P Commands

This chapter describes the Cisco Nexus 1000V commands that begin with the letter P.

password strength-check

To enable password-strength checking, use the **password strength-check** command. To disable the checking of password strength, use the **no** form of this command.

password strength-check

no password strength-check

Syntax Description

This command has no arguments or keywords.

Defaults

This feature is enabled by default.

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Examples

This example shows how to enable the checking of password strength:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# password strength-check
n1000v(config)#
```

This example shows how to disable the checking of password strength:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# no password strength-check
n1000v(config)#
```

Related Commands

Command	Description
role name	Names a user role and places you in role configuration mode for that role.
show password strength-check	Displays the configuration for checking the password strength.
username	Creates a user account.

permit (IPv4)

To create an IPv4 access control list (ACL) rule that permits traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

General Syntax

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

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

no *sequence-number*

Internet Control Message Protocol (ICMP)

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

Internet Group Management Protocol (IGMP)

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

Internet Protocol v4

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

Transmission Control Protocol

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

User Datagram Protocol (UDP)

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

Syntax Description

sequence-number	(Optional) Sequence number of the **permit** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
protocol	Name or number of the protocol of packets that the rule matches. Valid numbers are from 0 to 255. Valid protocol names are the following keywords: • **icmp**—Specifies that the rule applies to ICMP traffic only. When you use this keyword, the *icmp-message* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **igmp**—Specifies that the rule applies to IGMP traffic only. When you use this keyword, the *igmp-type* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **ip**—Specifies that the rule applies to all IPv4 traffic. When you use this keyword, only the other keywords and arguments that apply to all IPv4 protocols are available. They include the following: – **dscp** – **precedence** • **tcp**—Specifies that the rule applies to TCP traffic only. When you use this keyword, the *flags* and *operator* arguments and the **portgroup** and **established** keywords are available, in addition to the keywords that are available for all valid values of the *protocol* argument. • **udp**—Specifies that the rule applies to UDP traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol* argument.
source	Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
destination	Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.

dscp *dscp*	(Optional) Specifies that the rule matches only those packets with the specified 6-bit differentiated services value in the Differentiated Services Code Point (DSCP) field of the IP header. The *dscp* argument can be one of the following numbers or keywords: • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only those packets that have the following bits in the DSCP field: 001010. • **af11**—Assured Forwarding (AF) class 1, low drop probability (001010) • **af12**—AF class 1, medium drop probability (001100) • **af13**—AF class 1, high drop probability (001110) • **af21**—AF class 2, low drop probability (010010) • **af22**—AF class 2, medium drop probability (010100) • **af23**—AF class 2, high drop probability (010110) • **af31**—AF class 3, low drop probability (011010) • **af32**—AF class 3, medium drop probability (011100) • **af33**—AF class 3, high drop probability (011110) • **af41**—AF class 4, low drop probability (100010) • **af42**—AF class 4, medium drop probability (100100) • **af43**—AF class 4, high drop probability (100110) • **cs1**—Class-selector (CS) 1, precedence 1 (001000) • **cs2**—CS2, precedence 2 (010000) • **cs3**—CS3, precedence 3 (011000) • **cs4**—CS4, precedence 4 (100000) • **cs5**—CS5, precedence 5 (101000) • **cs6**—CS6, precedence 6 (110000) • **cs7**—CS7, precedence 7 (111000) • **default**—Default DSCP value (000000) • **if**—Expedited Forwarding (101110)

precedence *precedence*	(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the *precedence* argument. The *precedence* argument can be a number or a keyword, as follows: • 0–7—Decimal equivalent of the 3 bits of the IP Precedence field. For example, if you specify 3, the rule matches only packets that have the following bits in the DSCP field: 011. • **critical**—Precedence 5 (101) • **flash**—Precedence 3 (011) • **flash-override**—Precedence 4 (100) • **immediate**—Precedence 2 (010) • **internet**—Precedence 6 (110) • **network**—Precedence 7 (111) • **priority**—Precedence 1 (001) • **routine**—Precedence 0 (000)
icmp-message	(ICMP only: Optional) ICMP message type that the rule matches. This argument can be an integer from 0 to 255 or one of the keywords listed under "ICMP Message Types" in the "Usage Guidelines" section.
igmp-message	(IGMP only: Optional) IGMP message type that the rule matches. The *igmp-message* argument can be the IGMP message number, which is an integer from 0 to 15. It can also be one of the following keywords: • **dvmrp**—Distance Vector Multicast Routing Protocol • **host-query**—Host query • **host-report**—Host report • **pim**—Protocol Independent Multicast • **trace**—Multicast trace

operator port [*port*]	(Optional; TCP and UDP only) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. The *port* argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see "TCP Port Names" and "UDP Port Names" in the "Usage Guidelines" section. A second *port* argument is required only when the *operator* argument is a range. The *operator* argument must be one of the following keywords: • **eq**—Matches only if the port in the packet is equal to the *port* argument. • **gt**—Matches only if the port in the packet is greater than and not equal to the *port* argument. • **lt**—Matches only if the port in the packet is less than and not equal to the *port* argument. • **neq**—Matches only if the port in the packet is not equal to the *port* argument. • **range**—Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument.
flags	(TCP only; Optional) TCP control bit flags that the rule matches. The value of the *flags* argument must be one or more of the following keywords: • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**

Defaults

A newly created IPv4 ACL contains no rules.

If you do not specify a sequence number, the device assigns to the rule a sequence number that is 10 greater than the last rule in the ACL.

Command Modes

IPv4 ACL configuration (config-acl)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Usage Guidelines

When the device applies an IPv4 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule that has conditions that are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

Source and Destination

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method you use to specify one of these arguments does not affect how you specify the other. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and network wildcard—You can use an IPv4 address followed by a network wildcard to specify a host or a network as a source or destination. The syntax is as follows:

  ```
  IPv4-address network-wildcard
  ```

  This example shows how to specify the *source* argument with the IPv4 address and network wildcard for the 192.168.67.0 subnet:

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

- Address and variable-length subnet mask—You can use an IPv4 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  ```
  IPv4-address/prefix-len
  ```

  This example shows how to specify the *source* argument with the IPv4 address and VLSM for the 192.168.67.0 subnet:

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

- Host address—You can use the **host** keyword and an IPv4 address to specify a host as a source or destination. The syntax is as follows:

  ```
  host IPv4-address
  ```

  This syntax is equivalent to *IPv4-address*/32 and *IPv4-address* 0.0.0.0.

  This example shows how to specify the *source* argument with the **host** keyword and the 192.168.67.132 IPv4 address:

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

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv4 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

ICMP Message Types

The *icmp-message* argument can be the ICMP message number, which is an integer from 0 to 255. It can also be one of the following keywords:

- **administratively-prohibited**—Administratively prohibited
- **alternate-address**—Alternate address
- **conversion-error**—Datagram conversion
- **dod-host-prohibited**—Host prohibited
- **dod-net-prohibited**—Net prohibited
- **echo**—Echo (ping)
- **echo-reply**—Echo reply

- **general-parameter-problem**—Parameter problem
- **host-isolated**—Host isolated
- **host-precedence-unreachable**—Host unreachable for precedence
- **host-redirect**—Host redirect
- **host-tos-redirect**—Host redirect for ToS
- **host-tos-unreachable**—Host unreachable for ToS
- **host-unknown**—Host unknown
- **host-unreachable**—Host unreachable
- **information-reply**—Information replies
- **information-request**—Information requests
- **mask-reply**—Mask replies
- **mask-request**—Mask requests
- **mobile-redirect**—Mobile host redirect
- **net-redirect**—Network redirect
- **net-tos-redirect**—Net redirect for ToS
- **net-tos-unreachable**—Network unreachable for ToS
- **net-unreachable**—Net unreachable
- **network-unknown**—Network unknown
- **no-room-for-option**—Parameter required but no room
- **option-missing**—Parameter required but not present
- **packet-too-big**—Fragmentation needed and DF set
- **parameter-problem**—All parameter problems
- **port-unreachable**—Port unreachable
- **precedence-unreachable**—Precedence cutoff
- **protocol-unreachable**—Protocol unreachable
- **reassembly-timeout**—Reassembly timeout
- **redirect**—All redirects
- **router-advertisement**—Router discovery advertisements
- **router-solicitation**—Router discovery solicitations
- **source-quench**—Source quenches
- **source-route-failed**—Source route failed
- **time-exceeded**—All time exceeded messages
- **timestamp-reply**—Timestamp replies
- **timestamp-request**—Timestamp requests
- **traceroute**—Traceroute
- **ttl-exceeded**—TTL exceeded
- **unreachable**—All unreachables

TCP Port Names

When you specify the *protocol* argument as **tcp**, the *port* argument can be a TCP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

bgp—Border Gateway Protocol (179)

chargen—Character generator (19)

cmd—Remote commands (rcmd, 514)

daytime—Daytime (13)

discard—Discard (9)

domain—Domain Name Service (53)

drip—Dynamic Routing Information Protocol (3949)

echo—Echo (7)

exec—Exec (rsh, 512)

finger—Finger (79)

ftp—File Transfer Protocol (21)

ftp-data—FTP data connections (2)

gopher—Gopher (7)

hostname—NIC hostname server (11)

ident—Ident Protocol (113)

irc—Internet Relay Chat (194)

klogin—Kerberos login (543)

kshell—Kerberos shell (544)

login—Login (rlogin, 513)

lpd—Printer service (515)

nntp—Network News Transport Protocol (119)

pim-auto-rp—PIM Auto-RP (496)

pop2—Post Office Protocol v2 (19)

pop3—Post Office Protocol v3 (11)

smtp—Simple Mail Transport Protocol (25)

sunrpc—Sun Remote Procedure Call (111)

tacacs—TAC Access Control System (49)

talk—Talk (517)

telnet—Telnet (23)

time—Time (37)

uucp—UNIX-to-UNIX Copy Program (54)

whois—WHOIS/NICNAME (43)

www—World Wide Web (HTTP, 8)

UDP Port Names

When you specify the *protocol* argument as **udp**, the *port* argument can be a UDP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

biff—Biff (mail notification, comsat, 512)

bootpc—Bootstrap Protocol (BOOTP) client (68)

bootps—Bootstrap Protocol (BOOTP) server (67)

discard—Discard (9)

dnsix—DNSIX security protocol auditing (195)

domain—Domain Name Service (DNS, 53)

echo—Echo (7)

isakmp—Internet Security Association and Key Management Protocol (5)

mobile-ip—Mobile IP registration (434)

nameserver—IEN116 name service (obsolete, 42)

netbios-dgm—NetBIOS datagram service (138)

netbios-ns—NetBIOS name service (137)

netbios-ss—NetBIOS session service (139)

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

ntp—Network Time Protocol (123)

pim-auto-rp—PIM Auto-RP (496)

rip—Routing Information Protocol (router, in.routed, 52)

snmp—Simple Network Management Protocol (161)

snmptrap—SNMP Traps (162)

sunrpc—Sun Remote Procedure Call (111)

syslog—System Logger (514)

tacacs—TAC Access Control System (49)

talk—Talk (517)

tftp—Trivial File Transfer Protocol (69)

time—Time (37)

who—Who service (rwho, 513)

xdmcp—X Display Manager Control Protocol (177)

Examples

This example shows how to configure an IPv4 ACL named acl-lab-01 with rules permitting all TCP and UDP traffic from the 10.23.0.0 and 192.168.37.0 networks to the 10.176.0.0 network:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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
```

Related Commands

Command	Description
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
ip access-list	Configures an IPv4 ACL.
remark	Configures a remark in an ACL.
show ip access-list	Displays all IPv4 ACLs or one IPv4 ACL.

permit (MAC)

To create a MAC access control list (ACL) rule that permits traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

[*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*

Syntax Description

sequence-number	(Optional) Sequence number of the **permit** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
source	Source MAC addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
destination	Destination MAC addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
protocol	(Optional) Protocol number that the rule matches. Valid protocol numbers are 0x0 to 0xffff. For listings of valid protocol names, see “MAC Protocols” in the “Usage Guidelines” section.
cos *cos-value*	(Optional) Specifies that the rule matches only packets with an IEEE 802.1Q header that contains the Class of Service (CoS) value given in the *cos-value* argument. The *cos-value* argument can be an integer from 0 to 7.
vlan *vlan-id*	(Optional) Specifies that the rule matches only packets with an IEEE 802.1Q header that contains the VLAN identification number given. The *vlan-id* argument can be an integer from 1 to 4094.

Defaults

None

Command Modes

MAC ACL configuration (config-acl)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Usage Guidelines

A newly created MAC ACL contains no rules.

If you do not specify a sequence number, the device assigns a sequence number that is 10 greater than the last rule in the ACL.

When the device applies a MAC ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule that has conditions that are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

Source and Destination

You can specify the *source* and *destination* arguments in one of two ways. In each rule, the method you use to specify one of these arguments does not affect how you specify the other. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and mask—You can use a MAC address followed by a mask to specify a single address or a group of addresses. The syntax is as follows:

  MAC-address MAC-mask

  This example specifies the *source* argument with the MAC address 00c0.4f03.0a72:

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

  This example specifies the *destination* argument with a MAC address for all hosts with a MAC vendor code of 00603e:

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

- Any address—You can use the **any** keyword to specify that a source or destination is any MAC address. For examples of the use of the **any** keyword, see the examples in this section. Each of the examples shows how to specify a source or destination by using the **any** keyword.

MAC Protocols

The *protocol* argument can be the MAC protocol number or a keyword. The protocol number is a four-byte hexadecimal number prefixed with 0x. Valid protocol numbers are from 0x0 to 0xffff. Valid keywords are the following:

- **aarp**—Appletalk Address Resolution Protocol (ARP) (0x80f3)
- **appletalk**—Appletalk (0x809b)
- **decnet-iv**—DECnet Phase IV (0x6003)
- **diagnostic**—DEC Diagnostic Protocol (0x6005)
- **etype-6000**—Ethertype 0x6000 (0x6000)
- **etype-8042**—Ethertype 0x8042 (0x8042)
- **ip**—Internet Protocol v4 (0x0800)
- **lat**—DEC LAT (0x6004)
- **lavc-sca**—DEC LAVC, SCA (0x6007)
- **mop-console**—DEC MOP Remote console (0x6002)
- **mop-dump**—DEC MOP dump (0x6001)

- **vines-echo**—VINES Echo (0x0baf)

Examples

This example shows how to configure a MAC ACL named mac-ip-filter with a rule that permits all IPv4 traffic between two groups of MAC addresses:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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
```

Related Commands

Command	Description
deny (MAC)	Configures a deny rule in a MAC ACL.
mac access-list	Configures a MAC ACL.
remark	Configures a remark in an ACL.
show mac access-list	Displays all MAC ACLs or one MAC ACL.

permit interface

To specify the interfaces that users assigned to this role can access, use the **permit interface** command.

To remove the policy restrictions, use the **no** form of this command.

permit interface *interface-list*

no permit interface *interface-list*

Syntax Description

interface-list	Interface(s) that can be accessed by users with a specified role. The list name is alphanumeric, case-sensitive, and can be up to 16 characters long.

Defaults

None

Command Modes

Interface configuration (config-role-interface)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Usage Guidelines

Repeat this command to specify all interface lists that users assigned to this role are permitted to access.

Examples

This example shows how to specify ethernet 2/1-4 as interfaces that users assigned to this role can access:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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)#
```

This example shows how to remove the policy restrictions for ethernet 2/1-4:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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)#
```

Related Commands

Command	Description
interface policy deny	Enters the interface configuration mode and denies all interface access for the role.
role name	Specifies a user role and enters role configuration mode for the named role.
show role	Displays the role configuration.

ping

To determine the network connectivity to another device using IPv4 addressing, use the **ping** command.

ping [*dest_ipv4_address* | *hostname* | **multicast** *multicast_group_add* **interface** [**ethernet** *slot/port* | **loopback** *number* | **mgmt0** | **port-channel** *channel_number* | **vethernet veth**_*number*]] [**count** {*number* | **unlimited**}] [**df-bit**] [**interval** *seconds*] [**packet-size** *bytes*] [**source** *src_ipv4_address*] [**timeout** *seconds*] [**vrf** *vrf_name*]

Syntax Description

dest_ipv4_address	(Optional) IPv4 address of destination device. The format is *A.B.C.D*.
hostname	(Optional) Hostname of destination device. The hostname is case-sensitive and can be up to 28 characters.
multicast	(Optional) Multicast ping.
multicast_group_add	(Optional) Multicast group address. The format is *A.B.C.D*.
interface	(Optional) Specifies the interface to send the multicast packet.
ethernet	(Optional) Specifies the slot and port number for the Ethernet interface.
slot/port	Slot/port number. The range is from 1 to 66.
loopback	(Optional) Specifies a virtual interface number.
number	Virtual interface number. The range is from 0 to 1023.
mgmt0	(Optional) Specifies the management interface.
port-channel	(Optional) Specifies a port-channel interface.
channel_number	Port channel number. The range is from 1 to 4096.
vethernet	(Optional) Specifies a virtual Ethernet interface.
veth_number	Virtual Ethernet number. The range is from 1 to 1048575.
count	(Optional) Specifies the number of transmissions to send.
number	Number of pings. The range is from 1 to 655350. The default is 5.
unlimited	Allows an unlimited number of pings.
df-bit	(Optional) Enables the do-not-fragment bit in the IPv4 header. The default is disabled.
interval	(Optional) Specifies the interval in seconds between transmissions.
seconds	The range is from 0 to 60. The default is 1 second.
packet-size *bytes*	(Optional) Specifies the packet size in bytes to transmit. The range is from 1 to 65468. The default is 56 bytes.
source *scr_ipv4_address*	(Optional) Specifies the source IPv4 address to use. Source IPv4 address. The format is *A.B.C.D*. The default is the IPv4 address for the management interface of the device.
timeout	(Optional) Specifies the nonresponse timeout interval in seconds.
seconds	The range is from 1 to 60. The default is 2 seconds.
vrf	(Optional) Specifies a virtual routing and forwarding (VRF) name.
vrf_name	The name is a maximum of 32 case-sensitive, alphanumeric characters. The default is the default VRF.

Defaults For the default values, see the “Syntax Description” section for this command.

Command Modes Any

SupportedUserRoles network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Usage Guidelines To determine the network connectivity to another device using IPv6 addressing, use the **ping6** command.

Examples This example shows how to determine connectivity to another device using IPv4 addressing:

```
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
```

Related Commands

Command	Description
ping6	Determines connectivity to another device using IPv6 addressing.

pinning id

To pin virtual Ethernet traffic to a specific subgroup, use the **pinning id** command. To remove the configuration, use the **no** form of this command.

pinning id *sub-group-id*

no pinning id

Syntax Description

sub-group-id	ID number of the subgroup. The range is from 0 to 31.

Defaults

None

Command Modes

Interface configuration mode (config-if)
Port profile configuration (config-port-prof)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Examples

This example shows how to pin virtual Ethernet interfaces to subgroup 3:

```
n1000v(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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 Vethernet1
 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
```

Related Commands

Command	Description
module vem execute vemcmd show pinning	Displays the pinning configuration on the specified VEM.
show port-profile	Displays port profile information.
show running-config interface vethernet	Displays the running configuration of the specified virtual Ethernet interface, including the pinning configuration.
show running-config port-profile	Displays the running configuration of the specified port profile, including the pinning configuration.

port-channel load-balance ethernet

To configure Ethernet port channel load balance, use the **port-channel load-balance ethernet** command. To restore the default value, use the **no** form of this command.

port-channel load-balance ethernet {**dest-ip-port** | **dest-ip-port-vlan** | **destination-ip-vlan** | **destination-mac** | **destination-port** | **source-dest-ip-port** | **source-dest-ip-port -vlan** | **source-dest-ip-vlan** | **source-dest-mac** | **source-dest-port** | **source-ip-port** | **source-ip-port-vlan** | **source-ip-vlan** | **source-mac** | **source-port** | **source-virtual-port-id** | **vlan-only**} [**module** *module*]

no port-channel load-balance ethernet {**dest-ip-port** | **dest-ip-port-vlan** | **destination-ip-vlan** | **destination-mac** | **destination-port** | **source-dest-ip-port** | **source-dest-ip-port -vlan** | **source-dest-ip-vlan** | **source-dest-mac** | **source-dest-port** | **source-ip-port** | **source-ip-port-vlan** | **source-ip-vlan** | **source-mac** | **source-port** | **source-virtual-port-id** | **vlan-only**} [**module** *module*]

Syntax Description

dest-ip-port	Destination IP address and Layer 4 port.
dest-ip-port-vlan	Destination IP address, Layer 4 port, and VLAN.
destination-ip-vlan	Destination IP address and VLAN.
destination-mac	Destination MAC address.
destination-port	Destination Layer 4 port.
source-dest-ip-port	Source and destination IP address and Layer 4 port.
source-dest-ip-port -vlan	Source and destination IP address, Layer 4 port, and VLAN.
source-dest-ip-vlan	Source and destination IP address and VLAN.
source-dest-mac	Source and destination MAC address.
source-dest-port	Source and destination Layer 4 port.
source-ip-port	Source IP address
source-ip-port-vlan	Source IP address, Layer 4, and VLAN.
source-ip-vlan	Source IP address and VLAN.
source-mac	Source MAC address (the default).
source-port	Source port.
source-virtual-port-id	Source virtual port ID.
vlan-only	VLAN only.
module	(Optional) Specifies a module to load balance independently. If you do not specify a module, the specified algorithm is applied to all device modules.
module	Module number. The range is from 1 to 66.

Defaults

Source MAC address

Command Modes

Global configuration (config)

SupportedUserRoles network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Usage Guidelines

If you do not specify a module, the algorithm is applied globally to all port channels.

If you specify a module, the algorithm is applied to all port channels in the specified module.

The per module configuration takes precedence over the algorithm configured globally.

If the traffic on a port channel is going only to a single MAC address and you load balance on a destination MAC address, the port channel always chooses the same link in that port channel. In this case, using source addresses or IP addresses might result in better load balancing.

Examples

This example shows how to specify the source port as the global algorithm for balancing loads on the interfaces in channel-groups:

```
n1000V# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# port-channel load-balance ethernet src-port
n1000v(config)#
```

This example shows how to configure the source IP load-balancing algorithm for port channels on module 5:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# port-channel load-balance ethernet source-ip module 5
```

Related Commands

Command	Description
show port-channel load-balance	Displays information about port channel load balancing.

port-profile

To create a port profile and enter port profile configuration mode, use the **port-profile** command. To remove the port profile configuration, use the **no** form of this command.

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

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

Syntax Description

profile_name	Port profile name. The name can be up to 80 characters in length, alphanumeric, and case-sensitive.
type	(Optional) Specifies an interface of type Ethernet or virtual Ethernet.
ethernet	The Ethernet type.
vethernet	The virtual Ethernet type.

Defaults

The default type is virtual Ethernet.

Command Modes

Configure port profile (config-net-seg).

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Usage Guidelines

The port profile name must be unique for each port profile on the Cisco Nexus 1000V.

The port profile type can be Ethernet or virtual Ethernet. Once configured, the type cannot be changed.

Defining a port profile type as Ethernet allows the port profile to be used for physical (Ethernet) ports. In the Microsoft System Center Virtual Machine Manager (SCVMM) server, the corresponding uplink port profile can be selected and assigned to physical ports (PNICs).

If a port profile is configured as an Ethernet type, it cannot be used to configure a vNIC or Microsoft Hyper-V virtual port.

Classification profiles carry the feature configuration for Ethernet and virtual Ethernet interfaces. The classification profile type determines which type of interfaces can inherit them. virtual Ethernet classification profiles are published to the SCVMM server while Ethernet profiles are inherited by uplink networks.

To configure a virtual Ethernet profile with features:

1. Create network-segments with VLANs to be assigned for virtual Ethernet interfaces.

2. Create classification profile of type “vethernet” with required features.

3. Publish classification profile to the SCVMM server.

4. On the SCVMM server attach both nsm network segment and the classification profile to the virtual Ethernet interface.

To configure a virtual Ethernet profile with port binding:

1. Once a virtual Ethernet port profile has been created as a port group on the SCVMM server, you cannot change its port binding type.

2. You cannot configure maximum port limits for virtual Ethernet port profiles with ephemeral port binding.

3. You cannot configure port binding for Ethernet type port profiles. Port binding is available only for virtual Ethernet port profiles.

4. Manual configurations on an interface are purged when the system administrator changes its port profile if either port profile is configured with ephemeral port binding regardless of the auto purge setting.

Examples

This example shows how to create an Ethernet type port profile with the name PortChannelProfile:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# port-profile type ethernet PortChannelProfile
n1000v(config-port-prof)# channel-group auto
n1000v(config-port-prof)# no shutdown
n1000v(config-port-prof)# state enabled
```

This example shows how to remove the port profile with the name PortChannelProfile:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v#(config)# port-profile type ethernet PortChannelProfile
n1000v#(config-port-prof)# no shutdown
n1000v#(config-port-prof)# publish port-profile
n1000v#(config-port-prof)# state enabled
n1000v#(config-port-prof)# publish port-profile
```

This example shows how to configure a classification profile:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# port-profile type vethernet ACL
n1000v(config-port-prof)# service-policy input mark
n1000v(config-port-prof)# state enabled
n1000v(config-port-prof)# publish port-profile
n1000v(config-port-prof)# no shut
```

This example shows how to create an Ethernet profile carrying a port channel configuration:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# port-profile type ethernet PORT_CHANNEL
n1000v(config-port-prof)# channel-group auto mode on
n1000v(config-port-prof)# state enabled
n1000v(config-port-prof)# no shut
n1000v(config-port-prof)# end
n1000v
```

This example shows how to configure a virtual Ethernet profile with features:

```
n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# nsm logical network Hyper-v
```

```
n1000v(config-log-net)# description "Hyper-v Logic"
n1000v(config-log-net)# end
n1000v

n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# nsm network segment pool net-seg-pool
n1000v(config-net-seg-pool)# nsm network logical Hyper-v
n1000v(config-net-seg-pool)# end
n1000v

n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# nsm network segment net-seg-101
n1000v(config-net-seg)# switchport access vlan 101
n1000v(config-net-seg)# nsm network segment pool net-seg-pool
n1000v(config-net-seg)# publish network-segment
n1000v(config-net-seg)# end
n1000v

n1000v# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# port-profile type vethernet ACL
n1000v(config-port-prof)# service-policy input police
n1000v(config-port-prof)# ip port access-group security in
n1000v(config-port-prof)# publish port-profile
n1000v(config-port-prof)# state enabled
n1000v(config-port-prof)# no shut
n1000v(config-port-prof)# end
n1000v
```

Related Commands

Command	Description
show port-profile	Displays the port profile configuration, including assigned roles.
show running-config port-profile	Displays the port profile configuration.
switchport mode	Designates whether the interfaces in the port profile are to be used as access or trunking ports.

pwd

To view the current directory, use the **pwd** command.

pwd

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Examples

This example shows how to view the current directory:

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