



P Commands

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

password strength-check

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

password strength-check

no password strength-check

Syntax Description

Defaults

Disabled

Command Modes

Global configuration

Supported User Roles

vdc-admin

Command History

4.0(3)	This command was introduced.
--------	------------------------------

Usage Guidelines

When you enable password-strength checking, the NX-OS software only allows you to create strong passwords. The characteristics for strong passwords include the following:

- At least eight characters long
- Does not contain many consecutive characters (such as “abcd”)

-
-
-
-
-

The following are examples of strong passwords:

- If2CoM18
2004AsdfLkj30
Cb1955S21



Note

This command does not require a license.

Examples

```
switch# configure terminal  
switch(config)# password strength-check
```

```
    configure terminal  
        no password strength-check
```

Enables password-strength checking.

```
show running-config security
```

periodic

```
[sequence-number] weekday time weekday time
{sequence-number | periodic to }
[ ] list-of-weekdays time time
sequence-number list-of-weekdays time time
```

sequence-number

A sequence number can be any integer between 1 and 4294967295.

By default, the first rule in a time range has a sequence number of 10.

If you do not specify a sequence number, the device adds the rule to the end of the time range 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.

Day of the week that the range begins or ends. The first occurrence of this argument is the day that the range starts. The second occurrence is the day that the range ends. If the second occurrence is omitted, the end of the range is on the same day as the start of the range.

The following keywords are valid values for the argument:

monday
tuesday
wednesday
thursday
friday
saturday
sunday

You can specify the argument in 24-hour notation, in the format *hours minutes hours minutes seconds*. For example, 8:00 a.m. is 8:00 and 8:00 p.m. is 20:00.

Separates the first and second occurrences of the argument.

(Optional) Days that the range is in effect. Valid values of this argument are as follows:

A space-delimited list of weekdays, such as the following:

monday thursday friday

daily—All days of the week.

—Monday through Friday.

—Saturday through Sunday.

Time-range configuration

network-admin

vdc-admin

4.0(1)

This command was introduced.

This command does not require a license.

This example shows how to create a time range named weekend-remote-access-times and configure a periodic rule that allows traffic between 4:00 a.m. and 10:00 p.m. on Saturday and Sunday:

```
switch(config-time-range) # periodic weekend 04:00:00 to 22:00:00
```

```
    configure terminal
```

```
        time-range mwf-evening
```

```
            periodic monday wednesday friday 18:00:00 to 22:00:00
```

absolute

time-range

permit (ARP)

To create an ARP ACL rule that permits ARP traffic that matches its conditions, use the command. To remove a rule, use the form of this command.

General Syntax

```

sequence-number
    sender-IP sender-IP
    sender-MAC sender-MAC sender-MAC-mask

sequence-number
    sender-IP sender-IP sender-IP-mask
    sender-MAC sender-MAC sender-MAC-mask

sequence-number
    target-IP target-IP target-IP-mask
    sender-MAC sender-MAC-mask
    target-MAC \ target-MAC target-MAC-mask

sequence-number
    sender-IP sender-IP sender-IP-mask
    sender-MAC sender-MAC-mask
    sender-IP sender-IP sender-IP-mask
    sender-MAC sender-MAC sender-MAC-mask

sequence-number
    target-IP target-IP-mask
    sender-IP sender-IP sender-IP-mask
    sender-MAC sender-MAC sender-MAC-mask
    target-MAC \ target-MAC target-MAC-mask
    
```

sequence-number

sender-IP

sender-IP

sender-IP

sender-IP

sender-IP-mask

sender-IP

sender-IP-mask

sender-IP-mask


```
switch(config-arp-acl)# permit request ip 10.32.143.0 255.255.255.0 mac any
```

```
deny (ARP)  
arp access-list  
ip arp inspection filter  
remark  
show arp access-list
```

permit (IPv4)

General Syntax

```
                                protocol source destination      dscp      precedence  
                                time-range-name  
  
                                protocol source destination      dscp      precedence  
                                time-range-name  
  
                                sequence-number
```

Internet Control Message Protocol

Internet Group Management Protocol

Internet Protocol v4

Transmission Control Protocol

User Datagram Protocol

Syntax Description

-
-
-
-
-
-
-
-

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

af12

af13

af21

af22

af23

af31

af32

af33

af41

af42

af43

cs1

cs2

cs3

cs4

cs5

cs6

cs7

default

ef

precedence

critical
flash
flash-override
immediate
internet
network
priority
routine

fragments

log

time-range

time-range

dvmrp
host-query—Host query
host-report—Host report
pim—Protocol Independent Multicast
trace—Multicast trace

[]

(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 `port` and `port-range` arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the `port` argument or after the `port-range` 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-range` argument is required only when the `port` argument is a range.

The `port-range` argument must be one of the following keywords:

—Matches only if the port in the packet is equal to the `port` argument.

—Matches only if the port in the packet is greater than and not equal to the `port` argument.

—Matches only if the port in the packet is less than and not equal to the `port` argument.

—Matches only if the port in the packet is not equal to the `port` argument.

—Requires two `port-range` arguments and matches only if the port in the packet is equal to or greater than the first `port-range` argument and equal to or less than the second `port-range` argument.

(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 `ip-port-object-group` 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 `port` argument or after the `ip-port-object-group` argument.

Use the **object-group ip port**

ack

fin

psh

rst

syn

urg

established

an established TCP connection. The device considers TCP packets with the ACK or RST bits set to belong to an established connection.

A newly created IPv4 ACL contains no rules.

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

IPv4 ACL configuration

network-admin
vdc-admin

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

-

address-group-name

```
permit ip any addrgroup lab-gateway-svrs
```

IPv4-address network-wildcard

```
permit tcp 192.168.67.0 0.0.0.255 any
```

IPv4-address/prefix-len

```
permit udp 192.168.67.0/24 any
```

```
host IPv4-address
```

IPv4-address/32 and *IPv4-address 0.0.0.0*.

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

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.

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
- Alternate address
- Datagram conversion
- Host prohibited
- Net prohibited
- Echo (ping)
- Echo reply
- Parameter problem
- Host isolated
- Host unreachable for precedence
- Host redirect
- Host redirect for ToS
- Host unreachable for ToS
- Host unknown
- Host unreachable
- Information replies
- Information requests
- Mask replies
- Mask requests
- Mobile host redirect
- Network redirect
- Net redirect for ToS
- Network unreachable for ToS
- Net unreachable
- Network unknown
- Parameter required but no room
- Parameter required but not present
- Fragmentation needed and DF set

- All parameter problems
- Port unreachable
 - Precedence cutoff
 - Protocol unreachable
 - Reassembly timeout
- All redirects
 - Router discovery advertisements
 - Router discovery solicitations
- Source quenches
 - Source route failed

time-exceeded

timestamp-reply

timestamp-request

traceroute

ttl-exceeded

unreachable

TCP Port Names

UDP Port Names

non500-isakmp

ntp

pim-auto-rp

rip

snmp

snmptrap

sunrpc
syslog
tacacs
talk
tftp
time
who
xdmcp

all IP traffic from an IP-address object group named eng_workstations to an IP-address object group named marketing_group:

```
permit ip addrgroup eng_workstations addrgroup marketing_group
```

deny (IPv4)
ip access-list
object-group ip address
object-group ip port
remark
show ip access-list
statistics per-entry
time-range

permit (MAC)

VLAN-ID

source destination protocol cos-value VLAN-ID

sequence-number

sequence-number

source

destination

protocol

<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.
------------------	--

<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.
----------------	---

A newly created MAC ACL contains no rules.

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

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

This command does not require a license.

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

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

MAC-address *MAC-mask*

MAC Protocols

-
-
-
-
-
- **etype-8042**
 - ip**
 - lat**
 - larc-sca**
 - mop-console**

mop-dump
vines-echo

deny (MAC)
mac access-list
remark
statistics per-entry
show mac access-list

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

```
switch# configure terminal  
switch(config)# cts role-based access-list MySGACL  
switch(config-rbacl)# no permit icmp
```

permit interface

Syntax Description

/

-

Defaults

Command Modes

SupportedUserRoles

Command History

Usage Guidelines

Examples

```
role name MyRole
  interface policy deny
    permit interface ethernet 2/1 - 8
```

```
configure terminal
  role name MyRole
    interface policy deny
      permit interface ethernet 1/1, ethernet 1/3, ethernet 1/5,
ethernet 1/7
```

```
configure terminal
  role name MyRole
    interface policy deny
      no permit interface ethernet 2/1
```

interface policy deny

role name

show role

permit vlan

no

permit vlan -

no permit vlan

**vlan policy deny
permit vlan**

```
configure terminal
  role name MyRole
  vlan policy deny
switch(config-role-vlan)#
```

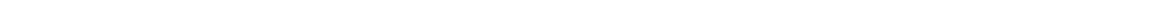
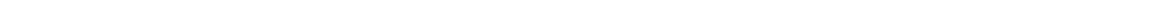
```
switch#
switch(config)#
switch(config-role)#
switch(config-role-vlan)#
```

```
switch#
switch(config)#
switch(config-role)#
switch(config-role-vlan)#
```

```
switch#
switch(config)#
switch(config-role)#
switch(config-role-vlan)#
```

```
switch#
switch(config)#
switch(config-role)#
switch(config-role-vrf)#
```

```
switch#
switch(config)#
switch(config-role)#
switch(config-role-vrf)#
```



platform access-list update

Syntax Description

Defaults

Command Modes

SupportedUserRoles

Command History

Release	Modification

Usage Guidelines



■ platform access-list update

Examples

Related Commands

Command

Description

■ platform rate-limit

SupportedUserRoles

Command History

Release	Modification

Usage Guidelines

Examples

Related Commands

Command	Description

police (policy map)

```

                                burst-size

                                cir-rate

                                prec-value      cos-value      dscp-value
                                } exceed drop set dscp dscp table
                                violate drop set dscp dscp table pir-markdown-map
                                transmit
                                transmit

    police cir      bps gbps kbps mbps pps
    pir      bps gbps kbps mbps be extended-burst-size

                                cir-rate

                                cir-rate      ]      bytes | kbytes | mbytes |
    ms | packets | us

    no police cir      bps gbps kbps mbps pps
    conform drop set-cos-transmit      set-dscp-transmit
    set-prec-transmit      transmit} exceed drop set dscp dscp table
    cir-markdown-map transmit violate drop set dscp dscp table pir-markdown-map
    transmit

    no police cir      bps gbps kbps mbps pps
    pir      bps gbps kbps mbps pps be      bytes | kbytes | mbytes
    | ms | packets | us
    
```

cir	
bps gbps kbps mbps pps	
bc	(Optional) Specifies the committed burst size. Committed burst size. The range is from 1 to 512000000.
 	(Optional) Specifies the units for a burst in bytes, kilobytes, megabytes, milliseconds, packets, or microseconds.
	Configures an action when the traffic conforms to the specified rates and bursts.
	Specifies the drop action.
	Specifies setting the class of service (CoS) value. The range is from 0 to 7.


```
configure terminal
  policy-map type control-plane PolicyMapA
    class ClassMapA
      no police 2000 kbps
```



hhh.



```
switch(config-if-cts-manual)# policy dynamic identity DeviceB
                               exit
                               shutdown
                               no shutdown
```

```
configure terminal
interface ethernet 2/3
  cts manual
                               no policy dynamic identity DeviceB
                               exit
  shutdown
  no shutdown
```

```
configure terminal
interface ethernet 2/4
  cts manual
                               policy static sgt 0x100
                               exit
  shutdown
  no shutdown
```

```
configure terminal
interface ethernet 2/4
  cts manual
                               no policy static sgt 0x100
                               exit
  shutdown
  no shutdown
```



```
configure terminal
  policy-map type control-plane PolicyMapA
```

```
configure terminal
  no policy-map type control-plane PolicyMapA
```



```
configure terminal
interface ethernet 2/1
  cts dot1x
```

```
switch(config-if-cts-dot1x)#
switch(config-if-cts-dot1x)#
switch(config-if)#
switch(config-if)#
```

```
switch#
switch(config)#
switch(config-if)#
switch(config-if-cts-dot1x)#
switch(config-if-cts-dot1x)#
switch(config-if)#
switch(config-if)#
```
