D Commands

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

deadtime

To configure the duration of time for which a non-reachable RADIUS or TACACS+ server is skipped, use the **deadtime** command. To revert to the default, use the **no** form of this command.

deadtime *minutes*

no deadtime *minutes*

Syntax Description

minutes	Number of minutes, from 0 to 1440, for the interval.

Defaults

0 minutes

Command Modes

RADlUS server group configuration (**config-radius**)
TACACS+ server group configuration (**config-tacacs+**)
Global configuration (**config**)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

Before you can configure it, you must enable TACACS+ using the **tacacs+ enable** command.

The dead-time can be configured either globally and applied to all RADIUS or TACACS+ servers; or per server group.

If the dead-time interval for a RADIUS or TACACS+ server group is greater than zero (0), that value takes precedence over the global dead-time value.

Setting the dead-time interval to 0 disables the timer.

When the dead-time interval is 0 minutes, RADIUS and TACACS+ servers are not marked as dead even if they are not responding.

Examples

This example shows how to set the dead-time interval to 2 minutes for a RADIUS server group:

```
n1000v# config t
n1000v(config)# aaa group server radius RadServer
n1000v(config-radius)# deadtime 2
```

This example shows how to set a global dead-time interval to 5 minutes for all TACACS+ servers and server groups:

```
n1000v# config t
n1000v(config)# tacacs-server deadtime 5
n1000v(config)#
```

This example shows how to set the dead-time interval to 5 minutes for a TACACS+ server group:

```
n1000v# config t
n1000v(config)# aaa group server tacacs+ TacServer
n1000v(config-tacacs+)# deadtime 5
```

This example shows how to revert to the dead-time interval default:

```
n1000v# config t
n1000v(config)# feature tacacs+
n1000v(config)# aaa group server tacacs+ TacServer
n1000v(config-tacacs+)# no deadtime 5
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
radius-server host	Configures a RADIUS server.
show radius-server groups	Displays RADIUS server group information.
show tacacs-server groups	Displays TACACS+ server group information.
tacacs+ enable	Enables TACACS+.
tacacs-server host	Configures a TACACS+ server.

debug logfile

To direct the output of the **debug** commands to a specified file, use the **debug logfile** command. To revert to the default, use the **no** form of this command.

debug logfile *filename* [**size** *bytes*]

no debug logfile *filename* [**size** *bytes*]

Syntax Description

filename	Name of the file for **debug** command output. The filename is alphanumeric, case sensitive, and has a maximum of 64 characters.
size *bytes*	(Optional) Specifies the size of the logfile in bytes. The range is from 4096 to 4194304.

Defaults

Default filename: syslogd_debugs

Default file size: 4194304 bytes

Command Modes

Any

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

The logfile is created in the log: file system root directory.

Use the **dir log:** command to display the log files.

Examples

This example shows how to specify a debug logfile:

```
n1000v# debug logfile debug_log
```

This example shows how to revert to the default debug logfile:

```
n1000v# no debug logfile debug_log
```

Related Commands

Command	Description
dir	Displays the contents of a directory.
show debug	Displays the debug configuration.
show debug logfile	Displays the debug logfile contents.

debug logging

To enable **debug** command output logging, use the **debug logging** command. To disable debug logging, use the **no** form of this command.

debug logging

no debug logging

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Any

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to enable the output logging for the **debug** command:

```
n1000v# debug logging
```

This example shows how to disable the output logging for the **debug** command:

```
n1000v# no debug logging
```

Related Commands

Command	Description
debug logfile	Configures the logfile for the **debug** command output.

default switchport (port profile)

To remove a particular switchport characteristc from a port profile, use the **default switchport** command.

default switchport {**mode** | **access vlan** | **trunk** {**native** | **allowed**} **vlan** | **private-vlan** {**host-association** | **mapping** [**trunk**]} | **port-security**}

Syntax Description

mode	Removes the port mode characteristic from a port profile, which causes the port mode to revert to global or interface defaults (access mode). This is equivalent to executing the **no switchport mode port-profile** command.
access vlan	Removes an access VLAN configuration.
trunk allowedvlan	Removes trunking allowed VLAN characteristics.
trunk native vlan	Removes trunking native VLAN characteristics.
private-vlan host-association	Removes PVLAN host-association.
private-vlan mapping	Removes PVLAN mapping.
port-security	Removes port-security characteristics.

Defaults

None

Command Modes

Port profile configuration (**config-port-prof**)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

The functionally of this command is equivalent to using the no form of a specific switchport command. For example, the effect of the following commands is the same:

- **default switchport mode** command = **no switchport mode** command
- **default switchport access vlan** command = **no switchport access vlan** command
- **default switchport trunk native vlan** command= **no switchport trunk native vlan** command

Examples

This example shows how to revert port profile ports to switch access ports.

```
n1000v(config-port-prof)# default switchport mode
```

This example shows how to remove the trunking allowed VLAN characteristics of a port profile.

```
n1000v(config-port-prof)# default switchport trunk allowed vlan
```

This example shows how toremove the private VLAN host association of a port profile.

```
n1000v(config-port-prof)# default switchport private-vlan host-association
```

This example shows how to remove port security characteristics of a port profile.

```
n1000v(config-port-prof)# default switchport port-security
```

Related Commands

Command	Description
show port-profile	Displays information about port profile(s).

default shutdown (port profile)

To remove the admin status characteristic (config attribute) from a port-profile, use the **default shutdown** command. This will set the admin status of the interfaces inheriting this port-profile to the global or interface default (usually, the default admin status is shutdown).

default shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Port profile configuration (**config- port-prof**)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to change the ports in a port profile to the shutdown state:

```
n1000v# config t
n1000v# port-profile DataProfile
n1000v(config-port-prof)# default shutdown
n1000v(config-port-prof)# show port-profile name DataProfile
port-profile DataProfile
  description:
  status: enabled
  capability uplink: no
  capability l3control: no
  system vlans: none
  port-group: DataProfile
  max-ports: 32
  inherit:
  config attributes:
    switchport mode access
  evaluated config attributes:
    switchport mode access
  assigned interfaces:
    Vethernet1switch(config-port-prof)#
```

Related Commands

Command	Description
show port-profile	Displays the configuration for a port profile.

default shutdown (interface)

To remove any interface-level override for the admin status, use the **default shutdown** command. This command removes any configuration for admin status entered previously. This allows the port-profile config to take effect.

default shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Interface configuration (**config- if**)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to change the ports to the shutdown state:

```
n1000v# config t
n1000v(config)# interface ethernet 3/2
n1000v(config-if)# default shutdown
n1000v(config-if)#
```

Related Commands

Command	Description
show running-config interface	Displays the configuration of an interface.

default switchport port-security (VEthernet)

To remove any user configuration for the switchport port-security characteristic from a VEthernet interface, use the **default switchport port-security** command. This has the effect of setting the default (disabled) for port-security for that interface.

default switchport port-security

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration (**config-if**)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to disable port security on VEthernet 2:

```
n1000v# config t
n1000v(config)# interface veth 2
n1000v(config-if)# default switchport port-security
n1000v(config-if)#
```

Related Commands

Command	Description
show running-config port-security	Displays the port security configuration.
show port-security	Displays the port security status.

delay

To assign an informational throughput delay value to an Ethernet interface, use the **delay** command. To remove delay value, use the **no** form of this command.

delay *value*

no delay [*value*]

Syntax Description

delay_val	Specifies the throughput delay time in tens of microseconds. Allowable values are between 1 and 16777215.

Defaults

None

Command Modes

Interface configuration (**`config-if`**)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

The actual Ethernet interface throughput delay time does not change when you set this value—the setting is for informational purposes only.

Examples

This example shows how to assign the delay time to an Ethernet slot 3 port 1 interface:

```
n1000v# config t
n1000v(config)# interface ethernet 3/1
n1000v(config-if)# delay 10000
n1000v(config-if)#
```

This example shows how to remove the delay time configuration:

```
n1000v# config t
n1000v(config)# interface ethernet 3/1
n1000v(config-if)# no delay 10000
n1000v(config-if)#
```

Related Commands

Command	Description
show interface	Displays configuration information for an interface.

delete

To delete a file, use the **delete** command.

delete [*filesystem***:**[**//***directory***/**] | *directory***/**]*filename*

Syntax Description

*filesystem***:**	(Optional) Name of the file system. Valid values are **bootflash** or **volatile**.
//*directory***/**	(Optional) Name of the directory. The directory name is case sensitive.
filename	Name of the file. The name is case sensitive.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

Use the **dir** command to locate the file you that want to delete.

Examples

This example shows how to delete a file:

```
n1000v# delete bootflash:old_config.cfg
```

Related Commands

Command	Description
dir	Displays the contents of a directory.

deny (IPv4)

To create an IPv4 ACL rule that denies traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

General Syntax

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

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

no *sequence-number*

Internet Control Message Protocol

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

Internet Group Management Protocol

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

Internet Protocol v4

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

Transmission Control Protocol

[*sequence-number*] **deny tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*] [*flags*] [**established**]

User Datagram Protocol

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

Syntax Description

sequence-number	(Optional) Sequence number of the **deny** 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 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 is 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 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) • **ef**—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 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
4.0(4)SV1(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 that you use to specify one of these arguments does not affect how you specify the other argument. 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
  ```

  The following 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)# deny 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
  ```

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

  ```
  n1000v(config-acl)# deny 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.

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

  ```
  n1000v(config-acl)# deny 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**—Time-stamp replies
- **timestamp-request**—Time-stamp 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 that deny all TCP and UDP traffic from the 10.23.0.0 and 192.168.37.0 networks to the 10.176.0.0 network and a final rule that permits all other IPv4 traffic:

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

```
n1000v(config-acl)# permit ip any any
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
permit (IPv4)	Configures a permit rule in an IPv4 ACL.
remark	Configures a remark in an IPv4 ACL.
show ip access-list	Displays all IPv4 ACLs or one IPv4 ACL.
statistics per-entry	Enables collection of statistics for each entry in an ACL.

deny (MAC)

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

[*sequence-number*] **deny** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *VLAN-ID*]

no deny *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *VLAN-ID*]

no *sequence-number*

Syntax Description

sequence-number	(Optional) Sequence number of the **deny** 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 ID given. The *VLAN-ID* argument can be an integer from 1 to 4094.

Defaults

A newly created MAC ACL contains no rules.

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

Command Modes

MAC ACL configuration (**config-mac-acl**)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

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 that you use to specify one of these arguments does not affect how you specify the other argument. 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
  ```

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

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

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

  ```
  n1000v(config-acl)# deny 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 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 rules that permit any non-IPv4 traffic between two groups of MAC addresses:

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

Related Commands

Command	Description
mac access-list	Configures a MAC ACL.
permit (MAC)	Configures a deny rule in a MAC ACL.
remark	Configures a remark in an ACL.
show mac access-list	Displays all MAC ACLs or one MAC ACL.
statistics per-entry	Enables collection of statistics for each entry in an ACL.

description (interface)

To do add a description for the interface and save it in the running configuration, use the **description** command. To remove the interface description, use the **no** form of this command.

description *text*

no description

Syntax Description

text	Describes the interface. The maximum number of characters is 80.

Defaults

None

Command Modes

Interface configuration (config-if)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to add the description for the interface and save it in the running configuration.:

```
n1000v(config-if)# description Ethernet port 3 on module 1
```

This example shows how to remove the interface description.

```
n1000v(config-if)# no description Ethernet port 3 on module 1
```

Related Commands

Command	Description
interface vethernet	Creates a virtual Ethernet interface.
interface port-channel	Creates a port-channel interface.
interface ethernet	Creates an Ethernet interface.
interface mgmt	Configure the management interface.
show interface	Displays the interface status, including the description.

description (NetFlow)

To add a description to a flow record, flow monitor, or flow exporter, use the **description** command. To remove the description, use the **no** form of this command.

description *line*

no description

Syntax Description

line	Description of up to 63 characters.

Defaults

None

Command Modes

NetFlow flow record (config-flow-record)

NetFlow flow exporter (config-flow-exporter)

Netflow flow monitor (config-flow-monitor)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to add a description to a flow record:

```
n1000v(config)# flow record RecordTest
n1000v(config-flow-record)# description Ipv4flow
```

This example shows how to add a description to a flow exporter:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# description ExportHamilton
```

This example shows how to add a description to a flow monitor:

```
n1000v# config t
n1000v(config)# flow monitor MonitorTest
n1000v(config-flow-monitor)# description Ipv4Monitor
```

Related Commands

Command	Description
flow exporter	Creates a Flexible NetFlow flow exporter.
flow record	Creates a Flexible NetFlow flow record.

Command	Description
flow monitor	Creates a Flexible NetFlow flow monitor.
show flow exporter	Displays information about the NetFlow flow exporter.
show flow record	Displays information about NetFlow flow records.
show flow monitor	Displays information about the NetFlow flow monitor.

description (QoS)

To add a description to a QoS class map, policy map, use the **description** command. To remove the description, use the **no** form of this command.

description *text*

no description *text*

Syntax Description

text	Description, of up to 200 characters, for the class map or policy map.

Defaults

None

Command Modes

QoS class map configuration (**config-cmap-qo**s)
QoS policy map configuration (**config-pmap-qos**)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to add a description to a policy map:

```
n1000v(config)# policy-map my_policy1
n1000v(config-pmap)# description this policy applies to input packets
n1000v(config-pmap)#
```

Related Commands

Command	Description
class-map	Creates or modifies a class map.
policy-map	Creates or modifies a policy map.

description (role)

To add a description for a role, use the **description** command. To remove a description of a role, use the **no** form of this command.

description *string*

no description

Syntax Description

string	Describes the role. The string can include spaces.

Defaults

None

Command Modes

Role configuration (**config-role**)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to add a description to a role:

```
n1000v(config-role)# description admin
```

This example shows how to remove the role description:

```
n1000v(config-role)# no description admin
```

Related Commands

Command	Description
username	Creates a user account including the assignment of a role.
show role	Displays a role configuration.

description (SPAN)

To add a description to a SPAN session, use the **description** command. To remove the description, use the **no** form of this command.

description *string*

no description

Syntax Description

string	Specifies a description of up to 32 alphanumeric characters.

Defaults

Blank (no description)

Command Modes

SPAN monitor configuration (config-monitor)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to add a description to a SPAN session:

```
n1000v# config t
n1000v(config)# monitor session 8
n1000v(config-monitor)# description span_session_8a
n1000v(config-monitor)#
```

This example shows how to remove a description from a SPAN session:

```
n1000v# config t
n1000v(config)# monitor session 8
n1000v(config)# no description span_session_8a
n1000v(config-monitor)#
```

Related Commands

Command	Description
show monitor session	Displays session information.

destination (NetFlow)

To add a destination IP address or VRF to a NetFlow flow exporter, use the **destination** command. To remove the IP address or VRF, use the **no** form of this command.

destination {*ipaddr* | *ipv6addr*} [**use-vrf** *vrf_name*]

no destination

Syntax Description

ipaddr	Destination IP address for collector.
ipv6addr	Destination IPv6 address for collector.
use-vrf *vrf_name*	(Optional) Optional VRF label.

Defaults

None

Command Modes

NetFlow flow exporter configuration (**config-flow-exporter**)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to add a destination IP address to a Netflow flow exporter:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# destination 192.0.2.1
```

This example shows how to remove the IP address from a flow exporter:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# no destination 192.0.2.1
```

Related Commands

Command	Description
flow exporter	Creates a Flexible NetFlow flow exporter.
flow record	Creates a Flexible NetFlow flow record.
flow monitor	Creates a Flexible NetFlow flow monitor.
show flow exporter	Displays information about the NetFlow flow exporter.
show flow record	Displays information about NetFlow flow records.
show flow monitor	Displays information about the NetFlow flow monitor.

destination interface (SPAN)

To configures the port(s) in a SPAN session to act as destination(s) for copied source packets, use the **destination interface** command. To remove the destination interface, use the **no** form of this command.

destination interface *type number(s)_or_range*

no destination interface *type number(s)_or_range*

Syntax Description

ethernet *slot/port_or_range*	Designates the SPAN destination(s) Ethernet interface(s).
port-channel *number(s)_or_range*	Designates the SPAN destination(s) port channel(s).
vethernet *number(s)_or_range*	Designates the SPAN destination(s) virtual Ethernet interface(s).

Defaults

None

Command Modes

SPAN monitor configuration (**config-monitor**)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

SPAN destination ports must already be configured as either access or trunk ports.

SPAN sessions are created in the shut state by default.

When you create a SPAN session that already exists, any additional configuration is added to that session. To make sure the session is cleared of any previous configuration, you can delete the session first using the command, **no monitor session**.

Examples

This example shows how to configure ethernet interfaces 2/5 and 3/7 in a SPAN session to act as destination(s) for copied source packets:

```
n1000v# config t
n1000v(config)# monitor session 8
n1000v(config-monitor)# destination interface ethernet 2/5, ethernet 3/7
```

This example shows how to remove the SPAN configuration from destination interface ethernet 2/5:

```
n1000v# config t
n1000v(config)# monitor session 8
n1000v(config-monitor)# no destination interface ethernet 2/5
```

Related Commands

Command	Description
show interface	Displays the interface trunking configuration for the specified destination interface.
show monitor	Displays Ethernet SPAN information.
monitor session	Starts the specified SPAN monitor session(s).

dir

To display the contents of a directory or file, use the **dir** command.

dir [**bootflash:** | **debug:** | **log:** | **volatile:**]

Syntax Description

bootflash:	(Optional) Directory or filename.
debug:	(Optional) Directory or filename on expansion flash.
log:	(Optional) Directory or filename on log flash.
volatile:	(Optional) Directory or filename on volatile flash.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

Use the **pwd** command to identify the directory you are currently working in.

Use the **cd** command to change the directory you are currently working in.

Examples

This example shows how to display the contents of the bootflash: directory

```
n1000v# dir bootflash:
```

Related Commands

Command	Description
cd	Changes the current working directory.
pwd	Displays the current working directory.

domain id

To assign a domain-id, use the **domain id** command. To remove a domain-id, use the **no** form of this command.

domain id *number*

no domain id

Syntax Description

number	Specifies the domain-id number. The allowable domain IDs are 1 to 4095.

Defaults

None

Command Modes

Domain configuration (**config-svs-domain**)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

During installation of the Cisco Nexus 1000V the setup utility prompts you to configure a domain, including the domain ID and control and packet VLANs.

Examples

This example shows how to assign a domain id:

```
n1000v# config t
n1000v(config)# sve-domain
n1000v(config-svs-domain)# domain-id number 32
n1000v(config-svs-domain)#
```

This example shows how to remove the domain-id:

```
n1000v# config t
n1000v(config)# sve-domain
n1000v(config-svs-domain)# no domain-id number 32
n1000v(config-svs-domain)#
```

Related Commands

Command	Description
show svs domain	Displays domain configuration.

dscp (NetFlow)

To add a differentiated services codepoint (DSCP) to a NetFlow flow exporter, use the **dscp** command. To remove the DSCP, use the **no** form of this command.

dscp *value*

no dscp

Syntax Description

value	Specifies a DSCP between 0 and 63.

Defaults

None

Command Modes

NetFlow flow exporter configuration (**config-flow-exporter**)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Examples

This example shows how to configure DSCP for a NetFlow flow exporter:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# dscp 2
n1000v(config-flow-exporter)#
```

This example shows how to remove DSCP from the NetFlow flow exporter:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# no dscp 2
n1000v(config-flow-exporter)#
```

Related Commands

Command	Description
flow exporter	Creates a Flexible NetFlow flow exporter.
flow record	Creates a Flexible NetFlow flow record.
flow monitor	Creates a Flexible NetFlow flow monitor.
show flow exporter	Displays information about the NetFlow flow exporter.
show flow record	Displays information about NetFlow flow records.
show flow monitor	Displays information about the NetFlow flow monitor.

duplex

To set the duplex mode for an interface as full, half, or autonegotiate, use the **duplex** command. To revert back to the default setting, use the **no** form of this command.

duplex {**full** | **half** | **auto**}

no duplex [**full** | **half** | **auto**]

Syntax Description

full	Specifies full-duplex mode for the interface.
half	Specifies half-duplex mode for the interface.
auto	Sets the duplex mode on the interface to autonegotiate with the connecting port.

Defaults

None

Command Modes

Interface configuration (config-if)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

When you use the no version of this command, an argument (such as full, half, or auto) is optional. To return to the default duplex setting, you can use either of the following commands (if, for example, the setting had been changed to full):

```
n1000v(config-if)# no duplex
```

```
n1000v(config-if)# no duplex full
```

Examples

This example shows how to set the Ethernet port 1 on the module in slot 3 to full-duplex mode:

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

This example shows how to revert to the default duplex setting for the Ethernet port 1 on the module in slot 3:

```
n1000v config t
n1000v(config)# interface ethernet 2/1
n1000v(config-if)# no duplex
```

Related Commands

Command	Description
interface	Specifies the interface that you are configuring.
speed	Sets the speed for the port channel interface.
show interface	Displays the interface status, which includes the speed and duplex mode parameters.