P コマンド

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

packet vlan

ID を指定してパケット VLAN を作成するには、**packet vlan** コマンドを使用します。パケット VLAN を削除するには、このコマンドの **no** 形式を使用します。

packet vlan {*vlan-number*}

no packet vlan {*vlan-number*}

構文の説明

vlan-number	パケット VLAN ID を指定します。有効値の範囲は、1 ～ 3967 と 4048 ～ 4093 です。

デフォルト

なし

コマンド モード

SVS ドメイン（config-svs-domain）

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、パケット VLAN 261 を作成する例を示します。

```
n1000v# configure terminal
n1000v(config)# svs-domain
n1000v(config-svs-domain)# packet vlan 261
n1000v(config-svs-domain)#
```

次に、パケット VLAN 261 を削除する例を示します。

```
n1000v# configure terminal
n1000v(config)# svs-domain
n1000v(config-svs-domain)# no packet vlan 261
n1000v(config-svs-domain)#
```

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションに関する情報を表示します。

password strength-check

パスワードの強度の確認をイネーブルにするには、**password strength-check** コマンドを使用します。パスワードの強度の確認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。

password strength-check

no password strength-check

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

この機能は、デフォルトでイネーブルにされています。

コマンド モード

グローバル コンフィギュレーション（config）

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、パスワードの強度の確認をイネーブルにする例を示します。

```
n1000v# config t
n1000v(config)# password strength-check
n1000v(config)#
```

次に、パスワードの強度の確認をディセーブルにする例を示します。

```
n1000v# config t
n1000v(config)# no password strength-check
n1000v(config)#
```

関連コマンド

コマンド	説明
show password strength-check	パスワードの強度の確認の設定を表示します。
username	ユーザ アカウントを作成します。
role name	ユーザ ロールに名前をつけて、そのロールのロール コンフィギュレーション モードに切り替えます。

permit（IPv4）

条件と一致するトラフィックを許可する IPv4 アクセス コントロール リスト（ACL）ルールを作成するには、**permit** コマンドを使用します。ル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。

基本構文

[*sequence-number*] **permit** *protocol source destination* [**dscp** *dscp* | **precedence** *precedence*]

no permit *protocol source destination* [**dscp** *dscp* | **precedence** *precedence*]

no *sequence-number*

インターネット制御メッセージ プロトコル

[*sequence-number*] **permit icmp** *source destination* [*icmp-message*] [**dscp** *dscp* | **precedence** *precedence*]

インターネット グループ管理プロトコル

[*sequence-number*] **permit igmp** *source destination* [*igmp-message*] [**dscp** *dscp* | **precedence** *precedence*]

インターネット プロトコル v4（IPv4）

[*sequence-number*] **permit ip** *source destination* [**dscp** *dscp* | **precedence** *precedence*]

伝送制御プロトコル（TCP）

[*sequence-number*] **permit tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **precedence** *precedence*]

ユーザ データグラム プロトコル

[*sequence-number*] **permit udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **precedence** *precedence*]

構文の説明

sequence-number	（任意）**permit** コマンドのシーケンス番号。デバイスによってアクセス リストの該当番号の位置にコマンドが挿入されます。シーケンス番号は、ACL 内でルールの順序を保ちます。 シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。 デフォルトでは、ACL の最初のルールには、10 のシーケンス番号が与えられます。 シーケンス番号を指定しないと、デバイスによって、ACL の最後にルールが追加され、1 つ前のルールのシーケンス番号に 10 を加算した値が、シーケンス番号として割り当てられます。 ルールのシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
protocol	ルールで一致させるパケットのプロトコルの名前または番号。有効な番号は、0 ～ 255 です。有効なプロトコル名は、次のキーワードです。 • **icmp**：ルールを ICMP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*icmp-message* 引数を使用できます。 • **igmp**：ルールを IGMP トラフィックだけに適用します。このキーワードを使用すると、***protocol*** 引数のすべての有効値に使用できるキーワードに加え、***igmp-type*** 引数を使用できます。 • **ip**：このルールがすべての IPv4 トラフィックに適用されることを指定します。このキーワードを使用する場合は、すべての IPv4 プロトコルに適用される他のキーワードおよび引数だけを使用できます。使用できるキーワードには次のものがあります。 – **dscp** – **precedence** • **tcp**：ルールを TCP トラフィックだけに適用します。このキーワードを使用すると、***protocol*** 引数のすべての有効値に使用できるキーワードに加え、***flags*** 引数および **operator** 引数、**portgroup** キーワードおよび ***established*** キーワードを使用できます。 • **udp**：ルールを UDP トラフィックだけに適用します。このキーワードを使用すると、***protocol*** 引数のすべての有効値に使用できるキーワードに加え、**operator** 引数および ***portgroup*** キーワードを使用できます。
source	ルールで一致させる送信元 IPv4 アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の項の「送信元と宛先」の説明を参照してください。
destination	ルールで一致させる宛先 IPv4 アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の項の「送信元と宛先」の説明を参照してください。

dscp *dscp*	（任意）IP ヘッダーの DSCP フィールドに特定の 6 ビット diffserv（ディファレンシエーテッド サービス）値が設定されているパケットだけをルールと一致させるように指定します。*dscp* 引数には、次の数値またはキーワードのいずれかを指定します。 • 0 ～ 63：DSCP フィールドの 6 ビットと同等の 10 進数。たとえば 10 を指定した場合、ルールは DSCP フィールドのビットが 001010 であるパケットだけに一致します。 • **af11**：Assured Forwarding（AF）クラス 1、低い廃棄確率（001010） • **af12**：AF クラス 1、中程度の廃棄確率（001100） • **af13**：AF クラス 1、高い廃棄確率（001110） • **af21**：AF クラス 2、低い廃棄確率（010010） • **af22**：AF クラス 2、中程度の廃棄確率（010100） • **af23**：AF クラス 2、高い廃棄確率（010110） • **af31**：AF クラス 3、低い廃棄確率（011010） • **af32**：AF クラス 3、中程度の廃棄確率（011100） • **af33**：AF クラス 3、高い廃棄確率（011110） • **af41**：AF クラス 4、低い廃棄確率（100010） • **af42**：AF クラス 4、中程度の廃棄確率（100100） • **af43**：AF クラス 4、高い廃棄確率（100110） • **cs1**：Class-selector（CS）1、優先順位 1（001000） • **cs2**：CS2、優先順位 2（010000） • **cs3**：CS3、優先順位 3（011000） • **cs4**：CS4、優先順位 4（100000） • **cs5**：CS5、優先順位 5（101000） • **cs6**：CS6、優先順位 6（110000） • **cs7**：CS7、優先順位 7（111000） • **default**：デフォルトの DSCP 値（000000） • **ef**：Expedited Forwarding（EF）（101110）

precedence *precedence*	（任意）*precedence* 引数で指定された値が IP Precedence フィールドに設定されているパケットだけをルールと一致させるように指定します。*precedence* 引数には、次の数値またはキーワードを指定します。 • 0 ～ 7 : IP Precedence フィールドの 3 ビットと同等の 10 進数。たとえば、3 を指定した場合、DSCP フィールドに次のビットが設定されているパケットだけがルールと一致します : 011 • **critical**：優先順位 5（101） • **flash**：優先順位 3（011） • **flash-override**：優先順位 4（100） • **immediate**：優先順位 2（010） • **internet**：優先順位 6（110） • **network**：優先順位 7（111） • **priority**：優先順位 1（001） • **routine**：優先順位 0（000）
icmp-message	（ICMP のみ：任意）ルールと一致させる ICMP メッセージのタイプ。この引数には、0 ～ 255 の整数、または「使用上のガイドライン」の項の「ICMP メッセージ タイプ」にリストされているキーワードの 1 つを指定します。
igmp-message	（IGMP のみ：任意）ルールと一致させる IGMP メッセージのタイプ。*igmp-message* 引数には、0 ～ 15 の整数である IGMP メッセージ番号を指定します。また、次のいずれかのキーワードを指定できます。 • **dvmrp**：Distance Vector Multicast Routing Protocol（DVMRP; ディスタンス ベクトル マルチキャスト ルーティング プロトコル） • **host-query**：ホスト クエリー • **host-report**：ホスト レポート • **pim**：Protocol Independent Multicast（PIM） • **trace**：マルチキャスト トレース

operator port [*port*]	（任意：TCP および UDP のみ）*operator* 引数および *port* 引数の条件と一致する送信元ポートから送信されたパケット、または一致する宛先ポートに送信されたパケットだけを、ルールと一致させます。これらの引数が送信元ポートまたは宛先ポートのどちらに適用されるかは、*source* 引数または *destination* 引数のどちらの後に指定したかによって異なります。 *port* 引数には、TCP または UDP ポートの名前または番号を指定します。有効な番号は 0 ～ 65535 の整数です。有効なポート名のリストは、「使用上のガイドライン」の項の「TCP ポート名」および「UDP ポート名」を参照してください。 2 番目の *port* 引数は、*operator* 引数が範囲である場合だけ必要です。 *operator* 引数には、次のいずれかのキーワードを指定する必要があります。 • **eq**：パケットのポートが *port* 引数と同等である場合だけ一致します。 • **gt**：パケットのポートが *port* 引数より大きい場合および同等ではない場合だけ一致します。 • **lt**：パケットのポートが *port* 引数より小さい場合および同等ではない場合だけ一致します。 • **neq**：パケットのポートが *port* 引数と同等ではない場合だけ一致します。 • **range**：2 つの *port* 引数が必要です。パケットのポートが最初の *port* 引数以上で、2 番目の *port* 引数以下である場合だけ一致します。
flags	（TCP のみ：任意）ルールと一致させる TCP 制御コントロール ビット フラグ。*flags* 引数の値には、次の 1 つ以上のキーワードを指定する必要があります。 • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**

デフォルト

新しく作成した IPv4 ACL には、ルールは含まれていません。

シーケンス番号を指定しないと、デバイスは ACL の最後のルールのシーケンス番号に 10 を加算したシーケンス番号を割り当てます。

コマンド モード

IPv4 ACL コンフィギュレーション（config-acl）

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

パケットに IPv4 ACL が適用されると、ACL 内のすべてのルールに対してパケットが評価されます。パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、デバイスはシーケンス番号が最も低いルールを施行します。

送信元と宛先

source 引数および *destination* 引数は、次のいずれかの方法で指定できます。どのルールも、1 つの引数の指定方法によって、他の引数の指定方法が決まることはありません。ルールの設定時に使用できる *source* 引数および *destination* 引数の指定方法は、次のとおりです。

- アドレスおよびネットワーク ワイルドカード：IPv4 アドレスおよびネットワーク ワイルドカードを使用して、送信元または宛先とするホストまたはネットワークを指定できます。構文は次のとおりです。

  IPv4-address network-wildcard

  次に、192.168.67.0 サブネットの IPv4 アドレスおよびネットワーク ワイルドカードを使用して、*source* 引数を指定する例を示します。

  ```
  n1000v(config-acl)# permit tcp 192.168.67.0 0.0.0.255 any
  ```

- アドレスおよび Variable-Length Subnet Mask（VLSM; 可変長サブネット マスク）：IPv4 アドレスおよび VLSM を使用して、送信元または宛先とするホストまたはネットワークを指定できます。構文は次のとおりです。

  IPv4-address/prefix-len

  次に、192.168.67.0 サブネットの IPv4 アドレスおよび VLSM を使用して、*source* 引数を指定する例を示します。

  ```
  n1000v(config-acl)# permit udp 192.168.67.0/24 any
  ```

- ホスト アドレス：**host** キーワードおよび IPv4 アドレスを使用して、送信元または宛先とするホストを指定できます。構文は次のとおりです。

  host *IPv4-address*

  この構文は、*IPv4-address*/32 および *IPv4-address* 0.0.0.0 と同じです。

  次に、*host* キーワードおよび 192.168.67.132 IPv4 アドレスを使用して、**source** 引数を指定する例を示します。

  ```
  n1000v(config-acl)# permit icmp host 192.168.67.132 any
  ```

- 任意のアドレス：**any** キーワードを使用して、送信元または宛先として任意の IPv4 アドレスを指定できます。**any** キーワードの使用例は、このセクションの例を参照してください。各例に、**any** キーワードを使用した送信元または宛先の指定方法が示されています。

ICMP メッセージ タイプ

igmp-message 引数には、0 ～ 255 の整数である ICMP メッセージ番号を指定できます。また、次のいずれかのキーワードを指定できます。

- **administratively-prohibited**：管理上の禁止
- **alternate-address**：代替アドレス
- **conversion-error**：データグラム変換
- **dod-host-prohibited**：ホスト禁止
- **dod-net-prohibited**：ネット禁止
- **echo**：エコー（ping）

- **echo-reply**：エコー応答
- **general-parameter-problem**：パラメータの問題
- **host-isolated**：ホスト分離
- **host-precedence-unreachable**：優先順位のホスト到達不能
- **host-redirect**：ホスト リダイレクト
- **host-tos-redirect**：ToS ホスト リダイレクト
- **host-tos-unreachable**：ToS ホスト到達不能
- **host-unknown**：ホスト未知
- **host-unreachable**：ホスト到達不能
- **information-reply**：情報応答
- **information-request**：情報要求
- **mask-reply**：マスク応答
- **mask-request**：マスク要求
- **mobile-redirect**：モバイル ホスト リダイレクト
- **net-redirect**：ネットワーク リダイレクト
- **net-tos-redirect**：ToS ネット リダイレクト
- **net-tos-unreachable**：ToS ネット到達不能
- **net-unreachable**：ネット到達不能
- **network-unknown**：ネットワーク未知
- **no-room-for-option**：パラメータが必要だが空きなし
- **option-missing**：パラメータが必要だが存在しない
- **packet-too-big**：フラグメンテーションが必要、DF 設定
- **parameter-problem**：すべてのパラメータの問題
- **port-unreachable**：ポート到達不能
- **precedence-unreachable**：優先順位カットオフ
- **protocol-unreachable**：プロトコル到達不能
- **reassembly-timeout**：再構成タイムアウト
- **redirect**：すべてのリダイレクト
- **router-advertisement**：ルータ ディスカバリ アドバタイズメント
- **router-solicitation**：ルータ ディスカバリ要求
- **source-quench**：送信元抑制
- **source-route-failed**：送信元ルート障害
- **time-exceeded**：すべてのタイム超過メッセージ
- **timestamp-reply**：タイムスタンプ応答
- **timestamp-request**：タイムスタンプ要求
- **traceroute**：トレースルート
- **ttl-exceeded**：TTL 超過
- **unreachable**：すべての到達不能

TCP ポート名

protocol 引数に **tcp** を指定した場合、*port* 引数として 0 ～ 65535 の整数である TCP ポート番号を指定できます。また、次のいずれかのキーワードを指定できます。

bgp：ボーダー ゲートウェイ プロトコル（BGP）（179）

chargen：キャラクタ ジェネレータ（19）

cmd：リモート コマンド（rcmd、514）

daytime：デイタイム（13）

discard：廃棄（9）

domain：ドメイン ネーム サービス（DNS）（53）

drip：ダイナミック ルーティング情報プロトコル（DRIP）（3949）

echo：エコー（7）

exec：Exec（rsh、512）

finger：フィンガー（79）

ftp：File Transfer Protocol（FTP; ファイル転送プロトコル）（21）

ftp-data：FTP データ接続（2）

gopher：Gopher（7）

hostname：NIC ホストネーム サーバ（11）

ident：Ident プロトコル（113）

irc：Internet Relay Chat（IRC; インターネット リレー チャット）（194）

klogin：Kerberos ログイン（543）

kshell：Kerberos シェル（544）

login：ログイン（rlogin、513）

lpd：プリンタ サービス（515）

nntp：Network News Transport Protocol（NNTP）（119）

pim-auto-rp：PIM Auto-RP（496）

pop2：Post Office Protocol v2（POP2）（19）

pop3：Post Office Protocol v3（POP3）（11）

smtp：Simple Mail Transport Protocol（SMTP; シンプル メール転送プロトコル）（25）

sunrpc：Sun Remote Procedure Call（RPC; リモート プロシージャ コール）（111）

tacacs：TAC Access Control System（49）

talk：Talk（517）

telnet：Telnet（23）

time：Time（37）

uucp：UNIX-to-UNIX Copy Program（UUCP; UNIX 間コピー プログラム）（54）

whois：WHOIS/NICNAME（43）

www：World Wide Web（HTTP、8）

UDP ポート名

protocol 引数に **udp** を指定した場合、*port* 引数として 0 ～ 65535 の整数である UDP ポート番号を指定できます。また、次のいずれかのキーワードを指定できます。

biff：BIFF（メール通知、comsat、512）

bootpc：Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）クライアント（68）

bootps：ブートストラップ プロトコル（BOOTP）サーバ（67）

discard：廃棄（9）

dnsix：DNSIX セキュリティ プロトコル監査（195）

domain：ドメイン ネーム サービス（DNS）（53）

echo：エコー（7）

isakmp：Internet Security Association and Key Management Protocol（ISAKMP）（5）

mobile-ip：モバイル IP レジストレーション（434）

nameserver：IEN116 ネーム サービス（旧式、42）

netbios-dgm：NetBIOS データグラム サービス（138）

netbios-ns：NetBIOS ネーム サービス（137）

netbios-ss：NetBIOS セッション サービス（139）

non500-isakmp：Internet Security Association and Key Management Protocol（ISAKMP）（45）

ntp：Network Time Protocol（NTP; ネットワーク タイム プロトコル）（123）

pim-auto-rp：PIM Auto-RP（496）

rip：Routing Information Protocol（RIP）（ルータ、in.routed、52）

snmp：Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）（161）

snmptrap：SNMP トラップ（162）

sunrpc：Sun Remote Procedure Call（RPC; リモート プロシージャ コール）（111）

syslog：システム ロギング（514）

tacacs：TAC Access Control System（49）

talk：Talk（517）

tftp：Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）（69）

time：Time（37）

who：Who サービス（rwho、513）

xdmcp：X Display Manager Control Protocol（XDMCP）（177）

例

次に、acl-lab-01 という IPv4 ACL を作成し、10.23.0.0 および 192.168.37.0 ネットワークから 10.176.0.0 ネットワークへのすべての TCP および UDP トラフィックを許可するルールを設定する例を示します。

```
n1000v# config t
n1000v(config)# ip access-list acl-lab-01
n1000v(config-acl)# permit tcp 10.23.0.0/16 10.176.0.0/16
n1000v(config-acl)# permit udp 10.23.0.0/16 10.176.0.0/16
n1000v(config-acl)# permit tcp 192.168.37.0/16 10.176.0.0/16
n1000v(config-acl)# permit udp 192.168.37.0/16 10.176.0.0/16
```

次に、acl-eng-to-marketing という IPv4 ACL を作成し、eng_workstations という IP アドレス オブジェクト グループから marketing_group という IP アドレス オブジェクト グループへのすべての IP トラフィックを許可するルールを設定する例を示します。

```
n1000v# config t
n1000v(config)# ip access-list acl-eng-to-marketing
n1000v(config-acl)# permit ip addrgroup eng_workstations addrgroup marketing_group
```

関連コマンド

コマンド	説明
deny（IPv4）	IPv4 ACL に拒否（deny）ルールを設定します。
ip access-list	IPv4 ACL を設定します。
remark	ACL に備考を設定します。
show ip access-list	すべての IPv4 ACL または 1 つの IPv4 ACL を表示します。
statistics per-entry	ACL の各エントリの統計情報の収集をイネーブルにします。

permit（MAC）

条件と一致するトラフィックを許可する MAC ACL ルールを作成するには、**permit** コマンドを使用します。ル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。

[*sequence-number*] **permit** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *vlan-id*]

no permit *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *vlan-id*]

no *sequence-number*

構文の説明

sequence-number	（任意）**permit** コマンドのシーケンス番号。デバイスによってアクセス リストの該当番号の位置にコマンドが挿入されます。シーケンス番号は、ACL 内でルールの順序を保ちます。 シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。 デフォルトでは、ACL の最初のルールには、10 のシーケンス番号が与えられます。 シーケンス番号を指定しないと、デバイスによって、ACL の最後にルールが追加され、1 つ前のルールのシーケンス番号に 10 を加算した値が、シーケンス番号として割り当てられます。 ルールのシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
source	ルールで一致させる送信元 MAC アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の項の「送信元と宛先」の説明を参照してください。
destination	ルールで一致させる宛先 MAC アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の項の「送信元と宛先」の説明を参照してください。
protocol	（任意）ルールで一致させるプロトコルの番号。有効なプロトコル番号は 0x0 ～ 0xffff です。有効なプロトコル名のリストは、「使用上のガイドライン」の項の「MAC プロトコル」を参照してください。
cos *cos-value*	（任意）IEEE 802.1Q ヘッダーに、*cos-value* 引数で指定したサービス クラス（CoS）値が含まれているパケットだけを一致させるルールを指定します。*cos-value* 引数は、0 ～ 7 の整数です。
vlan *vlan-id*	（任意）IEEE 802.1Q ヘッダーに、指定した VLAN ID が含まれているパケットだけを一致させるルールを指定します。*vlan-id* 引数は、1 ～ 4094 の整数に指定できます。

デフォルト

なし

コマンド モード

MAC ACL コンフィギュレーション（config-acl）

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

新しく作成した MAC ACL には、ルールは含まれていません。

シーケンス番号を指定しないと、ACL の最後のルールのシーケンス番号に 10 を加算したシーケンス番号が割り当てられます。

パケットに MAC ACL が適用されると、ACL 内のすべてのルールに対してパケットが評価されます。パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、デバイスはシーケンス番号が最も低いルールを施行します。

送信元と宛先

source 引数および *destination* 引数は、次のいずれかの方法で指定できます。どのルールも、1 つの引数の指定方法によって、他の引数の指定方法が決まることはありません。ルールの設定時に使用できる *source* 引数および *destination* 引数の指定方法は、次のとおりです。

- アドレスおよびマスク：MAC アドレスの後にマスクを指定して、1 つのアドレスまたはアドレスグループを指定できます。構文は次のとおりです。

  ```
  MAC-address MAC-mask
  ```

  次に、*source* 引数に、MAC アドレス 00c0.4f03.0a72 を指定する例を示します。

  ```
  n1000v(config-acl)# permit 00c0.4f03.0a72 0000.0000.0000 any
  ```

  次に、*destination* 引数に、MAC ベンダー コードが 00603e のすべてのホストの MAC アドレスを指定する例を示します。

  ```
  n1000v(config-acl)# permit any 0060.3e00.0000 0000.0000.0000
  ```

- 任意のアドレス：**any** キーワードを使用して、送信元または宛先として任意の MAC アドレスを指定できます。**any** キーワードの使用例は、このセクションの例を参照してください。各例に、**any** キーワードを使用した送信元または宛先の指定方法が示されています。

MAC プロトコル

protocol 引数には、MAC プロトコルの番号またはキーワードを指定します。プロトコル番号は、プレフィクスが 0x である 4 バイト 16 進数です。有効なプロトコル番号は 0x0 ～ 0xffff です。有効なキーワードは、次のとおりです。

- **aarp**：Appletalk ARP（0x80f3）
- **appletalk**：Appletalk（0x809b）
- **decnet-iv**：DECnet Phase IV（0x6003）
- **diagnostic**：DEC 診断プロトコル（0x6005）
- **etype-6000**：Ethertype 0x6000（0x6000）
- **etype-8042**：Ethertype 0x8042（0x8042）
- **ip**：インターネット プロトコル v4（0x0800）
- **lat**：DEC LAT（0x6004）
- **lavc-sca**：DEC LAVC、SCA（0x6007）
- **mop-console**：DEC MOP リモート コンソール（0x6002）
- **mop-dump**：DEC MOP ダンプ（0x6001）

- **vines-echo**：VINES エコー（0x0baf）

例

次に、2 つの MAC アドレス グループ間ですべての IPv4 トラフィックを許可するルールが含まれる mac-ip-filter という名前の MAC ACL を作成する例を示します。

```
n1000v# config t
n1000v(config)# mac access-list mac-ip-filter
n1000v(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff
ip
```

関連コマンド

コマンド	説明
deny（MAC）	MAC ACL に拒否（deny）ルールを設定します。
mac access-list	MAC ACL を設定します。
remark	ACL に備考を設定します。
statistics per-entry	ACL の各エントリの統計情報の収集をイネーブルにします。
show mac access-list	すべての MAC ACL または 1 つの MAC ACL を表示します。

permit interface

このロールに割り当てられたユーザにアクセスを許可するインターフェイスを指定するには、**permit interface** コマンドを使用します。

ポリシーの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。

permit interface *interface-list*

no permit interface *interface-list*

構文の説明

interface-list	指定したロールのユーザがアクセスできる 1 つ以上のインターフェイスのリストです。

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（config-role-interface）

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

このロールに割り当てられたユーザにアクセスを許可するインターフェイスがすべて指定されるまで、このコマンドを繰り返します。

例

次に、このロールに割り当てられたユーザにアクセスを許可するインターフェイスとしてイーサネット 2/1-4 を指定する例を示します。

```
n1000v# config t
n1000v(config)# role name network-observer
n1000v(config-role)# interface policy deny
n1000v(config-role-interface)# permit interface ethernet 2/1-4
n1000v(config-role-interface)#
```

次に、イーサネット 2/1-4 のポリシー制限を削除する例を示します。

```
n1000v# config t
n1000v(config)# role name network-observer
n1000v(config-role)# interface policy deny
n1000v(config-role-interface)# no permit interface ethernet 2/1-4
n1000v(config-role-interface)#
```

関連コマンド

コマンド	説明
role name	ユーザ ロールを指定して、そのロールのロール コンフィギュレーション モードを開始します。
interface policy deny	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、このロールによるすべてのインターフェイス アクセスを拒否します。
show role	ロール設定を表示します。

ping

別のデバイスへのネットワーク接続を IPv4 アドレス指定を使用して判別するには、**ping** コマンドを使用します。

ping [*dest-ipv4-address* | *hostname* | **mulitcast** *multicast-group-address* **interface [ethernet** *slot/port* | **loopback** *number* | **mgmt0** | **port-channel** *channel-number* | **vethernet** *number***]**] [**count** {*number* | **unlimited**}] [**df-bit**] [**interval** *seconds*] [**packet-size** *bytes*] [**source** *src-ipv4-address*] [**timeout** *seconds*] [**vrf** *vrf-name*]

構文の説明

dest-ipv4-address	宛先デバイスの IPv4 アドレスを指定します。形式は、*A.B.C.D* です。
hostname	宛先デバイスのホスト名。ホスト名では、大文字と小文字が区別されます。
multicast	マルチキャスト ping です。
multicast-group-address	マルチキャスト グループ アドレスを指定します。形式は、*A.B.C.D* です。
interface	マルチキャスト パケットを送信するインターフェイスを指定します。
ethernet *slot/port*	イーサネット インターフェイスのスロットとポート番号を指定します。
loopback *number*	仮想インターフェイス番号を 0 ～ 1023 の範囲内で指定します。
mgmt0	管理インターフェイスを指定します。
port-channel *channel-number*	ポート チャネル インターフェイスを 1 ～ 4096 の範囲内で指定します。
vethernet *number*	仮想イーサネット インターフェイスを 1 ～ 1048575 の範囲内で指定します。
count	（任意）送信の回数を指定します。
number	ping の数。有効な範囲は 1 ～ 655350 です。デフォルトは 5 です。
unlimited	無制限の回数の ping を許可します。
df-bit	（任意）IPv4 ヘッダーの do-not-fragment ビットをイネーブルにします。デフォルトはディセーブルです。
interval *seconds*	（任意）送信の間隔を秒数で指定します。有効な範囲は 0 ～ 60 です。デフォルトは 1 秒です。
packet-size *bytes*	（任意）送信するパケットサイズをバイト数で指定します。有効な範囲は 1 ～ 65468 です。デフォルト値は 56 バイトです。
source *scr-ipv4-address*	（任意）使用する送信元 IPv4 アドレスを指定します。形式は、*A.B.C.D* です。デフォルトは、デバイスの管理インターフェイスの IPv4 アドレスです。
timeout *seconds*	（任意）無応答タイムアウトの間隔を秒数で指定します。指定できる範囲は 1 ～ 60 です。デフォルト値は 2 秒です。
vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF; 仮想ルーティングおよびフォワーディング）の名前を指定します。デフォルトはデフォルト VRF です。

デフォルト

デフォルト値については、このコマンドの「構文の説明」の項を参照してください。

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

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 IPv6 アドレスを使用して別のデバイスとのネットワーク接続を確認するには、**ping6** コマンドを使用します。

例 次に、別のデバイスへの接続を IPv4 アドレス指定を使用して判別する例を示します。

```
n1000v# ping 172.28.231.246 vrf management
PING 172.28.231.246 (172.28.231.246): 56 data bytes
Request 0 timed out
64 bytes from 172.28.231.246: icmp_seq=1 ttl=63 time=0.799 ms
64 bytes from 172.28.231.246: icmp_seq=2 ttl=63 time=0.597 ms
64 bytes from 172.28.231.246: icmp_seq=3 ttl=63 time=0.711 ms
64 bytes from 172.28.231.246: icmp_seq=4 ttl=63 time=0.67 ms

--- 172.28.231.246 ping statistics ---
5 packets transmitted, 4 packets received, 20.00% packet loss
round-trip min/avg/max = 0.597/0.694/0.799 ms
```

関連コマンド

コマンド	説明
ping6	IPv6 アドレスを使用して別のデバイスとの接続を確認します。

pinned-sgid

コントロールまたはパケット VLAN のトラフィックを特定のサブグループに固定（ピニング）するには、**pinning** 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。

pinned-sgid {**control-vlan-pinned-sgid** | **packet-vlan-pinned-sgid**} *sub-group_id*

no pinned-sgid {**control-vlan-pinned-sgid** | **packet-vlan-pinned-sgid**} *sub-group_id*

構文の説明

control-vlan-pinned-sgid	コントロール VLAN トラフィックを特定のサブグループに固定することを指定します。
packet-vlan-pinned-sgid	パケット VLAN トラフィックを特定のサブグループに固定することを指定します。
sub-group-id	サブグループの ID 番号です。指定できる範囲は 0 ～ 31 です。

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(2)	このコマンドが追加されました。

例

次に、コントロール VLAN 上のトラフィックをサブグループ 0 に固定する例を示します。

```
n1000v# config t
n1000v(config)# port-profile SystemProfile1
n1000v(config-port-prof)# pinned-sgid control-vlan-pinned-sgid 3
n1000v(config-port-prof)# show port-profile SystemProfile1
port-profile SystemProfile1
  description:
  type: ethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: 3
  pinning packet-vlan: -
  system vlans: 1
  port-group: SystemProfile1
  max ports: -
  inherit:
  config attributes:
    switchport mode trunk
    switchport trunk allowed vlan 1-5
    no shutdown
  evaluated config attributes:
    switchport mode trunk
```

```
    switchport trunk allowed vlan 1-5
    no shutdown
  assigned interfaces:
n1000v(config-port-prof)# copy running-config startup-config
```

次に、パケット VLAN 上のトラフィックをサブグループ 0 に固定する例を示します。

```
n1000v# config t
n1000v(config)# port-profile SystemProfile1
n1000v(config-port-prof)# pinned-sgid packet-vlan-pinned-sgid 0
n1000v(config-port-prof)# show port-profile name SystemProfile1
port-profile SystemProfile1
  description:
  type: ethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: 0
  system vlans: 1
  port-group:
  max ports: -
  inherit:
  config attributes:
    switchport mode access
    switchport access vlan 1
    switchport trunk native vlan 1
    no shutdown
  evaluated config attributes:
    switchport mode access
    switchport access vlan 1
    switchport trunk native vlan 1
    no shutdown
  assigned interfaces:
n1000v(config-port-prof)# copy running-config startup-config
```

関連コマンド

コマンド	説明
show port-profile [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]	ポート プロファイル情報を表示します。
show running-config port-profile *profile-name*	指定されたポート プロファイルの実行コンフィギュレーションを表示します。この中に、ピニング コンフィギュレーションも含まれます。

pinning id

仮想イーサネット トラフィックを特定のサブグループに固定（ピニング）するには、**pinning id** 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。

pinning id *sub-group-id*

no pinning id

構文の説明

sub-group-id	サブグループの ID 番号です。指定できる範囲は 0 ～ 31 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 モード（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、仮想イーサネット インターフェイスをサブグループ 3 に固定する例を示します。

```
n1000v(config)# config t
n1000v(config)# interface vethernet 1
n1000v(config-if)# pinning id 0
n1000v(config-if)# show running-config interface vethernet 1
version 4.0(4)SV1(2)

interface Vethernet3
  service-policy type qos input policy1
  pinning id 0

n1000v(config-if)# exit
n1000v(config)# exit
n1000v# module vem 3 execute vemcmd show pinning
  LTL    IfIndex  PC_LTL  VSM_SGID  VEM_SGID  Eff_SGID
   48   1b040000     304         0         0         0

n1000v(config-if)# copy running-config startup-config
```

関連コマンド

コマンド	説明
module vem *module_number* **execute vemcmd show pinning**	指定された VEM のピニング コンフィギュレーションを表示します。
show port-profile [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]	ポート プロファイル情報を表示します。
show running-config interface vethernet *interface-number*	指定された仮想イーサネット インターフェイスの実行コンフィギュレーションを表示します。この中に、ピニング コンフィギュレーションも含まれます。
show running-config port-profile *profile-name*	指定されたポート プロファイルの実行コンフィギュレーションを表示します。この中に、ピニング コンフィギュレーションも含まれます。

police

トラフィック レートを制御するには、**police** コマンドを使用します。制御を削除するには、このコマンドの **no** 形式を使用します。

police {{[**cir**] {*cir* [**bps**|**kbps**|**mbps**|**gbps**] | **percent** *cir-percent*} [[**bc**] {*committed-burst* [**bytes**|**kbytes**|**mbytes**|**ms**|**us**]}] [**pir** {*pir-* [**bps2**|**kbps2**|**mbps2**|**gbps2**] | **percent** *pir-percent*} [[**be**] {*extended-burst* [**bytes2**|**kbytes2**|**mbytes2**|**ms2**|**us2**]}]] [**conform** {**transmit** | **set-prec-transmit** {*precedence-number*} | **set-dscp-transmit** {*dscp-value* | *dscp-number*} | **set-cos-transmit** *cos-value* | **set-discard-class-transmit** *discard-class-value* | **set-qos-transmit** *qos-group-value*} [**exceed** {**drop1** | **set** *exc-from-field exc-to-field* **table cir-markdown-map**}] [**violate** {**drop2** | **set** *vio-from-field vio-to-field* **table2 pir-markdown-map**}]]}}

no police {{[**cir**] {*cir* [**bps**|**kbps**|**mbps**|**gbps**] | **percent** *cir-percent*} [[**bc**] {*committed-burst* [**bytes**|**kbytes**|**mbytes**|**ms**|**us**]}] [**pir** {*pir* [**bps2**|**kbps2**|**mbps2**|**gbps2**] | **percent** *pir-percent*} [[**be**] {*extended-burst* [**bytes2**|**kbytes2**|**mbytes2**|**ms2**|**us2**]}]] [**conform** {**transmit** | **set-prec-transmit** {*precedence-number*} | **set-dscp-transmit** {*dscp-value* | *dscp-number*} | **set-cos-transmit** *cos-value* | **set-discard-class-transmit** *discard-class-value* | **set-qos-transmit** *qos-group-value*} [**exceed** {**drop1** | **set** *exc-from-field exc-to-field* **table cir-markdown-map**}] [**violate** {**drop2** | **set** *vio-from-field vio-to-field* **table2 pir-markdown-map**}]]}}

構文の説明

cir	（任意）Committed Information Rate（CIR; 認定情報レート）を指定します。
cir	**bps**、**kbps**、**mbps**、または **gbps** 単位の CIR です。
bps	（任意）ビット/秒を指定します。
kbps	（任意）キロビット/秒を指定します。
mbps	（任意）メガビット/秒を指定します。
gbps	（任意）ギガビット/秒を指定します。
percent	CIR のパーセンテージを指定します。
cir-percent	CIR のパーセンテージです。
bc	（任意）BC（認定バースト）を指定します。
committed-burst	パケット バーストです。
bytes	（任意）バースト サイズをバイト単位で指定します。
kbytes	（任意）バースト サイズをキロバイト単位で指定します。
mbytes	（任意）バースト サイズをメガバイト単位で指定します。
ms	（任意）バースト間隔をミリ秒単位で指定します。
us	（任意）バースト間隔をマイクロ秒単位で指定します。
pir	（任意）PIR（Peak Information Rate; 最大情報レート）を指定します。
pir	**bps**、**kbps**、**mbps**、または **gbps** 単位の PIR です。
bps2	（任意）ビット/秒を指定します。
kbps2	（任意）キロビット/秒を指定します。
mbps2	（任意）メガビット/秒を指定します。
gbps2	（任意）ギガビット/秒を指定します。
be	（任意）拡張バーストを指定します。
extended-burst	拡張パケット バーストです。

ms2	（任意）バースト間隔をミリ秒単位で指定します。
us2	（任意）バースト間隔をマイクロ秒単位で指定します。
conform	（任意）準拠アクションを指定します。
transmit	パケット送信を指定します。
set-prec-transmit	指定したプレシデンスを送信します。
precedence-number	プレシデンス番号です。有効な番号は次のとおりです。 • 0 - Routine プレシデンス • 1 - Priority プレシデンス • 2 - Immediate プレシデンス • 3 - Flash プレシデンス • 4 - Flash override プレシデンス • 5 - Critical プレシデンス • 6 - Internetwork control プレシデンス • 7 - Network control プレシデンス
set-dscp-transmit	指定した Differentiated Services Code Point（DSCP; DiffServ コード ポイント）を送信します。
dscp-number	DSCP 番号またはコードです。有効な値の範囲は 1 ～ 63 です。DSCP を次のいずれかのコードに設定することもできます。 • af11 - AF11 dscp（001010） • af12 - AF12 dscp（001100） • af13 - AF13 dscp（001110） • af21 - AF21 dscp（010010） • af22 - AF22 dscp（010100） • af23 - AF23 dscp（010110） • af31 - AF31 dscp（011010） • af32 - AF32 dscp（011100） • af33 - AF33 dscp（011110） • af41 - AF41 dscp（100010） • af42 - AF42 dscp（100100） • af43 - AF43 dscp（100110） • cs1 - CS1（プレシデンス 1）dscp（001000） • cs2 - CS2（プレシデンス 2）dscp（010000） • cs3 - CS3（プレシデンス 3）dscp（011000） • cs4 - CS4（プレシデンス 4）dscp（100000） • cs5 - CS5（プレシデンス 5）dscp（101000） • cs6 - CS6（プレシデンス 6）dscp（110000） • cs7 - CS7（プレシデンス 7）dscp（111000） • default - デフォルト dscp（000000） • ef - EF dscp（101110）

set-cos-transmit	指定した CoS 番号を送信します。
cos-value	CoS グループ番号です。有効な値の範囲は、0 ～ 7 です。
set-discard-class-transmit	指定した廃棄クラス番号を送信します。
discard-class-value	廃棄クラス番号です。有効な値の範囲は、0 ～ 63 です。
set-qos-transmit	指定した QoS グループ番号を送信します。
qos-group-value	QoS グループ番号です。有効な値の範囲は、0 ～ 126 です。
exceed	（任意）超過アクションです。
drop1	パケットをドロップすることを指定します。
set	テーブルまたはマークダウン マップの中の特定の値を指定します。
exc-from-field	.
exc-to-field	.
table	.
cir-markdown-map	.
violate	（任意）違反アクションを指定します。
drop2	パケットをドロップすることを指定します。
vio-from-field	.
vio-to-field	.
table2	.
pir-markdown-map	.

デフォルト

なし

コマンド モード

ポリシー マップ コンフィギュレーション（config-pmap-c-qos）

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、トラフィック レートを制御する例を示します。

```
n1000v# configure terminal
n1000v(config)# policy-map pm10
n1000v(config-pmap-qos)# class class-default
n1000v(config-pmap-c-qos)# police 100000 bps 10000 bytes
n1000v(config-pmap-c-qos)#
```

関連コマンド

コマンド	説明
show policy-map	すべてのポリシー マップ、または指定したポリシー マップに対するポリシー マップ設定を表示します。

policy-map

QoS ポリシー マップを作成および設定するには、**policy-map** コマンドを使用します。ポリシー 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。

policy-map {*name* | **type qos** *name*}

no policy-map {*name* | **type qos** *name*}

構文の説明

name	ポリシー マップ名です。有効な値の範囲は、1 ～ 40 です。
type qos	ポリシー マップのタイプを「QoS」と指定します。

デフォルト

ポリシー マップは存在しません。

コマンド モード

グローバル コンフィギュレーション（config）

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

ポリシー マップを作成または設定するときは、自動的にポリシー マップ コンフィギュレーション モードが開始します。

例

次に、ポリシー マップを作成する例を示します。

```
n1000v# configure terminal
n1000v(config)# policy-map pm20
n1000v(config-pmap-qos)#
```

次に、ポリシー マップを削除する例を示します。

```
n1000v# configure terminal
n1000v(config)# no policy-map pm20
n1000v(config)#
```

関連コマンド

コマンド	説明
show policy-map	ポリシー マップの情報を表示します。

policy-map type queuing

キューイング パケットの QoS クラスベース重み付け均等化キューイング（CBWFQ）のポリシー マップを作成または変更するには、**policy-map type queuing** コマンドを使用します。ポリシー マップをデフォルトの状態にするには、このコマンドの **no** 形式を使用します。

policy-map {[name | **type queuing** *name*] | **[match-first] }**

no policy-map {[name | **type queuing** *name*] | **[match-first] }**

構文の説明

name	ポリシー マップ名です。最大 40 文字までの英数字で指定します。
match-first	最初に一致したクラスのアクションを実行します。

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
4.2(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

policy-map type queueing コマンドは、アップリンク ポートでのみサポートされます。

例

次に、my_policymap1 という名前のキューイング タイプのポリシー マップを作成する例を示します。

```
n1000v# config t
n1000v(config)# policy-map type queuing my_policy1
n1000v(config-pmap-que)
```

次に、my_policymap1 という名前のキューイング タイプのポリシー マップを削除する例を示します。

```
n1000v# config t
n1000v(config)# no policy-map type queuing my_policy1
```

関連コマンド

コマンド	説明
show policy-map	ポリシー マップの情報を表示します。
class type queuing	指定したポリシー マップにクラスベース重み付け均等化キューイング（CBWFQ）クラスを割り当てます。
show policy-map type queuing	システムで設定されているすべてのキューイング ポリシー マップを表示します。

port-binding

ポート プロファイルのポート バインディングを設定するには、**port-binding** 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。

port-binding {static | dynamic | ephemeral}

no port-binding [static | dynamic | ephemeral]

構文の説明

static	スタティック ポート バインディングを指定します。ポートは、VM の電源がオンのときに接続され、電源がオフになると切断されます。最大ポート数の制限が適用されます。
dynamic	ダイナミック ポート バインディングを指定します。ポートは、VM の電源がオンのときに作成され、電源がオフになると破棄されます。最大ポート数の制限は適用されません。
ephemeral	エフェメラル ポート バインディングを指定します。ポートは、VM の電源がオンのときに作成され、電源がオフになると破棄されます。最大ポート数の制限は適用されません。

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
4.2(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、accessprof という名前の vEthernet ポート プロファイルにスタティック ポート バインディングを追加する例を示します。

```
n1000v# config t
n1000v(config)# port-profile type accessprof
n1000v(config-port-prof)# port-binding static
n1000v(config-port-prof)#
```

次に、accessprof という名前の vEthernet ポート プロファイルからスタティック ポート バインディングを削除する例を示します。

```
n1000v# config t
n1000v(config)# port-profile type accessprof
```

```
n1000v(config-port-prof)# no port-binding static
n1000v(config-port-prof)#
```

関連コマンド

コマンド	説明
show port-profile name profile_name	指定されたポート プロファイルの設定を表示します。
port-profile	ポート プロファイルを作成します。

port-channel load-balance ethernet

チャネル グループのインターフェイスのロード バランシングをするアルゴリズムを設定するには、**port-channel load-balance ethernet** 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。

port-channel load-balance ethernet *algorithm* [**module** *module*]

no port-channel load-balance ethernet [*algorithm* [**module** *module*]]

構文の説明

algorithm	ロードバランシング方式をモジュールに対してまたはグローバルに指定します。
dest-ip-port	宛先 IP アドレスおよび L4 ポート
dest-ip-port-vlan	宛先 IP アドレス、L4 ポート、および VLAN
destination-ip-vlan	宛先 IP アドレスおよび VLAN
destination-mac	宛先 MAC アドレス
destination-port	宛先 L4 ポート
source-dest-ip-port	送信元および宛先 IP アドレスおよび L4 ポート
source-dest-ip-port-vlan	送信元および宛先 IP アドレス、L4 ポート、および VLAN
source-dest-ip-vlan	送信元および宛先 IP アドレスおよび VLAN
source-dest-mac	送信元および宛先 MAC アドレス
source-dest-port	送信元および宛先 L4 ポート
source-ip-port	送信元 IP アドレス
source-ip-port-vlan	送信元 IP アドレス、L4、および VLAN
source-ip-vlan	送信元 IP アドレスおよび VLAN
source-mac	送信元 MAC アドレス（デフォルト）
source-port	送信元ポート
source-virtual-port-id	送信元仮想ポート ID
vlan-only	VLAN のみ
module	（任意）個別にロード バランシングを実行するモジュール番号（1 ～ 66）を指定します。モジュールを指定しない場合は、指定されたアルゴリズムはデバイスのすべてのモジュールに適用されます。

デフォルト

送信元 MAC 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（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

モジュールを指定しない場合、アルゴリズムはすべてのポート チャネルにグローバルに適用されます。

モジュールを指定すると、アルゴリズムは指定されたモジュールのすべてのポート チャネルに適用されます。

グローバルに設定されたアルゴリズムよりもモジュールごとの設定が優先されます。

ポート チャネル上のトラフィックが単一 MAC アドレスだけを宛先とし、宛先 MAC アドレスでバランシングを行う場合、ポート チャネルは、そのポート チャネル内の同じリンクを常に選択します。この場合、送信元アドレスまたは IP アドレスを使用した方が、ロード バランシングの効率がよくなることがあります。

例

次に、チャネル グループのインターフェイス上でロード バランシングを実行するグローバルなアルゴリズムとして送信元ポートを指定する例を示します。

```
n1000v(config)# port-channel load-balance ethernet src-port
n1000v(config)#
```

次に、モジュール 5 のポート チャネルに対して、送信元 IP ロードバランシング アルゴリズムを設定する例を示します。

```
n1000v# config t
n1000v(config)# port-channel load-balance ethernet source-ip module 5
```

関連コマンド

コマンド	説明
show port-channel load-balance	ポート チャネルのロード バランシングに関する情報を表示します。

port-profile

ポート プロファイルを作成してポート プロファイル コンフィギュレーション モードを開始するには、**port-profile** コマンドを使用します。ポート プロファイル コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

port-profile [**type** {**ethernet** | **vethernet**}] *profilename*

no port-profile [**type** {**ethernet** | **vethernet**}] *profilename*

構文の説明

type	（任意）ethernet または vethernet のインターフェイス タイプを指定します。
name	ポート プロファイル名を指定します。名前の長さは最大 80 文字です。

デフォルト

デフォルト タイプは vethernet 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)	ポート プロファイルはアップリンクとして分類されるのではなく、イーサネット タイプまたは vEthernet タイプとして設定されるようになりました。
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 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。

ポート プロファイル タイプはイーサネットまたは vEthernet です。設定が完了すると、タイプは変更できません。

ポート プロファイル タイプをイーサネットとして定義すると、ポート プロファイルを物理（イーサネット）ポートに使用できます。vCenter Server では、対応するポート グループを選択し、物理ポート（PNIC）に割り当てることができます。

ポート プロファイルを Ethernet タイプとして設定すると、VMware 仮想ポートの設定には使用できなくなります。

例

次に、AccessProf という名前のイーサネット タイプ ポート プロファイルを作成する例を示します。

```
n1000v# configure terminal
n1000v(config)# port-profile type ethernet AccessProf
n1000v(config-port-prof)
```

次に、AccessProf という名前のポート プロファイルを削除する例を示します。

```
n1000v# configure terminal
n1000v(config)# no port-profile AccessProf
n1000v(config)
```

関連コマンド

コマンド	説明
show port-profile	割り当てられているロールを含むポート プロファイル設定を表示します。
show running-config port-profile [*profile-name*]	ポート プロファイルの設定を表示します。
port-profile-role	ユーザおよびグループごとにアクセスを制限するためのポート プロファイルのロールを作成します。
vmware port-group [*pg_name*]	VMware ポート グループとしてポート プロファイルを指定します。
switchport mode {**access** | **trunk**}	ポート プロファイル内のインターフェイスをアクセスまたはトランキング ポートとして使用するかどうかを指定します。

port-profile default port-binding

すべての新しい vEthernet ポート プロファイルに自動的に適用されるデフォルト ポート バインディングを設定するには、**port-profile default port-binding** コマンドを使用します。

デフォルト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。

port-profile default port-binding {**static** | **dynamic** | **ephemeral**}

no port-profile default port-binding [**static** | **dynamic** | **ephemeral**]

構文の説明

static	ポートは、ポート グループにポートを割り当てるときに作成されて、アダプタの存続中は維持されます。ポートは常に接続されます。最大ポート数の制限は適用されます。
dynamic	ポートは、VM の電源がオンのときに接続され、電源がオフになると切断されます。最大ポート数の制限は適用されます。
ephemeral	ポートは、VM の電源がオンのときに作成され、電源がオフになると破棄されます。最大ポート数の制限は適用されません。

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

- vEthernet ポート プロファイルが vCenter Server 上のポート グループとしていったん作成されると、その後ポート バインディングのタイプを変更できません。
- エフェメラル ポート バインディングの vEthernet ポート プロファイルに対しては最大ポート数を設定できません。
- イーサネット タイプのポート プロファイルにはポート バインディングを設定できません。ポート バインディングは、vEthernet ポート プロファイルにだけ使用できます。
- システム管理者がインターフェイスのポート プロファイルを変更し、いずれかのポート プロファイルにエフェメラル ポート バインディングが設定されている場合、インターフェイスの手動設定は消去されます。これは、自動消去設定に関係なく発生します。

svs auto-config-purge コマンドの詳細については、『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4)*』を参照してください。

例

次に、作成するすべての新しい vEthernet ポート プロファイルのデフォルトとしてエフェメラル ポート バインディング タイプを設定する例を示します。

```
n1000v# config t
n1000v(config)# port-profile default port-binding ephemeral
n1000v(config)#
```

次に、デフォルト ポート バインディングの設定を削除する例を示します。

```
n1000v# config t
n1000v(config)# no port-profile default port-binding
n1000v(config)#
```

関連コマンド

コマンド	説明
port-profile	ポート プロファイルを作成します。
show port-profile	ポート プロファイルに割り当てられたロールを含むポート プロファイル設定を表示します。
feature port-profile-role	ポート プロファイルのロールの制限のサポートをイネーブルにします。
show port-profile-role	ロール名、説明、割り当てられたユーザ、および割り当てられたグループなど、ポート プロファイルのロール設定を表示します。
inherit port-profile	継承される設定をデフォルトの設定として新しいポート プロファイルに追加します。
port-profile-role	ポート プロファイルのロールを作成します。

port-profile-role

ユーザおよびグループごとにアクセスを制限するためのポート プロファイルのロールを作成するには、**port-profile-role** コマンドを使用します。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。

port-profile-role *port-profile-role-name*

no port-profile-role *port-profile-role-name*

構文の説明

port-profile-role-name	ポート プロファイルのロールの名前を指定します。

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
4.2(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

ポート プロファイルに現在割り当てられているポート プロファイルのロールは削除できません。最初に、ポート プロファイルからロールを削除する必要があります。

例

次に、adminUser ポート プロファイルのロールを作成する例を示します。

```
n1000v# config t
n1000v(config)# port-profile-role adminUser
n1000v(config-port-prof-role)#
```

次に、adminUser ポート プロファイルのロールを削除する例を示します。

```
n1000v# config t
n1000v(config)# no port-profile-role adminUser
n1000v(config)#
```

次に、adminUser ポート プロファイルのロールをポート プロファイルに割り当てられているままで削除しようとすると表示されるエラー メッセージの例を示します。

```
n1000v(config)# no port-profile-role adminUser
ERROR: Cannot remove role because it is assigned to one or more port-profiles
n1000v(config)#
```

関連コマンド

コマンド	説明
show port-profile-role	ロール名、説明、割り当てられたユーザ、および割り当てられたグループなど、ポート プロファイルのロール設定を表示します。
show port-profile-role users	使用可能なユーザおよびグループを表示します。
show port-profile	ポート プロファイルに割り当てられたロールを含むポート プロファイル設定を表示します。
user	ポート プロファイルのロールにユーザを割り当てます。
group	ポート プロファイルのロールにグループを割り当てます。
assign port-profile-role	特定のポート プロファイルにポート プロファイルのロールを割り当てます。
feature port-profile-role	ポート プロファイルのロールの制限のサポートをイネーブルにします。
port-profile	ポート プロファイルを作成します。

port-security stop learning

ポートが新しい MAC アドレスを学習することがないように Drop on Source Miss（DSM）ビットをポートに設定するには、**port-security stop learning** コマンドを使用します。DSM ビットをクリアするには、このコマンドの **no** 形式を使用します。

port-security stop learning

no port-security stop learning

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

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。

例

次に、ポートの DSM ビットを設定する例を示します。

```
n1000v# port-security stop learning
n1000v#
```

次に、ポートの DSM ビットをクリアする例を示します。

```
n1000v# no port-security stop learning
n1000v#
```

関連コマンド

コマンド	説明
show port-security	システムで保護されている MAC アドレスを表示します。
module vem execute	Cisco Nexus 1000V から仮想イーサネット モジュール（VEM）でコマンドをリモートで実行します。
show cdp neighbors	アップストリーム デバイスの設定と機能を表示します。

private-vlan association

プライマリおよびセカンダリ プライベート VLAN 間の関連付けを設定するには、**private-vlan association** コマンドを使用します。関連付けを削除するには、このコマンドの **no** 形式を使用します。

private-vlan association [{**add** | **remove**}] *secondary-vlan-ids*

no private-vlan association [*secondary-vlan-ids*]

構文の説明

add	プライベート VLAN リストにセカンダリ VLAN を追加します。
remove	プライベート VLAN リストからセカンダリ VLAN を削除します。
secondary-vlan-ids	追加または削除するセカンダリ VLAN の ID。

デフォルト

なし

コマンド モード

VLAN（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

設定するプライベート VLAN コマンドが CLI で表示されるようにするには、プライベート VLAN 機能（**feature private-vlan** コマンド）をイネーブルにする必要があります。

例

次に、セカンダリ VLAN 303 にプライマリ VLAN 202 を関連付ける例を示します。

```
n1000v#configure t
n1000v(config)# vlan 202
n1000v(config-vlan)# private-vlan association add 303
n1000v(config-vlan)#
```

関連コマンド

コマンド	説明
private-vlan primary	プライベート VLAN をプライマリに指定します。
private-vlan {**community** | **isolated**}	プライベート VLAN をコミュニティまたは独立に指定します。
show vlan private-vlan	プライベート VLAN の設定を表示します。

private-vlan { community | isolated}

コミュニティまたは独立プライベート VLAN として VLAN を指定するには、**private-vlan** {**community | isolated**} 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。

private-vlan {**community | isolated**}

no private-vlan {**community | isolated**}

構文の説明

community	VLAN をコミュニティ プライマリ VLAN に指定します。
isolated	VLAN を独立プライベート VLAN として指定します。

デフォルト

なし

コマンド モード

VLAN（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

設定するプライベート VLAN コマンドが CLI で表示されるようにするには、プライベート VLAN 機能（**feature private-vlan** コマンド）をイネーブルにする必要があります。

例

次に、コミュニティ プライベート VLAN として VLAN 303 を設定する例を示します。

```
n1000v#configure t
n1000v(config)# vlan 303
n1000v(config-vlan)# private-vlan community
n1000v(config-vlan)#
```

関連コマンド

コマンド	説明
private-vlan primary	プライベート VLAN をプライマリに指定します。
private-vlan association	プライマリ VLAN とセカンダリ VLAN の間の関連付けを設定します
show vlan private-vlan	プライベート VLAN の設定を表示します。

private-vlan primary

プライマリ VLAN としてプライベート VLAN を指定するには、**private-vlan primary** 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。

private-vlan primary

no private-vlan primary

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

VLAN（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

設定するプライベート VLAN コマンドが CLI で表示されるようにするには、プライベート VLAN 機能（**feature private-vlan** コマンド）をイネーブルにする必要があります。

例

次に、プライベート VLAN のプライマリ VLAN として VLAN 202 を設定する例を示します。

```
n1000v#configure t
n1000v(config)# vlan 202
n1000v(config-vlan)# private-vlan primary
n1000v(config-vlan)# show vlan private-vlan
Primary Secondary Type Ports
------- --------- --------------- ----------------------------------------
202 primary
n1000v(config-vlan)#
```

関連コマンド

コマンド	説明
private-vlan {community | isolated}	プライベート VLAN をコミュニティまたは独立に指定します。
show vlan private-vlan	プライベート VLAN の設定を表示します。
private-vlan association	プライマリおよびセカンダリ プライベート VLAN を関連付けます。

protocol vmware-vim

VMware VI SDK をイネーブルにするには、protocol vmware-vim コマンドを使用します。VMware VI SDK 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 vmware-vim

no protocol vmware-vim

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

VMware VI SDK はディセーブルです。

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

VMware VI SDK は、VMware によって公開され、クライアントが VMware vCenter と対話できるようになります。

VMware VI SDK をイネーブルにする前に SVS 接続をまず作成する必要があります。

例

次に、VMware VI SDK をイネーブルにする例を示します。

```
n1000v# configure terminal
n1000v(config)# svs connection svs1
n1000v(config-svs-conn)# protocol vmware-vim
n1000v(config-svs-conn)#
```

関連コマンド

コマンド	説明
show svs connection	SVS 接続の情報を表示します。

pwd

現在のディレクトリを表示するには、**pwd** コマンドを使用します。

pwd

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

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。

例

次に、現在のディレクトリを表示する例を示します。

```
n1000v# pwd
bootflash:
n1000v#
```