替えます。
<b>description</b>	指定された ERSPAN セッションの場合、説明を追加して、実行コンフィギュレーションに保存します。
<b>source</b>	指定されたセッションに対し、モニタする送信元とトラフィックの方向を設定し、情報を実行コンフィギュレーションに保存します。
<b>filter vlan</b>	指定されたセッションに対し、モニタする VLAN、VLAN リスト、または VLAN 範囲を設定し、実行コンフィギュレーションにこの情報を保存します。
<b>destination ip</b>	カプセル化されたトラフィックが送信されるホストの IP アドレスを設定し、実行コンフィギュレーションに保存します。
<b>ip ttl</b>	ERSPAN トラフィックのパケットに対し、IP 存続可能時間値を指定し、実行コンフィギュレーションに保存します。

コマンド	説明
<b>ip prec</b>	ERSPAN トラフィックの packets に対し、IP precedence 値を指定し、実行コンフィギュレーションに保存します。
<b>mtu</b>	ERSPAN トラフィックの最大伝送単位 (MTU) サイズを指定し、実行コンフィギュレーションに保存します。
<b>erspan-id</b>	ERSPAN ID をセッション設定に追加して、実行コンフィギュレーションに保存します。
<b>no shut</b>	ERSPAN セッションをイネーブルにし、実行コンフィギュレーションに保存します。
<b>show monitor session session_id</b>	実行コンフィギュレーション内に存在する ERSPAN セッション コンフィギュレーションを表示します。

# ip flow monitor

ルータが受信または転送するトラフィックの Flexible NetFlow フロー モニタをイネーブルにするには、**ip flow monitor** インターフェイス コンフィギュレーション モード コマンドを使用します。Flexible NetFlow フロー モニタ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 flow monitor** *monitor-name* {input | output}

**no ip flow monitor** *monitor-name* {input | output}

## 構文の説明

<i>monitor-name</i>	事前に設定したフロー モニタの名前
<b>input</b>	ルータがインターフェイス上で受信するトラフィックをモニタします。
<b>output</b>	ルータがインターフェイス上から送信するトラフィックをモニタします。

## 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 (config-if)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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 flow monitor** コマンドを使用して特定のインターフェイスにフロー モニタを適用し、Flexible NetFlow によるトラフィック モニタリングをイネーブルにするには、**flow monitor** コマンドを使用して事前にフロー モニタを作成しておく必要があります。

## 例

次に、入力トラフィックのモニタリングのためにフロー モニタをイネーブルにする例を示します。

```
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 input
```

次に、出力トラフィックのモニタリングのためにフロー モニタをイネーブルにする例を示します。

```
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

次に、同一のインターフェイスで入出力トラフィックのモニタリングのために同じフロー モニタをイネーブルにする例を示します。

```
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 input
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

次に、同一のインターフェイスで入出力トラフィックのモニタリングのために 2 つの異なるフロー モニタをイネーブルにする例を示します。

```
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 input
n1000v(config-if)# ip flow monitor FLOW-MONITOR-2 output
```

次に、異なる 2 つのインターフェイスで入出力トラフィックのモニタリングのために同じフロー モニタをイネーブルにする例を示します。

```
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 input
n1000v(config)# interface ethernet1/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

次に、異なる 2 つのインターフェイスで入出力トラフィックのモニタリングのために 2 つの異なるフロー モニタをイネーブルにする例を示します。

```
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 input
n1000v(config)# interface ethernet1/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-2 output
```

## 関連コマンド

コマンド	説明
<b>flow exporter</b>	フロー エクスポートを作成します。
<b>flow monitor</b>	フロー モニタを作成します。
<b>flow record</b>	フロー レコードを作成します。

# ip igmp snooping (グローバル)

IGMP スヌーピングをイネーブルにするには、**ip igmp snooping** コマンドを使用します。IGMP スヌーピ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。

**ip igmp snooping**

**no ip igmp snooping**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

イネーブル

## コマンドモード

グローバル コンフィギュレーション (config)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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

IGMP スヌーピングのグローバル設定がディセーブルになっている場合は、すべての VLAN が、イネーブルかどうかに関係なくディセーブルと見なされます。

## 例

次に、IGMP スヌーピングをイネーブルにする例を示します。

```
n1000v(config)# ip igmp snooping
n1000v(config)#
```

次の例では、IGMP スヌーピングをディセーブルにする方法を示します。

```
n1000v(config)# no ip igmp snooping
n1000v(config)#
```

## 関連コマンド

コマンド	説明
<b>show ip igmp snooping</b>	IGMP スヌーピング情報を表示します。

# ip igmp snooping (VLAN)

VLAN インターフェイスで IGMP スヌーピングをイネーブルにするには、**ip igmp snooping** コマンドを使用します。インターフェイスでの IGMP スヌーピ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。

**ip igmp snooping**

**no ip igmp snooping**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

イネーブル

## コマンドモード

VLAN コンフィギュレーション (config-vlan)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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

IGMP スヌーピングのグローバル設定がディセーブルになっている場合は、すべての VLAN が、イネーブルかどうかに関係なくディセーブルと見なされます。

## 例

次の例では、IGMP スヌーピングを VLAN インターフェイスでイネーブルにする方法を示します。

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping
n1000v(config-vlan)#
```

次の例では、IGMP スヌーピングを VLAN インターフェイスでディセーブルにする方法を示します。

```
n1000v(config)# vlan 1
n1000v(config-vlan)# no ip igmp snooping
n1000v(config-vlan)#
```

## 関連コマンド

コマンド	説明
<b>show ip igmp snooping</b>	IGMP スヌーピング情報を表示します。

# ip igmp snooping explicit-tracking

VLAN 単位で、各ポートに対する個々のホストからの IGMPv3 メンバーシップ レポートの追跡をイネーブルにするには、**ip igmp snooping explicit-tracking** コマンドを使用します。追跡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 igmp snooping explicit-tracking**

**no ip igmp snooping explicit-tracking**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

イネーブル

## コマンド モード

VLAN コンフィギュレーション (config-vlan)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(1)	このコマンドが追加されました。

## 例

次の例では、VLAN インターフェイスでの IGMPv3 メンバーシップ レポートの追跡をイネーブルにする方法を示します。

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping explicit-tracking
n1000v(config-vlan)#
```

次の例では、IGMP スヌーピングを VLAN インターフェイスでディセーブルにする方法を示します。

```
n1000v(config)# vlan 1
n1000v(config-vlan)# no ip igmp snooping explicit-tracking
n1000v(config-vlan)#
```

## 関連コマンド

コマンド	説明
<b>show ip igmp snooping</b>	IGMP スヌーピング情報を表示します。



# ip igmp snooping fast-leave

IGMPv2 プロトコルのホスト レポート抑制メカニズムのために明示的に追跡できない IGMPv2 ホストのサポートをイネーブルにするには、**ip igmp snooping fast-leave** コマンドを使用します。IGMPv2 ホストのサポー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 igmp snooping fast-leave**

**no ip igmp snooping fast-leave**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

ディセーブル

## コマンド モード

VLAN コンフィギュレーション (config-vlan)

## サポートされるユーザ ロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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

高速脱退がイネーブルの場合、IGMP ソフトウェアは、各 VLAN ポートに接続されたホストが 1 つだけであると見なします。

## 例

次の例では、IGMPv2 ホストのサポートをイネーブルにする方法を示します。

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping fast-leave
n1000v(config-vlan)#
```

次の例では、IGMPv2 ホストのサポートをディセーブルにする方法を示します。

```
n1000v(config)# vlan 1
n1000v(config-vlan)# no ip igmp snooping fast-leave
n1000v(config-vlan)#
```

## 関連コマンド

コマンド	説明
<b>show ip igmp snooping</b>	IGMP スヌーピング情報を表示します。

# ip igmp snooping last-member-query-interval

ソフトウェアがグループを削除するクエリー間隔を設定するには、**ip igmp snooping last-member-query-interval** コマンドを使用します。クエリー間隔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 igmp snooping last-member-query-interval** *interval*

**no ip igmp snooping last-member-query-interval** [*interval*]

## 構文の説明

*interval* 秒単位のクエリー間隔です。有効な範囲は 1 ～ 25 です。デフォルトは 1 です。

## デフォルト

クエリー間隔は 1 です。

## コマンドモード

VLAN コンフィギュレーション (config-vlan)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(1)	このコマンドが追加されました。

## 例

次の例では、ソフトウェアがグループを削除するクエリー間隔を設定する方法を示します。

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping last-member-query-interval 3
n1000v(config-vlan)#
```

次の例では、クエリー間隔をデフォルトにリセットする方法を示します。

```
n1000v(config)# vlan 1
n1000v(config-vlan)# no ip igmp snooping last-member-query-interval
n1000v(config-vlan)#
```

## 関連コマンド

コマンド	説明
<b>show ip igmp snooping</b>	IGMP スヌーピング情報を表示します。

# ip igmp snooping link-local-groups-suppression (VLAN)

リンクローカル グループ IP のスヌーピングを抑制するには、**ip igmp snooping link-local-groups-suppression** コマンドを使用します。無制限のスヌーピングを許可するには、このコマンドの **no** 形式を使用します。

**ip igmp snooping link-local-groups-suppression**

**no ip igmp snooping link-local-groups-suppression**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

イネーブル

## コマンド モード

VLAN コンフィギュレーション (config-vlan)

## サポートされるユーザ ロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.2(1)SV1(4)	このコマンドが追加されました。

## 使用上のガイドライン

グローバル コンフィギュレーション モードでこのコマンドを入力することで、VSM 上のすべてのインターフェイスに、リンクローカル グループ抑制を適用できます。

## 例

次に、VLAN2 から送信される IGMP トラフィックを制限する例を示します。

```
n1000v# config t
n1000v(config)# vlan vlan2
n1000v(config-vlan)# ip igmp snooping link-local-groups-suppression
```

次に、VLAN2 から送信される IGMP トラフィックを再開する例を示します。

```
n1000v# config t
n1000v(config)# vlan vlan2
n1000v(config-vlan)# no ip igmp snooping link-local-groups-suppression
n1000v(config-vlan)#
```

## 関連コマンド

コマンド	説明
<b>show ip igmp snooping</b>	IGMP スヌーピング情報を表示します。
<b>ip igmp snooping</b>	VLAN 上で IGMP スヌーピングをイネーブルにします。

# ip igmp snooping link-local-groups-suppression (グローバル)

リンクローカル グループ IP のスヌーピングを抑制するには、**ip igmp snooping link-local-groups-suppression** コマンドを使用します。無制限のスヌーピングを許可するには、このコマンドの **no** 形式を使用します。

**ip igmp snooping link-local-groups-suppression**

**no ip igmp snooping link-local-groups-suppression**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

イネーブル

## コマンド モード

グローバル コンフィギュレーション (config)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.2(1)SV1(4)	このコマンドが追加されました。

## 使用上のガイドライン

VLAN コンフィギュレーション モードでこのコマンドを入力して、単一の VLAN にリンクローカル グループ抑制を適用できます。

## 例

次に、VSM のすべてのインターフェイスから送信される IGMP トラフィックを制限する例を示します。

```
n1000v# config t
n1000v(config)# ip igmp snooping link-local-groups-suppression
n1000v(config)#
```

次に、VSM のすべてのインターフェイスから無制限の IGMP トラフィックの送信を再開する例を示します。

```
n1000v# config t
n1000v(config)# no ip igmp snooping link-local-groups-suppression
n1000v(config)#
```

## | 関連コマンド

コマンド	説明
<b>show ip igmp snooping</b>	IGMP スヌーピング情報を表示します。
<b>ip igmp snooping</b>	VLAN 上で IGMP スヌーピングをイネーブルにします。

# ip igmp snooping mrouter interface

マルチキャスト ルータへのスタティック接続を設定するには、**ip igmp snooping mrouter interface** コマンドを使用します。スタティック接続を削除するには、このコマンドの **no** 形式を使用します。

**ip igmp snooping mrouter interface** *if-type if-number*

**no ip igmp snooping mrouter interface** *if-type if-number*

構文の説明	
<i>if-type</i>	インターフェイス タイプ。詳細については、疑問符 (?) オンライン ヘルプ機能を使用します。
<i>if-number</i>	インターフェイスまたはサブインターフェイスの番号です。ネットワークング デバイスに対する番号付け構文の詳細については、疑問符 (?) のオンライン ヘルプ機能を使用してください。

デフォルト なし

コマンド モード VLAN コンフィギュレーション (config-vlan)

サポートされるユーザ ロール ネットワーク管理者

コマンド履歴	リリース	変更内容
	4.0(4)SV1(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 ルータと接続するインターフェイスが、選択した VLAN に含まれている必要があります。

例 次に、マルチキャスト ルータへのスタティックな接続を設定する例を示します。

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping mrouter interface ethernet 2/1
n1000v(config-vlan)#
```

次の例では、マルチキャスト ルータへのスタティック接続を削除する方法を示します。

```
n1000v(config)# vlan 1
n1000v(config-vlan)# no ip igmp snooping mrouter interface ethernet 2/1
n1000v(config-vlan)#
```

関連コマンド	コマンド	説明
	<b>show ip igmp snooping</b>	IGMP スヌーピング情報を表示します。

# ip igmp snooping report-suppression (グローバル)

VLAN に IGMPv1 または GMPv2 のレポート抑制を設定するには、**ip igmp snooping report-suppression** コマンドを使用します。IGMPv1 または GMPv2 のレポート抑制を削除するには、このコマンドの **no** 形式を使用します。

**ip igmp snooping report-suppression**

**no ip igmp snooping report-suppression**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

イネーブル

## コマンドモード

グローバル コンフィギュレーション (config)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(1)	このコマンドが追加されました。

## 例

次に、VLAN に IGMPv1 または GMPv2 のレポート抑制を設定する例を示します。

```
n1000v(config)# ip igmp snooping report-suppression
```

次に、IGMPv1 または GMPv2 のレポート抑制を削除する例を示します。

```
n1000v(config)# no ip igmp snooping report-suppression
```

## 関連コマンド

コマンド	説明
<b>show ip igmp snooping</b>	IGMP スヌーピング情報を表示します。

# ip igmp snooping report-suppression (VLAN)

VLAN に IGMPv1 または GMPv2 のレポート抑制を設定するには、**ip igmp snooping report-suppression** コマンドを使用します。IGMPv1 または GMPv2 のレポート抑制を削除するには、このコマンドの **no** 形式を使用します。

**ip igmp snooping report-suppression**

**no ip igmp snooping report-suppression**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

イネーブル

## コマンドモード

VLAN コンフィギュレーション (config-vlan)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(1)	このコマンドが追加されました。

## 例

次に、VLAN に IGMPv1 または GMPv2 のレポート抑制を設定する例を示します。

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping report-suppression
n1000v(config-vlan)#
```

次に、IGMPv1 または GMPv2 のレポート抑制を削除する例を示します。

```
n1000v(config)# vlan 1
n1000v(config-vlan)# no ip igmp snooping report-suppression
n1000v(config-vlan)#
```

## 関連コマンド

コマンド	説明
<b>show ip igmp snooping</b>	IGMP スヌーピング情報を表示します。



# ip igmp snooping static-group

VLAN のレイヤ 2 ポートをマルチキャスト グループのスタティック メンバーとして設定するには、**ip igmp snooping static-group** コマンドを使用します。スタティック メンバーを削除するには、このコマンドの **no** 形式を使用します。

**ip igmp snooping static-group group interface if-type if-number**

**no ip igmp snooping static-group group interface if-type if-number**

## 構文の説明

<i>group</i>	グループの IP アドレスです。
<b>interface</b>	スタティック グループのインターフェイスを指定します。
<i>if-type</i>	インターフェイス タイプ。詳細については、疑問符 (?) オンライン ヘルプ機能を使用します。
<i>if-number</i>	インターフェイスまたはサブインターフェイスの番号です。ネットワーキング デバイスに対する番号付け構文の詳細については、疑問符 (?) のオンライン ヘルプ機能を使用してください。

## デフォルト

なし

## コマンド モード

VLAN コンフィギュレーション (config-vlan)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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

ethernet slot/port のように、インターフェイスをタイプおよび番号で指定できます。

## 例

次の例では、マルチキャスト グループのスタティック メンバーを設定する方法を示します。

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
n1000v(config-vlan)#
```

次の例では、マルチキャスト グループのスタティック メンバーを削除する方法を示します。

```
n1000v(config)# vlan 1
n1000v(config-vlan)# no ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
n1000v(config-vlan)#
```

## 関連コマンド

コマンド	説明
show ip igmp snooping	IGMP スヌーピング情報を表示します。

# ip igmp snooping v3-report-suppression (グローバル)

IGMPv3 のレポート抑制およびプロキシ レポートを設定するには、**ip igmp snooping v3-report-suppression** コマンドを使用します。IGMPv3 のレポート抑制およびプロキシ レポ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 igmp snooping v3-report-suppression**  
**no ip igmp snooping v3-report-suppression**

**構文の説明** このコマンドには、引数またはキーワードはありません。

**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 (config)

**サポートされるユーザロール** ネットワーク管理者

コマンド履歴	リリース	変更内容
	4.0(4)SV1(1)	このコマンドが追加されました。

**例** 次に、IGMPv3 のレポート抑制およびプロキシ レポートを設定する例を示します。

```
n1000v(config)# ip igmp snooping v3-report-suppression
```

次に、IGMPv3 のレポート抑制およびプロキシ レポートを削除する例を示します。

```
n1000v(config)# no ip igmp snooping v3-report-suppression
```

関連コマンド	コマンド	説明
	<b>show ip igmp snooping</b>	IGMP スヌーピング情報を表示します。

# ip igmp snooping v3-report-suppression (VLAN)

VLAN に対して IGMPv3 レポート抑制とプロキシ レポートを設定するには、**ip igmp snooping v3-report-suppression** コマンドを使用します。IGMPv3 レポート抑制を削除するには、このコマンドの **no** 形式を使用します。

**ip igmp snooping v3-report-suppression**

**no ip igmp snooping v3-report-suppression**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

ディセーブル

## コマンドモード

VLAN コンフィギュレーション (config-vlan)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(1)	このコマンドが追加されました。

## 例

次の例では、VLAN に対して IGMPv3 レポート抑制とプロキシ レポートを設定する方法を示します。

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping v3-report-suppression
n1000v(config-vlan)#
```

次に、VLAN の IGMPv3 のレポート抑制およびプロキシ レポートを削除する例を示します。

```
n1000v(config)# vlan 1
n1000v(config-vlan)# no ip igmp snooping v3-report-suppression
n1000v(config-vlan)#
```

## 関連コマンド

コマンド	説明
<b>show ip igmp snooping</b>	IGMP スヌーピング情報を表示します。

# ip port access-group

アクセス グループを作成するには、**ip port access-group** コマンドを使用します。アクセス コントロールを削除するには、このコマンドの **no** 形式を使用します。

```
ip port access-group name {in | out}
```

```
no ip port access-group name {in | out}
```

## 構文の説明

<i>name</i>	グループ名です。有効な値の範囲は、1 ~ 64 です。
<b>in</b>	着信トラフィックを指定します。
<b>out</b>	発信トラフィックを指定します。

## デフォルト

アクセス グループは作成されていません。

## コマンド モード

ポート プロファイル コンフィギュレーション (config-port-prof)

## サポートされるユーザ ロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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

パケットのアクセス コントロールを ACL で指定するには、アクセス グループを作成します。

## 例

次に、アクセス グループを作成する例を示します。

```
n1000v# configure terminal
n1000v(config)# port-profile 1
n1000v(config-port-prof)# ip port access-group group1 in
n1000v(config-port-prof)#
```

## 関連コマンド

コマンド	説明
<b>show access-lists</b>	アクセス リストを表示します。
<b>show port-profile</b>	ポート プロファイル情報を表示します。

# ip prec

ERSPAN トラフィックのパケットの IP precedence 値を指定し、実行コンフィギュレーションで保存するには、**ip prec** コマンドを保存します。

**ip prec precedence\_value**

## 構文の説明

*precedence\_value*      ERSPAN トラフィック パケットの IP precedence 値。範囲は、0 ～ 7 です。

## デフォルト

なし

## コマンドモード

CLI ERSPAN 送信元コンフィギュレーション (config-monitor-erspan-src)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(1)	このコマンドが追加されました。

## 例

次に、ERSPAN トラフィックのパケットに IP precedence 値を 1 で指定して、実行コンフィギュレーションに保存する例を示します。

```
n1000v# config t
n1000v(config)# monitor session 3 type erspa
n1000v(config-erspan-src)# destination ip 10.54.54.1
n1000v(config-monitor-erspan-src)# ip prec 1
n1000v(config-monitor-erspan-src)#
```

## 関連コマンド

コマンド	説明
<b>monitor session type erspan-source</b>	任意のセッション番号でセッションを作成し、CLI ERSPAN 送信元コンフィギュレーション モードに切り替えます。
<b>description</b>	指定された ERSPAN セッションの場合、説明を追加して、実行コンフィギュレーションに保存します。
<b>source</b>	指定されたセッションに対し、モニタする送信元とトラフィックの方向を設定し、情報を実行コンフィギュレーションに保存します。
<b>filter vlan</b>	指定されたセッションに対し、モニタする VLAN、VLAN リスト、または VLAN 範囲を設定し、実行コンフィギュレーションにこの情報を保存します。
<b>destination ip</b>	カプセル化されたトラフィックが送信されるホストの IP アドレスを設定し、実行コンフィギュレーションに保存します。

コマンド	説明
<b>ip ttl</b>	ERSPAN トラフィックのパケットに対し、IP 存続可能時間値を指定し、実行コンフィギュレーションに保存します。
<b>ip dscp</b>	ERSPAN トラフィックのパケットに対し、IP DSCP 値を指定し、実行コンフィギュレーションに保存します。
<b>mtu</b>	ERSPAN トラフィックの最大伝送単位 (MTU) サイズを指定し、実行コンフィギュレーションに保存します。
<b>erspan-id</b>	ERSPAN ID をセッション設定に追加して、実行コンフィギュレーションに保存します。
<b>no shut</b>	ERSPAN セッションをイネーブルにし、実行コンフィギュレーションに保存します。
<b>show monitor session session_id</b>	実行コンフィギュレーション内に存在する ERSPAN セッション コンフィギュレーションを表示します。

# ip source binding

レイヤ 2 vEthernet インターフェイスのスタティック IP ソース エントリを作成するには、**ip source binding** コマンドを使用します。固定 IP ソース エントリ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 source binding** *IP-address MAC-address* **vlan** *vlan-id* **interface** **vethernet** *interface-number*

**no ip source binding** *IP-address MAC-address* **vlan** *vlan-id* **interface** **vethernet** *interface-number*

## 構文の説明

<i>IP-address</i>	特定のインターフェイス上で使用する IPv4 アドレス。有効なエントリは、ドット付き 10 進表記です。
<i>MAC-address</i>	特定のインターフェイス上で使用する MAC アドレス。有効なエントリは、ドット付き 16 進表記です。
<b>vlan</b> <i>vlan-id</i>	IP ソース エントリに関連付ける VLAN を指定します。
<b>interface</b> <b>vethernet</b> <i>interface-number</i>	スタティック IP エントリと関連付けるレイヤ 2 vEthernet インターフェイスを指定します。

## 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 (config)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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

デフォルトでは、固定 IP ソース エントリは作成されません。

## 例

次に、vEthernet インターフェイス 3 に VLAN 100 と関連付けられたスタティック IP ソース エントリを作成する例を示します。

```
n1000v# configure terminal
n1000v(config)# ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface vethernet 3
n1000v(config)#
```

## 関連コマンド



コマンド	説明
<b>ip verify source dhcp-snooping-vlan</b>	インターフェイスの IP ソース ガードをイネーブルにします。
<b>show ip verify source</b>	IP と MAC アドレスのバインディングを表示します。

# ip source-route

IP ソース ルートをイネーブルにするには、**ip source-route** コマンドを使用します。IP ソース ルー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 source-route**

**no ip source-route**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## 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 (config)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(1)	このコマンドが追加されました。

## 例

次に、IP ソース ルートをイネーブルにする例を示します。

```
n1000v# configure terminal
n1000v(config)# ip source-route
n1000v(config)#
```

## 関連コマンド

コマンド	説明
<b>show ip static-route</b>	スタティック ルートを表示します。

# ip ttl

Encapsulated Remote Switch Port Analyzer (ERSPAN) トラフィックのパケットの IP 存続可能時間値を指定し、実行コンフィギュレーションで保存するには、**ip ttl** コマンドを使用します。

**ip ttl *ttl\_value***

<b>構文の説明</b>	<i>ttl_value</i> 1 ~ 255 の存続可能時間値 (秒)。
--------------	--

<b>デフォルト</b>	なし
--------------	----

<b>コマンド モード</b>	CLI ERSPAN 送信元コンフィギュレーション (config-monitor-erspan-src)
-----------------	---

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

<b>コマンド履歴</b>	リリース	変更内容
	4.0(4)SV1(1)	このコマンドが追加されました。

**例**      次に、ERSPAN トラフィックのパケットに 64 秒の存続可能時間値を指定する例を示します。

```
n1000v# config t
n1000v(config)# monitor session 3 type erspa
n1000v(config-erspan-src)# destination ip 10.54.54.1
n1000v(config-monitor-erspan-src)# ip ttl 64
n1000v(config-monitor-erspan-src)#
```

<b>関連コマンド</b>	コマンド	説明
	<b>monitor session type erspan-source</b>	任意のセッション番号でセッションを作成し、CLI ERSPAN 送信元コンフィギュレーション モードに切り替えます。
	<b>description</b>	指定された ERSPAN セッションの場合、説明を追加して、実行コンフィギュレーションに保存します。
	<b>source</b>	指定されたセッションに対し、モニタする送信元とトラフィックの方向を設定し、情報を実行コンフィギュレーションに保存します。
	<b>filter vlan</b>	指定されたセッションに対し、モニタする VLAN、VLAN リスト、または VLAN 範囲を設定し、実行コンフィギュレーションにこの情報を保存します。
	<b>destination ip</b>	カプセル化されたトラフィックが送信されるホストの IP アドレスを設定し、実行コンフィギュレーションに保存します。
	<b>ip prec</b>	ERSPAN トラフィックのパケットに対し、IP precedence 値を指定し、実行コンフィギュレーションに保存します。

コマンド	説明
<b>ip dscp</b>	ERSPAN トラフィックのパケットに対し、IP DSCP 値を指定し、実行コンフィギュレーションに保存します。
<b>mtu</b>	ERSPAN トラフィックの最大伝送単位 (MTU) サイズを指定し、実行コンフィギュレーションに保存します。
<b>erspan-id</b>	ERSPAN ID をセッション設定に追加して、実行コンフィギュレーションに保存します。
<b>no shut</b>	ERSPAN セッションをイネーブルにし、実行コンフィギュレーションに保存します。
<b>show monitor session session_id</b>	実行コンフィギュレーション内に存在する ERSPAN セッション コンフィギュレーションを表示します。

# ip verify source dhcp-snooping-vlan

レイヤ 2 vEthernet インターフェイスで IP ソース ガードをイネーブルにするには、**ip verify source dhcp-snooping-vlan** コマンドを使用します。インターフェイス上で IP ソース ガード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。デフォルトの設定を復元するには、このコマンドの **default** 形式を使用します。

**ip verify source dhcp-snooping-vlan**

**no ip verify source dhcp-snooping-vlan**

**default ip verify source dhcp-snooping-vlan**

## 構文の説明

このコマンドには、引数またはキーワードはありません。

## デフォルト

なし

## コマンド モード

インターフェイス コンフィギュレーション (config-if)  
ポート プロファイル コンフィギュレーション (config-port-prof)

## サポートされるユーザロール

ネットワーク管理者

## コマンド履歴

リリース	変更内容
4.0(4)SV1(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

デフォルトでは、すべてのインターフェイス上で IP ソース ガードはディセーブルです。

## 例

次に、インターフェイス上で IP ソース ガードをイネーブルにする例を示します。

```
n1000v# configure terminal
n1000v(config)# interface vethernet 2
n1000v(config-if)# ip verify source dhcp-snooping-vlan
n1000v(config-if)#
```

## 関連コマンド

コマンド	説明
<b>ip source binding</b>	指定した vEthernet インターフェイスのスタティック IP ソース エントリを作成します。
<b>show ip verify source</b>	IP と MAC アドレスのバインディングを表示します。

■ ip verify source dhcp-snooping-vlan