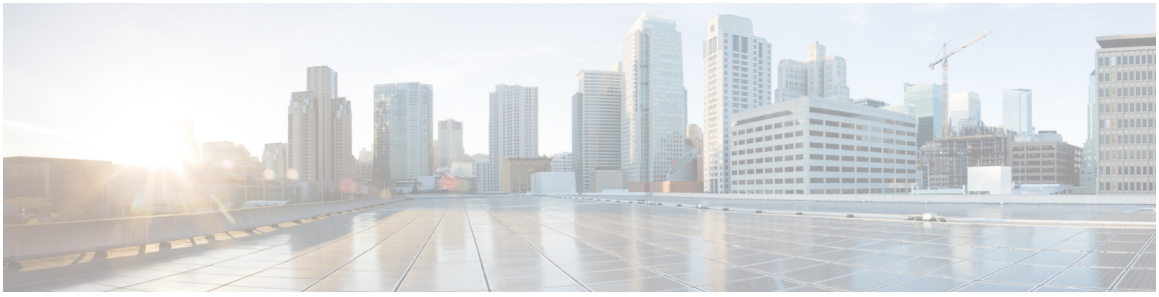
Cisco Nexus 7000 Series Switches Configuration Guide: The Catena Solution

First Published: 2016-12-21

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

Preface

This preface describes the audience, organization and conventions of the *Cisco Nexus 7000 Series NX-OS Catena Configuration Guide*. It also provides information on how to obtain related documentation.

Preface

This preface describes the audience, organization, and conventions of the Book Title. It also provides information on how to obtain related documentation.

This chapter includes the following topics:

Audience

This publication is for experienced network administrators who configure and maintain Cisco NX-OS on Cisco Nexus 7000 Series Platform switches.

Document Conventions

Note

- As part of our constant endeavor to remodel our documents to meet our customers' requirements, we have modified the manner in which we document configuration tasks. As a result of this, you may find a deviation in the style used to describe these tasks, with the newly included sections of the document following the new format.
- The Guidelines and Limitations section contains general guidelines and limitations that are applicable to all the features, and the feature-specific guidelines and limitations that are applicable only to the corresponding feature.

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.

Convention	Description
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

Documentation for Cisco Nexus 7000 Series Switches is available at:

- Configuration Guides

  http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-installation-and-configuration-guides-list.html

- Command Reference Guides

  http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-command-reference-list.html

- Release Notes

  http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-release-notes-list.html

- Install and Upgrade Guides

  http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-installation-guides-list.html

- Licensing Guide

  http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-licensing-information-listing.html

Documentation for Cisco Nexus 7000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders is available at the following URL:

http://www.cisco.com/c/en/us/support/switches/nexus-2000-series-fabric-extenders/products-installation-and-configuration-guides-list.html

Documentation Feedback

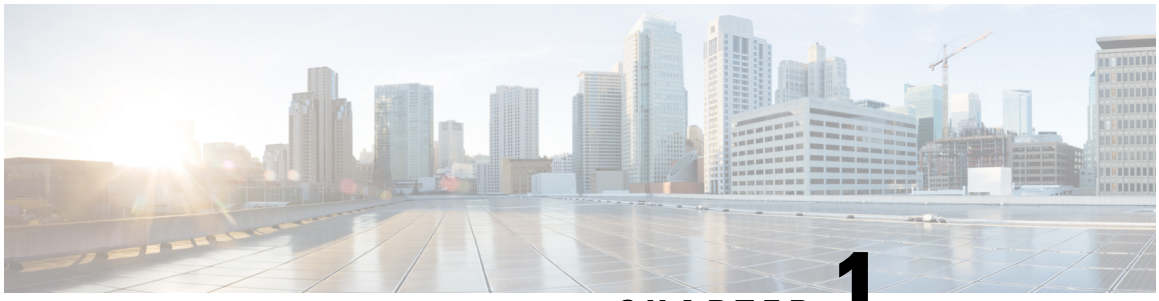
To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus7k-docfeedback@cisco.com. We appreciate your feedback.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



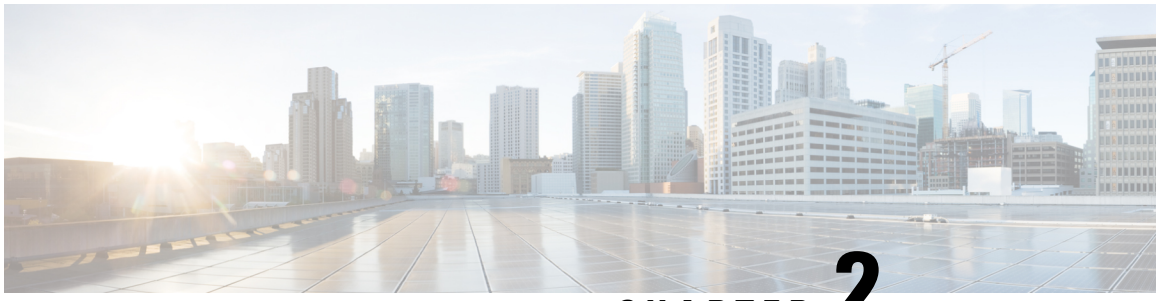
CHAPTER 1

New and Changed Information

The table below summarizes the new and changed information in this document, and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 1: New and Changed Catena Features

Feature Name	Description	Release	Where Documented
The Catena Solution	Introduced this feature. The following commands were introduced: • **access-list** • **catena** • **catena device-group** • **catena port-group** • **catena vlan-group** • **chain** • **feature catena** • **interface** • **node** • **probe** • **show catena** • **show running-config catena** • **vlan**	8.0(1)	Configuring the Catena Solution



CHAPTER 2

Configuring the Catena Solution

This chapter describes how to configure Catena, which is a hardware-based application chaining solution for Cisco Nexus devices.

Licensing Requirements

For a complete explanation of Cisco NX-OS licensing recommendations and how to obtain and apply licenses, see the *Cisco NX-OS Licensing Guide*.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the New and Changed Information chapter or the Feature History table below.

Feature History for Catena

Feature Name	Release	Feature Information
Catena Solution	8.0(1)	This feature was introduced.

Information About Catena

Catena is a multi-terabit security, chaining, load-balancing, analytics and L4-L7 applications integration solution, natively on the switch or router. Catena provides a hardware-based application chaining solution for Cisco Nexus devices so that packets can be redirected through multiple physical or virtual devices without changing the topology or the existing configuration. The solution works with all L4-L7 virtual and physical devices, such as firewall, IPS, IDS, DOS Protection, WAAS, SSL offload engines, networking monitoring devices, switches, virtual appliances, and containers.

Catena Feature Overview

Catena allows users to create multiple chains with multiple elements in each chain. Users can configure security policies to specify which segments of traffic go through which chain. An element could be a cluster of devices, in which case, catena load balances to the cluster. Catena performs health monitoring and failure handling of devices, along with sophisticated analytics.

The catena solution is natively embedded in the switch or router; therefore, you don't need to buy any service module or external hardware.

Some of the key features of Catena are as follows:

Note Catena supports IPv4 and IPv6 addresses.

- Supports full ACL including source IP, destination IP, source L4 port number, and destination L4 port number.
- Enables wire-speed performance.
- Provides hardware independence.
- Adds zero-latency to traffic.
- Allows you to insert additional appliances without disrupting existing device architecture or making complex changes to the wiring.
- Deploys appliances with the zero-touch feature. Catena does not need special header or data path packet modification. It is compatible with your existing hardware and software. It accepts standard space packets and does not require special tunneling, or headers. As a result, any appliance works without any special certification or support from the vendor.
- Provides per-segment telemetry and analytics at different points in the network.
- Does not place any additional load on the supervisor because the hardware handles all the packets.
- Provides selective traffic segmentation and chaining using ACLs. For example, any traffic entering at the ingress port is matched against your ACL and if the traffic matches your ACL, it is ingested into the appropriate traffic chain.
- Redirects line-rate traffic to multiple appliances.
- Monitors the health of devices using PING (ICMP), TCP, UDP, or DNS probes. Catena sends periodic probe packets to all the appliances. When an appliance responds in a healthy manner within a specified

time, it is used to load balance the traffic. Catena also handles automatic failure. Note that at the time of failure, you do not need to intervene.

Benefits of Catena

Catena offers a range of features for chaining devices without affecting the existing topology or configuration. Some of the key benefits of catena are as follows:

- Segmentation of traffic.
- User can select the traffic to be chained via ACLs.
- No dependency on Nexus hardware architecture; independent of line card types, ASICs, or Nexus switch types.
- No proprietary packet headers.
- User does not have to buy any service module or specialized hardware.
- CAPEX savings.
- OPEX savings: Without catena, the user has to do VLAN stitching or create a default gateway, which is very hard to deploy; it is hard to add or remove devices.
- Telemetry and analytics.
- Without catena, all traffic is either in a chain or not in a chain. Catena allows partitioning of traffic securely through multiple chains.
- Without catena, the user cannot create multiple chains using the same network elements.
- Catena is also a platform, for which users can write applications.

Enabling Chaining with Catena

You can create multiple chains, each comprising multiple functions and services; configure each chain to run on multiple devices; and apply network policies to these elements.You can create two types of chains:

- Transparent mode: This is a Layer 2 chain, where the appliances are directly connected to the Nexus switch.
- Routed mode: This is a Layer 3 chain, where the appliances are connected to each other through the Nexus switch.

If you create an appliance cluster, then the traffic is equally distributed to these appliances.

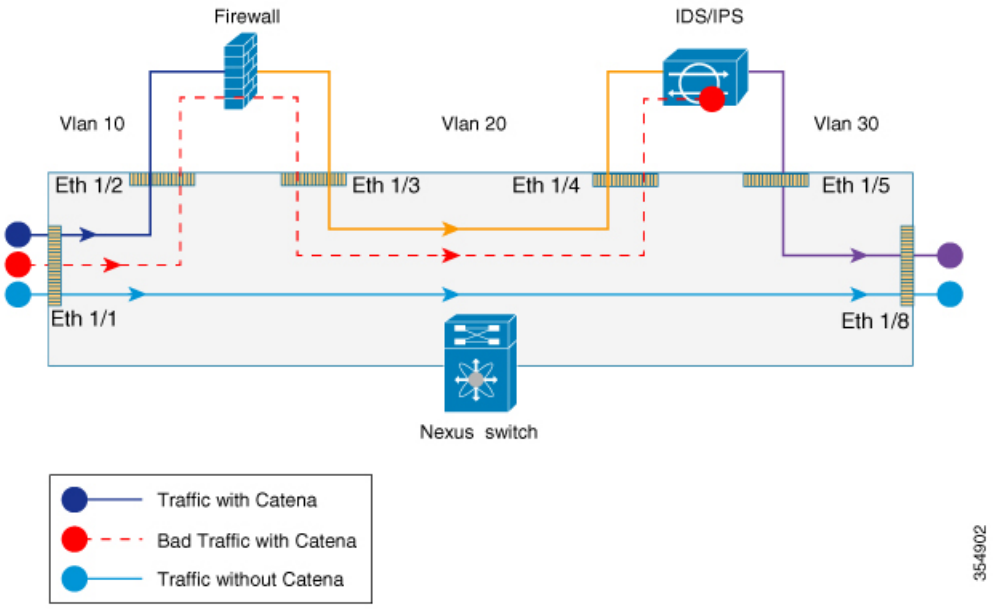
Deployment Modes

This section describes the various modes in which the Catena solution can be deployed.

Transparent Mode

Figure 1: Transparent Mode shows the traffic flow between appliances in the transparent mode when Catena is enabled, enabled with bad traffic, and disabled. Any traffic that is not secured and is expected to be blocked by the firewall is bad traffic.

Figure 1: Transparent Mode



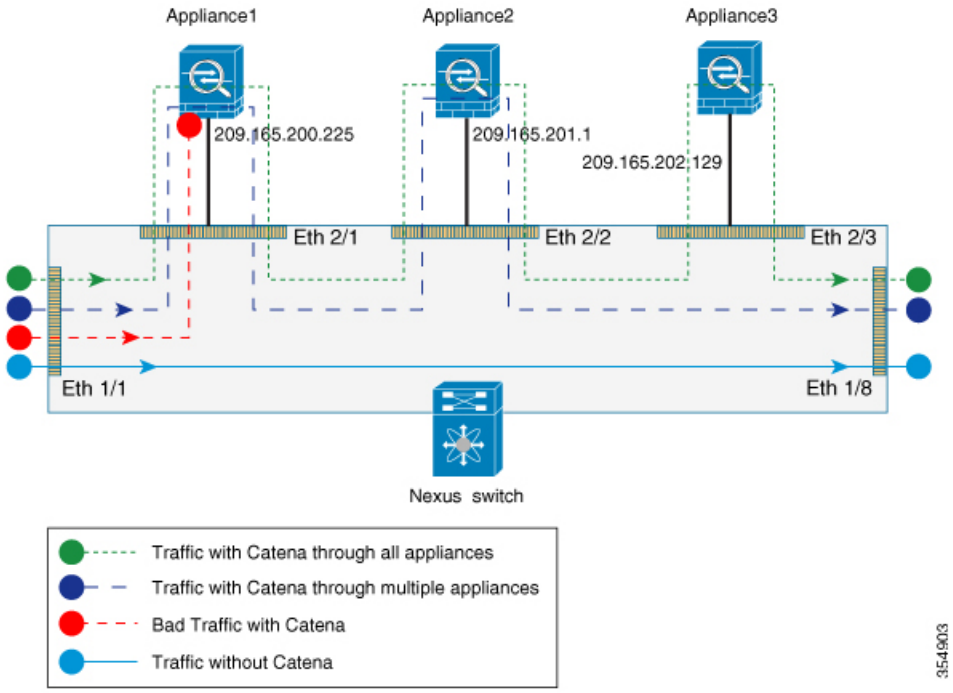
Hash-based Load Balancing

Catena uses source IP or destination IP to determine the egress interface. Egress interface ports are bundled using the link aggregation control protocol (LACP), and hash algorithms are used for symmetric load balancing.

Routed Mode

Figure 2: Routed Mode shows the traffic flow between appliances in the routed mode when Catena is enabled, enabled with bad traffic, and disabled.

Figure 2: Routed Mode



Configuring the Catena Solution

You can configure Cisco Nexus devices such that packets can be redirected through multiple devices using Catena.

Enabling or Disabling the Catena Solution

By default, Catena is disabled on the Cisco NX-OS device. You must explicitly enable Catena to configure and verify the authentication commands.

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Enable the Catena feature:

switch(config)# **feature catena**

Step 3 (Optional) Disable the Catena feature. When you disable catena, all related configurations are automatically discarded:

switch(config)# **no feature catena**

Step 4 (Optional) Copy the running configuration to the start up configuration:

switch(config)# **copy running config startup-config**

Configuring a Port Group

A port group consists of a set of interfaces. You must configure port groups if you plan to connect to transparent nodes or Layer 2 devices, such as load balancers.

Execute this command in the configuration mode to create or delete a port group.

Note If the egress port has multiple ports, then traffic is load balanced.

Before you begin

Enable the Catena solution. For details about how to enable this, see "Enabling or Disabling the Catena Solution."

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Create a port group and enter port group configuration mode:

switch(config)# **catena port-group** *port-group-name*

Step 3 Assign interface to the configured port group (repeat this step to specify all the interfaces):

switch(config-port-group)# **interface** *interface-reference*

Step 4 Configure load balancing using the hash-based method:

switch(config-port-group)# **load-balance port-channel**

Step 5 (Optional) Copy the running configuration to the start up configuration:

switch(config)# **copy running config startup-config**

Configuring a VLAN Group

Before you begin

Enable the Catena solution. For details about how to enable this, see "Enabling or Disabling the Catena Solution."

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Create a VLAN group and enter VLAN group configuration mode:

switch(config)# **catena vlan-group** *vlan-group-name*

Step 3 Assign VLAN to the configured VLAN group (repeat this step to specify all VLANs):

switch(config-vlan-group)# **vlan** *vlan-range*

Configuring a Device Group

A device group contains a list of node IP addresses. If you are creating a Layer 3 routed mode deployment you must create a device group.

Execute this command in the CLI config mode to create or delete a device group.

Note If there are multiple nodes, then traffic is load balanced accordingly.

Before you begin

Enable the Catena solution. For details about how to enable this, see "Enabling or Disabling the Catena Solution."

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Create a device group and enter device-group configuration mode:

switch(config)# **catena device-group** *device-group-name*

Step 3 Assign nodes to the configured device group:

switch(config-device-group)# **node** {**ip** *ipv4-address* | **IPv6** *ipv6-address*}

Step 4 Configure the device group probe:

switch(config-device-group)# **probe** *probe-id* [**control** *status*] [**host** *host-name*] [**frequency** *frequency-number* | **timeout** *timeout* | **retry-down-count** *down-count* | **retry-up-count** *up-count* | **ip** *ipv4-address*]

You can specify Internet Control Message Protocol (ICMP), TCP, UDP, or Domain Name System (DNS) protocol as the probe for the Catena instance.

Descriptions for some of the keyword-argument pairs are provided below:

- **control** *status*—Specifies the control protocol status.
- **frequency** *frequency-number*—Specifies the time interval, in seconds, between successive probes sent to the node.
- **timeout** *timeout*—Specifies the number of seconds to wait for the probe's response.
- **retry-down-count** *down-count*—Specifies the consecutive number of times the probe must have failed prior to the node being marked as DOWN.
- **retry-up-count** *up-count*—Specifies the consecutive number of times the probe must have succeeded prior to the node being marked as UP.

Note IPv6, TCP, UDP, and HTTP probes are not supported.

Configuring an IP ACL

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Create the IP ACL and enter IP ACL configuration mode:

switch(config)# **ip access-list** *acl-name*

The *acl-name* argument can be up to 64 characters in length.

Step 3 Create a rule in the IP ACL:

switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination*

You can create many rules. The *sequence-number* range is from 1 and 4294967295. The **permit** and **deny** keywords support different ways of identifying traffic.

Configuring a Port ACL

Port ACLs (PACLs) are used as filters in transparent mode. They are used to seggregate IP traffic for transparent mode PACL. The traffic is redirected to a particular egress interface based on the access control entries (ACE).

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Enable the feature catena:

switch(config)# **feature catena**

Step 3 Configure catena port ACL:

switch(config)# **catena port-acl** *acl-name*

Step 4 Configure the sequence list:

switch(config-port-acl)# [*sequence-number*] {**deny | permit**} **ip** *source-address destination-address*

Configuring a Catena Instance

Before you begin

1. Enable the Catena solution. For details about how to enable this, see "Enabling or Disabling the Catena Solution."
2. Configure the port group, VLAN group, device group, and access control list for the Catena instance. For details about how to enable these respectively, see "Configuring a Port Group", "Configuring a VLAN Group", "Configuring a Device Group", and "Configuring an IP ACL".

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Create a Catena instance and enter Catena instance configuration mode:

switch(config)# **catena** *instance-name*

Step 3 Create a chain ID:

switch(config-catena-instance)# **chain** *chain-id*

Step 4 Configure the sequence list:

switch(config-catena)# *sequence-number* **access-list** *acl-name* {**vlan-group** *vg-name* | **ingress-port-group** *ipg-name*} {**egress-port-group** *epg-name* | **egress-device-group** *edg-name*} [**mode** *mode*]

Descriptions for some of the keyword-argument pairs are provided below:

- *sequence-number*—Specifies the sequence number.
- **access-list** *acl-name*—Specifies the access list.
- **vlan-group** *vg-name*—Specifies the VLAN group.
- **ingress-port-group** *ipg-name*—Specifies the ingress port group.
- **egress-port-group** *epg-name*—Specifies the egress port group.

- **egress-device-group** *edg-name*—Specifies the egress device group.
- **mode** *mode*—Specifies the mode types—**drop**, **bypass**, or **forward**—for the received packets.

Currently, you must configure separate instances for Layer 2 and Layer 3 modes. A catena instance can comprise multiple chains that are independent of each other. The traffic in each chain is forwarded as defined. However, if there is an overlap between packets from different chains at the ingress port, then all the chains configured on that ingress interface will be evaluated. If a match is found on the ingress interface, then the matching chain is accepted and forwarded.

Enabling a Catena Instance

Before you begin

1. Enable the Catena solution. For details about how to enable this, see "Enabling or Disabling the Catena Solution."
2. Configure the Catena instance. For details about how to enable this, see "Configuring a Catena Instance."
3. In the routed mode deployment, you must run the following commands before enabling the Catena instance:
   - **feature pbr**
   - **feature sla sender**
   - **feature sla responder**

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Create a Catena instance and enter Catena instance configuration mode:

switch(config)# **catena** *instance-name*

Step 3 Enable the Catena instance:

switch(config-catena-instance)# **no shutdown**

Verifying the Catena Configuration

To verify the Catena configuration, use one of the following commands:

Table 2: Verifying the Catena Configuration

Command	Purpose
show catena *instance-name* **brief**	Displays the status and configuration for the specified Catena instance. • Use the *instance-name* argument to display the status and configuration for the specified instance. • Use the **brief** keyword to display the summary status and configuration information.
show running-config catena	Displays the running Catena configuration.

Configuration Examples for Catena

This example shows how to enable Catena:

```
switch# configure terminal
switch(config)# feature catena
```

This example shows how to configure a port group:

```
switch# configure terminal
switch(config)# catena port-group pg1
switch(config-port-group)# interface Eth 2/2
switch(config-port-group)# interface Eth 2/3
```

This example shows how to configure a VLAN group:

```
switch# configure terminal
switch(config)# catena vlan-group vg1
switch(config-vlan-group)# vlan 10
switch(config-vlan-group)# vlan 20-30
switch(config-vlan-group)# vlan 40,50
```

This example shows how to configure a device group:

```
switch# configure terminal
switch(config)# catena device-group s-dg-1
switch(config-device-group)# node ip 209.165.200.225/27
switch(config-device-group)# node ip 209.165.201.1/27
switch(config-device-group)# probe icmp
```

This example shows how to configure an instance:

```
switch# configure terminal
switch(config)# catena ins1
switch(config-catena-instance)#
```

This example shows how to configure chains and sequence lists:

```
switch# configure terminal
switch(config)# catena ins1
switch(config-catena-instance)# chain 10
switch(config-catena)# 10 access-list acl11 vlan-group vg1 egress-port-group pg1 mode forward
switch(config-catena)# catena ins2
switch(config-catena-instance)# chain 20
```

```
switch(config-catena)# 20 access-list acl12 ingress-port-group pg1 egress-device-group
s-dg-1 mode forward
```

This example shows the full ACL support including source IP, destination IP, source L4 port number, and destination L4 port number.

```
switch# show ip access-lists test1
IP access list test1
        10 permit ip 10.1.1.1/24 any
        20 permit tcp 10.2.1.1/24 eq 1034 172.16.0.1/24 eq 3456
        30 permit udp 10.3.1.1/24 eq 2345 192.168.0.1/24 eq 2134
switch# show run catena
feature catena

catena port-group pg1
 int eth1/4

catena device-group dg1
 node ip 1.1.1.2

catena ins1
 chain 10
  10 access-list test1 ingress-port-group pg1 egress-device-group dg1 mode forward
 no shutdown
```

Configuration Example for Catena—Transparent Mode VACL

This example shows how to configure Catena in transparent mode:

```
switch# configure terminal
switch(config)# feature catena
switch(config)# catena port-group pg1
switch(config-port-group)# interface Eth 1/2
switch(config-pg-node)# catena port-group pg2
switch(config-port-group)# interface Eth 1/4
switch(config-pg-node)# catena vlan-group vg1
switch(config-vlan-group)# vlan 10
switch(config-vlan-group)# catena vlan-group vg2
switch(config-vlan-group)# vlan 20
switch(config)# ip access-list acl1
switch(config-acl)# 10 permit ip 192.0.2.1/24 any
switch(config)# ip access-list acl2
switch(config-acl)# 10 permit ip 198.51.100.1/24 any
switch(config)# ip access-list acl3
switch(config-acl)# 10 permit ip 203.0.113.1/24 any
switch(config-acl)# exit
switch(config)# catena ins_redirect
switch(config-catena-instance)# chain 10
switch(config-catena)# 10 access-list acl1 vlan-group vg1 egress port-group pg1 mode forward
switch(config-catena)# 20 access-list acl1 vlan-group vg2 egress port-group pg2 mode forward
switch(config-catena)# no shutdown
switch(config-catena-)# catena ins_bypass
switch(config-catena-instance)# chain 10
switch(config-catena)#10 access-list acl2 vlan-group vg1 egress port-group pg1 mode bypass
switch(config-catena)# no shutdown
switch(config-catena-)# catena ins_drop
switch(config-catena-instance)# chain 10
switch(config-catena)#10 access-list acl3 vlan-group vg1 egress port-group pg1 mode forward
switch(config-catena)#20 access-list acl3 vlan-group vg1 egress port-group pg1 mode drop
switch(config-catena)# no shutdown
```

```
switch# show running-config catena

feature catena

catena vlan-group vg1
vlan 10

catena vlan-group vg2
vlan 20

catena port-group pg1
interface Eth1/2

catena port-group pg2
interface Eth1/4

catena ins_redirect
chain 10
10 access-list acl1 vlan-group vg1 egress-port-group pg1 mode forward
20 access-list acl1 vlan-group vg2 egress-port-group pg2 mode forward
no shutdown

catena ins_bypass
chain 10
10 access-list acl2 vlan-group vg1 egress-port-group pg1 mode bypass
no shutdown

catena ins_drop
chain 10
10 access-list acl3 vlan-group vg1 egress-port-group pg1 mode forward
20 access-list acl3 vlan-group vg2 egress-port-group pg2 mode drop
no shutdown
```

Configuration Example for Catena—Transparent Mode PACL

This example shows how to configure Catena in transparent mode:

```
switch# configure terminal
switch(config)# feature catena
switch(config)# catena port-group pg1
switch(config-port-group)# interface Eth 1/1
switch(config-pg-node)# catena port-group pg2
switch(config-port-group)# interface Eth 1/2
switch(config-pg-node)# catena port-group pg3
switch(config-port-group)# interface Eth 1/3
switch(config-pg-node)# catena port-group pg4
switch(config-port-group)# interface Eth 1/4
switch(config-pg-node)# catena port-acl acl1
switch(config-port-acl)# 10 permit ip 192.0.2.1/24 any
switch(config-port-acl)# 20 deny ip 198.51.100.1/24 any
switch(config-port-acl)# catena ins_1
switch(config-catena-instance)# chain 10
switch(config-catena)# 10 access-list acl1 ingress-port-group pg1 egress port-group pg2
mode forward
switch(config-catena)# 20 access-list acl1 ingress-port-group pg3 egress port-group pg4
mode forward
switch(config-catena)# no shutdown

switch# show running-config catena

feature catena

catena port-acl acl1
```

```
  10 permit ip 192.0.2.1/24 any
  20 deny ip 198.51.100.1/24 any

catena port-group pg1
  interface Eth1/1

catena port-group pg2
  interface Eth1/2

catena port-group pg3
  interface Eth1/3

catena port-group pg4
  interface Eth1/4

catena ins1
  chain 10
    10 access-list acl1 ingress-port-group pg1 egress-port-group pg2 mode forward
    20 access-list acl1 ingress-port-group pg3 egress-port-group pg4 mode forward
  no shutdown
```

Configuration Example for Catena—Hash-based Load Balancing

This example shows how to configure hash-based load balancing:

```
switch# configure terminal
switch(config)# feature catena
switch(config)# catena port-group pg1
switch(config-port-group)# interface Ethernet 1/2
switch(config-pg-node)# interface Ethernet 1/3
switch(config-pg-node)# load-balance port-channel
switch(config-port-group)# exit
switch(config)# catena port-group pg2
switch(config-port-group)# interface Ethernet 1/6
switch(config-pg-node)# interface Ethernet 1/7
switch(config-pg-node)# load-balance port-channel
switch(config-port-group)# catena vlan-group vg1
switch(config-vlan-group)# vlan 10
switch(config-vlan-group)# catena vlan-group vg2
switch(config-vlan-group)# vlan 20
switch(config-vlan-group)#)# ip access-list acl1
switch(config-acl)# 10 permit ip 192.0.2.1/24 any
switch(config-acl)# ip access-list acl2
switch(config-acl)# 10 permit ip 198.51.100.1/24
switch(config-acl)# ip access-list acl3
switch(config-acl)# 10 permit ip 203.0.113.1/24
switch(config-acl)# catena ins_redirect
switch(config-catena-instance)# chain 10
switch(config-catena)# chain 10
switch(config-catena)#10 access-list acl1 vlan-group vg1 egress-port-group pg1 mode forward
switch(config-catena)# 10 access-list acl1 vlan-group vg2 egress-port-group pg2 mode forward
switch(config-catena-)# no shutdown
switch(config-catena-instance)# chain 10
switch(config-catena)#10 access-list acl3 vlan-group vg1 egress port-group pg1 mode forward
switch(config-catena)#20 access-list acl3 vlan-group vg1 egress port-group pg1 mode drop
switch(config-catena)# no shutdown
switch(config-catena-instance)# catena ins_bypass
switch(config-catena-instance)# chain 10
switch(config-catena)#10 access-list acl2 vlan-group vg1 egress port-group pg1 mode bypass
switch(config-catena)#no shutdown
switch(config-catena-instance)# catena ins_drop
switch(config-catena-instance)# chain 10
```

```
switch(config-catena)#10 access-list acl3 vlan-group vg1 egress port-group pg1 mode drop
switch(config-catena)#no shutdown

switch# show running-config catena

feature catena

catena vlan-group vg1
vlan 10

catena vlan-group vg2
vlan 20

catena port-group pg1
interface Eth1/1
interface Eth1/2
load-balance port-channel

catena port-group pg2
interface Eth1/6
intergace Eth1/7
load-balance port-channel

catena ins_redirect
chain 10
10 access-list acl1 vlan-group vg1 egress-port-group pg1 mode forward
20 access-list acl1 vlan-group vg2 egress-port-group pg2 mode forward
no shutdown

catena ins_bypass
chain 10
10 access-list acl2 vlan-group vg1 egress-port-group pg1 mode bypass
no shutdown

catena ins_drop
chain 10
10 access-list acl3 vlan-group vg1 egress-port-group pg1 mode forward
no shutdown
```

Configuration Example for Catena—Routed Mode

This example shows how to configure Catena in routed mode:

```
switch# configure terminal
switch(config)# feature catena
switch(config)# catena port-group pg1
switch(config-port-group)# interface Eth 1/1
switch(config-pg-node)# catena port-group pg2
switch(config-port-group)# interface Eth 2/1
switch(config-pg-node)# catena port-group pg3
switch(config-port-group)# interface Eth 2/2
switch(config-pg-node)# catena device-group dg1
switch(config-device-group)# node ip 209.165.200.225/27
switch(config-device-group)# probe icmp
switch(config-device-group)# catena device-group dg2
switch(config-device-group)# node ip 209.165.201.1/27
switch(config-device-group)# probe icmp
switch(config-device-group)# catena device-group dg3
switch(config-device-group)# node ip 209.165.202.129/27
switch(config-device-group)# probe icmp
switch(config-device-group)# ip access-list acl1
switch(config-acl)# 10 permit ip 192.0.2.1/24 any
switch(config)# ip access-list acl2
```

```
switch(config-acl)# 10 permit ip 198.51.100.1/24 any
switch(config-acl)# ip access-list acl3
switch(config-acl)# 10 permit ip 203.0.113.1/24 any
switch(config-acl)# ip access-list acl4
switch(config-acl)# 10 permit ip 10.0.0.1/8 any
switch(config)# catena ins_1
switch(config-catena-instance)# chain 10
switch(config-catena)# 10 access-list acl1 ingress-port-group pg1 egress-device-group dg1
mode forward
switch(config-catena)# 20 access-list acl1 ingress-port-group pg2 egress-device-group dg2
mode forward
switch(config-catena)# 30 access-list acl1 ingress-port-group pg3 egress-device-group dg3
mode forward
switch(config-catena)# no shutdown
switch(config-catena-instance)# catena ins_2
switch(config-catena-instance)# chain 10
switch(config-catena)# 10 access-list acl2 ingress-port-group pg1 egress-device-group dg1
mode forward
switch(config-catena)# 20 access-list acl2 ingress-port-group pg2 egress-device-group dg2
mode forward
switch(config-catena)# no shutdown
```

```
Switch#show running-config catena

feature catena

catena device-group dg1
  node ip 209.165.200.225/27
catena device-group dg2
  node ip 209.165.201.1/27
catena device-group dg3
  node ip 209.165.202.129/27

catena port-group pg1
  interface Eth1/1
catena port-group pg2
  interface Eth2/1
catena port-group pg3
  interface Eth3/1

catena ins1
  chain 10
    10 access-list acl1 ingress-port-group pg1 egress-device-group dg1 mode forward
    20 access-list acl1 ingress-port-group pg2 egress-device-group dg2 mode forward
    30 access-list acl1 ingress-port-group pg3 egress-device-group dg3 mode forward
  no shutdown

catena ins2
  chain 10
    10 access-list acl2 ingress-port-group pg1 egress-device-group dg1 mode forward
    20 access-list acl2 ingress-port-group pg2 egress-device-group dg2 mode forward
  no shutdown
```

Verifying Configuration Examples for Catena

The following examples show how to verify a Catena configuration:

```
switch# show running-config catena
catena vlan-group vg1
  vlan 10

catena vlan-group vg2
```

```
  vlan 20

catena port-group pg1
  interface Eth1/2

catena port-group pg2
  interface Eth1/4

catena ins_redirect
  chain 10
    10 access-list acl1 vlan-group vg1 egress-port-group pg1 mode forward
    20 access-list acl1 vlan-group vg2 egress-port-group pg2 mode forward
    no shutdown
catena ins_bypass
  chain 10
    10 access-list acl2 vlan-group vg1 egress-port-group pg1 mode bypass
    no shutdown
catena ins_drop
  chain 10
    10 access-list acl3 vlan-group vg1 egress-port-group pg1 mode forward
    20 access-list acl3 vlan-group vg2 egress-port-group pg2 mode drop
    no shutdown
```

```
switch# show running-config catena
feature catena
catena device-group dg1
  node ip 192.0.2.1/24
catena device-group dg2
  node ip 198.51.100.1/24
catena device-group dg3
  node ip 203.0.113.1/24
catena port-group pg1
  interface Eth1/1
catena port-group pg2
  interface Eth2/1
catena port-group pg3
  interface Eth3/1
catena ins1
  chain 10
    10 access-list acl1 ingress-port-group pg1 egress-device-group dg1 mode forward
    20 access-list acl1 ingress-port-group pg2 egress-device-group dg2 mode forward
    30 access-list acl1 ingress-port-group pg3 egress-device-group dg3 mode forward
    no shutdown
catena ins2
  chain 10
    10 access-list acl2 ingress-port-group pg1 egress-device-group dg1 mode forward
    20 access-list acl2 ingress-port-group pg2 egress-device-group dg2 mode forward
    no shutdown
```

```
switch# show catena ins1
-----------------------------------
Instance name                Status
-------------------       ---------
ins1                         ACTIVE
-----------------------------------


chain 10
-------------------------------------------------------------------------------
sequence no     access-list  ingress-port-group  egress-device-group       mode
-------------------------------------------------------------------------------
         10            acl1                 pg1                  dg1    forward
         20            acl1                 pg2                  dg2    forward
         30            acl1                 pg3                  dg3    forward
```

Related Documents for Catena

Table 3: Related Documents for Catena

Related Topic	Document Title
Catena commands	Cisco Nexus 7000 Series Command Reference: The Catena Solution