P Commands

permit (IPv4)

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

CSCsy01403: Make sure there are no extra spaces in the syntax diagram block following

General Syntax:

[*sequence-number*]**permit** *protocol source destination QA Test: CSCsv22488 The following groupchose should appear with square brackets only* [**dscp** *dscp*| **QA test CSCsz89741: check that a space appears after this** *precedence*]

[*QA Test: CSCsx24477*] **This synblk must appear on a different line** *protocol source destination*

QA Test Sprint 9 CSCtc25038 and CSCsw43905 There should be a pipe separator between this sentence| and this sentence. There should also be a single space before the pipe and after the pipe

QA Test Sprint 9: Open this command in firefox and check that the fonts for the command syntax is the same size.

no deny *protocol* { *source-ipv6-prefix*/*prefix-length* **|** **any** | **host** *source-ipv6-address* } [*operator* [*port-number*]] { *destination-ipv6-prefix*/*prefix-length* **|** **any** | **host** *destination-ipv6-address* } [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [log] [log-input] [mobility]** [**mobility-type** [*mh-number* | *mh-type*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] **[undetermined-transport]**

Syntax Description

sequence-number	Sequence number of the **permit** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence number to rules.
protocol	Name or number of the protocol of packets that the rule matches. Valid numbers are from 0 to 255. Valid protocol names are the following keywords: **icmp** Specifies that the rule applies to ICMP traffic only. When you use this keyword, the *icmp-message* argument is available, in addition to the keywords that are available for all valid values of the *protocol* ardument. **ip** Specifies that the rule applies to all IPv4 traffic. When you use this keyword, only the other keywords and arguments that apply to all IPv4 protocols are available. They include the following: • **dscp**

- **fragments**
- **log**
- **precedence**
- **time-range**

tcp Specifies that the rule applies to TCP traffic only. When you use this keyword, the *flags* and *operation* argumnets and the **portgroup** and **established** keywords are available, in addition to the keywords that are available for all valid values of the *protocol* argument.

udp Specifies that the rule applies to UDP traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *portocol* argument.

source Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see "Source and Destination" in the "Usage Guidelines" section.

destination Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see "Source and Destination" in the "Usage Guidelines" section.

dscp*dscp* (Optional) Specifies that the rule matches only those packets with the specified 6-bit differentiated services value in the DSCP field of the IP header. The dscp argument can be one of the following numbers or keywords:

0-63	The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only those packets that have the following bits in the DSCP field: 001010.
af12	AF class 1, medium drop probabilty (001100)
af13	AF class 1, high drop probabilty (001100)
af21	AF class 2, low drop probabilty (001100)
af22	AF class 2, medium drop probabilty (001100)
af23	AF class 2, high drop probabilty (001100)
af31	AF class 3, low drop probabilty (001100)
af32	AF class 3, medium drop probabilty (001100)
af33	AF class 3, high drop probabilty (001100)
af41	AF class 4, low drop probabilty (001100)
af42	AF class 4, medium drop probabilty (001100)
af43	AF class 4, high drop probabilty (001100)
cs1	Class-selector (CS) 1, precedence 1 (001000)

	cs2	Class-selector (CS) 2 (001000)
	cs3	Class-selector (CS) 3 (001000)
	cs4	Class-selector (CS) 4(001000)
	cs5	Class-selector (CS) 5 (001000)
	cs6	Class-selector (CS) 6(001000)
	cs7	Class-selector (CS) 7(001000)
	default	Default DSCP value (000000)
	if	Expedited Forwarding (101110)

precedence*precedence* (Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the precedence argument. The precedence argument can be a number or a keyword, as follows:

0-7	Decimal equivalent of the 3 bits of the IP Precedence field. For example, if you specify 3, the rule matches only packets that have the following bits in the DSCP field: 011.
critical	Precedence 5 (101)
flash	Precedence 3(011)
flash-override	Precedence 4(100)
immediate	Precedence 2 (010)
internet	Precedence 6 (110)
network	Precedence 7 (111)
priority	Precedence 1 (001)
routine	Precedence 0 (000)

fragments (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.

log (Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information:

Whether the protocol was TCP, UDP, ICMP or a number

Source and destination addresses

Source and destination port numbers, if applicable

tine-range*time-range* (Optional) Specifies the time range that applies to this rule.

Use the **time-range** command to a time range.

icmp-message	(ICMP only: Optional) ICMP message type that the rule matches. This argument can be an integer from 0 to 255 or one of the keywords listed under "ICMP Message Types" in the "Usage Guidelines" section.
igmp-message	(IGMP only: Optional) IGMP message type that the rule matches. The igmp-message argument can be the IGMP message number, which is an integer from 0 to 15. It can also be one of the following keywords: **dvmrp** Distance Vector Multicast Routing Protocol **host-query** Host query **host-report** Host report **pim** Protocol Independent Multicast **trace** Multicast trace
*operator*port	(Optional; TCP and UDP only) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the operator and port arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the source argument or after the destination argument. The port argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see "TCP Port Names" and "UDP Port Names" in the "Usage Guidelines" section. A second port argument is required only when the operator argument is a range. The operator argument must be one of the following keywords: **eq** Matches only if the port in the packet is equal to the port argument. **gt** Matches only if the port in the packet is greater than the port argument. **lt** Matches only if the port in the packet is less than the port argument. **neq** Matches only if the port in the packet is not equal to the port argument. **range** Requires two port arguments and matches only if the port in the packet is equal to or greater than the first port argument and equal to or less than the second port argument.
portgroup*portgroup*	(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 portgroup 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 source argument or after the destination argument. Use the **object-group ip port** command to create and change IP port object objects
	(TCP only; Optional) TCP control bit flags that the rule matches. The value of the flags argument must be one or more of the following keywords:

- **ack**
- **fin**
- **psh**
- **rst**
- **syn**
- **urg**

established	(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.

Command Default

A Newly created IPv4 ACL contains no rules

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

Command Modes

IPv4 ACL configuration

Command History

Release	Modification
4.0(1)	This Command was introduced

Usage Guidelines

QA Test Sprint 9 : Test That this Cross chapter xref link works. Check offline PDF. Run the publication WF and check the html and PDF.create vnic-egress-policy

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 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:

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: QA: CSCsz86893. These sep elements after addrgroup should render with a space (2 spaces). This is outside of a syntaxdiagram. **addrgroup** `space` *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)# permit 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-addressnetwork-willdcard* 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)#`

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

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
chargen	Character generator
cmd	Remote commands (rcmd,514)

Examples

QA Test: CSCsw88555. A Title "Examples" should be autognerated on the left hand side over here.This example shows how to configure an IPv4 ACL named acl-lab-01 with rules permitting all TCP and UDP traffic from the 10.23.0.0 and 192.168.37.0 networks to the 10.176.0.0 network:

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

QA Test Sprint 9 CSCta60192: The following long URL should not be jumbled up http://www.cisco.com/en/US/products/hw/phones/ps379/en/US/products/hw/phones/ps379/en/US/products/hw/phones/ps379/en/US/products/hw/phones/ps379/tsd_products_support_translated_end_user_guides_list.html

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

```
switch#config t
switch(config-acl)# permit tcp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# permit tcp 10.23.0.0/16 10.176.0.0/16
```

Task ID

QA Test: CSCsw88544 Task ID Text should be autogenerated toward the left of this table

This is a test	This is a test
QA Test Sprint 9 CSCta60192: The following long URL should not be jumbled up http://www.cisco.com/en/US/products/hw/phones/ps379/en/US/products/	This is a test

hw/phones/ps379/en/US/products/hw/phones/ps379/
en/US/products/hw/phones/ps379/tsd_products_
support_translated_end_user_guides_list.html

Table 1: Link Test

QA Test Sprint 9 CSCta60192: The following long URL should not be jumbled up http://www.cisco.com/en/US/products/hw/phones/ps379/en/US/products/hw/phones/ps379/en/US/products/hw/phones/ps379/en/US/products/hw/phones/ps379/tsd_products_support_translated_end_user_guides_list.html	test

Related Commands

QA Test Sprint 9 US195: This Related Command Section should render as a table. The Second column should contain the Shortdescription of the respective related command. Also make sure that the shortdescription text does not get concatenated to the linktext

Command	Description
create vnic, page 9	This is the create vnic Command
create vnic-egress-policy	This is short dfescription for create vnic-egress-policy command
create vnic-templ	This is the create vnic-templ Command

create vnic

QA Test Sprint 9 CSCta77961: Test that each Command appears in its own page.

To create a VNIC (Virtual Network Interface Card), use the **create vnic** command.

create vnic *name* { **fabric** { **a | a-b | b | b-a** } | **eth-if** *eth-if* } *

Syntax Description

name	VNIC template name. The range of valid values is 1 to 16.
fabric	Specifies the fabric switch identification number.
a	Specifies switch A.
a-b	Specifies redundant, with switch A as primary.
b	Specifies switch B.
b-a	Specifies redundant, with switch B as primary.
eth-if	Specifies a Ethernet interface.
eth-if	Ethernet interface name. The range of valid values is 1 to 16.

Command Default

None

Command Modes

Service profile (/org/service-profile)

Command History

Release	Modification
1.0(1)	This command was introduced.

Usage Guidelines

Use this command to create a vNIC with the specified name, and enters organization virtual NIC mode.

Examples

This example shows how to create a vNIC:

```
switch-A# scope org org3
switch-A /org # scope service-profile sp1
switch-A /org/service-profile # create vnic vnic110
switch-A /org/service-profile/vnic* # commit-buffer
switch-A /org/service-profile/vnic #
```

Related Commands

QA Test: CSCtd06182 Check that the shortdescriptions appear on the dfescription column below. Also click on the first cross chapter link and see that it works in html and pdf chapters

Command	Description
create vsan, page 12	This is short description for vsan command
create vnic-egress-policy	This is short dfescription for create vnic-egress-policy command

create wwn-pool

To create a WWN (World Wide Name) pool, use the **create wwn-pool** command.

create wwn-pool *name* {**node-wwn-assignment**| **port-wwn-assignment**}

Syntax Description

name	WWN pool name. The range of valid values is 1 to 16.
node-wwn-assignment	Specifies world wide node name assignment.
port-wwn-assignment	Specifies world wide node port assignment.

Command Default

None

Command Modes

Organization (/org)

Command History

Release	Modification
1.0(1)	This command was introduced.

Usage Guidelines

Use this command to create a WWN pool with the specified name, and enters organization WWN pool mode. A WWN pool can include only WWNNs or WWPNs in the 20:xx range. All other WWN ranges are reserved.

Examples

This example shows how to create a WWN pool:

```
switch-A# scope org org3
switch-A /org # create wwn-pool wwnp1 port-wwn-assignment
switch-A /org/wwn-pool* # commit-buffer
switch-A /org/wwn-pool #
```

create vsan

QA Test Sprint 9 CSCta77961: Test that each Command appears in its own page.

To create a VSAN, use the **create vsan** command.

create vsan *name id fcoe-vlan*

Syntax Description

name	VSAN name. The range of valid values is 1 to 16.
id	VSAN identification number. The range of valid values is 1 to 4093.
default-2	Specifies default 1.
fcoe-vlan	Fibre Channel over Ethernet VLAN. The range of valid values is 1 to 4093.
default-1	Specifies default 2.

Command Default

None

Command Modes

Fibre Channel uplink (/fc-uplink)

Switch (/fc-uplink/switch)

Command History

Release	Modification
1.0(1)	This command was introduced.

Usage Guidelines

Use this command to create a VSAN with the specified name, and enters organization VSAN mode.

You can create a named VSAN with IDs from 1 to 4093. VSANs configured on different FCoE VLANs cannot share the same ID.

Examples

This example shows how to create a VSAN:

```
switch-A# scope fc-uplink
switch-A /fc-uplink # create vsan vs2 6 10
switch-A /fc-uplink/vsan* # commit-buffer
switch-A /fc-uplink/vsan #
```