D Commands

- deny, page 2

deny

To prevent traffic from a source IP address to a destination IP address, use the **deny** command. To remove a deny rule, if any, use the **no** form of this command.

[*sequence-number*] **deny ip** *source-address destination-address*

no *sequence-number*

Syntax Description

sequence-number	(Optional) Specifies the sequence number. The range is from 1–4294967295. The default is 10. **Note** The sequence number is not optional in the **no** form of the **deny** command.
source-address	Specifies the source IP address.
destination-address	Specifies the destination IP address.

Command Default

No rule is created on traffic.

Command Modes

ACL port configuration (config-port-acl)

Command History

Release	Modification
Cisco NX-OS 8.2(1)	This command was introduced.

Usage Guidelines

Catena must be enabled and configured before using this command. For more information about these tasks, see "Cisco Nexus 7000 Series Switches Configuration Guide: The Catena Solution."

Examples

This example shows how to deny traffic from a source IP address to a destination IP address:

```
switch(config)# catena port-acl pa1
switch(config-port-acl)# 2 deny ip host 0.0.0.0 host 10.0.0.1
```

Related Commands

Command	Description
catena	Creates a Catena instance.
catena port-acl	Configures an ACL port.

Command	Description
permit	Allows traffic from a source IP address to a destination IP address.