



## D Commands

---

This chapter describes the Cisco NX-OS security commands that begin with D.

### deadtime

To configure the dead-time interval for a RADIUS or TACACS+ server group, 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 for the interval. The range is from 0 to 1440 minutes.

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

---

---

#### Defaults

0 minutes

---

#### Command Modes

RADIUS server group configuration  
TACACS+ server group configuration

---

#### Supported User Roles

network-admin  
vdc-admin

---

#### Command History

Release	Modification
4.0(1)	This command was introduced.

---

---

#### Usage Guidelines

You must use the **feature tacacs+** command before you configure TACACS+. This command does not require a license.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

### Examples

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

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

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

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

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

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

### Related Commands

Command	Description
<b>aaa group server</b>	Configures AAA server groups.
<b>radius-server host</b>	Configures a RADIUS server.
<b>show radius-server groups</b>	Displays RADIUS server group information.
<b>show tacacs-server groups</b>	Displays TACACS+ server group information.
<b>feature tacacs+</b>	Enables TACACS+.
<b>tacacs-server host</b>	Configures a TACACS+ server.

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

## deny (ARP)

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

### General Syntax

```
[sequence-number] deny ip {any | host sender-IP | sender-IP sender-IP-mask} mac {any | host sender-MAC | sender-MAC sender-MAC-mask} [log]
```

```
[sequence-number] deny request ip {any | host sender-IP | sender-IP sender-IP-mask} mac {any | host sender-MAC | sender-MAC sender-MAC-mask} [log]
```

```
[sequence-number] deny response ip {any | host sender-IP | sender-IP sender-IP-mask} {any | host target-IP | target-IP target-IP-mask} mac {any | host sender-MAC | sender-MAC sender-MAC-mask} [any | host target-MAC | target-MAC target-MAC-mask] [log]
```

**no** sequence-number

```
no deny ip {any | host sender-IP | sender-IP sender-IP-mask} mac {any | host sender-MAC | sender-MAC sender-MAC-mask} [log]
```

```
no deny request ip {any | host sender-IP | sender-IP sender-IP-mask} mac {any | host sender-MAC | sender-MAC sender-MAC-mask} [log]
```

```
no deny response ip {any | host sender-IP | sender-IP sender-IP-mask} {any | host target-IP | target-IP target-IP-mask} mac {any | host sender-MAC | sender-MAC sender-MAC-mask} [any | host target-MAC | target-MAC target-MAC-mask] [log]
```

### Syntax Description

<i>sequence-number</i>	(Optional) Sequence number of the <b>deny</b> 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 <b>resequence</b> command to reassign sequence numbers to rules.
<b>ip</b>	Introduces the IP address portion of the rule.
<b>any</b>	(Optional) Specifies that any host matches the part of the rule that contains the <b>any</b> keyword. You can use the <b>any</b> to specify the sender IP address, target IP address, sender MAC address, and target MAC address.
<b>host sender-IP</b>	(Optional) Specifies that the rule matches ARP packets only when the sender IP address in the packet matches the value of the <i>sender-IP</i> argument. Valid values for the <i>sender-IP</i> argument are IPv4 addresses in dotted-decimal format.
<i>sender-IP</i> <i>sender-IP-mask</i>	(Optional) IPv4 address and mask for the set of IPv4 addresses that the sender IP address in the packet can match. The <i>sender-IP</i> and <i>sender-IP-mask</i> argument must be given in dotted-decimal format. Specifying 255.255.255.255 as the <i>sender-IP-mask</i> argument is the equivalent of using the <b>host</b> keyword.

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

<b>mac</b>	Introduces the MAC address portion of the rule.
<b>host</b> <i>sender-MAC</i>	(Optional) Specifies that the rule matches ARP packets only when the sender MAC address in the packet matches the value of the <i>sender-MAC</i> argument. Valid values for the <i>sender-MAC</i> argument are MAC addresses in dotted-hexadecimal format.
<i>sender-MAC</i> <i>sender-MAC-mask</i>	(Optional) MAC address and mask for the set of MAC addresses that the sender MAC address in the packet can match. The <i>sender-MAC</i> and <i>sender-MAC-mask</i> argument must be given in dotted-hexadecimal format. Specifying ffff.ffff.ffff as the <i>sender-MAC-mask</i> argument is the equivalent of using the <b>host</b> keyword.
<b>log</b>	(Optional) Specifies that the device logs ARP packets that match the rule.
<b>request</b>	(Optional) Specifies that the rule applies only to packets containing ARP request messages.  <b>Note</b> If you omit both the <b>request</b> and the <b>response</b> keywords, the rule applies to all ARP messages.
<b>response</b>	(Optional) Specifies that the rule applies only to packets containing ARP response messages.  <b>Note</b> If you omit both the <b>request</b> and the <b>response</b> keywords, the rule applies to all ARP messages.
<b>host</b> <i>target-IP</i>	(Optional) Specifies that the rule matches ARP packets only when the target IP address in the packet matches the value of the <i>target-IP</i> argument. You can specify <b>host</b> <i>target-IP</i> only when you use the <b>response</b> keyword. Valid values for the <i>target-IP</i> argument are IPv4 addresses in dotted-decimal format.
<i>target-IP</i> <i>target-IP-mask</i>	(Optional) IPv4 address and mask for the set of IPv4 addresses that the target IP address in the packet can match. You can specify <i>target-IP</i> <i>target-IP-mask</i> only when you use the <b>response</b> keyword. The <i>target-IP</i> and <i>target-IP-mask</i> argument must be given in dotted-decimal format. Specifying 255.255.255.255 as the <i>target-IP-mask</i> argument is the equivalent of using the <b>host</b> keyword.
<b>host</b> <i>target-MAC</i>	(Optional) Specifies that the rule matches ARP packets only when the target MAC address in the packet matches the value of the <i>target-MAC</i> argument. You can specify <b>host</b> <i>target-MAC</i> only when you use the <b>response</b> keyword. Valid values for the <i>target-MAC</i> argument are MAC addresses in dotted-hexadecimal format.
<i>target-MAC</i> <i>target-MAC-mask</i>	(Optional) MAC address and mask for the set of MAC addresses that the target MAC address in the packet can match. You can specify <i>target-MAC</i> <i>target-MAC-mask</i> only when you use the <b>response</b> keyword. The <i>target-MAC</i> and <i>target-MAC-mask</i> argument must be given in dotted-hexadecimal format. Specifying ffff.ffff.ffff as the <i>target-MAC-mask</i> argument is the equivalent of using the <b>host</b> keyword.

**Defaults**

None

**Command Modes**

ARP ACL configuration

**SupportedUserRoles**network-admin  
vdc-admin

## Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

### Command History

Release	Modification
4.0(1)	This command was introduced.

### Usage Guidelines

A newly created ARP 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.

When the device applies an ARP 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.

If you do not specify either the **response** or **request** keyword, the rule applies to packets that contain any ARP message.

This command does not require a license.

### Examples

This example shows how to enter ARP access list configuration mode for an ARP ACL named arp-acl-01 and add a rule that denies ARP request messages that contain a sender IP address that is within the 10.32.143.0 subnet:

```
switch# conf t
switch(config)# arp access-list arp-acl-01
switch(config-arp-acl)# deny request ip 10.32.143.0 255.255.255.0 mac any
```

### Related Commands

Command	Description
<b>arp access-list</b>	Configures an ARP ACL.
<b>ip arp inspection filter</b>	Applies an ARP ACL to a VLAN.
<b>permit (ARP)</b>	Configures a permit rule in an ARP ACL.
<b>remark</b>	Configures a remark in an ACL.
<b>show arp access-list</b>	Displays all ARP ACLs or one ARP ACL.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## 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]
[fragments] [log] [time-range time-range-name]
```

```
no deny protocol source destination [dscp dscp | precedence precedence] [fragments] [log]
[time-range time-range-name]
```

```
no sequence-number
```

### Internet Control Message Protocol

```
[sequence-number] deny icmp source destination [icmp-message] [dscp dscp | precedence
precedence] [fragments] [log] [time-range time-range-name]
```

### Internet Group Management Protocol

```
[sequence-number] deny igmp source destination [igmp-message] [dscp dscp | precedence
precedence] [fragments] [log] [time-range time-range-name]
```

### Internet Protocol v4

```
[sequence-number] deny ip source destination [dscp dscp | precedence precedence] [fragments]
[log] [time-range time-range-name]
```

### 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] | portgroup portgroup] destination
[operator port [port] | portgroup portgroup] [dscp dscp | precedence precedence] [fragments]
[log] [time-range time-range-name]
```

## Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Syntax Description	
<i>sequence-number</i>	<p>(Optional) Sequence number of the <b>deny</b> 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.</p> <p>A sequence number can be any integer between 1 and 4294967295.</p> <p>By default, the first rule in an ACL has a sequence number of 10.</p> <p>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.</p> <p>Use the <b>resequence</b> command to reassign sequence numbers to rules.</p>
<i>protocol</i>	<p>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:</p> <ul style="list-style-type: none"> <li>• <b>icmp</b>—Specifies that the rule applies to ICMP traffic only. When you use this keyword, the <i>icmp-message</i> argument is available, in addition to the keywords that are available for all valid values of the <i>protocol</i> argument.</li> <li>• <b>igmp</b>—Specifies that the rule applies to IGMP traffic only. When you use this keyword, the <i>igmp-type</i> argument is available, in addition to the keywords that are available for all valid values of the <i>protocol</i> argument.</li> <li>• <b>ip</b>—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: <ul style="list-style-type: none"> <li>– <b>dscp</b></li> <li>– <b>fragments</b></li> <li>– <b>log</b></li> <li>– <b>precedence</b></li> <li>– <b>time-range</b></li> </ul> </li> <li>• <b>tcp</b>—Specifies that the rule applies to TCP traffic only. When you use this keyword, the <i>flags</i> and <i>operator</i> arguments and the <b>portgroup</b> and <b>established</b> keywords are available, in addition to the keywords that are available for all valid values of the <i>protocol</i> argument.</li> <li>• <b>udp</b>—Specifies that the rule applies to UDP traffic only. When you use this keyword, the <i>operator</i> argument and the <b>portgroup</b> keyword are available, in addition to the keywords that are available for all valid values of the <i>protocol</i> argument.</li> </ul>
<i>source</i>	<p>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.</p>
<i>destination</i>	<p>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.</p>

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

---

<b>dscp</b> <i>dscp</i>	<p>(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 <i>dscp</i> argument can be one of the following numbers or keywords:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• <b>af11</b>—Assured Forwarding (AF) class 1, low drop probability (001010)</li><li>• <b>af12</b>—AF class 1, medium drop probability (001100)</li><li>• <b>af13</b>—AF class 1, high drop probability (001110)</li><li>• <b>af21</b>—AF class 2, low drop probability (010010)</li><li>• <b>af22</b>—AF class 2, medium drop probability (010100)</li><li>• <b>af23</b>—AF class 2, high drop probability (010110)</li><li>• <b>af31</b>—AF class 3, low drop probability (011010)</li><li>• <b>af32</b>—AF class 3, medium drop probability (011100)</li><li>• <b>af33</b>—AF class 3, high drop probability (011110)</li><li>• <b>af41</b>—AF class 4, low drop probability (100010)</li><li>• <b>af42</b>—AF class 4, medium drop probability (100100)</li><li>• <b>af43</b>—AF class 4, high drop probability (100110)</li><li>• <b>cs1</b>—Class-selector (CS) 1, precedence 1 (001000)</li><li>• <b>cs2</b>—CS2, precedence 2 (010000)</li><li>• <b>cs3</b>—CS3, precedence 3 (011000)</li><li>• <b>cs4</b>—CS4, precedence 4 (100000)</li><li>• <b>cs5</b>—CS5, precedence 5 (101000)</li><li>• <b>cs6</b>—CS6, precedence 6 (110000)</li><li>• <b>cs7</b>—CS7, precedence 7 (111000)</li><li>• <b>default</b>—Default DSCP value (000000)</li><li>• <b>ef</b>—Expedited Forwarding (101110)</li></ul>
-------------------------	--

---

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

<b>precedence</b> <i>precedence</i>	<p>(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the <i>precedence</i> argument. The <i>precedence</i> argument can be a number or a keyword, as follows:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• <b>critical</b>—Precedence 5 (101)</li> <li>• <b>flash</b>—Precedence 3 (011)</li> <li>• <b>flash-override</b>—Precedence 4 (100)</li> <li>• <b>immediate</b>—Precedence 2 (010)</li> <li>• <b>internet</b>—Precedence 6 (110)</li> <li>• <b>network</b>—Precedence 7 (111)</li> <li>• <b>priority</b>—Precedence 1 (001)</li> <li>• <b>routine</b>—Precedence 0 (000)</li> </ul>
<b>fragments</b>	<p>(Optional) Specifies that the rule matches only those packets that are noninitial fragments. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the devices requires to evaluate those options is contained only in initial fragments.</p>
<b>log</b>	<p>(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information:</p> <ul style="list-style-type: none"> <li>• Whether the protocol was TCP, UDP, ICMP or a number</li> <li>• Source and destination addresses</li> <li>• Source and destination port numbers, if applicable</li> </ul>
<b>time-range</b> <i>time-range-name</i>	<p>(Optional) Specifies the time range that applies to this rule. You can configure a time range by using the <b>time-range</b> command. The <i>time-range-name</i> argument can be up to 64 alphanumeric, case-sensitive characters.</p>
<i>icmp-message</i>	<p>(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.</p>
<i>igmp-message</i>	<p>(IGMP only: Optional) IGMP message type that the rule matches. The <i>igmp-message</i> argument can be the IGMP message number, which is an integer from 0 to 15. It can also be one of the following keywords:</p> <ul style="list-style-type: none"> <li>• <b>dvmp</b>—Distance Vector Multicast Routing Protocol</li> <li>• <b>host-query</b>—Host query</li> <li>• <b>host-report</b>—Host report</li> <li>• <b>pim</b>—Protocol Independent Multicast</li> <li>• <b>trace</b>—Multicast trace</li> </ul>

## Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

<i>operator port</i> [ <i>port</i> ]	<p>(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 <i>operator</i> and <i>port</i> arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>The <i>port</i> 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.</p> <p>A second <i>port</i> argument is required only when the <i>operator</i> argument is a range. The <i>operator</i> argument must be one of the following keywords:</p> <ul style="list-style-type: none"> <li>• <b>eq</b>—Matches only if the port in the packet is equal to the <i>port</i> argument.</li> <li>• <b>gt</b>—Matches only if the port in the packet is greater than and not equal to the <i>port</i> argument.</li> <li>• <b>lt</b>—Matches only if the port in the packet is less than and not equal to the <i>port</i> argument.</li> <li>• <b>neq</b>—Matches only if the port in the packet is not equal to the <i>port</i> argument.</li> <li>• <b>range</b>—Requires two <i>port</i> arguments and matches only if the port in the packet is equal to or greater than the first <i>port</i> argument and equal to or less than the second <i>port</i> argument.</li> </ul>
<b>portgroup</b> <i>portgroup</i>	<p>(Optional; TCP and UDP only) Specifies that the rule matches only packets that are from a source port or to a destination port that is a member of the IP port object group specified by the <i>portgroup</i> argument, which can be up to 64 alphanumeric, case-sensitive characters. Whether the IP port object group applies to a source port or a destination port depends upon whether you specify it after the <i>source</i> argument or after the <i>destination</i> argument.</p> <p>Use the <b>object-group ip port</b> command to create and change IP port object groups.</p>
<i>flags</i>	<p>(TCP only; Optional) TCP control bit flags that the rule matches. The value of the <i>flags</i> argument must be one or more of the following keywords:</p> <ul style="list-style-type: none"> <li>• <b>ack</b></li> <li>• <b>fin</b></li> <li>• <b>psh</b></li> <li>• <b>rst</b></li> <li>• <b>syn</b></li> <li>• <b>urg</b></li> </ul>
<b>established</b>	<p>(TCP only; Optional) Specifies that the rule matches only packets that belong to an established TCP connection. The device considers TCP packets with the ACK or RST bits set to belong to an established connection.</p>

### 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.

## Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

**Command Modes** IPv4 ACL configuration

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	4.0(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.

This command does not require a license.

### 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:

- IP address group object—You can use an IPv4 address group object to specify a *source* or *destination* argument. Use the **object-group ip address** command to create and change IPv4 address group objects. The syntax is as follows:

```
addrgroup address-group-name
```

The following example shows how to use an IPv4 address object group named lab-gateway-svrs to specify the *destination* argument:

```
switch(config-acl)# deny ip any addrgroup lab-gateway-svrs
```

- 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:

```
switch(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:

```
switch(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
```

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

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:

```
switch(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

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

- **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)

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

**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)

## Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

**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:

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

This example shows how to configure an IPv4 ACL named `acl-eng-to-marketing` with a rule that denies all IP traffic from an IPv4 address object group named `eng_workstations` to an IP address object group named `marketing_group` followed by a rule that permits all other IPv4 traffic:

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

### Related Commands

Command	Description
<b>ip access-list</b>	Configures an IPv4 ACL.
<b>object-group ip address</b>	Configures an IPv4 address object group.
<b>object-group ip port</b>	Configures an IP port object group.
<b>permit (IPv4)</b>	Configures a permit rule in an IPv4 ACL.
<b>remark</b>	Configures a remark in an IPv4 ACL.
<b>show ip access-list</b>	Displays all IPv4 ACLs or one IPv4 ACL.
<b>statistics per-entry</b>	Enables collection of statistics for each entry in an ACL.
<b>time-range</b>	Configures a time range.

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

## 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

<i>sequence-number</i>	(Optional) Sequence number of the <b>deny</b> 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 <b>resequence</b> command to reassign sequence numbers to rules.
<i>source</i>	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.
<i>destination</i>	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.
<i>protocol</i>	(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.
<b>cos</b> <i>cos-value</i>	(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 <i>cos-value</i> argument. The <i>cos-value</i> argument can be an integer from 0 to 7.
<b>vlan</b> <i>VLAN-ID</i>	(Optional) Specifies that the rule matches only packets with an IEEE 802.1Q header that contains the VLAN ID given. The <i>VLAN-ID</i> 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

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	4.0(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.

This command does not require a license.

### 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:

```
switch(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:

```
switch(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)
- **larc-sca**—DEC LARC, SCA (0x6007)

## *Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*

- **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:

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

### Related Commands

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

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## deny (role-based access control list)

To configure a deny action in the security group access control list (SGACL), use the **deny** command. To remove the action, use the **no deny** form of this command.

```
deny {all | icmp | igmp | ip | {{tcp | udp} [[src | dest] {{eq | gt | lt | neq} port-number} |
range port-number1 port-number2}}}
```

```
no deny {all | icmp | igmp | ip | {{tcp | udp} [[src | dest] {{eq | gt | lt | neq} port-number} |
range port-number1 port-number2}}}
```

Syntax Description		
<b>all</b>		Specifies all traffic.
<b>icmp</b>		Specifies Internet Control Message Protocol (ICMP) traffic.
<b>igmp</b>		Specifies Internet Group Management Protocol (IGMP) traffic.
<b>ip</b>		Specifies IP traffic.
<b>tcp</b>		Specifies TCP traffic.
<b>udp</b>		Specifies User Datagram Protocol (UDP) traffic.
<b>src</b>		Specifies the source port number.
<b>dest</b>		Specifies the destination port number
<b>eq</b>		Specifies equal to the port number.
<b>gt</b>		Specifies greater than the port number.
<b>lt</b>		Specifies less than the port number.
<b>neq</b>		Specifies not equal to the port number.
<i>port-number</i>		Port number for TCP or UDP. The range is from 0 to 65535.
<b>range</b>		Specifies a port range for TCP or UDP.
<i>port-number1</i>		First port in the range. The range is from 0 to 65535.
<i>port-number2</i>		Last port in the range. The range is from 0 to 65535.

**Defaults** None

**Command Modes** role-based access control list

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

This command requires the Advanced Services license.

**Examples**

This example shows how to add a deny action to an SGACL:

```
switch# config t
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# deny icmp
```

This example shows how to remove a deny action from an SGACL:

```
switch# config t
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# no deny icmp
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>cts role-based access-list</b>	Configures Cisco TrustSec SGACLs.
<b>feature cts</b>	Enables the Cisco TrustSec feature.
<b>show cts role-based access-list</b>	Displays the Cisco TrustSec SGACL configuration.

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)**

## description (identity policy)

To configure a description for an identity policy, use the **description** command. To revert to the default, use the **no** form of this command.

```
description "text"
```

```
no description
```

Syntax Description	"text"	Text string that describes the identity policy. The string is alphanumeric. The maximum length is 100 characters.
--------------------	--------	---

Defaults	None
----------	------

Command Modes	Identity policy configuration
---------------	-------------------------------

SupportedUserRoles	network-admin vdc-admin VDC user
--------------------	--

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.
------------------	--

Examples	This example shows how to configure the description for an identity policy:
	<pre>switch# config t switch(config)# identity policy AdminPolicy switch(config-id-policy)# description "Administrator identity policy"</pre>

This example shows how to remove the description from an identity policy:

```
switch# config t
switch(config)# identity policy AdminPolicy
switch(config-id-policy)# no description
```

Related Commands	Command	Description
	<b>identity policy</b>	Creates or specifies an identity policy and enters identity policy configuration mode.
	<b>show identity policy</b>	Displays identity policy information.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

## description (user role)

To configure a description for a user role, use the **description** command. To revert to the default, use the **no** form of this command.

**description** *text*

**no description**

Syntax Description	<i>text</i>	Text string that describes the user role. The string is alphanumeric. The maximum length is 128 characters.
--------------------	-------------	---

Defaults	None
----------	------

Command Modes	User role configuration
---------------	-------------------------

SupportedUserRoles	network-admin vdc-admin
--------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	You can include blank spaces in the user role description text. This command does not require a license.
------------------	---

Examples	This example shows how to configure the description for a user role: <pre>switch# <b>config t</b> switch(config)# <b>role name MyRole</b> switch(config-role)# <b>description User role for my user account.</b></pre>
----------	---

This example shows how to remove the description from a user role:

```
switch# config t  
switch(config)# role name MyRole  
switch(config-role)# no description
```

Related Commands	Command	Description
	<b>role name</b>	Creates or specifies a user role and enters user role configuration mode.
	<b>show role</b>	Displays user role information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## device

To add a supplicant device to the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) identity profile exception list, use the **device** command. To remove a supplicant device, use the **no** form of this command.

```
device { authenticate | not-authenticate } { ip-address ipv4-address [subnet-mask] | mac-address
mac-address [mac-address-mask] } policy policy-name
```

```
no device { authenticate | not-authenticate } { ip-address ipv4-address [subnet-mask] |
mac-address mac-address [mac-address-mask] } policy policy-name
```

### Syntax Description

<b>authenticate</b>	Specifies to allow authentication of the device using the policy.
<b>not-authenticate</b>	Specifies to not allow authentication of the device using the policy.
<b>ip-address</b> <i>ipv4-address</i>	Specifies the IPv4 address for the supplicant device in the A.B.C.D format.
<i>subnet-mask</i>	(Optional) IPv4 subnet mask for the IPv4 address.
<b>mac-address</b> <i>mac-address</i>	Specifies the MAC address for the supplicant device in the XXXX.XXXX.XXXX format.
<i>mac-address-mask</i>	(Optional) Mask for the MAC address.
<b>policy</b> <i>policy-name</i>	Specifies the policy to use for the supplicant device.

### Defaults

None

### Command Modes

Identity policy configuration

### Supported User Roles

network-admin  
vdc-admin  
VDC user

### Command History

Release	Modification
4.0(1)	This command was introduced.

### Usage Guidelines

This command does not require a license.

### Examples

This example shows how to add a device to the EAPoUDP identity profile:

```
switch# config t
switch(config)# identity profile eapoupd
switch(config-id-policy)# device authenticate 10.10.1.1 255.255.255.245 policy AdminPolicy
```

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

This example shows how to remove a device from the EAPoUDP identity profile:

```
switch# config t  
switch(config)# identity profile eapoupd  
switch(config-id-policy)# no device authenticate 10.10.2.2 255.255.255.245 policy  
UserPolicy
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>identity policy</b>	Creates or specifies an identity policy and enters identity policy configuration mode.
<b>show identity policy</b>	Displays identity policy information.

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*

## dot1x default

To reset the 802.1X global or interface configuration to the default, use the **dot1x default** command.

**dot1x default**

**Syntax Description** This command has no arguments or keywords.

**Defaults** None

**Command Modes** Global configuration  
Interface configuration

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** You must use the **feature dot1x** command before you configure 802.1X.  
This command does not require a license.

**Examples** This example shows how to set the global 802.1X parameters to the default:

```
switch# config t
switch(config)# dot1x default
```

This example shows how to set the interface 802.1X parameters to the default:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x default
```

Related Commands	Command	Description
	<b>feature dot1x</b>	Enables the 802.1X feature.
	<b>show dot1x</b>	Displays 802.1X feature status information.

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*

## dot1x host-mode

To allow 802.1X authentication for either a single supplicant or multiple supplicants on an interface, use the **dot1x host-mode** command. To revert to the default, use the **no** form of this command.

```
dot1x host-mode { multi-host | single-host }
```

```
no dot1x host-mode
```

Syntax Description	Command	Description
	<b>multi-host</b>	Allows 802.1X authentication for multiple supplicants on the interface.
	<b>single-host</b>	Allows 802.1X authentication for only a single supplicant on the interface.

Defaults	Default
	<b>single-host</b>

Command Modes	Mode
	Interface configuration

Supported User Roles	Roles
	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Guidelines
	You must use the <b>feature dot1x</b> command before you configure 802.1X. This command does not require a license.

Examples	Example
	This example shows how to allow 802.1X authentication of multiple supplicants on an interface:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x host-mode multi-host
```

This example shows how to revert to the default host mode on an interface:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# no dot1x host-mode
```

Related Commands	Command	Description
	<b>feature dot1x</b>	Enables the 802.1X feature.
	<b>show dot1x all</b>	Displays all 802.1X information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## dot1x initialize

To initialize 802.1X authentication for supplicants, use the **dot1x initialize** command.

```
dot1x initialize [interface ethernet slot/port]
```

<b>Syntax Description</b>	<b>interface ethernet slot/port</b> (Optional) Specifies the interface for 802.1X authentication initialization.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Any command mode
----------------------	------------------

<b>SupportedUserRoles</b>	network-admin vdc-admin
---------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	You must use the <b>feature dot1x</b> command before you configure 802.1X. This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to initialize 802.1X authentication for supplicants on the NX-OS device: <pre>switch# dot1x initialize</pre> This example shows how to initialize 802.1X authentication for supplicants on an interface: <pre>switch# dot1x initialize interface ethernet 2/1</pre>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>feature dot1x</b>	Enables the 802.1X feature.
<b>show dot1x all</b>	Displays all 802.1X information.	

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*

## dot1x mac-auth-bypass

To enable MAC address authentication bypass on interfaces with no 802.1X supplicants, use the **dot1x mac-auth-bypass** command. To disable MAC address authentication bypass, use the **no** form of this command.

**dot1x mac-auth-bypass [eap]**

**no dot1x mac-auth-bypass**

Syntax Description	Command	Description
	<b>eap</b>	Specifies that the bypass use Extensible Authentication Protocol (EAP).

Defaults	Value
	Disabled

Command Modes	Mode
	Interface configuration

Supported User Roles	Roles
	network-admin vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Guidelines
	You must use the <b>feature dot1x</b> command before you configure 802.1X. This command does not require a license.

Examples	Example
	This example shows how to enable MAC address authentication bypass:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x mac-auth-bypass
```

This example shows how to disable MAC address authentication bypass:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x mac-auth-bypass
```

Related Commands	Command	Description
	<b>feature dot1x</b>	Enables the 802.1X feature.
	<b>show dot1x all</b>	Displays all 802.1X information.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

## dot1x max-reauth-req

To change the maximum number of times that the NX-OS device retransmits reauthentication requests to supplicants on an interface before the session times out, use the **dot1x max-reauth-req** command. To revert to the default, use the **no** form of this command.

```
dot1x max-reauth-req retry-count
```

```
no dot1x max-reauth-req
```

Syntax Description	<i>retry-count</i>	Retry count for reauthentication requests. The range is from 1 to 10.
--------------------	--------------------	---

Defaults	2 retries
----------	-----------

Command Modes	Interface configuration
---------------	-------------------------

SupportedUserRoles	network-admin vdc-admin
--------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	You must use the <b>feature dot1x</b> command before you configure 802.1X. This command does not require a license.
------------------	--

Examples	This example shows how to change the maximum number of reauthorization request retries for an interface:
----------	--

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x max-reauth-req 3
```

This example shows how to revert to the default maximum number of reauthorization request retries for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x max-reauth-req
```

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

Related Commands	Command	Description
	<b>feature dot1x</b>	Enables the 802.1X feature.
	<b>show dot1x all</b>	Displays all 802.1X information.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

## dot1x max-req

To change the maximum number of requests that the NX-OS device sends to a supplicant before restarting the 802.1X authentication, use the **dot1x max-req** command. To revert to the default, use the **no** form of this command.

```
dot1x max-req retry-count
```

```
no dot1x max-req
```

### Syntax Description

<i>retry-count</i>	Retry count for request sent to supplicant before restarting 802.1X reauthentication. The range is from 1 to 10.
--------------------	--

### Defaults

Global configuration: 2 retries

Interface configuration: Global configuration setting

### Command Modes

Global configuration  
Interface configuration

### Supported User Roles

network-admin  
vdc-admin

### Command History

Release	Modification
4.0(1)	This command was introduced.

### Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

### Examples

This example shows how to change the maximum number of request retries for the global 802.1X configuration:

```
switch# config t
switch(config)# dot1x max-req 3
```

This example shows how to revert to the default maximum number of request retries for the global 802.1X configuration:

```
switch# config t
switch(config)# no dot1x max-req
```

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

This example shows how to change the maximum number of request retries for an interface:

```
switch# config t  
switch(config)# interface ethernet 1/1  
switch(config-if)# dot1x max-req 4
```

This example shows how to revert to the default maximum number of request retries for an interface:

```
switch# config t  
switch(config)# interface ethernet 1/1  
switch(config-if)# no dot1x max-req
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>feature dot1x</b>	Enables the 802.1X feature.
<b>show dot1x all</b>	Displays all 802.1X information.

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*

## dot1x port-control

To control the 802.1X authentication performed on an interface, use the **dot1x port-control** command. To revert to the default, use the **no** form of this command.

```
dot1x port-control { auto | force-authorized | force-unauthorized }
```

```
no dot1x port-control { auto | force-authorized | force-unauthorized }
```

Syntax Description	auto	force-authorized	force-unauthorized
	Enables 802.1X authentication on the interface.	Disables 802.1X authentication on the interface and allows all traffic on the interface without authentication.	Disallows all authentication on the interface.

**Defaults** force-authorized

**Command Modes** Interface configuration

**Supported User Roles** network-admin  
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** You must use the **feature dot1x** command before you configure 802.1X. This command does not require a license.

**Examples** This example shows how to change the 802.1X authentication action performed on an interface:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x port-control auto
```

This example shows how to revert to the default 802.1X authentication action performed on an interface:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x port-control auto
```

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>feature dot1x</b>	Enables the 802.1X feature.
<b>show dot1x interface ethernet</b>	Displays 802.1X information for an interface.

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*

## dot1x radius-accounting

To enable RADIUS accounting for 802.1X, use the **dot1x radius-accounting** command. To revert to the default, use the **no** form of this command.

**dot1x radius-accounting**

**no dot1x radius-accounting**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Disabled

**Command Modes** Global configuration

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** You must use the **feature dot1x** command before you configure 802.1X.  
This command does not require a license.

**Examples** This example shows how to enable RADIUS accounting for 802.1X authentication:

```
switch# config t
switch(config)# dot1x radius-accounting
```

This example shows how to disable RADIUS accounting for 802.1X authentication:

```
switch# config t
switch(config)# no dot1x radius-accounting
```

Related Commands	Command	Description
	<b>feature dot1x</b>	Enables the 802.1X feature.
	<b>show running-config dot1x all</b>	Displays all 802.1X information in the running configuration.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## dot1x re-authentication (EXEC)

To manually reauthenticate 802.1X supplicants, use the **dot1x re-authentication** command.

```
dot1x re-authentication [interface ethernet slot/port]
```

<b>Syntax Description</b>	<b>interface ethernet slot/port</b> (Optional) Specifies the interface for manual reauthentication.
---------------------------	---

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	EXEC
----------------------	------

<b>SupportedUserRoles</b>	network-admin vdc-admin
---------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	You must use the <b>feature dot1x</b> command before you configure 802.1X. This command does not require a license.
-------------------------	--

<b>Examples</b>	This example shows how to reauthenticate 802.1X supplicants manually:
-----------------	---

```
switch# dot1x re-authentication
```

This example shows how to reauthenticate the 802.1X supplicant on an interface manually:

```
switch# dot1x re-authentication interface ethernet 2/1
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>feature dot1x</b>	Enables the 802.1X feature.
<b>show dot1x all</b>	Displays all 802.1X information.	

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*

# dot1x re-authentication (global configuration and interface configuration)

To enable periodic reauthenticate of 802.1X supplicants, use the **dot1x re-authentication** command. To revert to the default, use the **no** form of this command.

**dot1x re-authentication**

**no dot1x re-authentication**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Global configuration: Disabled  
Interface configuration: Global configuration setting

**Command Modes** Global configuration  
Interface configuration

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** You must use the **feature dot1x** command before you configure 802.1X.

In global configuration mode, this command configures periodic reauthentication for all supplicants on the NX-OS device. In interface configuration mode, this command configures periodic reauthentication only for supplicants on the interface.

This command does not require a license.

**Examples** This example shows how to enable periodic reauthentication of 802.1X supplicants:

```
switch# config t
switch(config)# dot1x re-authentication
```

This example shows how to disable periodic reauthentication of 802.1X supplicants:

```
switch# config t
switch(config)# no dot1x re-authentication
```

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

This example shows how to enable periodic reauthentication of 802.1X supplicants on an interface:

```
switch# config t  
switch(config)# interface ethernet 2/1  
switch(config-if)# dot1x re-authentication
```

This example shows how to disable periodic reauthentication of 802.1X supplicants on an interface:

```
switch# config t  
switch(config)# interface ethernet 2/1  
switch(config-if)# no dot1x re-authentication
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>feature dot1x</b>	Enables the 802.1X feature.
<b>show dot1x all</b>	Displays all 802.1X information.

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*

## dot1x system-auth-control

To enable 802.1X authentication, use the **dot1x system-auth-control** command. To disable 802.1X authentication, use the **no** form of this command.

**dot1x system-auth-control**

**no dot1x system-auth-control**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Enabled

**Command Modes** Global configuration

**SupportedUserRoles** network-admin  
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** The **dot1x system-auth-control** command does not delete the 802.1X configuration. You must use the **feature dot1x** command before you configure 802.1X. This command does not require a license.

**Examples** This example shows how to disable 802.1X authentication:

```
switch# config t
switch(config)# no dot1x system-auth-control
```

This example shows how to enable 802.1X authentication:

```
switch# config t
switch(config)# dot1x system-auth-control
```

Related Commands	Command	Description
	<b>feature dot1x</b>	Enables the 802.1X feature.
	<b>show dot1x</b>	Displays 802.1X feature status information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## dot1x timeout quiet-period

To configure the 802.1X quiet-period timeout globally or for an interface, use the **dot1x timeout quiet-period** command. To revert to the default, use the **no** form of this command.

**dot1x timeout quiet-period** *seconds*

**no dot1x timeout quiet-period**

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds for the 802.1X quiet-period timeout. The range is from 1 to 65535.
---------------------------	----------------	--

<b>Defaults</b>	Global configuration: 60 seconds Interface configuration: The value of the global configuration
-----------------	--

<b>Command Modes</b>	Global configuration Interface configuration
----------------------	---

<b>SupportedUserRoles</b>	network-admin vdc-admin
---------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	The 802.1X quiet-period timeout is the number of seconds that the device remains in the quiet state following a failed authentication exchange with a supplicant.
-------------------------	---

You must use the **feature dot1x** command before you configure 802.1X.



<b>Note</b>	You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.
-------------	---

This command does not require a license.

<b>Examples</b>	This example shows how to configure the global 802.1X quiet-period timeout:
-----------------	---

```
switch# config t
switch(config)# dot1x timeout quiet-period 45
```

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

This example shows how to revert to the default global 802.1X quiet-period timeout:

```
switch# config t  
switch(config)# no dot1x timeout quiet-period
```

This example shows how to configure the 802.1X quiet-period timeout for an interface:

```
switch# config t  
switch(config)# interface ethernet 1/1  
switch(config-if)# dot1x timeout quiet-period 50
```

This example shows how to revert to the default 802.1X quiet-period timeout for an interface:

```
switch# config t  
switch(config)# interface ethernet 1/1  
switch(config-if)# no dot1x timeout quiet-period
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>feature dot1x</b>	Enables the 802.1X feature.
<b>show dot1x all</b>	Displays all 802.1X information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## dot1x timeout ratelimit-period

To configure the 802.1X rate-limit period timeout for the supplicants on an interface, use the **dot1x timeout ratelimit-period** command. To revert to the default, use the **no** form of this command.

**dot1x timeout ratelimit-period** *seconds*

**no dot1x timeout ratelimit-period**

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds for the 802.1X rate-limit period timeout. The range is from 1 to 65535.
---------------------------	----------------	---

<b>Defaults</b>	0 seconds
-----------------	-----------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>SupportedUserRoles</b>	network-admin vdc-admin
---------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

**Usage Guidelines**

The 802.1X rate-limit timeout period is the number of seconds that the authenticator ignores EAPOL-Start packets from supplicants that have successfully authenticated. This value overrides the global quiet period timeout.

You must use the **feature dot1x** command before you configure 802.1X.



**Note**

You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.

This command does not require a license.

**Examples**

This example shows how to configure the 802.1X rate-limit period timeout on an interface:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout ratelimit-period 60
```

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

This example shows how to revert to the default 802.1X rate-limit period timeout on an interface:

```
switch# config t  
switch(config)# interface ethernet 2/1  
switch(config-if)# dot1x timeout ratelimit-period 60
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>feature dot1x</b>	Enables the 802.1X feature.
<b>show dot1x interface ethernet</b>	Displays 802.1X information for an interface.

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)*

## dot1x timeout re-authperiod

To configure the 802.1X reauthentication-period timeout either globally or on an interface, use the **dot1x timeout re-authperiod** command. To revert to the default, use the **no** form of this command.

**dot1x timeout re-authperiod** *seconds*

**no dot1x timeout re-authperiod**

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds for the 802.1X reauthentication-period timeout. The range is from 1 to 65535.
---------------------------	----------------	---

<b>Defaults</b>	Global configuration: 3600 seconds Interface configuration: Global configuration setting
-----------------	---

<b>Command Modes</b>	Global configuration Interface configuration
----------------------	---

<b>SupportedUserRoles</b>	network-admin vdc-admin
---------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	The 802.1X reauthentication timeout period is the number of seconds between reauthentication attempts. You must use the <b>feature dot1x</b> command before you configure 802.1X.
-------------------------	---



<b>Note</b>	You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.
-------------	---

This command does not require a license.

<b>Examples</b>	This example shows how to configure the global 802.1X reauthentication-period timeout: <pre>switch# <b>config t</b> switch(config)# <b>dot1x timeout re-authperiod 3000</b></pre>
-----------------	--

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

This example shows how to configure the 802.1X reauthentication-period timeout on an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x timeout re-authperiod 3300
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>feature dot1x</b>	Enables the 802.1X feature.
<b>show dot1x all</b>	Displays all 802.1X information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## dot1x timeout server-timeout

To configure the 802.1X server timeout for an interface, use the **dot1x timeout server-timeout** command. To revert to the default, use the **no** form of this command.

**dot1x timeout server-timeout** *seconds*

**no dot1x timeout server-timeout**

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds for the 802.1X server timeout. The range is from 1 to 65535.
---------------------------	----------------	--

<b>Defaults</b>	30 seconds
-----------------	------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>SupportedUserRoles</b>	network-admin vdc-admin
---------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

**Usage Guidelines**

The 802.1X server timeout for an interface is the number of seconds that the NX-OS device waits before retransmitting a packet to the authentication server. This value overrides the global reauthentication period timeout.

You must use the **feature dot1x** command before you configure 802.1X.



**Note**

You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.

This command does not require a license.

**Examples**

This example shows how to configure the global 802.1X server timeout interval:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout server-timeout 45
```

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

This example shows how to revert to the default global 802.1X server timeout interval:

```
switch# config t  
switch(config)# interface ethernet 2/1  
switch(config-if)# dot1x timeout server-timeout 45
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>feature dot1x</b>	Enables the 802.1X feature.
<b>show dot1x interface ethernet</b>	Displays 802.1X information for an interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## dot1x timeout supp-timeout

To configure the 802.1X supplicant timeout for an interface, use the **dot1x timeout supp-timeout** command. To revert to the default, use the **no** form of this command.

**dot1x timeout supp-timeout** *seconds*

**no dot1x timeout supp-timeout**

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds for the 802.1X supplicant timeout. The range is from 1 to 65535.
---------------------------	----------------	--

<b>Defaults</b>	30 seconds
-----------------	------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Supported User Roles</b>	network-admin vdc-admin
-----------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

**Usage Guidelines**

The 802.1X supplicant timeout for an interface is the number of seconds that the NX-OS device waits for the supplicant to respond to an EAP request frame before the NX-OS device retransmits the frame. You must use the **feature dot1x** command before you configure 802.1X.



**Note**

You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.

This command does not require a license.

**Examples**

This example shows how to configure the 802.1X server timeout interval on an interface:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout supp-timeout 45
```

This example shows how to revert to the default 802.1X server timeout interval on an interface:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# no dot1x timeout supp-timeout
```

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

Related Commands	Command	Description
	<b>feature dot1x</b>	Enables the 802.1X feature.
	<b>show dot1x interface ethernet</b>	Displays 802.1X information for an interface.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

## dot1x timeout tx-period

To configure the 802.1X transmission-period timeout either globally or for an interface, use the **dot1x timeout tx-period** command. To revert to the default, use the **no** form of this command.

**dot1x timeout tx-period** *seconds*

**no dot1x timeout tx-period**

<b>Syntax Description</b>	<i>seconds</i>	Specifies number of seconds for the 802.1X transmission-period timeout. The range is from 1 to 65535.
---------------------------	----------------	---

<b>Defaults</b>	Global configuration: 60 seconds Interface configuration: Global configuration setting
-----------------	---

<b>Command Modes</b>	Global configuration Interface configuration
----------------------	---

<b>SupportedUserRoles</b>	network-admin vdc-admin
---------------------------	----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	The 802.1X transmission-timeout period is the number of seconds that the NX-OS device waits for a response to an EAP-request/identity frame from the supplicant before retransmitting the request. You must use the <b>feature dot1x</b> command before you configure 802.1X.
-------------------------	--



<b>Note</b>	You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.
-------------	---

This command does not require a license.

<b>Examples</b>	This example shows how to configure the global 802.1X transmission-period timeout: <pre>switch# <b>config t</b> switch(config)# <b>dot1x timeout tx-period 45</b></pre>
-----------------	--

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***

This example shows how to revert to the default global 802.1X transmission-period timeout:

```
switch# config t  
switch(config)# no dot1x timeout tx-period
```

This example shows how to configure the 802.1X transmission-period timeout for an interface:

```
switch# config t  
switch(config)# interface ethernet 1/1  
switch(config-if)# dot1x timeout tx-period 45
```

This example shows how to revert to the default 802.1X transmission-period timeout for an interface:

```
switch# config t  
switch(config)# interface ethernet 1/1  
switch(config-if)# no dot1x timeout tx-period
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>feature dot1x</b>	Enables the 802.1X feature.
<b>show dot1x all</b>	Displays all 802.1X information.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)***