I Commands

This chapter describes the Cisco NX-OS Border Gateway Protocol (BGP) commands that begin with I.

ip as-path access-list

To configure an access-list filter for Border Gateway Protocol (BGP) autonomous system (AS) numbers, use the **ip as-path access-list** command. To remove the filter, use the **no** form of this command.

ip as-path access-list *name* {**deny** | **permit**} *regexp*

no ip as-path access-list *name* {**deny** | **permit**} *regexp*

Syntax Description

name	AS path access list name. The name can be any alphanumeric string up to 63 characters.
deny	Rejects packets with AS numbers that match the *regexp* argument.
permit	Allows packets with AS numbers that match the *regexp* argument.
regexp	Regular expression to match BGP AS paths. See the *Cisco Nexus 5500 Series NX-OS Fundamentals Configuration Guide, Release 6.0* at the following URL for details on regular expressions: http://www.cisco.com/en/US/docs/switches/datacenter/nexus5500/sw/fundamentals/621_n1_1/Cisco_Nexus_5500_Series_NX-OS_Fundamentals_Configuration_Guide_Release_6_2_1_N1_1_chapter4.html#con_1237003

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip as-path access-list** command to configure an autonomous system path filter. You can apply autonomous system path filters to both inbound and outbound BGP paths. Each filter is defined by the regular expression. If the regular expression matches the representation of the autonomous system path of the route as an ASCII string, then the permit or deny condition applies. The autonomous system path should not contain the local autonomous system number.

Examples

This example shows how to configure an AS path filter for BGP to permit AS numbers 55:33 and 20:01 and apply it to a BGP peer for inbound filtering:

```
switch# configure terminal
switch(config)# ip as-path access-list filter1 permit 55:33,20:01
switch(config) router bgp 65536:20
switch(config-router)# neighbor 192.0.2.1/16 remote-as 65536:20
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# filter-list filter1 in
```

Related Commands

Command	Description
filter-list	Assigns an AS path filter to a BGP peer.
show ip as-path access-list	Displays information about IP AS path access lists.

ip community-list

To create a community list entry, use the **ip community-list** command. To remove the entry, use the **no** form of this command.

ip community-list standard *list-name* {**deny** | **permit**} {*aa*:*nn* | **internet** | **local-AS** | **no-advertise** | **no-export**}

no ip community-list standard *list-name*

ip community-list expanded *list-name* {**deny** | **permit**} *regexp*

no ip community-list expanded *list-name*

Syntax Description

standard *list-name*	Configures a named standard community list.
permit	Permits access for a matching condition.
deny	Denies access for a matching condition.
aa:*nn*	Autonomous system number and network number entered in the 4-byte new community format. This value is configured with two 2-byte numbers separated by a colon. A number from 1 to 65535 can be entered each 2-byte number. A single community can be entered or multiple communities can be entered, each separated by a space. You can pick more than one of these optional community keywords.
internet	Specifies the Internet community. Routes with this community are advertised to all peers (internal and external). You can pick more than one of these optional community keywords.
no-export	Specifies the no-export community. Routes with this community are advertised to only peers in the same autonomous system or to only other subautonomous systems within a confederation. These routes are not advertised to external peers. You can pick more than one of these optional community keywords.
local-AS	Specifies the local-as community. Routes with community are advertised to only peers that are part of the local autonomous system or to only peers within a subautonomous system of a confederation. These routes are not advertised external peers or to other subautonomous systems within a confederation. You can pick more than one of these optional community keywords.
no-advertise	Specifies the no-advertise community. Routes with this community are not advertised to any peer (internal or external). You can pick more than one of these optional community keywords.

expanded *list-name*	Configures a named expanded community list.
regexp	Regular expression that is used to specify a pattern to match against an input string. See the *Cisco Nexus 5500 Series NX-OS Fundamentals Configuration Guide, Release 6.0* at the following URL for details on regular expressions: http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/fundamentals/421_n1_1/Cisco_Nexus_5000_Series_NX-OS_Fundamentals_Configuration_Guide_Release_4_2_1_N1_1_chapter4.html#con_1237003 **Note** Regular expressions can be used with expanded community lists only.

Command Default

Community exchange is not enabled by default.

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

The **ip community-list** command is used to configure BGP community filtering. BGP community values are configured as a 4-byte number. The first two bytes represent the autonomous system number, and the last two bytes represent a user-defined network number. BGP community attribute exchange between BGP peers is enabled when the **send-community** command is configured for the specified neighbor. The BGP community attribute is defined in RFC 1997 and RFC 1998.

BGP community exchange is not enabled by default. Use the **send-community** command in BGP neighbor fix-family configuration mode to enable a BGP community attribute exchange between BGP peers.

The Internet community is applied to all routes or prefixes by default until any other community value is configured with this command or the **set community** command.

Once you configure a permit value to match a given set of communities, the community list defaults to an implicit deny for all other community values. Use the **internet** community to apply an implicit permit to the community list.

Standard Community Lists

Standard community lists are used to configure well-known communities and specific community numbers. You can pick more than one of the optional community keywords. A maximum of 32 communities can be configured in a standard community list. If you attempt to configure, the trailing communities that exceed the limit are not processed or saved to the running configuration file. The route-map can also match up to 32 community lists in one sequence.

Expanded Community Lists

Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is the longest construct is first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it matches the earliest part first.

Community List Processing

When multiple values are configured in the same community list statement, a logical AND condition is created. All community values must match to satisfy an AND condition. When multiple values are configured in separate community list statements, a logical OR condition is created. The first list that matches a condition is processed.

Examples

This example shows how to configure a standard community list where the routes with this community are advertised to all peers (internal and external):

```
switch(config)# ip community-list standard test1 permit internet
switch(config)#
```

This example shows how to configure a logical AND condition; all community values must match in order for the list to be processed:

```
switch(config)# ip community-list standard test1 permit 65534:40 65412:60 no-export
switch(config)#
```

In the above example, a standard community list is configured that permits routes from the following:

- Network 40 in autonomous system 65534 and from network 60 in autonomous system 65412.
- Peers in the same autonomous system or from subautonomous system peers in the same confederation.

This example shows how to configure a standard community list that denies routes that carry communities from network 40 in autonomous system 65534 and from network 60 in autonomous system 65412. This example shows a logical AND condition; all community values must match in order for the list to be processed.

```
switch(config)# ip community-list standard test2 deny 65534:40 65412:60
```

This example shows how to configure a named standard community list that permits all routes within the local autonomous system or permits routes from network 20 in autonomous system 40000. This example shows a logical OR condition; the first match is processed.

```
switch(config)# ip community-list standard RED permit local-AS

switch(config)# ip community-list standard RED permit 40000:20
switch(config)#
```

This example shows how to configure an expanded community list that denies routes that carry communities from any private autonomous system:

```
switch(config)# ip community-list expanded 500 deny
_64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_
switch(config)#
```

This example shows how to configure a named expanded community list that denies routes from network 1 through 99 in autonomous system 50000:

```
switch(config)# ip community-list list expanded BLUE deny 50000:[0-9][0-9]_
```

```
switch(config)#
```

Related Commands

Command	Description
feature bgp	Enables BGP.
match community	Matches a community in a route map.
send-community	Configures BGP to propagate community attributes to BGP peers.
set community	Sets a community in a route map.

ip directed-broadcast

To enable the translation of a directed broadcast to physical broadcasts, use the **ip directed-broadcast** command. To disable this function, use the no form of this command.

ip directed-broadcast [*acl-name*]

ip directed-broadcast [*acl-name*]

Syntax Description

acl-name	Access control list (ACL) name. An ACL name can be any case-sensitive, alphanumeric string up to 63 characters.

Defaults

Disabled; all IP directed broadcasts are dropped.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
6.0(2)N1(2)	This command was introduced.

Usage Guidelines

An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet, but which originates from a node that is not itself part of that destination subnet.

A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is exploded as a broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.

If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached will be exploded as broadcasts on that subnet.

If the **no ip directed-broadcast** command has been configured for an interface, directed broadcasts destined for the subnet to which that interface is attached will be dropped, rather than being broadcast.

Note Because directed broadcasts, and particularly Internet Control Message Protocol (ICMP) directed broadcasts, have been abused by malicious persons, we recommend that security-conscious users disable the **ip directed-broadcast** command on any interface where directed broadcasts are not needed and that they use access lists to limit the number of exploded packets.

This command does not require a license.

Examples

This example shows how to enable forwarding of IP directed broadcasts on Ethernet interface 2/1:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ip directed-broadcast
```

ip extcommunity-list

To create an extended community list entry, use the **ip extcommunity-list** command. To remove the entry, use the **no** form of this command.

ip extcommunity-list standard *list-name* {**deny** | **permit**} **generic** {**transitive** | **nontransitive**} *aa4*:*nn*

no ip extcommunity-list standard generic {**transitive** | **nontransitive**} *list-name*

ip extcommunity-list expanded *list-name* {**deny** | **permit**} **generic** {**transitive** | **nontransitive**} *regexp*

no ip extcommunity-list expanded generic {**transitive** | **nontransitive**} *list-name*

Syntax Description

standard *list-name*	Configures a named standard extended community list.
deny	Denies access for a matching condition.
permit	Permits access for a matching condition.
generic	Specifies the generic specific extended community type.
transitive	Configures BGP to propagate the extended community attributes to other autonomous systems.
nontransitive	Configures BGP to propagate the extended community attributes to other autonomous systems.
aa4:*nn*	Autonomous system number and network number. This value is configured with a 4-byte AS number and a 2-byte network number separated by a colon. The 4-byte AS number range is from 1 to 4294967295 in plaintext notation, or from 1.0 to 56636.65535 in AS.dot notation. You can enter a single community or multiple communities, each separated by a space.
expanded *list-name*	Configures a named expanded extended community list.
regexp	Regular expression that is used to specify a pattern to match against an input string. See the *Cisco Nexus 5500 Series NX-OS Fundamentals Configuration Guide, Release 6.0* at the following URL for details on regular expressions: http://www.cisco.com/en/US/docs/switches/datacenter/nexus5500/sw/fundamentals/621_n1_1/Cisco_Nexus_5500_Series_NX-OS_Fundamentals_Configuration_Guide_Release_6_2_1_N1_1_chapter4.html#con_1237003 **Note** Regular expressions can be used with expanded extended community lists only.

Command Default

Community exchange is not enabled by default.

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip extcommunity-list** command to configure extended community filtering for BGP. Extended community values are configured as a 6-byte number. The first four bytes represent the autonomous system number, and the last two bytes represent a user-defined network number. The BGP generic specific community attribute is defined in draft-ietf-idr-as4octet-extcomm-generic-subtype-00.txt.

BGP extended community exchange is not enabled by default. Use the **send-extcommunity** command in BGP neighbor fix-family configuration mode to enable extended community attribute exchange between BGP peers.

Once you configure a permit value to match a given set of extended communities, the extended community list defaults to an implicit deny for all other extended community values.

Standard Extended Community Lists

Use standard extended community lists to configure specific extended community numbers. You can configure a maximum of 16 extended communities in a standard extended community list.

Expanded Extended Community Lists

Use expanded extended community lists to filter communities using a regular expression. Use regular expressions to configure patterns to match community attributes. The order for matching using the * or + character is the longest construct is first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it matches the earliest part first.

Community List Processing

When you configure multiple values in the same extended community list statement, a logical AND condition is created. All extended community values must match to satisfy the AND condition. When you configure multiple values in separate community list statements, a logical OR condition is created. The first list that matches a condition is processed.

Examples

This example shows how to configure a standard generic specific extended community list that permits routes from network 40 in autonomous system 1.65534 and from network 60 in autonomous system 1.65412:

```
switch(config)# ip extcommunity-list standard test1 permit generic transitive 1.65534:40
1.65412:60
switch(config)#

All community values must match in order for the list to be processed.
```

Related Commands

Command	Description
feature bgp	Enables BGP.
match extcommunity	Matches an extended community in a route map.
send-community	Configures BGP to propagate community attributes to BGP peers.
set extcommunity	Sets an extended community in a route map.

ip prefix-list

To create a prefix list to match IP packets or routes against, use the **ip prefix-list** command. To remove the prefix-list, use the **no** form of this command.

ip prefix-list *name [***seq** *number] {***permit** | **deny***} prefix [***eq** *length* | *[***ge** *length*] [**le** *length]]*

no ip prefix-list *name [***seq** *number] {***permit** | **deny***} prefix [***eq** *length* | *[***ge** *length*] [**le** *length]]*

Syntax Description

name	IP prefix list name. The name can be any alphanumeric string up to 63 characters.
seq *number*	(Optional) Specifies the number to order entries in the prefix list. The range is from 1 to 4294967294.
permit	Allows routes or IP packets that match the prefix list.
deny	Rejects routes or IP packets that match the prefix list.
prefix	IP prefix in A.B.C.D/length format.
eq *length*	(Optional) Specifies the prefix length to match. The range is from 1 to 32.
ge *length*	(Optional) Specifies the prefix length to match. The range is from 1 to 32.
le *length*	(Optional) Specifies the prefix length to match. The range is from 1 to 32.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip prefix-list** command to configure IP prefix filtering. Configure prefix lists with **permit** or **deny** keywords to either permit or deny the prefix based on the matching condition. A prefix list consists of an IP address and a bit mask. The bit mask is entered as a number from 1 to 32. An implicit deny is applied to traffic that does not match any prefix-list entry.

You can configure prefix lists to match an exact prefix length or a prefix range. Use the **ge** and **le** keywords to specify a range of the prefix lengths to match, which provides a more flexible configuration. If you do not configure a sequence number, Cisco NX-OS applies a default sequence number of 5 to the prefix list and subsequent prefix list entries are incremented by 5 (for example, 5, 10, 15, and so on). If you configure a sequence number for the first prefix list entry but not subsequent entries, then Cisco NX-OS increments the subsequent entries by 5 (for example, if the first configured sequence number is 3, then subsequent entries will be 8, 13, 18, and so on). You can suppress default sequence numbers by entering the **no** form of this command with the **seq** keyword.

Cisco NX-OS evaluates prefix lists that start with the lowest sequence number and continue down the list until a match is made. Once a match is made, the **permit** or **deny** statement is applied to that network and the rest of the list is not evaluated.

Tip For the best performance of your network, you should configure the most frequently processed prefix list statements with the lowest sequence numbers. The **seq** *number* keyword and argument can be used for resequencing.

The prefix list is applied to inbound or outbound updates for specific peer by entering the **prefix-list** command in neighbor address-family mode. Prefix list information and counters are displayed in the output of the **show ip prefix-list** command. Prefix-list counters can be reset by entering the **clear ip prefix-list** command.

Examples

This example shows how to configure a prefix list and apply it to a Border Gateway Protocol (BGP) peer:

```
switch# configure terminal
switch(config)# ip prefix-list allowprefix 10 permit 192.0.2.0 eq 24
switch(config)# ip prefix-list allowprefix 20 permit 209.165.201.0 eq 27
switch(config) router bgp 65536:20
switch(config-router)# neighbor 192.0.2.1/16 remote-as 65536:20
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# prefix-list allowprefix in
switch(config-router-neighbor-af)#
```

Related Commands

Command	Description
clear ip prefix-list	Clears counters for IP prefix lists.
prefix-list	Applies a prefix list to BGP peer.
show ip prefix-list	Displays information about IP prefix lists.

ip prefix-list description

To configure a description string for an IP prefix list, use the **ip prefix-list description** command. To revert to default, use the **no** form of this command.

ip prefix-list *name* **description** *string*

no ip prefix-list *name* **description**

Syntax Description

name	Name of the prefix list. The name can be any alphanumeric string up to 63 characters.
string	Descriptive string for the prefix list. The string can be any alphanumeric string up to 90 characters.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to configure a description for an IP prefix list:

```
switch# configure terminal
switch(config)# ip prefix-list test1 description "this is a test"
switch(config)#
```

Related Commands

Command	Description
show ip prefix-list	Displays information about IPv4 prefix lists.