



Inspur

*CN12900 Series*

INOS-CN System Management Configuration  
Guide



**Inspur-Cisco Networking Technology Co.,Ltd.** provides customers with comprehensive technical support and services. For any assistance, please contact our local office or company headquarters.

Website: <http://www.inspur.com/>

Technical Support Tel: 400-691-1766

Technical Support Email: [icnt\\_service@inspur.com](mailto:icnt_service@inspur.com)

Technical Document Support Email: [icnt\\_service@inspur.com](mailto:icnt_service@inspur.com)

Address: 1036 Langchao Road, Lixia District, Jinan City, Shandong Province

Postal code: 250101

---

## Notice

Copyright © 2020

Inspur Group.

All rights reserved.

No part of this publication may be excerpted, reproduced, translated or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in Writing from **Inspur-Cisco Networking Technology Co.,Ltd.**

**inspur** 浪潮

is the trademark of **Inspur-Cisco Networking Technology Co.,Ltd.**

All other trademarks and trade names mentioned in this document are the property of their respective holders.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied

# Preface

---

## Objectives

This guide describes main functions of the CN12900 Series. To have a quick grasp of the CN12900 Series, please read this manual carefully.

## Versions





The following table lists the product versions related to this document.

Product name	Version
CN12900 Series	

## Conventions

### Symbol conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 <b>Warning</b>	Indicates a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
 <b>Caution</b>	Indicates a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.
 <b>Note</b>	Provides additional information to emphasize or supplement important points of the main text.
 <b>Tip</b>	Indicates a tip that may help you solve a problem or save time.

## General conventions

Convention	Description
Boldface	Names of files, directories, folders, and users are in <b>boldface</b> . For example, log in as user <b>root</b> .
Italic	Book titles are in <i>italics</i> .
Lucida Console	Terminal display is in <code>Lucida Console</code> .

## Command conventions

Convention	Description
Boldface	The keywords of a command line are in <b>boldface</b> .
Italic	Command arguments are in <i>italics</i> .
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x   y   ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[ x   y   ... ]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x   y   ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[ x   y   ... ] *	The parameter before the & sign can be repeated 1 to n times.

## GUI conventions

Convention	Description
Boldface	Buttons, menus, parameters, tabs, windows, and dialog titles are in <b>boldface</b> . For example, click <b>OK</b> .
>	Multi-level menus are in boldface and separated by the ">" signs. For example, choose <b>File &gt; Create &gt; Folder</b> .

## Keyboard operation

Format	Description
Key	Press the key. For example, press <b>Enter</b> and press <b>Tab</b> .

Format	Description
Key 1+Key 2	Press the keys concurrently. For example, pressing <b>Ctrl+C</b> means the two keys should be pressed concurrently.
Key 1, Key 2	Press the keys in turn. For example, pressing <b>Alt, A</b> means the two keys should be pressed in turn.

## Mouse operation

Action	Description
Click	Select and release the primary mouse button without moving the pointer.
Double-click	Press the primary mouse button twice continuously and quickly without moving the pointer.
Drag	Press and hold the primary mouse button and move the pointer to a certain position.

## Change history

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

### Issue 01 (2020-02-24)

Initial commercial release

# Contents

---

<b>CHAPTER 1 New and Changed Information.....</b>	<b>1</b>
1.1 New and Changed Information.....	1
<b>CHAPTER 2 Overview.....</b>	<b>2</b>
2.1 Software Image.....	2
2.2 Precision Time Protocol.....	2
2.3 Cisco Discovery Protocol.....	2
2.4 System Messages.....	2
2.5 Rollback.....	2
2.6 Session Manager.....	3
2.7 SNMP.....	3
2.8 SPAN.....	3
2.9 ERSPAN.....	3
2.10 LLDP.....	3
2.11 sFlow.....	3
2.12 Troubleshooting Features.....	3
<b>CHAPTER 3 Configuring PTP.....</b>	<b>5</b>
3.1 About PTP.....	5
3.2 Licensing Requirements for PTP.....	7
3.3 Guidelines and Limitations for PTP.....	7
3.4 Default Settings for PTP.....	8
3.5 Configuring PTP.....	8
3.6 Verifying the PTP Configuration.....	15
3.7 Configuration Examples for PTP.....	15
3.8 Additional References.....	17
<b>CHAPTER 4 Configuring CDP.....</b>	<b>18</b>
4.1 About CDP.....	18
4.2 Licensing Requirements for CDP.....	19
4.3 Guidelines and Limitations for CDP.....	19

---

4.4 Default Settings for CDP.....	19
4.5 Configuring CDP.....	19
4.6 Verifying the CDP Configuration.....	21
4.7 Configuration Example for CDP.....	22
<b>CHAPTER 5 Configuring SNMP.....</b>	<b>23</b>
5.1 About SNMP.....	23
5.2 Licensing Requirements for SNMP.....	27
5.3 Guidelines and Limitations for SNMP.....	27
5.4 Default Settings for SNMP.....	27
5.5 Configuring SNMP.....	28
5.6 Configuring the SNMP Local Engine ID.....	47
5.7 Verifying SNMP Configuration.....	48
5.8 Configuration Examples for SNMP.....	49
5.9 Additional References.....	50
<b>CHAPTER 6 Configuring SPAN.....</b>	<b>51</b>
6.1 About SPAN.....	51
6.2 Licensing Requirements for SPAN.....	52
6.3 Prerequisites for SPAN.....	52
6.4 Guidelines and Limitations for SPAN.....	52
6.5 Default Settings for SPAN.....	54
6.6 Configuring SPAN.....	54
6.7 Verifying the SPAN Configuration.....	61
6.8 Configuration Examples for SPAN.....	62
6.9 Additional References.....	65
<b>CHAPTER 7 Configuring ERSPAN.....</b>	<b>66</b>
7.1 About ERSPAN.....	66
7.2 Licensing Requirements for ERSPAN.....	67
7.3 Prerequisites for ERSPAN.....	67
7.4 Guidelines and Limitations for ERSPAN.....	67
7.5 Default Settings.....	68
7.6 Configuring ERSPAN.....	68

---

7.7 Verifying the ERSPAN Configuration.....	80
7.8 Configuration Examples for ERSPAN.....	80
7.9 Additional References.....	83
<b>CHAPTER 8 Configuring LLDP.....</b>	<b>84</b>
8.1 About LLDP.....	84
8.2 Licensing Requirements for LLDP.....	85
8.3 Guidelines and Limitations for LLDP.....	85
8.4 Default Settings for LLDP.....	85
8.5 Configuring LLDP.....	86
8.6 Verifying the LLDP Configuration.....	89
8.7 Configuration Example for LLDP.....	90
<b>CHAPTER 9 Configuring sFlow.....</b>	<b>91</b>
9.1 About sFlow.....	91
9.2 Licensing Requirements for sFlow.....	91
9.3 Guidelines and Limitations for sFlow.....	91
9.4 Default Settings for sFlow.....	92
9.5 Configuring sFlow.....	92
9.6 Verifying the sFlow Configuration.....	98
9.7 Monitoring and Clearing sFlow Statistics.....	99
9.8 Configuration Examples for sFlow.....	99
9.9 Additional References.....	99
<b>CHAPTER 10 Configuring Graceful Insertion and Removal.....</b>	<b>100</b>
10.1 About Graceful Insertion and Removal.....	100
10.2 Licensing Requirements for GIR.....	101
10.3 Guidelines and Limitations for GIR.....	101
10.4 GIR Workflow.....	102
10.5 Configuring the Maintenance-Mode Profile.....	102
10.6 Configuring the Normal-Mode Profile.....	104
10.7 Creating a Snapshot.....	105
10.8 Adding Show Commands to Snapshots.....	107
10.9 Triggering Graceful Removal.....	109



---

10.10 Triggering Graceful Insertion.....	111
10.11 Maintenance Mode Enhancements.....	112
10.12 Verifying the GIR Configuration.....	113
10.13 Configuration Examples for GIR.....	114
<b>CHAPTER 11 Configuring Rollback.....</b>	<b>116</b>
11.1 About Rollbacks.....	116
11.2 Licensing Requirements for Rollbacks.....	117
11.3 Guidelines and Limitations for Rollbacks.....	117
11.4 Default Settings for Rollbacks.....	117
11.5 Configuring Rollbacks.....	118
11.6 Verifying the Rollback Configuration.....	119
11.7 Configuration Example for Rollback.....	119
11.8 Additional References.....	120

# Figure

---

*Figure 1 : SPAN Configuration..... 52*

# Table

---

<i>Table 1 : New and Changed Features for Inspur CN12900</i> .....	1
<i>Table 2 : Default PTP Parameters</i> .....	8
<i>Table 3 : PTP Show Commands</i> .....	15
<i>Table 4 : SNMP Security Models and Levels</i> .....	25
<i>Table 5 : Enabling SNMP Notifications</i> .....	36
<i>Table 6 : Default ERSPAN Parameters</i> .....	68
<i>Table 7 : Default sFlow Parameters</i> .....	92
<i>Table 8 : sFlow Show Commands</i> .....	99
<i>Table 9 : .....</i>	102

# CHAPTER 1 New and Changed Information

---

This chapter provides release-specific information for each new and changed feature in the *Inspur CN12900 Series INOS-CN System Management Configuration Guide*.

## 1.1 New and Changed Information

This *table* summarizes the new and changed features for the *Inspur CN12900 Series INOS-CN System Management Configuration Guide* and tells you where they are documented.

**Table 1: New and Changed Features for Inspur CN12900**

Feature	Description	Changed in	Where Documented
Checkpoint and Rollback	Introduced in F1(1)	N/A	
DCBX	Introduced in F1(1)	N/A	
ERSPAN	Introduced in F1(1)	N/A	
LLDP	Introduced in F1(1)	N/A	
Maintenance Mode (GIR)	Introduced in F1(1)	N/A	
PTP	Introduced in F3(3)	N/A	
gPTP	Introduced in 9.2(1i)	N/A	
sFlow	Introduced in F2(1)	N/A	
SNMP v2 and v3	Introduced in F1(1)	N/A	
SPAN	Introduced in F1(1)	N/A	
Span Sources	Introduced in F2(1)	N/A	

## CHAPTER 2 Overview

---

This chapter describes the system management features that you can use to monitor and manage Inspur INOS-CN devices.

This chapter contains the following sections:

### 2.1 Software Image

The Inspur INOS-CN software consists of one INOS-CN software image. This image runs on all Inspur CN12900 Series switches.

#### 2.1.1 Configuring with CLI

You can configure Inspur INOS-CN devices using the command-line interface (CLI) over Secure Shell (SSH) as follows:

- CLI from an SSH session, a Telnet session, or the console port—You can configure devices using the CLI from an SSH session, a Telnet session, or the console port. SSH provides a secure connection to the device. For more information, see the *Inspur CN12900 Series INOS-CN Fundamentals Configuration Guide*.

### 2.2 Precision Time Protocol

The Precision Time Protocol (PTP) is a time synchronization protocol for nodes distributed across a network. Its hardware timestamp feature provides greater accuracy than other time synchronization protocols such as Network Time Protocol (NTP).

### 2.3 Cisco Discovery Protocol

You can use the Cisco Discovery Protocol (CDP) to discover and view information about all Cisco equipment that is directly attached to your device. CDP runs on all Cisco-manufactured equipment including routers, bridges, access and communication servers, and switches. CDP is media and protocol independent, and gathers the protocol addresses of neighboring devices, discovering the platform of those devices. CDP runs over the data link layer only. Two systems that support different Layer 3 protocols can learn about each other.

### 2.4 System Messages

You can use system message logging to control the destination and to filter the severity level of messages that system processes generate. You can configure logging to a terminal session, a log file, and syslog servers on remote systems.

For more information about the system message format and the messages that the device generates, see the *Inspur INOS-CN System Messages Reference*.

### 2.5 Rollback

The rollback feature allows you to take a snapshot, or checkpoint, of the device configuration and then reapply that configuration at any point without having to reload. Rollback allows any authorized administrator to apply this checkpoint configuration without requiring expert knowledge of the features configured in the checkpoint.

Session Manager allows you to create a configuration session and apply all commands within that session atomically.

## 2.6 Session Manager

Session Manager allows you to create a configuration and apply it in batch mode after the configuration is reviewed and verified for accuracy and completeness.

## 2.7 SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

## 2.8 SPAN

You can configure an Ethernet Switched Port Analyzer (SPAN) to monitor traffic in and out of your device. The SPAN features allow you to duplicate packets from source ports to destination ports.

## 2.9 ERSPAN

Encapsulated Remote Switched Port Analyzer (ERSPAN) is used to transport mirrored traffic in an IP network. ERSPAN supports source ports, source VLANs, and destinations on different switches, which provide remote monitoring of multiple switches across your network.

To configure an ERSPAN source session, you associate a set of source ports or VLANs with a destination IP address, ERSPAN ID number, and virtual routing and forwarding (VRF) name.

## 2.10 LLDP

Link Layer Discovery Protocol (LLDP) is a vendor-neutral, one-way device discovery protocol that allows network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other. You can enable LLDP globally or per interface.

## 2.11 sFlow

Sampled flow (sFlow) allows you to monitor real-time traffic in data networks that contain switches and routers and to forward the sample data to a central data collector.

## 2.12 Troubleshooting Features

Inspur INOS-CN provides troubleshooting tools such as ping, traceroute, Ethalyzer, and the Blue Beacon feature.

When a service fails, the system generates information that can be used to determine the cause of the failure. The following sources of information are available:

- Every service restart generates a syslog message of level LOG\_ERR.
- If SNMP traps are enabled, the SNMP agent sends a trap when a service is restarted.

- When a service failure occurs on a local module, you can view a log of the event by entering the **show processes log** command in that module. The process logs are persistent across supervisor switchovers and resets.
- When a service fails, a system core image file is generated. You can view recent core images by entering the **show cores** command on the active supervisor. Core files are not persistent across supervisor switchovers and resets, but you can configure the system to export core files to an external server using the file transfer utility Trivial File Transfer Protocol (TFTP) by entering the **system cores** command. ICNT-SYSTEM-MIB contains a table for cores (cseSwCoresTable)

## CHAPTER 3 Configuring PTP

---

This chapter describes how to configure the Precision Time Protocol (PTP) on Inspur INOS-CN devices. This chapter includes the following sections:

### 3.1 About PTP

PTP is a time synchronization protocol defined in IEEE 1588 for nodes distributed across a network. With PTP, it is possible to synchronize distributed clocks with an accuracy of less than 1 microsecond via Ethernet networks. In addition, PTP's hardware timestamping feature provides timestamp information in the ERSPAN Type III header that can be used to calculate packet latency among edge, aggregate, and core switches.

A PTP system can consist of a combination of PTP and non-PTP devices. PTP devices include ordinary clocks, boundary clocks, and transparent clocks. Non-PTP devices include ordinary network switches, routers, and other infrastructure devices.

PTP is a distributed protocol that specifies how real-time PTP clocks in the system synchronize with each other. These clocks are organized into a master-slave synchronization hierarchy with the grandmaster clock, which is the clock at the top of the hierarchy, determining the reference time for the entire system. Synchronization is achieved by exchanging PTP timing messages, with the members using the timing information to adjust their clocks to the time of their master in the hierarchy. PTP operates within a logical scope called a PTP domain.

PTP supports the following functionality:

- Multicast and unicast PTP transport—In the multicast transport mode, PTP uses multicast destination IP address 224.0.1.129 as per IEEE 1588 standards for communication between devices. For the source IP address, it uses the user configurable global IP address under the PTP domain. In the unicast transport mode, PTP uses configurable unicast source and destination IP addresses that can be configured under an interface. In both, the unicast and the multicast modes, PTP uses UDP ports, 319 for event messages and 320 for general messages communication between devices.
- Clock mode (two step and one step)—In the Two-step mode, PTP master sends follow-up messages to pass on the precise transmit timestamp for sync messages. Where as in the One-step mode, no follow up message is used because the sync message itself contains the transmit timestamp as well as the correction filed to obtain the precise transmit timestamp.
- PTP interfaces types—PTP is supported on L3 and L2 SVI interface types. PTP multicast mode is supported on both, the L3 and L2 SVI interface types. However, unicast PTP is supported only on the L3 interface type. For L3/L2 SVI Port-channel interface types, PTP must be configured under the member interfaces.
- PTP encapsulation over UDP over IP—PTP uses UDP as the transport protocol over IP. In both, the unicast and multicast modes, PTP uses UDP ports 319 for event messages and 320 for general messages communication between devices. L2 encapsulation mode is not supported.
- PTP profiles—PTP supports default (1588) , AES67, and SMPTE 2059-2 profiles. They all have different ranges of sync and delay request intervals. For information on the default profile, refer to IEEE 1588. For more information on AES67 and SMPTE 2059-2, refer to the respective specifications.
- Path delay measurement—We support delay request and response mechanism to measure the delay between the master and slave devices. Peer delay request and response mechanism is not supported.
- Message intervals—You can configure the interval at which the announce, syn,c and delay request messages needs to be sent between devices.
- Best master clock (BMC) selection—BMC algorithm is used to select master, slave, and passive states of the PTP enabled interfaces based on the Announce message received as per 1588 specification.



## 3.1.1 PTP Device Types

### Clocks

The following clocks are common PTP devices:

#### Ordinary clock

Communicates with the network based on a single physical port, similar to an end host. An ordinary clock can function as a grandmaster clock.

#### Boundary clock

Typically has several physical ports, with each port behaving like a port of an ordinary clock. However, each port shares the local clock, and the clock data sets are common to all ports. Each port decides its individual state, either master (synchronizing other ports connected to it) or slave (synchronizing to a downstream port), based on the best clock available to it through all of the other ports on the boundary clock. Messages related to synchronization and establishing the master-slave hierarchy terminate in the protocol engine of a boundary clock and are not forwarded.

#### Transparent clock

Forwards all PTP messages like an ordinary switch or router but measures the residence time of a packet in the switch (the time that the packet takes to traverse the transparent clock) and in some cases the link delay of the ingress port for the packet. The ports have no state because the transparent clock does not need to synchronize to the grandmaster clock.

There are two kinds of transparent clocks:

#### End-to-end transparent clock

Measures the residence time of a PTP message and accumulates the times in the correction field of the PTP message or an associated follow-up message.

#### Peer-to-peer transparent clock

Measures the residence time of a PTP message and computes the link delay between each port and a similarly equipped port on another node that shares the link. For a packet, this incoming link delay is added to the residence time in the correction field of the PTP message or an associated follow-up message.

## 3.1.2 PTP Process

The PTP process consists of two phases: establishing the master-slave hierarchy and synchronizing the clocks.

Within a PTP domain, each port of an ordinary or boundary clock follows this process to determine its state:

- Examines the contents of all received announce messages (issued by ports in the master state)
- Compares the data sets of the foreign master (in the announce message) and the local clock for priority, clock class, accuracy, and so on
- Determines its own state as either master or slave

After the master-slave hierarchy has been established, the clocks are synchronized as follows:

- The master sends a synchronization message to the slave and notes the time it was sent.
- The slave receives the synchronization message and notes the time that it was received. For every synchronization message, there is a follow-up message. Hence, the number of sync messages should be equal to the number of follow-up messages.
- The slave sends a delay-request message to the master and notes the time it was sent.
- The master receives the delay-request message and notes the time it was received.
- The master sends a delay-response message to the slave. The number of delay request messages should be equal to the number of delay response messages.
- The slave uses these timestamps to adjust its clock to the time of its master.

### 3.1.3 High Availability for PTP

Stateful restarts are supported for PTP. After a reboot or a supervisor switchover, the running configuration is applied. For more information on high availability, see the *Inspur CN12900 Series INOS-CN High Availability and Redundancy Guide*.

## 3.2 Licensing Requirements for PTP

Product	License Requirement
Inspur INOS-CN	PTP requires no license. Any feature not included in a license package is bundled with the INOS-CN image and is provided at no extra charge to you

## 3.3 Guidelines and Limitations for PTP

- To match PTP control packets using RACL, enable PIM on the L3 interface.
  - PTP is supported for all Inspur CN12900 Series.
  - The **ptp correction-range**, **ptp correction-range logging**, and **ptp mean-path-delay** commands are not supported on the Inspur CN12908 line cards.
  - PTP operates only in boundary clock mode. End-to-end transparent clock and peer-to-peer transparent clock modes are not supported.
  - PTP supports transport over User Datagram Protocol (UDP). Transport over Ethernet is not supported.
  - PTP supports multicast communication. PTP also supports unicast communication and the unicast mode is optional.
  - Inspur CN129-X636C-R, and CN129-X636Q-R line cards support IEEE 802.1AS. IEEE 802.1AS is not supported on the Inspur CN129-X6136YC-R line card or the Inspur CN12904.
  - Inspur CN129-X636C-R, and CN129-X636Q-R line cards support IEEE 802.1AS. IEEE 802.1AS is not supported on the Inspur CN129-X6136YC-R line card or the Inspur CN12904.
  - PTP Offloading is not supported on the Inspur CN12908 switch with an -R series line card
- PTP One Step is not supported on the Inspur CN12908 switch with an -R series line card.
- PTP Offloading is not supported on the Inspur CN12908 switch with an -R series line card
  - PTP One Step is not supported on the Inspur CN12908 switch with an -R series line card.

### Default Settings for PTP

- PTP is not supported on the Inspur CN12908 switches with CN129-X6136YC-R line card.
- PTP supports unicast communication on Inspur CN12908 switches with CN129-X636C-R and CN129-X636Q-R line cards.
- For PTP to work, you must use the latest SUP and LC FPGA versions.
- PTP configuration with UC and MC on either sides is not supported on Inspur CN12908 switches with CN129-X636C-R and CN129-X636Q-R line cards.
- Forwarding PTP management packets is supported on Inspur CN12908 switches with CN129-X636C-R and CN129-X636Q-R line cards.
- PTP is limited to a single domain per network.
- All management messages are forwarded on ports on which PTP is enabled. Handling management messages is not supported.
- PTP-capable ports do not identify PTP packets and do not time-stamp or redirect those packets unless you enable PTP on those ports.
- PTP can be enabled on port-channel member ports.
- We recommend that the PTP device can either have multicast or unicast PTP mode configured, but not both multicast and unicast mode together.

- We recommend that you have the one-step or two-step PTP in the PTP device and the associated downstream switches.

## 3.4 Default Settings for PTP

The following table lists the default settings for PTP parameters.

**Table 2: Default PTP Parameters**

Parameters	Default
PTP	Disabled
PTP version	2
PTP domain	0
PTP priority 1 value when advertising the clock	255
PTP priority 2 value when advertising the clock	255
PTP announce interval	1 log second
PTP announce timeout	3 announce intervals
PTP delay-request interval	0 log seconds
PTP sync interval	2 log seconds
PTP VLAN	gPTP supports only default vlan 1, and no other user configured VLANs.

## 3.5 Configuring PTP

### 3.5.1 Configuring PTP Globally

You can enable or disable PTP globally on a device. You can also configure various PTP clock parameters to help determine which clock in the network has the highest priority to be selected as the grandmaster.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>[no] feature ptp</b> <b>Example:</b> switch(config)# feature ptp	Enables or disables PTP on the device. <b>Note</b> Enabling PTP on the switch does not enable PTP on each interface.
<b>Step 3</b>	<b>[no] ptp device-type [generalized-ptp   boundary-clock]</b> <b>Example:</b> switch(config)# ptp device-type generalized-ptp	Configures the device type as gPTP or boundary clock. The <b>generalized-ptp</b> option is available only for Inspur CN12908 switches with an -R series line card.
<b>Step 4</b>	<b>[no] ptp source ip-address [vrf vrf]</b>	Configures the source IPv4 address for all the PTP

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>switch(config)# ptp source 10.10.10.1</pre>	packets in the multicast PTP mode.
<b>Step 5</b>	<p>(Optional) <b>[no] ptp domain <i>number</i></b></p> <p><b>Example:</b></p> <pre>switch(config)# ptp domain 1</pre>	<p>Configures the domain number to use for this clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network.</p> <p>The range for the <i>number</i> is from 0 to 128.</p>
<b>Step 6</b>	<p>Required: <b>[no] ptp offload</b></p> <p><b>Example:</b></p> <pre>switch(config)# ptp offload</pre>	Increases the number of PTP sessions by offloading some timers to the line card.
<b>Step 7</b>	<p>(Optional) <b>[no] ptp priority1 <i>value</i></b></p> <p><b>Example:</b></p> <pre>switch(config)# ptp priority1 1</pre>	<p>Configures the priority1 value to use when advertising this clock. This value overrides the default criteria (clock quality, clock class, etc.) for best master clock selection.</p> <p>Lower values take precedence.</p> <p>The range for the <i>value</i> is from 0 to 255.</p>
<b>Step 8</b>	<p>(Optional) <b>[no] ptp clock-mode one-step</b></p> <p><b>Example:</b></p> <pre>switch(config)# ptp clock-mode one-step</pre>	<p>Configures the PTP clock mode to the one-step mode. In this case, the timestamp message is sent as a part of the sync message. A followup message is not sent in this mode.</p> <p>The range for the <i>value</i> is from 0 to 255.</p>
<b>Step 9</b>	<p>(Optional) <b>[no] ptp priority2 <i>value</i></b></p> <p><b>Example:</b></p> <pre>switch(config)# ptp priority2 1</pre>	<p>Configures the priority2 value to use when advertising this clock. This value is used to decide between two devices that are otherwise equally matched in the default criteria.</p> <p>For example, you can use the priority2 value to give a specific switch priority over other identical switches.</p> <p>The range for the <i>value</i> is from 0 to 255.</p>
<b>Step 10</b>	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

### 3.5.2 Configuring PTP on an Interface

After you globally enable PTP, it is not enabled on all supported interfaces by default. You must enable PTP interfaces individually.

#### Before you begin

Make sure that you have globally enabled PTP on the switch and configured the source IP address for PTP communication.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>interface ethernet slot/port</b> <b>Example:</b> switch(config)# interface ethernet 2/1 switch(config-if)#	Specifies the interface on which you are enabling PTP and enters the interface configuration mode.
<b>Step 3</b>	<b>[no] ptp</b> <b>Example:</b> switch(config-if)# ptp	Enables or disables PTP on an interface in a multicast mode.
<b>Step 4</b>	(Optional) <b>[no] ptp announce {interval log-seconds   timeout count}</b> <b>Example:</b> switch(config-if)# ptp announce interval 3	Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface. The range for the PTP announcement interval is from 0 to 4 log seconds, and the range for the interval timeout is from 2 to 4 intervals.
<b>Step 5</b>	(Optional) <b>[no] ptp announce {interval log-seconds   timeout count}</b>	Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface. The range for the PTP announcement interval is from 0 to 4 log seconds, and the range for the interval timeout is from 2 to 4 intervals.
<b>Step 6</b>	(Optional) <b>[no] ptp delay-request minimum interval [aes67-2015   smpte-2059-2] log-seconds</b> <b>Example:</b>	Configures the minimum interval allowed between PTP delay messages when the port is in the master state. <i>Table 5: PTP Delay-Request Minimum Interval Range and Default Values</i>

	Command or Action	Purpose												
	<pre>switch(config-if)# ptp delay-request minimum interval aes67-2015-1</pre>	<table border="1"> <thead> <tr> <th data-bbox="906 310 1068 352">Option</th> <th data-bbox="1068 310 1255 352">Range</th> <th data-bbox="1255 310 1453 352">Default Value</th> </tr> </thead> <tbody> <tr> <td data-bbox="906 415 1068 457"><b>aes67-2015</b></td> <td data-bbox="1068 415 1255 499">-4 to 5 log seconds</td> <td data-bbox="1255 415 1453 457">0 log seconds</td> </tr> <tr> <td data-bbox="906 541 1068 625"><b>smpte-2059-2</b></td> <td data-bbox="1068 541 1255 625">-4 to 5 log seconds</td> <td data-bbox="1255 541 1453 583">0 log seconds</td> </tr> <tr> <td data-bbox="906 678 1068 888">Without the <b>aes67-2015</b> or <b>smpte-2059-2</b> option</td> <td data-bbox="1068 678 1255 888">-1 to 6 log seconds (where -1 = 1 frame per second)</td> <td data-bbox="1255 678 1453 720">0 log seconds</td> </tr> </tbody> </table>	Option	Range	Default Value	<b>aes67-2015</b>	-4 to 5 log seconds	0 log seconds	<b>smpte-2059-2</b>	-4 to 5 log seconds	0 log seconds	Without the <b>aes67-2015</b> or <b>smpte-2059-2</b> option	-1 to 6 log seconds (where -1 = 1 frame per second)	0 log seconds
Option	Range	Default Value												
<b>aes67-2015</b>	-4 to 5 log seconds	0 log seconds												
<b>smpte-2059-2</b>	-4 to 5 log seconds	0 log seconds												
Without the <b>aes67-2015</b> or <b>smpte-2059-2</b> option	-1 to 6 log seconds (where -1 = 1 frame per second)	0 log seconds												
<p><b>Step 7</b></p>	<p>(Optional) [no] <b>ptp sync interval</b> <i>log-seconds</i></p> <p><b>Example:</b></p> <pre>switch(config-if)# ptp sync interval 1</pre>	<p>Configures the interval between PTP synchronization messages on an interface. The range is from log(-3) to log(1) seconds.</p>												
<p><b>Step 8</b></p>	<p>(Optional) [no] <b>ptp sync interval</b> [<b>aes67-2015</b>   <b>smpte-2059-2</b>] <i>log-seconds</i></p> <p><b>Example:</b></p> <pre>switch(config-if)# ptp sync interval aes67 1</pre>	<p>Configures the interval between PTP synchronization messages on an interface.</p> <p><b>Table 6: PTP Synchronization Interval Range and Default Values</b></p> <table border="1"> <thead> <tr> <th data-bbox="906 1360 1068 1402">Option</th> <th data-bbox="1068 1360 1255 1402">Range</th> <th data-bbox="1255 1360 1453 1402">Default Value</th> </tr> </thead> <tbody> <tr> <td data-bbox="906 1465 1068 1507"><b>aes67-2015</b></td> <td data-bbox="1068 1465 1255 1549">-4 to 1 log seconds</td> <td data-bbox="1255 1465 1453 1507">-2 log seconds</td> </tr> <tr> <td data-bbox="906 1570 1068 1654"><b>smpte-2059-2</b></td> <td data-bbox="1068 1570 1255 1654">-4 to -1 log seconds</td> <td data-bbox="1255 1570 1453 1612">-2 log seconds</td> </tr> <tr> <td data-bbox="906 1686 1068 1856">Without the <b>aes67-2015</b> or <b>smpte-2059-2</b></td> <td data-bbox="1068 1686 1255 1770">-3 to 1 log seconds</td> <td data-bbox="1255 1686 1453 1728">-2 log seconds</td> </tr> </tbody> </table>	Option	Range	Default Value	<b>aes67-2015</b>	-4 to 1 log seconds	-2 log seconds	<b>smpte-2059-2</b>	-4 to -1 log seconds	-2 log seconds	Without the <b>aes67-2015</b> or <b>smpte-2059-2</b>	-3 to 1 log seconds	-2 log seconds
Option	Range	Default Value												
<b>aes67-2015</b>	-4 to 1 log seconds	-2 log seconds												
<b>smpte-2059-2</b>	-4 to -1 log seconds	-2 log seconds												
Without the <b>aes67-2015</b> or <b>smpte-2059-2</b>	-3 to 1 log seconds	-2 log seconds												

	Command or Action	Purpose		
		option		
<b>Step 9</b>	(Optional) <b>[no] ptp vlan <i>vlan-id</i></b>  <b>Example:</b>  switch(config-if)# ptp vlan 1	Specifies the VLAN for the interface where PTP is being enabled. You can only enable PTP on one VLAN on an interface.  The range is from 1 to 4094.		
<b>Step 10</b>	(Optional) <b>show ptp brief</b>  <b>Example:</b>  switch(config-if)# show ptp brief	Displays the PTP status.		
<b>Step 11</b>	(Optional) <b>show ptp port interface <i>interface slot/port</i></b>  <b>Example:</b>  switch(config-if)# show ptp port interface ethernet 2/1	Displays the status of the PTP port.		
<b>Step 12</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b>  switch(config-if)# copy running-config startup-config	Copies the running configuration to the startup configuration.		

### 3.5.3 Configuring PTP in Unicast Mode

#### Configuring Unicast Mode

Traditional PTP messages are delivered to the nodes that are capable of receiving PTP multicast messages. (For example, announce, sync, delay\_req, delay\_resp and follow\_up). In Unicast mode, all PTP messages are delivered only to a particular PTP node. Multicast address is not used. In unicast mode, you can configure master/slave role and assign corresponding peer slave/master IP addresses.

Up to 8 master IPs can be configured for a slave unicast port and 64 slave IPs can be configured for a master port with a maximum 256 slave IP total for all ports. The following commands are used to configure the unicast slave IPs and unicast master IPs. Unicast packets are only sent to and received from these IPs. Packets received from other IPs are ignored.

```
switch(config-if)# ptp transport ipv4 ucast master
switch(config-if-ptp-master)# slave ipv4 10.10.10.2
switch(config-if)# ptp transport ipv4 ucast slave
switch(config-if-ptp-slave)# master ipv4 10.10.10.1
```

#### Assigning Master Role

Complete the following steps to assign a master role:

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>interface ethernet <i>slot/port</i></b> <b>Example:</b> switch(config)# interface ethernet 2/1 switch(config-if)#	Specifies the interface on which you are enabling PTP and enters the interface configuration mode.
<b>Step 3</b>	<b>[no] ptp transport ipv4 ucast master</b> <b>Example:</b> switch(config-if)# ptp transport ipv4 ucast master switch(config-if-ptp-master)#	Enables PTP master on a particular port (Layer 3 interface). In the master sub-mode, you can enter the slave IPv4 addresses.
<b>Step 4</b>	<b>slave ipv4 &lt;IP_address&gt;</b> <b>Example:</b> switch-1(config)# interface ethernet 1/1  switch-1(config-if)# ptp transport ipv4 ucast master switch-1(config-if-ptp-master)# slave ipv4 1.2.3.1 switch-1(config-if-ptp-master)# slave ipv4 1.2.3.2 switch-1(config-if-ptp-master)# slave ipv4 1.2.3.3 switch-1(config-if-ptp-master)# slave ipv4 1.2.3.4 switch-1(config-if-ptp-master)#	Enters the slave IPv4 addresses. Maximum of 64 IP addresses are allowed per master, but this number varies and it depends on the sync interval configuration. The master sends announce, sync, follow-up, and delay_resp only to these slave addresses. You have to make sure that the slave IP is reachable.

**Assigning Slave Role**

Complete the following steps to assign a slave role:

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>interface ethernet <i>slot/port</i></b> <b>Example:</b>	Specifies the interface on which you are enabling PTP and enters the interface configuration mode.



	<pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	
<b>Step 3</b>	<p><b>[no] ptp transport ipv4 ucast slave</b></p> <p><b>Example:</b></p> <pre>switch(config-if)# ptp transport ipv4 ucast slave switch(config-if-ptp-slave)#</pre>	<p>Enables PTP slave on a particular port (Layer 3 interface).</p> <p>In the slave sub-mode, you can enter the master IPv4 addresses.</p>
<b>Step 4</b>	<p><b>master ipv4 &lt;IP_address&gt;</b></p> <p><b>Example:</b></p> <pre>switch-1(config)# interface ethernet 1/1 switch-1(config-if)# ptp transport ipv4 ucast slave switch-1(config-if-ptp-slave)# master ipv4 4.4.4.1 switch-1(config-if-ptp-slave)# master ipv4 4.4.4.2 switch-1(config-if-ptp-slave)# master ipv4 4.4.4.3</pre>	<p>Enters the master IPv4 addresses. Maximum of 64 IP addresses are allowed per master, but this number varies and it depends on the sync interval configuration. The master sends announce, sync, follow-up, and delay_resp only to these slave addresses. You have to make sure that the slave IP is reachable. Maximum of 8 IP addresses are allowed per slave. The announce, sync, and follow-up messages are received only from the configured master and all other are rejected. This slave sends a delay request to the best master among the configured masters. You have to make sure that the master IP is reachable.</p>

## Configuring Unicast Source Address

Complete the following steps to configure unicast source address:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<p><b>interface ethernet slot/port</b></p> <p><b>Example:</b></p> <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	Specifies the interface on which you are enabling PTP and enters the interface configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>ptp transport ipv4 ucast slave   master</b>	Configures PTP in slave or master mode.
<b>Step 4</b>	<p><b>[no]ptp ucast-source</b></p> <p><b>Example:</b></p> <pre>switch(config-if)# ptp ucast-source A.B.C.D IPv4 address (A.B.C.D) of source</pre>	<p>You can configure PTP source address per interface level.</p> <p>This IP address is used only for unicast PTP messages. You have to make sure that the PTP unicast source IP address is reachable.</p>

### 3.6 Verifying the PTP Configuration

Use one of the following commands to verify the configuration:

**Table 3: PTP Show Commands**

Command	Purpose
<b>show ptp brief</b>	Displays the PTP status.
<b>show ptp clock</b>	Displays the properties of the local clock, including clock identity.
<b>show ptp clock foreign-masters-record</b>	Displays the state of foreign masters known to the PTP process. For each foreign master, the output displays the clock identity, basic clock properties, and whether the clock is being used as a grandmaster.
<b>show ptp corrections</b>	Displays the last few PTP corrections.
<b>show ptp counters [all   interface ethernet slot/port]</b>	Displays the PTP packet counters for all interfaces or for a specified interface.
<b>show ptp parent</b>	Displays the properties of the PTP parent.
<b>show ptp port interface ethernet slot/port</b>	Displays the status of the PTP port on the switch.
<b>show ptp time-property</b>	Displays the PTP clock properties.
<b>show running-config ptp [all]</b>	Displays the running configuration for PTP.
<b>clear ptp counters [all   interface ethernet slot/port]</b>	Clears all PTP messages that are received and transmitted on a specific interface or on all interfaces that has PTP enabled.
<b>clear ptp corrections</b>	Clears the history of the PTP corrections.

### 3.7 Configuration Examples for PTP

This example shows how to configure PTP globally on the device, specify the source IP address for PTP communications, and configure a preference level for the clock:

```
switch# configure terminal
switch(config)# feature ptp
switch(config)# ptp source 10.10.10.1
switch(config)# ptp priority1 1
switch(config)# ptp priority2 1
switch(config)# show ptp brief
```

```

PTP port status
-----
Port State
-----
switch(config)# show ptp clock
PTP Device Type: Boundary clock
Clock Identity : 04:31:10
Clock Domain: 0
Number of PTP ports: 0
Priority1 : 1

Priority2 : 1
Clock Quality:
  Class : 248
  Accuracy : 254
  Offset (log variance) : 65535
Offset From Master : 0
Mean Path Delay : 0
Steps removed : 0
Local clock time:Mon Dec 22 14:13:24 2014

```

This example shows how to configure PTP on an interface and configure the intervals for the announce, delay-request, and synchronization messages:

```

switch# configure terminal switch(config)#
interface ethernet 2/1 switch(config-if)#
ptp
switch(config-if)# ptp announce interval 3
switch(config-if)# ptp announce timeout 2
switch(config-if)# ptp delay-request minimum interval -1
switch(config-if)# ptp sync interval 1 switch(config-if)#
show ptp brief
PTP port status
-----
Port State
-----
Eth2/1 Master
switch(config-if)# show ptp port interface ethernet 2/1
PTP Port Dataset: Eth2/1
Port identity: clock identity: 04:31:10
Port identity: port number: 1028
PTP version: 2
Port state: Master
Delay request interval(log mean): 4
Announce receipt time out: 2
Peer mean path delay: 0
Announce interval(log mean): 3
Sync interval(log mean): 1
Delay Mechanism: End to End
Peer delay request interval(log mean): 0

```

This example shows how to configure master/slave role and assign corresponding peer slave/master IP addresses.

```

switch-1(config)# interface ethernet 1/1
switch-1(config-if)# ptp transport ipv4 ucast master
switch-1(config-if-ptp-master)# slave ipv4 1.2.3.1
switch-1(config-if-ptp-master)# slave ipv4 1.2.3.2
switch-1(config-if-ptp-master)# slave ipv4 1.2.3.3
switch-1(config-if-ptp-master)# slave ipv4 1.2.3.4
switch-1(config-if-ptp-master)#

```

```

switch-1(config-if)# ptp transport ipv4 ucast slave
switch-1(config-if-ptp-slave)# master ipv4 4.4.4.1
switch-1(config-if-ptp-slave)# master ipv4 4.4.4.2
switch-1(config-if-ptp-slave)# master ipv4 4.4.4.3
switch-1(config-if-ptp-slave)# ptp ucast-source 9.9.9.9
switch-1(config-if)# sh running-config ptp

!Command: show running-config ptp
!Time: Mon Oct      1 17:37:09 2018

version      9.2(1i)
feature ptp
ptp source 1.1.1.1

interface Ethernet1/1
  ptp transport ipv4 ucast master
  slave ipv4 1.2.3.1
  slave      ipv4
  1.2.3.2    slave
  ipv4      1.2.3.3
  slave      ipv4
  1.2.3.4

interface Ethernet1/2
  ptp transport ipv4 ucast slave
  master ipv4 4.4.4.1
  master ipv4 4.4.4.2
  master ipv4 4.4.4.3
  ptp ucast-source 9.9.9.9
switch-1(config-if)#

```

## 3.8 Additional References

### 3.8.1 Related Documents

Related Topic	Document Title
ERSPAN	Configuring ERSPAN
1588 IEEE	1588 IEEE standards

## CHAPTER 4 Configuring CDP

---

### 4.1 About CDP

The Cisco Discovery Protocol (CDP) is a media-independent .

CDP gathers protocol addresses of neighboring devices and discovers the platform of those devices. CDP runs over the data link layer only. Two systems that support different Layer 3 protocols can learn about each other.

Each device that you configure for CDP sends periodic advertisements to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain hold-time information, which indicates the length of time that a receiving device should hold CDP information before removing it. You can configure the advertisement or refresh timer and the hold timer.

CDP Version-2 (CDPv2) allows you to track instances where the native VLAN ID or port duplex states do not match between connecting devices.

CDP advertises the following type-length-value fields (TLVs):

- Device ID
- Address
- Port ID
- Capabilities
- Version
- Platform
- Native VLAN
- Full/Half Duplex
- MTU
- SysName
- SysObjectID
- Management Address
- Physical Location
- VTP

All CDP packets include a VLAN ID. If you configure CDP on a Layer 2 access port, the CDP packets sent from that access port include the access port VLAN ID. If you configure CDP on a Layer 2 trunk port, the CDP packets sent from that trunk port include the lowest configured VLAN ID allowed on that trunk port. The trunk port can receive CDP packets that include any VLAN ID in the allowed VLAN list for that trunk port. For more information on VLANs, see the *Inspur CN12900 Series INOS-CN Layer 2 Switching Configuration Guide*.

#### 4.1.1 VTP Feature Support

CDP sends the VLAN Trunking Protocol (VTP) type-length-value field (TLV) if the following conditions are met:

- CDP Version 2 is enabled
- The VTP feature is enabled
- A VTP domain name is configured

You can view the VTP information with the **show cdp neighbors detail** command.

#### 4.1.2 High Availability

Inspur INOS-CN supports both stateful and stateless restarts and switchover for CDP. For more information on high availability, see the *Inspur CN12900 Series INOS-CN High Availability and Redundancy Guide*.

### 4.1.3 Virtualization Support

Inspur INOS-CN supports one instance of CDP.

## 4.2 Licensing Requirements for CDP

Product	License Requirement
Inspur-INOS	CDP requires no license. Any feature not included in a license package is bundled with the INOS image and is provided at no extra charge to you.

## 4.3 Guidelines and Limitations for CDP

CDP has the following configuration guidelines and limitations:

- CDP can discover up to 256 neighbors per port if the port is connected to a hub with 256 connections.
- CDP must be enabled on the device or you cannot enable it on any interfaces.
- You can configure CDP on physical interfaces and port channels only.

## 4.4 Default Settings for CDP

This table lists the default settings for CDP parameters.

Parameters	Default
CDP	Enabled globally and on all interfaces
CDP version	Version 2
CDP device ID	Serial number
CDP timer	60 seconds
CDP hold timer	180 seconds

## 4.5 Configuring CDP

### 4.5.1 Enabling or Disabling CDP Globally

CDP is enabled by default. You can disable CDP and then reenabling it.

You must enable CDP on the device before you enable CDP on any interfaces. If CDP is disabled globally and you enable CDP on specified interfaces, CDP will not be active on those interfaces; the system does not return an error message.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>[no] cdp enable</b> <b>Example:</b>	Enables or disables the CDP feature on the entire device. It is enabled by default.

	Command or Action	Purpose
	<code>switch(config)# cdp enable</code>	
<b>Step 3</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <code>switch(config)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

## 4.5.2 Enabling or Disabling CDP on an Interface

CDP is enabled by default on an interface. You can disable CDP on an interface.

If CDP is disabled globally and you enable CDP on specified interfaces, CDP will not be active on those interfaces; the system does not return an error message.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <code>switch# configure terminal</code> <code>switch(config)#</code>	Enters global configuration mode.
<b>Step 2</b>	<b>interface <i>interface slot/port</i></b> <b>Example:</b> <code>switch(config)# interface ethernet 1/2</code> <code>switch(config-if)#</code>	Enters interface configuration mode.
<b>Step 3</b>	<b>[no] cdp enable</b> <b>Example:</b>  <code>switch(config-if)# cdp enable</code>	Enables or disables CDP on this interface. It is enabled by default.  Note
<b>Step 4</b>	(Optional) <b>show cdp interface <i>interface slot/port</i></b> <b>Example:</b> <code>switch(config-if)# show cdp interface ethernet 1/2</code>	Displays CDP information for an interface.
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <code>switch(config)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

### 4.5.3 Configuring Optional CDP Parameters

You can use the optional commands in this procedure to modify CDP.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	(Optional) <b>cdp advertise {v1   v2}</b> <b>Example:</b> <pre>switch(config)# cdp advertise v1</pre>	Sets the CDP version supported by the device. The default is v2.
<b>Step 3</b>	(Optional) <b>cdp format device-id {mac-address   serial-number   system-name}</b> <b>Example:</b> <pre>switch(config)# cdp format device-id mac-address</pre>	Sets the CDP device ID. The options are as follows: <ul style="list-style-type: none"> <li>• <b>mac-address</b>—The MAC address of the chassis.</li> <li>• <b>serial-number</b>—The chassis serial number/Organizationally Unique Identifier (OUI).</li> <li>• <b>system-name</b>—The system name or fully qualified domain name.</li> </ul> The default is <b>system-name</b> .
<b>Step 4</b>	(Optional) <b>cdp holdtime seconds</b> <b>Example:</b> <pre>switch(config)# cdp holdtime 150</pre>	Sets the time that CDP holds onto neighbor information before removing it. The range is from 10 to 255 seconds. The default is 180 seconds.
<b>Step 5</b>	(Optional) <b>cdp timer seconds</b> <b>Example:</b> <pre>switch(config)# cdp timer 50</pre>	Sets the refresh time when CDP sends advertisements to neighbors. The range is from 5 to 254 seconds. The default is 60 seconds.
<b>Step 6</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

### 4.6 Verifying the CDP Configuration

To display the CDP configuration, perform one of the following tasks:



Command	Purpose
<b>show cdp all</b>	Displays all interfaces that have CDP enabled.
<b>show cdp entry</b> {all   name <i>entry-name</i> }	Displays the CDP database entries.
<b>show cdp global</b>	Displays the CDP global parameters.
<b>show cdp interface</b> <i>interface slot/port</i>	Displays the CDP interface status.
<b>show cdp neighbors</b> { <i>device-id</i>   <b>interface</b> <i>interface slot/port</i> } [ <b>detail</b> ]	Displays the CDP neighbor status.
<b>show cdp interface</b> <i>interface slot/port</i>	Displays the CDP traffic statistics on an interface.

Use the **clear cdp counters** command to clear CDP statistics on an interface.

Use the **clear cdp table** command to clear the CDP cache for one or all interfaces.

## 4.7 Configuration Example for CDP

This example shows how to enable the CDP feature and configure the refresh and hold timers:

```
configure terminal
cdp enable
cdp timer 50
cdp holdtime 100
```

## CHAPTER 5 Configuring SNMP

This chapter describes how to configure the SNMP feature on Inspur INOS-CN devices. This chapter contains the following sections:

### 5.1 About SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

#### 5.1.1 SNMP Functional Overview

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems. The Inspur device supports the agent and MIB. To enable the SNMP agent, you must define the relationship between the manager and the agent.
- A managed information base (MIB)—The collection of managed objects on the SNMP agent SNMP is defined in RFCs 3411 to 3418.

The device supports SNMPv1, SNMPv2c, and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security.

Inspur INOS-CN supports SNMP over IPv6.

#### 5.1.2 SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

Inspur INOS-CN generates SNMP notifications as either traps or informs. A trap is an asynchronous, unacknowledged message sent from the agent to the SNMP managers listed in the host receiver table. Informs are asynchronous messages sent from the SNMP agent to the SNMP manager which the manager must acknowledge receipt of.

Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap. The device cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the device never receives a response, it can send the inform request again.

You can configure Inspur INOS-CN to send notifications to multiple host receivers.

The following table lists the SNMP traps that are enabled by default.

Trap Type	Description
Generic	: coldStart
Entity	: entity_fan_status_change
Entity	: entity_mib_change
Entity	: entity_module_status_change
Entity	: entity_module_inserted
Entity	: entity_module_removed

Trap Type	Description
Entity	: entity_power_out_change
Entity	: entity_power_status_change
Entity	: entity_unrecognised_module
Link	: cErrDisableInterfaceEventRev1
Link	: cieLinkDown
Link	: cieLinkUp
Link	: cmn-mac-move-notification
Link	: delayed-link-state-change
Link	: extended-linkDown
Link	: extended-linkUp
Link	: linkDown
Link	: linkUp
Rf	: redundancy_framework
License	: notify-license-expiry
License	: notify-no-license-for-feature
License	: notify-licensefile-missing
License	: notify-license-expiry-warning
Entity	: entity_sensor
Rmon	: fallingAlarm
Rmon	: hcRisingAlarm
Rmon	: hcFallingAlarm
Rmon	: risingAlarm

### 5.1.3 SNMPv3

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The security features provided in SNMPv3 are the following:

- Message integrity—Ensures that a packet has not been tampered with in-transit.
- Authentication—Determines the message is from a valid source.
- Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

#### Security Models and Levels for SNMPv1, v2, v3

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- noAuthNoPriv—Security level that does not provide authentication or encryption. This level is not supported for SNMPv3.
- authNoPriv—Security level that provides authentication but does not provide encryption.
- authPriv—Security level that provides both authentication and encryption.

Three security models are available: SNMPv1, SNMPv2c, and SNMPv3. The security model combined with the security level determine the security mechanism applied when the SNMP message is processed. The following table identifies what the combinations of security models and levels mean.

**Table 4: SNMP Security Models and Levels**

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA).
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

### User-Based Security Model

The SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur nonmaliciously.
- Message origin authentication—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.
- Message confidentiality—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMPv3 authorizes management operations only by configured users and encrypts SNMP messages.

Inspur INOS-CN uses two authentication protocols for SNMPv3:

- HMAC-MD5-96 authentication protocol
- HMAC-SHA-96 authentication protocol

Inspur INOS-CN uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826.

The **priv** option offers a choice of DES or 128-bit AES encryption for SNMP security encryption. The **priv** option and the **aes-128** token indicate that this privacy password is for generating a 128-bit AES key. The AES **priv** password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 case-sensitive, alphanumeric characters. If you use the localized key, you can specify a maximum of 130 characters.

## CLI and SNMP User Synchronization

SNMPv3 user management can be centralized at the Access Authentication and Accounting (AAA) server level. This centralized user management allows the SNMP agent in Inspur INOS-CN to leverage the user authentication service of the AAA server. Once user authentication is verified, the SNMP PDUs are processed further. Additionally, the AAA server is also used to store user group names. SNMP uses the group names to apply the access/role policy that is locally available in the switch.

Any configuration changes made to the user group, role, or password results in database synchronization for both SNMP and AAA.

Inspur INOS-CN synchronizes the user configuration in the following ways:

- The authentication passphrase specified in the **snmp-server user** command becomes the password for the CLI user.
- The password specified in the **username** command becomes the authentication and privacy passphrases for the SNMP user.
- If you create or delete a user using either SNMP or the CLI, the user is created or deleted for both SNMP and the CLI.
- User-role mapping changes are synchronized in SNMP and the CLI.
- Role changes (deletions or modifications) from the CLI are synchronized to SNMP.

## Group-Based SNMP Access

SNMP access rights are organized by groups. Each group in SNMP is similar to a role through the CLI. Each group is defined with read access or read-write access.

You can begin communicating with the agent once your username is created, your roles are set up by your administrator, and you are added to the roles.

### 5.1.4 SNMP and Embedded Event Manager

The Embedded Event Manager (EEM) feature monitors events, including SNMP MIB objects, and triggers an action based on these events. One of the actions could be to send an SNMP notification. EEM sends the `cEventMgrPolicyEvent` of `ICNT-EMBEDDED-EVENT-MGR-MIB` as the SNMP notification.

### 5.1.5 Multiple Instance Support

A device can support multiple instances of a logical network entity, such as protocol instances or virtual routing and forwarding (VRF) instances. Most existing MIBs cannot distinguish between these multiple logical network entities. For example, the original OSPF-MIB assumes a single protocol instance on a device, but you can now configure multiple OSPF instances on a device.

SNMPv3 uses contexts to distinguish between these multiple instances. An SNMP context is a collection of management information that you can access through the SNMP agent. A device can support multiple contexts for different logical network entities. An SNMP context allows the SNMP manager to access one of the multiple instances of a MIB module supported on the device for the different logical network entities.

Inspur INOS-CN supports the `ICNT-CONTEXT-MAPPING-MIB` to map between SNMP contexts and logical network entities. You can associate an SNMP context to a VRF, protocol instance, or topology.

SNMPv3 supports contexts with the `contextName` field of the SNMPv3 PDU. You can map this `contextName` field to a particular protocol instance or VRF.

For SNMPv2c, you can map the SNMP community to a context using the `snmpCommunityContextName` MIB

object in the SNMP-COMMUNITY-MIB (RFC 3584). You can then map this `snmpCommunityContextName` to a particular protocol instance or VRF using the ICNT-CONTEXT-MAPPING-MIB or the CLI.

### 5.1.6 High Availability for SNMP

Inspur INOS-CN supports stateless restarts for SNMP. After a reboot or supervisor switchover, Inspur INOS-CN applies the running configuration.

### 5.1.7 Virtualization Support for SNMP

Inspur INOS-CN supports one instance of the SNMP. SNMP supports multiple MIB module instances and maps them to logical network entities.

SNMP is also VRF aware. You can configure SNMP to use a particular VRF to reach the SNMP notification host receiver. You can also configure SNMP to filter notifications to an SNMP host receiver based on the VRF where the notification occurred.

## 5.2 Licensing Requirements for SNMP

Product	License Requirement
Inspur INOS-CN	SNMP requires no license. Any feature not included in a license package is bundled with the INOS-CN image and is provided at no extra charge to you.

## 5.3 Guidelines and Limitations for SNMP

SNMP has the following configuration guidelines and limitations:

- Access control list (ACLs) can be applied only to local SNMPv3 users configured on the switch. ACLs cannot be applied to remote SNMPv3 users stored on Authentication, Authorization, and Accounting (AAA) servers.
- Inspur INOS-CN does not support the SNMPv3 `noAuthNoPriv` security level.
- Inspur CN12900 Series switches support the configuration of the SNMP local engine ID.
- For a nondisruptive downgrade path to an earlier release, if a local engine ID has been configured, then you must unconfigure the local engine ID, and then reconfigure the SNMP users and the community strings.
- The default SNMP PDU value is 1500 bytes. The SNMP agent drops any response PDU that is greater than 1500 bytes, causing the SNMP request to fail. To receive MIB data values larger than 1500 bytes, use the `snmp-server packetsize <byte-count>` command to reconfigure the packet size. The valid byte-count range is from 484 to 17382. When a GETBULK response exceeds the packet size, the data can get truncated.
- You must use either the CLI or SNMP to configure a feature on your switch. Do not configure a feature using both interfaces to the switch.
- Using `cefcFanTrayOperStatus snmpwalk` on an individual fan OID tree where the fan is not populated in chassis, can return a response for next OID entry in the tree. To prevent this behavior, use the `-CI` option in `snmpwalk`.
- The behavior is not seen when polling parent OID, or when using `getmany`.

## 5.4 Default Settings for SNMP

The following table lists the default settings for SNMP parameters.

Parameters	Default
License notifications	Enabled

## 5.5 Configuring SNMP

### 5.5.1 Configuring SNMP Users

You can configure a user for SNMP.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>snmp-server user name [auth {md5   sha} passphrase [auto] [priv [aes-128] passphrase] [engineID id] [localizedkey]]</b> <b>Example:</b> <pre>switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh</pre>	Configures an SNMP user with authentication and privacy parameters. The passphrase can be any case-sensitive, alphanumeric string up to 64 characters. If you use the <b>localizedkey</b> keyword, the passphrase can be any case-sensitive, alphanumeric string up to 130 characters. The engineID format is a 12-digit, colon-separated decimal number.
<b>Step 3</b>	(Optional) <b>show snmp user</b> <b>Example:</b> <pre>switch(config) # show snmp user</pre>	Displays information about one or more SNMP users.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

### 5.5.2 Message Encryption

You can configure SNMP to require authentication or encryption for incoming requests. By default, the SNMP agent accepts SNMPv3 messages without authentication and encryption. When you enforce privacy, Inspur INOS-CN responds with an authorization error for any SNMPv3 PDU request using a security level parameter of either **noAuthNoPriv** or **authNoPriv**.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>	Enters global configuration mode.

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
<b>Step 2</b>	<b>snmp-server user <i>name</i> enforcePriv</b> <b>Example:</b> switch(config)# snmp-server user Admin enforcePriv	Enforces SNMP message encryption for this user.
<b>Step 3</b>	<b>snmp-server globalEnforcePriv</b> <b>Example:</b> switch(config)# snmp-server globalEnforcePriv	Enforces SNMP message encryption for all users.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

### 5.5.3 Assigning SNMPv3 Users to Multiple Roles

After you configure an SNMP user, you can assign multiple roles for the user.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>snmp-server user <i>name</i> group</b> <b>Example:</b> switch(config)# snmp-server user Admin superuser	Associates this SNMP user with the configured user role.
<b>Step 3</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

### 5.5.4 Creating SNMP Communities

You can create SNMP communities for SNMPv1 or SNMPv2c.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>	Enters global configuration mode.



	Command or Action	Purpose
	switch# configure terminal switch(config)#	
<b>Step 2</b>	<b>snmp-server community</b> <i>name</i> { <b>group</b> <i>group</i>   <b>ro</b>   <b>rw</b> } <b>Example:</b> switch(config)# snmp-server community public ro	Creates an SNMP community string.
<b>Step 3</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

### 5.5.5 Filtering SNMP Requests

You can assign an access control list (ACL) to an SNMPv2 community or SNMPv3 user to filter SNMP requests. If the assigned ACL allows the incoming request packet, SNMP processes the request. If the ACL denies the request, SNMP drops the request and sends a system message.

Create the ACL with the following parameters:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Protocol (UDP or TCP)

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>snmp-server community</b> <i>name</i> [ <b>use-ipv4acl</b> <i>acl-name</i>   <b>use-ipv6acl</b> <i>acl-name</i> ] <b>Example:</b> switch(config)# snmp-server community public use-ipv4acl myacl	Assigns an IPv4 or IPv6 ACL to an SNMPv2 community to filter SNMP requests. <b>Note</b> IPv6 ACLs are supported for SNMPv2 Communities.
<b>Step 3</b>	<b>snmp-server user</b> <i>username</i> [ <b>use-ipv4acl</b> <i>acl-name</i>   <b>use-ipv6acl</b> <i>acl-name</i> ] <b>Example:</b> switch(config)# snmp-server user user1 use-ipv4acl myacl	Assigns an IPv4 or IPv6 ACL to an SNMPv3 user to filter SNMP requests.

	Command or Action	Purpose
<b>Step 4</b>	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## 5.5.6 Configuring SNMP Notification Receivers

You can configure Inspur INOS-CN to generate SNMP notifications to multiple host receivers.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<p><b>snmp-server host <i>ip-address</i> traps version 1 <i>community</i> [<i>udp_port number</i>]</b></p> <p><b>Example:</b></p> <pre>switch(config)# snmp-server host 192.0.2.1 traps version 1 public</pre>	Configures a host receiver for SNMPv1 traps. The <i>ip-address</i> can be an IPv4 or IPv6 address. The <i>community</i> can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.
<b>Step 3</b>	<p><b>snmp-server host <i>ip-address</i> {traps   informs} version 2c <i>community</i> [<i>udp_port number</i>]</b></p> <p><b>Example:</b></p> <pre>switch(config)# snmp-server host 192.0.2.1 informs version 2c public</pre>	Configures a host receiver for SNMPv2c traps or informs. The <i>ip-address</i> can be an IPv4 or IPv6 address. The <i>community</i> can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.
<b>Step 4</b>	<p><b>snmp-server host <i>ip-address</i> {traps   informs} version 3 {auth   noauth   priv} <i>username</i> [<i>udp_port number</i>]</b></p> <p>Command or Action</p> <p>Example:</p> <pre>switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS</pre>	Configures a host receiver for SNMPv3 traps or informs. The <i>ip-address</i> can be an IPv4 or IPv6 address. The <i>username</i> can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

	Command or Action	Purpose
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b>  <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

### 5.5.7 Configuring a Source Interface for SNMP Notifications

You can configure SNMP to use the IP address of an interface as the source IP address for notifications. When a notification is generated, its source IP address is based on the IP address of this configured interface.

You can configure a source interface as follows:

- All notifications sent to all SNMP notification receivers.
- All notifications sent to a specific SNMP notification receiver. This configuration overrides the global source interface configuration.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>  <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>snmp-server host ip-address source-interface if-type if-number traps version 2c name</b> <b>Example:</b>  <pre>snmp-server host 192.0.2.1 source-interface ethernet 2/1 traps version 2c public</pre>	(Optional) Send Traps messages to this host.  The traps version is the SNMP version to use for notification messages. 2c indicates that SNMPv2c is to be used.
<b>Step 3</b>	<b>snmp-server host ip-address source-interface if-type if-number use-vrf vrf-name</b> <b>Example:</b>  <pre>snmp-server host 192.0.2.1 source-interface ethernet 2/1 use-vrf default</pre>	Configures SNMP to use the selected VRF to communicate with the host receiver. The ip-address can be an IPv4 or IPv6 address. The VRF name can be any alphanumeric string up to 32 characters.  <b>Note</b> This command does not remove the host configuration.
<b>Step 4</b>	<b>snmp-server host ip-address source-interface if-type if-number [udp_port number]</b> <b>Example:</b>	Configures a host receiver for SNMPv2c traps or informs. The ip-address can be an IPv4 or IPv6 address. Use ? to determine the supported interface types. The UDP port number range is from 0 to 65535.

	Command or Action	Purpose
	<pre>switch(config)# snmp-server host 192.0.2.1  source-interface ethernet 2/1</pre>	This configuration overrides the global source interface configuration.
<b>Step 5</b>	<p><b>snmp-server source-interface</b> {traps   informs} <i>if-type</i> <i>if-number</i></p> <p><b>Example:</b></p> <pre>switch(config)# snmp-server source-interface traps ethernet 2/1</pre>	Configures a source interface for sending out SNMPv2c traps or informs. Use ? to determine the supported interface types.
<b>Step 6</b>	<p><b>show snmp source-interface</b></p> <p><b>Example:</b></p> <pre>switch(config)# show snmp source-interface</pre>	Displays information about configured source interfaces.

## 5.5.8 Configuring the Notification Target User

You must configure a notification target user on the device to send SNMPv3 inform notifications to a notification host receiver.

Inspur INOS-CN uses the credentials of the notification target user to encrypt the SNMPv3 inform notification messages to the configured notification host receiver.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<p><b>snmp-server user</b> <i>name</i> [auth {md5   sha} <i>passphrase</i> [auto] [priv [aes-128] <i>passphrase</i>] [engineID <i>id</i>]</p> <p><b>Example:</b></p> <pre>switch(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID 00:00:00:63:00:01:00:10:20:15:10:03</pre>	Configures the notification target user with the specified engine ID for the notification host receiver. The engine ID format is a 12-digit colon-separated decimal number.
<b>Step 3</b>	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## 5.5.9 Configuring SNMP Notification Receivers with VRFs

SNMP adds entries into the `cExtSnmptargetVrfTable` of the ICNT-SNMP-TARGET-EXT-MIB when you configure the VRF reachability and filtering options for an SNMP notification receiver.

You can configure Inspur INOS-CN to use a configured VRF to reach the host receiver or to filter notifications based on the VRF in which the notification occurred.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>[no] snmp-server host ip-address use-vrf vrf-name</b> <b>[udp_port number]</b> <b>Example:</b> <pre>switch(config)# snmp-server host 192.0.2.1 use-vrf Blue</pre>	Configures SNMP to use the selected VRF to communicate with the host receiver. The <i>ip-address</i> can be an IPv4 or IPv6 address. The VRF name can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535. This command adds an entry into the <code>ExtSnmptargetVrfTable</code> of the ICNT-SNMP-TARGET-EXT-MB. The <b>no</b> form of this command removes the VRF reachability information for the configured host and removes the entry from the <code>ExtSnmptargetVrfTable</code> of the ICNT-SNMP-TARGET-EXT-MB. <b>Note</b> This command does not remove the host configuration.
<b>Step 3</b>	<b>[no] snmp-server host ip-address filter-vrf vrf-name</b> <b>[udp_port number]</b> <b>Example:</b> <pre>switch(config)# snmp-server host 192.0.2.1 filter-vrf Red</pre>	Filters notifications to the notification host receiver based on the configured VRF. The <i>ip-address</i> can be an IPv4 or IPv6 address. The VRF name can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535. This command adds an entry into the <code>ExtSnmptargetVrfTable</code> of the ICNT-SNMP-TARGET-EXT-MB. The <b>no</b> form of this command removes the VRF filter

	Command or Action	Purpose
		information for the configured host and removes the entry from the ExtSnmptargetVrfTable of the ICNT-SNMP-TARGET-EXT-MB. <b>Note</b> This command does not remove the host configuration.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b>  switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

### 5.5.10 Configuring SNMP to Send Traps Using an Inband Port

You can configure SNMP to send traps using an inband port. To do so, you must configure the source interface (at the global or host level) and the VRF used to send the traps.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>  switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>snmp-server source-interface traps <i>if-type if-number</i></b> <b>Example:</b>  switch(config)# snmp-server source-interface traps ethernet 1/2	Globally configures a source interface for sending out SNMP traps. Use ? to determine the supported interface types.  You can configure the source interface at the global level or at a host level. When the source interface is configured globally, any new host configuration uses the global configuration to send the traps. <b>Note</b> To configure a source interface at the host level, use the <b>snmp-server host <i>ip-address source-interface if-type if-number</i></b> command.
<b>Step 3</b>	(Optional) <b>show snmp source-interface</b> <b>Example:</b>  switch(config)# show snmp source-interface	Displays information about configured source interfaces.

	Command or Action	Purpose
<b>Step 4</b>	<p><b>snmp-server host</b> <i>ip-address</i> <b>use-vrf</b> <i>vrf-name</i> [<b>udp_port</b> <i>number</i>]</p> <p><b>Example:</b></p> <pre>switch(config)# snmp-server host 171.71.48.164 use-vrf default</pre>	<p>Configures SNMP to use the selected VRF to communicate with the host receiver. The <i>ip-address</i> can be an IPv4 or IPv6 address. The VRF name can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535. This command adds an entry into the ExtSnmpTargetVrfTable of the ICNT-SNMP-TARGET-EXT-MB.</p> <p><b>Note</b> By default, SNMP sends the traps using the management VRF. If you do not want to use the management VRF, you must use this command to specify the desired VRF.</p>
<b>Step 5</b>	<p>(Optional) <b>show snmp host</b></p> <p><b>Example:</b></p> <pre>switch(config)# show snmp host</pre>	Displays information about configured SNMP hosts.
<b>Step 6</b>	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

### 5.5.11 Enabling SNMP Notifications

You can enable or disable notifications. If you do not specify a notification name, Inspur INOS-CN enables all notifications except BGP, EIGRP, and OSPF notifications.

The following table lists the commands that enable the notifications for Inspur INOS-CN MIBs.

**Table 5: Enabling SNMP Notifications**

MIB	Related Commands
All notifications (except BGP, EIGRP, and OSPF)	<b>snmp-server enable traps</b>
ICNT-AAA-SERVER-MIB	<b>snmp-server enable traps aaa</b> <b>snmp-server enable traps aaa server-state-change</b>
ICNT-BGP4-MIB	<b>snmp-server enable traps bgp</b>
ICNT-CALLHOME-MIB	<b>snmp-server enable traps callhome</b> <b>snmp-server enable traps callhome event-notify</b> <b>snmp-server enable traps callhome smtp-send-fail</b>
ICNT-CONFIG-MAN-MIB	<b>snmp-server enable traps config</b> <b>snmp-server enable traps config</b>

<b>MIB</b>	<b>Related Commands</b>
	<b>ccmCLIRunningConfigChanged</b>
ICNT-EIGRP-MIB	<b>snmp-server enable traps eigrp</b> [ <i>tag</i> ]
ICNT-ERR-DISABLE-MIB	<b>snmp-server enable traps link</b> <b>cerrDisableInterfaceEventRev1</b>
ENTITY-MIB, ICNT-ENTITY-SENSOR-MIB	<b>snmp-server enable traps entity</b> <b>snmp-server enable traps entity</b> <b>entity_fan_status_change</b> <b>snmp-server enable traps entity entity_mib_change</b> <b>snmp-server enable traps entity</b> <b>entity_module_inserted</b> <b>snmp-server enable traps entity</b> <b>entity_module_removed</b> <b>snmp-server enable traps entity</b> <b>entity_module_status_change</b> <b>snmp-server enable traps entity</b> <b>entity_power_out_change</b> <b>snmp-server enable traps entity</b> <b>entity_power_status_change</b> <b>snmp-server enable traps entity</b> <b>entity_unrecognised_module</b>
ICNT-FEATURE-CONTROL-MIB	<b>snmp-server enable traps feature-control</b> <b>snmp-server enable traps feature-control</b> <b>FeatureOpStatusChange</b>
ICNT-HSRP-MIB	<b>snmp-server enable traps hsrp</b> <b>snmp-server enable traps hsrp state-change</b>
ICNT-LICENSE-MGR-MIB	<b>snmp-server enable traps license</b> <b>snmp-server enable traps license</b> <b>notify-license-expiry</b> <b>snmp-server enable traps license</b> <b>notify-license-expiry-warning</b> <b>snmp-server enable traps license</b> <b>notify-licensefile-missing</b> <b>snmp-server enable traps license</b> <b>notify-no-license-for-feature</b>
IF-MIB	<b>snmp-server enable traps link</b> <b>snmp-server enable traps link</b> <b>IETF-extended-linkDown</b> <b>snmp-server enable traps link</b> <b>IETF-extended-linkUp</b> <b>snmp-server enable traps link</b>



<b>MIB</b>	<b>Related Commands</b>
	<b>icnt-extended-linkDown</b> <b>snmp-server enable traps link</b> <b>icnt-extended-linkUp</b> <b>snmp-server enable traps link linkDown</b> <b>snmp-server enable traps link Up</b>
OSPF-MIB, OSPF-TRAP-MIB	<b>snmp-server enable traps ospf [tag]</b> <b>snmp-server enable traps ospf lsa</b> <b>snmp-server enable traps ospf rate-limit rate</b>
ICNT-RF-MIB	<b>snmp-server enable traps rf</b> <b>snmp-server enable traps rf</b> <b>redundancy_framework</b>
ICNT-RMON-MIB	<b>snmp-server enable traps rmon</b> <b>snmp-server enable traps rmon fallingAlarm</b> <b>snmp-server enable traps rmon hcFallingAlarm</b> <b>snmp-server enable traps rmon hcRisingAlarm</b> <b>snmp-server enable traps rmon risingAlarm</b>
SNMPv2-MIB	<b>snmp-server enable traps snmp</b>
ICNT-MAC-NOTIFICATION-MIB	<b>snmp-server enable traps snmp authentication</b> <b>snmp-server enable trap link</b> <b>cmn-mac-move-notification</b>
ICNT-PORT-STORM-CONTROL-MIB	<b>storm-control action trap</b>
ICNT-STP-EXTENSIONS-MIB	<b>snmp-server enable traps stpx</b> <b>stpxMstInconsistencyUpdate</b>
ICNT-STP-BRIDGE-MIB	<b>snmp-server enable traps bridge</b> <b>snmp-server enable traps bridge newroot</b> <b>snmp-server enable traps bridge topologychange</b>
ICNT-STPX-MIB	<b>snmp-server enable traps stpx</b> <b>snmp-server enable traps stpx inconsistency</b> <b>snmp-server enable traps stpx loop-inconsistency</b> <b>snmp-server enable traps stpx root-inconsistency</b>
ICNT-SYSTEM-EXT-MIB	<b>snmp-server enable traps sysmgr</b> <b>snmp-server enable traps sysmgr</b> <b>cseFailSwCoreNotifyExtended</b>
VTP-MIB	<b>snmp-server enable traps vtp</b> <b>snmp-server enable traps vtp notifs</b> <b>snmp-server enable traps vtp vlancreate</b> <b>snmp-server enable traps vtp vlandelete</b>

Use the following commands in the configuration mode shown to enable the specified notification:

Command	Purpose
<b>snmp-server enable traps</b> <b>Example:</b> <pre>switch(config)# snmp-server enable traps</pre>	Enables all SNMP notifications.
<b>snmp-server enable traps aaa [server-state-change]</b> <b>Example:</b> <pre>switch(config)# snmp-server enable traps aaa</pre>	Enables the AAA SNMP notifications. Optionally, enables the following specific notifications: <ul style="list-style-type: none"> <li>• <b>server-state-change</b>—Enables AAA server state-change notifications.</li> </ul>
<b>snmp-server enable traps bgp</b> <b>Example:</b> <pre>switch(config)# snmp-server enable traps bgp</pre>	Enables Border Gateway Protocol (BGP) SNMP notifications.
<b>snmp-server enable traps bridge [newroot] [topologychange]</b> <b>Example:</b> <pre>switch(config)# snmp-server enable traps bridge</pre>	Enables STP bridge SNMP notifications. Optionally, enables the following specific notifications: <ul style="list-style-type: none"> <li>• <b>newroot</b>—Enables STP new root bridge notifications.</li> <li>• <b>topologychange</b>—Enables STP bridge topology-change notifications.</li> </ul>
<b>snmp-server enable traps callhome [event-notify] [smtp-send-fail]</b> <b>Example:</b> <pre>switch(config)# snmp-server enable traps callhome</pre>	Enables Call Home notifications. Optionally, enables the following specific notifications: <ul style="list-style-type: none"> <li>• <b>event-notify</b>—Enables Call Home external event notifications.</li> <li>• <b>smtp-send-fail</b>—Enables Simple Mail Transfer Protocol (SMTP) message send fail notifications.</li> </ul>
<b>snmp-server enable traps config [ccmCLIRunningConfigChanged]</b> <b>Example:</b> <pre>switch(config)# snmp-server enable traps config</pre>	Enables SNMP notifications for configuration changes. <ul style="list-style-type: none"> <li>• <b>ccmCLIRunningConfigChanged</b>—Enables SNMP notifications for configuration changes in the running or startup configuration.</li> </ul>
<b>snmp-server enable traps eigrp [tag]</b> <b>Example:</b> <pre>switch(config)# snmp-server enable traps eigrp</pre>	Enables ICNT-HSRP-MIB SNMP notifications.

Command	Purpose
<p><b>snmp-server enable traps entity</b>  [entity_fan_status_change] [entity_mib_change]  [entity_module_inserted] [entity_module_removed]  [entity_module_status_change]  [entity_power_out_change]  [entity_power_status_change]  [entity_unrecognised_module]</p> <p><b>Example:</b>  switch(config)# snmp-server enable traps entity</p>	<p>Optionally, enables the following specific notifications nables ENTITY-MIB SNMP notifications.</p> <p>Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> <li>• <b>entity_fan_status_change</b>—Enables entity fan status-change notifications.</li> <li>• <b>entity_mib_change</b>—Enables entity MIB change notifications.</li> <li>• <b>entity_module_inserted</b>—Enables entity module inserted notifications.</li> <li>• <b>entity_module_removed</b>—Enables entity module removed notifications.</li> <li>• <b>entity_module_status_change</b>—Enables entity module status-change notifications.</li> <li>• <b>entity_power_out_change</b>—Enables entity power-out change notifications.</li> <li>• <b>entity_power_status_change</b>—Enables entity power status-change notifications.</li> <li>• <b>entity_unrecognised_module</b>—Enables entity unrecognized module notifications.</li> </ul>
<p><b>snmp-server enable traps feature-control</b>  [FeatureOpStatusChange]</p> <p><b>Example:</b>  switch(config)# snmp-server enable traps feature-control</p>	<p>Enables feature-control SNMP notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> <li>• <b>FeatureOpStatusChange</b>—Enables feature operation status-change notifications.</li> </ul>
<p><b>snmp-server enable traps hsrp state-change</b></p> <p><b>Example:</b>  switch(config)# snmp-server enable traps hsrp</p>	<p>Enables ENTITY-HSRP-MIB SNMP notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> <li>• <b>notify-license-expiry</b>—Enables HSRP state-change notifications.</li> </ul>
<p><b>snmp-server enable traps license</b>  [notify-license-expiry]  [notify-license-expiry-warning]  [notify-licensefile-missing]  [notify-no-license-for-feature]</p> <p><b>Example:</b>  switch(config)# snmp-server enable traps license</p>	<p>Enables ENTITY-MIB SNMP notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> <li>• <b>notify-license-expiry</b>—Enables license expiry notifications.</li> <li>• <b>notify-license-expiry-warning</b>—Enables license expiry warning notifications.</li> <li>• <b>notify-licensefile-missing</b>—Enables license file-missing notifications.</li> <li>• <b>notify-no-license-for-feature</b>—Enables no-license-installed-for-feature notifications.</li> </ul>
<p><b>snmp-server enable traps link [cieLinkDown]</b></p>	<p>Enables IF-MIB link notifications. Optionally, enable</p>

Command	Purpose
<p><b>[cieLinkUp ] [cmn-mac-move-notification ] [IETF-extended-linkDown ] [IETF-extended-linkUp ] [ICNT-extended-linkDown ] [ICNT-extended-linkUp ][linkDown ] [linkUp]</b></p> <p><b>Example:</b></p> <pre>switch(config)# snmp-server enable traps link</pre>	<p>the following specific notifications:</p> <ul style="list-style-type: none"> <li>• <b>IETF-extended-linkDown</b>—Enables Inspur extended link state down notifications.</li> <li>• <b>IETF-extended-linkUp</b>—Enables Inspur extended link state up notifications.</li> <li>• <b>cmn-mac-move-notification</b>—Enables MAC address move notifications.</li> <li>• <b>ICNT-extended-linkDown</b>—Enables Internet Engineering Task Force (IETF) extended link state down notifications.</li> <li>• <b>ICNT-extended-linkUp</b>—Enables Internet Engineering Task Force (IETF) extended link state up notifications.</li> <li>• <b>linkDown</b>—Enables IETF link state down notifications.</li> <li>• <b>linkUp</b>—Enables IETF link state up notifications.</li> </ul>
<p><b>snmp-server enable traps ospf [tag] [lsa]</b></p> <p><b>Example:</b></p> <pre>switch(config)# snmp-server enable traps ospf</pre>	<p>Enables Open Shortest Path First (OSPF) notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> <li>• <b>lsa</b>—Enables OSPF link state advertisement (LSA) notifications.</li> </ul>
<p><b>snmp-server enable traps rf [redundancy-framework]</b></p> <p><b>Example:</b></p> <pre>switch(config)# snmp-server enable traps rf</pre>	<p>Enables redundancy framework (RF) SNMP notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> <li>• <b>redundancy-framework</b>—Enables RF supervisor switchover MIB notifications.</li> </ul>
<p><b>snmp-server enable traps rmon [fallingAlarm] [hcFallingAlarm] [hcRisingAlarm] [risingAlarm]</b></p> <p><b>Example:</b></p> <pre>switch(config)# snmp-server enable traps rmon</pre>	<p>Enables remote monitoring (RMON) SNMP notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> <li>• <b>fallingAlarm</b>—Enables RMON falling alarm notifications.</li> <li>• <b>hcFallingAlarm</b>—Enables RMON high-capacity falling alarm notifications.</li> <li>• <b>hcRisingAlarm</b>—Enables RMON high-capacity rising alarm notifications.</li> <li>• <b>risingAlarm</b>—Enables RMON rising alarm notifications.</li> </ul>

Command	Purpose
<p><b>snmp-server enable traps snmp [authentication]</b>  <b>Example:</b></p> <pre>switch(config)# snmp-server enable traps snmp</pre>	<p>Enables general SNMP notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> <li>• <b>authentication</b>—Enables SNMP authentication notifications.</li> </ul>
<p><b>snmp-server enable traps stpx [inconsistency] [loop-inconsistency] [root-inconsistency]</b>  <b>Example:</b></p> <pre>switch(config)# snmp-server enable traps stpx</pre>	<p>Enables remote monitoring (RMON) SNMP notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> <li>• <b>inconsistency</b>—Enables SNMP STPX MIB inconsistency update notifications.</li> <li>• <b>loop-inconsistency</b>—Enables SNMP STPX MIB loop-inconsistency update notifications.</li> <li>• <b>root-inconsistency</b>—Enables SNMP STPX MIB root-inconsistency update notifications.</li> </ul>
<p><b>snmp-server enable traps sysmgr [cseFailSwCoreNotifyExtended]</b>  <b>Example:</b></p> <pre>switch(config)# snmp-server enable traps sysmgr</pre> <p><b>snmp-server enable traps upgrade [UpgradeJobStatusNotify] [UpgradeOpNotifyOnCompletion]</b>  <b>Example:</b></p> <pre>switch(config)# snmp-server enable traps upgrade</pre>	<p>Enables software change notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> <li>• <b>cseFailSwCoreNotifyExtended</b>—Enables software core notifications.</li> </ul> <p>Enables upgrade notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> <li>• <b>UpgradeJobStatusNotify</b>—Enables upgrade job status notifications.</li> <li>• <b>UpgradeOpNotifyOnCompletion</b>—Enables upgrade global status notifications.</li> </ul>
<p><b>snmp-server enable traps vtp [notifs] [vlancreate] [vlandelete]</b>  <b>Example:</b></p> <pre>switch(config)# snmp-server enable traps vtp</pre>	<p>Enables VTP notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> <li>• <b>notifs</b>—Enables VTP notifications.</li> <li>• <b>vlancreate</b>—Enables VLAN creation notifications.</li> <li>• <b>vlandelete</b>—Enables VLAN deletion notifications.</li> </ul>
<p><b>storm-control action traps</b>  <b>Example:</b></p>	<p>Enables traffic storm control notifications when the traffic storm control limit is reached.</p>

Command	Purpose
<code>switch(config-if)# storm-control action traps</code>	

## 5.5.12 Disabling Link Notifications on an Interface

You can disable linkUp and linkDown notifications on an individual interface. You can use this limit notifications on flapping interface (an interface that transitions between up and down repeatedly).

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <code>switch# configure terminal</code> <code>switch(config)#</code>	Enters global configuration mode.
<b>Step 2</b>	<b>interface <i>type slot/port</i></b> <b>Example:</b> <code>switch(config)# interface ethernet 2/2</code>	Disables SNMP link-state traps for the interface. This command is enabled by default.
<b>Step 3</b>	<b>no snmp trap link-status</b> <b>Example:</b> <code>switch(config-if)# no snmp trap link-status</code>	Disables SNMP link-state traps for the interface. This command is enabled by default.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <code>switch(config-if)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

## 5.5.13 Displaying SNMP ifIndex for an Interface

The SNMP ifIndex is used across multiple SNMP MIBs to link related interface information.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>show interface snmp-ifindex</b> <b>Example:</b> <code>switch# show interface snmp-ifindex   grep -i</code>  <code>Eth12/1</code> <code>Eth12/1 441974784 (0x1a580000)</code>	Displays the persistent SNMP ifIndex value from the IF-MIB for all interfaces. Optionally, use the   keyword and the <b>grep</b> keyword to search for a particular interface in the output.

### 5.5.14 Enabling a One-Time Authentication for SNMP over TCP

You can enable a one-time authentication for SNMP over a TCP session.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>snmp-server tcp-session [auth]</b> <b>Example:</b> <pre>switch(config)# snmp-server tcp-session</pre>	Enables a one-time authentication for SNMP over a TCP session. The default is disabled.
<b>Step 3</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

### 5.5.15 Assigning SNMP Device Contact and Location Information

You can assign the device contact information, which is limited to 32 characters (without spaces) and the device location.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>S nmp-server contact <i>name</i></b> <b>Example:</b> <pre>switch(config)# snmp-server contact Admin</pre>	Configures sysContact, which is the SNMP contact name.
<b>Step 3</b>	<b>snmp-server location <i>name</i></b> <b>Example:</b> <pre>switch(config)# snmp-server location Lab-7</pre>	Configures sysLocation, which is the SNMP location.
<b>Step 4</b>	(Optional) <b>show snmp</b> <b>Example:</b> <pre>switch(config)# show snmp</pre>	Displays information about one or more destination profiles.

	Command or Action	Purpose
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## 5.5.16 Configuring the Context to Network Entity Mapping

You can configure an SNMP context to map to a logical network entity, such as a protocol instance or VRF.

### Before you begin

Determine the logical network entity instance. For more information on VRFs and protocol instances, see the *Inspur CN12900 Series INOS-CN Unicast Routing Configuration Guide* or the *Inspur CN12900 Series INOS-CN Multicast Routing Configuration Guide*.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>[no] snmp-server context context-name [instance instance-name] [vrf vrf-name] [topology topology-name]</b> <b>Example:</b> <pre>switch(config)# snmp-server context public1 vrf red</pre>	Maps an SNMP context to a protocol instance, VRF, or topology. The names can be any alphanumeric string up to 32 characters. The <b>no</b> option deletes the mapping between an SNMP context and a protocol instance, VRF, or topology. <b>Note</b> Do not enter an instance, VRF, or topology to delete a context mapping. If you use the instance, VRF, or topology keywords, you configure a mapping between the context and a zero-length string.
<b>Step 3</b>	(Optional) <b>snmp-server mib community-map community-name context context-name</b> <b>Example:</b> <pre>switch(config)# snmp-server mib community-map public context public1</pre>	Maps an SNMPv2c community to an SNMP context. The names can be any alphanumeric string up to 32 characters.
<b>Step 4</b>	(Optional) <b>show snmp context</b>	Displays information about one or more SNMP



	Command or Action	Purpose
	<b>Example:</b> <pre>switch(config)# show snmp context</pre>	contexts.
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## 5.5.17 Disabling SNMP

You can disable SNMP on the device.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>no snmp-server protocol enable</b> <b>Example:</b> <pre>switch(config)# no snmp-server protocol enable</pre>	Disables SNMP. SNMP is enabled by default.

## 5.5.18 Managing the SNMP Server Counter Cache Update Timer

You can modify how long, in seconds Inspur INOS-CN holds the cache port state.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>snmp-server counter cache timeout <i>seconds</i></b> <b>Example:</b> <pre>switch(config)# snmp-server counter cache timeout 1200</pre>	Defines how long in seconds, the port states are held in the local cache. The counter cache is enabled by default, and the default cache timeout value is 10 seconds. When disabled, the default cache timeout value is 50 seconds. The range is 1-3600.  <b>Note</b> For end of row (EoR) switching - The range is from 10 to 3600.

	Command or Action	Purpose
<b>Step 3</b>	(Optional) <b>show running-config snmp all   i cac</b>  <b>Example:</b>  switch(config)# copy running-config snmp all   i cac	Displays the configured SNMP-server counter cache update timeout value.
<b>Step 4</b>	<b>no snmp-server counter cache enable</b>  <b>Example:</b>  switch(config)# no snmp-server counter cache enable	Disables the counter cache update.  <b>Note</b> When the counter cache update is disabled, the value set in the timeout parameter determines length of time the port states are held the counter cache.

### 5.5.19 Modifying the AAA Synchronization Time

You can modify how long Inspur INOS-CN holds the synchronized user configuration.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b>  switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>snmp-server aaa-user cache-timeout <i>seconds</i></b>  <b>Example:</b>  switch(config)# snmp-server aaa-user cache-timeout 1200	Configures how long the AAA synchronized user configuration stays in the local cache. The range is from 1 to 86400 seconds. The default is 3600.
<b>Step 3</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b>  switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

## 5.6 Configuring the SNMP Local Engine ID

You can configure the engine ID on a local device.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b>  switch# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
	<code>switch(config)#</code>	
<b>Step 2</b>	<b>snmp-server engineID local</b> <i>engineid-string</i> <b>Example:</b> <code>switch(config)# snmp-server engineID local</code> AA:BB:CC:1A:2C:10	Changes the SNMP engine ID of the local device. The local engine ID should be configured as a list of colon-specified hexadecimal octets, where there are even number of hexadecimal characters that range from 10 to 64 and every two hexadecimal characters are separated by a colon. For example, 80:00:02:b8:04:61:62:63.
<b>Step 3</b>	<b>show snmp engineID</b> <b>Example:</b> <code>switch(config)# show snmp engineID</code>	Displays the identification of the configured SNMP engine.
<b>Step 4</b>	<b>[no] snmp-server engineID local</b> <i>engineid-string</i> <b>Example:</b> <code>switch(config)# no snmp-server engineID local</code> AA:BB:CC:1A:2C:10	Disables the local engine ID and the default auto-generated engine ID is configured.
Step 5	Required: <code>copy running-config startup-config</code> <b>Example:</b> <code>switch(config)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

## 5.7 Verifying SNMP Configuration

To display SNMP configuration information, perform one of the following tasks:

Command	Purpose
<b>show interface snmp-ifindex</b>	Displays the SNMP ifIndex value for all interfaces (from IF-MIB).
<b>show running-config snmp [all]</b>	Displays the SNMP running configuration.
<b>show snmp</b> <b>show snmp community</b>	Displays the SNMP status. Displays the SNMP community strings. <b>Note</b> If the name of the SNMP context in the <b>snmp-server mib community-map</b> command is more than 11 characters, the output of the <b>show snmp community</b> command is displayed in a vertical format instead of a tabular format.
<b>show snmp context</b>	Displays the SNMP context mapping.
<b>show snmp engineID</b>	Displays the SNMP engineID.

Command	Purpose
<b>show snmp group</b>	Displays SNMP roles.
<b>show snmp host</b>	Displays information about configured SNMP hosts.
<b>show snmp session</b>	Displays SNMP sessions.
<b>show snmp source-interface</b>	Displays information about configured source interfaces.
<b>show snmp trap</b>	Displays the SNMP notifications enabled or disabled.
<b>show snmp user</b>	Displays SNMPv3 users.

## 5.8 Configuration Examples for SNMP

This example shows how to configure Inspur INOS-CN to send the ICNT linkUp or Down notifications to one notification host receiver using the Blue VRF and defines two SNMP users, Admin and NMS:

```

configure terminal
snmp-server contact Admin@company.com
snmp-server user Admin auth sha abcd1234 priv abcdefgh snmp-
server user NMS auth sha abcd1234 priv abcdefgh engineID
00:00:00:63:00:01:00:22:32:15:10:03
snmp-server host 192.0.2.1 informs version 3 auth NMS
snmp-server host 192.0.2.1 use-vrf Blue
snmp-server enable traps link ICNT

```

This example shows how to configure SNMP to send traps using an inband port configured at the host level:

```

switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server host 171.71.48.164 version 2c public
switch(config)# snmp-server host 171.71.48.164 source-interface ethernet
1/2
switch(config)# show snmp host
-----
Host Port Version Level Type SecName
-----
171.71.48.164 162 v2c noauth trap
public Source interface: Ethernet
1/2
-----
switch(config)# snmp-server host 171.71.48.164 use-vrf
default
switch(config)# show snmp host
-----
Host Port Version Level Type SecName
-----
171.71.48.164 162 v2c noauth trap
public Use VRF: default
Source interface: Ethernet 1/2
-----

```

This example shows how to configure SNMP to send traps using a globally configured inband port:

```

switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server source-interface traps ethernet 1/2
switch(config)# show snmp source-interface
-----
Notification source-interface
-----

```

```

-----
trap Ethernet1/2
inform -
-----
switch(config)# snmp-server host 171.71.48.164 use_vrf default
switch(config)# show snmp host
-----
Host Port Version Level Type SecName
-----
171.71.48.164 162 v2c noauth trap public
Use VRF: default
Source interface: Ethernet 1/2
-----

```

This example shows how to map VRF red to the SNMPv2c public community string:

```

switch# configure terminal
Enter configuration commands, one per line. End with
CNTL/Z. switch(config)# vrf context red
switch(config-vrf)# exit
switch(config)# snmp-server context public1 vrf red
switch(config)# snmp-server mib community-map public context public1

```

This example shows how to map OSPF instance Enterprise to the same SNMPv2c public community string:

```

switch# configure terminal
Enter configuration commands, one per line. End with
CNTL/Z. switch(config)# feature ospf
switch(config)# router ospf Enterprise
switch(config-router)# exit
switch(config)# snmp-server context public1 instance Enterprise
switch(config)# snmp-server mib community-map public context public1

```

## 5.9 Additional References

### 5.9.1 Related Documents

Related Topic	Document Title
IP ACLs and AAA	<i>Inspur CN12900 Series INOS-CN Security Configuration Guide</i>

### 5.9.2 RFCs

RFC	Title
RFC 3414	<i>User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)</i>
RFC 3415	<i>View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)</i>

## CHAPTER 6 Configuring SPAN

---

This chapter describes how to configure an Ethernet switched port analyzer (SPAN) to analyze traffic between ports on Inspur INOS-CN devices.

This chapter contains the following sections:

### 6.1 About SPAN

SPAN analyzes all traffic between source ports by directing the SPAN session traffic to a destination port with an external analyzer attached to it.

You can define the sources and destinations to monitor in a SPAN session on the local device.

#### 6.1.1 SPAN Sources

The interfaces from which traffic can be monitored are called SPAN sources. Sources designate the traffic to monitor and whether to copy ingress (Rx), egress (Tx), or both directions of traffic. SPAN sources include the following:

- Ethernet ports (but not subinterfaces)
- Port channels
- The inband interface to the control plane CPU
- VLANs

#### Characteristics of Source Ports

SPAN source ports have the following characteristics:

- A port configured as a source port cannot also be configured as a destination port.
- If you use the supervisor inband interface as a SPAN source, the following packets are monitored:
- All packets that arrive on the supervisor hardware (ingress)
- All packets generated by the supervisor hardware (egress)

#### 6.1.2 SPAN Destinations

SPAN destinations refer to the interfaces that monitor source ports. Destination ports receive the copied traffic from SPAN sources. SPAN destinations include the following:

- Ethernet ports in either access or trunk mode
- Port channels in either access or trunk mode

#### Characteristics of Destination Ports

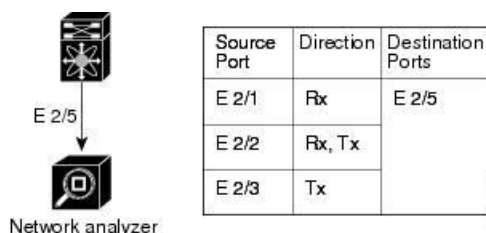
SPAN destination ports have the following characteristics:

- A port configured as a destination port cannot also be configured as a source port.
- A destination port can be configured in only one SPAN session at a time.
- Destination ports do not participate in any spanning tree instance. SPAN output includes bridge protocol data unit (BPDU) Spanning Tree Protocol hello packets.

#### 6.1.3 SPAN Sessions

You can create SPAN sessions to designate sources and destinations to monitor.

This figure shows a SPAN configuration. Packets on three Ethernet ports are copied to destination port Ethernet 2/5. Only traffic in the direction specified is copied.

**Figure 1 : SPAN Configuration**

## Localized SPAN Sessions

A SPAN session is localized when all of the source interfaces are on the same line card. A session destination interface can be on any line card.

### 6.1.4 SPAN Truncation

You can configure the truncation of source packets for each SPAN session based on the size of the MTU. Truncation helps to decrease SPAN bandwidth by reducing the size of monitored packets. Any SPAN packet that is larger than the configured MTU size is truncated to the given size. For example, if you configure the MTU as 300 bytes, the packets with greater than 300 bytes are truncated to 300 bytes.

SPAN truncation is disabled by default. To use truncation, you must enable it for each SPAN session.

### 6.1.5 ACL TCAM Regions

You can change the size of the ACL ternary content addressable memory (TCAM) regions in the hardware. For information on the TCAM regions used by SPAN sessions, see the "Configuring IP ACLs" chapter of the *Inspur CN12900 Series INOS-CN Security Configuration Guide*.

### 6.1.6 High Availability

The SPAN feature supports stateless and stateful restarts. After a reboot or supervisor switchover, the running configuration is applied. For more information on high availability, see the *Inspur CN12900 Series INOS-CN High Availability and Redundancy Guide*.

## 6.2 Licensing Requirements for SPAN

Product	License Requirement
Inspur INOS-CN	SPAN requires no license. Any feature not included in a license package is bundled with the INOS-CN image and is provided at no extra charge to you.

## 6.3 Prerequisites for SPAN

SPAN has the following prerequisites:

- You must first configure the ports on each device to support the desired SPAN configuration. For more information, see the *Inspur CN12900 Series INOS-CN Interfaces Configuration Guide*.

## 6.4 Guidelines and Limitations for SPAN

SPAN has the following configuration guidelines and limitations:

- All SPAN replication is performed in the hardware. The supervisor CPU is not involved.

- You can configure only one destination port in a SPAN session.
- A destination port can be configured in only one SPAN session at a time.
- Configuring two SPAN or ERSPAN sessions on the same source interface, with only one filter is not supported.
- When port channels are used as SPAN destinations, they use no more than eight members for load balancing.
- You cannot configure a port as both a source and destination port.
- Enabling UniDirectional Link Detection (UDLD) on the SPAN source and destination ports simultaneously is not supported. If UDLD frames are expected to be captured on the source port of such SPAN session, disable UDLD on the destination port of the SPAN session.
- SPAN is not supported for management ports.
- Statistics are not support for the filter access group.
- SPAN is supported in Layer 3 mode; however, SPAN is not supported on Layer 3 subinterfaces or Layer 3 port-channel subinterfaces.
- The same source can be part of multiple sessions.
- When a SPAN session contains source ports that are monitored in the transmit or transmit and receive direction, packets that these ports receive might be replicated to the SPAN destination port even though the packets are not actually transmitted on the source ports. Some examples of this behavior on source ports are as follows:
  - Traffic that results from flooding
  - Broadcast and multicast traffic
- SPAN sessions cannot capture packets with broadcast or multicast MAC addresses that reach the supervisor, such as ARP requests and Open Shortest Path First (OSPF) protocol hello packets, if the source of the session is the supervisor Ethernet in-band interface. To capture these packets, you must use the physical interface as the source in the SPAN sessions.
- VLAN SPAN monitors only the traffic that enters Layer 2 ports in the VLAN.
- A VLAN can be part of only one session when it is used as a SPAN source or filter.
- VLANs can be SPAN sources in the ingress and egress direction on Inspur CN12900 Series switches with CN129-X636C-R, CN129-X636Q-R and CN129-X6136YC-R line cards. For all other switches, VLANs are supported as SPAN sources only in the ingress direction.
- VLAN ACL redirects to SPAN destination ports are not supported.
- The combination of VLAN source session and port source session is not supported. If the traffic stream matches the VLAN source session as well as port source session, two copies are needed at two destination ports. Due to the hardware limitation, only the VLAN source SPAN and the specific destination port receive the SPAN packets.
- Supervisor-generated stream of bytes module header (SOBMH) packets have all of the information to go out on an interface and can bypass all forwarding lookups in the hardware, including SPAN and ERSPAN. The Inspur CN129-X636C-R, CN129-X636Q-R and CN129-X6136YC-R line cards support inband SPAN and local SPAN.
- Inspur INOS-CN does not span Link Layer Discovery Protocol (LLDP) or Link Aggregation Control Protocol (LACP) packets when the source interface is not a host interface port channel.

The following guidelines and limitations apply to egress (Tx) SPAN:

- SPAN copies for multicast packets are made prior to rewrite. Therefore, the TTL, VLAN ID, any remarking due to egress policy, and so on are not captured in the SPAN copy.
- The flows for post-routed unknown unicast flooded packets are in the SPAN session, even if the SPAN session is configured to not monitor the ports on which this flow is forwarded. This limitation applies to Network Forwarding Engine (NFE) and NFE2-enabled EOR switches and SPAN sessions that have Tx port sources.

The following guidelines and limitations apply to ingress (Rx) SPAN:

- The CPU SPAN source can be added only for the Rx direction (SPAN packets coming from the CPU).
- Multiple ACL filters are not supported on the same source.



- SPAN packets to the CPU are rate limited and are dropped in the inband path. You can change the rate limit using the **hardware rate-limiter span** command. You can analyze SPAN copies on the supervisor using the **ethanalyzer local interface inband mirror detail** command.

The following guidelines and limitations apply to VXLAN/VTEP:

- SPAN source or destination is supported on any port.
- Rx SPAN is supported. Tx or both (Tx and Rx) are not supported.

## 6.5 Default Settings for SPAN

The following table lists the default settings for SPAN parameters.

Parameters	Default
SPAN sessions	Created in the shut state

## 6.6 Configuring SPAN

### 6.6.1 Configuring a SPAN Session

You can configure a SPAN session on the local device only. By default, SPAN sessions are created in the shut state.

#### Before you begin

You must configure the destination ports in access or trunk mode. For more information, see the *Inspur CN12900 Series INOS-CN Interfaces Configuration Guide*.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>interface <i>interface slot/port</i></b> <b>Example:</b> <pre>switch(config)# interface ethernet 2/5 switch(config-if)#</pre>	Enters interface configuration mode on the selected slot and port.
<b>Step 3</b>	<b>switchport</b> <b>Example:</b> <pre>switch(config-if)# switchport</pre>	Configures switchport parameters for the selected slot and port or range of ports.
<b>Step 4</b>	<b>switchport monitor</b> <b>Example:</b> <pre>switch(config-if)# switchport monitor</pre>	Configures the switchport interface as a SPAN destination.

	Command or Action	Purpose
<b>Step 5</b>	(Optional) Repeat Steps 2 through 4 to configure monitoring on additional SPAN destinations.	—
<b>Step 6</b>	<b>no monitor session</b> <i>session-number</i>  <b>Example:</b>  <pre>switch(config)# no monitor session 3</pre>	<p>Clears the configuration of the specified SPAN session.</p> <p>The new session configuration is added to the existing session configuration.</p>
<b>step 7</b>	<b>monitor session</b> <i>session-number</i> [ <b>rx</b>   <b>tx</b> ] [ <b>shut</b> ]  <b>Example:</b>  <pre>switch(config)# monitor session 3 rx</pre> <pre>switch(config-monitor)#</pre> <b>Example:</b> <pre>switch(config)# monitor session 3 tx</pre> <pre>switch(config-monitor)#</pre> <b>Example:</b> <pre>switch(config)# monitor session 3 shut</pre> <pre>switch(config-monitor)#</pre>	<p>Enters the monitor configuration mode. The new session configuration is added to the existing session configuration.</p> <p>By default, the session is created in the shut state, and the session is a local SPAN session. The optional keyword shut specifies a shut state for the selected session.</p>
<b>Step 8</b>	<b>description</b> <i>description</i>  <b>Example:</b>  <pre>switch(config-monitor)# description</pre> <pre>my_span_session_3</pre>	<p>Configures a description for the session. By default, no description is defined. The description can be up to 32 alphanumeric characters.</p>
<b>Step 9</b>	<b>source</b> { <b>interface</b> <i>type</i> [ <b>rx</b>   <b>tx</b>   <b>both</b> ]   <b>vlan</b> { <i>number</i>   <i>range</i> } [ <b>rx</b> ]}  <b>Example:</b>  <pre>switch(config-monitor)# source interface</pre> <pre>ethernet</pre> <pre>2/1-3, ethernet 3/1 rx</pre> <b>Example:</b> <pre>switch(config-monitor)# source interface</pre> <pre>port-channel 2</pre> <b>Example:</b> <pre>switch(config-monitor)# source interface</pre>	<p>Configures sources and the traffic direction in which to copy packets. You can enter a range of Ethernet ports, a port channel, an inband interface, a range of VLANs, or a satellite port or host interface port channel.</p> <p>You can configure one or more sources, as either a series of comma-separated entries or a range of numbers.</p> <p>You can specify the traffic direction to copy as ingress (rx), egress (tx), or both.</p> <p><b>Note</b> Source VLANs are supported only in the</p>

	Command or Action	Purpose
	<pre>sup-eth  0 both <b>Example:</b> switch(config-monitor)# source vlan 3, 6-8 rx  <b>Example:</b> switch(config-monitor)# source interface ethernet 101/1/1-3</pre>	<p>ingress direction.</p> <p>For a unidirectional session, the direction of the source must match the direction specified in the session.</p>
<b>Step 10</b>	(Optional) Repeat Step 9 to configure all SPAN sources.	—
<b>Step 11</b>	(Optional) <b>filter vlan</b> {number   range} <b>Example:</b> <pre>switch(config-monitor)# filter vlan 3-5, 7</pre>	Configures which VLANs to select from the configured sources. You can configure one or more VLANs, as either a series of comma-separated entries or a range of numbers.
<b>Step 12</b>	(Optional) Repeat Step 11 to configure all source VLANs to filter.	—
<b>Step 13</b>	(Optional) <b>filter access-group</b> <i>acl-filter</i> <b>Example:</b> <pre>switch(config-monitor)# filter access-group ACL1</pre>	Associates an ACL with the SPAN session.
<b>Step 14</b>	Required: <b>destination interface</b> <i>type slot/port</i> <b>Example:</b> <pre>switch(config-monitor)# destination interface</pre> <b>Example:</b> <pre>switch(config-monitor)# destination interface</pre>	Configures a destination for copied source packets. <b>Note</b> The SPAN destination port must be either an access port or a trunk port.  destination port.
<b>Step 15</b>	Required: <b>no shut</b> <b>Example:</b> <pre>switch(config-monitor)# no shut</pre>	Enables the SPAN session. By default, the session is created in the shut state.
<b>Step 16</b>	(Optional) <b>show monitor session</b> {all   session-number   range session-range} [brief] <b>Example:</b>	Displays the SPAN configuration.

	Command or Action	Purpose
	<code>switch(config-monitor)# show monitor session 3</code>	
<b>Step 17</b>	<p>(Optional) <b>copy running-config startup-config</b>  <b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## 6.6.2 Configuring UDF-Based SPAN

You can configure the device to match on user-defined fields (UDFs) of the outer or inner packet fields (header or payload) and to send the matching packets to the SPAN destination. Doing so can help you to analyze and isolate packet drops in the network.

### Before you begin

Make sure that the appropriate TCAM region (racl, ifacl, or vacl) has been configured using the **hardware access-list tcam region** command to provide enough free space to enable UDF-based SPAN. For information, see the "Configuring ACL TCAM Region Sizes" section in the *Inspur CN12900 Series INOS-CN Security Configuration Guide*.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>configure terminal</b>  <b>Example:</b></p> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<p><b>udf udf-name offset-base offset length</b>  <b>Example:</b></p> <pre>switch(config)# udf udf-x packet-start 12 1 switch(config)# udf udf-y header outer 13 20 2</pre>	<p>Defines the UDF as follows:</p> <ul style="list-style-type: none"> <li>• <i>udf-name</i>—Specifies the name of the UDF. You can enter up to 16 alphanumeric characters for the name.</li> <li>• <i>offset-base</i>—Specifies the UDF offset base as follows, where <b>header</b> is the packet header to consider for the offset: <b>packet-start   header {outer   inner {13   14}}</b>.</li> <li>• <i>offset</i>—Specifies the number of bytes offset from the offset base. To match the first byte from the offset base (Layer 3/Layer 4 header), configure the offset as 0.</li> <li>• <i>length</i>—Specifies the number of bytes from the offset. Only 1 or 2 bytes are supported. To match additional bytes, you must define multiple UDFs.</li> </ul>

	Command or Action	Purpose
		You can define multiple UDFs, but Inspur recommends defining only required UDFs.
<b>Step 3</b>	<p><b>hardware access-list tcam region</b> {racl   ifacl   vacl}  <b>qualify udf</b> <i>udf-names</i></p> <p><b>Example:</b>  switch(config)# hardware access-list tcam region  racl qualify udf udf-x udf-y</p>	<p>Attaches the UDFs to one of the following TCAM regions:</p> <ul style="list-style-type: none"> <li>• <b>racl</b>—Applies to Layer 3 ports.</li> <li>• <b>ifacl</b>—Applies to Layer 2 ports.</li> <li>• <b>vacl</b>—Applies to source VLANs.</li> </ul> <p>You can attach up to 8 UDFs to a TCAM region.</p> <p><b>Note</b> When the UDF qualifier is added, the TCAM region goes from single wide to double wide. Make sure enough free space is available; otherwise, this command will be rejected. If necessary, you can reduce the TCAM space from unused regions and then re-enter this command. For more information, see the "Configuring ACL <b>TCAM Region Sizes</b>" section in the <i>Inspur CN12900 Series INOS-CN Security Configuration Guide</i></p> <p><b>Note</b> The <b>no</b> form of this command detaches the UDFs from the TCAM region and returns the region to single wide.</p>
<b>Step 4</b>	<p>Required: <b>copy running-config startup-config</b></p> <p><b>Example:</b>  switch(config)# copy running-config startup-config</p>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.
<b>Step 5</b>	<p>Required: <b>reload</b></p> <p><b>Example:</b>  switch(config)# reload</p>	<p>Reloads the device.</p> <p><b>Note</b> Your UDF configuration is effective only after you enter <b>copy running-config startup-config + reload</b>.</p>
<b>Step 6</b>	<b>ip access-list</b> <i>span-acl</i>	Creates an IPv4 access control list (ACL) and enters

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>switch(config)# ip access-list span-acl-udf-only switch(config-acl)#</pre>	IP access list configuration mode.
<b>Step 7</b>	<p>Enter one of the following commands:</p> <ul style="list-style-type: none"> <li>• <b>permit udf</b> <i>udf-name value mask</i></li> <li>• <b>permit ip</b> <i>source destination udf udf-name value mask</i></li> </ul> <p><b>Example:</b></p> <pre>switch(config-acl)# permit udf udf-x 0x40 0xF0 udf-y 0x1001 0xF00F</pre> <p><b>Example:</b></p> <pre>switch(config-acl)# permit ip 10.0.0./24 any udf udf-x 0x02 0x0F udf-y 0x1001 0xF00F</pre>	Configures the ACL to match only on UDFs (example 1) or to match on UDFs along with the current access control entries (ACEs) for the outer packet fields (example 2). A single ACL can have ACEs with and without UDFs together. Each ACE can have different UDF fields to match, or all ACEs can match for the same list of UDFs.
<b>Step 8</b>	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

### 6.6.3 Configuring SPAN Truncation

You can configure truncation for local and SPAN source sessions only.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<p><b>monitor session</b> <i>session-number</i></p> <p><b>Example:</b></p> <pre>switch(config)# monitor session 5 switch(config-monitor)#</pre>	Enters monitor configuration mode for the specified SPAN session.
<b>Step 3</b>	<p><b>source interface</b> <i>type slot/port [rx   tx   both]</i></p> <p><b>Example:</b></p> <pre>switch(config-monitor)# source interface ethernet 1/5 both</pre>	Configures the source interface.

	Command or Action	Purpose
<b>Step 4</b>	<b>mtu size</b> <b>Example:</b> <pre>switch(config-monitor)# mtu 512</pre>	Configures the MTU size for truncation. Any SPAN packet that is larger than the configured MTU size is truncated to the configured size. The MTU size range is 320 to 1518 Bytes.
<b>Step 5</b>	<b>destination interface type slot/port</b> <b>Example:</b> <pre>switch(config-monitor)# destination interface Ethernet 1/39</pre>	Configures the Ethernet SPAN destination port.
<b>Step 6</b>	<b>no shut</b> <b>Example:</b> <pre>switch(config-monitor)# no shut</pre>	Enables the SPAN session. By default, the session is created in the shut state.
<b>Step 7</b>	<b>(Optional) show monitor session session</b> <b>Example:</b> <pre>switch(config-monitor)# show monitor session 5</pre>	Displays the SPAN configuration.
<b>Step 8</b>	<b>copy running-config startup-config</b> <b>Example:</b>	Copies the running configuration to the startup configuration.

## 6.6.4 Shutting Down or Resuming a SPAN Session

You can shut down SPAN sessions to discontinue the copying of packets from sources to destinations. You can shut down one session in order to free hardware resources to enable another session. By default, SPAN sessions are created in the shut state.

You can resume (enable) SPAN sessions to resume the copying of packets from sources to destinations. In order to enable a SPAN session that is already enabled but operationally down, you must first shut it down and then enable it.

You can configure the shut and enabled SPAN session states with either a global or monitor configuration mode command.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>[no] monitor session {session-range   all} shut</b> <b>Example:</b>	Shuts down the specified SPAN sessions. By default, sessions are created in the shut state.

	Command or Action	Purpose
	<code>switch(config)# monitor session 3 shut</code>	The <b>no</b> form of the command resumes (enables) the specified SPAN sessions. By default, sessions are created in the shut state. <b>Note</b> If a monitor session is enabled but its operational status is down, to enable the session, you must first specify the <b>monitor session shut</b> command followed by the <b>no monitor session shut</b> command.
<b>Step 3</b>	<b>monitor session</b> <i>session-number</i>  <b>Example:</b> <code>switch(config)# monitor session 3</code> <code>switch(config-monitor)#</code>	Enters the monitor configuration mode. The new session configuration is added to the existing session configuration.
<b>Step 4</b>	<b>[no] shut</b>  <b>Example:</b> <code>switch(config-monitor)# shut</code>	Shuts down the SPAN session. By default, the session is created in the shut state.  The <b>no</b> form of the command enables the SPAN session. By default, the session is created in the shut state.
<b>Step 5</b>	(Optional) <b>show monitor</b>  <b>Example:</b> <code>switch(config-monitor)# show monitor</code>	Displays the status of SPAN sessions.
<b>Step 6</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <code>switch(config)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

## 6.7 Verifying the SPAN Configuration

To display the SPAN configuration, perform one of the following tasks:

Command	Purpose
<b>show monitor session</b> { <b>all</b>   <i>session-number</i>   <i>session-range</i> } [ <b>brief</b> ]	<b>range</b> Displays the SPAN session configuration.



## 6.8 Configuration Examples for SPAN

### 6.8.1 Configuration Example for a SPAN Session

To configure a SPAN session, follow these steps:

#### SUMMARY STEPS

1. Configure destination ports in access mode and enable SPAN monitoring.

#### Configure a SPAN session.

#### PROCEDURE

- Step 1** Configure destination ports in access mode and enable SPAN monitoring.

#### Example:

```
switch# configure terminal
switch(config)# interface ethernet 2/5
switch(config-if)# switchport
switch(config-if)# switchport
monitor switch(config-if)# no shut
switch(config-if)# exit
switch(config)#
```

- Step 2** Configure a SPAN session.

#### Example:

```
switch(config)# no monitor session 3
switch(config)# monitor session 3
switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-monitor)# source interface port-channel 2
switch(config-monitor)# source interface sup-eth 0 both
switch(config-monitor)# source vlan 3, 6-8 rx
switch(config-monitor)# source interface ethernet 101/1/1-3
switch(config-monitor)# filter vlan 3-5, 7
switch(config-monitor)# destination interface ethernet 2/5
switch(config-monitor)# no shut
switch(config-monitor)# exit
```

### 6.8.2 Configuration Example for a Unidirectional SPAN Session

To configure a unidirectional SPAN session, follow these steps:

#### SUMMARY STEPS

1. Configure destination ports in access mode and enable SPAN monitoring.

#### Configure a SPAN session.

#### PROCEDURE

- Step 1** Configure destination ports in access mode and enable SPAN monitoring.

#### Example:

```

switch# configure terminal
switch(config)# interface ethernet 2/5
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# no shut
switch(config-if)# exit
switch(config)#

```

**Step 2** Configure a SPAN session.

**Example:**

```

switch(config)# no monitor session 3
switch(config)# monitor session 3 rx
switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-monitor)# filter vlan 3-5, 7
switch(config-monitor)# destination interface ethernet 2/5
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 3
switch(config)# copy running-config startup-config

```

### 6.8.3 Configuration Example for a SPAN ACL

This example shows how to configure a SPAN ACL:

```

switch# configure terminal
switch(config)# ip access-list match_11_pkts
switch(config-acl)# permit ip 11.0.0.0 0.255.255.255
any
switch(config-acl)# exit
switch(config)# ip access-list match_12_pkts
switch(config-acl)# permit ip 12.0.0.0 0.255.255.255
any
switch(config-acl)# exit
switch(config)# vlan access-map span_filter 5
switch(config-access-map)# match ip address
match_11_pkts
switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# vlan access-map span_filter 10
switch(config-access-map)# match ip address
match_12_pkts
switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# monitor session 1
switch(config-erspan-src)# filter access_group
span_filter

```

### 6.8.4 Configuration Examples for UDF-Based SPAN

This example shows how to configure UDF-based SPAN to match on the inner TCP flags of an encapsulated IP-in-IP packet using the following match criteria:

- Outer source IP address: 10.0.0.2
- Inner TCP flags: Urgent TCP flag is set
- Bytes: Eth Hdr (14) + Outer IP (20) + Inner IP (20) + Inner TCP (20, but TCP flags at 13th byte)
- Offset from packet-start: 14 + 20 + 20 + 13 = 67
- UDF match value: 0x20

- UDF mask: 0xFF

```

udf udf_tcpflags packet-start 67 1
hardware access-list tcam region racl qualify udf
udf_tcpflags copy running-config startup-config
reload
ip access-list acl-udf
    permit ip 10.0.0.2/32 any udf udf_tcpflags 0x20
0xff monitor session 1
    source interface Ethernet
    1/1 filter access-group
    acl-udf

```

This example shows how to configure UDF-based SPAN to match regular IP packets with a packet signature (DEADBEEF) at 6 bytes after a Layer 4 header start using the following match criteria:

- Outer source IP address: 10.0.0.2
- Inner TCP flags: Urgent TCP flag is set
- Bytes: Eth Hdr (14) + IP (20) + TCP (20) + Payload: 112233445566DEADBEEF7788
- Offset from Layer 4 header start: 20 + 6 = 26
- UDF match value: 0xDEADBEEF (split into two-byte chunks and two UDFs)
- UDF mask: 0xFFFFFFFF

```

udf udf_pktsig_msb header outer 13 26 2
udf udf_pktsig_lsb header outer 13 28 2
hardware access-list tcam region racl qualify udf udf_pktsig_msb
udf_pktsig_lsb copy running-config startup-config
reload
ip access-list acl-udf-pktsig
    permit udf udf_pktsig_msb 0xDEAD 0xFFFF udf udf_pktsig_lsb 0xBEEF
0xFFFF monitor session 1
    source interface Ethernet 1/1
    filter access-group
    acl-udf-pktsig

```

## 6.8.5 Configuration Example for SPAN Truncation

This example shows how to configure SPAN truncation for use with MPLS stripping:

```

mpls strip
ip access-list mpls
    statistics
    per-entry
    20 permit ip any any redirect Ethernet1/5

interface
    Ethernet1/5
    switchport
    switchport mode
    trunk mtu 9216
    no shutdown

monitor session 1
    source interface Ethernet1/5
    tx mtu 64
    destination interface
    Ethernet1/6 no shut

```

## 6.9 Additional References

### 6.9.1 Related Documents

Related Topic	Document Title
ACL TCAM regions	<i>Inspur CN12900 Series INOS-CN Security Configuration Guide</i>

## CHAPTER 7 Configuring ERSPAN

---

This chapter describes how to configure an encapsulated remote switched port analyzer (ERSPAN) to transport mirrored traffic in an IP network on Inspur INOS-CN devices.

This chapter contains the following sections:

### 7.1 About ERSPAN

ERSPAN transports mirrored traffic over an IP network, which provides remote monitoring of multiple switches across your network. The traffic is encapsulated at the source router and is transferred across the network. The packet is decapsulated at the destination router and then sent to the destination interface.

#### 7.1.1 ERSPAN Types

Inspur CN12900 Series switches support only ERSPAN.

#### 7.1.2 ERSPAN Sources

The interfaces from which traffic can be monitored are called ERSPAN sources. Sources designate the traffic to monitor and whether to copy ingress, egress, or both directions of traffic. ERSPAN sources include the following:

- Ethernet ports (but not subinterfaces)
- Port channels
- The inband interface to the control plane CPU
- VLANs

#### 7.1.3 ERSPAN Sessions

You can create ERSPAN sessions that designate sources to monitor.

##### Localized ERSPAN Sessions

An ERSPAN session is localized when all of the source interfaces are on the same line card.

#### 7.1.4 ERSPAN Truncation

You can configure the truncation of source packets for each ERSPAN session based on the size of the MTU. Truncation helps to decrease ERSPAN bandwidth by reducing the size of monitored packets. Any ERSPAN packet that is larger than the configured MTU size is truncated to the given size. For ERSPAN, an additional ERSPAN header is added to the truncated packet from 54 to 166 bytes depending on the ERSPAN header type. For example, if you configure the MTU as 300 bytes, the packets are replicated with an ERSPAN header size from 354 to 466 bytes depending on the ERSPAN header type configuration.

ERSPAN truncation is disabled by default. To use truncation, you must enable it for each ERSPAN session.

#### 7.1.5 High Availability

The ERSPAN feature supports stateless and stateful restarts. After a reboot or supervisor switchover, the running configuration is applied.

For more information on high availability, see the *Inspur CN12900 Series INOS-CN High Availability and Redundancy Guide*.

## 7.2 Licensing Requirements for ERSPAN

The following table shows the licensing requirements for this feature:

Product	License Requirement
Inspur INOS-CN	ERSPAN requires no license. Any feature not included in a license package is bundled with the INOS-CN image and is provided at no extra charge to you.

## 7.3 Prerequisites for ERSPAN

ERSPAN has the following prerequisites:

- You must first configure the ports on each device to support the desired ERSPAN configuration. For more information, see the *Inspur CN12900 Series INOS-CN Interfaces Configuration Guide*.

## 7.4 Guidelines and Limitations for ERSPAN

ERSPAN has the following configuration guidelines and limitations:

- The number of ERSPAN sessions per line card reduces to two if the same interface is configured as a bidirectional source in more than one session.
- Only ERSPAN source sessions are supported. Destination sessions are not supported.
- Statistics are not supported for the filter access group.
- An access-group filter in an ERSPAN session must be configured as vlan-accessmap.
- All ERSPAN replication is performed in the hardware. The supervisor CPU is not involved.
- Control plane packets generated by the supervisor cannot be ERSPAN encapsulated or filtered by an ERSPAN access control list (ACL).
- ERSPAN is not supported for management ports.
- ERSPAN does not support destinations on Layer 3 port-channel subinterfaces.
- Supervisor-generated stream of bytes module header (SOBMH) packets have all of the information to go out on an interface and can bypass all forwarding lookups in the hardware, including SPAN and ERSPAN. The Inspur CN129-X636C-R, CN129-X636Q-R and CN129-X6136YC-R line cards both support inband SPAN and local SPAN.
- A VLAN can be part of only one session when it is used as an ERSPAN source or filter.
- VLAN ERSPAN monitors only the traffic that leaves or enters Layer 2 ports in the VLAN.
- If you enable ERSPAN on a vPC and ERSPAN packets need to be routed to the destination through the vPC, packets that come through the vPC peer link cannot be captured.
- ERSPAN is not supported over a VXLAN overlay.
- ERSPAN copies for multicast packets are made prior to rewrite. Therefore, the TTL, VLAN ID, any remarking due to egress policy, and so on are not captured in the ERSPAN copy.
- The timestamp granularity of ERSPAN Type III sessions is not configurable through the CLI. It is 100 picoseconds and driven through PTP.
- ERSPAN works on default and nondefault VRFs, but ERSPAN marker packets work only on the default VRF.

The following guidelines and limitations apply to egress (Tx) ERSPAN:

- The flows for post-routed unknown unicast flooded packets are in the ERSPAN session, even if the ERSPAN session is configured to not monitor the ports on which this flow is forwarded. This limitation applies to Network Forwarding Engine (NFE) and NFE2-enabled EOR switches and ERSPAN sessions that have TX port sources.

The following guidelines and limitations apply to ingress (Rx) ERSPAN:

- VLAN sources are spanned only in the Rx direction.
- Session filtering functionality (VLAN or ACL filters) is supported only for Rx sources.
- VLANs are supported as ERSPAN sources only in the ingress direction.

Priority flow control (PFC) ERSPAN has the following limitations:

- It cannot co-exist with filters.
- It is supported only in the Rx direction on physical or port-channel interfaces. It is not supported in the Rx direction on VLAN interfaces or in the Tx direction.

The following guidelines and limitations apply to ERSPAN truncation:

- Truncation is supported only for local and ERSPAN source sessions. It is not supported for ERSPAN destination sessions.
- For ERSPAN sessions, the configured MTU value excludes the ERSPAN header. The egress packet for ERSPAN will have the MTU value + the number of bytes for the ERSPAN header.
- The bytes specified are retained starting from the header of the packets. The rest are truncated if the packet is longer than the MTU.
- The cyclic redundancy check (CRC) is recalculated for the truncated packet.

## 7.5 Default Settings

The following table lists the default settings for ERSPAN parameters.

**Table 6: Default ERSPAN Parameters**

Parameters	Default
ERSPAN sessions	Created in the shut state
ERSPAN marker packet interval	100 microseconds
Timestamp granularity of ERSPAN Type III sessions	100 picoseconds

## 7.6 Configuring ERSPAN

### 7.6.1 Configuring an ERSPAN Source Session

You can configure an ERSPAN session on the local device only. By default, ERSPAN sessions are created in the shut state.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>monitor erspan origin ip-address ip-address global</b> <b>Example:</b> <pre>switch(config)# monitor erspan origin ip-address 10.0.0.1 global</pre>	Configures the ERSPAN global origin IP address.

	Command or Action	Purpose
<b>Step 3</b>	<p><b>no monitor session</b> {<i>session-number</i>   <b>all</b>}</p> <p><b>Example:</b></p> <pre>switch(config)# no monitor session 3</pre>	<p>Clears the configuration of the specified ERSPAN session.</p> <p>The new session configuration is added to the existing session configuration.</p>
<b>Step 4</b>	<p><b>monitor session</b> {<i>session-number</i>   <b>all</b>} <b>type</b></p> <p><b>erspan-source</b> [<b>shut</b>]</p> <p><b>Example:</b></p> <pre>switch(config)# monitor session 3 type erspan-source switch(config-erspan-src)#</pre>	<p>Configures an ERSPAN Type II source session. By default the session is bidirectional. The optional keyword <b>shut</b> specifies a shut state for the selected session.</p>
<b>Step 5</b>	<p><b>description</b> <i>description</i></p> <p><b>Example:</b></p> <pre>switch(config-erspan-src)# description erspan_src_session_3</pre>	<p>Configures a description for the session. By default, no description is defined. The description can be up to 32 alphanumeric characters.</p>
<b>Step 6</b>	<p><b>source</b> {<b>interface</b> <i>type</i> [<b>rx</b>   <b>tx</b>   <b>both</b>] [<b>allow-pfc</b>]   <b>vlan</b> {<i>number</i>   <i>range</i>} [<b>rx</b>]} [<b>forward-drops rx</b> [<b>priority-low</b>]]</p> <p><b>Example:</b></p> <pre>switch(config-erspan-src)# source interface ethernet 2/1-3, ethernet 3/1 rx</pre> <p><b>Example:</b></p> <pre>switch(config-erspan-src)# source interface ethernet 2/1 rx allow-pfc</pre> <p><b>Example:</b></p> <pre>switch(config-erspan-src)# source interface port-channel 2</pre> <p><b>Example:</b></p> <pre>switch(config-erspan-src)# source interface</pre>	<p>Configures the sources and traffic direction in which to copy packets. You can enter a range of Ethernet ports, a port channel, an inband interface, a range of VLANs, or a satellite port or host interface port channel.</p> <p>You can configure one or more sources, as either a series of comma-separated entries or a range of numbers. You can specify the traffic direction to copy as ingress, egress, or both.</p> <p>The <b>allow-pfc</b> option initiates a span of the priority flow control (PFC) frames that are received on a port. PFC frames are allowed in the ingress pipeline instead of being dropped. If ERSPAN is configured for that port, those PFC frames are spanned to the appropriate egress interface.</p>



	Command or Action	Purpose
	<pre>sup-eth 0 both</pre> <p><b>Example:</b></p> <pre>switch(config-erspan-src)# source vlan 3, 6-8 rx</pre> <p><b>Example:</b></p> <pre>switch(config-erspan-src)# source interface</pre> <pre>ethernet 101/1/1-3</pre> <p><b>Example:</b></p> <pre>switch(config-erspan-src)# source forward-drops rx</pre>	<p>Ports configured with this option can also span normal data traffic. This option supports the spanning of PFC frames only in the Rx direction. An error message appears if you configure <b>allow-pfc</b> with the <b>tx</b> or <b>both</b> option.</p> <p>As an alternative to configuring interfaces or VLANs as an ERSPAN source, you can configure ERSPAN to span the maximum number of forward packet drops possible in the ingress pipeline. Doing so can help you to analyze and isolate packet drops in the network. By default, the <b>source forward-drops rx</b> command captures packet drops for all ports on the network forwarding module. The <b>priority-low</b> option causes this ERSPAN access control entry (ACE) matching drop condition to take a lesser priority to any other ERSPAN session configured with a VLAN source. For a unidirectional session, the direction of the source must match the direction specified in the session.</p> <p><b>Note</b> Source VLANs are supported only in the ingress direction.</p>
<b>Step 7</b>	(Optional) Repeat Step 7 to configure all ERSPAN sources.	—
<b>Step 8</b>	<p>(Optional) <b>filter vlan</b> {<i>number</i>   <i>range</i>}</p> <p><b>Example:</b></p> <pre>switch(config-erspan-src)# filter vlan 3-5, 7</pre>	<p>Configures which VLANs to select from the configured sources. You can configure one or more VLANs, as either a series of comma-separated entries or a range of numbers.</p> <p>For information on the VLAN range, see the <i>Inspur CN12900 Series INOS-CN Layer 2 Switching Configuration Guide</i>.</p>
<b>Step 9</b>	(Optional) Repeat Step 9 to configure all source VLANs	—

	Command or Action	Purpose
	to filter.	
<b>Step 10</b>	<p>(Optional) <b>filter access-group</b> <i>acl-filter</i></p> <p><b>Example:</b></p> <pre>switch(config-erspan-src)# filter access-group ACL1</pre>	<p>Associates an ACL with the ERSPAN session. (You can create an ACL using the standard ACL configuration process. For more information, see the <i>Inspur CN12900 Series INOS-CN Security Configuration Guide</i>.)</p> <p><b>Note</b> You cannot use this command if you have configured ERSPAN to span forward packet drops in the ingress pipeline.</p>
<b>Step 11</b>	<p><b>destination ip</b> <i>ip-address</i></p> <p><b>Example:</b></p> <pre>switch(config-erspan-src)# destination ip 10.1.1.1</pre>	<p>Configures the destination IP address in the ERSPAN session. Only one destination IP address is supported per ERSPAN source session.</p>
<b>Step 12</b>	<p><b>erspan-id</b> <i>erspan-id</i></p> <p><b>Example:</b></p> <pre>switch(config-erspan-src)# erspan-id 5</pre>	<p>Configures the ERSPAN ID for the ERSPAN source session. The ERSPAN range is from 1 to 1023.</p>
<b>Step 13</b>	<p><b>vrf</b> <i>vrf-name</i></p> <p><b>Example:</b></p> <pre>switch(config-erspan-src)# vrf default</pre>	<p>Configures the virtual routing and forwarding (VRF) instance that the ERSPAN source session uses for traffic forwarding. The VRF name can be any case-sensitive, alphanumeric string up to 32 characters.</p>
<b>Step 14</b>	<p>(Optional) <b>ip ttl</b> <i>ttl-number</i></p> <p><b>Example:</b></p> <pre>switch(config-erspan-src)# ip ttl 25</pre>	<p>Configures the IP time-to-live (TTL) value for the ERSPAN traffic. The range is from 1 to 255.</p>
<b>Step 15</b>	<p>(Optional) <b>ip dscp</b> <i>dscp-number</i></p> <p><b>Example:</b></p> <pre>switch(config-erspan-src)# ip dscp 42</pre>	<p>Configures the differentiated services code point (DSCP) value of the packets in the ERSPAN traffic. The range is from 0 to 63.</p>
<b>Step 16</b>	<b>no shut</b>	<p>Enables the ERSPAN source session. By default, the</p>

	Command or Action	Purpose
	<b>Example:</b>  <pre>switch(config-erspan-src)# no shut</pre>	session is created in the shut state.
<b>Step 17</b>	<b>exit</b> <b>Example:</b> <pre>switch(config-erspan-src)# exit switch(config)#</pre>	Exits the monitor configuration mode.
<b>Step 18</b>	(Optional) <b>show monitor session</b> {all   <i>session-number</i>   <b>range</b> <i>session-range</i> } [ <b>brief</b> ] <b>Example:</b> <pre>switch(config)# show monitor session 3</pre>	Displays the ERSPAN session configuration.
<b>Step 19</b>	(Optional) <b>show running-config monitor</b> <b>Example:</b> <pre>switch(config)# show running-config monitor</pre>	Displays the running ERSPAN configuration.
<b>Step 20</b>	(Optional) <b>show startup-config monitor</b> <b>Example:</b> <pre>switch(config)# show startup-config monitor</pre>	Displays the ERSPAN startup configuration.
<b>Step 21</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## 7.6.2 Shutting Down or Activating an ERSPAN Session

You can shut down ERSPAN sessions to discontinue the copying of packets from sources to destinations. You can shut down one session in order to free hardware resources to enable another session. By default, ERSPAN sessions are created in the shut state.

You can enable ERSPAN sessions to activate the copying of packets from sources to destinations. To enable an ERSPAN session that is already enabled but operationally down, you must first shut it down and then enable it. You can shut down and enable the ERSPAN session states with either a global or monitor configuration mode command.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	<b>monitor session</b> { <i>session-range</i>   <b>all</b> } <b>shut</b> <b>Example:</b> <pre>switch(config)# monitor session 3 shut</pre>	Shuts down the specified ERSPAN sessions. By default, sessions are created in the shut state.
<b>Step 3</b>	<b>no monitor session</b> { <i>session-range</i>   <b>all</b> } <b>shut</b> <b>Example:</b> <pre>switch(config)# no monitor session 3 shut</pre>	Resumes (enables) the specified ERSPAN sessions. By default, sessions are created in the shut state. If a monitor session is enabled but its operational status is down, then to enable the session, you must first specify the <b>monitor session shut</b> command followed by the <b>no monitor session shut</b> command.
<b>Step 4</b>	<b>monitor session</b> <i>session-number</i> <b>type</b> <b>erspan-source</b> <b>Example:</b> <pre>switch(config)# monitor session 3 type erspan-source switch(config-erspan-src)#</pre>	Enters the monitor configuration mode for the ERSPAN source type. The new session configuration is added to the existing session configuration.
<b>Step 5</b>	<b>shut</b> <b>Example:</b> <pre>switch(config-erspan-src)# shut</pre>	Shuts down the ERSPAN session. By default, the session is created in the shut state.
<b>Step 6</b>	<b>no shut</b> <b>Example:</b> <pre>switch(config-erspan-src)# no shut</pre>	Enables the ERSPAN session. By default, the session is created in the shut state.
<b>Step 7</b>	<b>exit</b> <b>Example:</b> <pre>switch(config-erspan-src)# exit switch(config)#</pre>	Exits the monitor configuration mode.
<b>Step 8</b>	(Optional) <b>show monitor session all</b> <b>Example:</b> <pre>switch(config)# show monitor session all</pre>	Displays the status of ERSPAN sessions.
<b>Step 9</b>	(Optional) <b>show running-config monitor</b> <b>Example:</b> <pre>switch(config)# show running-config monitor</pre>	Displays the ERSPAN running configuration.

	Command or Action	Purpose
<b>Step 10</b>	(Optional) <b>show startup-config monitor</b>  <b>Example:</b> switch(config)# show startup-config monitor	Displays the ERSPAN startup configuration.
<b>Step 11</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

### 7.6.3 Configuring an ERSPAN ACL

You can create an IPv4 ERSPAN ACL on the device and add rules to it.

#### Before you begin

To modify the DSCP value or the GRE protocol, you need to allocate a new destination monitor session. A maximum of four destination monitor sessions are supported.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>ip access-list <i>acl-name</i></b> <b>Example:</b> switch(config)# ip access-list erspan-acl switch(config-acl)#	Creates the ERSPAN ACL and enters IP ACL configuration mode. The <i>acl-name</i> argument can be up to 64 characters.
<b>Step 3</b>	[ <i>sequence-number</i> ] { <b>permit</b>   <b>deny</b> } <i>protocol source destination</i> [ <b>set-erspan-dscp</b> <i>dscp-value</i> ] [ <b>set-erspan-gre-proto</b> <i>protocol-value</i> ] <b>Example:</b> switch(config-acl)# permit ip 192.168.2.0/24 any set-erspan-dscp 40 set-erspan-gre-proto 5555	Creates a rule in the ERSPAN ACL. You can create many rules. The <i>sequence-number</i> argument can be a whole number between 1 and 4294967295. The <b>permit</b> and <b>deny</b> commands support many ways of identifying traffic. The <b>set-erspan-dscp</b> option sets the DSCP value in the ACL is from 0 to 63. The DSCP value configured in the ERSPAN ACL overrides the value configured in the monitor session. If you do not include this option in the ERSPAN ACL, 0

	Command or Action	Purpose
		<p>or the DSCP value configured in the monitor session will be set.</p> <p>The <b>set-erspan-gre-proto</b> option sets the protocol value in the ERSPAN GRE header. The range for the protocol value is from 0 to 65535. If you do not include this option in the ERSPAN ACL, the default value of 0x88be will be set as the protocol in the GRE header for ERSPAN-encapsulated packets.</p> <p>Each access control entry (ACE) with the <b>set-erspan-gre-proto</b> or <b>set-erspan-dscp</b> action consumes one destination monitor session. A maximum of three ACEs with one of these actions is supported per ERSPAN ACL.</p> <p>For example, you can configure one of the following:</p> <ul style="list-style-type: none"> <li>• One ERSPAN session with an ACL having a maximum of three ACEs with the <b>set-erspan-gre-proto</b> or <b>set-erspan-dscp</b> action</li> <li>• One ERSPAN session with an ACL having two ACEs with the <b>set-erspan-gre-proto</b> or <b>set-erspan-dscp</b> action and one additional local or ERSPAN session</li> <li>• A maximum of two ERSPAN sessions with an ACL having one ACE with the <b>set-erspan-gre-proto</b> or <b>set-erspan-dscp</b> action</li> </ul>
<b>Step 4</b>	(Optional) <b>show ip access-lists</b> <i>name</i> <b>Example:</b> <pre>switch(config-acl)# show ip access-lists erspan-acl</pre>	Displays the ERSPAN ACL configuration.
<b>Step 5</b>	(Optional) <b>show monitor session</b> { <b>all</b>   <i>session-number</i>   <b>range</b> <i>session-range</i> } [ <b>brief</b> ] <b>Example:</b>	Displays the ERSPAN session configuration.

	Command or Action	Purpose
	<code>switch(config-acl)# show monitor session 1</code>	
<b>Step 6</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <code>switch(config-acl)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

## 7.6.4 Configuring UDF-Based ERSPAN

You can configure the device to match on user-defined fields (UDFs) of the outer or inner packet fields (header or payload) and to send the matching packets to the ERSPAN destination. Doing so can help you to analyze and isolate packet drops in the network.

### Before you begin

Make sure that the appropriate TCAM region (racl, ifacl, or vacl) has been configured using the **hardware access-list tcam region** command to provide enough free space to enable UDF-based ERSPAN. For information, see the "Configuring ACL TCAM Region Sizes" section in the *Inspur CN12900 Series INOS-CN Security Configuration Guide*.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <code>switch# configure terminal</code> <code>switch(config)#</code>	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	<p><b>udf</b> <i>udf-name</i> <i>offset-base</i> <i>offset</i> <i>length</i></p> <p><b>Example:</b></p> <pre>switch(config)# udf udf-x packet-start 12 1 switch(config)# udf udf-y header outer 13 20 2</pre>	<p>Defines the UDF as follows:</p> <ul style="list-style-type: none"> <li>• <i>udf-name</i>—Specifies the name of the UDF. You can enter up to 16 alphanumeric characters for the name.</li> <li>• <i>offset-base</i>—Specifies the UDF offset base as follows, where <b>header</b> is the packet header to consider for the offset: <b>packet-start   header {outer   inner {13   14}}</b>.</li> <li>• <i>offset</i>—Specifies the number of bytes offset from the offset base. To match the first byte from the offset base (Layer 3/Layer 4 header), configure the offset as 0.</li> <li>• <i>length</i>—Specifies the number of bytes from the offset.</li> </ul> <p>Only 1 or 2 bytes are supported. To match additional bytes, you must define multiple UDFs. You can define multiple UDFs, but Inspur recommends defining only required UDFs.</p>
<b>Step 3</b>	<p><b>hardware access-list tcam region</b> {<b>racl</b>   <b>ifacl</b>   <b>vacl</b>}</p> <p><b>qualify udf</b> <i>udf-names</i></p> <p><b>Example:</b></p> <pre>switch(config)# hardware access-list tcam region racl qualify udf udf-x udf-y</pre>	<p>Attaches the UDFs to one of the following TCAM regions:</p> <ul style="list-style-type: none"> <li>• <b>racl</b>—Applies to Layer 3 ports.</li> <li>• <b>ifacl</b>—Applies to Layer 2 ports.</li> <li>• <b>vacl</b>—Applies to source VLANs.</li> </ul> <p>You can attach up to 8 UDFs to a TCAM region.</p> <p><b>Note</b> When the UDF qualifier is added, the TCAM region goes from single wide to double wide. Make sure enough free space is available; otherwise, this command will be rejected. If necessary, you can reduce the TCAM space from unused regions and then re-enter this command. For more information, see the "Configuring ACL TCAM Region Sizes" section in the <i>Inspur CN12900 INOS-CN Security Configuration Guide</i>.</p>



	Command or Action	Purpose
		<p><b>Note</b> The <b>no</b> form of this command detaches the UDFs from the TCAM region and returns the region to single wide.</p>
<b>Step 4</b>	<p>Required: <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.
<b>Step 5</b>	<p>Required: <b>reload</b></p> <p><b>Example:</b></p> <pre>switch(config)# reload</pre>	<p>Reloads the device.</p> <p><b>Note</b> Your UDF configuration is effective only after you enter <b>copy running-config startup-config + reload</b>.</p>
<b>Step 6</b>	<p><b>ip access-list erspan-acl</b></p> <p><b>Example:</b></p> <pre>switch(config)# ip access-list erspan-acl-udf-only switch(config-acl)#</pre>	Creates an IPv4 access control list (ACL) and enters IP access list configuration mode.
<b>Step 7</b>	<p>Enter one of the following commands:</p> <ul style="list-style-type: none"> <li>• <b>permit udf udf-name value mask</b></li> <li>• <b>permit ip source destination udf udf-name value mask</b></li> </ul> <p><b>Example:</b></p> <pre>switch(config-acl)# permit udf udf-x 0x40 0xF0 udf-y 0x1001 0xF00F</pre> <p><b>Example:</b></p> <pre>switch(config-acl)# permit ip 10.0.0./24 any udf udf-x 0x02 0x0F udf-y 0x1001 0xF00F</pre>	<p>Configures the ACL to match only on UDFs (example 1) or to match on UDFs along with the current access control entries (ACEs) for the outer packet fields (example 2).</p> <p>A single ACL can have ACEs with and without UDFs together. Each ACE can have different UDF fields to match, or all ACEs can match for the same list of UDFs.</p>
<b>Step 8</b>	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## 7.6.5 Configuring ERSPAN Truncation

You can configure truncation for local and ERSPAN source sessions only.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>monitor session <i>session-number</i></b> <b>Example:</b> <pre>switch(config)# monitor session 5 switch(config-monitor)#</pre>	Enters monitor configuration mode for the specified ERSPAN session.
<b>Step 3</b>	<b>source interface <i>type slot/port [rx   tx   both]</i></b> <b>Example:</b> <pre>switch(config-monitor)# source interface ethernet 1/5 both</pre>	Configures the source interface.
<b>Step 4</b>	<b>mtu <i>size</i></b> <b>Example:</b> <pre>switch(config-monitor)# mtu 512</pre>	Configures the MTU size for truncation. Any ERSPAN packet that is larger than the configured MTU size is truncated to the configured size. The MTU size range is 512 to 1518 bytes
<b>Step 5</b>	<b>destination interface <i>type slot/port</i></b> <b>Example:</b> <pre>switch(config-monitor)# destination interface Ethernet 1/39</pre>	Configures the Ethernet ERSPAN destination port.
<b>Step 6</b>	<b>no shut</b> <b>Example:</b> <pre>switch(config-monitor)# no shut</pre>	Enables the ERSPAN session. By default, the session is created in the shut state.
<b>Step 7</b>	(Optional) <b>show monitor session <i>session</i></b> <b>Example:</b> <pre>switch(config-monitor)# show monitor session 5</pre>	Displays the ERSPAN configuration.
<b>Step 8</b>	<b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config-monitor)# copy running-config</pre>	Copies the running configuration to the startup configuration.

Command or Action	Purpose
startup-config	

## 7.7 Verifying the ERSPAN Configuration

To display the ERSPAN configuration, perform one of the following tasks:

Command	Purpose
<b>show ip access-lists</b> <i>name</i>	Displays the ERSPAN ACL configuration.
<b>show monitor session</b> { <b>all</b>   <i>session-number</i>   <b>range</b> <i>session-range</i> } [ <b>brief</b> ]	Displays the ERSPAN session configuration.  The output includes the egress interface that is used to send the ERSPAN packets. The output varies depending on the type of egress interface used: <ul style="list-style-type: none"> <li>• Physical Layer 3 interface—Displays the interface name.</li> <li>• SVI interface—Displays the member interface through which the route was learned.</li> <li>• Layer 3 port channel—Displays the port-channel interface name.</li> <li>• Layer 3 subinterface—Displays the parent interface name.</li> <li>• ECMP path—Displays the name of one of the equal-cost multipath (ECMP) member interfaces. Only the interface that is displayed will be used for mirroring the traffic even though the route is ECMP.</li> <li>• PFC on interfaces—Displays the priority flow control (PFC) status on the interface.</li> </ul>
<b>show running-config monitor</b>	Displays the running ERSPAN configuration.
<b>show startup-config monitor</b>	Displays the ERSPAN startup configuration.

## 7.8 Configuration Examples for ERSPAN

### 7.8.1 Configuration Example for a Unidirectional ERSPAN Session

This example shows how to configure a unidirectional ERSPAN session:

```
switch# configure terminal
switch(config)# interface ethernet
14/30
switch(config-if)# no shut
switch(config-if)# exit
```

```

switch(config)# no monitor session 3
switch(config)# monitor session 3 rx
switch(config-erspan-src)# source interface ethernet 2/1-3 rx
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 9.1.1.2
switch(config-erspan-src)# no shut
switch(config-erspan-src)# exit
switch(config)# show monitor session 1

```

## 7.8.2 Configuration Example for an ERSPAN ACL

This example shows how to configure an ERSPAN ACL:

```

switch# configure terminal
switch(config)# ip access-list match_11_pkts
switch(config-acl)# permit ip 11.0.0.0 0.255.255.255
any switch(config-acl)# exit
switch(config)# ip access-list match_12_pkts
switch(config-acl)# permit ip 12.0.0.0 0.255.255.255
any switch(config-acl)# exit
switch(config)# vlan access-map erspan_filter 5
switch(config-access-map)# match ip address
match_11_pkts switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# vlan access-map erspan_filter 10
switch(config-access-map)# match ip address
match_12_pkts switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# filter access_group erspan_filter

```

## 7.8.3 Configuration Example for a Marker Packet

This example shows how to enable the ERSPAN marker packet with an interval of 2 seconds:

```

switch# configure terminal
switch(config)# monitor erspan origin ip-address 172.28.15.250 global
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# header-type 3
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 9.1.1.2
switch(config-erspan-src)# source interface ethernet 1/15 both
switch(config-erspan-src)# marker-packet 100
switch(config-erspan-src)# no shut
switch(config-erspan-src)# show monitor session 1
session 1
-----
type          : erspan-source
state         : up
granularity   : nanoseconds
erspan-id     : 1
vrf-name      : default
destination-ip : 9.1.1.2
ip-ttl        : 16
ip-dscp       : 5

```

```

header-type      : 3
origin-ip       : 172.28.15.250 (global)
source intf     :
rx              : Eth1/15
tx              : Eth1/15
both            : Eth1/15
source VLANs   :
rx              :
marker-packet   : enabled
packet interval : 100
packet sent     : 25
packet failed   : 0
egress-intf     :

```

## 7.8.4 Configuration Examples for UDF-Based ERSPAN

This example shows how to configure UDF-based ERSPAN to match on the inner TCP flags of an encapsulated IP-in-IP packet using the following match criteria:

- Outer source IP address: 10.0.0.2
- Inner TCP flags: Urgent TCP flag is set
- Bytes: Eth Hdr (14) + Outer IP (20) + Inner IP (20) + Inner TCP (20, but TCP flags at 13th byte)
- Offset from packet-start: 14 + 20 + 20 + 13 = 67
- UDF match value: 0x20
- UDF mask: 0xFF

```

udf udf_tcpflags packet-start 67 1
hardware access-list tcam region racl qualify udf udf_tcpflags
copy running-config startup-config
reload
ip access-list acl-udf
 permit ip 10.0.0.2/32 any udf udf_tcpflags 0x20 0xff
monitor session 1 type erspan-source
 source interface Ethernet 1/1
 filter access-group acl-udf

```

This example shows how to configure UDF-based ERSPAN to match regular IP packets with a packet signature (DEADBEEF) at 6 bytes after a Layer 4 header start using the following match criteria:

- Outer source IP address: 10.0.0.2
- Inner TCP flags: Urgent TCP flag is set
- Bytes: Eth Hdr (14) + IP (20) + TCP (20) + Payload: 112233445566DEADBEEF7788
- Offset from Layer 4 header start: 20 + 6 = 26
- UDF match value: 0xDEADBEEF (split into two-byte chunks and two UDFs)
- UDF mask: 0xFFFFFFFF

```

udf udf_pktsig_msb header outer 13 26 2
udf udf_pktsig_lsb header outer 13 28 2
hardware access-list tcam region racl qualify udf udf_pktsig_msb
udf_pktsig_lsb copy running-config startup-config
reload
ip access-list acl-udf-pktsig
 permit udf udf_pktsig_msb 0xDEAD 0xFFFF udf udf_pktsig_lsb 0xBEEF
0xFFFF monitor session 1 type erspan-source
 source interface Ethernet 1/1 filter
 access-group acl-udf-pktsig

```

## 7.8.5 Configuration Example for ERSPAN Truncation

This example shows how to configure ERSPAN truncation for use with MPLS stripping:

```

mpls strip
ip access-list mpls
  statistics per-entry
  20 permit ip any any redirect Ethernet1/5

interface Ethernet1/5
  switchport
  switchport mode trunk
  mtu 9216
  no shutdown

monitor session 1
  source interface Ethernet1/5 tx
  mtu 64
  destination interface Ethernet1/6
  no shut
monitor session 21 type erspan-
  source description "ERSPAN Session
  21" header-type 3
  erspan-id 21
  vrf default
  destination ip 19.1.1.2
  source interface Ethernet1/5 tx
  mtu 64
  no shut
monitor session 22 type erspan-
  source description "ERSPAN Session
  22" erspan-id 22
  vrf default
  destination ip 19.2.1.2
  source interface Ethernet1/5 tx
  mtu 750
  no shut
monitor session 23 type erspan-
  source description "ERSPAN Session
  23" header-type 3
  marker-packet 1000
  erspan-id 23
  vrf default
  destination ip 19.3.1.2
  source interface Ethernet1/5 tx
  mtu 1000
  no shut

```

## 7.9 Additional References

### 7.9.1 Related Documents

Related Topic	Document Title
ACL TCAM regions	<i>Inspur CN12900 Series INOS-CN Security Configuration Guide</i>
Precision Time Protocol (PTP)	<i>Inspur CN12900 Series INOS-CN System Management Configuration Guide</i>

## CHAPTER 8 Configuring LLDP

---

This chapter describes how to configure the Link Layer Discovery Protocol (LLDP) in order to discover other devices on the local network.

This chapter contains the following sections:

### 8.1 About LLDP

To permit the discovery of non-Cisco devices, the switch also supports the Link Layer Discovery Protocol (LLDP), a vendor-neutral device discovery protocol that is defined in the IEEE 802.1ab standard. LLDP allows network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.

LLDP is a one-way protocol that transmits information about the capabilities and current status of a device and its interfaces. LLDP devices use the protocol to solicit information only from other LLDP devices.

LLDP supports a set of attributes that it uses to discover other devices. These attributes contain type, length, and value (TLV) descriptions. LLDP devices can use TLVs to send and receive information to other devices on the network. Details such as configuration information, device capabilities, and device identity can be advertised using this protocol.

LLDP advertises the following TLVs by default:

- DCBXP
- Management address
- Port description
- Port VLAN
- System capabilities
- System description
- System name

#### 8.1.1 About DCBXP

The Data Center Bridging Exchange Protocol (DCBXP) is an extension of LLDP. It is used to announce, exchange, and negotiate node parameters between peers. DCBXP parameters are packaged as DCBXP TLVs in the LLDP packet. If CEE is used, DCBXP will use an acknowledgment mechanism over LLDP. When the port comes up, DCBX TLVs are sent and any DCBX TLVs received are processed. By default, the DCBX protocol is set to auto-detect, and the latest protocol version supported by both the peers is used.

Features that need to exchange and negotiate parameters with peer nodes using DCBXP are as follows:

- Priority-based Flow Control (PFC)—PFC is an enhancement to the existing Pause mechanism in Ethernet. It enables Pause based on user priorities or classes of service. A physical link that is divided into eight virtual links with PFC provides the capability to use Pause on a single virtual link without affecting traffic on the other virtual links. Enabling Pause on a per-user-priority basis allows administrators to create lossless links for traffic requiring no-drop service while retaining packet-drop congestion management for IP traffic.
- Enhanced Transmission Selection (ETS) — ETS enables optimal bandwidth management of virtual links. ETS is also called priority grouping. It enables differentiated treatments within the same priority classes of PFC. ETS provides prioritized processing based on bandwidth allocation, low latency, or best effort, resulting in per-group traffic class allocation. For example, an Ethernet class of traffic may have a high-priority designation and a best effort within that same class. ETS allows differentiation between traffic of the same priority class, thus creating priority groups.
- Application Priority Configuration — Carries information about the priorities that are assigned to specific protocols.

- Priority to DSCP Mapping — The mapping of the DSCP and COS values configured in the QoS policy are sent in the Application Priority TLV.

DCBXP is enabled by default, provided LLDP is enabled. When LLDP is enabled, DCBXP can be enabled or disabled using the `[no] lldp tlv-select dcbxp` command. DCBXP is disabled on ports where LLDP transmit or receive is disabled.

### 8.1.2 High Availability

The LLDP feature supports stateless and stateful restarts. After a reboot or supervisor switchover, the running configuration is applied.

For more information on high availability, see the *Inspur CN12900 Series INOS-CN High Availability and Redundancy Guide*.

### 8.1.3 Virtualization Support

One instance of LLDP is supported.

## 8.2 Licensing Requirements for LLDP

Product	License Requirement
Inspur INOS-CN	LLDP requires no license. Any feature not included in a license package is bundled with the INOS-CN image and is provided at no extra charge to you.

## 8.3 Guidelines and Limitations for LLDP

LLDP has the following configuration guidelines and limitations:

- LLDP must be enabled on the device before you can enable or disable it on any interfaces.
- LLDP is supported only on physical interfaces.
- LLDP can discover up to one device per port.
- DCBXP incompatibility messages might appear when you change the network QoS policy if a physical loopback connection is in the device. The incompatibility exists for only a short time and then clears.
- ETS Configuration and Recommendation TLVs are sent only when the input queuing is configured and applied at the system level.
- PFC TLV are sent when pause is enabled for at-least one COS value in network-qos policy and priority-flow-control mode should be auto in the Interface level.

## 8.4 Default Settings for LLDP

This table lists the LLDP default settings.

Parameters	Default
Global LLDP	Disabled
LLDP on interfaces	Enabled, after LLDP is enabled globally
LLDP hold time (before discarding)	120 seconds
LLDP reinitialization delay	2 seconds
LLDP timer (packet update frequency)	30 seconds
LLDP TLVs	Enabled



Parameters	Default
LLDP receive	Enabled, after LLDP is enabled globally
LLDP transmit	Enabled, after LLDP is enabled globally
DCBXP	Enabled, provided LLDP is enabled
DCBXP version	Auto-detect

## 8.5 Configuring LLDP

### 8.5.1 Enabling or Disabling LLDP Globally

You can enable or disable LLDP globally on a device. You must enable LLDP globally to allow a device to send and receive LLDP packets.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>[no] feature lldp</b> <b>Example:</b> switch(config)# feature lldp	Enables or disables LLDP on the device. LLDP is disabled by default.
<b>Step 3</b>	(Optional) <b>show lldp running-config</b> <b>Example:</b> switch(config)# show running-config lldp	Displays the global LLDP configuration. If LLDP is enabled, it shows "feature lldp." If LLDP is disabled, it shows an "Invalid command" error.
<b>Step 4</b>	(Optional) <b>copy startup-config running-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

### 8.5.2 Enabling or Disabling LLDP on an Interface

After you globally enable LLDP, it is enabled on all supported interfaces by default. However, you can enable or disable LLDP on individual interfaces or selectively configure an interface to only send or only receive LLDP packets.

#### Before you begin

Make sure that you have globally enabled LLDP on the device

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>interface</b> <i>interface slot/port</i> <b>Example:</b> switch(config)# interface ethernet 7/1 switch(config-if)#	Specifies the interface on which you are enabling LLDP and enters the interface configuration mode.
<b>Step 3</b>	<b>[no] transmit</b> <b>lldp</b> <b>Example:</b> switch(config-if)# lldp transmit	Enables or disables the transmission of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.
<b>Step 4</b>	<b>[no] lldp receive</b> <b>Example:</b> switch(config-if)# lldp receive	
<b>Step 5</b>	(Optional) <b>show lldp</b> <i>interface slot/port</i> <b>interface</b> <b>Example:</b> switch(config-if)# show lldp interface ethernet 7/1	Displays the LLDP configuration on the interface.
<b>Step 6</b>	(Optional) <b>copy</b> <b>startup-config</b> <b>running-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

### 8.5.3 Configuring the DCBXP Protocol Version

You can specify the protocol version in which the DCBX TLVs are sent.

#### Before you begin

Make sure that you have globally enabled LLDP on the device.

#### Procedure

	Command or Action	Purpose
--	-------------------	---------

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>interface <i>interface slot/port</i></b> <b>Example:</b> <pre>switch(config)# interface ethernet 1/25 switch(config-if)#</pre>	Enters interface configuration mode.
<b>Step 3</b>	<b>lldp dcbx version <i>cee/ieee/auto</i></b> <b>Example:</b> <pre>switch(config-if)#lldp dcbx version cee</pre>	Specifies the protocol version mode sent. <ul style="list-style-type: none"> <li>• The <i>cee</i> variable sets the port to only send TLVs in Converged Enhanced Ethernet (CEE) protocol version.</li> <li>• The <i>ieee</i> variable sets the port to only send TLVs in IEEE 802.1Qaz protocol version.</li> <li>• The <i>auto</i> variable sets the port to send TLVs in the latest protocol version supported by both the peers.</li> </ul> The default is set to <i>auto</i> .

### 8.5.4 Configuring Optional LLDP Parameters

You can configure the frequency of LLDP updates, the amount of time for a receiving device to hold the information before discarding it, and the initialization delay time. You can also select the TLVs to include in LLDP packets.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	(Optional) [no] <b>holdtime</b> <b>lldp</b> <i>seconds</i> <b>Example:</b> <pre>switch(config)# lldp holdtime 200</pre>	Specifies the amount of time in seconds that a receiving device should hold the information that is sent by your device before discarding it.  The range is 10 to 255 seconds; the default is 120 seconds.

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 3</b>	(Optional) <b>[no] reinit <i>seconds</i></b> <b>lldp</b> <b>Example:</b> <pre>switch(config)# lldp reinit 5</pre>	Specifies the delay time in seconds for LLDP to initialize on any interface. The range is 1 to 10 seconds; the default is 2 seconds.
<b>Step 4</b>	(Optional) <b>lldp timer <i>seconds</i></b> <b>[no]</b> <b>Example:</b> <pre>switch(config)# lldp timer 50</pre>	Specifies the transmission frequency of LLDP updates in seconds. The range is 5 to 254 seconds; the default is 30 seconds.
<b>Step 5</b>	(Optional) <b>lldp timers</b> <b>show</b> <b>Example:</b> <pre>switch(config)# show lldp timers</pre>	Displays the LLDP hold time, delay time, and update frequency configuration.
<b>Step 6</b>	(Optional) <b>lldp tlv-select <i>tlv</i></b> <b>[no]</b> <b>Example:</b> <pre>switch(config)# lldp tlv-select system-name</pre>	Specifies the TLVs to send and receive in LLDP packets. The available TLVs are dcbxp, management-address, port-description, port-vlan, system-capabilities, system-description, and system-name. All available TLVs are enabled by default.
<b>Step 7</b>	(Optional) <b>lldp tlv-select</b> <b>show</b> <b>Example:</b> <pre>switch(config)# show lldp tlv-select</pre>	Displays the LLDP TLV configuration.
<b>Step 8</b>	(Optional) <b>running-config startup-config</b> <b>copy</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## 8.6 Verifying the LLDP Configuration

To display the LLDP configuration, perform one of the following tasks:

<b>Command</b>	<b>Purpose</b>
<b>show running-config lldp</b>	Displays the global LLDP configuration.

Command	Purpose
<b>show lldp all</b>	Displays the LLDP DCBXP, transmit and receive configuration for all interfaces.
<b>show lldp interface</b> <i>interface slot/port</i>	Displays the LLDP interface configuration.
<b>show lldp timers</b>	Displays the LLDP hold time, delay time, and update frequency configuration.
<b>show lldp tlv-select</b>	Displays the LLDP TLV configuration.
<b>show lldp dcbx interface</b> <i>interface slot/port</i>	Displays DCBXP TLV information for a specific interface.
<b>show lldp neighbors</b> { <b>detail</b>   <b>interface</b> <i>interface slot/port</i> }	Displays the LLDP neighbor device status.
<b>show lldp traffic</b>	Displays the LLDP counters, including the number of LLDP packets sent and received by the device, the number of discarded packets, and the number of unrecognized TLVs.
<b>show lldp traffic interface</b> <i>interface slot/port</i>	Displays the number of LLDP packets sent and received on the interface.
<b>show qos dcbxp interface</b> <i>interface slot/port</i>	Displays DCBXP information for a specific interface.

## 8.7 Configuration Example for LLDP

This example shows how to enable LLDP on a device; disable LLDP on some interfaces; configure optional parameters such as hold time, delay time, and update frequency; and disable several LLDP TLVs:

```
switch# configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
switch(config)# feature lldp
switch(config)# interface ethernet
7/9
switch(config-if)# no lldp transmit
switch(config-if)# no lldp receive
switch(config-if)# exit
switch(config)# interface ethernet
7/10
switch(config-if)# no lldp transmit
switch(config-if)# no lldp receive
switch(config-if)# exit
switch(config)# lldp holdtime 200
switch(config)# lldp reinit 5
switch(config)# lldp timer 50
switch(config)# no lldp tlv-select port-vlan
switch(config)# no lldp tlv-select system-name
```

## CHAPTER 9 Configuring sFlow

This chapter describes how to configure sFlow on Inspur INOS-CN devices.  
This chapter includes the following sections:

### 9.1 About sFlow

Sampled flow (sFlow) allows you to monitor real-time traffic in data networks that contain switches and routers. It uses the sampling mechanism in the sFlow agent software on switches and routers to monitor traffic and to forward the sample data to the central data collector.

#### 9.1.1 sFlow Agent

The sFlow agent, which is embedded in the Inspur INOS-CN software, periodically samples or polls the interface counters that are associated with a data source of the sampled packets. The data source can be an Ethernet interface, an EtherChannel interface, or a range of Ethernet interfaces. The sFlow agent queries the Ethernet port manager for the respective EtherChannel membership information and also receives notifications from the Ethernet port manager for membership changes.

When you enable sFlow sampling, based on the sampling rate and the hardware internal random number, the ingress packets and egress packets are sent to the CPU as an sFlow-sampled packet. The sFlow agent processes the sampled packets and sends an sFlow datagram to the sFlow analyzer. In addition to the original sampled packet, an sFlow datagram includes information about the ingress port, the egress port, and the original packet length. An sFlow datagram can have multiple sFlow samples.

### 9.2 Licensing Requirements for sFlow

Product	License Requirement
Inspur INOS-CN	sFlow requires no license. Any feature not included in a license package is bundled with the INOS-CN image and is provided at no extra charge to you.

### 9.3 Guidelines and Limitations for sFlow

sFlow has the following guidelines and limitations:

- sFlow export over VXLAN is supported.
- When you enable sFlow for an interface, it is enabled for both ingress and egress. You cannot enable sFlow for only ingress or only egress.

For Inspur CN12900 Series switches with CN129-X636C-R and CN129-X636Q-R line cards, sFlow can be enabled for an interface only in the ingress direction.

- sFlow is not supported on the SVIs.
- sFlow ingress sampling for multicast, broadcast, or unknown unicast packets is supported only for Inspur CN12900 Series switches with CN129-X636C-R, CN129-X636Q-R and CN129-X6136YC-R line cards.
- You should configure the sampling rate based on the sFlow configuration and traffic in the system.
- The switch supports only one sFlow collector.

- sFlow and network address translation (NAT) are not supported on the same port.
- sFlow is supported on the Inspur CN12900 Series switches.
- sFlow is supported on Inspur CN12900 Series switches with CN129-X636C-R, CN129-X636Q-R and CN129-X6136YC-R line cards.
- sFlow and SPAN can co-exist only for Inspur CN12900 Series switches with CN129-X636C-R, CN129-X636Q-R and CN129-X6136YC-R line cards.
- This combination of features is not supported for other Inspur CN12900 Series switches. sFlow and SPAN sessions cannot share data sources.
- If at least one sFlow data source is configured, the SPAN sessions cannot be brought up.
- If at least one SPAN session is configured as **no shut**, sFlow data sources cannot be added.
- The sampling mode used for sFlow is based on an algorithm known as LFSR. Due to the use of LFSR, it is not guaranteed that one in every few packets are sampled with the sampling rate of n. However, the number of packets sampled is equal to the total packets/n over a period of time.
- sFlow supports sampling IPv6 traffic but only on IPv4 collector ports.
- Subinterfaces are not supported for sFlow.

## 9.4 Default Settings for sFlow

The following table lists the default settings for sFlow parameters.

**Table 7: Default sFlow Parameters**

Parameters	Default
sFlow sampling rate	4096
sFlow sampling size	128
sFlow counter poll interval	20
sFlow maximum datagram size	1400
sFlow collector IP address	0.0.0.0
sFlow collector port	6343
sFlow agent IP address	0.0.0.0

## 9.5 Configuring sFlow

### 9.5.1 Enabling sFlow

You must enable the sFlow feature before you can configure sFlow settings on the switch.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>[no] feature sflow</b> <b>Example:</b> <pre>switch(config)# feature sflow</pre>	Enables or disables sFlow.

	Command or Action	Purpose
<b>Step 3</b>	(Optional) <b>show feature</b> <b>Example:</b> switch(config)# show feature	Displays the enabled and disabled features.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

## 9.5.2 Configuring the Sampling Rate

You can configure the sampling rate for sFlow.

### Before you begin

Make sure that you have enabled sFlow.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	[no] <b>sflow sampling-rate <i>sampling-rate</i></b> <b>Example:</b> switch(config)# sflow sampling-rate 50000	Configures the sFlow sampling rate for packets. The <i>sampling-rate</i> can be an integer between 4096 and 1000000000.
<b>Step 3</b>	(Optional) <b>show sflow</b> <b>Example:</b> switch(config)# show sflow	Displays the sFlow configuration.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

## 9.5.3 Configuring the Maximum Sampled Size

You can configure the maximum number of bytes that should be copied from a sampled packet.

### Before you begin

Make sure that you have enabled sFlow.

### Procedure

	Command or Action	Purpose
--	-------------------	---------



	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>[no] sflow max-sampled-size <i>sampling-size</i></b> <b>Example:</b> switch(config)# sflow max-sampled-size 200	Configures the sFlow maximum sampling size. The range for the <i>sampling-size</i> is from 64 to 256 bytes.
<b>Step 3</b>	(Optional) <b>show sflow</b> <b>Example:</b> switch(config)# show sflow	Displays the sFlow configuration.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

## 9.5.4 Configuring the Counter Poll Interval

You can configure the maximum number of seconds between successive samples of the counters that are associated with the data source. A sampling interval of 0 disables counter sampling.

### Before you begin

Make sure that you have enabled sFlow.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>[no] sflow counter-poll-interval <i>poll-interval</i></b> <b>Example:</b> switch(config)# sflow counter-poll-interval 100	Configures the sFlow poll interval for an interface.  The range for the <i>poll-interval</i> is from 0 to 2147483647 seconds.
<b>Step 3</b>	(Optional) <b>show sflow</b> <b>Example:</b> switch(config)# show sflow	Displays the sFlow configuration.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b>	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	<code>switch(config)# copy running-config startup-config</code>	

## 9.5.5 Configuring the Maximum Datagram Size

You can configure the maximum number of data bytes that can be sent in a single sample datagram.

### Before you begin

Make sure that you have enabled sFlow.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <code>switch# configure terminal</code> <code>switch(config)#</code>	Enters global configuration mode.
<b>Step 2</b>	<b>[no] sflow max-datagram-size <i>datagram-size</i></b> <b>Example:</b> <code>switch(config)# sflow max-datagram-size 2000</code>	Configures the sFlow maximum datagram size. The range for the <i>datagram-size</i> is from 200 to 9000 bytes.
<b>Step 3</b>	<b>(Optional) show sflow</b> <b>Example:</b> <code>switch(config)# show sflow</code>	Displays the sFlow configuration.
<b>Step 4</b>	<b>(Optional) copy running-config startup-config</b> <b>Example:</b> <code>switch(config)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

## 9.5.6 Configuring the sFlow Collector Address

You can configure the IPv4 address of the sFlow data collector that is connected to the management port.

### Before you begin

Make sure that you have enabled sFlow.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <code>switch# configure terminal</code> <code>switch(config)#</code>	Enters global configuration mode.
<b>Step 2</b>	<b>[no] sflow collector-ip <i>ip-address</i> vrf <i>vrf</i> [<i>source</i></b>	Configures the IPv4 address for the sFlow collector.

	Command or Action	Purpose
	<p><i>ip-address</i>]</p> <p><b>Example:</b></p> <pre>switch(config)# sflow collector-ip 192.0.2.5 vrf management</pre>	<p>If the IP address is set to 0.0.0.0, all sampling is disabled. The <i>vrf</i> can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>A user-defined VRF name</b>—You can specify a maximum of 32 alphanumeric characters.</li> <li>• <b>vrf management</b>—You must use this option if the sFlow data collector is on the network connected to the management port.</li> <li>• <b>vrf default</b>—You must use this option if the sFlow data collector is on the network connected to the front-panel ports.</li> </ul> <p>The <b>source</b> <i>ip-address</i> option causes the sent sFlow datagram to use the source IP address as the IP packet source address. The source IP address has to be already configured on one of the switch local interfaces; otherwise, an error message appears. If the interface with the source IP address is changed or removed after this option is configured, the sFlow datagram will no longer be sent out, and an event history error and syslog error will be logged. When the source <i>ip-address</i> option is not configured, Inspur INOS-CN picks the IP packet source address automatically for the sent sFlow datagram.</p>
<b>Step 3</b>	<p>(Optional) <b>show sflow</b></p> <p><b>Example:</b></p> <pre>switch(config)# show sflow</pre>	Displays the sFlow configuration.
<b>Step 4</b>	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## 9.5.7 Configuring the sFlow Collector Port

You can configure the destination port for sFlow datagrams.

### Before you begin

Make sure that you have enabled sFlow.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>[no] sflow collector-port <i>collector-port</i></b> <b>Example:</b> <pre>switch(config)# sflow collector-port 7000</pre>	Configures the UDP port of the sFlow collector. The range for the <i>collector-port</i> is from 0 to 65535.
<b>Step 3</b>	<b>(Optional) show sflow</b> <b>Example:</b> <pre>switch(config)# show sflow</pre>	Displays the sFlow configuration.
<b>Step 4</b>	<b>(Optional) copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## 9.5.8 Configuring the sFlow Agent Address

You can configure the IPv4 address of the sFlow agent.

### Before you begin

Make sure that you have enabled sFlow.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>[no] sflow agent-ip <i>ip-address</i></b> <b>Example:</b> <pre>switch(config)# sflow agent-ip 192.0.2.3</pre>	Configures the IPv4 address of the sFlow agent. The default IP address is 0.0.0.0, which means that all sampling is disabled on the switch. You must specify a valid IP address to enable sFlow functionality. <b>Note</b> This IP address is not necessarily the source IP address for sending the sFlow datagram to the collector.
<b>Step 3</b>	<b>(Optional) show sflow</b>	Displays the sFlow configuration.

	Command or Action	Purpose
	<b>Example:</b> <pre>switch(config)# show sflow</pre>	
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## 9.5.9 Configuring the sFlow Sampling Data Source

You can configure the source of the data for the sFlow sampler as an Ethernet port, a range of Ethernet ports, or a port channel.

### Before you begin

Make sure that you have enabled sFlow.

If you want to use a port channel as the data source, make sure that you have already configured the port channel and you know the port channel number.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>[no] sflow data-source interface [ethernet slot/port[-port]   port-channel channel-number]</b> <b>Example:</b> <pre>switch(config)# sflow data-source interface ethernet 1/5-12</pre>	Configures the sFlow sampling data source.  For an Ethernet data source, <i>slot</i> is the slot number, and <i>port</i> can be either a single port number or a range of ports designated as <i>port-port</i> .
<b>Step 3</b>	(Optional) <b>show sflow</b> <b>Example:</b> <pre>switch(config)# show sflow</pre>	Displays the sFlow configuration.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## 9.6 Verifying the sFlow Configuration

Use these commands to display the sFlow configuration.

**Table 8: sFlow Show Commands**

Command	Purpose
<b>show sflow</b>	Displays all the data sources of the sFlow samplers and the sFlow agent configuration.
<b>show process</b>	Verifies whether the sFlow process is running.
<b>show running-config sflow [all]</b>	Displays the current sFlow running configuration.

## 9.7 Monitoring and Clearing sFlow Statistics

Use the **show sflow statistics** command to display the sFlow statistics.

Use the following commands to clear the sFlow statistics:

Command	Description
<b>clear sflow statistics</b>	Clears most of the sFlow statistics from the <b>show sflow statistics</b> command.
<b>clear counters interface all</b>	Clears the Total Packets field from the <b>show sflow statistics</b> command.
<b>clear hardware rate-limiter sflow</b>	Clears the Total Samples field from the <b>show sflow statistics</b> command.

## 9.8 Configuration Examples for sFlow

This example shows how to configure sFlow:

```
feature sflow
sflow sampling-rate 5000 sflow
max-sampled-size 200 sflow
counter-poll-interval 100
sflow max-datagram-size 2000
sflow collector-ip 192.0.2.5 vrf
management sflow collector-port 7000
sflow agent-ip 192.0.2.3
sflow data-source interface ethernet 1/5
```

## 9.9 Additional References

### 9.9.1 Related Documents

Related Topic	Document Title
ACL TCAM regions	Configuring IP ACLs

# CHAPTER 10 Configuring Graceful Insertion and Removal

This chapter describes how to configure graceful insertion and removal (GIR) on the Inspur CN12900 Series switches.

This chapter contains the following sections:

## 10.1 About Graceful Insertion and Removal

You can use graceful insertion and removal to gracefully eject a switch and isolate it from the network in order to perform debugging or upgrade operations. The switch is removed from the regular forwarding path with minimal traffic disruption. When you are finished performing debugging or upgrade operations, you can use graceful insertion to return the switch to its fully operational (normal) mode.

When you place the switch in maintenance mode, all configured Layer 3 control-plane protocols are isolated from the network. Directly connected routes are not withdrawn or modified during this state. When normal mode is restored, the advertisement of all routes is restored.

In graceful removal, all protocols and vPC domains are gracefully brought down and the switch is isolated from the network. In graceful insertion, all protocols and vPC domains are restored.

The following protocols are supported (for both IPv4 and IPv6 address families):

- Border Gateway Protocol (BGP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Intermediate System-to-Intermediate System (ISIS)
- Open Shortest Path First (OSPF)
- Protocol Independent Multicast (PIM)
- Routing Information Protocol (RIP)

### 10.1.1 Profiles

By default, the system isolates all enabled protocols during graceful removal and restores them during graceful insertion. The protocols are isolated and restored in a predefined order.

If you want to isolate, shut down, or restore the protocols individually (or perform additional configurations), you can create a profile with configuration commands that can be applied during graceful removal or graceful insertion. However, you need to make sure that the order of the protocols is correct and any dependencies are considered.

The switch supports the following profiles:

- Maintenance-mode profile—Contains all the commands that will be executed during graceful removal, when the switch enters maintenance mode.
- Normal-mode profile—Contains all the commands that will be executed during graceful insertion, when the switch returns to normal mode.

The following commands (along with any configuration commands) are supported in the profiles.

Command	Description
<b>isolate</b>	Isolates the protocol from the switch and puts the protocol in maintenance mode.
<b>no isolate</b>	Restores the protocol and puts the protocol in normal mode.
<b>shutdown</b>	Shuts down the protocol or vPC domain.

Command	Description
<b>no shutdown</b>	Brings up the protocol or vPC domain.
<b>sleep instance</b> <i>instance-number seconds</i>	Delays the execution of the command by a specified number of seconds. You can delay multiple instances of the command. The range for the <i>instance-number</i> and <i>seconds</i> arguments is from 0 to 2177483647.
<b>python instance</b> <i>instance-number uri</i> [ <i>python-arguments</i> ] Example: <b>python instance 1 bootflash://script1.py</b>	Configures Python script invocations to the profile. You can add multiple invocations of the command to the profile. You can enter a maximum of 32 alphanumeric characters for the Python arguments.

## 10.1.2 Snapshots

In Inspur INOS-CN, a snapshot is the process of capturing the running states of selected features and storing them on persistent storage media.

Snapshots are useful to compare the state of a switch before graceful removal and after graceful insertion. The snapshot process consists of three parts:

- Creating a snapshot of the states of a few preselected features on the switch and storing them on the persistent storage media
- Listing the snapshots taken at various time intervals and managing them
- Comparing snapshots and showing the differences between features

## 10.2 Licensing Requirements for GIR

Product	License Requirement
Inspur INOS-CN	Graceful insertion and removal (GIR) requires no license. Any feature not included in a license package is bundled with the INOS-CN image and is provided at no extra charge to you

## 10.3 Guidelines and Limitations for GIR

Graceful Insertion and Replacement has the following configuration guidelines and limitations:

- Graceful Insertion and Replacement is supported. When moving from normal to maintenance mode, MCT goes down resulting in north to south traffic convergence. Zero packet loss is not supported. The following table provides an example of traffic convergence of 10 VPCs with 2 port member on each VPC port and 60k mac scale.



**Table 9:**

Trigger	Role	North to South Traffic	South to North Traffic
Normal to maintenance mode	Primary	760 ms	1320 ms
Maintenance mode to normal	Primary	13155 ms	27980 ms
Normal to maintenance mode	Secondary	300 ms	1375 ms
Maintenance mode to normal	Secondary	15905 ms	23350 ms

- If you configure the isolate option for OSPF, direct routes and stub routes are advertised as max-metric routes. As a result, north-to-south traffic to the SVI hosts goes through the vPC peer when only one vPC switch is isolated.
- Remove all existing custom profiles before creating new custom profiles for normal-mode and maintenance-mode.

## 10.4 GIR Workflow

Follow these steps to complete the graceful insertion and removal (GIR) workflow:

1. (Optional) Create the maintenance-mode profile. (See Configuring the Maintenance-Mode Profile.)
2. (Optional) Create the normal-mode profile. (See Configuring the Normal-Mode Profile.)
3. Take a snapshot before triggering graceful removal. (See Creating a Snapshot.)
4. Trigger graceful removal to put the switch in maintenance mode. (See Triggering Graceful Removal .)
5. Trigger graceful insertion to return the switch to normal mode. (See Triggering Graceful Insertion.)
6. Take a snapshot after triggering graceful insertion. (See Creating a Snapshot.)
7. Use the **show snapshots compare** command to compare the operational data before and after the graceful removal and insertion of the switch to make sure that everything is running as expected. (See Verifying the GIR Configuration.)

## 10.5 Configuring the Maintenance-Mode Profile

You can create a maintenance-mode profile with configuration commands that can be applied during graceful removal or graceful insertion.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>[no] configure maintenance profile</b></p> <p><b>maintenance-mode</b></p> <p><b>Example:</b></p> <pre>switch# configure maintenance profile maintenance-mode</pre> <p>Enter configuration commands, one per line. End with CNTL/Z.</p>	<p>Enters a configuration session for the maintenance-mode profile. The <b>no</b> option deletes the maintenance profile maintenance-mode.</p> <p>Depending on which protocols you have configured, you must now enter the appropriate commands to bring down the protocols. For a list of supported commands, see Profiles.</p>

	Command or Action	Purpose
	switch(config-mm-profile)#	
<b>Step 2</b>	<b>end</b> <b>Example:</b> switch(config-mm-profile)# end switch#	Closes the maintenance-mode profile.
<b>Step 3</b>	<b>show maintenance profile maintenance-mode</b> <b>Example:</b> switch# show maintenance profile maintenance-mode	Displays the details of the maintenance-mode profile.

**Example**

This example shows how to create a maintenance-mode profile:

```
switch# configure maintenance profile maintenance-mode

Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# ip pim isolate
switch(config-mm-profile)# vpc domain 10
switch(config-mm-profile-config-vpc-domain)# shutdown
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# shutdown
switch(config-mm-profile)# router eigrp 10
switch(config-mm-profile-router)# shutdown
switch(config-mm-profile-router)# address-family ipv6 unicast
switch(config-mm-profile-router-af)# shutdown
switch(config-mm-profile)# system interface shutdown
switch(config-mm-profile)# end
```

```
Exit maintenance profile mode.
switch# show maintenance profile maintenance-mode

[Maintenance Mode] ip
pim isolate
vpc domain 10
  shutdown
router bgp 100
  shutdown
router eigrp 10
  shutdown
  address-family ipv6 unicast
    shutdown
system interface shutdown
```

This example shows how to configure sleep instance in a custom profile to add a delay before the next protocol change.

```
switch# configure maintenance profile maintenance-mode

Enter configuration commands, one per line. End with CNTL/Z.

switch(config-mm-profile)# router bgp 65001
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# sleep instance 1 10
switch(config-mm-profile)# router eigrp 200
```

```

switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# sleep instance 2 15
switch(config-mm-profile)# router ospf 100
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# sleep instance 3 20
switch(config-mm-profile)# router ospfv3 300
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# sleep instance 4 5
switch(config-mm-profile)# router isis 400
switch(config-mm-profile-router)# isolate
switch(config-mm-profile)#end
Exit maintenance profile
mode.
switch#

```

## 10.6 Configuring the Normal-Mode Profile

You can create a normal-mode profile with configuration commands that can be applied during graceful removal or graceful insertion.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>[no] configure maintenance profile normal-mode</b></p> <p><b>Example:</b></p> <pre> switch# configure maintenance profile normal-mode  Enter configuration commands, one per line. End with CNTL/Z.  switch(config-mm-profile)# </pre>	<p>Enters a configuration session for the normal-mode profile.</p> <p>The <b>no</b> version removes the maintenance profile normal-mode.</p> <p>Depending on which protocols you have configured, you must now enter the appropriate commands to bring up the protocols. For a list of supported commands, see Profiles.</p>
<b>Step 2</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre> switch(config-mm-profile)# end switch# </pre>	Closes the normal-mode profile.
<b>Step 3</b>	<p><b>show maintenance profile normal-mode</b></p> <p><b>Example:</b></p> <pre> switch# show maintenance profile normal-mode </pre>	Displays the details of the normal-mode profile.

### Example

This example shows how to create a maintenance-mode profile:

```

switch# configure maintenance profile normal-mode
switch(config-mm-profile)# no system interface shutdown
switch(config-mm-profile)# router eigrp 10

```

```

switch(config-mm-profile-router)# no shutdown
switch(config-mm-profile-router)# address-family ipv6 unicast
switch(config-mm-profile-router-af)# no shutdown
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# no shutdown
switch(config-mm-profile)# vpc domain 10
switch(config-mm-profile-config-vpc-domain)# no shutdown
switch(config-mm-profile)# no ip pim isolate
switch(config-mm-profile)# end

```

```

Exit maintenance profile mode.
switch# show maintenance profile normal-mode
[Normal Mode]
no system interface
shutdown router eigrp 10
no shutdown
address-family ipv6
unicast no shutdown
router bgp 100
no shutdown
vpc domain 10
no shutdown
no ip pim isolate

```

## 10.7 Creating a Snapshot

You can create a snapshot of the running states of selected features. When you create a snapshot, a predefined set of **show** commands are run and the outputs are saved.

### Procedure

	Command or Action	Purpose
Step 1	<p><b>snapshot create</b> <i>snapshot-name description</i></p> <p><b>Example:</b></p> <pre> switch# snapshot create snap_before_maintenance Taken before maintenance  Executing 'show interface'... Done Executing 'show ip route summary vrf all'... Done Executing 'show ipv6 route summary vrf all'... Done Executing 'show bgp sessions vrf all'... Done Executing 'show ip eigrp topology summary'... Done Executing 'show ipv6 eigrp topology summary'... Done Feature 'vpc' not enabled, skipping... Executing 'show ip ospf vrf all'... Done Feature 'ospfv3' not enabled, skipping... Feature 'isis' not enabled, skipping... Feature 'rip' not enabled, skipping... Snapshot 'snap_before_maintenance' created </pre>	<p>Captures the running state or operational data of selected features and stores the data on persistent storage media.</p> <p>You can enter a maximum of 64 alphanumeric characters for the snapshot name and a maximum of 254 alphanumeric characters for the description.</p> <p>Use the <b>snapshot delete</b> <b>{all   <i>snapshot-name</i>}</b> command to delete all snapshots or a specific snapshot.</p>
Step 2	<b>show snapshots</b>	Displays snapshots present on the switch.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>switch# show snapshots      Time Snapshot Name   Description ----- snap_before_maintenance   Wed Aug 19 13:53:28 2015 Taken before maintenance</pre>	
<b>Step 3</b>	<p><b>show snapshots compare <i>snapshot-name-1</i> <i>snapshot-name-2</i> [summary   ipv4routes   ipv6routes]</b></p> <p><b>Example:</b></p> <pre>switch# show snapshots compare snap_before_maintenance snap_after_maintenance</pre>	<p>Displays a comparison of two snapshots. The <b>summary</b> option displays just enough information to see the overall changes between the two snapshots. The <b>ipv4routes</b> and <b>ipv6routes</b> options display the changes in IPv4 and IPv6 routes between the two snapshots.</p>

### Example

The following example shows a summary of the changes between two snapshots:

```
switch# show snapshots compare snapshot1 snapshot2 summary
feature                               snapshot1    snapshot2    changed
basic summary
  # of interfaces                      16           12           *
  # of vlans                            10           4            *
  # of ipv4 routes                      33           3            *
.....
interfaces
  # of eth interfaces                   3            0            *
  # of eth interfaces up                 2            0            *
  # of eth interfaces down               1            0            *
  # of eth interfaces other              0            0
  # of vlan interfaces                   3            1            *
  # of vlan interfaces up                 3            1            *
  # of vlan interfaces down              0            0
  # of vlan interfaces other             0            1            *
.....
```

The following example shows the changes in IPv4 routes between two snapshots:

```
switch# show snapshots compare snapshot1 snapshot2 ipv4routes
metric                               snapshot1    snapshot2    changed
# of routes                           33           3            *
# of adjacencies                       10           4            *

Prefix                               Changed Attribute
-----                               -
23.0.0.0/8                            not in snapshot2
```

```

10.10.10.1/32      not in snapshot2
21.1.2.3/8        adjacency index has changed from 29 (snapshot1) to 38 (snapshot2)
.....
There were 28 attribute changes detected

```

## 10.8 Adding Show Commands to Snapshots

You can specify additional **show** commands to be captured in snapshots. These **show** commands are defined in user-specified snapshot sections.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>snapshot section add</b> <i>section</i> "<i>show-command</i>"  <i>row-id</i>  <i>element-key1</i> [<i>element-key2</i>]</p> <p><b>Example:</b></p> <pre>switch# snapshot section add myshow "show ip interface brief" ROW_intf intf-name</pre>	<p>Adds a user-specified section to snapshots. The <i>section</i> is used to name the <b>show</b> command output. You can use any word to name the section.</p> <p>The <b>show</b> command must be enclosed in quotation marks. Non-<b>show</b> commands will not be accepted. The <i>row-id</i> argument specifies the tag of each row entry of the <b>show</b> command's XML output. The <i>element-key1</i> and <i>element-key2</i> arguments specify the tags used to distinguish among row entries. In most cases, only the <i>element-key1</i> argument needs to be specified to be able to distinguish among row entries.</p> <p><b>Note</b> To delete a user-specified section from snapshots, use the <b>snapshot section delete</b> <i>section</i> command.</p>
<b>Step 2</b>	<p><b>show snapshots sections</b></p> <p><b>Example:</b></p> <pre>switch# show snapshots sections</pre>	<p>Displays the user-specified snapshot sections.</p>
<b>Step 3</b>	<p><b>show snapshots compare</b> <i>snapshot-name-1</i>  <i>snapshot-name-2</i> [<b>summary</b>   <b>ipv4routes</b>   <b>ipv6routes</b>]</p> <p><b>Example:</b></p> <pre>switch# show snapshots compare snap1 snap2</pre>	<p>Displays a comparison of two snapshots. The <b>summary</b> option displays just enough information to see the overall changes between the two snapshots. The <b>ipv4routes</b> and <b>ipv6routes</b> options display the changes</p>

	Command or Action	Purpose
		in IPv4 and IPv6 routes between the two snapshots.

**Example**

The following example adds the **show ip interface brief** command to the myshow snapshot section. It also compares two snapshots (snap1 and snap2) and shows the user-specified sections in both snapshots.

```

switch# snapshot section add myshow "show ip interface brief" ROW_intf intf-name
switch# show snapshots sections
user-specified snapshot sections
-----
[myshow]
  cmd: show ip interface brief
  row: ROW_intf
  key1: intf-name
  key2: -

[sect2]
  cmd: show ip ospf vrf all
  row: ROW_ctx
  key1: instance_number
  key2: cname

switch# show snapshots compare snap1 snap2
=====
Feature                Tag                snap1                snap2
=====
[bgp]
-----

[interface]
-----

  [interface:mgmt0]
                vdc_lvl_in_pkts                692310                **692317**
                vdc_lvl_in_mcast                575281                **575287**
                vdc_lvl_in_bcast                77209                 **77210**
                vdc_lvl_in_bytes                63293252              **63293714**
                vdc_lvl_out_pkts                41197                 **41198**
                vdc_lvl_out_ucast                33966                 **33967**
                vdc_lvl_out_bytes                6419714               **6419788**

[ospf]
-----

[myshow]
-----

  [interface:Ethernet1/1]
                state                up                **down**
                admin_state            up                **down**
.....

```

## 10.9 Triggering Graceful Removal

In order to perform debugging or upgrade operations, you can trigger a graceful removal of the switch, which will eject the switch and isolate it from the network.

### Before you begin

If you want the system to use a maintenance-mode profile that you create, see [Configuring the Maintenance-Mode Profile](#).

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>system mode maintenance [dont-generate-profile   timeout value   shutdown   on-reload reset-reason reason]</b> <b>Example:</b> <pre>switch(config)# system mode maintenance Following configuration will be applied:  ip pim isolate  router bgp 65502   isolate  router ospf p1   isolate  router ospfv3 p1   isolate  Do you want to continue (y/n)? [no] <b>y</b>  Generating a snapshot before going into maintenance mode  Starting to apply commands...  Applying : ip pim isolate Applying : router bgp 65502</pre>	Puts all enabled protocols in maintenance mode (using the <b>isolate</b> command).  The following options are available: <ul style="list-style-type: none"> <li>• <b>dont-generate-profile</b>—Prevents the dynamic searching of enabled protocols and executes commands configured in a maintenance-mode profile. Use this option if you want the system to use a maintenance-mode profile that you have created.</li> <li>• <b>timeout value</b>—Keeps the switch in maintenance mode for a specified number of minutes. The range is from 5 to 65535. Once the configured time elapses, the switch returns to normal mode automatically. The <b>no system mode maintenance timeout</b> command disables the timer.</li> <li>• <b>shutdown</b>—Shuts down all protocols, vPC domains, and interfaces except the management interface (using the <b>shutdown</b> command). This option is disruptive while the default (which uses the <b>isolate</b> command) is</li> </ul>



	Command or Action	Purpose
	<pre>Applying : isolate Applying : router ospf p1 Applying : isolate Applying : router ospfv3 p1 Applying : isolate  Maintenance mode operation successful.</pre>	<p>not.</p> <ul style="list-style-type: none"> <li>• <b>on-reload reset-reason</b> <i>reason</i>—Boots the switch into maintenance mode automatically in the event of a specified system crash. The <b>no system mode maintenance on-reload reset-reason</b> command prevents the switch from being brought up in maintenance mode in the event of a system crash. The maintenance mode reset reasons are as follows: <ul style="list-style-type: none"> <li>• HW_ERROR—Hardware error</li> <li>• SVC_FAILURE—Critical service failure</li> <li>• KERN_FAILURE—Kernel panic</li> <li>• WDOG_TIMEOUT—Watchdog timeout</li> <li>• FATAL_ERROR—Fatal error</li> <li>• LC_FAILURE—Line card failure</li> <li>• MATCH_ANY—Any of the above reasons</li> </ul> </li> </ul> <p>The system prompts you to continue. Enter <b>y</b> to continue or <b>n</b> to terminate the process.</p>
<b>Step 3</b>	<p>(Optional) <b>show system mode</b></p> <p><b>Example:</b></p> <pre>switch(config)# show system mode  System Mode: Maintenance</pre>	<p>Displays the current system mode. The switch is in maintenance mode. You can now perform any desired debugging or upgrade operations on the switch.</p>
<b>Step 4</b>	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>	<p>Copies the running configuration to the startup configuration. This command is required if you want to preserve maintenance mode following a reboot.</p>

### Example

This example shows how to shut down all protocols, vPC domains, and interfaces on the switch:

```
switch(config)# system mode maintenance shutdown
```

Following configuration will be applied:

```
vpc domain 10
shutdown
```

```

router bgp 65502
 shutdown
router ospf p1
 shutdown
router ospfv3
 p1 shutdown
system interface shutdown
Do you want to continue (y/n)? [no] y

Generating a snapshot before going into maintenance mode

Starting to apply commands...

Applying : vpc domain 10
Applying : shutdown
Applying : router bgp 65502
Applying : shutdown
Applying : router ospf p1
Applying : shutdown
Applying : router ospfv3 p1
Applying : shutdown
Applying : shutdown

Maintenance mode operation successful.

```

This example shows how to automatically boot the switch into maintenance mode if a fatal error occurs:

```
switch(config)# system mode maintenance on-reload reset-reason fatal_error
```

## 10.10 Triggering Graceful Insertion

When you finish performing any debugging or upgrade operations, you can trigger a graceful insertion to restore all protocols.

### Before you begin

If you want the system to use a normal-mode profile that you create, see [Configuring the Maintenance-Mode Profile](#).

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>no system mode maintenance [dont-generate-profile]</b> <b>Example:</b> <pre>switch(config)# no system mode maintenance dont-generate-profile</pre> <p>Following configuration will be applied:</p> <pre>no ip pim isolate</pre>	Puts all enabled protocols in normal mode (using the <b>no isolate</b> command). The <b>dont-generate-profile</b> option prevents the dynamic searching of enabled protocols and executes commands configured in a normal-mode profile. Use this option if you want the system to use a normal-mode profile that you have

	Command or Action	Purpose
	<pre> router bgp 65502   no isolate router ospf pl   no isolate router ospfv3 pl   no isolate Do you want to continue (y/n)? [no] <b>y</b>  Starting to apply commands...  Applying : no ip pim isolate Applying : router bgp 65502 Applying : no isolate Applying : router ospf pl Applying : no isolate Applying : router ospfv3 pl Applying : no isolate Maintenance mode operation successful. Generating Current Snapshot </pre>	<p>created.</p> <p>The system prompts you to continue. Enter <b>y</b> to continue or <b>n</b> to terminate the process.</p>
<b>Step 3</b>	<p>(Optional) <b>show system mode</b></p> <p><b>Example:</b></p> <pre> switch(config)# show system mode System Mode: Normal </pre>	<p>Displays the current system mode. The switch is now in normal mode and is fully operational.</p>

## 10.11 Maintenance Mode Enhancements

The following maintenance mode enhancements have been added to Inspur CN12900 Series switches:

- In the system maintenance shutdown mode, the following message is added:

NOTE: The command `system interface shutdown` will shutdown all interfaces excluding `mgmt 0`.

- Entering the CLI command, **system mode maintenance** checks and sends alerts for the orphan ports.
- In isolate mode, when the vPC is configured, the following message is added:

NOTE: If you have vPC orphan interfaces, please ensure `vpc orphan-port suspend` is configured under them, before proceeding further.

- Custom Profile Configuration: A new CLI command, **system mode maintenance always-use-custom-profile** is added for custom profile configuration. A new CLI command, **system mode maintenance non-interactive** is added for Inspur CN12900 Series switches only. It provides a way to facilitate the transition to maintenance mode or normal mode without confirmation being done or each step being printed on the CLI session.

When you create a custom profile (in maintenance or normal mode), it displays the following message:

Please use the command **system mode maintenance always-use-custom-profile** if you want to always use the custom profile.

- A delay has been added before the `after_maintenance` snapshot is taken. The **no system mode maintenance** command exits once all the configuration for the normal mode has been applied, the mode has been changed to normal mode, and a timer has been started to take the `after_maintenance` snapshot. Once the timer expires, the `after_maintenance` snapshot is taken in the background and a new warning `syslog, MODE_SNAPSHOT_DONE` is sent once the snapshot is complete.

The final output of the CLI command **no system mode maintenance** indicates when the `after_maintenance` snapshot is generated:

The `after_maintenance` snapshot will be generated in `<delay>` seconds. After that time, please use `show snapshots compare before_maintenance after_maintenance` to check the health of the system. The timer delay for the `after_maintenance` snapshot is defaulted to 120 seconds but it can be changed by a new configuration command.

The new configuration command to change the timer delay for the `after_maintenance` snapshot is **system mode maintenance snapshot-delay <seconds>**. This configuration overrides the default setting of 120 seconds to any value between 0 and 65535 and it is displayed in the ASCII configuration.

A new show command, **show maintenance snapshot-delay** has also been added to display the current `snapshot-delay` value. This new show command supports the XML output.

- A visible CLI indicator has been added to display when the system is in the maintenance mode, for example, `switch(maint-mode)#`.
- Support for the SNMP traps has been added when the device moves from the maintenance mode to the normal mode and vice-versa through CLI reload, or system reset. The **snmp-server enable traps mmode cseMaintModeChangeNotify** trap is added to enable changing to the maintenance mode trap notification.

The **snmp-server enable traps mmode cseNormalModeChangeNotify** is added to enable changing to the normal mode trap notification. Both the traps are disabled by default.

## 10.12 Verifying the GIR Configuration

To display the GIR configuration, perform one of the following tasks:

Command	Purpose
<b>show interface brief</b>	Displays abbreviated interface information.
<b>show maintenance on-reload reset-reasons</b>	Displays the reset reasons for which the switch comes up in maintenance mode. For a description of the maintenance mode reset reasons, see <a href="#">Triggering Graceful Removal</a> .
<b>show maintenance profile</b> [ <b>maintenance-mode</b>   <b>normal-mode</b> ]	Displays the details of the maintenance-mode or normal-mode profile.
<b>show maintenance timeout</b>	Displays the maintenance-mode timeout period, after which the switch automatically returns to normal mode.
<b>show</b> { <b>running-config</b>   <b>startup-config</b> } <b>mmode</b> [ <b>all</b> ]	Displays the maintenance-mode section of the running or startup configuration. The <b>all</b> option includes the default values.
<b>show snapshots</b> <b>show snapshots compare</b> <i>snapshot-name-1</i> <i>snapshot-name-2</i> [ <b>summary</b>   <b>ipv4routes</b>   <b>ipv6routes</b> ]	Displays snapshots present on the switch. Displays a comparison of two snapshots. The <b>summary</b> option displays just enough information to see the overall changes between the two snapshots. The <b>ipv4routes</b> and <b>ipv6routes</b> options display the changes in IPv4 and IPv6 routes between the two snapshots.
<b>show snapshots dump</b> <i>snapshot-name</i>	Displays the content of each file that was generated

Command	Purpose
<b>show snapshots sections</b>	when the snapshot was taken. Displays the user-specified snapshot sections.
<b>show system mode</b>	Displays the current system mode.

## 10.13 Configuration Examples for GIR

The **redistribute direct** configuration under Border Gateway Protocol (BGP) will attract traffic as the BGP isolate mode does not withdraw direct routes. This example shows how to use the **route-map** command to enable BGP to withdraw direct routes in isolate mode.

### Policy Configuration

Use the **route-map my-rmap-deny** command in maintenance mode to exclude SVIs with a tag 200 configuration.

```
switch(config)# route-map my-rmap-deny deny 10
switch(config-route-map)# match tag 200
switch(config-route-map)# exit
switch(config)# route-map my-rmap-deny permit 20
```

Use the **route-map my-rmap-permit** command in normal mode to include SVIs with a tag 200 configuration.

```
switch(config)# route-map my-rmap-permit permit 10
switch(config-route-map)# match tag 200
switch(config-route-map)# exit
switch(config)# route-map my-rmap-permit permit 20
```

### Virtual IP (vIP)/Switch Virtual Interface (SVI) Configuration

```
switch(config)# interface loopback 200
switch(config-if)# ip address 192.0.2.100/8 tag 200
switch(config)# interface vlan 2 switch(config-if)#
ip address 192.0.2.108/8 tag 200
....
switch(config)# interface vlan 3 switch(config-if)#
ip address 192.0.2.102/8 tag 200
```

### BGP Configuration

```
switch(config)# feature bgp switch(config)#
router bgp 100 switch(config-router)# neighbor
192.0.2.100
....
```

### Maintenance Mode Profile

```
switch# configure maintenance profile maintenance-mode
switch(config-mm-profile)# router bgp 200
switch(config-mm-profile-router)# address-family ipv4 unicast
switch(config-mm-profile-router-af)# redistribute direct route-map my-rmap-deny
switch(config-mm-profile-router-af)# exit
switch(config-mm-profile)# sleep instance 1 10
```

### Normal Mode Profile

```
switch# configure maintenance profile normal-mode
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# address-family ipv4 unicast
```

```
switch(config-mm-profile-router-af)# redistribute direct route-map my-rmap-permit
switch(config-mm-profile-router-af)# exit
switch(config-mm-profile)# sleep instance 1 20
```

# CHAPTER 11 Configuring Rollback

---

This chapter describes how to configure rollback on Inspur INOS-CN devices. This chapter contains the following sections:

## 11.1 About Rollbacks

A rollback allows you to take a snapshot, or user checkpoint, of the Inspur INOS-CN configuration and then reapply that configuration to your device at any point without having to reload the device. A rollback allows any authorized administrator to apply this checkpoint configuration without requiring expert knowledge of the features configured in the checkpoint.

Inspur INOS-CN automatically creates system checkpoints. You can use either a user or system checkpoint to perform a rollback.

You can create a checkpoint copy of the current running configuration at any time. Inspur INOS-CN saves this checkpoint as an ASCII file which you can use to roll back the running configuration to the checkpoint configuration at a future time. You can create multiple checkpoints to save different versions of your running configuration.

When you roll back the running configuration, you can trigger the following rollback types:

- atomic—Implement a rollback only if no errors occur.
- best-effort—Implement a rollback and skip any errors.
- stop-at-first-failure—Implement a rollback that stops if an error occurs.

The default rollback type is atomic.

When you are ready to roll back to a checkpoint configuration, you can view the changes that will be applied to your current running configuration before committing to the rollback operation. If an error occurs during the rollback operation, you can choose to cancel the operation, or ignore the error and proceed with the rollback. If you cancel the operation, Inspur INOS-CN provides a list of changes already applied before the error occurred. You need to clean up these changes manually.

### 11.1.1 Automatically Generated System Checkpoints

The Inspur INOS-CN software automatically generates system checkpoints to help you avoid a loss of configuration information. System checkpoints are generated by the following events:

- Disabling an enabled feature with the **no feature** command
- Removing an instance of a Layer 3 protocol, such as with the **no router bgp** command or the **no ip pim sparse-mode** command
- License expiration of a feature

If one of these events causes system configuration changes, the feature software creates a system checkpoint that you can use to roll back to the previous system configuration. The system generated checkpoint filenames begin with “system-” and include the feature name. For example, the first time that you disable the EIGRP feature, the system creates the checkpoint named `system-fm-__inst_1__eigrp`.

### 11.1.2 High Availability

Whenever a checkpoint is created using the `checkpoint` or `checkpoint checkpoint_name` commands, the checkpoint is synchronized to the standby unit.

A rollback remembers the states of the checkpoint operation, so if the checkpoint operation is interrupted and the system is left in an inconsistent state, a rollback can complete the checkpoint operation (synchronize the checkpoint with the standby unit) before proceeding with the rollback operation.

Your checkpoint files are still available after a process restart or supervisor switchover. Even if there is an interruption during the process restart or supervisor switchover, the checkpoint will complete successfully before

proceeding with the operation. In a supervisor switchover, the checkpoint is completed on the new active unit.

If a process restart or supervisor switchover occurs during a rollback operation, after the restart or switchover completes, the rollback will resume from its previous state and complete successfully.

### 11.1.3 Virtualization Support

Inspur INOS-CN creates a checkpoint of the running configuration. You can create different checkpoint copies.

## 11.2 Licensing Requirements for Rollbacks

Product	License Requirement
Inspur INOS-CN	The rollback feature requires no license. Any feature not included in a license package is bundled with the INOS-CN image and is provided at no extra charge to you.

To configure rollback, you must have network-admin user privileges.

## 11.3 Guidelines and Limitations for Rollbacks

Rollbacks have the following configuration guidelines and limitations:

- You can create up to ten checkpoint copies.
- Your checkpoint filenames must be 80 characters or less.
- You cannot start a checkpoint filename with the word system.
- You can start a checkpoint filename with the word auto.
- You can name a checkpoint file summary or any abbreviation of the word summary.
- Only one user can perform a checkpoint, rollback, or copy the running configuration to the startup configuration at the same time.
- After the system executes the **write erase** or **reload** command, checkpoints are deleted. You can use the **clear checkpoint database** command to clear out all checkpoint files.
- Although a rollback is not supported for checkpoints across software versions, users can perform a rollback at their own discretion and can use the best-effort mode to recover from errors.
- When checkpoints are created on bootflash, differences with the running-system configuration cannot be performed before performing the rollback, and the system reports “No Changes.”
- Checkpoints created using the **checkpoint** and **checkpoint *checkpoint\_name*** commands are present upon a switchover.
- Checkpoints are present upon reload unless a **write-erase** command is issued before a reload.
- A rollback to files on bootflash is supported only on files created using the **checkpoint *checkpoint\_name*** command and not on any other type of ASCII file.
- Checkpoint names must be unique. You cannot overwrite previously saved checkpoints with the same name.
- Rollback is not supported in the context of auto configurations. Checkpoints do not store auto configurations. Therefore, after a rollback is performed, the corresponding auto configurations will not be present

## 11.4 Default Settings for Rollbacks

This table lists the default settings for rollback parameters.



Parameters	Default
Rollback type	Atomic

## 11.5 Configuring Rollbacks

### 11.5.1 Creating a Checkpoint

You can create up to ten checkpoints of your configuration.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>[no] checkpoint</b> <i>{[cp-name] [description descr]   file file-name }</i></p> <p><b>Example:</b></p> <pre>switch# checkpoint stable</pre>	<p>Creates a checkpoint of the running configuration to either a user checkpoint name or a file. The checkpoint name can be any alphanumeric string up to 80 characters but cannot contain spaces. If you do not provide a name, Inspur INOS-CN sets the checkpoint name to <i>user-checkpoint-number</i> where <i>number</i> is from 1 to 10. The description can contain up to 80 alphanumeric characters, including spaces. You can use the <b>no</b> form of the <b>checkpoint</b> command to remove a checkpoint name. Use the <b>delete</b> command to remove a checkpoint file.</p>
<b>Step 2</b>	<p>(Optional) <b>show checkpoint</b> <i>cp-name [all]</i></p> <p><b>Example:</b></p> <pre>switch# show checkpoint stable</pre>	<p>Displays the contents of the checkpoint name.</p>

### 11.5.2 Implementing a Rollback

You can implement a rollback to a checkpoint name or file. Before you implement a rollback, you can view the differences between source and destination checkpoints that reference current or saved configurations.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>show diff rollback-patch</b> <i>{checkpoint src-cp-name   running-config   startup-config   file source-file} {checkpoint dest-cp-name   running-config   startup-config   file dest-file}</i></p> <p><b>Example:</b></p> <pre>switch# show diff rollback-patch checkpoint stable</pre>	<p>Displays the differences between the source and destination checkpoint selections.</p>

	Command or Action	Purpose
	<code>running-config</code>	
<b>Step 2</b>	<b>rollback running-config</b> { <b>checkpoint</b> <i>cp-name</i>   <b>file</b> <i>cp-file</i> } [ <b>atomic</b>   <b>best-effort</b>   <b>stop-at-first-failure</b> ] <b>Example:</b> <pre>switch# rollback running-config checkpoint stable</pre>	<p>Creates a rollback to the specified checkpoint name or file.</p> <p>You can implement the following rollback types:</p> <ul style="list-style-type: none"> <li>• <b>atomic</b>—Implement a rollback only if no errors occur.</li> <li>• <b>best-effort</b>—Implement a rollback and skip any errors.</li> <li>• <b>stop-at-first-failure</b>—Implement a rollback that stops if an error occurs.</li> </ul> <p>The default is atomic.</p> <p>This example shows how to implement a rollback to a user checkpoint name.</p>

## 11.6 Verifying the Rollback Configuration

To display the rollback configuration information, perform one of the following tasks:

Command	Purpose
<b>show checkpoint</b> <i>name</i> [ <b>all</b> ]	Displays the contents of the checkpoint name.
<b>show checkpoint all</b> [ <b>user</b>   <b>system</b> ]	Displays the contents of all checkpoints. You can limit the displayed checkpoints to user or system generated checkpoints.
<b>show checkpoint summary</b> [ <b>user</b>   <b>system</b> ]	Displays a list of all checkpoints. You can limit the displayed checkpoints to user or system generated checkpoints.
<b>show diff rollback-patch</b> { <b>checkpoint</b> <i>src-cp-name</i>   <b>running-config</b>   <b>startup-config</b>   <b>file</b> <i>source-file</i> } { <b>checkpoint</b> <i>dest-cp-name</i>   <b>running-config</b>   <b>startup-config</b>   <b>file</b> <i>dest-file</i> }	Displays the differences between the source and destination checkpoint selections.
<b>show rollback log</b> [ <b>exec</b>   <b>verify</b> ]	Displays the contents of the rollback log.

Use the **clear checkpoint database** command to delete all checkpoint files.

## 11.7 Configuration Example for Rollback

This example shows how to create a checkpoint file and then implements a best-effort rollback to a user checkpoint name:

```
checkpoint stable
rollback running-config checkpoint stable best-effort
```

## 11.8 Additional References

### 11.8.1 Related Documents

Related Topic	Document Title
Configuration files	<i>Inspur CN12900 Series INOS-CN Fundamentals Configuration Guide</i>