



Inspur

CN12900 Series

INOS-CN Security 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

Technical Document Support Email: 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
 Warning	Indicates a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
 Caution	Indicates a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.
 Note	Provides additional information to emphasize or supplement important points of the main text.
 Tip	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 boldface . For example, log in as user root .

Convention	Description
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 boldface .
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 boldface . For example, click OK .
>	Multi-level menus are in boldface and separated by the ">" signs. For example, choose File > Create > Folder .

Keyboard operation

Format	Description
Key	Press the key. For example, press Enter and press Tab .
Key 1+Key 2	Press the keys concurrently. For example, pressing Ctrl+C means the two keys should be pressed concurrently.
Key 1, Key 2	Press the keys in turn. For example, pressing Alt, A 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

CHAPTER 1 New and Changed Information	1
1.1 New and Changed Information.....	1
CHAPTER 2 Overview	2
2.1 Authentication, Authorization, and Accounting.....	2
2.2 RADIUS and TACACS+ Security Protocols.....	2
2.3 SSH and Telnet.....	3
2.4 IP ACLs.....	3
2.5 MAC ACLs.....	3
2.6 VACLs.....	3
2.7 Traffic Storm Control.....	3
2.8 Control Plane Policing.....	3
CHAPTER 3 Configuring AAA	5
3.1 About AAA.....	5
3.2 Licensing Requirements for AAA.....	8
3.3 Prerequisites for AAA.....	8
3.4 Guidelines and Limitations for AAA.....	8
3.5 Default Settings for AAA.....	8
3.6 Configuring AAA.....	9
3.7 Monitoring and Clearing the Local AAA Accounting Log.....	27
3.8 Verifying the AAA Configuration.....	27
3.9 Configuration Examples for AAA.....	28
3.10 Configuration Examples for Login Parameters.....	29
3.11 Configuration Examples for the Password Prompt Feature.....	29
3.12 Additional References for AAA.....	30
CHAPTER 4 Configuring RADIUS	31
4.1 About RADIUS.....	31
4.2 Licensing Requirements for RADIUS.....	33
4.3 Prerequisites for RADIUS.....	33
4.4 Guidelines and Limitations for RADIUS.....	33

4.5 Default Settings for RADIUS.....	34
4.6 Configuring RADIUS Servers.....	34
4.7 Verifying the RADIUS Configuration.....	51
4.8 Monitoring RADIUS Servers.....	51
4.9 Clearing RADIUS Server Statistics.....	52
4.10 Configuration Example for RADIUS.....	52
4.11 Where to Go Next.....	52
4.12 Additional References for RADIUS.....	52
CHAPTER 5 Configuring TACACS+.....	54
5.1 About TACACS+.....	54
5.2 Licensing Requirements for TACACS+.....	57
5.3 Prerequisites for TACACS+.....	57
5.4 Guidelines and Limitations for TACACS+.....	57
5.5 Default Settings for TACACS+.....	57
5.6 Configuring TACACS+.....	58
5.7 Monitoring TACACS+ Servers.....	81
5.8 Clearing TACACS+ Server Statistics.....	81
5.9 Verifying the TACACS+ Configuration.....	82
5.10 Configuration Examples for TACACS+.....	82
5.11 Where to Go Next.....	84
5.12 Additional References for TACACS+.....	84
CHAPTER 6 Configuring SSH and Telnet.....	86
6.1 About SSH and Telnet.....	86
6.2 Licensing Requirements for SSH and Telnet.....	87
6.3 Prerequisites for SSH and Telnet.....	87
6.4 Guidelines and Limitations for SSH and Telnet.....	87
6.5 Default Settings for SSH and Telnet.....	87
6.6 Configuring SSH.....	88
6.7 Configuring Telnet.....	105
6.8 Verifying the SSH and Telnet Configuration.....	107
6.9 Configuration Example for SSH.....	107
6.10 Configuration Example for SSH Passwordless File Copy.....	108

6.11 Configuration Example for X.509v3 Certificate-Based SSH Authentication.....	110
6.12 Additional References for SSH and Telnet.....	110
CHAPTER 7 Configuring IP ACLs.....	112
7.1 About ACLs.....	112
7.2 Licensing Requirements for IP ACLs.....	122
7.3 Prerequisites for IP ACLs.....	122
7.4 Guidelines and Limitations for IP ACLs.....	122
7.5 Default Settings for IP ACLs.....	124
7.6 Configuring IP ACLs.....	125
7.7 Verifying the IP ACL Configuration.....	152
7.8 Monitoring and Clearing IP ACL Statistics.....	154
7.9 Configuration Examples for IP ACLs.....	154
7.10 About System ACLs.....	155
7.11 About System ACLs.....	155
7.12 Configuring Object Groups.....	159
7.13 Verifying the Object-Group Configuration.....	164
7.14 Configuring Time Ranges.....	164
7.15 Verifying the Time-Range Configuration.....	169
7.16 Additional References for IP ACLs.....	170
CHAPTER 8 Configuring MAC ACLs.....	171
8.1 About MAC ACLs.....	171
8.2 Licensing Requirements for MAC ACLs.....	171
8.3 Guidelines and Limitations for MAC ACLs.....	171
8.4 Default Settings for MAC ACLs.....	172
8.5 Configuring MAC ACLs.....	172
8.6 Verifying the MAC ACL Configuration.....	178
8.7 Monitoring and Clearing MAC ACL Statistics.....	179
8.8 Configuration Example for MAC ACLs.....	179
8.9 Additional References for MAC ACLs.....	179
CHAPTER 9 Configuring VLAN ACLs.....	180
9.1 About VLAN ACLs.....	180
9.2 Licensing Requirements for VACLs.....	180

9.3 Prerequisites for VACLs.....	181
9.4 Guidelines and Limitations for VACLs.....	181
9.5 Default Settings for VACLs.....	181
9.6 Configuring VACLs.....	182
9.7 Verifying the VACL Configuration.....	185
9.8 Monitoring and Clearing VACL Statistics.....	185
9.9 Configuration Example for VACLs.....	186
9.10 Additional References for VACLs.....	186
CHAPTER 10 Configuring Traffic Storm Control.....	187
10.1 About Traffic Storm Control.....	187
10.2 Licensing Requirements for Traffic Storm Control.....	188
10.3 Guidelines and Limitations for Traffic Storm Control.....	188
10.4 Default Settings for Traffic Storm Control.....	189
10.5 Configuring Traffic Storm Control.....	189
10.6 Verifying Traffic Storm Control Configuration.....	190
10.7 Monitoring Traffic Storm Control Counters.....	190
10.8 Configuration Examples for Traffic Storm Control.....	191
CHAPTER 11 Configuring Control Plane Policing.....	192
11.1 About CoPP.....	192
11.2 Licensing Requirements for CoPP.....	207
11.3 Guidelines and Limitations for CoPP.....	207
11.4 Default Settings for CoPP.....	208
11.5 Configuring CoPP.....	208
11.6 Verifying the CoPP Configuration.....	216
11.7 Displaying the CoPP Configuration Status.....	217
11.8 Monitoring CoPP.....	218
11.9 Clearing the CoPP Statistics.....	218
11.10 Configuration Examples for CoPP.....	219
11.11 Additional References for CoPP.....	221

Figure

<i>Figure 1 : Authorization and Authentication Flow for User Login.....</i>	<i>7</i>
<i>Figure 2 : RADIUS Server States.....</i>	<i>32</i>
<i>Figure 3 : TACACS+ Server States.....</i>	<i>55</i>
<i>Figure 4 : Order of ACL Application.....</i>	<i>114</i>
<i>Figure 5 : ACLs and Packet Flow.....</i>	<i>114</i>
<i>Figure 6 : Broadcast Suppression.....</i>	<i>187</i>

Table

<i>Table 1 : New and Changed Features for Inspur CN12900.....</i>	<i>1</i>
<i>Table 2 : AAA Service Configuration Commands.....</i>	<i>6</i>
<i>Table 3 : AAA Authentication Methods for AAA Services.....</i>	<i>7</i>
<i>Table 4 : Default AAA Parameter Settings.....</i>	<i>9</i>
<i>Table 5 : CHAP RADIUS and TACACS+ VSAs.....</i>	<i>17</i>
<i>Table 6 : MSCHAP and MSCHAP V2 RADIUS VSAs.....</i>	<i>18</i>
<i>Table 7 : Default RADIUS Parameter Settings.....</i>	<i>34</i>
<i>Table 8 : Default TACACS+ Parameters Settings.....</i>	<i>57</i>
<i>Table 9 : Default SSH and Telnet Parameters.....</i>	<i>88</i>
<i>Table 10 : Security ACL Applications.....</i>	<i>112</i>
<i>Table 11 : Features per ACL TCAM Region.....</i>	<i>120</i>
<i>Table 12 : Default IP ACL Parameters.....</i>	<i>124</i>
<i>Table 13 : Default TCAM Region Configuration (Ingress) - For Inspur CN12900 Series Switches.....</i>	<i>140</i>
<i>Table 14 : Default TCAM Region Configuration (Egress) - For Inspur CN12900 Series Switches.....</i>	<i>140</i>
<i>Table 15 : Updated TCAM Region Configuration After Reducing the IPv4 RA CL (Ingress).....</i>	<i>140</i>
<i>Table 16 : Updated TCAM Region Configuration After Removing Layer 3 QoS (Ingress).....</i>	<i>141</i>
<i>Table 17 : Default TCAM Region Configuration After Reducing the IPv4 RA CL (Egress).....</i>	<i>141</i>
<i>Table 18 : Default MAC ACLs Parameters.....</i>	<i>172</i>
<i>Table 19 : Default VA CL Parameters.....</i>	<i>181</i>
<i>Table 20 : Default Traffic Storm Control Parameters.....</i>	<i>189</i>
<i>Table 21 : Default CoPP Parameters Settings.....</i>	<i>208</i>

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 Security Guide, Release 9.x*.

1.1 New and Changed Information

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

Table 1: New and Changed Features for Inspur CN12900

Feature	Description	Changed in Release	Where Documented
AAA	Introduced in F1(1)	N/A	
ACL	Introduced in F1(1)	N/A	
ACL counters	Introduced in F1(1)	N/A	
CoPP	Introduced in F1(1)	N/A	
RADIUS	Introduced in F1(1)	N/A	
SSH	Introduced in F1(1)	N/A	
Traffic Strom Control	Introduced in F1(1)	N/A	
TACACS+	Introduced in F1(1)	N/A	
ACEs in system ACL	Introduced in F3(4)	N/A	
Configuring system ACLs	Introduced in F3(4)	N/A	

CHAPTER 2 Overview

The Inspur INOS-CN software supports security features that can protect your network against degradation or failure and also against data loss or compromise resulting from intentional attacks and from unintended but damaging mistakes by well-meaning network users.

This chapter includes the following sections:

2.1 Authentication, Authorization, and Accounting

Authentication, authorization, and accounting (AAA) is an architectural framework for configuring a set of three independent security functions in a consistent, modular manner.

Authentication

Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol that you select, encryption. Authentication is the way a user is identified prior to being allowed access to the network and network services. You configure AAA authentication by defining a named list of authentication methods and then applying that list to various interfaces.

Authorization

Provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet.

Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights, with the appropriate user. AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared with the information contained in a database for a given user, and the result is returned to AAA to determine the user's actual capabilities and restrictions.

Accounting

Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables you to track the services that users are accessing, as well as the amount of network resources that they are consuming.

2.2 RADIUS and TACACS+ Security Protocols

AAA uses security protocols to administer its security functions. If your router or access server is acting as a network access server, AAA is the means through which you establish communication between your network access server and your RADIUS or TACACS+ security server.

The chapters in this guide describe how to configure the following security server protocols:

RADIUS

A distributed client/server system implemented through AAA that secures networks against unauthorized access. In the Inspur implementation, RADIUS clients run on Inspur routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

TACACS+

A security application implemented through AAA that provides a centralized validation of users who are attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a

TACACS+ daemon running, typically, on a UNIX or Windows NT workstation.

TACACS+ provides for separate and modular authentication, authorization, and accounting facilities.

2.3 SSH and Telnet

You can use the Secure Shell (SSH) server to enable an SSH client to make a secure, encrypted connection to a Inspur INOS-CN device. SSH uses strong encryption for authentication. The SSH server in the Inspur INOS-CN software can interoperate with publicly and commercially available SSH clients.

The SSH client in the Inspur INOS-CN software works with publicly and commercially available SSH servers.

The Telnet protocol enables TCP/IP connections to a host. Telnet allows a user at one site to establish a TCP connection to a login server at another site and then passes the keystrokes from one device to the other. Telnet can accept either an IP address or a domain name as the remote device address.

2.4 IP ACLs

IP ACLs are ordered sets of rules that you can use to filter traffic based on IPv4 information in the Layer 3 header of packets. Each rule specifies a set of conditions that a packet must satisfy to match the rule. When the Inspur INOS-CN software determines that an IP ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether a packet is permitted or denied, or if there is no match, the Inspur INOS-CN software applies the applicable default rule. The Inspur INOS-CN software continues processing packets that are permitted and drops packets that are denied.

2.5 MAC ACLs

MAC ACLs are ACLs that filter traffic using the information in the Layer 2 header of each packet. Each rule specifies a set of conditions that a packet must satisfy to match the rule. When the Inspur INOS-CN software determines that a MAC ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether a packet is permitted or denied, or if there is no match, the Inspur INOS-CN software applies the applicable default rule. The Inspur INOS-CN software continues processing packets that are permitted and drops packets that are denied.

2.6 VACLs

A VLAN ACL (VACL) is one application of an IP ACL or MAC ACL. You can configure VACLs to apply to all packets that are routed into or out of a VLAN or are bridged within a VLAN. VACLs are strictly for security packet filtering and for redirecting traffic to specific physical interfaces. VACLs are not defined by direction (ingress or egress).

2.7 Traffic Storm Control

Traffic storm control (also called traffic suppression) allows you to monitor the levels of the incoming traffic over a 1-second interval. During this interval, the traffic level, which is a percentage of the total available bandwidth of the port, is compared with the traffic storm control level that you configured. When the ingress traffic reaches the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends.

2.8 Control Plane Policing

The Inspur INOS-CN device provides control plane policing to prevent denial-of-service (DoS) attacks from impacting performance. The supervisor module of the Inspur INOS-CN device has both the management plane and

control plane and is critical to the operation of the network. Any disruption to the supervisor module would result in serious network outages. Excessive traffic to the supervisor module could overload it and slow down the performance of the entire Inspur INOS-CN device. Attacks on the supervisor module can be of various types such as, denial-of-service (DoS) attacks that generate IP traffic streams to the control plane at a very high rate. These attacks result in the control plane spending a large amount of time in handling these packets, which makes the control plane unable to process genuine traffic.

CHAPTER 3 Configuring AAA

This chapter describes how to configure authentication, authorization, and accounting (AAA) on Inspur INOS-CN devices.

This chapter includes the following sections:

3.1 About AAA

This section includes information about AAA on Inspur INOS-CN devices.

3.1.1 AAA Security Services

The AAA feature allows you to verify the identity of, grant access to, and track the actions of users managing a Inspur INOS-CN device. Inspur INOS-CN devices support Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System Plus (TACACS+) protocols.

Based on the user ID and password combination that you provide, Inspur INOS-CN devices perform local authentication or authorization using the local database or remote authentication or authorization using one or more AAA servers. A preshared secret key provides security for communication between the Inspur INOS-CN device and AAA servers. You can configure a common secret key for all AAA servers or for only a specific AAA server.

AAA security provides the following services:

Authentication

Identifies users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol that you select, encryption.

Authentication is the process of verifying the identity of the person or device accessing the Inspur INOS-CN device, which is based on the user ID and password combination provided by the entity trying to access the Inspur INOS-CN device. Inspur INOS-CN devices allow you to perform local authentication (using the local lookup database) or remote authentication (using one or more RADIUS or TACACS+ servers).

Authorization

Provides access control. AAA authorization is the process of assembling a set of attributes that describe what the user is authorized to perform. Authorization in the Inspur INOS-CN software is provided by attributes that are downloaded from AAA servers. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user.

Accounting

Provides the method for collecting information, logging the information locally, and sending the information to the AAA server for billing, auditing, and reporting.

The accounting feature tracks and maintains a log of every management session used to access the Inspur INOS-CN device. You can use this information to generate reports for troubleshooting and auditing purposes. You can store accounting logs locally or send them to remote AAA servers.

3.1.2 Benefits of Using AAA

AAA provides the following benefits:

- Increased flexibility and control of access configuration
- Scalability
- Standardized authentication methods, such as RADIUS and TACACS+

- Multiple backup devices

3.1.3 Remote AAA Services

Remote AAA services provided through RADIUS and TACACS+ protocols have the following advantages over local AAA services:

- It is easier to manage user password lists for each Inspur INOS-CN device in the fabric.
- AAA servers are already deployed widely across enterprises and can be easily used for AAA services.
- You can centrally manage the accounting log for all Inspur INOS-CN devices in the fabric.
- It is easier to manage user attributes for each Inspur INOS-CN device in the fabric than using the local databases on the Inspur INOS-CN devices.

3.1.4 AAA Server Groups

You can specify remote AAA servers for authentication, authorization, and accounting using server groups. A server group is a set of remote AAA servers that implement the same AAA protocol. The purpose of a server group is to provide for failover servers in case a remote AAA server fails to respond. If the first remote server in the group fails to respond, the next remote server in the group is tried until one of the servers sends a response. If all the AAA servers in the server group fail to respond, then that server group option is considered a failure. If required, you can specify multiple server groups. If the Inspur INOS-CN device encounters errors from the servers in the first group, it tries the servers in the next server group.

3.1.5 AAA Service Configuration Options

The AAA configuration in Inspur INOS-CN devices is service based, which means that you can have separate AAA configurations for the following services:

- User Telnet or Secure Shell (SSH) login authentication
- Console login authentication
- User management session accounting

This table provides the related CLI command for each AAA service configuration option.

Table 2: AAA Service Configuration Commands

AAA Service Configuration	Related Command
Telnet or SSH login	aaa authentication login default
Console login	aaa authentication login console
User session accounting	aaa accounting default

You can specify the following authentication methods for the AAA services:

All RADIUS servers

Uses the global pool of RADIUS servers for authentication.

Specified server groups

Uses specified RADIUS, TACACS+, or LDAP server groups you have configured for authentication.

Local

Uses the local username or password database for authentication.

None

Specifies that no AAA authentication be used.

This table shows the AAA authentication methods that you can configure for the AAA services.

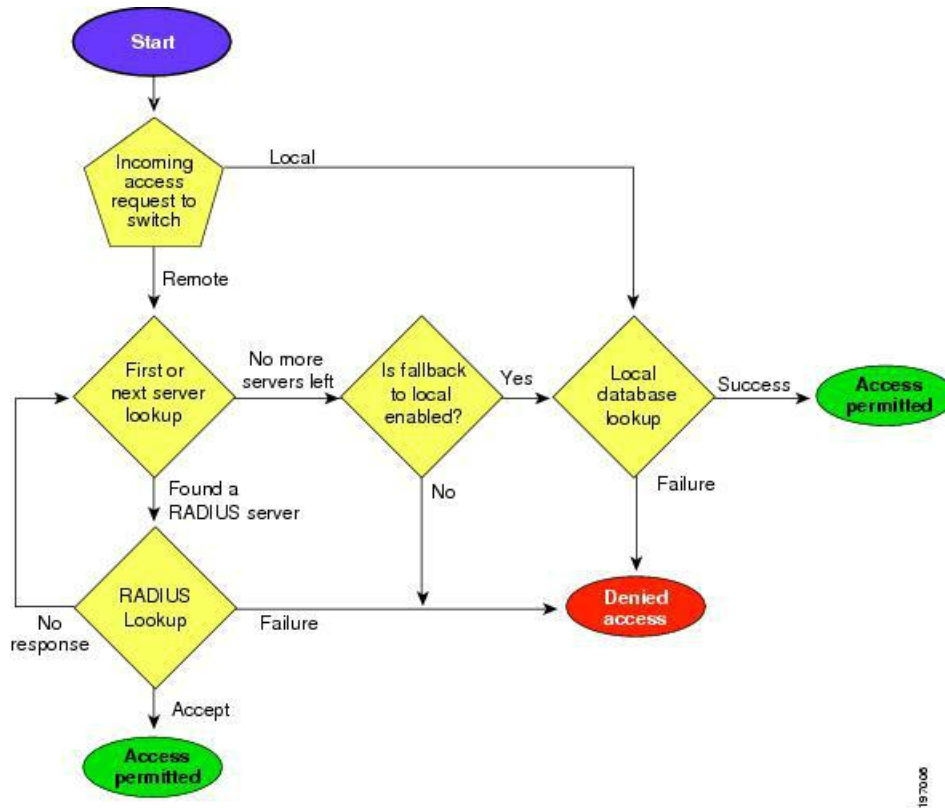
Table 3: AAA Authentication Methods for AAA Services

AAA Service	AAA Methods
Console login authentication	Server groups, local, and none
User login authentication	Server groups, local, and none
User management session accounting	Server groups and local

3.1.6 Authentication and Authorization Process for User Login

Figure 1: Authorization and Authentication Flow for User Login

This figure shows a flow chart of the authentication and authorization process for user login.



The following list explains the process:

- When you log in to the required Inspur INOS-CN device, you can use the Telnet, SSH, or console login options.
- When you have configured the AAA server groups using the server group authentication method, the Inspur INOS-CN device sends an authentication request to the first AAA server in the group as follows:
- If the AAA server fails to respond, the next AAA server is tried and so on until the remote server responds to the authentication request.
- If all AAA servers in the server group fail to respond, the servers in the next server group are tried.
- If all configured methods fail, the local database is used for authentication, unless fallback to local is disabled for the console login.
- If the Inspur INOS-CN device successfully authenticates you through a remote AAA server, then the following possibilities apply:
- If the AAA server protocol is RADIUS, then user roles specified in the Inspur-av-pair attribute are downloaded with an authentication response.

- If the AAA server protocol is TACACS+, then another request is sent to the same server to get the user roles specified as custom attributes for the shell.
- If your username and password are successfully authenticated locally, the Inspur INOS-CN device logs you in and assigns you the roles configured in the local database.

3.1.7 AES Password Encryption and Master Encryption Keys

You can enable strong, reversible 128-bit Advanced Encryption Standard (AES) password encryption, also known as type-6 encryption. To start using type-6 encryption, you must enable the AES password encryption feature and configure a master encryption key, which is used to encrypt and decrypt passwords.

After you enable AES password encryption and configure a master key, all existing and newly created clear-text passwords for supported applications (currently RADIUS and TACACS+) are stored in type-6 encrypted format, unless you disable type-6 password encryption. You can also configure Inspur INOS-CN to convert all existing weakly encrypted passwords to type-6 encrypted passwords.

3.2 Licensing Requirements for AAA

The following table shows the licensing requirements for this feature:

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

3.3 Prerequisites for AAA

Remote AAA servers have the following prerequisites:

- Ensure that at least one RADIUS, TACACS+, or LDAP server is reachable through IP.
- Ensure that the Inspur INOS-CN device is configured as a client of the AAA servers.
- Ensure that the secret key is configured on the Inspur INOS-CN device and the remote AAA servers.
- Ensure that the remote server responds to AAA requests from the Inspur INOS-CN device.

3.4 Guidelines and Limitations for AAA

AAA has the following guidelines and limitations:

- If you have a user account configured on the local Inspur INOS-CN device that has the same name as a remote user account on an AAA server, the Inspur INOS-CN software applies the user roles for the local user account to the remote user, not the user roles configured on the AAA server.
- Inspur CN12900 Series switches support the **aaa authentication login ascii-authentication** command only for TACACS+ (and not for RADIUS).
- If you modify the default login authentication method (without using the **local** keyword), the configuration overrides the console login authentication method. To explicitly configure the console authentication method, use the **aaa authentication login console {group group-list [none] | local | none}** command.
- The **login block-for** and **login quiet-mode** configuration mode commands are renamed to **system login block-for** and **system login quiet-mode**, respectively.

3.5 Default Settings for AAA

This table lists the default settings for AAA parameters.

Table 4: Default AAA Parameter Settings

Parameters	Default
Console authentication method	local
Default authentication method	local
Login authentication failure messages	Disabled
CHAP authentication	Disabled
MSCHAP authentication	Disabled
Default accounting method	local
Accounting log display length	250 KB

3.6 Configuring AAA

This section describes the tasks for configuring AAA on Inspur INOS-CN devices.

3.6.1 Process for Configuring AAA

Follow these steps to configure AAA authentication and accounting:

1. If you want to use remote RADIUS, TACACS+, or LDAP servers for authentication, configure the hosts on your Inspur INOS-CN device.
2. Configure console login authentication methods.
3. Configure default login authentication methods for user logins.
4. Configure default AAA accounting default methods.

3.6.2 Configuring Console Login Authentication Methods

This section describes how to configure the authentication methods for the console login.

The authentication methods include the following:

- Global pool of RADIUS servers
- Named subset of RADIUS, TACACS+, or LDAP servers
- Local database on the Inspur INOS-CN device
- Username only (none)

The default method is local, but you have the option to disable it.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication login console {group group-list [none] | local | none}**
3. **exit**
4. (Optional) **show aaa authentication**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters configuration mode.
Step 2	aaa authentication login console {group group-list [none] local none} Example: <pre>switch(config)# aaa authentication login console group radius</pre>	<p>Configures login authentication methods for the console.</p> <p>The <i>group-list</i> argument consists of a space-delimited list of group names. The group names are the following:</p> <p>radius</p> <p>Uses the global pool of RADIUS servers for authentication.</p> <p>named-group</p> <p>Uses a named subset of RADIUS, TACACS+, or LDAP servers for authentication.</p> <p>The local method uses the local database for authentication, and the none method specifies that no AAA authentication be used.</p> <p>The default console login method is local, which is used when no methods are configured or when all the configured methods fail to respond, unless fallback to local is disabled for the console login.</p>
Step 3	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 4	(Optional) show aaa authentication Example: <pre>switch# show aaa authentication</pre>	Displays the configuration of the console login authentication methods.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

3.6.3 Configuring Default Login Authentication Methods

The authentication methods include the following:

- Global pool of RADIUS servers
- Named subset of RADIUS, TACACS+, or LDAP servers
- Local database on the Inspur INOS-CN device
- Username only

The default method is local, but you have the option to disable it.

Before you begin

Configure RADIUS, TACACS+, or LDAP server groups, as needed.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication login default {group group-list [none] | local | none}**
3. **exit**
4. (Optional) **show aaa authentication**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters configuration mode.
Step 2	aaa authentication login default {group group-list [none] local none} Example: <pre>switch(config)# aaa authentication login default group radius</pre>	<p>Configures the default authentication methods.</p> <p>The <i>group-list</i> argument consists of a space-delimited list of group names. The group names are the following:</p> <ul style="list-style-type: none"> • radius—Uses the global pool of RADIUS servers for authentication. • named-group—Uses a named subset of RADIUS, TACACS+, or LDAP servers for authentication. <p>The local method uses the local database for authentication, and the none method specifies that no AAA authentication be used. The default login method is local, which is used when no methods are configured or when all the configured methods fail to respond, unless fallback to local is disabled for the console login.</p> <p>You can configure one of the following:</p> <ul style="list-style-type: none"> • AAA authentication groups

	Command or Action	Purpose
		<ul style="list-style-type: none"> • AAA authentication groups with no authentication • Local authentication • No authentication <p>Note The local keyword is not supported (and is not required) when configuring AAA authentication groups because local authentication is the default if remote servers are unreachable. For example, if you configure aaa authentication login default group g1, local authentication is tried if you are unable to authenticate using AAA group g1. In contrast, if you configure aaa authentication login default group g1 none, no authentication is performed if you are unable to authenticate using AAA group g1.</p>
Step 3	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 4	(Optional) show aaa authentication Example: <pre>switch# show aaa authentication</pre>	Displays the configuration of the default login authentication methods.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

3.6.4 Disabling Fallback to Local Authentication

By default, if remote authentication is configured for console or default login and all AAA servers are unreachable (resulting in an authentication error), the Inspur INOS-CN device falls back to local authentication to ensure that users are not locked out of the device. However, you can disable fallback to local authentication in order to increase security.

Caution	Disabling fallback to local authentication can lock your Inspur INOS-CN device, forcing you to perform
----------------	--

a password recovery in order to gain access. To prevent being locked out of the device, we recommend that you disable fallback to local authentication for only the default login or the console login, not both.

Before you begin

Configure remote authentication for the console or default login.

SUMMARY STEPS

1. **configure terminal**
2. **no aaa authentication login {console | default} fallback error local**
3. (Optional) **exit**
4. (Optional) **show aaa authentication**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters configuration mode.
Step 2	no aaa authentication login {console default} fallback error local Example: <pre>switch(config)# no aaa authentication login console fallback error local</pre>	Disables fallback to local authentication for the console or default login if remote authentication is configured and all AAA servers are unreachable. The following message appears when you disable fallback to local authentication: “WARNING!!! Disabling fallback can lock your switch.”
Step 3	(Optional) exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 4	(Optional) show aaa authentication Example: <pre>switch# show aaa authentication</pre>	Displays the configuration of the console and default login authentication methods.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

3.6.5 Enabling the Default User Role for AAA Authentication

You can allow remote users who do not have a user role to log in to the Inspur INOS-CN device through a RADIUS or TACACS+ remote authentication server using a default user role. When you disable the AAA default user role feature, remote users who do not have a user role cannot log in to the device.

SUMMARY STEPS

1. **configure terminal**
2. **aaa user default-role**
3. **exit**
4. (Optional) **show aaa user default-role**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	aaa user default-role Example: switch(config)# aaa user default-role	Enables the default user role for AAA authentication. The default is enabled. You can disable the default user role feature by using the no form of this command.
Step 3	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 4	(Optional) show aaa user default-role Example: switch# show aaa user default-role	Displays the AAA default user role configuration.
Step 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.6.6 Enabling Login Authentication Failure Messages

When you log in, the login is processed by rolling over to the local user database if the remote AAA servers do not respond. In such cases, the following messages display on the user's terminal if you have enabled login failure messages:

```
Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.
```

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication login error-enable**
3. **exit**
4. (Optional) **show aaa authentication**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	aaa authentication login error-enable Example: switch(config)# aaa authentication login error-enable	Enables login authentication failure messages. The default is disabled.
Step 3	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 4	(Optional) show aaa authentication Example: switch# show aaa authentication	Displays the login failure message configuration.
Step 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.6.7 Logging Successful and Failed Login Attempts

You can configure the switch to log all successful and failed login attempts to the configured syslog server.

SUMMARY STEPS

1. **configure terminal**
2. **[no] login on-failure log**
3. **[no] login on-success log**
4. (Optional) **show login on-failure log**
5. (Optional) **show login on-successful log**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.

	Command or Action	Purpose
	Example: <pre>switch# configure terminal</pre>	
Step 2	Required: [no] login on-failure log Example: <pre>switch(config)# login on-failure log</pre>	Logs all failed authentication messages to the configured syslog server. With this configuration, the following syslog message appears after the failed login: AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed for user admin from 172.22.00.00 Note When logging level authpriv is 6, additional Linux kernel authentication messages appear along with the previous message. If these additional messages need to be ignored, the authpriv value should be set to 3.
Step 3	Required: [no] login on-success log Example: <pre>switch(config)# login on-success log</pre>	Logs all successful authentication messages to the configured syslog server. With this configuration, the following syslog message appears after the successful login: AUTHPRIV-6-SYSTEM_MSG: pam_aaa:Authentication success for user admin from 172.22.00.00 Note When logging level authpriv is 6, additional Linux kernel authentication messages appear along with the previous message.
Step 4	(Optional) show login on-failure log Example: <pre>switch(config)# show login on-failure log</pre>	Displays whether the switch is configured to log failed authentication messages to the syslog server.
Step 5	(Optional) show login on-successful log Example: <pre>switch(config)# show login on-successful log</pre>	Displays whether the switch is configured to log successful authentication messages to the syslog server.
Step 6	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

3.6.8 Enabling CHAP Authentication

The Inspur INOS-CN software supports the Challenge Handshake Authentication Protocol (CHAP), a challenge-response authentication protocol that uses the industry-standard Message Digest (MD5) hashing scheme to encrypt responses. You can use CHAP for user logins to a Inspur INOS-CN device through a remote authentication server (RADIUS or TACACS+).

By default, the Inspur INOS-CN device uses Password Authentication Protocol (PAP) authentication between the Inspur INOS-CN device and the remote server. If you enable CHAP, you need to configure your RADIUS or TACACS+ server to recognize the CHAP vendor-specific attributes (VSAs).

This table shows the RADIUS and TACACS+ VSAs required for CHAP.

Table 5: CHAP RADIUS and TACACS+ VSAs

Vendor-ID Number	Vendor-Type Number	VSA	Description
311	11	CHAP-Challenge	Contains the challenge sent by an AAA server to a CHAP user. It can be used in both Access-Request and Access-Challenge packets.
211	11	CHAP-Response	Contains the response value provided by a CHAP user in response to the challenge. It is used only in Access-Request packets.

Before you begin

Disable AAA ASCII authentication for logins.

SUMMARY STEPS

1. **configure terminal**
2. **no aaa authentication login ascii-authentication**
3. **aaa authentication login chap enable**
4. (Optional) **exit**
5. (Optional) **show aaa authentication login chap**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	no aaa authentication login ascii-authentication Example: switch(config)# no aaa authentication login ascii-authentication	Disables ASCII authentication.
Step 3	aaa authentication login chap enable Example:	Enables CHAP authentication. The default is disabled. Note You cannot enable both CHAP and

	Command or Action	Purpose
	<pre>switch(config)# aaa authentication login chap enable</pre>	MSCHAP or MSCHAP V2 on your Inspur INOS-CN device.
Step 4	(Optional) exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 5	(Optional) show aaa authentication login chap Example: <pre>switch# show aaa authentication login chap</pre>	Displays the CHAP configuration.
Step 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

3.6.9 Enabling MSCHAP or MSCHAP V2 Authentication

Microsoft Challenge Handshake Authentication Protocol (MSCHAP) is the Microsoft version of CHAP. The Inspur INOS-CN software also supports MSCHAP Version 2 (MSCHAP V2). You can use MSCHAP for user logins to a Inspur INOS-CN device through a remote authentication server (RADIUS or TACACS+). MSCHAP V2 only supports user logins to a Inspur INOS-CN device through remote authentication RADIUS servers. If

you configure a TACACS+ group with MSCHAP V2, the AAA default login authentication uses the next configured method, or the local method, if no other server group is configured.

By default, the Inspur INOS-CN device uses Password Authentication Protocol (PAP) authentication between the Inspur INOS-CN device and the remote server. If you enable MSCHAP or MSCHAP V2, you need to configure your RADIUS server to recognize the MSCHAP and MSCHAP V2 vendor-specific attributes (VSAs).

This table shows the RADIUS VSAs required for MSCHAP.

Table 6: MSCHAP and MSCHAP V2 RADIUS VSAs

Vendor-ID Number	Vendor-Type Number	VSA	Description
311	11	MSCHAP-Challenge	Contains the challenge sent by an AAA server to an MSCHAP or MSCHAP V2 user. It can be used in both Access-Request and Access-Challenge packets.
211	11	MSCHAP-Response	Contains the response value provided by an MSCHAP or MSCHAP V2 user in response to the challenge. It is only used in Access-Request packets.

Before you begin

Disable AAA ASCII authentication for logins.

SUMMARY STEPS

1. **configure terminal**
2. **no aaa authentication login ascii-authentication**
3. **aaa authentication login {mschap | mschapv2} enable**
4. **exit**
5. (Optional) **show aaa authentication login {mschap | mschapv2}**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters configuration mode.
Step 2	no aaa authentication login ascii-authentication Example: <pre>switch(config)# no aaa authentication login ascii-authentication</pre>	Disables ASCII authentication.
Step 3	aaa authentication login {mschap mschapv2} enable Example: <pre>switch(config)# aaa authentication login mschap enable</pre>	Enables MSCHAP or MSCHAP V2 authentication. The default is disabled. Note You cannot enable both MSCHAP and MSCHAP V2 on your Inspur INOS-CN device.
Step 4	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 5	(Optional) show aaa authentication login {mschap mschapv2} Example: <pre>switch# show aaa authentication login mschap</pre>	Displays the MSCHAP or MSCHAP V2 configuration.
Step 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

3.6.10 Configuring AAA Accounting Default Methods

Inspur INOS-CN software supports TACACS+ and RADIUS methods for accounting. Inspur INOS-CN devices report user activity to TACACS+ or RADIUS security servers in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the AAA server.

When you activate AAA accounting, the Inspur INOS-CN device reports these attributes as accounting records,

which are then stored in an accounting log on the security server.

You can create default method lists defining specific accounting methods, which include the following:

RADIUS server group

Uses the global pool of RADIUS servers for accounting.

Specified server group

Uses a specified RADIUS or TACACS+ server group for accounting.

Local

Uses the local username or password database for accounting.

Before you begin

Configure RADIUS or TACACS+ server groups, as needed.

SUMMARY STEPS

1. **configure terminal**
2. **aaa accounting default {group *group-list* | local}**
3. **exit**
4. (Optional) **show aaa accounting**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters configuration mode.
Step 2	aaa accounting default {group <i>group-list</i> local} Example: <pre>switch(config)# aaa accounting default group radius</pre>	Configures the default accounting method. The <i>group-list</i> argument consists of a space-delimited list of group names. The group names are the following: <ul style="list-style-type: none"> • radius—Uses the global pool of RADIUS servers for accounting. • <i>named-group</i>—Uses a named subset of TACACS+ or RADIUS servers for accounting. The local method uses the local database for accounting. The default method is local , which is used when no server groups are configured or when all the configured server groups fail to respond.
Step 3	exit	Exits configuration mode.

	Command or Action	Purpose
	Example: <pre>switch(config)# exit switch#</pre>	
Step 4	(Optional) show aaa accounting Example: <pre>switch# show aaa accounting</pre>	Displays the configuration AAA accounting default methods.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

3.6.11 Using AAA Server VSAs with Inspur INOS-CN Devices

You can use vendor-specific attributes (VSAs) to specify Inspur INOS-CN user roles and SNMPv3 parameters on AAA servers.

About VSAs

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating VSAs between the network access server and the RADIUS server. The IETF uses attribute 26. VSAs allow vendors to support their own extended attributes that are not suitable for general use. The Inspur RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Inspur vendor ID is 48797, and the supported option is vendor type 1, which is named Inspur-av-pair. The value is a string with the following format:

```
protocol : attribute separator value *
```

The protocol is a Inspur attribute for a particular type of authorization, the separator is = (equal sign) for mandatory attributes, and * (asterisk) indicates optional attributes.

When you use RADIUS servers for authentication on a Inspur INOS-CN device, the RADIUS protocol directs the RADIUS server to return user attributes, such as authorization information, along with authentication results. This authorization information is specified through VSAs.

VSA Format

The following VSA protocol options are supported by the Inspur INOS-CN software:

Shell

Protocol used in access-accept packets to provide user profile information.

Accounting

Protocol used in accounting-request packets. If a value contains any white spaces, put it within double quotation marks.

The following attributes are supported by the Inspur INOS-CN software:

roles

Lists all the roles assigned to the user. The value field is a string that stores the list of group names delimited by white space. For example, if you belong to role network-operator and network-admin, the value field would be network-operator network-admin. This subattribute is sent in the VSA portion of the Access-Accept frames from the RADIUS server, and it can only be used with the shell protocol value. These examples use the roles attribute:


```
shell:roles=network-operator network-admin
shell:roles*network-operator network-admin
```

The following examples show the roles attribute as supported by FreeRADIUS:

```
Inspur-AVPair = shell:roles=\network-operator network-admin\
Inspur-AVPair = shell:roles*\network-operator network-admin\
```

accountinginfo

Stores accounting information in addition to the attributes covered by a standard RADIUS accounting protocol. This attribute is sent only in the VSA portion of the Account-Request frames from the RADIUS client on the switch, and it can only be used with the accounting protocol-related PDUs.

Specifying Inspur INOS-CN User Roles and SNMPv3 Parameters on AAA Servers

You can use the VSA Inspur-av-pair on AAA servers to specify user role mapping for the Inspur INOS-CN device using this format:

```
shell:roles="roleA roleB ..."
```

If you do not specify the role option in the Inspur-av-pair attribute, the default user role is network-operator.

You can also specify your SNMPv3 authentication and privacy protocol attributes as follows:

```
shell:roles="roleA roleB..." snmpv3:auth=SHA priv=AES-128
```

The SNMPv3 authentication protocol options are SHA and MD5. The privacy protocol options are AES-128 and DES. If you do not specify these options in the Inspur-av-pair attribute, MD5 and DES are the default authentication protocols.

3.6.12 Configuring Secure Login Features

Configuring Login Parameters

You can configure login parameters to automatically block further login attempts when a possible denial-of-service (DoS) attack is detected and slow down dictionary attacks by enforcing a quiet period if multiple failed connection attempts are detected.

SUMMARY STEPS

1. **configure terminal**
2. **[no] system login block-for *seconds* attempts *tries* within *seconds***
3. (Optional) **[no] system login quiet-mode access-class *acl-name***
4. (Optional) **show system login [failures]**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal	Enters global configuration mode.
Step 2	[no] system login block-for <i>seconds</i> attempts <i>tries</i> within	Configures the quiet mode time period. The range for all

	Command or Action	Purpose
	<p><i>seconds</i></p> <p>Example:</p> <pre>switch(config)# system login block-for 100 attempts 2 within 60</pre>	<p>arguments is from 1 to 65535.</p> <p>The example shows how to configure the switch to enter a 100-second quiet period if 2 failed login attempts are exceeded within 60 seconds.</p> <p>After you enter this command, all login attempts made through Telnet or SSH are denied during the quiet period.</p> <p>Access control lists (ACLs) are not exempt from the quiet period until the system command is entered.</p> <p>Note You must enter this command before any other login command can be used.</p>
Step 3	<p>(Optional) [no] system login quiet-mode access-class <i>acl-name</i></p> <p>Example:</p> <pre>switch(config)# system login quiet-mode access-class myacl</pre>	<p>Specifies an ACL that is to be applied to the switch when it changes to quiet mode. When the switch is in quiet mode, all login requests are denied, and the only available connection is through the console.</p>
Step 4	<p>(Optional) show system login [failures]</p> <p>Example:</p> <pre>switch(config)# show system login</pre>	<p>Displays the login parameters. The failures option displays information related only to failed login attempts.</p>
Step 5	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config)# copy running-config startup- config</pre>	<p>Copies the running configuration to the startup configuration.</p>

Restricting User Login Sessions

You can restrict the maximum number of simultaneous login sessions per user. Doing so prevents users from having multiple unwanted sessions and solves the potential security issue of unauthorized users accessing a valid SSH or Telnet session.

SUMMARY STEPS

1. **configure terminal**
2. **[no] user max-logins** *max-logins*
3. (Optional) **show running-config all | i max-login**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal</pre>	Enters global configuration mode.
Step 2	[no] user max-logins max-logins Example: <pre>switch(config)# user max-logins 1</pre>	Restricts the maximum number of simultaneous login sessions per user. The range is from 1 to 7. If you set the maximum login limit as 1, only one Telnet or SSH session is allowed per user. Note The configured login limit applies to all users. You cannot set a different limit for individual users.
Step 3	(Optional) show running-config all i max-login Example: <pre>switch(config)# show running-config all i max-login</pre>	Displays the maximum number of login sessions allowed per user.
Step 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Restricting the Password Length

You can restrict the minimum and maximum length of the user password. This feature enables you to increase system security by forcing the user to provide a strong password.

Before you begin

You must enable password strength checking using the **password strength-check** command. If you restrict the password length but do not enable password strength checking and the user enters a password that is not within the restricted length, an error appears, but a user account is created. To enforce the password length and prevent a user account from being created, you must enable password strength checking and restrict the password length.

SUMMARY STEPS

1. **configure terminal**
2. **[no] userpassphrase {min-length min-length | max-length max-length}**
3. (Optional) **show userpassphrase {length | max-length | min-length}**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal	Enters global configuration mode.
Step 2	[no] userpassphrase {min-length <i>min-length</i> max-length <i>max-length</i>} Example: switch(config)# userpassphrase min-length 8 max-length 80	Restricts the minimum and/or maximum length of the user password. The minimum password length is from 4 to 127 characters, and the maximum password length is from 80 to 127 characters.
Step 3	(Optional) show userpassphrase {length max-length min-length} Example: switch(config)# show userpassphrase length	Displays the minimum and maximum length of the user password.
Step 4	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Enabling the Password Prompt for the Username

You can configure the switch to prompt the user to enter a password after entering the username.

SUMMARY STEPS

1. **configure terminal**
2. **password prompt username**
3. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal	Enters global configuration mode.
Step 2	password prompt username Example: switch(config)# password prompt username Password prompt username is enabled.	Configures the switch to prompt the user to enter a password after she enters the username command without the password option or the snmp-server user command. The password that the user enters will be hidden. You can use the no form of this command to disable this feature.

	Command or Action	Purpose
	<p>After providing the required options in the username command, press enter.</p> <p>User will be prompted for the username password and password will be hidden.</p> <p>Note: Choosing password key in the same line while configuring user account, password will not be hidden.</p>	
Step 3	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Configuring the Shared Secret for RADIUS or TACACS+

The shared secret that you configure for remote authentication and accounting between the switch and the RADIUS or TACACS+ server should be hidden because it is sensitive information. You can use a separate command to generate an encrypted shared secret for the **radius-server [host] key** and **tacacs-server [host] key** commands. The SHA256 hashing method is used to store the encrypted shared secret.

SUMMARY STEPS

1. **configure terminal**
2. **generate type7_encrypted_secret**
3. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>switch# configure terminal</pre>	Enters global configuration mode.
Step 2	<p>generate type7_encrypted_secret</p> <p>Example:</p> <pre>switch(config)# generate type7_encrypted_secret</pre> <p>Type-7 (Vigenere) Encryption, Use this encrypted secret to configure radius and tacacs shared secret with key type 7.</p> <p>Copy complete secret with double quotes. Enter plain text secret: Confirm plain text secret:</p>	<p>Configures the RADIUS or TACACS+ shared secret with key type 7. You are prompted to enter the shared secret in plain text twice. The secret is hidden as you enter it. Then an encrypted version of the secret appears.</p> <p>Note You can generate the encrypted equivalent of a plain-text secret separately and configure the encrypted shared secret later using the radius-server [host] key and tacacs-server [host] key commands.</p>

	Command or Action	Purpose
	Type 7 Encrypted secret is : "fewhg"	
Step 3	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

3.7 Monitoring and Clearing the Local AAA Accounting Log

The Inspur INOS-CN device maintains a local log for the AAA accounting activity. You can monitor this log and clear it.

SUMMARY STEPS

1. **show accounting log** [*size* | **last-index** | **start-seqnum** *number* | **start-time** *year month day hh:mm:ss*]
2. (Optional) **clear accounting log** [**logflash**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	show accounting log [<i>size</i> last-index start-seqnum <i>number</i> start-time <i>year month day hh:mm:ss</i>] Example: switch# show accounting log	Displays the accounting log contents. By default, the command output contains up to 250,000 bytes of the accounting log. You can use the <i>size</i> argument to limit command output. The range is from 0 to 250000 bytes. You can also specify a starting sequence number or a starting time for the log output. The range of the starting index is from 1 to 1000000. Use the last-index keyword to display the value of the last index number in the accounting log file.
Step 2	(Optional) clear accounting log [logflash] Example: switch# clear aaa accounting log	Clears the accounting log contents. The logflash keyword clears the accounting log stored in the logflash.

3.8 Verifying the AAA Configuration

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

Command	Purpose

Command	Purpose
<code>show aaa accounting</code>	Displays AAA accounting configuration.
<code>show aaa authentication [login {ascii-authentication chap error-enable mschap mschapv2}]</code>	Displays AAA authentication login configuration information.
<code>show aaa groups</code>	Displays the AAA server group configuration.
<code>show login [failures]</code>	Displays the login parameters. The failures option displays information related only to failed login attempts. Note The clear login failures command clears the login failures in the current watch period.
<code>show login on-failure log</code>	Displays whether the switch is configured to log failed authentication messages to the syslog server.
<code>show login on-successful log</code>	Displays whether the switch is configured to log successful authentication messages to the syslog server.
<code>show running-config aaa [all]</code>	Displays the AAA configuration in the running configuration.
<code>show running-config all i max-login</code>	Displays the maximum number of login sessions allowed per user.
<code>show startup-config aaa</code>	Displays the AAA configuration in the startup configuration.
<code>show userpassphrase {length max-length min-length}</code>	Displays the minimum and maximum length of the user password.

3.9 Configuration Examples for AAA

The following example shows how to configure AAA:

```
aaa authentication login default group radius
aaa authentication login console group radius
```

```
aaa accounting default group radius
```

3.10 Configuration Examples for Login Parameters

The following example shows how to configure the switch to enter a 100-second quiet period if 3 failed login attempts is exceeded within 60 seconds. This example shows no login failures.

```
switch# configure terminal
switch(config)# login block-for 100 attempts 3 within
60 switch(config)# show login
No Quiet-Mode access list has been configured, default ACL will be applied.

Switch is enabled to watch for login Attacks.
If more than 3 login failures occur in 60 seconds or less,
logins will be disabled for 100 seconds.

Switch presently in Normal-Mode.
Current Watch Window remaining time 45 seconds.
Present login failure count 0.

switch(config)# show login failures
*** No logged failed login attempts with the device.***
```

The following example shows how to configure a quiet-mode ACL. All login requests are denied during the quiet period except hosts from the myacl ACL. This example also shows a login failure.

```
switch# configure terminal
switch(config)# login block-for 100 attempts 3 within
60 switch(config)# login quiet-mode access-class myacl
switch(config)# show login

Switch is enabled to watch for login Attacks.
If more than 3 login failures occur in 60 seconds or
less, logins will be disabled for 100 seconds.

Switch presently in Quiet-Mode.
Will remain in Quiet-Mode for 98 seconds.
Denying logins from all sources.

switch(config)# show login failures
Information about last 20 login failure's with the device.
-----
Username   Line SourceIPAddr Appname   TimeStamp
-----
asd        /dev/pts/0      171.70.55.158 login    Mon Oct  1 18:18:54 2018
qweq       /dev/pts/0      171.70.55.158 login    Mon Oct  1 18:19:02 2018
qwe        /dev/pts/0      171.70.55.158 login    Mon Oct  1 18:19:08 2018
-----
```

3.11 Configuration Examples for the Password Prompt Feature

The following example shows how to configure the switch to prompt the user to enter a password after she enters the **username** command and the error message that displays if she does not enter a password.


```

switch# configure terminal switch(config)#
password prompt username
Password prompt username is enabled.
After providing the required options in the username command, press enter. User
will be prompted for the username password and password will be hidden.
Note: Choosing password key in the same line while configuring user account, password will
not be hidden.

switch(config)# username user1

Enter password:
Confirm password:
warning: password for user:user1 not set. S/he may not be able to login

```

The following example shows how to configure the switch to prompt the user to enter a password after she enters the **snmp-server user** command and the prompts that then display to the user.

```

switch# configure terminal switch(config)#
password prompt username
Password prompt username is enabled.
After providing the required options in the username command, press enter.
User will be prompted for the username password and password will be hidden.
Note: Choosing password key in the same line while configuring user account, password will
not be hidden.

switch(config)# snmp-server user user1

Enter auth md5 password (Press Enter to Skip):
Enter auth sha password (Press Enter to Skip):

```

3.12 Additional References for AAA

This section includes additional information related to implementing AAA.

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not — been modified by this feature.	

CHAPTER 4 Configuring RADIUS

This chapter describes how to configure the Remote Access Dial-In User Service (RADIUS) protocol on Inspur INOS-CN devices.

This chapter includes the following sections:

4.1 About RADIUS

The RADIUS distributed client/server system allows you to secure networks against unauthorized access. In the Inspur implementation, RADIUS clients run on Inspur INOS-CN devices and send authentication and accounting requests to a central RADIUS server that contains all user authentication and network service access information.

4.1.1 RADIUS Network Environments

RADIUS can be implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

You can use RADIUS in the following network environments that require access security:

- Networks with multiple-vendor network devices, each supporting RADIUS. For example, network devices from several vendors can use a single RADIUS server-based security database.
- Networks already using RADIUS. You can add a Inspur INOS-CN device with RADIUS to the network. This action might be the first step when you make a transition to a AAA server.³⁹
- Networks that require resource accounting. You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider (ISP) might use a freeware-based version of the RADIUS access control and accounting software to meet special security and billing needs.
- Networks that support authentication profiles. Using the RADIUS server in your network, you can configure AAA authentication and set up per-user profiles. Per-user profiles enable the Inspur INOS-CN device to better manage ports using their existing RADIUS solutions and to efficiently manage shared resources to offer different service-level agreements.

4.1.2 RADIUS Operation

When a user attempts to log in and authenticate to a Inspur INOS-CN device using RADIUS, the following process occurs:

- The user is prompted for and enters a username and password.
- The username and encrypted password are sent over the network to the RADIUS server.
- The user receives one of the following responses from the RADIUS server:

ACCEPT

The user is authenticated.

REJECT

The user is not authenticated and is prompted to reenter the username and password, or access is denied.

CHALLENGE

A challenge is issued by the RADIUS server. The challenge collects additional data from the user.

CHANGE PASSWORD

A request is issued by the RADIUS server, asking the user to select a new password.

The ACCEPT or REJECT response is bundled with additional data that is used for EXEC or network authorization. You must first complete RADIUS authentication before using RADIUS authorization. The additional data included with the ACCEPT or REJECT packets consists of the following:

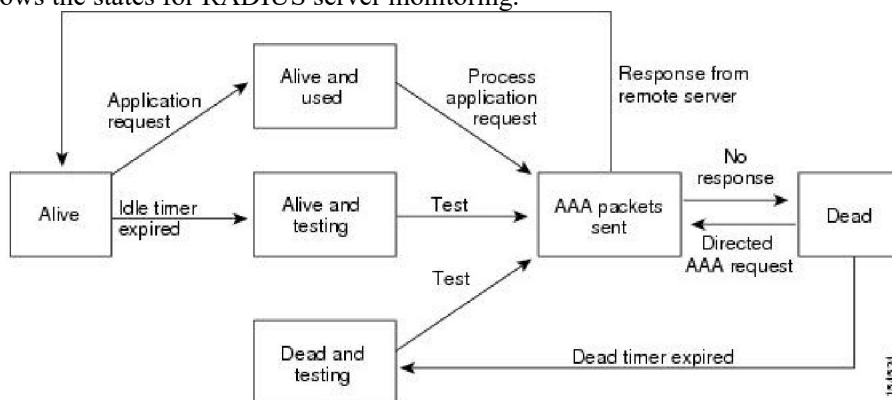
- Services that the user can access, including Telnet, rlogin, or local-area transport (LAT) connections, and Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services.
- Connection parameters, including the host or client IPv4 or IPv6 address, access list, and user timeouts.

4.1.3 RADIUS Server Monitoring

An unresponsive RADIUS server can cause a delay in processing AAA requests. You can configure the Inspur INOS-CN device to periodically monitor a RADIUS server to check whether it is responding (or alive) to save time in processing AAA requests. The Inspur INOS-CN device marks unresponsive RADIUS servers as dead and does not send AAA requests to any dead RADIUS servers. The Inspur INOS-CN device periodically monitors the dead RADIUS servers and brings them to the alive state once they respond. This monitoring process verifies that a RADIUS server is in a working state before real AAA requests are sent its way. Whenever a RADIUS server changes to the dead or alive state, a Simple Network Management Protocol (SNMP) trap is generated and the Inspur INOS-CN device displays an error message that a failure is taking place.

Figure 2: RADIUS Server States

This figure shows the states for RADIUS server monitoring.



4.1.4 Vendor-Specific Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating VSAs between the network access server and the RADIUS server. The IETF uses attribute 26. VSAs allow vendors to support their own extended attributes that are not suitable for general use. The Inspur RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Inspur vendor ID is 48797, and the supported option is vendor type 1, which is named Inspur-av-pair. The value is a string with the following format:

```
protocol : attribute separator value *
```

The protocol is a Inspur attribute for a particular type of authorization, the separator is = (equal sign) for mandatory attributes, and * (asterisk) indicates optional attributes.

When you use RADIUS servers for authentication on a Inspur INOS-CN device, the RADIUS protocol directs the RADIUS server to return user attributes, such as authorization information, with authentication results. This authorization information is specified through VSAs.

The following VSA protocol options are supported by the Inspur INOS-CN software:

Shell

Protocol used in access-accept packets to provide user profile information.

Accounting

Protocol used in accounting-request packets. If a value contains any white spaces, you should enclose the value within double quotation marks.

The Inspur INOS-CN software supports the following attributes:

roles

Lists all the roles to which the user belongs. The value field is a string that lists the role names delimited by white space. For example, if the user belongs to roles network-operator and network-admin, the value field would be network-operator network-admin. This subattribute, which the RADIUS server sends in the VSA portion of the Access-Accept frames, can only be used with the shell protocol value. The following examples show the roles attribute that is supported by the Inspur Access Control Server (ACS):

```
shell:roles=network-operator network-admin

shell:roles*"network-operator network-admin"
```

The following examples show the roles attribute that is supported by FreeRADIUS:

```
Inspur-AVPair = shell:roles=\network-operator network-admin\

Inspur-AVPair = shell:roles*\network-operator network-admin\
```

accountinginfo

Stores accounting information in addition to the attributes covered by a standard RADIUS accounting protocol. This attribute is sent only in the VSA portion of the Account-Request frames from the RADIUS client on the switch. It can be used only with the accounting protocol data units (PDUs).

4.2 Licensing Requirements for RADIUS

This table shows the licensing requirements for this feature.

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

4.3 Prerequisites for RADIUS

RADIUS has the following prerequisites:

- Obtain IPv4 or IPv6 addresses or hostnames for the RADIUS servers.
- Obtain keys from the RADIUS servers.
- Ensure that the Inspur INOS-CN device is configured as a RADIUS client of the AAA servers.

4.4 Guidelines and Limitations for RADIUS

RADIUS has the following guidelines and limitations:

- You can configure a maximum of 64 RADIUS servers on the Inspur INOS-CN device.

- If you have a user account configured on the local Inspur INOS-CN device that has the same name as a remote user account on an AAA server, the Inspur INOS-CN software applies the user roles for the local user account to the remote user, not the user roles configured on the AAA server.
- Only the RADIUS protocol supports one-time passwords.
- For CN129-X6136YC-R, CN129-X636C-R, and CN129-X636Q-R line cards and the CN12908-FM-R fabric module, RADIUS authentication fails for usernames with special characters.
- Inspur CN12900 Series switches support the CLI command, `aaa authentication login ascii-authentication`, only for TACAAS+, but not for RADIUS. Ensure that you have disabled `aaa authentication login ascii-authentication` switch so that the default authentication, PAP, is enabled. Otherwise, you will see syslog errors.

4.5 Default Settings for RADIUS

This table lists the default settings for RADIUS parameters.

Table 7: Default RADIUS Parameter Settings

Parameters	Default
Server roles	Authentication and accounting
Dead timer interval	0 minutes
Retransmission count	1
Retransmission timer interval	5 seconds
Authentication port	1812
Accounting port	1813
Idle timer interval	0 minutes
Periodic server monitoring username	test
Periodic server monitoring password	test

4.6 Configuring RADIUS Servers

This section describes how to configure RADIUS servers on a Inspur INOS-CN device.

4.6.1 RADIUS Server Configuration Process

1. Establish the RADIUS server connections to the Inspur INOS-CN device.
2. Configure the RADIUS secret keys for the RADIUS servers.
3. If needed, configure RADIUS server groups with subsets of the RADIUS servers for AAA authentication methods.
4. If needed, configure any of the following optional parameters:
 - Dead-time interval
 - RADIUS server specification allowed at user login
 - Timeout interval
 - TCP port
5. (Optional) If RADIUS distribution is enabled, commit the RADIUS configuration to the fabric.

4.6.2 Configuring RADIUS Server Hosts

To access a remote RADIUS server, you must configure the IP address or hostname of a RADIUS server. You can configure up to 64 RADIUS servers.

Before you begin

Ensure that the server is already configured as a member of the server group.

Ensure that the server is configured to authenticate RADIUS traffic.

Ensure that the Inspur INOS-CN device is configured as a RADIUS client of the AAA servers.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*}
3. (Optional) **show radius** {*pending* | *pending-diff*}
4. (Optional) **radius commit**
5. **exit**
6. (Optional) **show radius-server**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> }	Specifies the IPv4 or IPv6 address or hostname for a RADIUS server to use for authentication.
Step 3	(Optional) show radius { <i>pending</i> <i>pending-diff</i> }	Displays the RADIUS configuration pending for distribution.
Step 4	(Optional) radius commit Example: switch(config)# radius commit	Applies the RADIUS configuration changes in the temporary database to the running configuration.
Step 5	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 6	(Optional) show radius-server Example: switch# show radius-server	Displays the RADIUS server configuration.

	Command or Action	Purpose
Step 7	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

4.6.3 Configuring Global RADIUS Keys

You can configure RADIUS keys for all servers used by the Inspur INOS-CN device. A RADIUS key is a shared secret text string between the Inspur INOS-CN device and the RADIUS server hosts.

Before you begin

- Obtain the RADIUS key values for the remote RADIUS servers.
- Configure the RADIUS key on the remote RADIUS servers.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server key [0 | 6 | 7] key-value**
3. **exit**
4. (Optional) **show radius-server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	radius-server key [0 6 7] key-value Example: switch(config)# radius-server key 0 QsEfThUkO Example: switch(config)# radius-server key 7 "fewhg"	Specifies a RADIUS key for all RADIUS servers. You can specify that the <i>key-value</i> is in clear text format (0), is type-6 encrypted (6), or is type-7 encrypted (7). The Inspur INOS-CN software encrypts a clear text key before saving it to the running configuration. The default format is clear text. The maximum length is 63 characters. By default, no RADIUS key is configured. Note If you already configured a shared secret using the generate type7_encrypted_secret command, enter it in quotation marks, as shown in the second example.

	Command or Action	Purpose
Step 3	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 4	(Optional) show radius-server Example: switch# show radius-server	Displays the RADIUS server configuration. Note The RADIUS keys are saved in encrypted form in the running configuration. Use the show running-config command to display the encrypted RADIUS keys.
Step 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

4.6.4 Configuring a Key for a Specific RADIUS Server

You can configure a key on the Inspur INOS-CN device for a specific RADIUS server. A RADIUS key is a secret text string shared between the Inspur INOS-CN device and a specific RADIUS server.

Before you begin

- Configure one or more RADIUS server hosts.
- Obtain the key value for the remote RADIUS server.
- Configure the key on the RADIUS server.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **key** [0 | 6 | 7] *key-value*
3. **exit**
4. (Optional) **show radius-server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } key [0 6 7] <i>key-value</i> Example:	Specifies a RADIUS key for a specific RADIUS server. You can specify that the <i>key-value</i> is in clear text format (0), is type-6 encrypted (6), or is type-7 encrypted

	Command or Action	Purpose
	<pre>switch(config)# radius-server host 10.10.1.1 key 0 P1IjUhYg</pre> <p>Example:</p> <pre>switch(config)# radius-server host 10.10.1.1 key 7 "fewhg"</pre>	<p>(7). The Inspur INOS-CN software encrypts a clear text key before saving it to the running configuration. The default format is clear text. The maximum length is 63 characters. This RADIUS key is used instead of the global RADIUS key.</p> <p>Note If you already configured a shared secret using the generate type7_encrypted_secret command, enter it in quotation marks, as shown in the second example</p>
Step 3	<p>exit</p> <p>Example:</p> <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 4	<p>(Optional) show radius-server</p> <p>Example:</p> <pre>switch# show radius-server</pre>	<p>Displays the RADIUS server configuration.</p> <p>Note The RADIUS keys are saved in encrypted form in the running configuration. Use the show running-config command to display the encrypted RADIUS keys.</p>
Step 5	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

4.6.5 Configuring RADIUS Server Groups

You can specify one or more remote AAA servers for authentication using server groups. All members of a group must belong to the RADIUS protocol. The servers are tried in the same order in which you configure them.

You can configure these server groups at any time but they only take effect when you apply them to an AAA service.

Before you begin

Ensure that all servers in the group are RADIUS servers.

SUMMARY STEPS

1. **configure terminal**
2. **aaa group server radius *group-name***

3. **server** {*ipv4-address* | *ipv6-address* | *hostname*}
4. (Optional) **deadtime** *minutes*
5. (Optional) **server** {*ipv4-address* | *ipv6-address* | *hostname*}
6. (Optional) **use-vrf** *vrf-name*
7. **exit**
8. (Optional) **show radius-server groups** [*group-name*]
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	aaa group server radius <i>group-name</i> Example: <pre>switch(config)# aaa group server radius RadServer switch(config-radius)#</pre>	Creates a RADIUS server group and enters the RADIUS server group configuration submode for that group. The <i>group-name</i> argument is a case-sensitive alphanumeric string with a maximum length of 127 characters.
Step 3	server { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> }	Configures the RADIUS server as a member of the RADIUS server group. If the specified RADIUS server is not found, configure it using the radius-server host command and retry this command.
Step 4	(Optional) deadtime <i>minutes</i> Example: <pre>switch(config-radius)# deadtime 30</pre>	Configures the monitoring dead time. The default is 0 minutes. The range is from 1 through 1440. Note If the dead-time interval for a RADIUS server group is greater than zero (0), that value takes precedence over the global dead-time value.
Step 5	(Optional) server { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> }	Configures the RADIUS server as a member of the RADIUS server group. Tip If the specified RADIUS server is not found, configure it using the radius-server host command and retry this command.

	Command or Action	Purpose
Step 6	(Optional) <code>use-vrf vrf-name</code> Example: <code>switch(config-radius)# use-vrf vrf1</code>	Specifies the VRF to use to contact the servers in the server group.
Step 7	<code>exit</code> Example: <code>switch(config-radius)# exit</code> <code>switch(config)#</code>	Exits configuration mode.
Step 8	(Optional) <code>show radius-server groups [group-name]</code> Example: <code>switch(config)# show radius-server groups</code>	Displays the RADIUS server group configuration.
Step 9	(Optional) <code>copy running-config startup-config</code> Example: <code>switch(config)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

4.6.6 Configuring the Global Source Interface for RADIUS Server Groups

You can configure a global source interface for RADIUS server groups to use when accessing RADIUS servers. You can also configure a different source interface for a specific RADIUS server group. By default, the Inspur INOS-CN software uses any available interface.

SUMMARY STEPS

1. `configure terminal`
2. `ip radius source-interface interface`
3. `exit`
4. (Optional) `show radius-server`
5. (Optional) `copy running-config startup config`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>configure terminal</code> Example: <code>switch# configure terminal</code> <code>switch(config)</code>	Enters global configuration mode.
Step 2	<code>ip radius source-interface interface</code> Example: <code>switch(config)# ip radius source-interface mgmt 0</code>	Configures the global source interface for all RADIUS server groups configured on the device.
Step 3	<code>exit</code>	Exits configuration mode.

	Command or Action	Purpose
	Example: <pre>switch(config)# exit switch#</pre>	
Step 4	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	Displays the RADIUS server configuration information.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

4.6.7 Allowing Users to Specify a RADIUS Server at Login

By default, the Inspur INOS-CN device forwards an authentication request based on the default AAA authentication method. You can configure the Inspur INOS-CN device to allow the user to specify a VRF and RADIUS server to send the authentication request by enabling the directed-request option. If you enable this option, the user can log in as *username@vrfname:hostname*, where *vrfname* is the VRF to use and **hostname** is the name of a configured RADIUS server.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server directed-request**
3. (Optional) **show radius {pending | pending-diff}**
4. (Optional) **radius commit**
5. **exit**
6. (Optional) **show radius-server directed-request**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	radius-server directed-request Example: <pre>switch(config)# radius-server directed-request</pre>	Allows users to specify a RADIUS server to send the authentication request when logging in. The default is disabled.
Step 3	(Optional) show radius {pending pending-diff} Example:	Displays the RADIUS configuration pending for distribution.

	Command or Action	Purpose
	<code>switch(config)# show radius pending</code>	
Step 4	(Optional) radius commit Example: <code>switch(config)# radius commit</code>	Applies the RADIUS configuration changes in the temporary database to the running configuration.
Step 5	exit Example: <code>switch(config)# exit</code> <code>switch#</code>	Exits configuration mode.
Step 6	(Optional) show radius-server directed-request Example: <code>switch# show radius-server directed-request</code>	Displays the directed request configuration.
Step 7	(Optional) copy running-config startup-config Example: <code>switch# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

4.6.8 Configuring the Global RADIUS Transmission Retry Count and Timeout Interval

You can configure a global retransmission retry count and timeout interval for all RADIUS servers. By default, a Inspur INOS-CN device retries transmission to a RADIUS server only once before reverting to local authentication. You can increase this number up to a maximum of five retries per server. The timeout interval determines how long the Inspur INOS-CN device waits for responses from RADIUS servers before declaring a timeout failure.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server retransmit** *count*
3. **radius-server timeout** *seconds*
4. (Optional) **show radius** {**pending** | **pending-diff**}
5. (Optional) **radius commit**
6. **exit**
7. (Optional) **show radius-server**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	Enters global configuration mode.
Step 2	radius-server retransmit <i>count</i>	Specifies the retransmission count for all RADIUS

	Command or Action	Purpose
	Example: <pre>switch(config)# radius-server retransmit 3</pre>	servers. The default retransmission count is 1 and the range is from 0 to 5.
Step 3	radius-server timeout <i>seconds</i> Example: <pre>switch(config)# radius-server timeout 10</pre>	Specifies the transmission timeout interval for RADIUS servers. The default timeout interval is 5 seconds and the range is from 1 to 60 seconds.
Step 4	(Optional) show radius { pending pending-diff } Example: <pre>switch(config)# show radius pending</pre>	Displays the RADIUS configuration pending for distribution.
Step 5	(Optional) radius commit Example: <pre>switch(config)# radius commit</pre>	Applies the RADIUS configuration changes in the temporary database to the running configuration.
Step 6	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 7	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	Displays the RADIUS server configuration.
Step 8	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

4.6.9 Configuring the RADIUS Transmission Retry Count and Timeout Interval for a Server

By default, a Inspur INOS-CN device retries a transmission to a RADIUS server only once before reverting to local authentication. You can increase this number up to a maximum of five retries per server. You can also set a timeout interval that the Inspur INOS-CN device waits for responses from RADIUS servers before declaring a timeout failure.

Before you begin

Configure one or more RADIUS server hosts.

SUMMARY STEPS

1. **configure terminal**

2. **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **retransmit count**
3. **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **timeout seconds**
4. (Optional) **show radius** {**pending** | **pending-diff**}
5. (Optional) **radius commit**
6. **exit**
7. (Optional) **show radius-server**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } retransmit count Example: <pre>switch(config)# radius-server host server1 retransmit 3</pre>	Specifies the retransmission count for a specific server. The default is the global value. Note The retransmission count value specified for a RADIUS server overrides the count specified for all RADIUS servers.
Step 3	radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } timeout seconds Example: <pre>switch(config)# radius-server host server1 timeout 10</pre>	Specifies the transmission timeout interval for a specific server. The default is the global value. Note The timeout interval value specified for a RADIUS server overrides the interval value specified for all RADIUS servers.
Step 4	(Optional) show radius { pending pending-diff } Example: <pre>switch(config)# show radius pending</pre>	Displays the RADIUS configuration pending for distribution.
Step 5	(Optional) radius commit Example: <pre>switch(config)# radius commit</pre>	Applies the RADIUS configuration changes in the temporary database to the running configuration and distributes RADIUS configuration to other Inspur INOS-CN devices if you have enabled CFS configuration distribution for the user role feature.
Step 6	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.

	Command or Action	Purpose
Step 7	(Optional) show radius-server Example: switch# show radius-server	Displays the RADIUS server configuration.
Step 8	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

4.6.10 Configuring Accounting and Authentication Attributes for RADIUS Servers

You can specify that a RADIUS server is to be used only for accounting purposes or only for authentication purposes. By default, RADIUS servers are used for both accounting and authentication. You can also specify the destination UDP port numbers where RADIUS accounting and authentication messages should be sent if there is a conflict with the default port.

Before you begin

Configure one or more RADIUS server hosts.

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **acct-port** *udp-port*
3. (Optional) **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **accounting**
4. (Optional) **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **auth-port** *udp-port*
5. (Optional) **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **authentication**
6. (Optional) **show radius** {**pending** | **pending-diff**}
7. (Optional) **radius commit**
8. **exit**
9. (Optional) **show radius-server**
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	(Optional) radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } acct-port <i>udp-port</i> Example: switch(config)# radius-server host 10.10.1.1 acct-port 2004	Specifies a UDP port to use for RADIUS accounting messages. The default UDP port is 1813. The range is from 0 to 65535.

	Command or Action	Purpose
Step 3	(Optional) radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } accounting Example: <pre>switch(config)# radius-server host 10.10.1.1 accounting</pre>	Specifies to use the RADIUS server only for accounting purposes. The default is both accounting and authentication.
Step 4	(Optional) radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } auth-port <i>udp-port</i> Example: <pre>switch(config)# radius-server host 10.10.2.2 auth-port 2005</pre>	Specifies a UDP port to use for RADIUS authentication messages. The default UDP port is 1812. The range is from 0 to 65535.
Step 5	(Optional) radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } authentication Example: <pre>switch(config)# radius-server host 10.10.2.2 authentication</pre>	Specifies to use the RADIUS server only for authentication purposes. The default is both accounting and authentication.
Step 6	(Optional) show radius { <i>pending</i> <i>pending-diff</i> } Example: <pre>switch(config)# show radius pending</pre>	Displays the RADIUS configuration pending for distribution.
Step 7	(Optional) radius commit Example: <pre>switch(config)# radius commit</pre>	Applies the RADIUS configuration changes in the temporary database to the running configuration.
Step 8	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 9	(Optional) show radius-server Example: <pre>switch(config)# show radius-server</pre>	Displays the RADIUS server configuration.
Step 10	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

4.6.11 Configuring Global Periodic RADIUS Server Monitoring

You can monitor the availability of all RADIUS servers without having to configure the test parameters for each

server individually. Any servers for which test parameters are not configured are monitored using the global level parameters.

Before you begin

Enable RADIUS.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server test** {*idle-time minutes* | **password** *password* [*idle-time minutes*] | **username** *name* [**password** *password* [*idle-time minutes*]]}
3. **radius-server** **deadtime** *minutes*
4. **exit**
5. (Optional) **show radius-server**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	radius-server test { <i>idle-time minutes</i> password <i>password</i> [<i>idle-time minutes</i>] username <i>name</i> [password <i>password</i> [<i>idle-time minutes</i>]]} Example: switch(config)# radius-server test username user1 password Ur2Gd2BH idle-time 3	Specifies parameters for global server monitoring. The default username is test, and the default password is test. The default value for the idle timer is 0 minutes, and the valid range is from 0 to 1440 minutes. Note For periodic RADIUS server monitoring, the idle timer value must be greater than 0.
Step 3	radius-server deadtime <i>minutes</i> Example: switch(config)# radius-server deadtime 5	Specifies the number of minutes before the Inspur INOS-CN device checks a RADIUS server that was previously unresponsive. The default value is 0 minutes, and the valid range is from 0 to 1440 minutes.
Step 4	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 5	(Optional) show radius-server Example: switch# show radius-server	Displays the RADIUS server configuration.

	Command or Action	Purpose
Step 6	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

4.6.12 Configuring Periodic RADIUS Server Monitoring on Individual Servers

You can monitor the availability of individual RADIUS servers. The configuration parameters include the username and password to use for the server and an idle timer. The idle timer specifies the interval during which a RADIUS server receives no requests before the Inspur INOS-CN device sends out a test packet. You can configure this option to test servers periodically, or you can run a one-time only test.

Before you begin

Enable RADIUS.

Add one or more RADIUS server hosts.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **test** {**idle-time** *minutes* | **password** *password* [*idle-time minutes*] | **username** *name* [**password** *password* [*idle-time minutes*]]}
3. **radius-server deadtime** *minutes*
4. **exit**
5. (Optional) **show radius-server**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } test { idle-time <i>minutes</i> password <i>password</i> [<i>idle-time minutes</i>] username <i>name</i> [password <i>password</i> [<i>idle-time minutes</i>]]} Example: switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3	Specifies parameters for individual server monitoring. The default username is test, and the default password is test. The default value for the idle timer is 0 minutes, and the valid range is from 0 to 1440 minutes. Note For periodic RADIUS server monitoring, you must set the idle timer to a value greater than 0.
Step 3	radius-server deadtime <i>minutes</i>	Specifies the number of minutes before the Inspur

	Command or Action	Purpose
	Example: <pre>switch(config)# radius-server deadtime 5</pre>	INOS-CN device checks a RADIUS server that was previously unresponsive. The default value is 0 minutes, and the valid range is from 1 to 1440 minutes.
Step 4	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 5	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	Displays the RADIUS server configuration.
Step 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

4.6.13 Configuring the RADIUS Dead-Time Interval

You can configure the dead-time interval for all RADIUS servers. The dead-time interval specifies the time that the Inspur INOS-CN device waits after declaring a RADIUS server is dead, before sending out a test packet to determine if the server is now alive. The default value is 0 minutes.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server deadtime *minutes***
3. (Optional) **show radius {pending | pending-diff}**
4. (Optional) **radius commit**
5. **exit**
6. (Optional) **show radius-server**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	radius-server deadtime <i>minutes</i> Example: <pre>switch(config)# radius-server deadtime 5</pre>	Configures the dead-time interval. The default value is 0 minutes. The range is from 1 to 1440 minutes.

	Command or Action	Purpose
Step 3	(Optional) show radius {pending pending-diff} Example: switch(config)# show radius pending	Displays the RADIUS configuration pending for distribution.
Step 4	(Optional) radius commit Example: switch(config)# radius commit	Applies the RADIUS configuration changes in the temporary database to the running configuration.
Step 5	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 6	(Optional) show radius-server Example: switch# show radius-server	Displays the RADIUS server configuration.
Step 7	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

4.6.14 Configuring One-Time Passwords

One-time password (OTP) support is available for Inspur INOS-CN devices through the use of RSA SecurID token servers. With this feature, users authenticate to a Inspur INOS-CN device by entering both a personal identification number (or one-time password) and the token code being displayed at that moment on their RSA SecurID token.

Before you begin

On the Inspur INOS-CN device, configure a RADIUS server host and remote default login authentication. Ensure that the following are installed:

- Inspur Secure Access Control Server (ACS) version 4.2
- RSA Authentication Manager version 7.1 (the RSA SecurID token server)
- RSA ACE Agent/Client

No configuration (other than a RADIUS server host and remote authentication) is required on the Inspur INOS-CN device to support one-time passwords. However, you must configure the Inspur Secure ACS as follows:

1. Enable RSA SecurID token server authentication.
2. Add the RSA SecurID token server to the Unknown User Policy database.

4.6.15 Manually Monitoring RADIUS Servers or Groups

You can manually issue a test message to a RADIUS server or to a server group.

SUMMARY STEPS

1. **test aaa server radius {ipv4-address | ipv6-address | hostname} [vrf vrf-name] username password**
2. **test aaa group group-name username password**

DETAILED STEPS

	Command or Action	Purpose
Step 1	test aaa server radius { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } [vrf <i>vrf-name</i>] <i>username password</i> Example: <pre>switch# test aaa server radius 10.10.1.1 user1 Ur2Gd2BH</pre>	Sends a test message to a RADIUS server to confirm availability.
Step 2	test aaa group <i>group-name username password</i> Example: <pre>switch# test aaa group RadGroup user2 As3He3CI</pre>	Sends a test message to a RADIUS server group to confirm availability.

4.7 Verifying the RADIUS Configuration

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

Command	Purpose
show radius { status pending pending-diff }	Displays the RADIUS Inspur Fabric Services distribution status and other details.
show running-config radius [all]	Displays the RADIUS configuration in the running configuration.
show startup-config radius	Displays the RADIUS configuration in the startup configuration.
show radius-server [<i>hostname</i> <i>ipv4-address</i> <i>ipv6-address</i>] [directed-request groups sorted statistics]	Displays all configured RADIUS server parameters.

4.8 Monitoring RADIUS Servers

You can monitor the statistics that the Inspur INOS-CN device maintains for RADIUS server activity.

Before you begin

Configure one or more RADIUS server hosts.

SUMMARY STEPS

1. **show radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	show radius-server statistics { <i>hostname</i> <i>ipv4-address</i> <i>ipv6-address</i> }	Displays the RADIUS statistics.

Example:

```
switch# show radius-server statistics
10.10.1.1
```

4.9 Clearing RADIUS Server Statistics

You can display the statistics that the Inspur INOS-CN device maintains for RADIUS server activity.

Before you begin

Configure RADIUS servers on the Inspur INOS-CN device.

SUMMARY STEPS

1. (Optional) **show radius-server statistics** {hostname | ipv4-address | ipv6-address}
2. **clear radius-server statistics** {hostname | ipv4-address | ipv6-address}

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) show radius-server statistics {hostname ipv4-address ipv6-address} Example: switch# show radius-server statistics 10.10.1.1	Displays the RADIUS server statistics on the Inspur INOS-CN device.
Step 2	clear radius-server statistics {hostname ipv4-address ipv6-address} Example: switch# clear radius-server statistics 10.10.1.1	Clears the RADIUS server statistics.

4.10 Configuration Example for RADIUS

The following example shows how to configure RADIUS:

```
radius-server key 7 "ToIkLhPpG"
radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
ba group server radius
RadServer server 10.10.1.1
```

4.11 Where to Go Next

You can now configure AAA authentication methods to include the server groups.

4.12 Additional References for RADIUS

This section describes additional information related to implementing RADIUS.

Related Documents

Related Topic	Document Title
VRF configuration	<i>Inspur CN12900 Series INOS-CN Unicast Routing Configuration Guide</i>

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not — been modified by this feature.	

CHAPTER 5 Configuring TACACS+

This chapter describes how to configure the Terminal Access Controller Access Control System Plus (TACACS+) protocol on Inspur INOS-CN devices.

This chapter includes the following sections:

5.1 About TACACS+

The TACACS+ security protocol provides centralized validation of users attempting to gain access to a Inspur INOS-CN device. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your Inspur INOS-CN device are available.

TACACS+ provides for separate authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service—authentication, authorization, and accounting—independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

The TACACS+ client/server protocol uses TCP (TCP port 49) for transport requirements. Inspur INOS-CN devices provide centralized authentication using the TACACS+ protocol.

5.1.1 TACACS+ Advantages

TACACS+ has the following advantages over RADIUS authentication:

- Provides independent AAA facilities. For example, the Inspur INOS-CN device can authorize access without authenticating.
- Uses the TCP transport protocol to send data between the AAA client and server, making reliable transfers with a connection-oriented protocol.
- Encrypts the entire protocol payload between the switch and the AAA server to ensure higher data confidentiality. The RADIUS protocol only encrypts passwords.

5.1.2 TACACS+ Operation for User Login

When a user attempts a Password Authentication Protocol (PAP) login to a Inspur INOS-CN device using TACACS+, the following actions occur:

1. When the Inspur INOS-CN device establishes a connection, it contacts the TACACS+ daemon to obtain the username and password.
2. The Inspur INOS-CN device will eventually receive one of the following responses from the TACACS+ daemon:

ACCEPT

User authentication succeeds and service begins. If the Inspur INOS-CN device requires user authorization, authorization begins.

REJECT

User authentication failed. The TACACS+ daemon either denies further access to the user or prompts the user to retry the login sequence.

ERROR

An error occurred at some time during authentication either at the daemon or in the network connection between

the daemon and the Inspur INOS-CN device. If the Inspur INOS-CN device receives an ERROR response, the Inspur INOS-CN device tries to use an alternative method for authenticating the user.

After authentication, the user also undergoes an additional authorization phase if authorization has been enabled on the Inspur INOS-CN device. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

3. If TACACS+ authorization is required, the Inspur INOS-CN device again contacts the TACACS+ daemon and it returns an ACCEPT or REJECT authorization response. An ACCEPT response contains attributes that are used to direct the EXEC or NETWORK session for that user and determines the services that the user can access.

Services include the following:

- Telnet, rlogin, Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services
- Connection parameters, including the host or client IP address (IPv4 or IPv6), access list, and user timeouts

5.1.3 Default TACACS+ Server Encryption Type and Secret Key

You must configure the TACACS+ secret key to authenticate the switch to the TACACS+ server. A secret key is a secret text string shared between the Inspur INOS-CN device and the TACACS+ server host. The length of the key is restricted to 63 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global secret key for all TACACS+ server configurations on the Inspur INOS-CN device to use.

You can override the global secret key assignment by explicitly using the **key** option when configuring an individual TACACS+ server.

5.1.4 Command Authorization Support for TACACS+ Servers

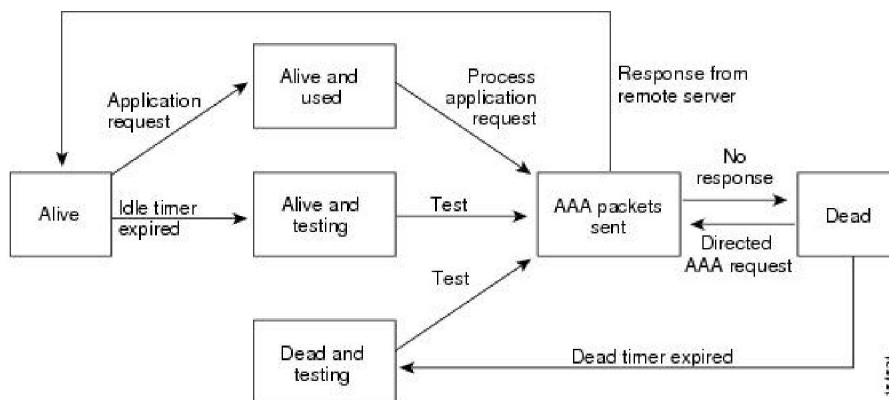
By default, command authorization is done against a local database in the Inspur INOS-CN software when an authenticated user enters a command at the command-line interface (CLI). You can also verify authorized commands for authenticated users using TACACS+.

5.1.5 TACACS+ Server Monitoring

An unresponsive TACACS+ server can delay the processing of AAA requests. A Inspur INOS-CN device can periodically monitor a TACACS+ server to check whether it is responding (or alive) to save time in processing AAA requests. The Inspur INOS-CN device marks unresponsive TACACS+ servers as dead and does not send AAA requests to any dead TACACS+ servers. A Inspur INOS-CN device periodically monitors dead TACACS+ servers and brings them to the alive state once they are responding. This process verifies that a TACACS+ server is in a working state before real AAA requests are sent its way. Whenever a TACACS+ server changes to the dead or alive state, a Simple Network Management Protocol (SNMP) trap is generated and the Inspur INOS-CN device displays an error message that a failure is taking place before it can impact performance.

Figure 3: TACACS+ Server States

This figure shows the server states for TACACS+ server monitoring.



5.1.6 Vendor-Specific Attributes for TACACS+

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific attributes (VSAs) between the network access server and the TACACS+ server. The IETF uses attribute 26. VSAs allow vendors to support their own extended attributes that are not suitable for general use.

Inspur VSA Format for TACACS+

The Inspur TACACS+ implementation supports one vendor-specific option using the format recommended in the IETF specification. The Inspur vendor ID is 48797, and the supported option is vendor type 1, which is named Inspur-av-pair. The value is a string with the following format:

```
protocol : attribute separator value *
```

The protocol is a Inspur attribute for a particular type of authorization, the separator is = (equal sign) for mandatory attributes, and * (asterisk) indicates optional attributes.

When you use TACACS+ servers for authentication on a Inspur INOS-CN device, the TACACS+ protocol directs the TACACS+ server to return user attributes, such as authorization information, along with authentication results. This authorization information is specified through VSAs.

The following VSA protocol options are supported by the Inspur INOS-CN software:

Shell

Protocol used in access-accept packets to provide user profile information.

Accounting

Protocol used in accounting-request packets. If a value contains any white spaces, you should enclose the value within double quotation marks.

The Inspur INOS-CN software supports the following attributes:

roles

Lists all the roles to which the user belongs. The value field is a string that lists the role names delimited by white space. For example, if the user belongs to roles network-operator and network-admin, the value field would be network-operator network-admin. This subattribute, which the TACACS+ server sends in the VSA portion of the Access-Accept frames, can only be used with the shell protocol value. The following examples show the roles attribute as supported by Inspur ACS:

```
shell:roles=network-operator network-admin
```

```
shell:roles*network-operator network-admin
```

accountinginfo

Stores accounting information in addition to the attributes covered by a standard TACACS+ accounting protocol. This attribute is sent only in the VSA portion of the Account-Request frames from the TACACS+ client on the switch. It can be used only with the accounting protocol data units (PDUs).

5.2 Licensing Requirements for TACACS+

The following table shows the licensing requirements for this feature:

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

5.3 Prerequisites for TACACS+

TACACS+ has the following prerequisites:

- Obtain the IPv4 or IPv6 addresses or hostnames for the TACACS+ servers.
- Obtain the secret keys from the TACACS+ servers, if any.
- Ensure that the Inspur INOS-CN device is configured as a TACACS+ client of the AAA servers.

5.4 Guidelines and Limitations for TACACS+

TACACS+ has the following guidelines and limitations:

- You can configure a maximum of 64 TACACS+ servers on the Inspur INOS-CN device.
- If you have a user account configured on the local Inspur INOS-CN device that has the same name as a remote user account on an AAA server, the Inspur INOS-CN software applies the user roles for the local user account to the remote user, not the user roles configured on the AAA server.
- Inspur recommends that you configure the dead-time interval if more than six servers are configured in a group. If you must configure more than six servers, make sure to set the dead-time interval to a value greater than 0 and enable dead server monitoring by configuring the test username and test password.
- Command authorization on TACACS+ servers is available only for non-console sessions. If you use a console to login to the server, command authorization is disabled.
- For CN129-X6136YC-R, CN129-X636C-R, and CN129-X636Q-R line cards and the CN12908-FM-R fabric module, TACACS+ authentication fails for usernames with special characters.

5.5 Default Settings for TACACS+

This table lists the default settings for TACACS+ parameters.

Table 8: Default TACACS+ Parameters Settings

Parameters	Default
TACACS+	Disabled
Dead timer interval	0 minutes
Timeout interval	5

Parameters	Default
	seconds
Idle timer interval	0 minutes
Periodic server monitoring username	test
Periodic server monitoring password	test
Privilege level support for TACACS+ authorization	Disabled

5.6 Configuring TACACS+

This section describes how to configure TACACS+ on a Inspur INOS-CN device.

5.6.1 TACACS+ Server Configuration Process

-
- Step 1** Enable TACACS+.
 - Step 2** Establish the TACACS+ server connections to the Inspur INOS-CN device.
 - Step 3** Configure the secret keys for the TACACS+ servers.
 - Step 4** If needed, configure TACACS+ server groups with subsets of the TACACS+ servers for AAA authentication methods.
 - Step 5** (Optional) Configure the TCP port.
 - Step 6** (Optional) If needed, configure periodic TACACS+ server monitoring.
 - Step 7** (Optional) If TACACS+ distribution is enabled, commit the TACACS+ configuration to the fabric.
-

5.6.2 Enabling TACACS+

By default, the TACACS+ feature is disabled on the Inspur INOS-CN device. You must explicitly enable the TACACS+ feature to access the configuration and verification commands for authentication.

SUMMARY STEPS

1. **configure terminal**
2. **feature tacacs+**
3. **exit**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	feature tacacs+	Enables TACACS+.

	Command or Action	Purpose
	Example: switch(config)# feature tacacs+	
Step 3	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 4	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

5.6.3 Configuring TACACS+ Server Hosts

To access a remote TACACS+ server, you must configure the IP address or the hostname for the TACACS+ server on the Inspur INOS-CN device. You can configure up to 64 TACACS+ servers.

Before you begin

Enable TACACS+.

Obtain the IPv4 or IPv6 addresses or the hostnames for the remote TACACS+ servers.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *hostname*}
3. (Optional) **show tacacs+** {**pending** | **pending-diff**}
4. (Optional) **tacacs+ commit**
5. **exit**
6. (Optional) **show tacacs-server**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	tacacs-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> }	Specifies the IPv4 or IPv6 address or hostname for a TACACS+ server.
	Example: switch(config)# tacacs-server host 10.10.2.2	
Step 3	(Optional) show tacacs+ { pending pending-diff }	Displays the TACACS+ configuration pending for distribution.
	Example: switch(config)# show tacacs+ pending	

	Command or Action	Purpose
Step 4	(Optional) tacacs+ commit Example: switch(config)# tacacs+ commit	Applies the TACACS+ configuration changes in the temporary database to the running configuration.
Step 5	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 6	(Optional) show tacacs-server Example: switch# show tacacs-server	Displays the TACACS+ server configuration.
Step 7	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

5.6.4 Configuring Global TACACS+ Keys

You can configure secret TACACS+ keys at the global level for all servers used by the Inspur INOS-CN device. A secret key is a shared secret text string between the Inspur INOS-CN device and the TACACS+ server hosts.

Before you begin

Enable TACACS+.

Obtain the secret key values for the remote TACACS+ servers.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server key [0 | 6 | 7] key-value**
3. **exit**
4. (Optional) **show tacacs-server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	tacacs-server key [0 6 7] key-value Example:	Specifies a TACACS+ key for all TACACS+ server. You can specify that the <i>key-value</i> is in clear text format (0), is type-6 encrypted (6), or is type-7 encrypted (7).

	Command or Action	Purpose
	<p><code>switch(config)# tacacs-server key 0 QsEfThUkO</code></p> <p>Example:</p>	<p>The Inspur software encrypts a clear text key before saving it to the running configuration. The default format is clear text. The maximum length is 53 characters. By default, no secret key is configured.</p> <p>Note If you already configured a shared secret using the generate type7_encrypted_secret command, enter it in quotation marks, as shown in the second example.</p>
Step 3	<p><code>exit</code></p> <p>Example:</p> <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 4	<p>(Optional) <code>show tacacs-server</code></p> <p>Example:</p> <pre>switch# show tacacs-server</pre>	<p>Displays the TACACS+ server configuration.</p> <p>Note The secret keys are saved in encrypted form in the running configuration. Use the show running-config command to display the encrypted secret keys.</p>
Step 5	<p>(Optional) <code>copy running-config startup-config</code></p> <p>Example:</p> <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

5.6.5 Configuring a Key for a Specific TACACS+ Server

You can configure secret keys for a TACACS+ server. A secret key is a shared secret text string between the Inspur INOS-CN device and the TACACS+ server host.

Before you begin

Enable TACACS+.

Obtain the secret key values for the remote TACACS+ servers.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [0 | 6 | 7] *key-value*
3. **exit**
4. (Optional) **show tacacs-server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	tacacs-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>host-name</i> } key [0 6 7] <i>key-value</i> Example: <pre>switch(config)# tacacs-server host 10.10.1.1 key</pre> Example: <pre>switch(config)# tacacs-server host 10.10.1.1 key 7 "fewhg"</pre>	<p>Specifies a secret key for a specific TACACS+ server. You can specify that the <i>key-value</i> is in clear text format (0), is type-6 encrypted (6), or is type-7 encrypted (7). The Inspur software encrypts a clear text key before saving it to the running configuration. The default format is clear text. The maximum length is 63 characters. This secret key is used instead of the global secret key.</p> <p>Note If you already configured a shared secret using the generate type7_encrypted_secret command, enter it in quotation marks, as shown in the second example.</p>
Step 3	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 4	(Optional) show tacacs-server Example: <pre>switch# show tacacs-server</pre>	Displays the TACACS+ server configuration. Note The secret keys are saved in encrypted form in the running configuration. Use the show running-config command to display the encrypted secret keys.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

5.6.6 Configuring TACACS+ Server Groups

You can specify one or more remote AAA servers to authenticate users using server groups. All members of a group must belong to the TACACS+ protocol. The servers are tried in the same order in which you configure them.

You can configure these server groups at any time but they only take effect when you apply them to an AAA service.

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. **aaa group server tacacs+ group-name**
3. **server {ipv4-address | ipv6-address | hostname}**
4. **exit**
5. (Optional) **show tacacs-server groups**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	aaa group server tacacs+ group-name Example: switch(config)# aaa group server tacacs+ TacServer switch(config-tacacs+)#	Creates a TACACS+ server group and enters the TACACS+ server group configuration mode for that group.
Step 3	server {ipv4-address ipv6-address hostname} Example: switch(config-tacacs+)# server 10.10.2.2	Configures the TACACS+ server as a member of the TACACS+ server group. If the specified TACACS+ server is not found, configure it using the tacacs-server host command and retry this command.
Step 4	exit Example: switch(config-tacacs+)# exit switch(config)#	Exits TACACS+ server group configuration mode.
Step 5	(Optional) show tacacs-server groups Example: switch(config)# show tacacs-server groups	Displays the TACACS+ server group configuration.
Step 6	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

5.6.7 Configuring the Global Source Interface for TACACS+ Server Groups

You can configure a global source interface for TACACS+ server groups to use when accessing TACACS+

servers. You can also configure a different source interface for a specific TACACS+ server group. By default, the Inspur INOS-CN software uses any available interface.

SUMMARY STEPS

1. **configure terminal**
2. **ip tacacs source-interface** *interface*
3. **exit**
4. (Optional) **show tacacs-server**
5. (Optional) **copy running-config startup config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)	Enters global configuration mode.
Step 2	ip tacacs source-interface <i>interface</i> Example: switch(config)# ip tacacs source-interface mgmt 0	Configures the global source interface for all TACACS+ server groups configured on the device.
Step 3	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 4	(Optional) show tacacs-server Example: switch# show tacacs-server	Displays the TACACS+ server configuration information.
Step 5	(Optional) copy running-config startup config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

5.6.8 Allowing Users to Specify a TACACS+ Server at Login

You can configure the switch to allow the user to specify which TACACS+ server to send the authentication request by enabling the directed-request option. By default, a Inspur INOS-CN device forwards an authentication request based on the default AAA authentication method. If you enable this option, the user can log in as *username@vrfname:hostname*, where *vrfname* is the VRF to use and *hostname* is the name of a configured TACACS+ server.

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server directed-request**
3. (Optional) **show tacacs+ {pending | pending-diff}**
4. (Optional) **tacacs+ commit**
5. **exit**
6. (Optional) **show tacacs-server directed-request**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	tacacs-server directed-request Example: <pre>switch(config)# tacacs-server directed-request</pre>	Allows users to specify a TACACS+ server to send the authentication request when logging in. The default is disabled.
Step 3	(Optional) show tacacs+ {pending pending-diff} Example: <pre>switch(config)# show tacacs+ pending</pre>	Displays the pending TACACS+ configuration.
Step 4	(Optional) tacacs+ commit Example: <pre>switch(config)# tacacs+ commit</pre>	Applies the TACACS+ configuration changes in the temporary database to the running configuration.
Step 5	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 6	(Optional) show tacacs-server directed-request Example: <pre>switch# show tacacs-server directed-request</pre>	Displays the TACACS+ directed request configuration.
Step 7	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

5.6.9 Configuring the Timeout Interval for a TACACS+ Server

You can set a timeout interval that the Inspur INOS-CN device waits for responses from a TACACS+ server before declaring a timeout failure. The timeout interval determines how long the Inspur INOS-CN device waits for

responses from a TACACS+ server before declaring a timeout failure.

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **timeout** *seconds*
3. (Optional) **show tacacs+** {**pending** | **pending-diff**}
4. (Optional) **tacacs+ commit**
5. **exit**
6. (Optional) **show tacacs-server**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	tacacs-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } timeout <i>seconds</i> Example: switch(config)# tacacs-server host server1 timeout 10	Specifies the timeout interval for a specific server. The default is the global value. Note The timeout interval value specified for a TACACS+ server overrides the global timeout interval value specified for all TACACS+ servers.
Step 3	(Optional) show tacacs+ { pending pending-diff } Example: switch(config)# show tacacs+ pending	Displays the TACACS+ configuration pending for distribution.
Step 4	(Optional) tacacs+ commit Example: switch(config)# tacacs+ commit	Applies the TACACS+ configuration changes in the temporary database to the running configuration.
Step 5	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 6	(Optional) show tacacs-server Example: switch# show tacacs-server	Displays the TACACS+ server configuration.
Step 7	(Optional) copy running-config startup-config	Copies the running configuration to the startup

Example: switch# <code>copy running-config startup-config</code>	configuration.
--	----------------

5.6.10 Configuring TCP Ports

You can configure another TCP port for the TACACS+ servers if there are conflicts with another application. By default, Inspur INOS-CN devices use port 49 for all TACACS+ requests.

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **port** *tcp-port*
3. (Optional) **show tacacs+** {**pending** | **pending-diff**}
4. (Optional) **tacacs+ commit**
5. **exit**
6. (Optional) **show tacacs-server**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# <code>configure terminal</code> switch(config)#	Enters global configuration mode.
Step 2	tacacs-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } port <i>tcp-port</i> Example: switch(config)# <code>tacacs-server host 10.10.1.1 port 2</code>	Specifies the TCP port to use for TACACS+ messages to the server. The default TCP port is 49. The range is from 1 to 65535.
Step 3	(Optional) show tacacs+ { pending pending-diff } Example: switch(config)# <code>show tacacs+ distribution pending</code>	Displays the TACACS+ configuration pending for distribution.
Step 4	(Optional) tacacs+ commit Example: switch(config)# <code>tacacs+ commit</code>	Applies the TACACS+ configuration changes in the temporary database to the running configuration.
Step 5	exit Example: switch(config)# <code>exit</code>	Exits configuration mode.

	Command or Action	Purpose
	switch#	
Step 6	(Optional) show tacacs-server Example: switch# show tacacs-server	Displays the TACACS+ server configuration.
Step 7	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

5.6.11 Configuring Global Periodic TACACS+ Server Monitoring

You can monitor the availability of all TACACS+ servers without having to configure the test parameters for each server individually. Any servers for which test parameters are not configured are monitored using the global level parameters.

Before you begin
Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server test** {idle-time *minutes* | password *password* [idle-time *minutes*] | username *name* [password *password* [idle-time *minutes*]]}
3. **tacacs-server dead-time** *minutes*
4. **exit**
5. (Optional) **show tacacs-server**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	tacacs-server test {idle-time <i>minutes</i> password <i>password</i> [idle-time <i>minutes</i>] username <i>name</i> [password <i>password</i> [idle-time <i>minutes</i>]]} Example: switch(config)# tacacs-server test username user1 password Ur2Gd2BH idle-time 3	Specifies parameters for global server monitoring. The default username is test, and the default password is test. The default value for the idle timer is 0 minutes, and the valid range is from 0 to 1440 minutes. Note For periodic TACACS+ server monitoring, the idle timer value must be greater than 0.

	Command or Action	Purpose
Step 3	tacacs-server dead-time <i>minutes</i> Example: <pre>switch(config)# tacacs-server dead-time 5</pre>	Specifies the number of minutes before the Inspur INOS-CN device checks a TACACS+ server that was previously unresponsive. The default value is 0 minutes, and the valid range is from 0 to 1440 minutes.
Step 4	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 5	(Optional) show tacacs-server Example: <pre>switch# show tacacs-server</pre>	Displays the TACACS+ server configuration.
Step 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

5.6.12 Configuring Periodic TACACS+ Server Monitoring on Individual Servers

You can monitor the availability of individual TACACS+ servers. The configuration parameters include the username and password to use for the server and an idle timer. The idle timer specifies the interval in which a TACACS+ server receives no requests before the Inspur INOS-CN device sends out a test packet. You can configure this option to test servers periodically, or you can run a one-time only test.

Before you begin

Enable TACACS+.

Add one or more TACACS+ server hosts.

SUMMARY STEPS

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}
3. **tacacs-server dead-time** *minutes*
4. **exit**
5. (Optional) **show tacacs-server**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.

	Command or Action	Purpose
	Example: <pre>switch# configure terminal switch(config)#</pre>	
Step 2	tacacs-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } test { <i>idle-time minutes</i> password <i>password</i> [<i>idle-time minutes</i>] username <i>name</i> [password <i>password</i> [<i>idle-time minutes</i>]]} Example: <pre>switch(config)# tacacs-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3</pre>	Specifies parameters for individual server monitoring. The default username is test, and the default password is test. The default value for the idle timer is 0 minutes, and the valid range is from 0 to 1440 minutes. Note For periodic TACACS+ server monitoring, the idle timer value must be greater than 0.
Step 3	tacacs-server dead-time <i>minutes</i> Example: <pre>switch(config)# tacacs-server dead-time 5</pre>	Specifies the number of minutes before the Inspur INOS-CN device checks a TACACS+ server that was previously unresponsive. The default value is 0 minutes, and the valid range is from 0 to 1440 minutes.
Step 4	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 5	(Optional) show tacacs-server Example: <pre>switch# show tacacs-server</pre>	Displays the TACACS+ server configuration.
Step 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

5.6.13 Configuring the TACACS+ Dead-Time Interval

You can configure the dead-time interval for all TACACS+ servers. The dead-time interval specifies the time that the Inspur INOS-CN device waits, after declaring a TACACS+ server is dead, before sending out a test packet to determine if the server is now alive.

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**

2. **tacacs-server** *deadtime* *minutes*
3. (Optional) **show tacacs+** {*pending* | *pending-diff*}
4. (Optional) **tacacs+** **commit**
5. **exit**
6. (Optional) **show tacacs-server**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	tacacs-server <i>deadtime</i> <i>minutes</i> Example: switch(config)# tacacs-server <i>deadtime</i> 5	Configures the global dead-time interval. The default value is 0 minutes. The range is from 1 to 1440 minutes.
Step 3	(Optional) show tacacs+ { <i>pending</i> <i>pending-diff</i> } Example: switch(config)# show tacacs+ <i>pending</i>	Displays the pending TACACS+ configuration.
Step 4	(Optional) tacacs+ commit Example: switch(config)# tacacs+ commit	Applies the TACACS+ configuration changes in the temporary database to the running configuration.
Step 5	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 6	(Optional) show tacacs-server Example: switch# show tacacs-server	Displays the TACACS+ server configuration.
Step 7	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

5.6.14 Configuring ASCII Authentication

You can enable ASCII authentication on the TACACS+ server.

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication login ascii-authentication**
3. (Optional) **show tacacs+ {pending | pending-diff}**
4. (Optional) **tacacs+ commit**
5. **exit**
6. (Optional) **show tacacs-server**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	aaa authentication login ascii-authentication Example: switch(config)# aaa authentication login ascii-authentication	Enables ASCII authentication. The default is disabled.
Step 3	(Optional) show tacacs+ {pending pending-diff} Example: switch(config)# show tacacs+ pending	Displays the pending TACACS+ configuration.
Step 4	(Optional) tacacs+ commit Example: switch(config)# tacacs+ commit	Applies the TACACS+ configuration changes in the temporary database to the running configuration.
Step 5	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 6	(Optional) show tacacs-server Example: switch# show tacacs-server	Displays the TACACS+ server configuration.
Step 7	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

5.6.15 Configuring AAA Authorization on TACACS+ Servers

You can configure the default AAA authorization method for TACACS+ servers.

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authorization ssh-certificate default {group *group-list* [none] | local | none}**
3. **exit**
4. (Optional) **show aaa authorization [all]**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	aaa authorization ssh-certificate default {group <i>group-list</i> [none] local none} Example: <pre>switch(config)# aaa authorization ssh-certificate default group TACACSServer1 TACACSServer2</pre>	Configures the default AAA authorization method for the TACACS+ servers. The ssh-certificate keyword configures TACACS+ or local authorization with certificate authentication. The default authorization is local authorization, which is the list of authorized commands for the user's assigned role. The <i>group-list</i> argument consists of a space-delimited list of TACACS+ server group names. Servers belonging to this group are contacted for AAA authorization. The local method uses the local database for authorization, and the none method specifies that no AAA authorization be used.
Step 3	exit Example: <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 4	(Optional) show aaa authorization [all] Example: <pre>switch# show aaa authorization</pre>	Displays the AAA authorization configuration. The all keyword displays the default values.
Step 5	(Optional) copy running-config startup-config	Copies the running configuration to the startup

	Command or Action	Purpose
	Example: <pre>switch# copy running-config startup-config</pre>	configuration.

5.6.16 Configuring Command Authorization on TACACS+ Servers

You can configure authorization for commands on TACACS+ servers.

Caution	Command authorization disables user role-based authorization control (RBAC), including the default roles.
----------------	---

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **configure terminal**
2. **aaa authorization** {**commands** | **config-commands**} {**console** | **default**} {**group** *group-list* [**local**] | **local**}
3. (Optional) **show tacacs+** {**pending** | **pending-diff**}
4. (Optional) **tacacs+ commit**
5. **exit**
6. (Optional) **show aaa authorization** [**all**]
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	aaa authorization { commands config-commands } { console default } { group <i>group-list</i> [local] local } Example: <pre>switch(config)# aaa authorization commands default group TacGroup Per command authorization will disable RBAC for all users. Proceed (y/n)?</pre>	Configures the command authorization method for specific roles on a TACACS+ server. The commands keyword configures authorization sources for all EXEC commands, and the config-commands keyword configures authorization sources for all configuration commands. The console keyword configures command authorization for a console session, and the default keyword configures command authorization for a non-console session.

	Command or Action	Purpose
		<p>The <i>group-list</i> argument consists of a space-delimited list of TACACS+ server group names. Servers belonging to this group are contacted for command authorization. The local method uses the local role-based database for authorization. The local method is used only if all the configured server groups fail to respond and you have configured local as the fallback method. The default method is local. If you have not configured a fallback method after the TACACS+ server group method, authorization fails if all server groups fail to respond. If you press Enter at the confirmation prompt, the default action is n.</p>
Step 3	(Optional) show tacacs+ {pending pending-diff} Example: <pre>switch(config)# show tacacs+ pending</pre>	Displays the pending TACACS+ configuration.
Step 4	(Optional) tacacs+ commit Example: <pre>switch(config)# tacacs+ commit</pre>	Applies the TACACS+ configuration changes in the temporary database to the running configuration.
Step 5	exit Example: <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 6	(Optional) show aaa authorization [all] Example: <pre>switch(config)# show aaa authorization</pre>	Displays the AAA authorization configuration. The all keyword displays the default values.
Step 7	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

5.6.17 Testing Command Authorization on TACACS+ Servers

You can test the command authorization for a user on the TACACS+ servers.

Before you begin

Enable TACACS+.

Ensure that you have configured command authorization for the TACACS+ servers.

SUMMARY STEPS

1. **test aaa authorization command-type** {commands | config-commands} **user** *username* **command** *command-string*

DETAILED STEPS

	Command or Action	Purpose
Step 1	test aaa authorization command-type {commands config-commands} user <i>username</i> command <i>command-string</i> Example: <pre>switch# test aaa authorization command-type commands user TestUser command reload</pre>	Tests a user's authorization for a command on the TACACS+ servers. The commands keyword specifies only EXEC commands and the config-commands keyword specifies only configuration commands. Note Put double quotes (") before and after the <i>command-string</i> argument if it contains spaces.

5.6.18 Enabling and Disabling Command Authorization Verification

You can enable and disable command authorization verification on the command-line interface (CLI) for the default user session or for another username.

SUMMARY STEPS

1. **terminal verify-only** [**username** *username*]
2. **terminal no verify-only** [**username** *username*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	terminal verify-only [username <i>username</i>] Example: <pre>switch# terminal verify-only</pre>	Enables command authorization verification. After you enter this command, the Inspur INOS-CN software indicates whether the commands you enter are authorized or not.
Step 2	terminal no verify-only [username <i>username</i>] Example: <pre>switch# terminal no verify-only</pre>	Disables command authorization verification.

5.6.19 Configuring Privilege Level Support for Authorization on TACACS+ Servers

You can configure privilege level support for authorization on TACACS+ servers.

Unlike the IOS devices, which use privilege levels to determine authorization, Inspur INOS-CN devices use role-based access control (RBAC). To enable both types of devices to be administered by the same TACACS+ servers, you can map the privilege levels configured on TACACS+ servers to user roles configured on Inspur INOS-CN devices.

When a user authenticates with a TACACS+ server, the privilege level is obtained and used to form a local user role name of the format “priv-*n*,” where *n* is the privilege level. The user assumes the permissions of this local role. Sixteen privilege levels, which map directly to corresponding user roles, are available. The following table shows the user role permissions that correspond to each privilege level.

Privilege Level	User Role Permissions
15	network-admin permissions
13 - 1	<ul style="list-style-type: none"> • Standalone role permissions, if the feature privilege command is disabled. • Same permissions as privilege level 0 with cumulative privileges for roles, if the feature privilege command is enabled.
0	Permission to execute show commands and exec commands (such as ping , trace , and ssh).

SUMMARY STEPS

1. **configure terminal**
2. **[no] feature privilege**
3. **[no] enable secret [0 | 5] password [priv-lvl priv-lvl | all]**
4. **[no] username username priv-lvl n**
5. (Optional) **show privilege**
6. (Optional) **copy running-config startup-config**
7. **exit**
8. **enable level**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	[no] feature privilege Example: <pre>switch(config)# feature privilege</pre>	Enables or disables the cumulative privilege of roles. Users can see the enable command only if this feature is enabled. The default is disabled.

	Command or Action	Purpose
Step 3	<p>[no] enable secret [0 5] password [priv-lvl priv-lvl all] Example:</p> <pre>switch(config)# enable secret 5 def456 priv-lvl 15</pre>	<p>Enables or disables a secret password for a specific privilege level. Users are prompted to enter the correct password upon each privilege level escalation. The default is disabled.</p> <p>You can enter 0 to specify that the password is in clear text or 5 to specify that the password is in encrypted format.</p> <p>The <i>password</i> argument can be up to 64 alphanumeric characters. The <i>priv-lvl</i> argument is from 1 to 15.</p> <p>Note To enable the secret password, you must have enabled the cumulative privilege of roles by entering the feature privilege command.</p>
Step 4	<p>[no] username username priv-lvl n Example:</p> <pre>switch(config)# username user2 priv-lvl 15</pre>	<p>Enables or disables a user to use privilege levels for authorization. The default is disabled.</p> <p>The priv-lvl keyword specifies the privilege level to which the user is assigned. There is no default privilege level.</p> <p>Privilege levels 0 to 15 (priv-lvl 0 to priv-lvl 15) map to user roles priv-0 to priv-15.</p>
Step 5	<p>(Optional) show privilege Example:</p> <pre>switch(config)# show privilege</pre>	<p>Displays the username, current privilege level, and status of cumulative privilege support.</p>
Step 6	<p>(Optional) copy running-config startup-config Example:</p> <pre>switch(config)# copy running-config startup-config</pre>	<p>Copies the running configuration to the startup configuration.</p>
Step 7	<p>exit Example:</p> <pre>switch(config)# exit switch#</pre>	<p>Exits global configuration mode.</p>
Step 8	<p>enable level Example:</p> <pre>switch# enable 15</pre>	<p>Enables a user to move to a higher privilege level. This command prompts for the secret password. The <i>level</i> argument specifies the privilege level to which the</p>

	Command or Action	Purpose
		user is granted access. The only available level is 15.

5.6.20 Permitting or Denying Commands for Users of Privilege Roles

As a network administrator, you can modify the privilege roles to permit users to execute specific commands or to prevent users from running those commands.

You must follow these guidelines when changing the rules of privilege roles:

- You cannot modify the priv-14 and priv-15 roles.
- You can add deny rules only to the priv-0 role.
- These commands are always permitted for the priv-0 role: **configure**, **copy**, **dir**, **enable**, **ping**, **show**, **ssh**, **telnet**, **terminal**, **traceroute**, **end**, and **exit**.

SUMMARY STEPS

1. **configure terminal**
2. **[no] role name priv-*n***
3. **rule number {deny | permit} command *command-string***
4. **exit**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	[no] role name priv-<i>n</i> Example: switch(config)# role name priv-5 switch(config-role)#	Enables or disables a privilege role and enters role configuration mode. The <i>n</i> argument specifies the privilege level and is a number between 0 and 13.
Step 3	rule number {deny permit} command <i>command-string</i> Example: switch(config-role)# rule 2 permit command pwd	Configures a command rule for users of privilege roles. These rules permit or deny users to execute specific commands. You can configure up to 256 rules for each role. The rule number determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1. The <i>command-string</i> argument can contain spaces.

	Command or Action	Purpose
		Note Repeat this command for as many rules as needed.
Step 4	exit Example: <pre>switch(config-role)# exit switch(config)#</pre>	Exits role configuration mode.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

5.6.21 Manually Monitoring TACACS+ Servers or Groups

You can manually issue a test message to a TACACS+ server or to a server group.

Before you begin

Enable TACACS+.

SUMMARY STEPS

1. **test aaa server tacacs+** {*ipv4-address* | *ipv6-address* | *hostname*} [**vrf** *vrf-name*] *username password*
2. **test aaa group** *group-name username password*

DETAILED STEPS

	Command or Action	Purpose
Step 1	test aaa server tacacs+ { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } [vrf <i>vrf-name</i>] <i>username password</i> Example: <pre>switch# test aaa server tacacs+ 10.10.1.1 user1 Ur2Gd2BH</pre>	Sends a test message to a TACACS+ server to confirm availability.
Step 2	test aaa group <i>group-name username password</i> Example: <pre>switch# test aaa group TacGroup user2 As3He3CI</pre>	Sends a test message to a TACACS+ server group to confirm availability.

5.6.22 Disabling TACACS+

You can disable TACACS+.

Caution	When you disable TACACS+, all related configurations are automatically discarded.
----------------	---

SUMMARY STEPS

1. **configure terminal**
2. **no feature tacacs+**
3. **exit**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	no feature tacacs+ Example: <pre>switch(config)# no feature tacacs+</pre>	Disables TACACS+.
Step 3	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 4	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

5.7 Monitoring TACACS+ Servers

You can monitor the statistics that the Inspur INOS-CN device maintains for TACACS+ server activity.

Before you begin

Configure TACACS+ servers on the Inspur INOS-CN device.

SUMMARY STEPS

1. **show tacacs-server statistics** *{hostname | ipv4-address | ipv6-address}*

DETAILED STEPS

	Command or Action	Purpose
Step 1	show tacacs-server statistics <i>{hostname ipv4-address ipv6-address}</i> Example: <pre>switch# show tacacs-server statistics 10.10.1.1</pre>	Displays the TACACS+ statistics.

5.8 Clearing TACACS+ Server Statistics

You can display the statistics that the Inspur INOS-CN device maintains for TACACS+ server activity.

Before you begin

Configure TACACS+ servers on the Inspur INOS-CN device.

SUMMARY STEPS

1. (Optional) **show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}
2. **clear tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) show tacacs-server statistics { <i>hostname</i> <i>ipv4-address</i> <i>ipv6-address</i> } Example: switch# show tacacs-server statistics 10.10.1.1	Displays the TACACS+ server statistics on the Inspur INOS-CN device.
Step 2	clear tacacs-server statistics { <i>hostname</i> <i>ipv4-address</i> <i>ipv6-address</i> } Example: switch# clear tacacs-server statistics 10.10.1.1	Clears the TACACS+ server statistics.

5.9 Verifying the TACACS+ Configuration

To display the TACACS+ configuration, perform one of the following tasks:

Command	Purpose
show tacacs+ { <i>status</i> <i>pending</i> <i>pending-diff</i> }	Displays the TACACS+ Inspur Fabric Services distribution status and other details.
show running-config tacacs [<i>all</i>]	Displays the TACACS+ configuration in the running configuration.
show startup-config tacacs	Displays the TACACS+ configuration in the startup configuration.
show tacacs-server [<i>host-name</i> <i>ipv4-address</i> <i>ipv6-address</i>] [<i>directed-request</i> <i>groups</i> <i>sorted</i> <i>statistics</i>]	Displays all configured TACACS+ server parameters.
show privilege	Displays the current privilege level, username, and status of cumulative privilege support.

5.10 Configuration Examples for TACACS+

The following example shows how to configure a TACACS+ server host and server group:

```

feature tacacs+
tacacs-server key 7 "ToIkLhPpG"
tacacs-server host 10.10.2.2 key 7 "ShMoMhTl"
bagroup    server    tacacs+
    TacServer server 10.10.2.2

```

The following example shows how to configure and use command authorization verification:

```

switch# terminal verify-only
switch# show interface ethernet 7/2 brief
%Success
switch# terminal no verify-only
switch# show interface ethernet 7/2 brief
-----
Ethernet VLAN Type Mode      Status   Reason   Speed   Port
Interface   Ch #
-----
Eth7/2     1    eth  access down  SFP not inserted  auto(D)  --

```

The following example shows how to enable the cumulative privilege of roles, configure a secret password for privilege level 2, and configure user3 for privilege level 2 authorization:

```

switch# configure terminal
switch(config)# feature privilege
switch(config)# enable secret def456 priv-lvl 2
switch(config)# username user3 priv-lvl 2
switch(config)# show privilege
User name: user3
Current privilege level: -2
Feature privilege: Enabled
switch(config)# copy running-config startup-config
switch(config)# exit

```

The following example shows how to change user3 from the priv-2 role to the priv-15 role. After entering the **enable 15** command, the user is prompted to enter the password that was configured by the administrator using the **enable secret** command. Privilege level 15 gives this user network-admin privileges under the enable mode.

```

User Access Verification
login: user3
Password: *****
Inspur Inspur Operating System (nos-cn)

Software TAC support: http://www.Inspur.com/tac
Copyright (©) 2018, Inspur-Cisco Networking Technology Co. Ltd.
All rights reserved. The copyrights to certain works contained in
this software are owned by other third parties and used and
distributed under license. Certain components of this software are
licensed under the GNU General Public License (GPL) version 2.0 or
the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of
each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch#
switch# enable 15

```

```

Password: def456
Inspur INOS- Operating System (nos-cn) Software
TAC support: http://www.Inspur.com/tac
Copyright (©) 2018, Inspur-Cisco Networking Technology Co. Ltd.
All rights reserved. The copyrights to certain works contained
in this software are owned by other third parties and used and
distributed under

```

```

license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of
each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch-enable#

```

The following example shows how to permit all users with roles priv-5 and above to execute the **pwd** command:

```

switch# configure terminal
switch(config)# role name priv-5
switch(config-role)# rule 1 permit command pwd

```

The following example shows how to deny the **show running-config** command to all users with roles below priv-5. First, you must remove the permission to execute this command from the priv-0 role; then you must permit the command at role priv-5 so that users with roles priv-5 and above have permission to run the command.

```

switch# configure terminal
switch(config)# role name priv-0
switch(config-role)# rule 2 deny command show running-
config switch(config-role)# exit
switch(config)# role name priv-5
switch(config-role)# rule 3 permit command show running-
config switch(config-role)# exit

```

5.11 Where to Go Next

You can now configure AAA authentication methods to include the server groups.

5.12 Additional References for TACACS+

This section includes additional information related to implementing TACACS+.

Related Documents

Related Topic	Document Title
VRF configuration	

Standards

Standards	Title
-----------	-------

No new or modified standards are supported by this feature, and support for existing standards has not — been modified by this feature.	
---	--

CHAPTER 6 Configuring SSH and Telnet

This chapter describes how to configure Secure Shell Protocol (SSH) and Telnet on Inspur INOS-CN devices. This chapter includes the following sections:

6.1 About SSH and Telnet

This section includes information about SSH and Telnet.

6.1.1 SSH Server

You can use the SSH server to enable an SSH client to make a secure, encrypted connection to a Inspur INOS-CN device. SSH uses strong encryption for authentication. The SSH server in the Inspur INOS-CN software can interoperate with publicly and commercially available SSH clients.

The user authentication mechanisms supported for SSH are RADIUS, TACACS+, LDAP, and the use of locally stored usernames and passwords.

6.1.2 SSH Client

The SSH client feature is an application that runs over the SSH protocol to provide device authentication and encryption. The SSH client enables a Inspur INOS-CN device to make a secure, encrypted connection to another Inspur INOS-CN device or to any other device that runs the SSH server. This connection provides an outbound connection that is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

The SSH client in the Inspur INOS-CN software works with publicly and commercially available SSH servers.

6.1.3 SSH Server Keys

SSH requires server keys for secure communications to the Inspur INOS-CN device. You can use SSH server keys for the following SSH options:

- SSH version 2 using Rivest, Shamir, and Adelman (RSA) public-key cryptography
- SSH version 2 using the Digital System Algorithm (DSA)
- SSH version 2 using the Elliptic Curve Digital Signature Algorithm (ECDSA)

Be sure to have an SSH server key-pair with the appropriate version before enabling the SSH service. You can generate the SSH server key-pair according to the SSH client version used. The SSH service accepts two types of key-pairs for use by SSH version 2:

- The **dsa** option generates the DSA key-pair for the SSH version 2 protocol.
- The **rsa** option generates the RSA key-pair for the SSH version 2 protocol.
- The **ecdsa** option generates the ECDSA key-pair for the SSH version 2 protocol.

By default, the Inspur INOS-CN software generates an RSA key using 1024 bits.

SSH supports the following public key formats:

- OpenSSH
- IETF Secure Shell (SECSH)
- Public Key Certificate in Privacy-Enhanced Mail (PEM)

Caution | If you delete all of the SSH keys, you cannot start the SSH services.

6.1.4 SSH Authentication Using Digital Certificates

SSH authentication on Inspur INOS-CN devices provide X.509 digital certificate support for host authentication. An X.509 digital certificate is a data item that ensures the origin and integrity of a message. It contains encryption keys for secured communications and is signed by a trusted certification authority (CA) to verify the identity of the presenter. The X.509 digital certificate support provides either DSA or RSA algorithms for authentication.

The certificate infrastructure uses the first certificate that supports the Secure Socket Layer (SSL) and is returned by the security infrastructure, either through a query or a notification. Verification of certificates is successful if the certificates are from any of the trusted CAs configured and if not revoked or expired.

You can configure your device for SSH authentication using an X.509 certificate. If the authentication fails, you are prompted for a password.

You can configure SSH authentication using X.509v3 certificates (RFC 6187). X.509v3 certificate-based SSH authentication uses certificates combined with a smartcard to enable two-factor authentication for Inspur INOS-CN device access. The SSH client is provided by Inspur partner Pragma Systems.

6.1.5 Telnet Server

The Telnet protocol enables TCP/IP connections to a host. Telnet allows a user at one site to establish a TCP connection to a login server at another site and then passes the keystrokes from one device to the other. Telnet can accept either an IP address or a domain name as the remote device address.

The Telnet server is disabled by default on the Inspur INOS-CN device.

6.2 Licensing Requirements for SSH and Telnet

The following table shows the licensing requirements for this feature:

Product	License Requirement
Inspur	SSH and Telnet require no license. Any feature not included in a license package is bundled Inspur image and is provided at no extra charge to you.

6.3 Prerequisites for SSH and Telnet

Make sure that you have configured IP on a Layer 3 interface, out-of-band on the mgmt 0 interface, or inband on an Ethernet interface.

6.4 Guidelines and Limitations for SSH and Telnet

SSH and Telnet have the following configuration guidelines and limitations:

- The Inspur INOS-CN software supports only SSH version 2 (SSHv2).
- You can configure your device for SSH authentication using an X.509 certificate. If the authentication fails, you are prompted for a password.
- The SFTP server feature does not support the regular SFTP **chown** and **chgrp** commands.
- When the SFTP server is enabled, only the admin user can use SFTP to access the device.

6.5 Default Settings for SSH and Telnet

This table lists the default settings for SSH and Telnet parameters.

Table 9: Default SSH and Telnet Parameters

Parameters	Default
SSH server	Enabled
SSH server key	RSA key generated with 1024 bits
RSA key bits for generation	1024
Telnet server	Disabled
Telnet port number	23
Maximum number of SSH login attempts	3
SCP server	Disabled
SFTP server	Disabled

6.6 Configuring SSH

This section describes how to configure SSH.

6.6.1 Generating SSH Server Keys

You can generate an SSH server key based on your security requirements. The default SSH server key is an RSA key that is generated using 1024 bits.

SUMMARY STEPS

1. **configure terminal**
2. **no feature ssh**
3. **ssh key {dsa [force] | rsa [bits[force]] | ecdsa [bits [force]]}**
4. **ssh rekey max-data max-data max-time max-time**
5. **feature ssh**
6. **exit**
7. (Optional) **show ssh key [dsa | rsa | ecdsa] [md5]**
8. **show run security all**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	no feature ssh Example:	Disables SSH.

	Command or Action	Purpose
	<code>switch(config)# no feature ssh</code>	
Step 3	<p><code>ssh key {dsa [force] rsa [bits[force]] ecdsa [bits [force]]}</code></p> <p>Example:</p> <pre>switch(config)# ssh key rsa 2048</pre>	<p>Generates the SSH server key.</p> <p>The <i>bits</i> argument is the number of bits used to generate the RSA key. The range is from 768 to 2048. The default value is 1024.</p> <p>You cannot specify the size of the DSA key. It is always set to 1024 bits.</p> <p>Use the force keyword to replace an existing key.</p> <p>Note If you configure <code>ssh key dsa</code>, you must do the following additional configurations: <code>ssh keytypes all</code> and <code>ssh kexalgs all</code></p>
Step 4	<p><code>ssh rekey max-data max-data max-time max-time</code></p> <p>Example:</p> <pre>switch(config)# ssh rekey max-data 1K max-time 1M</pre>	Configures the rekey parameters.
Step 5	<p><code>feature ssh</code></p> <p>Example:</p> <pre>switch(config)# feature ssh</pre>	Enables SSH.
Step 6	<p><code>exit</code></p> <p>Example:</p> <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 7	<p>(Optional) <code>show ssh key [dsa rsa ecdsa] [md5]</code></p> <p>Example:</p> <pre>switch# show ssh key</pre>	<p>Displays the SSH server keys.</p> <p>This command displays the fingerprint in SHA256 format by default. SHA256 is more secure than the old default format of MD5. However, the md5 option has been added, if you want to see the fingerprint in MD5 format for backward compatibility.</p>
Step 8	<code>show run security all</code>	
Step 9	<p>(Optional) <code>copy running-config startup-config</code></p> <p>Example:</p> <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

6.6.2 Specifying the SSH Public Keys for User Accounts

You can configure an SSH public key to log in using an SSH client without being prompted for a password. You can specify the SSH public key in one of these formats:

- OpenSSH format
- IETF SECSH format

Specifying the SSH Public Keys in IETF SECSH Format

You can specify the SSH public keys in IETF SECSH format for user accounts.

Before you begin

Generate an SSH public key in IETF SECSH format.

SUMMARY STEPS

1. **copy** *server-file* **bootflash:filename**
2. **configure terminal**
3. **username** *username* **sshkey file bootflash:filename**
4. **exit**
5. (Optional) **show user-account**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	copy <i>server-file</i> bootflash:filename Example: <pre>switch# copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub</pre>	Downloads the file containing the SSH key in IETF SECSH format from a server. The server can be FTP, secure copy (SCP), secure FTP (SFTP), or TFTP.
Step 2	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 3	username <i>username</i> sshkey file bootflash:filename Example: <pre>switch(config)# username User1 sshkey file bootflash:secsh_file.pub</pre>	Configures the SSH public key in IETF SECSH format.
Step 4	exit Example: <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 5	(Optional) show user-account Example:	Displays the user account configuration.

	Command or Action	Purpose
	switch# show user-account	
Step 6	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Specifying the SSH Public Keys in OpenSSH Format

You can specify the SSH public keys in OpenSSH format for user accounts.

Before you begin

Generate an SSH public key in OpenSSH format.

SUMMARY STEPS

1. **configure terminal**
2. **username** *username* **sshkey** *ssh-key*
3. **exit**
4. (Optional) **show user-account**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	username <i>username</i> sshkey <i>ssh-key</i> Example: switch(config)# username User1 sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZ19G+3f1XswK30iW4H7YyUyuA50rv7gsEPj h0BYmsi6PAVKu1nIf/DQhum+1JNqJP/eLowb7ubO+1VKRXYF/G+1JNlQW3g9igG30c6k6+ XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH3UD/vKyziEh5S4Tplx8=	Configures the SSH public key in OpenSSH format.
Step 3	exit Example: switch(config)# exit switch#	Exits global configuration mode.
Step 4	(Optional) show user-account Example: switch# show user-account	Displays the user account configuration.

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

6.6.3 Configuring a Maximum Number of SSH Login Attempts

You can configure the maximum number of SSH login attempts. If the user exceeds the maximum number of permitted attempts, the session disconnects.

SUMMARY STEPS

1. **configure terminal**
2. **ssh login-attempts** *number*
3. (Optional) **show running-config security all**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	ssh login-attempts <i>number</i> Example: switch(config)# ssh login-attempts 5	Configures the maximum number of times that a user can attempt to log into an SSH session. The default maximum number of login attempts is 3. The range is from 1 to 10. Note The no form of this command removes the previous login attempts value and sets the maximum number of login attempts to the default value of 3.
Step 3	(Optional) show running-config security all Example: switch(config)# show running-config security all	Displays the configured maximum number of SSH login attempts.
Step 4	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

6.6.4 Starting SSH Sessions

You can start SSH sessions using IPv4 or IPv6 to connect to remote devices from the Inspur INOS-CN device.

Before you begin

Obtain the hostname for the remote device and, if needed, the username on the remote device.

Enable the SSH server on the remote device.

SUMMARY STEPS

1. **ssh** [*username@*]{*ipv4-address* | *hostname*} [**vrf** *vrf-name*]
2. **ssh6** [*username@*]{*ipv6-address* | *hostname*} [**vrf** *vrf-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	ssh [<i>username@</i>]{ <i>ipv4-address</i> <i>hostname</i> } [vrf <i>vrf-name</i>] Example: switch# ssh 10.10.1.1	Creates an SSH IPv4 session to a remote device using IPv4. The default VRF is the default VRF.
Step 2	ssh6 [<i>username@</i>]{ <i>ipv6-address</i> <i>hostname</i> } [vrf <i>vrf-name</i>] Example: switch# ssh6 HostA	Creates an SSH IPv6 session to a remote device using IPv6.

6.6.5 Starting SSH Sessions from Boot Mode

You can start SSH sessions from the boot mode of the Inspur INOS-CN device to connect to remote devices.

Before you begin

Obtain the hostname for the remote device and, if needed, the username on the remote device.

Enable the SSH server on the remote device.

SUMMARY STEPS

1. **ssh** [*username@*]*hostname*
2. **exit**
3. **copy scp://**[*username@*]*hostname*/*filepath directory*

DETAILED STEPS

	Command or Action	Purpose
Step 1	ssh [<i>username@</i>] <i>hostname</i> Example: switch(boot)# ssh user1@10.10.1.1	Creates an SSH session to a remote device from the boot mode of the Inspur INOS-CN device. The default VRF is always used.
Step 2	exit	Exits boot mode.

	Command or Action	Purpose
	Example: <pre>switch(boot)# exit</pre>	
Step 3	copy scp://[username@]hostname/filepath directory Example: <pre>switch# copy scp://user1@10.10.1.1/users abc</pre>	Copies a file from the Inspur INOS-CN device to a remote device using the Secure Copy Protocol (SCP). The default VRF is always used.

6.6.6 Configuring SSH Passwordless File Copy

You can copy files from a Inspur INOS-CN device to a secure copy (SCP) or secure FTP (SFTP) server without a password. To do so, you must create an RSA or DSA identity that consists of public and private keys for authentication with SSH.

SUMMARY STEPS

1. **configure terminal**
2. **[no] username *username* keypair generate {rsa [*bits* [**force**]] | dsa [**force**]}**
3. (Optional) **show username *username* keypair**
4. **username *username* keypair export {bootflash:*filename* | volatile:*filename*} {rsa | dsa} [**force**]**
5. **username *username* keypair import {bootflash:*filename* | volatile:*filename*} {rsa | dsa} [**force**]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	[no] username <i>username</i> keypair generate {rsa [<i>bits</i> [force]] dsa [force]} Example: <pre>switch(config)# username user1 keypair generate rsa 2048 force</pre>	Generates the SSH public and private keys and stores them in the home directory (\$HOME/.ssh) of the Inspur INOS-CN device for the specified user. The Inspur INOS-CN device uses the keys to communicate with the SSH server on the remote machine. The <i>bits</i> argument is the number of bits used to generate the key. The range is from 768 to 2048. The default value is 1024. Use the force keyword to replace an existing key. The SSH keys are not generated if the force keyword is omitted and

	Command or Action	Purpose
		SSH keys are already present.
Step 3	<p>(Optional) show username <i>username</i> keypair</p> <p>Example:</p> <pre>switch(config)# show username user1 keypair</pre>	<p>Displays the public key for the specified user.</p> <p>Note For security reasons, this command does not show the private key.</p>
Step 4	<p>Required: username <i>username</i> keypair export</p> <p>{bootflash:<i>filename</i> volatile:<i>filename</i>} {rsa dsa} [force]</p> <p>Example:</p> <pre>switch(config)# username user1 keypair export bootflash:key_rsa rsa</pre>	<p>Exports the public and private keys from the home directory of the Inspur INOS-CN device to the specified bootflash or volatile directory.</p> <p>Use the force keyword to replace an existing key. The SSH keys are not exported if the force keyword is omitted and SSH keys are already present.</p> <p>To export the generated key pair, you are prompted to enter a passphrase that encrypts the private key. The private key is exported as the file that you specify, and the public key is exported with the same filename followed by a .pub extension. You can now copy this key pair to any Inspur INOS-CN device and use SCP or SFTP to copy the public key file (*.pub) to the home directory of the server.</p> <p>Note For security reasons, this command can be executed only from global configuration mode.</p>
Step 5	<p>Required: username <i>username</i> keypair import</p> <p>{bootflash:<i>filename</i> volatile:<i>filename</i>} {rsa dsa} [force]</p> <p>Example:</p> <pre>switch(config)# username user1 keypair import bootflash:key_rsa rsa</pre>	<p>Imports the exported public and private keys from the specified bootflash or volatile directory to the home directory of the Inspur INOS-CN device.</p> <p>Use the force keyword to replace an existing key. The SSH keys are not imported if the force keyword is omitted and SSH keys are already present.</p> <p>To import the generated key pair, you are prompted to enter a passphrase that decrypts the private key. The private key is imported as the file that you specify, and the</p>

	Command or Action	Purpose
		<p>public key is imported with the same filename followed by a .pub extension.</p> <p>Note For security reasons, this command can be executed only from global configuration mode.</p> <p>Note Only the users whose keys are configured on the server are able to access the server without a password.</p>

What to do next

On the SCP or SFTP server, use the following command to append the public key stored in the *.pub file (for example, key_rsa.pub) to the authorized_keys file:

```
$ cat key_rsa.pub >> $HOME/.ssh/authorized_keys
```

You can now copy files from the Inspur INOS-CN device to the server without a password using standard SSH and SCP commands.

6.6.7 Configuring SCP and SFTP Servers

You can configure an SCP or SFTP server on the Inspur INOS-CN device in order to copy files to and from a remote device. After you enable the SCP or SFTP server, you can execute an SCP or SFTP command on the remote device to copy the files to or from the Inspur INOS-CN device.

SUMMARY STEPS

1. **configure terminal**
2. **[no] feature scp-server**
3. **[no] feature sftp-server**
4. **exit**
5. (Optional) **show running-config security**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	<p>[no] feature scp-server</p> <p>Example:</p> <pre>switch(config)# feature scp-server</pre>	Enables or disables the SCP server on the Inspur INOS-CN device.
Step 3	Required: [no] feature sftp-server	Enables or disables the SFTP server on the Inspur

	Command or Action	Purpose
	Example: <pre>switch(config)# feature sftp-server</pre>	INOS-CN device.
Step 4	Required: exit Example: <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 5	(Optional) show running-config security Example: <pre>switch# show running-config security</pre>	Displays the configuration status of the SCP and SFTP servers.
Step 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

6.6.8 Configuring X.509v3 Certificate-Based SSH Authentication

You can configure SSH authentication using X.509v3 certificates.

Before you begin

Enable the SSH server on the remote device.

SUMMARY STEPS

1. **configure terminal**
2. **username** *user-id* [**password** [0 | 5] *password*]
3. **username** *user-id* **ssh-cert-dn** *dn-name* {**dsa** | **rsa**}
4. [**no**] **crypto ca trustpoint** *trustpoint*
5. **crypto ca authenticate** *trustpoint*
6. (Optional) **crypto ca crl request** *trustpoint* **bootflash:static-crl.crl**
7. (Optional) **show crypto ca certificates**
8. (Optional) **show crypto ca crl** *trustpoint*
9. (Optional) **show user-account**
10. (Optional) **show users**
11. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	username <i>user-id</i> [password [0 5] <i>password</i>]	Configures a user account. The <i>user-id</i> argument is

	Command or Action	Purpose
	<p>Example:</p> <pre>switch(config)# username jsmith password 4Ty18Rnt</pre>	<p>a case-sensitive, alphanumeric character string with a maximum length of 28 characters. Valid characters are uppercase letters A through Z, lowercase letters a through z, numbers 0 through 9, hyphen (-), period (.), underscore (<u> </u>), plus sign (+), and equal sign (=). The at symbol (@) is supported in remote usernames but not in local usernames. Usernames must begin with an alphanumeric character. The default password is undefined. The 0 option indicates that the password is clear text, and the 5 option indicates that the password is encrypted. The default is 0 (clear text).</p> <p>Note If you do not specify a password, the user might not be able to log in to the Inspur INOS-CN device.</p> <p>Note If you create a user account with the encrypted password option, the corresponding SNMP user will not be created.</p>
Step 3	<p>username <i>user-id</i> ssh-cert-dn <i>dn-name</i> {dsa rsa}</p> <p>Example:</p> <pre>switch(config)# username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1, emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith" rsa</pre>	<p>Specifies an SSH X.509 certificate distinguished name and DSA or RSA algorithm to use for authentication for an existing user account. The distinguished name can be up to 512 characters and must follow the format shown in the examples. Make sure the email address and state are configured as <i>emailAddress</i> and <i>ST</i>, respectively.</p>
Step 4	<p>[no] crypto ca trustpoint <i>trustpoint</i></p> <p>Example:</p> <pre>switch(config)# crypto ca trustpoint winca switch(config-trustpoint)#</pre>	<p>Configures a trustpoint.</p> <p>Note Before you delete a trustpoint using the no form of this command, you must first delete the CRL and CA certificate, using the delete crl and</p>

	Command or Action	Purpose
		delete ca-certificate commands.
Step 5	crypto ca authenticate trustpoint Example: <pre>switch(config-trustpoint)# crypto ca authenticate winca</pre>	Configures a CA certificate for the trustpoint. Note To delete a CA certificate, enter the delete ca-certificate command in the trustpoint configuration mode.
Step 6	(Optional) crypto ca crl request trustpoint bootflash:static-crl.crl Example: <pre>switch(config-trustpoint)# crypto ca crl request winca bootflash:crllist.crl</pre>	This command is optional but highly recommended. Configures the certificate revocation list (CRL) for the trustpoint. The CRL file is a snapshot of the list of revoked certificates by the trustpoint. This static CRL list is manually copied to the device from the Certification Authority (CA). Note Static CRL is the only supported revocation check method. Note To delete the CRL, enter the delete crl command.
Step 7	(Optional) show crypto ca certificates Example: <pre>switch(config-trustpoint)# show crypto ca certificates</pre>	Displays the configured certificate chain and associated trustpoint.
Step 8	(Optional) show crypto ca crl trustpoint Example: <pre>switch(config-trustpoint)# show crypto ca crl winca</pre>	Displays the contents of the CRL list of the specified trustpoint.
Step 9	(Optional) show user-account Example: <pre>switch(config-trustpoint)# show user-account</pre>	Displays configured user account details.
Step 10	(Optional) show users Example: <pre>switch(config-trustpoint)# show users</pre>	Displays the users logged into the device.
Step 11	(Optional) copy running-config startup-config Example:	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	switch(config-trustpoint)# copy running-config startup-config	

6.6.9 Configuring Legacy SSH Algorithm Support

You can configure support for legacy SSH security algorithms, message authentication codes (MACs), key types, and ciphers.

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **ssh kexalgs all**
3. (Optional) **ssh macs all**
4. (Optional) **ssh ciphers all**
5. (Optional) **ssh keytypes all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#?</pre>	Enters the global configuration mode.
Step 2	(Optional) ssh kexalgs all Example: <pre>switch(config)# ssh kexalgs all</pre>	Enables all supported KexAlgorithms which are the key exchange methods that are used to generate per-connection keys. Supported KexAlgorithms are: <ul style="list-style-type: none"> • curve25519-sha256 • diffie-hellman-group-exchange-sha256 • diffie-hellman-group14-sha1 • diffie-hellman-group1-sha1 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521
Step 3	(Optional) ssh macs all Example: <pre>switch(config)# ssh macs all</pre>	Enables all supported MACs which are the message authentication codes used to detect traffic modification. Supported MACs are: <ul style="list-style-type: none"> • hmac-sha1

	Command or Action	Purpose
		<ul style="list-style-type: none"> • hmac-sha2-256 • hmac-sha2-512
Step 4	<p>(Optional) ssh ciphers all</p> <p>Example:</p> <pre>switch(config)# ssh ciphers all</pre>	<p>Enables all supported ciphers to encrypt the connection.</p> <p>Supported ciphers are:</p> <ul style="list-style-type: none"> • aes128-cbc • aes192-cbc • aes256-cbc • aes128-ctr • aes192-ctr • aes256-ctr • aes256-gcm@openssh.com • aes128-gcm@openssh.com
Step 5	<p>(Optional) ssh keytypes all</p> <p>Example:</p> <pre>switch(config)# ssh keytypes all</pre>	<p>Enables all supported PubkeyAcceptedKeyTypes which are the public key algorithms that the server can use to authenticate itself to the client.</p> <p>Supported key types are:</p> <ul style="list-style-type: none"> • ecdsa-sha2-nistp256 • ecdsa-sha2-nistp384 • ecdsa-sha2-nistp521 • ssh-dss • ssh-rsa

6.6.10 Changing the Default SSH Server Port

Beginning with Inspur INOS-CN Release 9.2(1i), you can change the SSHv2 port number from the default port number 22. Encryptions used while changing the default SSH port provides you with connections that support stronger privacy and session integrity

SUMMARY STEPS

1. **configure terminal**
2. **no feature ssh**
3. **show sockets local-port-range**
4. **ssh port local-port**

5. **feature ssh**
6. **exit**
7. (Optional) **show running-config security all**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	no feature ssh Example: <pre>switch(config)# no feature ssh</pre>	Disables SSH.
Step 3	show sockets local-port-range Example: <pre>switch(config)# show sockets local port range (15001 - 58000) switch(config)# local port range (58001 - 63535) and nat port range (63536 - 65535)</pre>	Displays the available port range.
Step 4	ssh port local-port Example: <pre>switch(config)# ssh port 58003</pre>	Configures the port.
Step 5	feature ssh Example: <pre>switch(config)# feature ssh</pre>	Enables SSH.
Step 6	exit Example: <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
Step 7	(Optional) show running-config security all Example: <pre>switch# ssh port 58003</pre>	Displays the security configuration.
Step 8	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

6.6.11 Clearing SSH Hosts

When you download a file from a server using SCP or SFTP, or when you start an SSH session from this device

to a remote host, you establish a trusted SSH relationship with that server. You can clear the list of trusted SSH servers for your user account.

SUMMARY STEPS

6.6.12 Disabling the SSH Server

1. clear ssh hosts

DETAILED STEPS

	Command or Action	Purpose
Step 1	clear ssh hosts Example: switch# clear ssh hosts	Clears the SSH host sessions and the known host file.

By default, the SSH server is enabled on the Inspur INOS-CN device. You can disable the SSH server to prevent SSH access to the switch.

SUMMARY STEPS

1. configure terminal
2. no feature ssh
3. exit
4. (Optional) show ssh server
5. (Optional) copy running-config startup-config

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	no feature ssh Example: switch(config)# no feature ssh	Disables SSH.
Step 3	exit Example: switch(config)# exit switch#	Exits global configuration mode.
Step 4	(Optional) show ssh server Example: switch# show ssh server	Displays the SSH server configuration.
Step 5	(Optional) copy running-config startup-config Example:	Copies the running configuration to the startup configuration.

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

6.6.13 Deleting SSH Server Keys

You can delete SSH server keys on the Inspur INOS-CN device after you disable the SSH server.

SUMMARY STEPS

1. **configure terminal**
2. **no feature ssh**
3. **no ssh key [dsa | rsa | ecdsa]**
4. **exit**
5. (Optional) **show ssh key**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	Enters global configuration mode.
Step 2	no feature ssh Example: <code>switch(config)# no feature ssh</code>	Disables SSH.
Step 3	no ssh key [dsa rsa ecdsa] Example: <code>switch(config)# no ssh key rsa</code>	Deletes the SSH server key. The default is to delete all the SSH keys.
Step 4	exit Example: <code>switch(config)# exit</code> <code>switch#</code>	Exits global configuration mode.
Step 5	(Optional) show ssh key Example: <code>switch# show ssh key</code>	Displays the SSH server key configuration.
Step 6	(Optional) copy running-config startup-config Example: <code>switch# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

6.6.14 Clearing SSH Sessions

You can clear SSH sessions from the Inspur INOS-CN device.

SUMMARY STEPS

1. **show users**
2. **clear line vty-line**

DETAILED STEPS

	Command or Action	Purpose
Step 1	show users Example: switch# show users	Displays user session information.
Step 2	clear line vty-line Example: switch(config)# clear line pts/12	Clears a user SSH session.

6.7 Configuring Telnet

This section describes how to configure Telnet on the Inspur INOS-CN device.

6.7.1 Enabling the Telnet Server

You can enable the Telnet server on the Inspur INOS-CN device. By default, the Telnet server is disabled.

SUMMARY STEPS

1. **configure terminal**
2. **feature telnet**
3. **exit**
4. (Optional) **show telnet server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	feature telnet Example: switch(config)# feature telnet	Enables the Telnet server. The default is disabled.
Step 3	exit Example: switch(config)# exit switch#	Exits global configuration mode.
Step 4	(Optional) show telnet server	Displays the Telnet server configuration.

	Command or Action	Purpose
	Example: switch# show telnet server	
Step 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

6.7.2 Starting Telnet Sessions to Remote Devices

You can start Telnet sessions to connect to remote devices from the Inspur INOS-CN device. You can start Telnet sessions using either IPv4 or IPv6.

Before you begin

- Obtain the hostname or IP address for the remote device and, if needed, the username on the remote device.
- Enable the Telnet server on the Inspur INOS-CN device.
- Enable the Telnet server on the remote device.

SUMMARY STEPS

1. **telnet** {*ipv4-address* | *host-name*} [*port-number*] [**vrf** *vrf-name*]
2. **telnet6** {*ipv6-address* | *host-name*} [*port-number*] [**vrf** *vrf-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	telnet { <i>ipv4-address</i> <i>host-name</i> } [<i>port-number</i>] [vrf <i>vrf-name</i>] Example: switch# telnet 10.10.1.1	Starts a Telnet session to a remote device using IPv4. The default port number is 23. The range is from 1 to 65535. The default VRF is the default VRF.
Step 2	telnet6 { <i>ipv6-address</i> <i>host-name</i> } [<i>port-number</i>] [vrf <i>vrf-name</i>] Example: switch# telnet6 2001:0DB8::ABCD:1 vrf management	Starts a Telnet session to a remote device using IPv6. The default port number is 23. The range is from 1 to 65535. The default VRF is the default VRF.

6.7.3 Clearing Telnet Sessions

You can clear Telnet sessions from the Inspur INOS-CN device.

Before you begin

- Enable the Telnet server on the Inspur INOS-CN device.

SUMMARY STEPS

1. **show users**
2. **clear line vty-line**

DETAILED STEPS

	Command or Action	Purpose
Step 1	show users Example: switch# show users	Displays user session information.
Step 2	clear line vty-line Example: switch(config)# clear line pts/12	Clears a user Telnet session.

6.8 Verifying the SSH and Telnet Configuration

To display the SSH and Telnet configuration information, perform one of the following tasks:

Command or Action	Purpose
show ssh key [dsa rsa] [md5]	Displays the SSH server keys. This command displays the fingerprint in SHA256 format by default. SHA256 is more secure than the old default format of MD5. However, the md5 option has been added, if you want to see the fingerprint in MD5 format for backward compatibility.
show running-config security [all]	Displays the SSH and user account configuration in the running configuration. The all keyword displays the default values for the SSH and user accounts.
show ssh server	Displays the SSH server configuration.
show telnet server	Displays the Telnet server configuration.
show username username keypair	Displays the public key for the specified user.
show user-account	Displays configured user account details.
show users	Displays the users logged into the device.
show crypto ca certificates	Displays the configured CA certificate and associated trustpoint for X.509v3 certificate-based SSH authentication.
show crypto ca crl trustpoint	Displays the contents of the CRL list of the specified trustpoint for X.509v3 certificate-based SSH authentication.

6.9 Configuration Example for SSH

The following example shows how to configure SSH with an OpenSSH key:

Step 1 Disable the SSH server.

Example:

```
switch# configure terminal
switch(config)# no feature ssh
```

Step 2 Generate an SSH server key.

Example:

```
switch(config)# ssh key rsa
generating rsa key(1024 bits).....
generated rsa key
```

Step 3 Enable the SSH server.

Example:

```
switch(config)# feature ssh
```

Step 4 Display the SSH server key.

Example:

```
switch(config)# show ssh key
could not retrieve dsa key information
*****
rsa Keys generated:Tue Oct 01 13:13:47 2018
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDh4+DZboQJbJt10nJhgKBYL5101hsFM2oZRi9+JqEU
GA44I9ej+E5NIRZ1x8ohIt6Vx9Et5cs07Pw72rjUwR3UPmuAm7Inspur7I/SyLGEp3WUL7sqbLvNF5GqKXph
oqMT075WUdbGWphorA2g0tTObrRFIQBJVQ0SSBh3oEaaALqYUQ==
bitcount:1024
fingerprint:
SHA256:V6KAeLAIKRRUPBZm1Yq3r16JW7Eo7vhLi6CXYxnD/+Y
*****
*****
```

Step 5 Specify the SSH public key in OpenSSH format.

Example:

```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAEAy19oF6QaZ19G+3f1XswK30iW4H7YyUyuA50r
v7gsEPjhbOYmsi6PAVKu1nIf/DQhum+1JNqJP/eLowb7ubO+1VKRXY/G+1JNIQ
W3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH3UD/vKyzIEh5
4Tplx8=
```

Step 6 Save the configuration.

Example:

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

6.10 Configuration Example for SSH Passwordless File Copy

The following example shows how to copy files from a Inspur INOS-CN device to a secure copy (SCP) or secure FTP (SFTP) server without a password:

Step 1 Generate the SSH public and private keys and store them in the home directory of the Inspur INOS-CN device for the specified user.

Example:

```
switch# configure terminal
switch(config)# username admin keypair generate rsa
generating rsa key(1024 bits).....
```

```
generated rsa key
```

Step 2 Display the public key for the specified user.

Example:

```
switch(config)# show username admin keypair
*****
rsa Keys generated: Thu Oct  1 11:10:29 2018
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZE1TfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TByYDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoaJzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=
bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
*****
could not retrieve dsa key information
*****
```

Step 3 Export the public and private keys from the home directory of the Inspur INOS-CN device to the specified bootflash directory.

Example:

```
switch(config)# username admin keypair export bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# dir
.
.
.
951 Jul 09 11:13:59 2013 key_rsa
221 Jul 09 11:14:00 2013 key_rsa.pub
.
.
```

Step 4 After copying these two files to another Inspur INOS-CN device using the **copy scp** or **copy sftp** command, import them to the home directory of the Inspur INOS-CN device.

Example:

```
switch(config)# username admin keypair import bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# show username admin keypair
*****
rsa Keys generated: Thu Oct  1 11:10:29 2018
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZE1TfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TByYDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoaJzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=
bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
*****
could not retrieve dsa key information
*****
switch(config)#
```

Step 5 On the SCP or SFTP server, append the public key stored in key_rsa.pub to the authorized_keys file.

Example:

```
$ cat key_rsa.pub >> $HOME/.ssh/ authorized_keys
```

You can now copy files from the Inspur INOS-CN device to the server without a password using standard SSH and SCP commands.

Step 6 (Optional) Repeat this procedure for the DSA keys.

6.11 Configuration Example for X.509v3 Certificate-Based SSH Authentication

The following example shows how to configure SSH authentication using X.509v3 certificates:

```

configure terminal
username jsmith password 4Ty18Rnt
username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1,
emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN =
jsmith" rsa
crypto ca trustpoint tp1
crypto ca authenticate tp1
crypto ca crl request tp1 bootflash:crl1.crl

show crypto ca certificates
Trustpoint: tp1
CA certificate 0:
subject= /CN=SecDevCA
issuer= /CN=SecDevCA
serial=01AB02CD03EF04GH05IJ06KL07MN
notBefore=Oct 01 12:36:26 2018 GMT
notAfter=Oct 01 12:46:23 2021 GMT
SHA1 Fingerprint=47:29:E3:00:C1:C1:47:F2:56:8B:AC:B2:1C:64:48:FC:F4:8D:53:AF
purposes: sslserver sslclient

show crypto ca crl tp1
Trustpoint: tp1 CRL: Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: /CN=SecDevCA
  Last Update: Oct 1 20:03:15 2018 GMT
  Next Update: Oct 16 08:23:15 2018 GMT
  CRL extensions:
    X509v3 Authority Key Identifier:
      keyid:30:43:AA:80:10:FE:72:00:DE:2F:A2:17:E4:61:61:44:CE:78:FF:2A

show user-account
user:user1
  this user account has no expiry date
  roles:network-operator
  ssh cert DN : /C = US, ST = New York, L = Metropolis, O = Inspur , OU = csg, CN
= user1; Algo: x509v3-sign-rsa

show users
LINE          TIME          IDLE          PID          COMMENT
NAME
user1 pts/1        Jul 27 18:43 00:03        18796        (10.10.10.1) session=ssh

```

6.12 Additional References for SSH and Telnet

This section describes additional information related to implementing SSH and Telnet.

Related Documents

Related Topic	Document Title
VRF configuration	<i>Inspur CN12900 Series INOS-CN Unicast Routing Configuration Guide</i>

RFCs

RFCs	Title
RFC 6187	<i>X.509v3 Certificates for Secure Shell Authentication</i>

CHAPTER 7 Configuring IP ACLs

This chapter describes how to configure IP access control lists (ACLs) on Inspur INOS-CN devices.

Unless otherwise specified, the term IP ACL refers to IPv4 and IPv6 ACLs.

This chapter includes the following sections:

7.1 About ACLs

An ACL is an ordered set of rules that you can use to filter traffic. Each rule specifies a set of conditions that a packet must satisfy to match the rule. When the device determines that an ACL applies to a packet, it tests the packet against the conditions of all rules. The first matching rule determines whether the packet is permitted or denied. If there is no match, the device applies the applicable implicit rule. The device continues processing packets that are permitted and drops packets that are denied.

You can use ACLs to protect networks and specific hosts from unnecessary or unwanted traffic. For example, you could use ACLs to disallow HTTP traffic from a high-security network to the Internet. You could also use ACLs to allow HTTP traffic but only to specific sites, using the IP address of the site to identify it in an IP ACL.¹³²

7.1.1 ACL Types and Applications

The device supports the following types of ACLs for security traffic filtering:

IPv4 ACLs

The device applies IPv4 ACLs only to IPv4 traffic.

IPv6 ACLs

The device applies IPv6 ACLs only to IPv6 traffic.

MAC ACLs

The device applies MAC ACLs only to non-IP traffic.

IP and MAC ACLs have the following types of applications:

Port ACL

Filters Layer 2 traffic

Router ACL

Filters Layer 3 traffic

VLAN ACL

Filters VLAN traffic

VTY ACL

Filters virtual teletype (VTY) traffic

This table summarizes the applications for security ACLs.

Table 10 : Security ACL Applications

Application	Supported Interfaces	Types of ACLs Supported
Port ACL	• Layer 2 interfaces	• IPv4 ACLs

Application	Supported Interfaces	Types of ACLs Supported
	the ACL filters traffic on all VLANs on the	<ul style="list-style-type: none"> • IPv6 ACLs • MAC ACLs
Router ACL	<ul style="list-style-type: none"> • VLAN interfaces • Physical Layer 3 interfaces • Layer 3 Ethernet subinterfaces • Layer 3 Ethernet port-channel interfaces <p>interfaces globally before you can configure a VLAN interface.</p>	<ul style="list-style-type: none"> • IPv4 ACLs • IPv6 ACLs <p>Note MAC ACLs are supported on Layer 3 interfaces only if you enable MAC packet classification.</p>
VLAN ACL	<ul style="list-style-type: none"> • VLANs 	<ul style="list-style-type: none"> • IPv4 ACLs • IPv6 ACLs • MAC ACLs
VTY ACL	<ul style="list-style-type: none"> • VTYs 	<ul style="list-style-type: none"> • IPv4 ACLs • IPv6 ACLs

7.1.2 Order of ACL Application

When the device processes a packet, it determines the forwarding path of the packet. The path determines which ACLs that the device applies to the traffic. The device applies the ACLs in the following order:

1. Port ACL
2. Ingress VACL
3. Ingress router ACL
4. Ingress VTY ACL
5. Egress VTY ACL
6. Egress router ACL
7. Egress VACL

If the packet is bridged within the ingress VLAN, the device does not apply router ACLs. The following figure shows the order in which the device applies ACLs.

Figure 4: Order of ACL Application

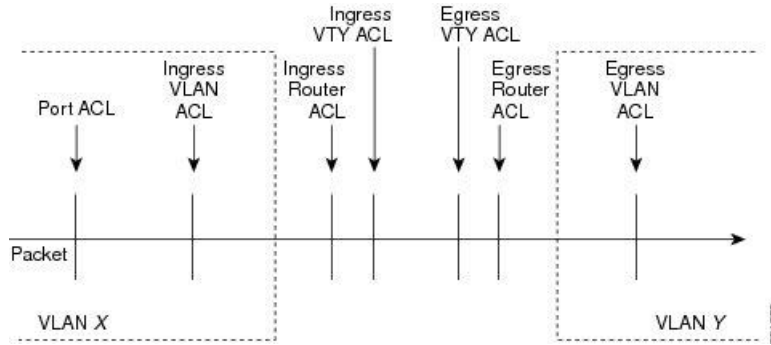
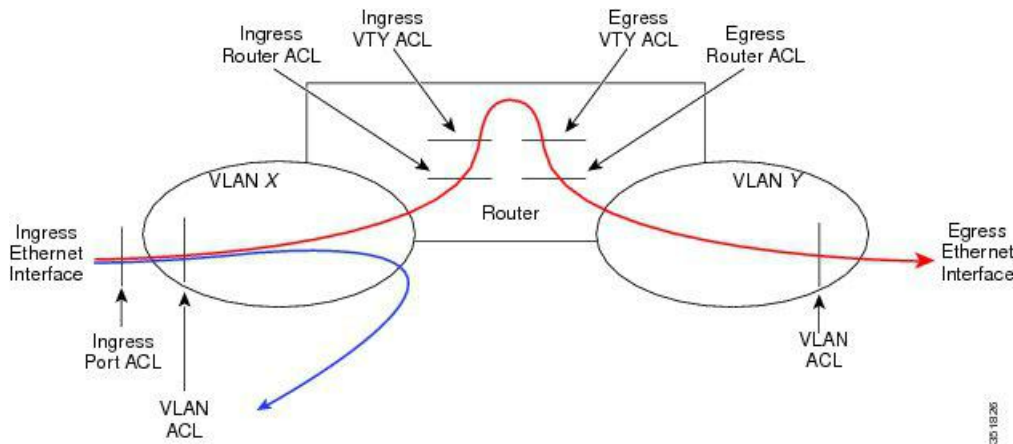


Figure 5: ACLs and Packet Flow

The following figure shows where the device applies ACLs, depending upon the type of ACL. The red path indicates a packet sent to a destination on a different interface than its source. The blue path indicates a packet that is bridged within its VLAN.

The device applies only the applicable ACLs. For example, if the ingress port is a Layer 2 port and the traffic is on a VLAN that is a VLAN interface, a port ACL and a router ACL both can apply. In addition, if a VACL is applied to the VLAN, the device applies that ACL too.



7.1.3 About Rules

Rules are what you create, modify, and remove when you configure how an ACL filters network traffic. Rules appear in the running configuration. When you apply an ACL to an interface or change a rule within an ACL that is already applied to an interface, the supervisor module creates ACL entries from the rules in the running configuration and sends those ACL entries to the applicable I/O module. Depending upon how you configure the ACL, there may be more ACL entries than rules, especially if you implement policy-based ACLs by using object groups when you configure rules.

You can create rules in access-list configuration mode by using the **permit** or **deny** command. The device allows traffic that matches the criteria in a permit rule and blocks traffic that matches the criteria in a deny rule. You have many options for configuring the criteria that traffic must meet in order to match the rule.

This section describes some of the options that you can use when you configure a rule.

Protocols for IP ACLs and MAC ACLs

IPv4, IPv6, and MAC ACLs allow you to identify traffic by protocol. For your convenience, you can specify

some protocols by name. For example, in an IPv4 or IPv6 ACL, you can specify ICMP by name.

You can specify any protocol by number. In MAC ACLs, you can specify protocols by the EtherType number of the protocol, which is a hexadecimal number. For example, you can use 0x0800 to specify IP traffic in a MAC ACL rule.

In IPv4 and IPv6 ACLs, you can specify protocols by the integer that represents the Internet protocol number.

Source and Destination

In each rule, you specify the source and the destination of the traffic that matches the rule. You can specify both the source and destination as a specific host, a network or group of hosts, or any host. How you specify the source and destination depends on whether you are configuring IPv4 ACLs, IPv6 ACLs, or MAC ACLs.

Implicit Rules for IP and MAC ACLs

IP and MAC ACLs have implicit rules, which means that although these rules do not appear in the running configuration, the device applies them to traffic when no other rules in an ACL match. When you configure the device to maintain per-rule statistics for an ACL, the device does not maintain statistics for implicit rules.

All IPv4 ACLs include the following implicit rule:

```
deny ip any any
```

This implicit rule ensures that the device denies unmatched IP traffic.

All IPv6 ACLs include the following implicit rule:

```
deny ipv6 any any
```

This implicit rule ensures that the device denies unmatched IPv6 traffic.

All MAC ACLs include the following implicit rule:

```
deny any any protocol
```

This implicit rule ensures that the device denies the unmatched traffic, regardless of the protocol specified in the Layer 2 header of the traffic.

Additional Filtering Options

You can identify traffic by using additional options. These options differ by ACL type. The following list includes most but not all additional filtering options:

- IPv4 ACLs support the following additional filtering options:
 - Layer 4 protocol
 - TCP and UDP ports
 - ICMP types and codes
 - IGMP types
 - Precedence level
 - Differentiated Services Code Point (DSCP) value
 - TCP packets with the ACK, FIN, PSH, RST, SYN, or URG bit set
 - Established TCP connections
 - Packet length
- IPv6 ACLs support the following additional filtering options:
 - Layer 4 protocol
 - Encapsulating Security Payload
 - Payload Compression Protocol
 - Stream Control Transmission Protocol (SCTP)
 - SCTP, TCP, and UDP ports
 - ICMP types and codes
 - DSCP value
 - TCP packets with the ACK, FIN, PSH, RST, SYN, or URG bit set
 - Established TCP connections
 - Packet length
- MAC ACLs support the following additional filtering options:

- Layer 3 protocol (Ethertype)
- VLAN ID
- Class of Service (CoS)

Sequence Numbers

The device supports sequence numbers for rules. Every rule that you enter receives a sequence number, either assigned by you or assigned automatically by the device. Sequence numbers simplify the following ACL tasks:

Adding new rules between existing rules

By specifying the sequence number, you specify where in the ACL a new rule should be positioned. For example, if you need to insert a rule between rules numbered 100 and 110, you could assign a sequence number of 105 to the new rule.

Removing a rule

Without using a sequence number, removing a rule requires that you enter the whole rule, as follows:

```
switch(config-acl)# no permit tcp 10.0.0.0/8 any
```

However, if the same rule had a sequence number of 101, removing the rule requires only the following command:

```
switch(config-acl)# no 101
```

Moving a rule

With sequence numbers, if you need to move a rule to a different position within an ACL, you can add a second instance of the rule using the sequence number that positions it correctly, and then you can remove the original instance of the rule. This action allows you to move the rule without disrupting traffic.

If you enter a rule without a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule to the rule. For example, if the last rule in an ACL has a sequence number of 225 and you add a rule without a sequence number, the device assigns the sequence number 235 to the new rule.

In addition, Inspur INOS-CN allows you to reassign sequence numbers to rules in an ACL. Resequencing is useful when an ACL has rules numbered contiguously, such as 100 and 101, and you need to insert one or more rules between those rules.

Logical Operators and Logical Operation Units

IP ACL rules for TCP and UDP traffic can use logical operators to filter traffic based on port numbers. Inspur INOS-CN supports logical operators in only the ingress direction.

The device stores operator-operand couples in registers called logical operator units (LOUs). The LOU usage for each type of operator is as follows:

eq

Is never stored in an LOU

gt

Uses 1 LOU

lt

Uses 1 LOU

neq

Uses 1 LOU

range

Uses 1 LOU

IPv4 ACL Logging

The IPv4 ACL logging feature monitors IPv4 ACL flows and logs statistics.

A flow is defined by the source interface, protocol, source IP address, source port, destination IP address, and destination port values. The statistics maintained for a flow include the number of forwarded packets (for each flow that matches the permit conditions of the ACL entry) and dropped packets (for each flow that matches the deny conditions of the ACL entry).

7.1.4 Time Ranges

You can use time ranges to control when an ACL rule is in effect. For example, if the device determines that a particular ACL applies to traffic arriving on an interface, and a rule in the ACL uses a time range that is not in effect, the device does not compare the traffic to that rule. The device evaluates time ranges based on its clock.

When you apply an ACL that uses time ranges, the device updates the affected I/O module whenever a time range referenced in the ACL starts or ends. Updates that are initiated by time ranges occur on a best-effort priority. If the device is especially busy when a time range causes an update, the device may delay the update by up to a few seconds.

IPv4, IPv6, and MAC ACLs support time ranges. When the device applies an ACL to traffic, the rules in effect are as follows:

- All rules without a time range specified
- Rules with a time range that includes the second when the device applies the ACL to traffic

The device supports named, reusable time ranges, which allows you to configure a time range once and specify it by name when you configure many ACL rules. Time range names have a maximum length of 64 alphanumeric characters.

A time range contains one or more rules. The two types of rules are as follows:

Absolute

A rule with a specific start date and time, specific end date and time, both, or neither. The following items describe how the presence or absence of a start or end date and time affect whether an absolute time range rule is active:

- Start and end date and time both specified—The time range rule is active when the current time is later than the start date and time and earlier than the end date and time.
- Start date and time specified with no end date and time—The time range rule is active when the current time is later than the start date and time.
- No start date and time with end date and time specified—The time range rule is active when the current time is earlier than the end date and time.
- No start or end date and time specified—The time range rule is always active.

For example, you could prepare your network to allow access to a new subnet by specifying a time range that allows access beginning at midnight of the day that you plan to place the subnet online. You can use that time range in ACL rules that apply to the subnet. After the start time and date have passed, the device automatically begins applying the rules that use this time range when it applies the ACLs that contain the rules.

Periodic

A rule that is active one or more times per week. For example, you could use a periodic time range to allow access to a lab subnet only during work hours on weekdays. The device automatically applies ACL rules that use this time range only when the range is active and when it applies the ACLs that contain the rules.

Time ranges also allow you to include remarks, which you can use to insert comments into a time range. Remarks have a maximum length of 100 alphanumeric characters.

The device determines whether a time range is active as follows:

- The time range contains one or more absolute rules—The time range is active if the current time is within one or more absolute rules.
- The time range contains one or more periodic rules—The time range is active if the current time is within one or more periodic rules.
- The time range contains both absolute and periodic rules—The time range is active if the current time is within one or more absolute rules and within one or more periodic rules.

When a time range contains both absolute and periodic rules, the periodic rules can only be active when at least one absolute rule is active.

7.1.5 Policy-Based ACLs

The device supports policy-based ACLs (PBACLs), which allow you to apply access control policies across object groups. An object group is a group of IP addresses or a group of TCP or UDP ports. When you create a rule, you specify the object groups rather than specifying IP addresses or ports.

Using object groups when you configure IPv4 or IPv6 ACLs can help reduce the complexity of updating ACLs when you need to add or remove addresses or ports from the source or destination of rules. For example, if three rules reference the same IP address group object, you can add an IP address to the object instead of changing all three rules.

PBACLs do not reduce the resources required by an ACL when you apply it to an interface. When you apply a PBACL or update a PBACL that is already applied, the device expands each rule that refers to object groups into one ACL entry per object within the group. If a rule specifies the source and destination both with object groups, the number of ACL entries created on the I/O module when you apply the PBACL is equal to the number of objects in the source group multiplied by the number of objects in the destination group.

The following object group types apply to port, router, policy-based routing (PBR), and VLAN ACLs:

IPv4 Address Object Groups

Can be used with IPv4 ACL rules to specify source or destination addresses. When you use the **permit** or **deny** command to configure a rule, the **addrgroup** keyword allows you to specify an object group for the source or destination.

IPv6 Address Object Groups

Can be used with IPv6 ACL rules to specify source or destination addresses. When you use the **permit** or **deny** command to configure a rule, the **addrgroup** keyword allows you to specify an object group for the source or destination.

Protocol Port Object Groups

Can be used with IPv4 and IPv6 TCP and UDP rules to specify source or destination ports. When you use the **permit** or **deny** command to configure a rule, the **portgroup** keyword allows you to specify an object group for the source or destination.

7.1.6 Statistics and ACLs

The device can maintain global statistics for each rule that you configure in IPv4, IPv6, and MAC ACLs. If an ACL is applied to multiple interfaces, the maintained rule statistics are the sum of packet matches (hits) on all the interfaces on which that ACL is applied.

For each ACL that you configure, you can specify whether the device maintains statistics for that ACL, which allows you to turn ACL statistics on or off as needed to monitor traffic filtered by an ACL or to help troubleshoot the configuration of an ACL.

The device does not maintain statistics for implicit rules in an ACL. For example, the device does not maintain a count of packets that match the implicit **deny ip any any** rule at the end of all IPv4 ACLs. If you want to maintain statistics for implicit rules, you must explicitly configure the ACL with rules that are identical to the implicit rules.

7.1.7 Atomic ACL Updates

By default, when a supervisor module of a Inspur CN12900 Series device updates an I/O module with changes to an ACL, it performs an atomic ACL update. An atomic update does not disrupt traffic that the updated ACL applies to; however, an atomic update requires that an I/O module that receives an ACL update has enough available resources to store each updated ACL entry in addition to all pre-existing entries in the affected ACL. After the update occurs, the additional resources used for the update are freed. If the I/O module lacks the required resources, the device generates an error message and the ACL update to the I/O module fails.

If an I/O module lacks the resources required for an atomic update, you can disable atomic updates by using the **no hardware access-list update atomic** command; however, during the brief time required for the device to remove the preexisting ACL and implement the updated ACL, traffic that the ACL applies to is dropped by default.

If you want to permit all traffic that an ACL applies to while it receives a nonatomic update, use the **hardware access-list update default-result permit** command.

This example shows how to disable atomic updates to ACLs:

```
switch# config t
switch(config)# no hardware access-list update atomic
```

This example shows how to permit affected traffic during a nonatomic ACL update:

```
switch# config t
switch(config)# hardware access-list update default-result permit
```

This example shows how to revert to the atomic update method:

```
switch# config t
switch(config)# no hardware access-list update default-result permit
switch(config)# hardware access-list update atomic
```

7.1.8 Session Manager Support for IP ACLs

Session Manager supports the configuration of IP and MAC ACLs. This feature allows you to verify ACL configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration.

7.1.9 ACL TCAM Regions

You can change the size of the ACL ternary content addressable memory (TCAM) regions in the hardware.

On Inspur CN12900 INOS-CN Series switches, the egress TCAM size is 1K, divided into four 256 entries. A slice is the unit of allocation. A slice can be allocated to one region only. For example, a 512-size slice cannot be used to configure two features of size 256 each. Similarly, a 256-size slice cannot be used to configure two features of size 128 each. The IPv4 TCAM regions are single wide. The IPv6, QoS, MAC, CoPP, and system TCAM regions are double wide and consume double the physical TCAM entries. For example, a logical region size of 256 entries actually consumes 512 physical TCAM entries.

You can create IPv6, port ACLs, VLAN ACLs, and router ACLs, and you can match IPv6 and MAC addresses for QoS. However, Inspur INOS-CN cannot support all of them simultaneously. You must remove or reduce the size of the existing TCAM regions (TCAM carving) to enable the IPv6, MAC, or other desired TCAM regions. For every TCAM region configuration command, the system evaluates if the new change can be fit in the TCAM. If not, it reports an error, and the command is rejected. You must remove or reduce the size of existing TCAM regions to make room for new requirements.

The concepts of TCAM slices and single- and double-wide regions do not apply to these switches. For example, the ing-ifacl region can host IPv4, IPv6, or MAC type entries. IPv4 and MAC types occupy one TCAM entry whereas IPv6 types occupy two TCAM entries.

ACL TCAM region sizes have the following guidelines and limitations:

- To enable RAACL or PACL on existing TCAM regions, you must carve the TCAM region beyond 12, 288.
- When a VACL region is configured, it is configured with the same size in both the ingress and egress directions. If the region size cannot fit in either direction, the configuration is rejected.

values. Any region size can be carved with a value only in multiples of 256 entries (with the exception of the span region, which can be carved only in multiples of 512 entries).

- RAACL v6, CoPP, and multicast have default TCAM sizes and these TCAM sizes must be non-zero on the following Inspur CN12904 and Inspur CN12908 to avoid line card failure during reload:
- CN129-X6136YC-R
- CN129-X636C-R
- CN129-X636Q-R

The following table summarizes the regions that need to be configured for a given feature to work. The region sizes should be selected based on the scale requirements of a given feature.

Table 11 : Features per ACL TCAM Region

Feature Name	Region Name
Port ACL	ifacl: For IPv4 port ACLs ifacl-udf: For UDFs on IPv4 port ACLs ing-ifacl: For ingress IPv4, IPv6, and MAC port ACLs ipv6-ifacl: For IPv6 port ACLs mac-ifacl: For MAC port ACLs
Port QoS (QoS classification policy applied on Layer 2 ports or ns-qos, port channels) e-qos, or e-qos-lite: For classifying IPv4	qos, qos-lite, rp-qos, rp-qos-lite, packets ing-l2-qos: For classifying ingress Layer 2 packets ipv6-qos, rp-ipv6-qos, ns-ipv6-qos, or e-ipv6-qos: For classifying IPv6 packets mac-qos, rp-mac-qos, ns-mac-qos, or e-mac-qos: For classifying non-IP packets.
VACL	vacl: For IPv4 packets ipv6-vacl: For IPv6 packets mac-vacl: For non-IP packets
VLAN QoS (QoS classification policy applied on a VLAN)	vqos or ns-vqos: For classifying IPv4 packets ipv6-vqos or ns-ipv6-vqos: For classifying IPv6 packets ing-l3-vlan-qos: For classifying ingress mac-vqos or ns-mac-vqos: For classifying non-IP packets
RAACL	egr-racl: For egress IPv4 RAACLs e-ipv6-racl: For egress IPv6 RAACLs ing-racl: For ingress IPv4 and IPv6 RAACLs racl: For IPv4 RAACLs ipv6-racl: For IPv6 RAACLs
Layer 3 QoS (QoS classification policy applied on Layer 3 ports or port channels)	l3qos, l3qos-lite, or ns-l3qos: For classifying IPv4 packets

Feature Name	Region Name
	ipv6-l3qos or ns-ipv6-l3qos: For classifying IPv6 packets
VLAN source or VLAN filter SPAN	span
SPAN filters	ifacl: For filtering IPv4 traffic on Layer 2 (switch port) source interfaces. ipv6-ifacl: For filtering IPv6 traffic on Layer 2 (switch port) source interfaces. mac-ifacl: For filtering Layer 2 traffic on Layer 2 (switch port) source interfaces. vacl: For filtering IPv4 traffic on VLAN sources. ipv6-vacl: For filtering IPv6 traffic on VLAN sources. mac-vacl: For filtering Layer 2 traffic on VLAN sources. racl: For filtering IPv4 traffic on Layer 3 interfaces. ipv6-racl: For filtering IPv6 traffic on Layer 3 interfaces.
SVI counters Note This region enables the packet counters for Layer 3 SVI interfaces.	svi
BFD, DHCP relay, or DHCPv6 relay	redirect
CoPP	copp Note The region size cannot be 0.
System-managed ACLs	system Note The region size cannot be changed.
vPC convergence Note This region boosts the convergence times when a vPC link goes down and traffic needs to be redirected to the peer link.	vpc-convergence Note Setting this region size to 0 might affect the convergence times of vPC link failures.
Fabric extender (FEX)	fex-ifacl, fex-ipv6-ifacl, fex-ipv6-qos, fex-mac-ifacl, fex-mac-qos, fex-qos, fex-qos-lite

Feature Name	Region Name
Dynamic ARP inspection (DAI)	arp-ether
IP source guard (IPSG)	ipsg
Multicast PIM Bidir	mcast_bidir
Static MPLS	mpls
Network address translation (NAT)	nat
NetFlow	ing-netflow
OpenFlow	openflow
sFlow	sflow

7.2 Licensing Requirements for IP ACLs

The following table shows the licensing requirements for this feature:

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

7.3 Prerequisites for IP ACLs

IP ACLs have the following prerequisites:

- You must be familiar with IP addressing and protocols to configure IP ACLs.
- You must be familiar with the interface types that you want to configure with ACLs.

7.4 Guidelines and Limitations for IP ACLs

IP ACLs have the following configuration guidelines and limitations:

- We recommend that you perform ACL configuration using the Session Manager. This feature allows you to verify ACL configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration. This is especially useful for ACLs that include more than 1000 rules. For more information about Session Manager, see the *Inspur CN12900 Series INOS-CN System Management Configuration Guide*.
- Configuring IPv4 PACLs in the range of 12k to 64k is supported on Inspur CN12900 Series switches.
- Duplicate ACL entries with different sequence numbers are allowed in the configuration. However, these duplicate entries are not programmed in the hardware access-list.
- Only 62 unique ACLs can be configured. Each ACL takes one label. If the same ACL is configured on multiple interfaces, the same label is shared. If each ACL has unique entries, the ACL labels are not shared, and the label limit is 62.
- In most cases, ACL processing for IP packets occurs on the I/O modules, which use hardware that

accelerates ACL processing. In some circumstances, processing occurs on the supervisor module, which can result in slower ACL processing, especially during processing that involves an ACL with a large number of rules. Management interface traffic is always processed on the supervisor module. If IP packets in any of the following categories are exiting a Layer 3 interface, they are sent to the supervisor module for processing:

- Packets that fail the Layer 3 maximum transmission unit check and therefore require fragmenting.
- IPv4 packets that have IP options (additional IP packet header fields following the destination address field).
- IPv6 packets that have extended IPv6 header fields.

Rate limiters prevent redirected packets from overwhelming the supervisor module.

- When you apply an ACL that uses time ranges, the device updates the ACL entries whenever a time range referenced in an ACL entry starts or ends. Updates that are initiated by time ranges occur on a best-effort priority. If the device is especially busy when a time range causes an update, the device may delay the update by up to a few seconds.
- To apply an IP ACL to a VLAN interface, you must have enabled VLAN interfaces globally. For more information about VLAN interfaces, see the *Inspur CN12900 Series INOS-CN Interfaces Configuration Guide*.
- The VTY ACL feature restricts all traffic for all VTY lines. You cannot specify different traffic restrictions for different VTY lines. Any router ACL can be configured as a VTY ACL.
- When you apply an undefined ACL to an interface, the system treats the ACL as empty and permits all traffic.
- IP tunnels do not support ACLs or QoS policies.
- The following guidelines apply to ACLs for VXLANs:
 - Ingress port ACLs applied on a Layer 2 port for traffic in the access to network direction (Layer 2 to Layer 3 encapsulation path) are supported on the inner payload.
 - We recommend using port ACLs on the access side to filter out traffic entering the overlay network.
 - Ingress router ACLs applied on an uplink Layer 3 interface matching on the inner or outer payload in the network to access direction (Layer 3 to Layer 2 decapsulation path) are not supported.
 - Egress router ACLs applied on an uplink Layer 3 interface matching on the inner or outer payload in the access to network direction (encapsulation path) are not supported.
- Inspur CN12900 INOS-CN Series switches, have the following limitations for ACL options that can be used on VXLAN traffic:
 - Does not support egress port ACLs applied on a Layer 2 port for traffic in the network to access direction (decapsulation path).
 - Supports ingress VACLs applied on a VLAN for traffic in the access to network direction (encapsulation path).
 - Supports egress VACLs applied on a VLAN for traffic in the network to access direction (decapsulation path).
 - Supports ingress RACLs applied on a tenant or server facing SVI for traffic in the access to network direction (encapsulation path).
 - Supports egress RACLs applied on a tenant or server facing SVI for traffic in the network to access direction (decapsulation path).
 - IPv6 ACL logging is not supported.
 - IPv4 ACL logging in the egress direction is not supported.
 - ACL logging for VACLs is not supported.
 - ACL logging applies to port ACLs configured by the **ip port access-group** command and to router ACLs configured by the **ip access-group** command only.
- The total number of IPv4 ACL flows is limited to a user-defined maximum value to prevent DoS attacks. If this limit is reached, no new logs are created until an existing flow finish.
- The number of syslog entries generated by IPv4 ACL logging is limited by the configured logging level of the ACL logging process. If the number of syslog entries exceeds this limit, the logging facility might

drop some logging messages. Therefore, IPv4 ACL logging should not be used as a billing tool or as an accurate source of the number of matches to an ACL.

- Egress ACLs are not supported for Inspur CN12908 switches with the CN129-X6136YC-R, CN129-X636C-R, and the CN129-X636Q-R line cards.
- For Network Forwarding Engine (NFE)-enabled switches, ingress RACLs matching the tunnel interface's outer header are not supported.
- If the same QoS policy and ACL are applied to multiple interfaces, the label will be shared only when the QoS policy is applied with the no-stats option.
- The switch hardware does not support range checks (Layer 4 operations) in the egress TCAM. Therefore, ACL and QoS policies with a Layer 4 operations-based classification need to be expanded to multiple entries in the egress TCAM. Make sure to consider this limitation for egress TCAM space planning.
- TCAM resources are shared in the following scenarios:
 - When a routed ACL is applied to multiple switched virtual interfaces (SVIs) in the ingress direction
 - When a routed ACL is applied to multiple physical Layer 3 interfaces in the ingress or egress direction
 - TCAM resources are not shared when a routed ACL is applied to multiple SVIs in the egress direction.
- HTTP methods are not supported on FEX ports.
- The **mode tap aggregation** command is not required for TAP aggregation unless it is used with MPLS stripping. However, HTTP methods are not supported after MPLS packets have been stripped.
- Layer 4 operations are not supported on egress TCAM regions.
- The MAC compression table size is 4096 + 512 overflow TCAM.
- An overlap of MAC addresses and MAC masks will be rejected.
- The ACL log rate limiter does not have any hardware counters for transmitted or dropped packets.
- The ACL log rate limiter is implemented at the per-TCAM entry level (instead of using aggregated rate limiting), and the default is 1 pps.
- The network address translation (NAT) exception counters are zero.
- Only PACL redirects are supported for TAP aggregation. VACL redirects are not supported.
- Only three of the following four features can be supported at a time: DHCPv4 snooping/relay, DHCPv6 relay, ARP snooping, VXLAN. The first three configured features will take effect, but the fourth one will fail because all three bridge domain label bits are already in use.
- RACLs cannot match on packets with multicast MAC destination addresses.
- For Broadcom-based Inspur CN12900 Series switches, when there is a SVI and subinterface matching the same VLAN tag, the traffic that gets routed out through a subinterface gets dropped if the access-list is configured on that SVI. This is due to an ASIC limitation and egress RACL on L3 subinterfaces is not supported due to this limitation.

7.5 Default Settings for IP ACLs

This table lists the default settings for IP ACL parameters.

Table 12 : Default IP ACL Parameters

Parameters	Default
IP ACLs	No IP ACLs exist by default
IP ACL entries	1024
ACL rules	Implicit rules apply to all ACLs
Object groups	No object groups exist by default

Parameters	Default
Time ranges	No time ranges exist by default

7.6 Configuring IP ACLs

7.6.1 Creating an IP ACL

You can create an IPv4 ACL or IPv6 ACL on the device and add rules to it.

Before you begin

We recommend that you perform the ACL configuration using the Session Manager. This feature allows you to verify the ACL configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration. This feature is especially useful for ACLs that include more than about 1000 rules.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
 - **ip access-list** *name*
 - **ipv6 access-list** *name*
3. (Optional) **fragments** {**permit-all** | **deny-all**}
4. [*sequence-number*] {**permit** | **deny**} *protocol* {*source-ip-prefix* | *source-ip-mask*} {*destination-ip-prefix* | *destination-ip-mask*}
5. (Optional) **statistics per-entry**
6. (Optional) Enter one of the following commands:
 - **show ip access-lists** *name*
 - **show ipv6 access-lists** *name*
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	Enter one of the following commands: <ul style="list-style-type: none"> • ip access-list <i>name</i> • ipv6 access-list <i>name</i> Example: <pre>switch(config)# ip access-list acl-01 switch(config-acl)#</pre>	Creates the IP ACL and enters IP ACL configuration mode. The <i>name</i> argument can be up to 64 characters.
Step 3	(Optional) fragments { permit-all deny-all } Example:	Optimizes fragment handling for noninitial fragments. When a device applies to traffic an ACL that contains the

	Command or Action	Purpose
	<pre>switch(config-acl)# fragments permit-all</pre>	fragments command, the fragments command only matches noninitial fragments that do not match any explicit permit or deny commands in the ACL.
Step 4	<p><i>[sequence-number] {permit deny} protocol</i></p> <p><i>{source-ip-prefix source-ip-mask} {destination-ip-prefix destination-ip-mask}</i></p> <p>Example:</p> <pre>switch(config-acl)# permit ip 192.168.2.0/24 any</pre> <p>Example:</p> <pre>switch(config-acl)# 10 permit ipv6 1::1 2::2 3::3 4::4</pre>	<p>Creates a rule in the IP ACL. You can create many rules.</p> <p>The <i>sequence-number</i> argument can be a whole number between 1 and 4294967295.</p> <p>The permit and deny commands support many ways of identifying traffic.</p> <p>For IPv4 and IPv6 access lists, you can specify a source and destination IPv4 or IPv6 prefix, which matches only on the first contiguous bits, or you can specify a source and destination IPv4 or IPv6 wildcard mask, which matches on any bit in the address.</p>
Step 5	<p>(Optional) statistics per-entry</p> <p>Example:</p> <pre>switch(config-acl)# statistics per-entry</pre>	Specifies that the device maintains global statistics for packets that match the rules in the ACL.
Step 6	<p>(Optional) Enter one of the following commands:</p> <ul style="list-style-type: none"> • show ip access-lists <i>name</i> • show ipv6 access-lists <i>name</i> <p>Example:</p> <pre>switch(config-acl)# show ip access-lists acl-01</pre>	Displays the IP ACL configuration.
Step 7	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config-acl)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

7.6.2 Changing an IP ACL

You can add and remove rules in an existing IPv4 or IPv6 ACL, but you cannot change existing rules. Instead, to change a rule, you can remove it and recreate it with the desired changes.

If you need to add more rules between existing rules than the current sequence numbering allows, you can use the **resequence** command to reassign sequence numbers.

Before you begin

We recommend that you perform ACL configuration using the Session Manager. This feature allows you to verify ACL configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration. This feature is especially useful for ACLs that include more than about 1000 rules.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
 - **ip access-list** *name*
 - **ipv6 access-list** *name*
3. (Optional) [*sequence-number*] {**permit** | **deny**} *protocol source destination*
4. (Optional) [**no**] **fragments** {**permit-all** | **deny-all**}
5. (Optional) **no** [*sequence-number*] {**permit** | **deny**} *protocol source destination*}
6. (Optional) [**no**] **statistics per-entry**
7. (Optional) Enter one of the following commands:
 - **show ip access-lists** *name*
 - **show ipv6 access-lists** *name*
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	Enter one of the following commands: <ul style="list-style-type: none"> • ip access-list <i>name</i> • ipv6 access-list <i>name</i> Example: <pre>switch(config)# ip access-list acl-01 switch(config-acl)#</pre>	Enters IP ACL configuration mode for the ACL that you specify by name.
Step 3	(Optional) [<i>sequence-number</i>] { permit deny } <i>protocol</i> <i>source destination</i> Example: <pre>switch(config-acl)# 100 permit ip 192.168.2.0/24 any</pre>	Creates a rule in the IP ACL. Using a sequence number allows you to specify a position for the rule in the ACL. Without a sequence number, the rule is added to the end of the rules. The <i>sequence-number</i> argument can be a whole number between 1 and 4294967295. The permit and deny commands support many ways of identifying traffic.
Step 4	(Optional) [no] fragments { permit-all deny-all }	Optimizes fragment handling for noninitial fragments. When

	Command or Action	Purpose
	<p>Example:</p> <pre>switch(config-acl)# fragments permit-all</pre>	<p>a device applies to traffic an ACL that contains the fragments command, the fragments command only matches noninitial fragments that do not match any explicit permit or deny commands in the ACL. The no option removes fragment-handling optimization.</p>
Step 5	<p>(Optional) no {<i>sequence-number</i> {permit deny} <i>protocol source destination</i>}</p> <p>Example:</p> <pre>switch(config-acl)# no 80</pre>	<p>Removes the rule that you specified from the IP ACL. The permit and deny commands support many ways of identifying traffic.</p>
Step 6	<p>(Optional) [no] statistics per-entry</p> <p>Example:</p> <pre>switch(config-acl)# statistics per-entry</pre>	<p>Specifies that the device maintains global statistics for packets that match the rules in the ACL. The no option stops the device from maintaining global statistics for the ACL.</p>
Step 7	<p>(Optional) Enter one of the following commands:</p> <ul style="list-style-type: none"> • show ip access-lists <i>name</i> • show ipv6 access-lists <i>name</i> <p>Example:</p> <pre>switch(config-acl)# show ip access-lists acl-01</pre>	<p>Displays the IP ACL configuration.</p>
Step 8	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config-acl)# copy running-config startup-config</pre>	<p>Copies the running configuration to the startup configuration.</p>

7.6.3 Creating a VTY ACL

You can configure a VTY ACL to control access to all IPv4 or IPv6 traffic over all VTY lines in the ingress or egress direction.

Before you begin

Set identical restrictions on all the virtual terminal lines because a user can connect to any of them.

We recommend that you perform ACL configuration using the Session Manager. This feature allows you to verify ACL configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration, which is especially useful for ACLs that include more than about 1000 rules.

SUMMARY STEPS

1. **configure terminal**
2. **{ip | ipv6} access-list** *name*

3. **{permit | deny}** *protocol source destination* [**log**] [**time-range time**]
4. **exit**
5. **line vty**
6. **{ip | ipv6}** **access-class name** **{in | out}**
7. (Optional) **show {ip | ipv6} access-lists**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	{ip ipv6} access-list name Example: switch(config)# ip access-list vtyacl	Creates an ACL and enters IP access list configuration mode for that ACL. The maximum length for the <i>name</i> argument is 64 characters.
Step 3	{permit deny} protocol source destination [log] [time-range time] Example: switch(config-ip-acl)# permit tcp any any	Creates an ACL rule that permits TCP traffic from and to the specified sources.
Step 4	exit Example: switch(config-ip-acl)# exit switch(config)#	Exits IP access list configuration mode.
Step 5	line vty Example: switch(config)# line vty switch(config-line)#	Specifies the virtual terminal and enters line configuration mode.
Step 6	{ip ipv6} access-class name {in out} Example: switch(config-line)# ip access-class vtyacl out	Restricts incoming or outgoing connections to and from all VTY lines using the specified ACL. The maximum length for the <i>name</i> argument is 64 characters.
Step 7	(Optional) show {ip ipv6} access-lists Example: switch# show ip access-lists	Displays the configured ACLs, including any VTY ACLs.

	Command or Action	Purpose
Step 8	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

7.6.4 Changing Sequence Numbers in an IP ACL

You can change all the sequence numbers assigned to the rules in an IP ACL.

Before you begin

We recommend that you perform ACL configuration using the Session Manager. This feature allows you to verify ACL configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration. This feature is especially useful for ACLs that include more than about 1000 rules.

SUMMARY STEPS

1. **configure terminal**
2. **resequence {ip | ipv6} access-list name starting-sequence-number increment**
3. (Optional) **show ip access-lists name**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	resequence {ip ipv6} access-list name <i>starting-sequence-number increment</i> Example: switch(config)# resequence access-list ip acl-01 100 10	Assigns sequence numbers to the rules contained in the ACL, where the first rule receives the starting sequence number that you specify. Each subsequent rule receives a number larger than the preceding rule. The difference in numbers is determined by the increment that you specify. The <i>starting-sequence-number</i> argument and the <i>increment</i> argument can be a whole number between 1 and 4294967295.
Step 3	(Optional) show ip access-lists name Example: switch(config)# show ip access-lists acl-01	Displays the IP ACL configuration.
Step 4	(Optional) copy running-config startup-config	Copies the running configuration to the startup

	Command or Action	Purpose
	Example: <pre>switch(config)# copy running-config startup-config</pre>	configuration.

7.6.5 Removing an IP ACL

You can remove an IP ACL from the device.

Before you begin

Ensure that you know whether the ACL is applied to an interface. The device allows you to remove ACLs that are currently applied. Removing an ACL does not affect the configuration of interfaces where you have applied the ACL. Instead, the device considers the removed ACL to be empty. Use the **show ip access-lists** command or the **show ipv6 access-lists** command with the summary keyword to find the interfaces that an IP ACL is configured on.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
 - **no ip access-list *name***
 - **no ipv6 access-list *name***
3. (Optional) Enter one of the following commands:
 - **show ip access-lists *name* summary**
 - **show ipv6 access-lists *name* summary**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	Enter one of the following commands: <ul style="list-style-type: none"> • no ip access-list <i>name</i> • no ipv6 access-list <i>name</i> Example: <pre>switch(config)# no ip access-list acl-01</pre>	Removes the IP ACL that you specified by name from the running configuration.
Step 3	(Optional) Enter one of the following commands: <ul style="list-style-type: none"> • show ip access-lists <i>name</i> summary • show ipv6 access-lists <i>name</i> summary Example: <pre>switch(config)# show ip access-lists acl-01</pre>	Displays the IP ACL configuration. If the ACL remains applied to an interface, the command lists the interfaces.

	Command or Action	Purpose
	summary	
Step 4	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

7.6.6 Configuring ACL TCAM Region Sizes

You can change the size of the ACL ternary content addressable memory (TCAM) regions in the hardware.

You can use this procedure for all Inspur CN12900 switches except for NFE2-enabled devices, which must use TCAM templates to configure ACL TCAM region sizes. For more information on using TCAM templates, see "Using Templates to Configure ACL TCAM Region Sizes."

SUMMARY STEPS

1. **configure terminal**
2. [no] **hardware access-list tcam region** *region tcam-size*
3. **copy running-config startup-config**
4. (Optional) **show hardware access-list tcam region**
5. **reload**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	[no] hardware access-list tcam region <i>region tcam-size</i> Example: switch(config)# hardware access-list tcam region mpls 256	Changes the ACL TCAM region size. These are the available regions: <ul style="list-style-type: none"> • cn12900-arp-acl—Configures the rate limit for arp packets entering an interface on their way to the CPU. You will have to set this rate limit per interface to ensure that arp packets conform to the configured rate. • arp-ether—Configures the size of the ARP/Layer 2 Ethertype TCAM region. • copp—Configures the size of the CoPP TCAM region. • e-flow—Configures the size of the egress flow counters TCAM region. • egr-racl—Configures the size of the egress IPv4 or IPv6 router ACL (RACL) TCAM region

	Command or Action	Purpose
		<ul style="list-style-type: none"> • e-ipv6-qos—Configures the size of the IPv6 egress QoS TCAM region. • e-ipv6-racl—Configures the size of the IPv6 egress router ACL (ERACL) TCAM region. • e-mac-qos—Configures the size of the egress MAC QoS TCAM region. • e-qos—Configures the size of the IPv4 egress QoS TCAM region. • e-qos-lite—Configures the size of the IPv4 egress QoS lite TCAM region. • e-racl—Configures the size of the IPv4 egress router ACL (ERACL) TCAM region. • fex-ifacl—Configures the size of the FEX IPv4 port ACL TCAM region. • fex-ipv6-ifacl—Configures the size of the FEX IPv6 port ACL TCAM region. • fex-ipv6-qos—Configures the size of the FEX IPv6 port QoS TCAM region. • fex-mac-ifacl—Configures the size of the FEX MAC port ACL TCAM region. • fex-mac-qos—Configures the size of the FEX MAC port QoS TCAM region. • fex-qos—Configures the size of the FEX IPv4 port QoS TCAM region. • fex-qos-lite—Configures the size of the FEX IPv4 port QoS lite TCAM region. • fhs—Configures the size of the fhs TCAM region. You can configure TCAM for the fhs region on the Inspur CN12900 Series switches. • flow—Configures the size of the ingress flow counters TCAM region. • ifacl—Configures the size of the IPv4 port ACL TCAM region. • ifacl-udf—Configures the size of the IPv4 port ACL user-defined field (UDF) TCAM region • ing-ifacl—Configures the size of the ingress IPv4, IPv6, or MAC port ACL TCAM region • ing-netflow—Configures the size of the NetFlow TCAM region. • ipsg—Configures the size of the IP source guard SMAC-IP binding TCAM region. • ipv6-ifacl—Configures the size of the IPv6 port ACL TCAM region. • ipv6-l3qos—Configures the size of the IPv6 Layer 3 QoS TCAM region. • ipv6-qos—Configures the size of the IPv6 port QoS TCAM region. • ipv6-racl—Configures the size of the IPv6 RACL TCAM region.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • ipv6-vacl—Configures the size of the IPv6 VACL TCAM region. • ipv6-vqos—Configures the size of the IPv6 VLAN QoS TCAM region. • l3qos—Configures the size of the IPv4 Layer 3 QoS TCAM region. • l3qos-lite—Configures the size of the IPv4 Layer 3 QoS lite TCAM region. • mac-ifacl—Configures the size of the MAC port ACL TCAM region. • mac-l3qos—Configures the size of the MAC Layer 3 QoS TCAM region. • mac-qos—Configures the size of the MAC port QoS TCAM region. • mac-vacl—Configures the size of the MAC VACL TCAM region. • mac-vqos—Configures the size of the MAC VLAN QoS TCAM region. • mcast_bidir—Configures the size of the multicast PIM Bidir TCAM region. • mpls—Configures the size of the static MPLS TCAM region. • nat—Configures the size of the network address translation (NAT) TCAM region. • openflow—Configures the size of the OpenFlow TCAM region. • qos—Configures the size of the IPv4 port QoS TCAM region. • qos-lite—Configures the size of the IPv4 port QoS lite TCAM region. • racl—Configures the size of the IPv4 router ACL (RACL) TCAM region. • redirect—Configures the size of the redirect TCAM region. • redirect-tunnel—Configures the size of the redirect-tunnel TCAM region, which is used for BFD over VXLAN. <p>Note This command is supported only if the TP_SERVICES_PKG license is installed.</p> <ul style="list-style-type: none"> • rp-ipv6-qos—Configures the size of the IPv6 port QoS TCAM region for the 100G 9408PC line card and the 100G M4PC generic expansion module (GEM). • rp-mac-qos—Configures the size of the MAC port QoS TCAM region for the 100G 9408PC line card and the 100G M4PC generic expansion module (GEM). • rp-qos—Configures the size of the IPv4 port QoS

	Command or Action	Purpose
		<p>TCAM region for the 100G 9408PC line card and the 100G M4PC generic expansion module (GEM).</p> <ul style="list-style-type: none"> • rp-qos-lite—Configures the size of the IPv4 port QoS lite TCAM region for the 100G 9408PC line card and the 100G M4PC generic expansion module (GEM). • span—Configures the size of the SPAN TCAM region. • svi—Configures the size of the ingress SVI counters TCAM region. • vacl—Configures the size of the IPv4 VACL TCAM region. • vpc-convergence—Configures the size of the vPC convergence TCAM region. • vqos—Configures the size of the IPv4 VLAN QoS TCAM region. • vqos-lite—Configures the size of the IPv4 VLAN QoS lite TCAM region. • <i>tcam-size</i>—TCAM size. The size has to a multiple of 256. If the size is more than 256, it has to be multiple of 512. For FHS, the range is from 0-4096. <p>You can use the no form of this command to revert to the default TCAM region size.</p> <p>Note You can attach IPv4 user-defined fields (UDFs) to the racl, ifacl, and vacl TCAM regions using the hardware access-list tcam region {racl ifacl vacl} qualify udf udf-names command to configure IPv4 UDF-based SPAN or ERSPAN. You can attach IPv6 UDFs to the ing-l2-span-filter and ing-l3-span-filter TCAM regions using the hardware access-list tcam region {ing-ifacl ing-l2-span-filter ing-l3-span-filter} qualify v6udf v6udf-names commands to configure IPv6 UDF-based ERSPAN. For more information and configuration instructions, see the latest <i>Inspur CN12900 INOS-CN System Management Configuration Guide</i>.</p>

	Command or Action	Purpose
Step 3	copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.
Step 4	(Optional) show hardware access-list tcam region Example: switch(config)# show hardware access-list tcam region	Displays the TCAM sizes that will be applicable on the next reload of the device.
Step 5	reload Example: switch(config)# reload	Reloads the device. Note The new size values are effective only after you enter copy running-config startup-config + reload or reload all line card modules.

Example

The following example shows how to change the size of the cn12900-arp-acl TCAM region on a Inspur INOS-CN NFE-enabled device:

```
switch(config)#hardware access-list tcam region cn12900-arp-acl
256switch(config)#copy r s switch(config)# reload
Configuring storm-control-cpu:
switch (config)# interface ethernet 1/10switch switch
(config-if)# storm-control-cpu arp rate 150
switch (config)# show access-list storm-control-cpu arp-stats interface ethernet 1/10
slot 1
```

The following example shows how to change the size of the RAACL TCAM region on a Inspur CN12900 Series switch:

```
switch(config)# hardware access-list tcam region racl 256
[SUCCESS] New tcam size will be applicable only at boot
time. You need to 'copy run start' and 'reload'
switch(config)# copy running-config startup-
config switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

This example shows how to display the TCAM region sizes to verify your changes:

```
switch(config)# show hardware access-list tcam region
*****WARNING*****
*****The output shows NFE tcam region info*****
***Please refer to 'show hardware access-list tcam template' for NFE2***
*****
IPV4 PACL [ifacl] size = 1024
IPV6 PACL [ipv6-ifacl] size = 1024
MAC PACL [mac-ifacl] size = 1952
IPV4 Port QoS [qos] size = 640
```

```

IPV6 Port QoS [ipv6-qos] size = 256
MAC Port QoS [mac-qos] size = 0
FEX IPV4 PACL [fex-ifacl] size = 0
FEX IPV6 PACL [fex-ipv6-ifacl] size = 0
FEX MAC PACL [fex-mac-ifacl] size = 0
FEX IPV4 Port QoS [fex-qos] size = 0
FEX IPV6 Port QoS [fex-ipv6-qos] size = 0
FEX MAC Port QoS [fex-mac-qos] size = 0
IPV4 VACL [vacl] size = 0
IPV6 VACL [ipv6-vacl] size = 0
MAC VACL [mac-vacl] size = 0
IPV4 VLAN QoS [vqos] size = 0
IPV6 VLAN QoS [ipv6-vqos] size = 0
MAC VLAN QoS [mac-vqos] size = 0
IPV4 RACL [racl] size = 2048
IPV6 RACL [ipv6-racl] size = 1024
IPV4 Port QoS Lite [qos-lite] size = 0
FEX IPV4 Port QoS Lite [fex-qos-lite] size = 0
IPV4 VLAN QoS Lite [vqos-lite] size = 0
IPV4 L3 QoS Lite [l3qos-lite] size = 0
Egress IPV4 QoS [e-qos] size = 0
Egress IPV6 QoS [e-ipv6-qos] size = 0
Egress MAC QoS [e-mac-qos] size = 0
Egress IPV4 VACL [vacl] size = 0
Egress IPV6 VACL [ipv6-vacl] size = 0
Egress MAC VACL [mac-vacl] size = 0
Egress IPV4 RACL [e-racl] size = 0
Egress IPV6 RACL [e-ipv6-racl] size = 0
Egress IPV4 QoS Lite [e-qos-lite] size = 0
IPV4 L3 QoS [l3qos] size = 640
IPV6 L3 QoS [ipv6-l3qos] size = 256
MAC L3 QoS [mac-l3qos] size = 0
Ingress System size = 0
Egress System size = 0
SPAN [span] size = 96
Ingress COPP [copp] size = 128
Ingress Flow Counters [flow] size = 0
Egress Flow Counters [e-flow] size = 0
Ingress SVI Counters [svi] size = 0
Redirect [redirect] size = 0
VPC Convergence/ES-Multi Home [vpc-convergence] size = 0
IPSG SMAC-IP bind table [ipsrg] size = 0
Ingress ARP-Ether ACL [arp-ether] size = 0
ranger+ IPV4 QoS Lite [rp-qos-lite] size = 0
ranger+ IPV4 QoS [rp-qos] size = 0
ranger+ IPV6 QoS [rp-ipv6-qos] size = 0
ranger+ MAC QoS [rp-mac-qos] size = 0
NAT ACL[nat] size = 0
Mpls ACL size = 0
MOD RSVD size = 0
sFlow ACL [sflow] size = 0
mcast bidir ACL [mcast_bidir] size = 0
Openflow size = 0
Openflow Lite [openflow-lite] size = 0
Ingress FCoE Counters [fcoe-ingress] size = 0
Egress FCoE Counters [fcoe-egress] size = 0
Redirect-Tunnel [redirect-tunnel] size = 0
SPAN+sFlow ACL [span-sflow] size = 0
Openflow IPv6 [openflow-ipv6] size = 0
mcast performance ACL [mcast-performance] size = 0
Mpls Double Width ACL size = 0
CN12900 ARP ACL [cn12900-arp-acl] size = 0
CN6K V6 Span size = 0
CN6K V6 L2 Span size = 0
Ingress Span size = 0
Redirect v4 size = 2048
Redirect v6 size = 2048
Fretta Nbm size = 0

```

```
TCP NAT ACL[tcp-nat] size = 0
vxlan p2p ACL [vxlan-p2p] size = 0
Vxlan Feature size = 0
switch(config)#
```

This example shows how to revert to the default RACL TCAM region size:

```
switch(config)# no hardware profile tcam region racl 512

[SUCCESS] New tcam size will be applicable only at boot
time. You need to 'copy run start' and 'reload'
switch(config)# copy running-config startup-
config switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

7.6.7 Using Templates to Configure ACL TCAM Region Sizes

You can use create and apply custom templates to configure ACL TCAM region sizes.

You can use this procedure to configure ACL TCAM region sizes. However, NFE2-enabled devices (such as the CN12908-FM-R fabric module) do not support the **hardware access-list tcam region** command and must use a template to configure the ACL TCAM region size.

SUMMARY STEPS

1. **configure terminal**
 2. **[no] hardware profile tcam resource template *template-name* ref-template {nfe | nfe2 | {I2-I3 | I3}}**
 3. (Optional) *region tcam-size*
 4. **exit**
 5. **[no] hardware profile tcam resource service-template *template-name***
 6. (Optional) **show hardware access-list tcam template {all | nfe | nfe2 | I2-I3 | I3 | *template-name*}**
 7. (Optional) **copy running-config startup-config**
 8. **reload**
-
2. **[no] hardware profile tcam resource template *template-name* ref-template {nfe | nfe2 | {I2-I3 | I3}}**
 3. (Optional) *region tcam-size*
 4. **exit**
 5. **[no] hardware profile tcam resource service-template *template-name***
 6. (Optional) **show hardware access-list tcam template {all | nfe | nfe2 | I2-I3 | I3 | *template-name*}**
 7. (Optional) **copy running-config startup-config**
 8. **reload**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	Required: [no] hardware profile tcam resource template <i>template-name</i> ref-template {nfe nfe2 {I2-I3 I3}}	Creates a template for configuring ACL TCAM region sizes. nfe —The default TCAM template for Network Forwarding

	Command or Action	Purpose
Step 3	<p>Example: (Optional) <i>region tcam-size</i></p> <p>Example:</p> <pre>switch(config-tcam-temp)# mpls 256</pre>	Engine (NFE)-enabled Inspur CN12900 Series. Adds any desired TCAM regions and their sizes to the template. Enter this command for each region you want to add to the template.
Step 4	<p>Required: exit</p> <p>Example:</p> <pre>switch(config-tcam-temp)# exit switch(config#)</pre>	Exits the TCAM template configuration mode.
Step 5	<p>Required: [no] hardware profile tcam resource</p> <p>service-template <i>template-name</i></p> <p>Example:</p> <pre>switch(config)# hardware profile tcam resource service-template SR_MPLS_CARVE</pre>	Applies the custom template to all line cards and fabric modules.
Step 6	<p>(Optional) show hardware access-list tcam template {all nfe nfe2 I2-I3 I3 <i>template-name</i>}</p> <p>Example:</p> <pre>switch(config)# show hardware access-list tcam template SR_MPLS_CARVE</pre>	Displays the configuration for all TCAM templates or for a specific template.
Step 7	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.
Step 8	<p>reload</p> <p>Example:</p> <pre>switch(config)# reload</pre>	<p>Reloads the device.</p> <p>Note The configuration is effective only after you enter copy running-config startup-config + reload.</p>

7.6.8 Configuring TCAM Carving

The default TCAM region configuration varies by platform and does not accommodate all TCAM regions. To enable any desired regions, you must decrease the TCAM size of one region and then increase the TCAM size for the desired region.

The following tables list the default sizes for the ingress and egress TCAM regions on different platforms.

Table 13: Default TCAM Region Configuration (Ingress) - For Inspur CN12900 Series Switches

Region Name	Size	Width	Total Size
IPv4 RACL	1536	1	1536
IPv4 Layer 3 QoS	256	2	512
SPAN	256	1	256
CoPP	256	2	512
System	256	2	512
Redirect	256	1	256
vPC convergence	512	1	512
			4K

Table 14: Default TCAM Region Configuration (Egress) - For Inspur CN12900 Series Switches

Region Name	Size	Width	Total Size
IPv4 RACL	768	1	768
System	256	1	256
			1K

The following example sets the IPv6 RACL TCAM size to 256 on a Inspur CN12900 Series switch. An IPv6 RACL of size 256 takes 512 entries because IPv6 is double wide.

To set the size of the ingress IPv6 RACL TCAM region on a Inspur CN12900 Series switch, perform one of two options.

Option #1

Reduce the ingress IPv4 RACL by 512 entries (1536 - 512 = 1024) and add an ingress IPv6 RACL with 512 entries—This option is preferred.

```
switch(config)# hardware access-list tcam region racl 1024
Warning: Please reload the linecard for the configuration to take effect
switch(config)# hardware access-list tcam region ipv6-racl 256
Warning: Please reload the linecard for the configuration to take effect
```

Table 15: Updated TCAM Region Configuration After Reducing the IPv4 RACL (Ingress)

Region Name	Size	Width	Total Size
IPv4 RACL	1024	1	1024
IPv6 RACL	256	2	512
IPv4 Layer 3 QoS	256	2	512
SPAN	256	1	256
CoPP	256	2	512
System	256	2	512

Redirect	256	1	256
vPC convergence	512	1	512
			4K

Option #2

Remove IPv4 Layer 3 QoS by reducing its size to 0 and add an ingress IPv6 RACL—This option is available if you are not using IPv4 Layer 3 QoS.

```
switch(config)# hardware access-list tcam region l3qos 0
Warning: Please reload the linecard for the configuration to take effect
switch(config)# hardware access-list tcam region ipv6-racl 256
Warning: Please reload the linecard for the configuration to take effect
```

Table 16: Updated TCAM Region Configuration After Removing Layer 3 QoS (Ingress)

Region Name	Size	Width	Total Size
IPv4 RACL	1536	1	1536
IPv6 RACL	256	2	512
IPv4 Layer 3 QoS	0	2	0
SPAN	256	1	256
CoPP	256	2	512
System	256	2	512
Redirect	256	1	256
vPC convergence	512	1	512
			4K

To enable an egress IPv6 RACL of size 256, reduce the egress IPv4 RACL to 256 and add the egress IPv6 RACL:

```
switch(config)# hardware access-list tcam region e-racl 256
Warning: Please reload the linecard for the configuration to take effect
switch(config)# hardware access-list tcam region e-ipv6-racl 256
Warning: Please reload the linecard for the configuration to take effect
```

Table 17: Default TCAM Region Configuration After Reducing the IPv4 RACL (Egress)

Region Name	Size	Width	Total Size
IPv4 RACL	256	1	256
IPv6 RACL	256	2	512
System	256	1	256
			1K

After you adjust the TCAM region sizes, enter the **show hardware access-list tcam region** command to display

the TCAM sizes that will be applicable on the next reload of the device.

Attention	To keep all modules synchronized, you must reload all line card modules or enter copy running-config startup-config + reload to reload the device. Multiple TCAM region configurations require only a single reload. You can wait until you complete all of your TCAM region configurations before you reload the device.
------------------	--

Depending on the configuration, you might exceed the TCAM size or run out of slices.

If you exceed the 4K ingress limit for all TCAM regions when you configure a TCAM region, the following message appears:

```
ERROR: Aggregate TCAM region configuration exceeded the available Ingress TCAM space.
Please re-configure.
```

If you exceed the number of slices, the following message appears:

```
ERROR: Aggregate TCAM region configuration exceeded the available Ingress TCAM
slices. Please re-configure.
```

If you exceed the 1K egress limit for all TCAM regions when you configure a TCAM region, the following message appears:

```
ERROR: Aggregate TCAM region configuration exceeded the available Egress TCAM space.
Please re-configure.
```

If TCAM for a particular feature is not configured and you try to apply a feature that requires TCAM carving, the following message appears:

```
ERROR: Module x returned status: TCAM region is not configured. Please configure
TCAM region and retry the command.
```

7.6.9 Configuring UDF-Based Port ACLs

You can configure UDF-based port ACLs for Inspur CN12900 switches. This feature enables the device to match on user-defined fields (UDFs) and to apply the matching packets to an IPv4 port ACL.

SUMMARY STEPS

1. **configure terminal**
2. **udf *udf-name offset-base offset length***
3. **hardware access-list tcam region ing-ifacl qualify {udf *udf-name* | v6udf *v6udf-name*}**
4. **copy running-config startup-config**
5. **reload**
6. **ip access-list *udf-acl***
7. Enter one of the following commands:
 - **permit udf *udf-name value mask***
 - **permit ip *source destination udf udf-name value mask***
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	udf udf-name offset-base offset length Example: <pre>switch(config)# udf pkttoff10 packet-start 10 2</pre> Example: <pre>switch(config)# udf pkttoff10 header outer 13 20 2</pre>	<p>Defines the UDF as follows:</p> <ul style="list-style-type: none"> • <i>udf-name</i>—Specifies the name of the UDF. You can enter up to 16 alphanumeric characters for the name. • <i>offset-base</i>—Specifies the UDF offset base as follows, where header is the packet header to consider for the offset: {packet-start header {outer inner {13 14}}} • <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. • <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. <p>You can define multiple UDFs, but Inspur recommends defining only required UDFs.</p>
Step 3	hardware access-list tcam region ing-ifacl qualify {udf udf-name v6udf v6udf-name} Example: <pre>switch(config)# hardware access-list tcam region</pre>	<p>Attaches the UDFs to the ing-ifacl TCAM region, which applies to IPv4 or IPv6 port ACLs. The number of UDFs that can be attached to a TCAM region varies by platform. You can attach up to 2 UDFs for Inspur.</p> <p>Note 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</p>

	Command or Action	Purpose
		<p>command.</p> <p>Note The no form of this command detaches the UDFs from the TCAM region and returns the region to single wide.</p>
Step 4	<p>Required: copy running-config startup-config</p> <p>Example:</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.
Step 5	<p>Required: reload</p> <p>Example:</p> <pre>switch(config)# reload</pre>	<p>Reloads the device.</p> <p>Note Your UDF configuration is effective only after you enter copy running-config startup-config + reload.</p>
Step 6	<p>ip access-list <i>udf-acl</i></p> <p>Example:</p> <pre>switch(config)# ip access-list udfacl switch(config-acl)#</pre>	Creates an IPv4 access control list (ACL) and enters IP access list configuration mode.
Step 7	<p>Enter one of the following commands:</p> <ul style="list-style-type: none"> • permit udf <i>udf-name value mask</i> • permit ip <i>source destination udf udf-name value mask</i> <p>Example:</p> <pre>switch(config-acl)# permit udf pkttofff10 0x1234 0xffff</pre> <p>Example:</p> <pre>switch(config-acl)# permit ip any any udf pkttofff10 0x1234 0xffff</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). The range for the <i>value</i> and <i>mask</i> arguments is from 0x0 to 0xffff.</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>
Step 8	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

7.6.10 Applying an IP ACL as a Router ACL

You can apply an IPv4 or IPv6 ACL to any of the following types of interfaces:

- Physical Layer 3 interfaces and subinterfaces
- Layer 3 Ethernet port-channel interfaces
- VLAN interfaces
- Management interfaces

ACLs applied to these interface types are considered router ACLs.

Before you begin

Ensure that the ACL you want to apply exists and that it is configured to filter traffic in the manner that you need for this application.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
 - **interface ethernet** *slot/port* [. *number*]
 - **interface port-channel** *channel-number*
 - **interface vlan** *vlan-id*
 - **interface mgmt** *port*
3. Enter one of the following commands:
 - **ip access-group** *access-list* {**in** | **out**}
 - **ipv6 traffic-filter** *access-list* {**in** | **out**}
4. (Optional) **show running-config aclmgr**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	Enter one of the following commands: <ul style="list-style-type: none"> • interface ethernet <i>slot/port</i> [. <i>number</i>] • interface port-channel <i>channel-number</i> • interface vlan <i>vlan-id</i> • interface mgmt <i>port</i> Example: <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>	Enters configuration mode for the interface type that you specified.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • ip access-group <i>access-list</i> {in out} • ipv6 traffic-filter <i>access-list</i> {in out} 	Applies an IPv4 or IPv6 ACL to the Layer 3 interface for traffic flowing in the direction specified. You can apply one router ACL per direction.

	Command or Action	Purpose
	Example: <pre>switch(config-if)# ip access-group acl1 in</pre>	
Step 4	(Optional) show running-config aclmgr Example: <pre>switch(config-if)# show running-config aclmgr</pre>	Displays the ACL configuration.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

7.6.11 Applying an IP ACL as a Port ACL

You can apply an IPv4 or IPv6 ACL to a Layer 2 interface, which can be a physical port or a port channel. ACLs applied to these interface types are considered port ACLs.

Before you begin

Ensure that the ACL you want to apply exists and that it is configured to filter traffic in the manner that you need for this application.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
 - **interface ethernet** *slot/port*
 - **interface port-channel** *channel-number*
3. Enter one of the following commands:
 - **ip port access-group** *access-list in*
 - **ipv6 port traffic-filter** *access-list in*
4. (Optional) **show running-config aclmgr**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	Enter one of the following commands: <ul style="list-style-type: none"> • interface ethernet <i>slot/port</i> • interface port-channel <i>channel-number</i> Example: <pre>switch(config)# interface ethernet 2/3</pre>	Enters configuration mode for the interface type that you specified.

	Command or Action	Purpose
	<code>switch(config-if)#</code>	
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • ip port access-group <i>access-list</i> in • ipv6 port traffic-filter <i>access-list</i> in Example: <pre>switch(config-if)# ip port access-group acl-12-marketing-group in</pre>	Applies an IPv4 or IPv6 ACL to the interface or port channel. Only inbound filtering is supported with port ACLs. You can apply one port ACL to an interface.
Step 4	(Optional) show running-config aclmgr Example: <pre>switch(config-if)# show running-config aclmgr</pre>	Displays the ACL configuration.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

7.6.12 Applying an IP ACL as a VACL

You can apply an IP ACL as a VACL.

7.6.13 Configuring IPv4 ACL Logging

To configure the IPv4 ACL logging process, you first create the access list, then enable filtering of IPv4 traffic on an interface using the specified ACL, and finally configure the ACL logging process parameters.

SUMMARY STEPS

1. **configure terminal**
2. **ip access-list** *name*
3. **{permit | deny} ip** *source-address destination-address* **log**
4. **exit**
5. **interface ethernet** *slot/port*
6. **ip access-group** *name* **in**
7. **exit**
8. **logging ip access-list cache interval** *interval*
9. **logging ip access-list cache entries** *number-of-flows*
10. **logging ip access-list cache threshold** *threshold*
11. **logging ip access-list detailed**
12. **hardware rate-limiter access-list-log** *packets*
13. **aclog match-log-level** *severity-level*
14. (Optional) **show logging ip access-list cache** [**detail**]

DETAILED STEPS

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

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	ip access-list <i>name</i> Example: <pre>switch(config)# ip access-list logging-test switch(config-acl)#</pre>	Creates an IPv4 ACL and enters IP ACL configuration mode. The <i>name</i> argument can be up to 64 characters.
Step 3	{permit deny} ip <i>source-address destination-address</i> log Example: <pre>switch(config-acl)# permit ip any 10.30.30.0/24 log</pre>	Creates an ACL rule that permits or denies IPv4 traffic matching its conditions. To enable the system to generate an informational logging message about each packet that matches the rule, you must include the log keyword. The <i>source-address</i> and <i>destination-address</i> arguments can be the IP address with a network wildcard, the IP address and variable-length subnet mask, the host address, or any to designate any address.
Step 4	exit Example: <pre>switch(config-acl)# exit switch(config)#</pre>	Updates the configuration and exits IP ACL configuration mode.
Step 5	interface ethernet <i>slot/port</i> Example: <pre>switch(config)# interface ethernet 1/1 switch(config-if)#</pre>	Enters interface configuration mode.
Step 6	ip access-group <i>name</i> in Example: <pre>switch(config-if)# ip access-group logging- test in</pre>	Enables the filtering of IPv4 traffic on an interface using the specified ACL. You can apply an ACL to inbound traffic.
Step 7	exit	Updates the configuration and exits interface configuration

	Command or Action	Purpose
	Example: <pre>switch(config-if)# exit switch(config)#</pre>	mode.
Step 8	logging ip access-list cache interval <i>interval</i> Example: <pre>switch(config)# logging ip access-list cache interval 490</pre>	Configures the log-update interval (in seconds) for the ACL logging process. The default value is 300 seconds. The range is from 5 to 86400 seconds.
Step 9	logging ip access-list cache entries <i>number-of-flows</i> Example: <pre>switch(config)# logging ip access-list cache entries 8001</pre>	Specifies the maximum number of flows to be monitored by the ACL logging process. The default value is 8000. The range of values supported is from 0 to 1048576.
Step 10	logging ip access-list cache threshold <i>threshold</i> Example: <pre>switch(config)# logging ip access-list cache threshold 490</pre>	If the specified number of packets is logged before the expiry of the alert interval, the system generates a syslog message.
Step 11	logging ip access-list detailed Example: <pre>switch(config)# logging ip access-list detailed</pre>	Enables the following information to be displayed in the output of the show logging ip access-list cache command: the access control entry (ACE) sequence number, ACE action, ACL name, ACL direction, ACL filter type, and ACL applied interface.
Step 12	hardware rate-limiter access-list-log <i>packets</i> Example: <pre>switch(config)# hardware rate-limiter access-list-log 200</pre>	Configures rate limits in packets per second for packets copied to the supervisor module for ACL logging. The range is from 0 to 30000.
Step 13	aclog match-log-level <i>severity-level</i> Example: <pre>switch(config)# aclog match-log-level 5</pre>	Specifies the minimum severity level to log ACL matches. The default is 6 (informational). The range is from 0 (emergency) to 7 (debugging).

	Command or Action	Purpose
Step 14	(Optional) show logging ip access-list cache [detail] Example: <pre>switch(config)# show logging ip access-list cache</pre>	Displays information on the active logged flows, such as source IP and destination IP addresses, source port and destination port information, source interfaces, and so on. If you entered the logging ip access-list detailed command, the output also includes the following information: the access control entry (ACE) sequence number, ACE action, ACL name, ACL direction, ACL filter type, and ACL applied interface.

7.6.14 Configuring ACLs Using HTTP Methods to Redirect Requests

You can configure ACLs to intercept and redirect specific HTTP methods to a server that is connected to a specific port.

The following HTTP methods can be redirected:

- connect
- delete
- get
- head
- post
- put
- trace

Before you begin

Enable the double-wide TCAM for the IFACL region using the **hardware access-list tcam region ifacl 512 double-wide** command. This command applies to the global configuration. Reload the switch for this configuration to take into effect.

SUMMARY STEPS

1. **configure terminal**
2. **ip access-list name**
3. **[sequence-number] permit protocol source destination http-method method [tcp-option-length length] [redirect interface]**
4. (Optional) **show ip access-lists name**
5. (Optional) **show run interface interface slot/port**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	<p>ip access-list <i>name</i></p> <p>Example:</p> <pre>switch(config)# ip access-list acl-01 switch(config-acl)#</pre>	<p>Creates the IP ACL and enters IP ACL configuration mode.</p> <p>The <i>name</i> argument can be up to 64 characters.</p>
Step 3	<p>[<i>sequence-number</i>] permit <i>protocol source destination</i></p> <p>http-method <i>method</i> [tcp-option-length <i>length</i>]</p> <p>[redirect <i>interface</i>]</p> <p>Example:</p> <pre>switch(config-acl)# permit tcp 1.1.1.1/32 any http-method get</pre>	<p>Configures the ACL to redirect specific HTTP methods to a server.</p> <p>The following HTTP methods are supported:</p> <ul style="list-style-type: none"> • connect—Matches HTTP packets with the CONNECT method [0x434f4e4e] • delete—Matches HTTP packets with the DELETE method [0x44454c45] • get—Matches HTTP packets with the GET method [0x47455420] • head—Matches HTTP packets with the HEAD method [0x48454144] • post—Matches HTTP packets with the POST method [0x504f5354] • put—Matches HTTP packets with the PUT method [0x50555420] • trace—Matches HTTP packets with the TRACE method [0x54524143] <p>The tcp-option-length option specifies the length of the TCP options header in the packets. You can configure up to four TCP option lengths (in multiples of four bytes) in the access control entries (ACEs). The <i>length</i> range is from 0 to 40. If you do not configure this option, the length is specified as 0, and only packets without the TCP options header can match the ACE. This option allows the HTTP method to be matched even on packets that have a variable-length TCP options header.</p> <p>The redirect option redirects an HTTP method to a</p>

	Command or Action	Purpose
		server that is connected to a specific port. The HTTP redirect feature does not work on Layer 3 ports.
Step 4	(Optional) show ip access-lists <i>name</i> Example: switch(config-acl)# show ip access-lists acl-01	Displays the IP ACL configuration.
Step 5	(Optional) show run interface <i>interface slot/port</i> Example: switch(config-acl)# show run interface ethernet 2/2	Displays the interface configuration.

Example

The following example specifies a length for the TCP options header in the packets and redirects the post HTTP method to a server that is connected to port channel 4001:

```
switch(config)# ip access-list http-redirect-acl
switch(config-acl)# 10 permit tcp any any http-method get tcp-option-length 4 redirect
port-channel4001

switch(config-acl)# 20 permit tcp any any http-method post redirect port-channel4001
switch(config-acl)# statistics per-entry
switch(config)# interface Ethernet 1/33
switch(config-if)# ip port access-group http-redirect-acl in
```

7.7 Verifying the IP ACL Configuration

To display IP ACL configuration information, perform one of the following tasks.

Command	Purpose
show hardware access-list tcam region	Displays the TCAM sizes that will be applicable on the next reload of the device.
show hardware access-list tcam template {all nfe nfe2 I2-I3 I3 <i>template-name</i> }	Displays the configuration for all TCAM templates or for a specific template. nfe —The default TCAM template for Network Forwarding Engine (NFE)-enabled Inspur CN12900 series switches.
show ip access-lists	Displays the IPv4 ACL configuration.

Command	Purpose
show ipv6 access-lists	Displays the IPv6 ACL configuration.
show logging ip access-list cache [detail]	Displays information on the active logged flows, such as source IP and destination IP addresses, source port and destination port information, and source interfaces. If you entered the logging ip access-list detailed command, the output also includes the following information: the access control entry (ACE) sequence number, ACE action, ACL name, ACL direction, ACL filter type, and ACL applied interface.
show logging ip access-list status	Displays the deny maximum flow count, the current effective log interval, and the current effective threshold value.
show running-config acllog	Displays the ACL log running configuration.
show running-config aclmgr [all]	Displays the ACL running configuration, including the IP ACL configuration and the interfaces to which IP ACLs are applied. Note This command displays the user-configured ACLs in the running configuration. The all option displays both the default (CoPP-configured) and user-configured ACLs in the running configuration.
show startup-config acllog	Displays the ACL log startup configuration.
show startup-config aclmgr [all]	Displays the ACL startup configuration. Note This command displays the user-configured ACLs in the startup

Command	Purpose
	configuration. The all option displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration.

7.8 Monitoring and Clearing IP ACL Statistics

To monitor or clear IP ACL statistics, use one of the commands in this table.

Command	Purpose
show ip access-lists	Displays the IPv4 ACL configuration. If the IPv4 ACL includes the statistics per-entry command, the show ip access-lists command output includes the number of packets that have matched each rule.
show ipv6 access-lists	Displays IPv6 ACL configuration. If the IPv6 ACL includes the statistics per-entry command, then the show ipv6 access-lists command output includes the number of packets that have matched each rule.
clear ip access-list counters	Clears statistics for all IPv4 ACLs or for a specific IPv4 ACL.
clear ipv6 access-list counters	Clears statistics for all IPv6 ACLs or for a specific IPv6 ACL.

7.9 Configuration Examples for IP ACLs

The following example shows how to create an IPv4 ACL named `acl-01` and apply it as a port ACL to Ethernet interface `2/1`, which is a Layer 2 interface:

```
ip access-list acl-01
  permit ip
  192.168.2.0/24 any
interface ethernet 2/1
  ip port access-group acl-01 in
```

The following example shows how to create an IPv6 ACL named `acl-120` and apply it as a router ACL to Ethernet interface `2/3`, which is a Layer 3 interface:

```
ipv6 access-list acl-120
  permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
interface ethernet 2/3
  ipv6 traffic-filter acl-120 in
```

The following example shows how to create a VTY ACL named `single-source` and apply it on input IP traffic

over the VTY line. This ACL allows all TCP traffic through and drops all other IP traffic:

```
ip access-list single-source
 permit tcp 192.168.7.5/24
 any exit
 line vty
 ip access-class single-source
 in show ip access-lists
```

The following example shows how to configure IPv4 ACL logging:

```
switch# configure terminal
Enter configuration commands, one per line. End with
CNTL/Z. switch(config)# ip access-list logging-test
switch(config-acl)# permit ip any 2001:DB8:1::1/64 log
switch(config-acl)# exit
switch(config)# interface ethernet 1/1
switch(config-if)# ip access-group logging-test
in switch(config-if)# exit
switch(config)# logging ip access-list cache interval 400
switch(config)# logging ip access-list cache entries 100
switch(config)# logging ip access-list cache threshold
900 switch(config)# hardware rate-limiter access-list-log
200 switch(config)# acllog match-log-level 5
```

The following example shows how to configure a UDF-based port ACL:

7.10 About System ACLs

```
switch# configure terminal
switch(config)# hardware access-list tcam region ing-ifacl 256
switch(config)# udf pktoff10 packet-start 10 2
switch(config)# udf pktoff20 packet-start 10 1
switch(config)# hardware access-list tcam region ing-ifacl qualify udf pktoff10 pktoff20
switch# configure terminal switch(config)#
ip access-list udfacl switch(config-acl)#
statistics per-entry
switch(config-acl)# 10 permit ip any any udf pktoff10 0x1234 0xffff
switch# configure terminal
switch(config)# interface Ethernet1/1
switch(config-if)# ip port access-group udfacl
in switch(config-if)# switchport
switch(config-if)# no shutdown
```

7.11 About System ACLs

You can configure system ACLs on Inspur CN12900 switches with -R line cards. With system ACLs, you can now configure a Layer 2 port ACL (PACL) on all the ports with the same access-list in the switch. Configuring system ACLs reduces the TCAM usage and also brings down the time and memory usage while the policy is being applied or modified.

See the following guidelines and limitations for configuring system ACLs:

- The system PACL is supported for Layer 2 interface only.
- Up to 10K ACEs are supported with all other basic features for the switch to come up on Inspur CN12900 switches with -R line cards. The hardware capacity on Inspur CN12900 switches with -R line cards is 64K ACEs.
- Configuring IPv4 PACL TCAM region (ifacl) with anything more than the total physical TCAM capacity of -R line cards of 12k will result in power down of -R line cards only.
- ACE statistics are not yet supported for the system ACLs.
- IPv6 is not yet supported in the system ACLs.
- System ACLs are not supported on the breakout port.
- The non-atomic update either drops or permits all the traffic. By default, the non-atomic update drops all the traffic until the ACL update completes. The non-atomic ACL update behavior can be controlled using the **hardware access-list update default-result permit** CLI command. This CLI works only for physical ports. See the following example:

```
hardware access-list update default-result permit    => #Allows all the traffic during
ACL updates. There may be < 10secs traffic drop.    => #This is the default behavior.
no hardware access-list update default-result permit
It denies all the traffic during ACL updates.
```

- The atomic ACL update is not supported on Inspur -R series line cards, but the non-atomic update **hardware access-list update default-result** is supported on Inspur eries line cards.

7.11.1 Carving a TCAM Region

Before configuring the system ACLs, carve the TCAM region first. Note that for configuring the ACLs less than 1k, you do not need to carve the TCAM region.

7.11.2 Configuring System ACLs

After an IPv4 ACL is created, configure the system ACL.

Before you begin

Create an IPv4 ACL on the device.

SUMMARY STEPS

1. **config t**
2. **system acl**
3. **ip port access-group <pacl name> in**

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t	Enters the configuration mode.
Step 2	system acl	Configures the system ACL.
Step 3	ip port access-group <pacl name> in	Applies a Layer 2 PACL to the interface. Only inbound filtering is supported with port ACLs. You can apply one port ACL to an interface.

7.11.3 Configuration and Show Command Examples for the System ACLs

See the following configuration examples for the system ACL show commands.

Configuring system PACL with 1K scale [using default TCAM]

See the following example for configuring system PACL with 1K scale [Using default TCAM].

Step 1: Create PACL.

```

config t
ip access-list PACL-DNA
 10 permit ip 1.1.1.1/32 any
 20 permit tcp 3.0.0.0/8 255.0.0.0 eq 1500
 25 deny udp any any eq 500
 26 deny tcp any any eq
 490 any .... ...
 1000 deny any any

```

Step 2: Apply PACL into system level.

```

configuration
terminal system
acl
  ip port access-group PACL-DNA in

```

To validate the system ACLs that are configured on the switch, use the **sh run aclmgr | sec system** command:

```

switch# sh run aclmgr | sec
system system acl
  ip port access-group
test in switch#

```

To validate the PACLs that are configured on the switch, use the **sh ip access-lists <name> [summary]** command:

```

switch# sh ip access-lists test
IP access list test

 10 deny udp any any eq 27
 20 permit ip 1.1.1.1/32 100.100.100.100/32
 30 permit ip 1.2.1.1/32 100.100.100.100/32
 40 permit ip 1.3.1.1/32 100.100.100.100/32
 50 permit ip 1.4.1.1/32 100.100.100.100/32
 60 permit ip 1.5.1.1/32 100.100.100.100/32
 70 permit ip 1.6.1.1/32 100.100.100.100/32
 80 permit ip 1.7.1.1/32 100.100.100.100/32
 90 permit ip 1.8.1.1/32 100.100.100.100/32

switch# sh ip access-lists test summary

IPV4 ACL test
Total ACEs Configured: 12279
Configured on interfaces:
Active on interfaces:
  - ingress
  - ingress

```



```
switch#
```

To validate PACL IPv4 (ifacl) TCAM region size, use the **show hardware access-list tcam region** command:

```
switch# show hardware access-list tcam region
*****WARNING*****
*****The output shows NFE tcam region info*****
*****Please refer to 'show hardware access-list tcam template' for NFE2*****
*****
          IPV4 PACL [ifacl] size = 12280
          IPV6 PACL [ipv6-ifacl] size = 0
          MAC PACL [mac-ifacl] size = 0
          IPV4 Port QoS [qos] size = 640
          IPV6 Port QoS [ipv6-qos] size = 256
          MAC Port QoS [mac-qos] size = 0
          FEX IPV4 PACL [fex-ifacl] size = 0
          FEX IPV6 PACL [fex-ipv6-ifacl] size = 0
          FEX MAC PACL [fex-mac-ifacl] size = 0
          FEX IPV4 Port QoS [fex-qos] size = 0
          FEX IPV6 Port QoS [fex-ipv6-qos] size = 0
          FEX MAC Port QoS [fex-mac-qos] size = 0
          IPV6 IPV4 VACL [vacl] size = 0
          VACL [ipv6-vacl] size = 0
          MAC VACL [mac-vacl] size = 0
          IPV4 VLAN QoS [vqos] size = 0
          IPV6 VLAN QoS [ipv6-vqos] size = 0
          MAC VLAN QoS [mac-vqos] size = 0
          IPV6 IPV4 RACL [racl] size = 0
          RACL [ipv6-racl] size = 128
          IPV4 Port QoS Lite [qos-lite] size = 0
          FEX IPV4 Port QoS Lite [fex-qos-lite] size = 0
          IPV4 VLAN QoS Lite [vqos-lite] size = 0
          IPV4 L3 QoS Lite [l3qos-lite] size = 0
          Egress IPV4 QoS [e-qos] size = 0
          Egress IPV6 QoS [e-ipv6-qos] size = 0
          Egress MAC QoS [e-mac-qos] size = 0
          Egress IPV4 VACL [vacl] size = 0
          Egress IPV6 VACL [ipv6-vacl] size = 0
          Egress MAC VACL [mac-vacl] size = 0
          Egress IPV4 RACL [e-racl] size = 0
          Egress IPV6 RACL [e-ipv6-racl] size = 0

          Egress IPV4 QoS Lite [e-qos-lite] size = 0
          IPV4 L3 QoS [l3qos] size = 640
          IPV6 L3 QoS [ipv6-l3qos] size = 256
          MAC L3 QoS [mac-l3qos] size = 0
          Ingress System size = 0
          Egress System size = 0
          Ingress SPAN [span] size = 96
          COPP [copp] size = 128
          Ingress Flow Counters [flow] size = 0

switch#
```

To view ACL related tech support information, use the **show tech-support aclmgr** and **show tech-support aclqos** commands.

```
show tech-support aclmgr
show tech-support aclqos
```

7.12 Configuring Object Groups

You can use object groups to specify source and destination addresses and protocol ports in IPv4 ACL and IPv6 ACL rules.

7.12.1 Session Manager Support for Object Groups

Session Manager supports the configuration of object groups. This feature allows you to create a configuration session and verify your object group configuration changes prior to committing them to the running configuration. For more information about Session Manager, see the *Inspur CN12900 Series INOS-CN System Management Configuration Guide*.

7.12.2 Creating and Changing an IPv4 Address Object Group

You can create and change an IPv4 address group object.

SUMMARY STEPS

1. **configure terminal**
2. **object-group ip address name**
3. Enter one of the following commands:
 - `[sequence-number] host IPv4-address`
 - `[sequence-number] IPv4-address/prefix-len`
 - `[sequence-number] IPv4-address network-wildcard`
4. Enter one of the following commands:
 - `no [sequence-number]`
 - `no host IPv4-address`
 - `no IPv4-address/prefix-len`
 - `no IPv4-address network-wildcard`
5. (Optional) **show object-group name**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	object-group ip address name Example: <pre>switch(config)# object-group ip address</pre>	Creates the IPv4 address object group and enters IPv4 address object-group configuration mode.

	Command or Action	Purpose
	<pre>ipv4-addr-group-13 switch(config-ipaddr-ogroup)#</pre>	
Step 3	<p>Enter one of the following commands:</p> <ul style="list-style-type: none"> • <i>[sequence-number] host IPv4-address</i> • <i>[sequence-number] IPv4-address/prefix-len</i> • <i>[sequence-number] IPv4-address network-wildcard</i> <p>Example:</p> <pre>switch(config-ipaddr-ogroup)# host 10.99.32.6</pre>	<p>Creates an entry in the object group. For each entry that you want to create, use the host command and specify a single host, or omit the host command to specify a network of hosts.</p> <p>You can specify a prefix length for an IPv4 object group, which matches only on the first contiguous bits, or you can specify a wildcard mask, which matches on any bit in the address.</p>
Step 4	<p>Enter one of the following commands:</p> <ul style="list-style-type: none"> • <i>no [sequence-number]</i> • <i>no host IPv4-address</i> • <i>no IPv4-address/prefix-len</i> • <i>no IPv4-address network-wildcard</i> <p>Example:</p> <pre>switch(config-ipaddr-ogroup)# no host 10.99.32.6</pre>	<p>Removes an entry in the object group. For each entry that you want to remove from the object group, use the no form of the host command.</p>
Step 5	<p>(Optional) show object-group name</p> <p>Example:</p> <pre>switch(config-ipaddr-ogroup)# show object- group ipv4-addr-group-13</pre>	<p>Displays the object group configuration.</p>
Step 6	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config-ipaddr-ogroup)# copy running- config startup-config</pre>	<p>Copies the running configuration to the startup configuration.</p>

7.12.3 Creating and Changing an IPv6 Address Object Group

You can create and change an IPv6 address group object.

SUMMARY STEPS

1. **configure terminal**
2. **object-group ipv6 address name**
3. Enter one of the following commands:
 - *[sequence-number] host IPv6-address*

- *[sequence-number] IPv6-address/prefix-len*
 - *[sequence-number] IPv6-address network-wildcard*
4. Enter one of the following commands:
 - **no** *sequence-number*
 - **no host** *IPv6-address*
 - **no** *IPv6-address/prefix-len*
 - **no** *IPv6-address network-wildcard*
 5. (Optional) **show object-group name**
 6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	object-group ipv6 address name Example: <pre>switch(config)# object-group ipv6 address ipv6-addr-group-A7 switch(config-ipv6addr-ogroup)#</pre>	Creates the IPv6 address object group and enters IPv6 address object-group configuration mode.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • <i>[sequence-number] host IPv6-address</i> • <i>[sequence-number] IPv6-address/prefix-len</i> • <i>[sequence-number] IPv6-address network-wildcard</i> 	Creates an entry in the object group. For each entry that you want to create, use the host command and specify a single host, or omit the host command to specify a network of hosts.
Step 4	Enter one of the following commands: <ul style="list-style-type: none"> • no <i>sequence-number</i> • no host <i>IPv6-address</i> • no <i>IPv6-address/prefix-len</i> • no <i>IPv6-address network-wildcard</i> Example: <pre>switch(config-ipv6addr-ogroup)# no host 2001:db8:0:3ab0::1</pre>	Removes an entry from the object group. For each entry that you want to remove from the object group, use the no form of the host command.
Step 5	(Optional) show object-group name Example: <pre>switch(config-ipv6addr-ogroup)# show object- group</pre>	Displays the object group configuration.

	Command or Action	Purpose
	ipv6-addr-group-A7	
Step 6	(Optional) copy running-config startup-config Example: switch(config-ipv6addr-ogroup)# copy running-config startup-config	Copies the running configuration to the startup configuration.

7.12.4 Creating and Changing a Protocol Port Object Group

You can create and change a protocol port object group.

SUMMARY STEPS

1. **configure terminal**
2. **object-group ip port name**
3. [*sequence-number*] *operator port-number* [*port-number*]
4. **no** {*sequence-number* | *operator port-number* [*port-number*]}
5. (Optional) **show object-group name**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	object-group ip port name Example: switch(config)# object-group ip port NYC-datacenter-ports switch(config-port-ogroup)#	Creates the protocol port object group and enters port object-group configuration mode.
Step 3	[<i>sequence-number</i>] <i>operator port-number</i> [<i>port-number</i>] Example: switch(config-port-ogroup)# eq 80	Creates an entry in the object group. For each entry that you want to create, use one of the following operator commands: <ul style="list-style-type: none"> • eq—Matches only the port number that you specify. • gt—Matches port numbers that are greater than (and not equal to) the port number that you specify. • lt—Matches port numbers that are less than (and not equal to) the port number that you specify. • neq—Matches all port numbers except for the port

	Command or Action	Purpose
		<p>number that you specify.</p> <ul style="list-style-type: none"> • range—Matches the range of port numbers between and including the two port numbers that you specify. <p>Note The range command is the only operator command that requires two <i>port-number</i> arguments.</p>
Step 4	<p>no {<i>sequence-number</i> <i>operator port-number</i> [<i>port-number</i>]}</p> <p>Example:</p> <pre>switch(config-port-ogroup)# no eq 80</pre>	Removes an entry from the object group. For each entry that you want to remove, use the no form of the applicable operator command.
Step 5	<p>(Optional) show object-group name</p> <p>Example:</p> <pre>switch(config-port-ogroup)# show object-group NYC-datacenter-ports</pre>	Displays the object group configuration.
Step 6	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config-port-ogroup)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

7.12.5 Removing an Object Group

You can remove an IPv4 address object group, an IPv6 address object group, or a protocol port object group.

SUMMARY STEPS

1. **configure terminal**
2. **no object-group {ip address | ipv6 address | ip port} name**
3. (Optional) **show object-group**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	<p>no object-group {ip address ipv6 address ip port}</p>	Removes the specified object group.

	Command or Action	Purpose
	<i>name</i> Example: <pre>switch(config)# no object-group ip address ipv4-addr-group-A7</pre>	
Step 3	(Optional) show object-group Example: <pre>switch(config)# show object-group</pre>	Displays all object groups. The removed object group should not appear.
Step 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

7.13 Verifying the Object-Group Configuration

To display object-group configuration information, enter one of the following commands:

Command	Purpose
show object-group	Displays the object-group configuration.
show {ip ipv6} access-lists <i>name</i> [expanded]	Displays expanded statistics for the ACL configuration.
show running-config aclmgr	Displays the ACL configuration, including object groups.

7.14 Configuring Time Ranges

7.14.1 Session Manager Support for Time Ranges

Session Manager supports the configuration of time ranges. This feature allows you to create a configuration session and verify your time-range configuration changes prior to committing them to the running configuration. For more information about Session Manager, see the *Inspur CN12900 Series INOS-CN System Management Configuration Guide*.

7.14.2 Creating a Time Range

You can create a time range on the device and add rules to it.

SUMMARY STEPS

1. **configure terminal**
2. **time-range *name***
3. (Optional) [*sequence-number*] **periodic *weekday* *time* to [*weekday*] *time***
4. (Optional) [*sequence-number*] **periodic *list-of-weekdays* *time* to *time***
5. (Optional) [*sequence-number*] **absolute *start time date* [*end time date*]**
6. (Optional) [*sequence-number*] **absolute [*start time date*] *end time date***
7. (Optional) **show time-range *name***

8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	time-range name Example: <pre>switch(config)# time-range workday-daytime switch(config-time-range)#</pre>	Creates the time range and enters time-range configuration mode.
Step 3	(Optional) [<i>sequence-number</i>] periodic weekday time to [weekday] time Example: <pre>switch(config-time-range)# periodic monday 00:00:00 to friday 23:59:59</pre>	Creates a periodic rule that is in effect for one or more contiguous days between and including the specified start and end days and times.
Step 4	(Optional) [<i>sequence-number</i>] periodic list-of-weekdays time to time Example: <pre>switch(config-time-range)# periodic weekdays 06:00:00 to 20:00:00</pre>	Creates a periodic rule that is in effect on the days specified by the <i>list-of-weekdays</i> argument between and including the specified start and end times. The following keywords are also valid values for the <i>list-of-weekdays</i> argument: <ul style="list-style-type: none"> • daily —All days of the week. • weekdays —Monday through Friday. • weekend —Saturday through Sunday.
Step 5	(Optional) [<i>sequence-number</i>] absolute start time date [end time date] Example: <pre>switch(config-time-range)# absolute start 1:00 15 march 2013</pre>	Creates an absolute rule that is in effect beginning at the time and date specified after the start keyword. If you omit the end keyword, the rule is always in effect after the start time and date have passed.
Step 6	(Optional) [<i>sequence-number</i>] absolute [start time date] end time date	Creates an absolute rule that is in effect until the time and date specified after the end keyword. If you omit

	Command or Action	Purpose
	Example: <pre>switch(config-time-range)# absolute end 23:59:59 31 may 2013</pre>	the start keyword, the rule is always in effect until the end time and date have passed.
Step 7	(Optional) show time-range name Example: <pre>switch(config-time-range)# show time-range workday-daytime</pre>	Displays the time-range configuration.
Step 8	(Optional) copy running-config startup-config Example: <pre>switch(config-time-range)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

7.14.3 Changing a Time Range

You can add and remove rules in an existing time range. You cannot change existing rules. Instead, to change a rule, you can remove it and recreate it with the desired changes.

If you need to add more rules between existing rules than the current sequence numbering allows, you can use the **resequence** command to reassign sequence numbers.

SUMMARY STEPS

1. **configure terminal**
2. **time-range name**
3. (Optional) [*sequence-number*] **periodic weekday time to** [*weekday*] *time*
4. (Optional) [*sequence-number*] **periodic list-of-weekdays time to time**
5. (Optional) [*sequence-number*] **absolute start time date** [**end time date**]
6. (Optional) [*sequence-number*] **absolute** [**start time date**] **end time date**
7. (Optional) **no** {*sequence-number* | **periodic arguments . . .** | **absolute arguments. . .**}
8. (Optional) **show time-range name**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	time-range name Example: <pre>switch(config)# time-range workday-daytime switch(config-time-range)#</pre>	Enters time-range configuration mode for the specified time range.

	Command or Action	Purpose
Step 3	<p>(Optional) [<i>sequence-number</i>] periodic <i>weekday</i> <i>time to</i> <i>[weekday] time</i></p> <p>Example:</p> <pre>switch(config-time-range)# periodic monday 00:00:00 to friday 23:59:59</pre>	Creates a periodic rule that is in effect for one or more contiguous days between and including the specified start and end days and times.
Step 4	<p>(Optional) [<i>sequence-number</i>] periodic <i>list-of-weekdays</i> <i>time to time</i></p> <p>Example:</p> <pre>switch(config-time-range)# 100 periodic weekdays 05:00:00 to 22:00:00</pre>	Creates a periodic rule that is in effect on the days specified by the <i>list-of-weekdays</i> argument between and including the specified start and end times. The following keywords are also valid values for the <i>list-of-weekdays</i> argument: <ul style="list-style-type: none"> • daily —All days of the week. • weekdays —Monday through Friday. • weekend —Saturday through Sunday.
Step 5	<p>(Optional) [<i>sequence-number</i>] absolute <i>start time date</i> <i>[end time date]</i></p> <p>Example:</p> <pre>switch(config-time-range)# absolute start 1:00 15 march 2013</pre>	Creates an absolute rule that is in effect beginning at the time and date specified after the start keyword. If you omit the end keyword, the rule is always in effect after the start time and date have passed.
Step 6	<p>(Optional) [<i>sequence-number</i>] absolute [<i>start time date</i>] end <i>time date</i></p> <p>Example:</p> <pre>switch(config-time-range)# absolute end 23:59:59 31 may 2013</pre>	Creates an absolute rule that is in effect until the time and date specified after the end keyword. If you omit the start keyword, the rule is always in effect until the end time and date have passed.
Step 7	<p>(Optional) no {<i>sequence-number</i> periodic <i>arguments . . .</i> absolute <i>arguments. . .</i>}</p> <p>Example:</p> <pre>switch(config-time-range)# no 80</pre>	Removes the specified rule from the time range.
Step 8	(Optional) show <i>time-range name</i>	Displays the time-range configuration.

	Command or Action	Purpose
	Example: <pre>switch(config-time-range)# show time-range workday-daytime</pre>	
Step 9	(Optional) copy running-config startup-config Example: <pre>switch(config-time-range)# copy running- config startup-config</pre>	Copies the running configuration to the startup configuration.

7.14.4 Removing a Time Range

You can remove a time range from the device.

Before you begin

Ensure that you know whether the time range is used in any ACL rules. The device allows you to remove time ranges that are used in ACL rules. Removing a time range that is in use in an ACL rule does not affect the configuration of interfaces where you have applied the ACL. Instead, the device considers the ACL rule using the removed time range to be empty.

SUMMARY STEPS

1. **configure terminal**
2. **no time-range** *name*
3. (Optional) **show time-range**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	no time-range <i>name</i> Example: <pre>switch(config)# no time-range daily-workhours</pre>	Removes the time range that you specified by name.
Step 3	(Optional) show time-range Example: <pre>switch(config-time-range)# show time-range</pre>	Displays the configuration for all time ranges. The removed time range should not appear.
Step 4	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

7.14.5 Changing Sequence Numbers in a Time Range

You can change all the sequence numbers assigned to rules in a time range.

SUMMARY STEPS

1. **configure terminal**
2. **resequence time-range name starting-sequence-number increment**
3. (Optional) **show time-range name**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	resequence time-range name starting-sequence-number increment Example: <pre>switch(config)# resequence time-range daily-workhours 100 10 switch(config)#</pre>	Assigns sequence numbers to the rules contained in the time range, where the first rule receives the starting sequence number that you specify. Each subsequent rule receives a number larger than the preceding rule. The difference in numbers is determined by the increment that you specify.
Step 3	(Optional) show time-range name Example: <pre>switch(config)# show time-range daily-workhours</pre>	Displays the time-range configuration.
Step 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

7.15 Verifying the Time-Range Configuration

To display time-range configuration information, perform one of the following tasks.

Command	Purpose
show time-range	Displays the time-range configuration.
show running-config aclmgr	Displays ACL configuration, including all time ranges.

7.16 Additional References for IP ACLs

Related Documents

Related Topic	Document Title
TAP aggregation	Configuring TAP Aggregation and MPLS Stripping

CHAPTER 8 Configuring MAC ACLs

This chapter describes how to configure MAC access lists (ACLs) on Inspur INOS-CN devices. This chapter contains the following sections:

8.1 About MAC ACLs

MAC ACLs are ACLs that use information in the Layer 2 header of packets to filter traffic. MAC ACLs share many fundamental concepts with IP ACLs, including support for virtualization.

8.1.1 MAC Packet Classification

MAC packet classification allows you to control whether a MAC ACL that is on a Layer 2 interface applies to all traffic entering the interface, including IP traffic, or to non-IP traffic only.

MAC Packet Classification State	Effect on Interface
Enabled	<ul style="list-style-type: none"> • A MAC ACL that is on the interface applies to all traffic entering the interface, including IP traffic. • You cannot apply an IP port ACL on the interface.
Disabled	<ul style="list-style-type: none"> • A MAC ACL that is on the interface applies only to non-IP traffic entering the interface. • You can apply an IP port ACL on the interface

8.2 Licensing Requirements for MAC ACLs

This table shows the licensing requirements for this feature.

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

8.3 Guidelines and Limitations for MAC ACLs

MAC ACLs have the following configuration guidelines and limitations:

- MAC ACLs apply to ingress traffic only.
- If you try to apply too many ACL entries, the configuration might be rejected.
- MAC packet classification is not supported when a MAC ACL is applied as part of a VACL.
- When you define a MAC ACL on the non EX/FX Inspur CN12900 Series switches, you must define the ethertype for the traffic to be appropriately matched.

- In the absence of a direct field for marking the packet as an L2 packet, the switches match all packets with certain fields, such as `src_mac`, `dst_mac`, and `vlan` in the key field. However, they cannot match on the `eth_type` field. Therefore, if you install two rules with identical fields, except the MAC protocol number field, then the match conditions will remain identical in the hardware. Hence, although the first entry in the rule sequence will hit for all the packets for all the protocol numbers, the MAC protocol number will be a no-op when the `mac-packet classify` is configured.

8.4 Default Settings for MAC ACLs

This table lists the default settings for MAC ACL parameters.

Table 18: Default MAC ACLs Parameters

Parameters	Default
MAC ACLs	No MAC ACLs exist by default
ACL rules	Implicit rules apply to all ACLs

8.5 Configuring MAC ACLs

8.5.1 Creating a MAC ACL

You can create a MAC ACL and add rules to it.

SUMMARY STEPS

1. **configure terminal**
2. **mac access-list name**
3. **{permit | deny} source destination-protocol**
4. (Optional) **statistics per-entry**
5. (Optional) **show mac access-lists name**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	mac access-list name Example: switch(config)# mac access-list acl-mac-01 switch(config-mac-acl)#	Creates the MAC ACL and enters ACL configuration mode.
Step 3	{permit deny} source destination-protocol	Creates a rule in the MAC ACL.

	Command or Action	Purpose
	Example: <pre>switch(config-mac-acl)# 100 permit mac 00c0.4f00.0000 0000.00ff.ffff any 0x0806</pre>	The permit and deny commands support many ways of identifying traffic.
Step 4	(Optional) statistics per-entry Example: <pre>switch(config-mac-acl)# statistics per-entry</pre>	Specifies that the device maintains global statistics for packets that match the rules in the ACL.
Step 5	(Optional) show mac access-lists name Example: <pre>switch(config-mac-acl)# show mac access-lists acl-mac-01</pre>	Displays the MAC ACL configuration.
Step 6	(Optional) copy running-config startup-config Example: <pre>switch(config-mac-acl)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

8.5.2 Changing a MAC ACL

You can remove a MAC ACL from the device.

Before you begin

Use the **show mac access-lists** command with the **summary** keyword to find the interfaces on which a MAC ACL is configured.

SUMMARY STEPS

1. **configure terminal**
2. **mac access-list name**
3. (Optional) *[sequence-number] {permit | deny} source destination-protocol*
4. (Optional) **no** *{sequence-number | {permit | deny} source destination-protocol}*
5. (Optional) **[no] statistics per-entry**
6. (Optional) **show mac access-lists name**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	mac access-list name Example:	Enters ACL configuration mode for the ACL that you specify by name.

	Command or Action	Purpose
	switch(config)# mac access-list acl-mac-01 switch(config-mac-acl)#	
Step 3	(Optional) [<i>sequence-number</i>] { permit deny } <i>source</i> <i>destination-protocol</i> Example: switch(config-mac-acl)# 100 permit mac 00c0.4f00.0000 0000.00ff.ffff any 0x0806	Creates a rule in the MAC ACL. Using a sequence number allows you to specify a position for the rule in the ACL. Without a sequence number, the rule is added to the end of the rules. The permit and deny commands support many ways of identifying traffic.
Step 4	(Optional) no { <i>sequence-number</i> { permit deny } <i>source</i> <i>destination-protocol</i> } Example: switch(config-mac-acl)# no 80	Removes the rule that you specify from the MAC ACL. The permit and deny commands support many ways of identifying traffic.
Step 5	(Optional) [no] statistics per-entry Example: switch(config-mac-acl)# statistics per-entry	Specifies that the device maintains global statistics for packets that match the rules in the ACL. The no option stops the device from maintaining global statistics for the ACL.
Step 6	(Optional) show mac access-lists <i>name</i> Example: switch(config-mac-acl)# show mac access-lists acl-mac-01	Displays the MAC ACL configuration.
Step 7	(Optional) copy running-config startup-config Example: switch(config-mac-acl)# copy running-config startup-config	Copies the running configuration to the startup configuration.

8.5.3 Changing Sequence Numbers in a MAC ACL

You can change all the sequence numbers assigned to rules in a MAC ACL. Resequencing is useful when you need to insert rules into an ACL and there are not enough available sequence numbers.

SUMMARY STEPS

1. **configure terminal**
2. **resequence mac access-list** *name* *starting-sequence-number* *increment*
3. (Optional) **show mac access-lists** *name*
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	resequence mac access-list <i>name</i> <i>starting-sequence-number increment</i> Example: switch(config)# resequence mac access-list acl-mac-01 100 10	Assigns sequence numbers to the rules contained in the ACL, where the first rule receives the number specified by the starting-sequence number that you specify. Each subsequent rule receives a number larger than the preceding rule. The difference in numbers is determined by the increment number that you specify.
Step 3	(Optional) show mac access-lists <i>name</i> Example: switch(config)# show mac access-lists acl-mac-01	Displays the MAC ACL configuration.
Step 4	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

8.5.4 Removing a MAC ACL

You can remove a MAC ACL from the device.

SUMMARY STEPS

1. **configure terminal**
2. **no mac access-list *name***
3. (Optional) **show mac access-lists *name* summary**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	no mac access-list <i>name</i> Example: switch(config)# no mac access-list acl-mac-01	Removes the MAC ACL that you specify by name from the running configuration.

	Command or Action	Purpose
	<code>switch(config)#</code>	
Step 3	(Optional) show mac access-lists <i>name</i> summary Example: <code>switch(config)# show mac access-lists acl-mac-01 summary</code>	Displays the MAC ACL configuration. If the ACL remains applied to an interface, the command lists the interfaces.
Step 4	(Optional) copy running-config startup-config Example: <code>switch(config)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

8.5.5 Applying a MAC ACL as a Port ACL

You can apply a MAC ACL as a port ACL to any of the following interface types:

- Layer 2 Ethernet interfaces
- Layer 2 port-channel interfaces

Before you begin

Ensure that the ACL that you want to apply exists and is configured to filter traffic in the manner that you need for this application.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
 - **interface ethernet *slot/port***
 - **interface port-channel *channel-number***
3. **mac port access-group *access-list***
4. (Optional) **show running-config aclmgr**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	Enters global configuration mode.
Step 2	Enter one of the following commands: <ul style="list-style-type: none"> • interface ethernet <i>slot/port</i> • interface port-channel <i>channel-number</i> Example: <code>switch(config)# interface ethernet 2/1</code>	<ul style="list-style-type: none"> • Enters interface configuration mode for a Layer 2 or Layer 3 interface. • Enters interface configuration mode for a Layer 2 or Layer 3 port-channel interface.

	Command or Action	Purpose
	<pre>switch(config-if)#</pre> <p>Example:</p> <pre>switch(config)# interface port-channel 5 switch(config-if)#</pre>	
Step 3	<p>mac port access-group <i>access-list</i></p> <p>Example:</p> <pre>switch(config-if)# mac port access-group acl-01</pre>	Applies a MAC ACL to the interface.
Step 4	<p>(Optional) show running-config aclmgr</p> <p>Example:</p> <pre>switch(config-if)# show running-config aclmgr</pre>	Displays the ACL configuration.
Step 5	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config-if)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

8.5.6 Applying a MAC ACL as a VACL

You can apply a MAC ACL as a VACL.

8.5.7 Enabling or Disabling MAC Packet Classification

You can enable or disable MAC packet classification on a Layer 2 interface.

Before you begin

The interface must be configured as a Layer 2 interface.

SUMMARY STEPS

1. **configure terminal**
2. Enter one of the following commands:
 - **interface ethernet** *slot/port*
 - **interface port-channel** *channel-number*
3. **[no] mac packet-classify**
4. (Optional) Enter one of the following commands:
 - **show running-config interface ethernet** *slot/port*
 - **show running-config interface port-channel** *channel-number*
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	Enter one of the following commands: <ul style="list-style-type: none"> • interface ethernet <i>slot/port</i> • interface port-channel <i>channel-number</i> Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre> Example: <pre>switch(config)# interface port-channel 5 switch(config-if)#</pre>	<ul style="list-style-type: none"> • Enters interface configuration mode for an Ethernet interface. • Enters interface configuration mode for a port-channel interface.
Step 3	[no] mac packet-classify Example: <pre>switch(config-if)# mac packet-classify</pre>	Enables MAC packet classification on the interface. The no option disables MAC packet classification on the interface.
Step 4	(Optional) Enter one of the following commands: <ul style="list-style-type: none"> • show running-config interface ethernet <i>slot/port</i> • show running-config interface port-channel <i>channel-number</i> Example: <pre>switch(config-if)# show running-config interface ethernet 2/1</pre> Example: <pre>switch(config-if)# show running-config interface port-channel 5</pre>	<ul style="list-style-type: none"> • Displays the running configuration of the Ethernet interface. • Displays the running configuration of the port-channel interface.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

8.6 Verifying the MAC ACL Configuration

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

Command	Purpose
show mac access-lists	Displays the MAC ACL configuration.
show running-config aclmgr	Displays the ACL configuration, including MAC ACLs and the interfaces

[all]	to which MAC ACLs are applied. Note This command displays the user-configured ACLs in the running configuration. The all option displays both the default (CoPP-configured) and user-configured ACLs in the running configuration.
show startup-config aclmgr [all]	Displays the ACL startup configuration. Note This command displays the user-configured ACLs in the startup configuration. The all option displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration.

8.7 Monitoring and Clearing MAC ACL Statistics

To monitor or clear MAC ACL statistics, use one of the commands in this table.

Command	Purpose
show mac access-lists	Displays the MAC ACL configuration. If the MAC ACL includes the statistics per-entry command, the show mac access-lists command output includes the number of packets that have matched each rule.
clear mac access-list counters	Clears statistics for MAC ACLs.

8.8 Configuration Example for MAC ACLs

The following example shows how to create a MAC ACL named `acl-mac-01` and apply it to Ethernet interface 2/1, which is a Layer 2 interface in this example:

```
mac access-list acl-mac-01
  permit 00c0.4f00.0000 0000.00ff.ffff any
0x0806 interface ethernet 2/1
  mac port access-group acl-mac-01
```

8.9 Additional References for MAC ACLs

Related Documents

Related Topic	Document Title
TAP aggregation	Configuring TAP Aggregation and MPLS Stripping

CHAPTER 9 Configuring VLAN ACLs

This chapter describes how to configure VLAN access lists (ACLs) on Inspur INOS-CN devices. This chapter includes the following sections:

9.1 About VLAN ACLs

A VLAN ACL (VACL) is one application of an IP ACL or a MAC ACL. You can configure VACLs to apply to all packets that are routed into or out of a VLAN or are bridged within a VLAN. VACLs are strictly for security packet filtering and for redirecting traffic to specific physical interfaces. VACLs are not defined by direction (ingress or egress).

9.1.1 VLAN Access Maps and Entries

VACLs use access maps to contain an ordered list of one or more map entries. Each map entry associates IP or MAC ACLs to an action. Each entry has a sequence number, which allows you to control the precedence of entries.

When the device applies a VACL to a packet, it applies the action that is configured in the first access map entry that contains an ACL that permits the packet.

9.1.2 VACLs and Actions

In access map configuration mode, you use the **action** command to specify one of the following actions:

Forward

Sends the traffic to the destination determined by the normal operation of the device.

Redirect

Redirects the traffic to one or more specified interfaces.

Drop

Drops the traffic. If you specify drop as the action, you can also specify that the device logs the dropped packets.

9.1.3 VACL Statistics

The device can maintain global statistics for each rule in a VACL. If a VACL is applied to multiple VLANs, the maintained rule statistics are the sum of packet matches (hits) on all the interfaces on which that VACL is applied.

For each VLAN access map that you configure, you can specify whether the device maintains statistics for that VACL. This feature allows you to turn VACL statistics on or off as needed to monitor traffic filtered by a VACL or to help troubleshoot VLAN access-map configuration.

9.1.4 Session Manager Support for VACLs

Session Manager supports the configuration of VACLs. This feature allows you to verify the ACL configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration. For more information about Session Manager, see the *Inspur CN12900 Series INOS-CN System Management Configuration Guide*.

9.2 Licensing Requirements for VACLs

This table shows the licensing requirements for this feature.

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

9.3 Prerequisites for VACLs

VACLs have the following prerequisite:

- Ensure that the IP ACL or MAC ACL that you want to use in the VACL exists and is configured to filter traffic in the manner that you need for this application.

9.4 Guidelines and Limitations for VACLs

VACLs have the following configuration guidelines:

- Inspur recommends using the Session Manager to configure ACLs. This feature allows you to verify the ACL configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration. For more information about Session Manager, see the Inspur CN12900 Series INOS-CN System Management Configuration Guide.
- If you try to apply too many ACL entries, the configuration might be rejected.
- VACL redirects to SPAN destination ports are not supported.
- VACL logging is not supported.
- TCAM resources are not shared when a VACL is applied to multiple VLANs.
- Deny statements are not supported on VACLs. Alternatively, you can use permit statements with the action 'drop' to achieve a similar outcome.
- When configuring a VACL with the "redirect" option, the interface that you define as the redirect interface, must be configured as a member of the VLAN which you apply this VACL to. This VLAN must also be in the forwarding state on this interface for the redirection to work. If these conditions are not met, then the switch will drop the packets which are matched by the VACL.

The following guidelines apply to VACLs for VXLANs:

- VACLs applied on a VXLAN VLAN in the access to network direction (Layer 2 to Layer 3 encapsulation path) are supported on the inner payload.
- We recommend using VACLs on the access side to filter out traffic entering the overlay network.
- Egress VACLs for decapsulated VXLAN traffic are not supported.

9.5 Default Settings for VACLs

This table lists the default settings for VACL parameters.

Table 19: Default VACL Parameters

Parameters	Default
VACLs	No IP ACLs exist by default
ACL rules	Implicit rules apply to all ACLs

9.6 Configuring VACLs

9.6.1 Creating a VACL or Adding a VACL Entry

You can create a VACL or add entries to an existing VACL. In both cases, you create a VACL entry, which is a VLAN access-map entry that associates one or more ACLs with an action to be applied to the matching traffic.

Before you begin

Ensure that the ACLs that you want to use in the VACL exist and are configured to filter traffic in the manner that you need for this application.

SUMMARY STEPS

1. **configure terminal**
2. **vlan access-map** *map-name* [*sequence-number*]
3. Enter one of the following commands:
 - **match** {**ip** | **ipv6**} **address** *ip-access-list*
 - **match mac address** *mac-access-list*
4. **action** {**drop** | **forward** | **redirect**}
5. (Optional) [**no**] **statistics per-entry**
6. (Optional) **show running-config aclmgr**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	vlan access-map <i>map-name</i> [<i>sequence-number</i>] Example: <pre>switch(config)# vlan access-map acl-mac-map switch(config-access-map)#</pre>	Enters VLAN access-map configuration mode for the VLAN access map specified. If the VLAN access map does not exist, the device creates it. If you do not specify a sequence number, the device creates a new entry whose sequence number is 10 greater than the last sequence number in the access map.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • match {ip ipv6} address <i>ip-access-list</i> • match mac address <i>mac-access-list</i> Example: <pre>switch(config-access-map)# match mac address acl-ip-lab</pre> Example: <pre>switch(config-access-map)# match mac address</pre>	Specifies an ACL for the access-map entry.

	Command or Action	Purpose
	acl-mac-01	
Step 4	action {drop forward redirect} Example: <pre>switch(config-access-map)# action forward</pre> Example: <pre>switch(config-access-map)# vlan access-map vacl1 switch(config-access-map)# action redirect e1/1 switch(config-access-map)# action redirect po100</pre>	Specifies the action that the device applies to traffic that matches the ACL. The action command supports the drop , forward , and redirect options.
Step 5	(Optional) [no] statistics per-entry Example: <pre>switch(config-access-map)# statistics per-entry</pre>	Specifies that the device maintains global statistics for packets that match the rules in the VACL. The no option stops the device from maintaining global statistics for the VACL.
Step 6	(Optional) show running-config aclmgr Example: <pre>switch(config-access-map)# show running-config aclmgr</pre>	Displays the ACL configuration.
Step 7	(Optional) copy running-config startup-config Example: <pre>switch(config-access-map)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

9.6.2 Removing a VACL or a VACL Entry

You can remove a VACL, which means that you will delete the VLAN access map.

You can also remove a single VLAN access-map entry from a VACL.

Before you begin

Ensure that you know whether the VACL is applied to a VLAN. The device allows you to remove VACLs that are currently applied. Removing a VACL does not affect the configuration of VLANs where you have applied the VACL. Instead, the device considers the removed VACL to be empty.

SUMMARY STEPS

1. **configure terminal**
2. **no vlan access-map** *map-name* [*sequence-number*]
3. (Optional) **show running-config aclmgr**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	no vlan access-map <i>map-name</i> [<i>sequence-number</i>] Example: switch(config)# no vlan access-map acl-mac-map 10	Removes the VLAN access map configuration for the specified access map. If you specify the <i>sequence-number</i> argument and the VACL contains more than one entry, the command removes only the entry specified.
Step 3	(Optional) show running-config aclmgr Example: switch(config)# show running-config aclmgr	Displays the ACL configuration.
Step 4	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

9.6.3 Applying a VACL to a VLAN

You can apply a VACL to a VLAN.

Before you begin

If you are applying a VACL, ensure that the VACL exists and is configured to filter traffic in the manner that you need for this application.

SUMMARY STEPS

1. **configure terminal**
2. **[no] vlan filter *map-name* *vlan-list* *list***
3. (Optional) **show running-config aclmgr**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	[no] vlan filter <i>map-name</i> <i>vlan-list</i> <i>list</i> Example:	Applies the VACL to the VLANs by the list that you specified. The no option unapplies the VACL.

	Command or Action	Purpose
	<pre>switch(config)# vlan filter acl-mac-map vlan- list 1-20,26-30 switch(config)#</pre>	
Step 3	(Optional) show running-config aclmgr Example: <pre>switch(config)# show running-config aclmgr</pre>	Displays the ACL configuration.
Step 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup- config</pre>	Copies the running configuration to the startup configuration.

9.7 Verifying the VACL Configuration

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

Command	Purpose
show running-config aclmgr [all]	Displays the ACL configuration, including the VACL-related configuration. Note This command displays the user-configured ACLs in the running configuration. The all option displays both the default (CoPP-configured) and user-configured ACLs in the running configuration.
show startup-config aclmgr [all]	Displays the ACL startup configuration. Note This command displays the user-configured ACLs in the startup configuration. The all option displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration.
show vlan filter	Displays information about VACLs that are applied to a VLAN.
show vlan access-map	Displays information about VLAN access maps.

9.8 Monitoring and Clearing VACL Statistics

To monitor or clear VACL statistics, use one of the commands in this table.

Command	Purpose
show vlan access-list	Displays the VACL configuration. If the VLAN access-map includes the statistics per-entry command, the show vlan access-list command output includes the number of packets that have matched each rule.
clear vlan access-list counters	Clears statistics for VACLs.

9.9 Configuration Example for VACLs

The following example shows how to configure a VACL to forward traffic permitted by a MAC ACL named acl-mac-01 and how to apply the VACL to VLANs 50 through 82:

```
conf t
vlan access-map acl-mac-map
  match mac address acl-mac-01
  action forward
vlan filter acl-mac-map vlan-list 50-82
```

9.10 Additional References for VACLs

Related Documents

Related Topic	Document Title
QoS configuration	<i>nspur CN12900 Series INOS-CN Quality of Service Configuration Guide</i>

CHAPTER 10 Configuring Traffic Storm Control

This chapter describes how to configure traffic storm control on the Inspur INOS-CN device. This chapter includes the following sections:

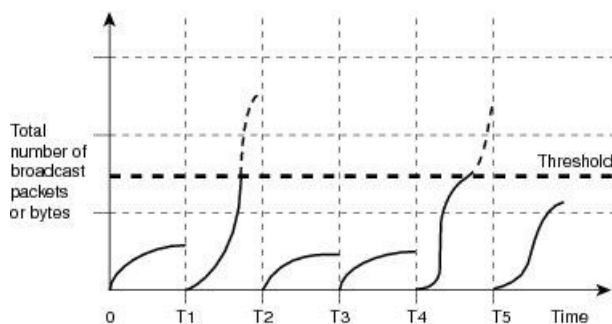
10.1 About Traffic Storm Control

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. You can use the traffic storm control feature to prevent disruptions on Layer 2 ports by a broadcast, multicast, or unicast traffic storm on physical interfaces.

Traffic storm control (also called traffic suppression) allows you to monitor the levels of the incoming broadcast, multicast, and unicast traffic over a 3.9-millisecond interval. During this interval, the traffic level, which is a percentage of the total available bandwidth of the port, is compared with the traffic storm control level that you configured. When the ingress traffic reaches the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends.

This table shows the broadcast traffic patterns on a Layer 2 interface over a given interval. In this example, traffic storm control occurs between times T1 and T2 and between T4 and T5. During those intervals, the amount of broadcast traffic exceeded the configured threshold.

Figure 6: Broadcast Suppression



The traffic storm control threshold numbers and the time interval allow the traffic storm control algorithm to work with different levels of granularity. A higher threshold allows more packets to pass through.

Traffic storm control on the Inspur CN12900 device is implemented in the hardware. The traffic storm control circuitry monitors packets that pass from a Layer 2 interface to the switching bus. Using the Individual/Group bit in the packet destination address, the circuitry determines if the packet is unicast or broadcast, tracks the current count of packets within the 3.9-millisecond interval, and filters out subsequent packets when a threshold is reached.

Traffic storm control uses a bandwidth-based method to measure traffic. You set the percentage of total available bandwidth that the controlled traffic can use. Because packets do not arrive at uniform intervals, the 3.9-millisecond interval can affect the behavior of traffic storm control.

The following are examples of traffic storm control behavior:

- If you enable broadcast traffic storm control, and broadcast traffic exceeds the level within the 3.9-millisecond interval, traffic storm control drops all broadcast traffic until the end of the interval.
- If you enable broadcast and multicast traffic storm control, and the combined broadcast and multicast traffic exceeds the level within the 3.9-millisecond interval, traffic storm control drops all broadcast and multicast traffic until the end of the interval.
- If you enable broadcast and multicast traffic storm control, and broadcast traffic exceeds the level within the 3.9-millisecond interval, traffic storm control drops all broadcast and multicast traffic until the end of

the interval.

- If you enable broadcast and multicast traffic storm control, and multicast traffic exceeds the level within the 3.9-millisecond interval, traffic storm control drops all broadcast and multicast traffic until the end of the interval.

By default, the Inspur certifies that it takes no corrective action when the traffic exceeds the configured level. However, you can configure an Embedded Event Management (EEM) action to error-disable an interface if the traffic does not subside (drop below the threshold) within a certain time period. For information about configuring EEM, see the *Inspur CN12900 Series INOS-CN System Management Configuration Guide*.

10.2 Licensing Requirements for Traffic Storm Control

The following table shows the licensing requirements for this feature:

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

10.3 Guidelines and Limitations for Traffic Storm Control

Traffic storm control has the following configuration guidelines and limitations:

- You can configure traffic storm control on a port-channel interface.
- Specify the traffic storm control level as a percentage of the total interface bandwidth:
- The pps range can be from 0 to 200000000.
- The optional fraction of a level can be from 0 to 99.
- 100 percent means no traffic storm control.
- 0.0 percent suppresses all traffic.
- For Inspur CN12900 platform switches you can use the storm control CLI to specify bandwidth level either as a percentage of port capacity or packets-per-second.
- For Inspur CN12900 NFE2-enabled devices, you can use the storm control-cpu to control the number of ARP packets sent to the CPU.
- Local link and hardware limitations prevent storm-control drops from being counted separately. Instead, storm-control drops are counted with other drops in the discards counter.
- Because of hardware limitations and the method by which packets of different sizes are counted, the traffic storm control level percentage is an approximation. Depending on the sizes of the frames that make up the incoming traffic, the actual enforced level might differ from the configured level by several percentage points.
- Due to a hardware limitation, the output for the **show interface counters storm-control** command does not show ARP suppressions when storm control is configured and the interface is actually suppressing ARP broadcast traffic. This limitation can lead to the configured action not being triggered but the incoming ARP broadcast traffic being correctly storm suppressed.
- Due to a hardware limitation, the packet drop counter cannot distinguish between packet drops caused by a traffic storm and packet drops caused by other discarded input frames. This limitation can lead to the configured action being triggered even in the absence of a traffic storm.
- Due to a hardware limitation, storm suppression packet statistics are not supported on uplink ports.
- Due to a hardware limitation, storm suppression packet statistics do not include broadcast traffic on VLANs with an active switched virtual interface (SVI).
- Due to a design limitation, storm suppression packet statistics do not work if the configured level is 0.0, which is meant to suppress all incoming storm packets.
- Traffic storm control is only for ingress traffic, specifically for unknown unicast, unknown multicast, and

broadcast traffic.

10.4 Default Settings for Traffic Storm Control

This table lists the default settings for traffic storm control parameters.

Table 20: Default Traffic Storm Control Parameters

Parameters	Default
Traffic storm control	Disabled
Threshold percentage	100

10.5 Configuring Traffic Storm Control

You can set the percentage of total available bandwidth that the controlled traffic can use.

SUMMARY STEPS

1. **configure terminal**
2. **interface** {*ethernet slot/port* | **port-channel number**}
3. **[no] storm-control** {**broadcast** | **multicast** | **unicast**} **level** { <*level-value %*> | **pps** <*pps-value*> }
4. **[no] storm-control action trap**
5. **[no] storm-control-cpu arp rate**
6. **exit**
7. (Optional) **show running-config interface** {*ethernet slot/port* | **port-channel number**}
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	interface { <i>ethernet slot/port</i> port-channel number }	Enters interface configuration mode.
Step 3	[no] storm-control { broadcast multicast unicast } level { < <i>level-value %</i> > pps < <i>pps-value</i> > } Example: <pre>switch(config-if)# storm-control unicast level 40</pre>	Configures traffic storm control for traffic on the interface. You can also configure bandwidth level as a percentage either of port capacity or packets-per-second. The default state is disabled.

	Command or Action	Purpose
	Example: switch(config-if)# storm-control broadcast level pps 8000	
Step 4	[no] storm-control action trap switch(config-if)# storm-control action trap	Generates an SNMP trap and the Inspur CN12900.
Step 5	[no] storm-control-cpu arp rate Example: switch(config-if)# storm-control-cpu arp rate	Configures traffic storm control rate for arp packets entering a port channel. This rate is divided equally among the members of the port channel.
Step 6	exit Example: switch(config-if)# exit switch(config)#	Exits interface configuration mode.
Step 7	(Optional) show running-config interface { ethernet <i>slot/port</i> port-channel number } Example: switch(config)# show running-config interface ethernet 1/1	Displays the traffic storm control configuration.
Step 8	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

10.6 Verifying Traffic Storm Control Configuration

To display traffic storm control configuration information, perform one of the following tasks:

Command	Purpose
show running-config interface	Displays the traffic storm control configuration.
show access-list storm-control arp-stats interface [ethernet port-channel] number	Displays the storm control statistics for arp packets on the interface.

10.7 Monitoring Traffic Storm Control Counters

You can monitor the counters the Inspur INOS-CN device maintains for traffic storm control activity.

Command	Purpose
---------	---------

show interface [ethernet <i>slot/port</i> port-channel <i>number</i>] counters storm-control	Displays the traffic storm control counters.
---	--

10.8 Configuration Examples for Traffic Storm Control

The following example shows how to configure traffic storm control:

```
switch(config)# interface Ethernet1/1
switch(config)# storm-control broadcast level
40 switch(config)# storm-control multicast
level 40 switch(config)# storm-control unicast
level 40 switch(config)# storm-control-cpu arp
rate 150
```

The following example checks the programmed configured rate and the statistics of dropped ARP packets:

```
switch(config)# sh access-list storm-control-cpu arp-stats
interface port-channel 132
slot 1
=====
-----
                        ARP Policer Entry Statistics
-----
Interface port-channel132:
-----
Member Interface    Entry-ID  Rate      RedPacket Count    GreenPacket Count
-----
Ethernet1/35        3976      50         0                    0
-----

slot 7
=====
-----
                        ARP Policer Entry Statistics
-----
Interface port-channel132:
-----
Member Interface    Entry-ID  Rate      RedPacket Count    GreenPacket Count
-----
```

CHAPTER 11 Configuring Control Plane Policing

This chapter contains the following sections:

11.1 About CoPP

Control Plane Policing (CoPP) protects the control plane and separates it from the data plane, which ensures network stability, reachability, and packet delivery.

This feature allows a policy map to be applied to the control plane. This policy map looks like a normal QoS policy and is applied to all traffic entering the switch from a non-management port. A common attack vector for network devices is the denial-of-service (DoS) attack, where excessive traffic is directed at the device interfaces.

The Inspur INOS-CN device provides CoPP to prevent DoS attacks from impacting performance. Such attacks, which can be perpetrated either inadvertently or maliciously, typically involve high rates of traffic destined to the supervisor module or CPU itself.

The supervisor module divides the traffic that it manages into three functional components or planes:

Data plane

Handles all the data traffic. The basic functionality of a Inspur INOS-CN device is to forward packets from one interface to another. The packets that are not meant for the switch itself are called the transit packets. These packets are handled by the data plane.

Control plane

Handles all routing protocol control traffic. These protocols, such as the Border Gateway Protocol (BGP) and the Open Shortest Path First (OSPF) Protocol, send control packets between devices. These packets are destined to router addresses and are called control plane packets.

Management plane

Runs the components meant for Inspur INOS-CN device management purposes such as the command-line interface (CLI) and Simple Network Management Protocol (SNMP).

The supervisor module has both the management plane and control plane and is critical to the operation of the network. Any disruption or attacks to the supervisor module will result in serious network outages. For example, excessive traffic to the supervisor module could overload and slow down the performance of the entire Inspur INOS-CN device. For example, a DoS attack on the supervisor module could generate IP traffic streams to the control plane at a very high rate, forcing the control plane to spend a large amount of time in handling these packets and preventing the control plane from processing genuine traffic.

Examples of DoS attacks include:

- Internet Control Message Protocol (ICMP) echo requests
- IP fragments
- TCP SYN flooding

These attacks can impact the device performance and have the following negative effects:

- Reduced service quality (such as poor voice, video, or critical applications traffic)
- High route processor or switch processor CPU utilization
- Route flaps due to loss of routing protocol updates or keepalives
- Unstable Layer 2 topology
- Slow or unresponsive interactive sessions with the CLI
- Processor resource exhaustion, such as the memory and buffers

- Indiscriminate drops of incoming packets

Caution

It is important to ensure that you protect the supervisor module from accidental or malicious attacks by configuring control plane protection.

11.1.1 Control Plane Protection

To protect the control plane, the Inspur INOS-CN device segregates different packets destined for the control plane into different classes. Once these classes are identified, the Inspur INOS-CN device polices the packets, which ensures that the supervisor module is not overwhelmed.

Control Plane Packet Types

Different types of packets can reach the control plane:

Receive packets

Packets that have the destination address of a router. The destination address can be a Layer 2 address (such as a router MAC address) or a Layer 3 address (such as the IP address of a router interface). These packets include router updates and keepalive messages. Multicast packets can also be in this category where packets are sent to multicast addresses that are used by a router.

Exception packets

Packets that need special handling by the supervisor module. For example, if a destination address is not present in the Forwarding Information Base (FIB) and results in a miss, the supervisor module sends an ICMP unreachable packet back to the sender. Another example is a packet with IP options set.

The following exceptions are possible from line cards only:

- match exception ip option
- match exception ipv6 option
- match exception ttl-failure

The following exceptions are possible from fabric modules only:

- match exception ipv6 icmp unreachable
- match exception ip icmp unreachable

The following exceptions are possible from line cards and fabric modules:

- match exception mtu-failure

Redirected packets

Packets that are redirected to the supervisor module.

Glean packets

If a Layer 2 MAC address for a destination IP address is not present in the FIB, the supervisor module receives the packet and sends an ARP request to the host.

All of these different packets could be maliciously used to attack the control plane and overwhelm the Inspur INOS-CN device. CoPP classifies these packets to different classes and provides a mechanism to individually control the rate at which the supervisor module receives these packets.

Classification for CoPP

For effective protection, the Inspur INOS-CN device classifies the packets that reach the supervisor modules to allow you to apply different rate controlling policies based on the type of the packet. For example, you might want to

be less strict with a protocol packet such as Hello messages but more strict with a packet that is sent to the supervisor module because the IP option is set. You configure packet classifications and rate controlling policies using class maps and policy maps.

Rate Controlling Mechanisms

Once the packets are classified, the Inspur INOS-CN device has different mechanisms to control the rate at which packets arrive at the supervisor module. Two mechanisms control the rate of traffic to the supervisor module. One is called policing and the other is called rate limiting.

Using hardware policers, you can define separate actions for traffic that conforms to or violates certain conditions. The actions can transmit the packet, mark down the packet, or drop the packet.

You can configure the following parameters for policing:

Committed information rate (CIR)

Desired bandwidth, specified as a bit rate or a percentage of the link rate.

Committed burst (BC)

Size of a traffic burst that can exceed the CIR within a given unit of time and not impact scheduling

In addition, you can set separate actions such as transmit or drop for conform and violate traffic.

For more information on policing parameters, see the *Inspur CN12900 Series INOS-CN Quality of Service Configuration Guide*.

Dynamic and Static CoPP ACLs

CoPP access control lists (ACLs) are classified as either dynamic or static. Inspur CN12900 switches use only dynamic CoPP ACLs.

Dynamic CoPP ACLs work only for Forwarding Information Base (FIB)-based supervisor redirected packets, and static CoPP ACLs work for ACL-based supervisor redirected packets. Dynamic CoPP ACLs are supported for myIP and link-local multicast traffic, and static CoPP ACLs are supported for all other types of traffic.

Static CoPP ACLs are identified by a substring. Any ACL that has one of these substrings is categorized as a static CoPP ACL.

- MAC-based static CoPP ACL substrings:
 - acl-mac-cdp-udld-vtp
 - acl-mac-cfsoe
 - acl-mac-dot1x
 - acl-mac-l2-tunnel
 - acl-mac-l3-isis
 - acl-mac-lacp
 - acl-mac-lldp
 - acl-mac-sdp-srp
 - acl-mac-stp
 - acl-mac-undesirable
- Protocol-based static CoPP ACL substrings:
 - acl-dhcp
 - acl-dhcp-relay-response
 - acl-dhcp6
 - acl-dhcp6-relay-response
 - acl-ptp
- Multicast-based static CoPP ACL substrings:
 - acl-igmp

Default Policing Policies

When you bring up your Inspur INOS-CN device for the first time, the Inspur INOS-CN software installs the default `copp-system-p-policy-strict` policy to protect the supervisor module from DoS attacks. You can set the level of protection by choosing one of the following CoPP policy options from the initial setup utility:

- **Strict**—This policy is 1 rate and 2 color.
- **Moderate**—This policy is 1 rate and 2 color. The important class burst size is greater than the strict policy but less than the lenient policy.
- **Lenient**—This policy is 1 rate and 2 color. The important class burst size is greater than the moderate policy but less than the dense policy.
- **Dense**—This policy is 1 rate and 2 color. The policer CIR values are less than the strict policy.
- **Skip**—No control plane policy is applied.

If you do not select an option or choose not to execute the setup utility, the software applies strict policing. We recommend that you start with the strict policy and later modify the CoPP policies as required.

The `copp-system-p-policy` policy has optimized values suitable for basic device operations. You must add specific class and access-control list (ACL) rules that meet your DoS protection requirements. The default CoPP policy does not change when you upgrade the software.

Caution	Selecting the skip option and not subsequently configuring CoPP protection can leave your Inspur INOS-CN device vulnerable to DoS attacks.
----------------	--

You can reassign the CoPP default policy by entering the setup utility again using the `setup` command from the CLI prompt or by using the `copp profile` command.

Default Class Maps

The `copp-system-class-critical` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-critical
  match access-group name copp-system-p-acl-bgp
  match access-group name copp-system-p-acl-rip match
  access-group name copp-system-p-acl-vpc match
  access-group name copp-system-p-acl-bgp6 match
  access-group name copp-system-p-acl-ospf match
  access-group name copp-system-p-acl-rip6 match
  access-group name copp-system-p-acl-eigrp match
  access-group name copp-system-p-acl-ospf6 match
  access-group name copp-system-p-acl-eigrp6 match
  access-group name copp-system-p-acl-auto-rp
  match access-group name copp-system-p-acl-mac-l3-isis
```

The `copp-system-class-exception` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-exception
  match exception ip option
  match exception ip icmp unreachable
  match exception ipv6 option
  match exception ipv6 icmp unreachable
```

The `copp-system-class-exception-dia` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-exception-dia
  match exception ttl-failure
  match exception mtu-failure
```

The `copp-system-class-important` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-important
  match access-group name copp-system-p-acl-hsrp
  match access-group name copp-system-p-acl-vrrp match
  access-group name copp-system-p-acl-hsrp6 match
  access-group name copp-system-p-acl-vrrp6 match
  access-group name copp-system-p-acl-mac-lldp
```

The `copp-system-class-l2-default` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-l2-default
  match access-group name copp-system-p-acl-mac-undesirable
```

The `copp-system-class-l2-unpoliced` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-l2-
  unpoliced match access-group name copp-system-p-acl-mac-stp
  match access-group name copp-system-p-acl-mac-lacp match
  access-group name copp-system-p-acl-mac-cfsoe match
  access-group name copp-system-p-acl-mac-sdp-srp match
  access-group name copp-system-p-acl-mac-l2-tunnel
  match access-group name copp-system-p-acl-mac-cdp-udld-vtp
```

The `copp-system-class-l3mc-data` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-l3mc-data
  match exception multicast rpf-failure
  match exception multicast dest-miss
```

The `copp-system-class-l3uc-data` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-l3uc-data
  match exception glean
```

The `copp-system-class-management` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-management
  match access-group name copp-system-p-acl-ftp
  match access-group name copp-system-p-acl-ntp
  match access-group name copp-system-p-acl-ssh
  match access-group name copp-system-p-acl-http
  match access-group name copp-system-p-acl-ntp6
  match access-group name copp-system-p-acl-sftp
  match access-group name copp-system-p-acl-snmp
  match access-group name copp-system-p-acl-ssh6
  match access-group name copp-system-p-acl-tftp

  match access-group name copp-system-p-acl-https
  match access-group name copp-system-p-acl-snmp6
  match access-group name copp-system-p-acl-tftp6
  match access-group name copp-system-p-acl-radius
  match access-group name copp-system-p-acl-tacacs
  match access-group name copp-system-p-acl-telnet
  match access-group name copp-system-p-acl-radius6
```

```
match access-group name copp-system-p-acl-tacacs6
match access-group name copp-system-p-acl-telnet6
```

The `copp-system-class-monitoring` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-
monitoring match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6 match
access-group name copp-system-p-acl-traceroute
```

The `copp-system-class-multicast-host` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-multicast-
host match access-group name copp-system-p-acl-mld
```

The `copp-system-class-multicast-router` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-multicast-
router match access-group name copp-system-p-acl-pim
match access-group name copp-system-p-acl-msdp match
access-group name copp-system-p-acl-pim6 match
access-group name copp-system-p-acl-pim-reg match
access-group name copp-system-p-acl-pim6-reg
match access-group name copp-system-p-acl-pim-mdt-join
```

The `copp-system-class-nat-flow` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-nat-flow
match exception nat-flow
```

The `copp-system-class-ndp` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-ndp
match access-group name copp-system-p-acl-ndp
```

The `copp-system-class-normal` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-
normal match access-group name copp-system-p-acl-mac-dot1x
match protocol arp
```

The `copp-system-class-normal-dhcp` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-normal-
dhcp match access-group name copp-system-p-acl-dhcp
match access-group name copp-system-p-acl-dhcp6
```

The `copp-system-class-normal-dhcp-relay-response` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-normal-dhcp-relay-
response match access-group name copp-system-p-acl-dhcp-relay-response
match access-group name copp-system-p-acl-dhcp6-relay-response
```


The `copp-system-class-normal-igmp` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-normal-igmp
  match access-group name copp-system-p-acl-igmp
```

The `copp-system-class-redirect` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-redirect
  match access-group name copp-system-p-acl-ntp
```

The `copp-system-class-undesirable` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-undesirable
  match access-group name copp-system-p-acl-undesirable
  match exception multicast sg-rpf-failure
```

The `copp-system-class-fcoe` class has the following configuration:

```
class-map type control-plane match-any copp-system-p-class-
  fcoe match access-group name copp-system-p-acl-mac-fcoe
```

```
class copp-system-p-class-normal-dhcp-relay-
  response set cos 1
  police cir 1500 kbps bc 64000 bytes conform transmit violate
  drop class copp-system-p-class-normal-igmp
  set cos 3
  police cir 3000 kbps bc 64000 bytes conform transmit violate
  drop class copp-system-p-class-redirect
  set cos 1
  police cir 280 kbps bc 32000 bytes conform transmit violate
  drop class copp-system-p-class-exception
  set cos 1
  police cir 150 kbps bc 32000 bytes conform transmit violate
  drop class copp-system-p-class-exception-dia
  set cos 1
  police cir 150 kbps bc 32000 bytes conform transmit violate
  drop class copp-system-p-class-monitoring
  set cos 1
  police cir 150 kbps bc 128000 bytes conform transmit violate
  drop class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 50 mbps bc 8192000 bytes conform transmit violate
  drop class copp-system-p-class-undesirable
  set cos 0
  police cir 200 kbps bc 32000 bytes conform transmit violate
  drop class copp-system-p-class-nat-flow
  set cos 7
  police cir 800 kbps bc 64000 bytes conform transmit violate
  drop class copp-system-p-class-l2-default
  set cos 0
  police cir 400 kbps bc 32000 bytes conform transmit violate
  drop class class-default
  set cos 0
```

```
police cir 400 kbps bc 32000 bytes conform transmit violate drop
```

On Inspur CN12900 Series switches, the strict CoPP policy has the following configuration:

```
policy-map type control-plane copp-system-p-policy-
strict class copp-system-p-class-l3uc-data
  set cos 1
  police cir 250 pps bc 32 packets conform transmit violate
drop class copp-system-p-class-critical
  set cos 7
  police cir 19000 pps bc 128 packets conform transmit violate
drop class copp-system-p-class-important
  set cos 6
  police cir 3000 pps bc 128 packets conform transmit violate
drop class copp-system-p-class-multicast-router
  set cos 6
  police cir 3000 pps bc 128 packets conform transmit violate
drop class copp-system-p-class-management
  set cos 2
  police cir 3000 pps bc 32 packets conform transmit violate
drop class copp-system-p-class-multicast-host
  set cos 1
  police cir 2000 pps bc 128 packets conform transmit violate
drop class copp-system-p-class-l3mc-data
  set cos 1
  police cir 3000 pps bc 32 packets conform transmit violate
drop class copp-system-p-class-normal
  set cos 1
  police cir 1500 pps bc 32 packets conform transmit violate
drop class copp-system-p-class-ndp
  set cos 6

  police cir 1500 pps bc 32 packets conform transmit violate
drop class copp-system-p-class-normal-dhcp
  set cos 1
  police cir 300 pps bc 32 packets conform transmit violate
drop class copp-system-p-class-normal-dhcp-relay-response
  set cos 1
  police cir 400 pps bc 64 packets conform transmit violate
drop class copp-system-p-class-normal-igmp
  set cos 3
  police cir 6000 pps bc 64 packets conform transmit violate
drop class copp-system-p-class-redirect
  set cos 1
  police cir 1500 pps bc 32 packets conform transmit violate
drop class copp-system-p-class-exception
  set cos 1
  police cir 50 pps bc 32 packets conform transmit violate
drop class copp-system-p-class-exception-diag
  set cos 1
  police cir 50 pps bc 32 packets conform transmit violate
drop class copp-system-p-class-monitoring
  set cos 1
  police cir 300 pps bc 128 packets conform transmit violate
drop class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 20000 pps bc 8192 packets conform transmit violate
drop class copp-system-p-class-undesirable
  set cos 0
  police cir 15 pps bc 32 packets conform transmit violate
drop class copp-system-p-class-fcoe
```

```

    set cos 6
    police cir 1500 pps bc 128 packets conform transmit violate
drop class copp-system-p-class-nat-flow
    set cos 7
    police cir 100 pps bc 64 packets conform transmit violate
drop class copp-system-p-class-l2-default
    set cos 0
    police cir 50 pps bc 32 packets conform transmit violate
drop class class-default
    set cos 0
    police cir 50 pps bc 32 packets conform transmit violate drop

    police cir 1000 kbps bc 192000 bytes conform transmit violate
drop class copp-system-p-class-l3mc-data
    set cos 1
    police cir 2400 kbps bc 32000 bytes conform transmit violate
drop class copp-system-p-class-normal
    set cos 1
    police cir 1400 kbps bc 48000 bytes conform transmit violate
drop class copp-system-p-class-ndp
    set cos 6
    police cir 1400 kbps bc 48000 bytes conform transmit violate
drop class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 1300 kbps bc 48000 bytes conform transmit violate
drop class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 1500 kbps bc 96000 bytes conform transmit violate
drop class copp-system-p-class-normal-igmp
    set cos 3
    police cir 3000 kbps bc 64000 bytes conform transmit violate
drop class copp-system-p-class-redirect
    set cos 1
    police cir 280 kbps bc 48000 bytes conform transmit violate
drop class copp-system-p-class-exception
    set cos 1
    police cir 150 kbps bc 48000 bytes conform transmit violate
drop class copp-system-p-class-exception-diag
    set cos 1
    police cir 150 kbps bc 48000 bytes conform transmit violate
drop class copp-system-p-class-monitoring
    set cos 1
    police cir 150 kbps bc 192000 bytes conform transmit violate
drop class copp-system-p-class-l2-unpoliced
    set cos 7
    police cir 50 mbps bc 8192000 bytes conform transmit violate
drop class copp-system-p-class-undesirable
    set cos 0
    police cir 200 kbps bc 48000 bytes conform transmit violate
drop class copp-system-p-class-nat-flow
    set cos 7
    police cir 800 kbps bc 64000 bytes conform transmit violate
drop class copp-system-p-class-l2-default
    set cos 0
    police cir 400 kbps bc 48000 bytes conform transmit violate
drop class class-default
    set cos 0
    police cir 400 kbps bc 48000 bytes conform transmit violate drop

```

On Inspur CN129000 switches, the moderate CoPP policy has the following configuration:

```
policy-map type control-plane copp-system-p-policy-
```

```
moderate class copp-system-p-class-l3uc-data
  set cos 1
  police cir 250 pps bc 32 packets conform transmit violate
drop class copp-system-p-class-critical
  set cos 7
  police cir 19000 pps bc 192 packets conform transmit violate
drop class copp-system-p-class-important
  set cos 6
  police cir 3000 pps bc 192 packets conform transmit violate
drop class copp-system-p-class-multicast-router
  set cos 6
  police cir 3000 pps bc 192 packets conform transmit violate
drop class copp-system-p-class-management

  set cos 2
  police cir 3000 pps bc 48 packets conform transmit violate
drop class copp-system-p-class-multicast-host
  set cos 1
  police cir 2000 pps bc 192 packets conform transmit violate
drop class copp-system-p-class-l3mc-data
  set cos 1
  police cir 3000 pps bc 32 packets conform transmit violate
drop class copp-system-p-class-normal
  set cos 1
  police cir 1500 pps bc 48 packets conform transmit violate
drop class copp-system-p-class-ndp
  set cos 6
  police cir 1500 pps bc 48 packets conform transmit violate
drop class copp-system-p-class-normal-dhcp
  set cos 1
  police cir 300 pps bc 48 packets conform transmit violate
drop class copp-system-p-class-normal-dhcp-relay-response
  set cos 1
  police cir 400 pps bc 96 packets conform transmit violate
drop class copp-system-p-class-normal-igmp
  set cos 3
  police cir 6000 pps bc 64 packets conform transmit violate
drop class copp-system-p-class-redirect
  set cos 1
  police cir 1500 pps bc 48 packets conform transmit violate
drop class copp-system-p-class-exception
  set cos 1
  police cir 50 pps bc 48 packets conform transmit violate
drop class copp-system-p-class-exception-diag
  set cos 1
  police cir 50 pps bc 48 packets conform transmit violate
drop class copp-system-p-class-monitoring
  set cos 1
  police cir 300 pps bc 192 packets conform transmit violate
drop class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 20000 pps bc 8192 packets conform transmit violate
drop class copp-system-p-class-undesirable
  set cos 0
  police cir 15 pps bc 48 packets conform transmit violate
drop class copp-system-p-class-fcoe
  set cos 6
  police cir 1500 pps bc 192 packets conform transmit violate
drop class copp-system-p-class-nat-flow
  set cos 7
  police cir 100 pps bc 64 packets conform transmit violate
drop class copp-system-p-class-l2-default
  set cos 0
```

```

    police cir 50 pps bc 48 packets conform transmit violate
drop class class-default
    set cos 0
    police cir 50 pps bc 48 packets conform transmit violate drop

```

Lenient Default CoPP Policy

```

    set cos 7
    police cir 36000 kbps bc 2560000 bytes conform transmit violate
drop class copp-system-p-class-important
    set cos 6
    police cir 2500 kbps bc 2560000 bytes conform transmit violate
drop class copp-system-p-class-multicast-router
    set cos 6
    police cir 2600 kbps bc 256000 bytes conform transmit violate
drop class copp-system-p-class-management
    set cos 2
    police cir 10000 kbps bc 64000 bytes conform transmit violate
drop class copp-system-p-class-multicast-host
    set cos 1
    police cir 1000 kbps bc 256000 bytes conform transmit violate
drop class copp-system-p-class-l3mc-data
    set cos 1
    police cir 2400 kbps bc 32000 bytes conform transmit violate
drop class copp-system-p-class-normal
    set cos 1
    police cir 1400 kbps bc 64000 bytes conform transmit violate
drop class copp-system-p-class-ndp
    set cos 6
    police cir 1400 kbps bc 64000 bytes conform transmit violate
drop class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 1300 kbps bc 64000 bytes conform transmit violate
drop class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 1500 kbps bc 128000 bytes conform transmit violate
drop class copp-system-p-class-normal-igmp
    set cos 3
    police cir 3000 kbps bc 64000 bytes conform transmit violate
drop class copp-system-p-class-redirect
    set cos 1
    police cir 280 kbps bc 64000 bytes conform transmit violate
drop class copp-system-p-class-exception
    set cos 1
    police cir 150 kbps bc 64000 bytes conform transmit violate
drop class copp-system-p-class-exception-diag
    set cos 1
    police cir 150 kbps bc 64000 bytes conform transmit violate
drop class copp-system-p-class-monitoring
    set cos 1
    police cir 150 kbps bc 256000 bytes conform transmit violate
drop class copp-system-p-class-l2-unpoliced
    set cos 7
    police cir 50 mbps bc 8192000 bytes conform transmit violate
drop class copp-system-p-class-undesirable
    set cos 0
    police cir 200 kbps bc 64000 bytes conform transmit violate
drop class copp-system-p-class-nat-flow
    set cos 7
    police cir 800 kbps bc 64000 bytes conform transmit violate
drop class copp-system-p-class-l2-default
    set cos 0
    police cir 400 kbps bc 64000 bytes conform transmit violate

```

```

drop class class-default
  set cos 0
  police cir 400 kbps bc 64000 bytes conform transmit violate drop

```

n:

```

policy-map type control-plane copp-system-p-policy-lenient
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 250 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 19000 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 3000 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 3000 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 3000 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 2000 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 3000 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 1500 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 6
    police cir 1500 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 300 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 400 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-normal-igmp
    set cos 3
    police cir 6000 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 1500 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 50 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-exception-diag
    set cos 1
    police cir 50 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 300 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    set cos 7
    police cir 20000 pps bc 8192 packets conform transmit violate drop
  class copp-system-p-class-undesirable
    set cos 0
    police cir 15 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-fcoe
    set cos 6
    police cir 1500 pps bc 256 packets conform transmit violate drop

```

```

class copp-system-p-class-nat-flow
  set cos 7
  police cir 100 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-l2-default
  set cos 0
  police cir 50 pps bc 64 packets conform transmit violate drop

class class-default
  set cos 0
  police cir 50 pps bc 64 packets conform transmit violate drop

```

Dense Default CoPP Policy

On Inspur CN12900 Series switches, the dense CoPP policy has the following configuration:

```

policy-map type control-plane copp-system-p-policy-
dense class copp-system-p-class-l3uc-data
  set cos 1
  police cir 800 kbps bc 32000 bytes conform transmit violate
drop class copp-system-p-class-critical
  set cos 7
  police cir 4500 kbps bc 1280000 bytes conform transmit violate
drop class copp-system-p-class-important
  set cos 6
  police cir 2500 kbps bc 1280000 bytes conform transmit violate
drop class copp-system-p-class-multicast-router
  set cos 6
  police cir 370 kbps bc 128000 bytes conform transmit violate
drop class copp-system-p-class-management
  set cos 2
  police cir 2500 kbps bc 128000 bytes conform transmit violate
drop class copp-system-p-class-multicast-host
  set cos 2
  police cir 300 kbps bc 128000 bytes conform transmit violate
drop class copp-system-p-class-l3mc-data
  set cos 1
  police cir 600 kbps bc 32000 bytes conform transmit violate
drop class copp-system-p-class-normal
  set cos 1
  police cir 1400 kbps bc 128000 bytes conform transmit violate
drop class copp-system-p-class-ndp
  set cos 1
  police cir 350 kbps bc 32000 bytes conform transmit violate
drop class copp-system-p-class-normal-dhcp
  set cos 1
  police cir 750 kbps bc 128000 bytes conform transmit violate
drop class copp-system-p-class-normal-dhcp-relay-response
  set cos 1
  police cir 750 kbps bc 128000 bytes conform transmit violate
drop class copp-system-p-class-normal-igmp
  set cos 3
  police cir 1400 kbps bc 128000 bytes conform transmit violate
drop class copp-system-p-class-redirect
  set cos 1
  police cir 200 kbps bc 32000 bytes conform transmit violate
drop class copp-system-p-class-exception
  set cos 1
  police cir 200 kbps bc 32000 bytes conform transmit violate
drop class copp-system-p-class-exception-diag
  set cos 1
  police cir 200 kbps bc 32000 bytes conform transmit violate

```

```

drop class copp-system-p-class-monitoring
  set cos 1
  police cir 150 kbps bc 128000 bytes conform transmit violate
drop class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 50 mbps bc 8192000 bytes conform transmit violate
drop class copp-system-p-class-undesirable
  set cos 0
  police cir 100 kbps bc 32000 bytes conform transmit violate drop

class copp-system-p-class-l2-default
  set cos 0
  police cir 200 kbps bc 32000 bytes conform transmit violate drop
class class-default
  set cos 0
  police cir 200 kbps bc 32000 bytes conform transmit violate drop

```

On Inspur CN12900 Series switches, the dense CoPP policy has the following configuration:

```

policy-map type control-plane copp-system-p-policy-dense
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 250 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 2500 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 1200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 1200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 1200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 2
    police cir 1000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 1200 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 750 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 1
    police cir 750 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 150 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-normal-igmp
    set cos 3
    police cir 2500 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 1500 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1

```



```

    police cir 50 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-exception-dia
  set cos 1
  police cir 50 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-monitoring
  set cos 1
  police cir 50 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 20000 pps bc 8192 packets conform transmit violate drop
class copp-system-p-class-undesirable
  set cos 0

```

```

    police cir 15 pps bc 32 packets conform transmit violate
drop class copp-system-p-class-fcoe
  set cos 6
  police cir 750 pps bc 128 packets conform transmit violate
drop class copp-system-p-class-l2-default
  set cos 0
  police cir 25 pps bc 32 packets conform transmit violate
drop class class-default
  set cos 0
  police cir 25 pps bc 32 packets conform transmit violate drop

```

Packets Per Second Credit Limit

The aggregate packets per second (PPS) for a given policy (sum of PPS of each class part of the policy) is capped by an upper PPS Credit Limit (PCL). If an increase in PPS of a given class causes a PCL exceed, the configuration is rejected. To increase the desired PPS, the additional PPS beyond PCL should be decreased from other class(es).

11.1.2 Modular QoS Command-Line Interface

CoPP uses the Modular Quality of Service Command-Line Interface (MQC). MQC is a CLI structure that allows you to define a traffic class, create a traffic policy (policy map), and attach the traffic policy to an interface. The traffic policy contains the CoPP feature that will be applied to the traffic class.

SUMMARY STEPS

1. Define a traffic class using the **class-map** command. A traffic class is used to classify traffic.
2. Create a traffic policy using the **policy-map** command. A traffic policy (policy map) contains a traffic class and one or more CoPP features that will be applied to the traffic class. The CoPP features in the traffic policy determine how to treat the classified traffic.
3. Attach the traffic policy (policy map) to the control plane using the **control-plane** and **service-policy** commands.

DETAILED STEPS

Step 1 Define a traffic class using the **class-map** command. A traffic class is used to classify traffic. This example shows how to create a new class-map called copp-sample-class:

```
class-map type control-plane copp-sample-class
```

Step 2 Define a traffic policy using the **policy-map** command. A traffic policy (policy map) contains a traffic class and one or more CoPP features that will be applied to the traffic class. The CoPP features in the traffic policy determine how to treat the classified traffic.

Step 3 Attach the traffic policy (policy map) to the control plane using the **control-plane** and **service-policy** commands.

This example shows how to attach the policy map to the control plane:

```
control-plane
service-policy input copp-system-policy
```

Note The copp-system-policy is always configured and applied. There is no need to use this command explicitly.

11.1.3 CoPP and the Management Interface

The Inspur INOS-CN device supports only hardware-based CoPP, which does not support the management interface (mgmt0). The out-of-band mgmt0 interface connects directly to the CPU and does not pass through the in-band traffic hardware where CoPP is implemented.

On the mgmt0 interface, ACLs can be configured to give or deny access to a particular type of traffic.

11.2 Licensing Requirements for CoPP

The following table shows the licensing requirements for this feature:

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

11.3 Guidelines and Limitations for CoPP

CoPP has the following configuration guidelines and limitations:

- We recommend that you use the strict default CoPP policy initially and then later modify the CoPP policies based on the data center and application requirements.
- Customizing CoPP is an ongoing process. CoPP must be configured according to the protocols and features used in your specific environment as well as the supervisor features that are required by the server environment. As these protocols and features change, CoPP must be modified.
- We recommend that you continuously monitor CoPP. If drops occur, determine if CoPP dropped traffic unintentionally or in response to a malfunction or attack. In either event, analyze the situation and evaluate the need to modify the CoPP policies.
- All the traffic that you do not specify in the other class maps is put into the last class, the default class. Monitor the drops in this class and investigate if these drops are based on traffic that you do not want or the result of a feature that was not configured and you need to add.
- All broadcast traffic is sent through CoPP logic in order to determine which packets (for example, ARP and DHCP) need to be redirected through an access control list (ACL) to the router processor. Broadcast traffic that does not need to be redirected is matched against the CoPP logic, and both conforming and violated packets are counted in the hardware but not sent to the CPU. Broadcast traffic that needs to be sent to the CPU and broadcast traffic that does not need to be sent to the CPU must be separated into different classes.
- After you have configured CoPP, delete anything that is not being used, such as old class maps and unused routing protocols.
- You must ensure that the CoPP policy does not filter critical traffic such as routing protocols or interactive access to the device. Filtering this traffic could prevent remote access to the Inspur INOS-CN device and

- require a console connection.
- The Inspur INOS-CN software does not support egress CoPP or silent mode. CoPP is supported only on ingress (you cannot use the **service-policy output copp** command to the control plane interface).
 - You can use the access control entry (ACE) hit counters in the hardware only for ACL logic. Use the software ACE hit counters and the **show access-lists** and **show policy-map type control-plane** commands to evaluate CPU traffic.
 - The Inspur INOS-CN device hardware performs CoPP on a per-forwarding-engine basis. CoPP does not support distributed policing. Therefore, you should choose rates so that the aggregate traffic does not overwhelm the supervisor module.
 - If multiple flows map to the same class, individual flow statistics will not be available.
 - If you upgrade from a Inspur INOS-CN release that supports the CoPP feature to a Inspur INOS-CN release that supports the CoPP feature with additional classes for new protocols, you must either run the setup utility using the **setup** command or use the **copp profile** command for the new CoPP classes to be available.
 - Before you downgrade from a Inspur INOS-CN release that supports the CoPP feature to an earlier Inspur INOS-CN release that supports the CoPP feature, you should verify compatibility using the **show incompatibility INOS bootflash:filename** command. If an incompatibility exists, disable any features that are incompatible with the downgrade image before downgrading the software.
 - You cannot disable CoPP. If you attempt to disable it, packets are rate limited at 50 packets per seconds.
 - The following guidelines and limitations apply to static CoPP ACLs:
 - Static CoPP ACLs can be remapped to a different CoPP class.
 - Access control entries (ACEs) cannot be modified or removed for static CoPP ACLs.
 - If a CoPP ACL has a static ACL substring, it will be mapped to that type of traffic. For example, if the ACL includes the `acl-mac-stp` substring, STP traffic will be classified to the class map for that ACL.
 - Static CoPP ACLs take priority over dynamic CoPP ACLs, regardless of their position in the CoPP policy, the order in which they are configured, and how they appear in the output of the `show policy-map type control-plane` command.
 - You must have static CoPP ACLs in the CoPP policy. Otherwise, the CoPP policy will be rejected.

11.4 Default Settings for CoPP

This table lists the default settings for CoPP parameters.

Table 21 : Default CoPP Parameters Settings

Parameters	Default
Default policy	Strict
Default policy	9 policy entries Note The maximum number of supported policies with associated class maps is 128.
Scale factor value	1.00

11.5 Configuring CoPP

This section describes how to configure CoPP.

11.5.1 Configuring a Control Plane Class Map

You must configure control plane class maps for control plane policies.

You can classify traffic by matching packets based on existing ACLs. The permit and deny ACL keywords are ignored in the matching.

You can configure policies for IP version 4 (IPv4) and IP version 6 (IPv6) packets.

Before you begin

Ensure that you have configured the IP ACLs if you want to use ACE hit counters in the class maps.

SUMMARY STEPS

1. **configure terminal**
2. **class-map type control-plane [match-all | match-any] class-map-name**
3. (Optional) **match access-group name access-list-name**
4. (Optional) **match exception {ip | ipv6} icmp redirect**
5. (Optional) **match exception {ip | ipv6} icmp unreachable**
6. (Optional) **match exception {ip | ipv6} option**
7. **match protocol arp**
8. **exit**
9. (Optional) **show class-map type control-plane [class-map-name]**
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	class-map type control-plane [match-all match-any] class-map-name Example: <pre>switch(config)# class-map type control-plane ClassMapA switch(config-cmap)#</pre>	Specifies a control plane class map and enters class map configuration mode. The default class matching is match-any. The name can be a maximum of 64 characters long and is case sensitive. Note You cannot use class-default, match-all, or match-any as class map names.
Step 3	(Optional) match access-group name access-list-name Example: <pre>switch(config-cmap)# match access-group name MyAccessList</pre>	Specifies matching for an IP ACL. Note The permit and deny ACL keywords are ignored in the CoPP matching.
Step 4	(Optional) match exception {ip ipv6} icmp redirect Example: <pre>switch(config-cmap)# match exception ip icmp</pre>	Specifies matching for IPv4 or IPv6 ICMP redirect exception packets.

	Command or Action	Purpose
	<code>redirect</code>	
Step 5	(Optional) match exception {ip ipv6} icmp unreachable Example: <code>switch(config-cmap)# match exception ip icmp unreachable</code>	Specifies matching for IPv4 or IPv6 ICMP unreachable exception packets.
Step 6	(Optional) match exception {ip ipv6} option Example: <code>switch(config-cmap)# match exception ip option</code>	Specifies matching for IPv4 or IPv6 option exception packets.
Step 7	match protocol arp Example: <code>switch(config-cmap)# match protocol arp</code>	Specifies matching for IP Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP) packets.
Step 8	exit Example: <code>switch(config-cmap)# exit</code> <code>switch(config)#</code>	Exits class map configuration mode.
Step 9	(Optional) show class-map type control-plane [class-map-name] Example: <code>switch(config)# show class-map type control-plane</code>	Displays the control plane class map configuration.
Step 10	(Optional) copy running-config startup-config Example: <code>switch(config)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

11.5.2 Configuring a Control Plane Policy Map

You must configure a policy map for CoPP, which includes policing parameters. If you do not configure a policer for a class, the following default is configured:

- 50 packets per second (pps) with a burst of 32 packets.
- 150 kilobits per second (kbps) with a burst of 32,000 bytes (

Before you begin

Ensure that you have configured a control plane class map.

SUMMARY STEPS

1. **configure terminal**
2. **policy-map type control-plane *policy-map-name***

3. **class** {*class-map-name* [**insert-before** *class-map-name2*] | **class-default**}
4. Enter one of the following commands:
 - **police** [**cir**] {*cir-rate* [*rate-type*]}
 - **police** [**cir**] {*cir-rate* [*rate-type*] [**bc**] *burst-size* [*burst-size-type*]}
 - **police** [**cir**] {*cir-rate* [*rate-type*] [**conform transmit**] [*violate drop*]}
5. (Optional) **logging drop threshold** [*drop-count* [*level syslog-level*]]
6. (Optional) **set cos** *cos-value*
7. **exit**
8. **exit**
9. (Optional) **show policy-map type control-plane** [**expand**] [**name** *class-map-name*]
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	policy-map type control-plane <i>policy-map-name</i> Example: <pre>switch(config)# policy-map type control- plane ClassMapA switch(config-pmap)#</pre>	Specifies a control plane policy map and enters policy map configuration mode. The policy map name can have a maximum of 64 characters and is case sensitive.
Step 3	class { <i>class-map-name</i> [insert-before <i>class-map-name2</i>] class-default }	Specifies a control plane class map name or the class default and enters control plane class configuration mode. The class-default class map is always at the end of the class map list for a policy map.
Step 4	Enter one of the following commands: <ul style="list-style-type: none"> • police [cir] {<i>cir-rate</i> [<i>rate-type</i>]} • police [cir] {<i>cir-rate</i> [<i>rate-type</i>] [bc] <i>burst-size</i>} • police [cir] {<i>cir-rate</i> [<i>rate-type</i>] [conform transmit] [<i>violate drop</i>]} Example: <pre>switch(config-pmap-c)# police cir 52000 bc 1000 packets</pre> Example:	Specifies the committed information rate (CIR). The rate range is as follows: <ul style="list-style-type: none"> • 0 to 268435456 pps (for Inspur CN129000) • 0 to 80000000000 bps/gbps/kbps/mbps Note The CIR rate range starts with 0. In previous releases, the CIR rate range starts with 1.

	Command or Action	Purpose
Step 5	<pre>switch(config-pmap-c)# police cir 3400 kbps bc 200 kbytes</pre> <p>(Optional) logging drop threshold [<i>drop-count</i> [<i>level</i> [<i>syslog-level</i>]]]</p> <p>Example:</p> <pre>switch(config-pmap-c)# logging drop threshold 100</pre>	<p>A value of 0 drops the packet.</p> <p>The committed burst (BC) range is as follows:</p> <ul style="list-style-type: none"> • 1 to 1073741 packets <p>The conform transmit action transmits the packet.</p> <p>Note You can specify the BC and conform action for the same CIR.</p> <p>Specifies the threshold value for dropped packets and generates a syslog if the drop count exceeds the configured threshold. The range for the <i>drop-count</i> argument is from 1 to 8000000000 bytes. The range for the <i>syslog-level</i> argument is from 1 to 7, and the default level is 4.</p>
Step 6	<p>(Optional) set cos <i>cos-value</i></p> <p>Example:</p> <pre>switch(config-pmap-c)# set cos 1</pre>	<p>Specifies the 802.1Q class of service (CoS) value. The range is from 0 to 7. The default value is 0.</p>
Step 7	<p>exit</p> <p>Example:</p> <pre>switch(config-pmap-c)# exit switch(config-pmap)#</pre>	<p>Exits policy map class configuration mode.</p>
Step 8	<p>exit</p> <p>Example:</p> <pre>switch(config-pmap)# exit switch(config)#</pre>	<p>Exits policy map configuration mode.</p>
Step 9	<p>(Optional) show policy-map type control-plane [expand] [<i>name class-map-name</i>]</p> <p>Example:</p> <pre>switch(config)# show policy-map type control- plane</pre>	<p>Displays the control plane policy map configuration.</p>
Step 10	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config)# copy running-config startup- config</pre>	<p>Copies the running configuration to the startup configuration.</p>

11.5.3 Configuring the Control Plane Service Policy

You can configure one or more policy maps for the CoPP service policy.

Before you begin

Ensure that you have configured a control plane policy map.

SUMMARY STEPS

1. **configure terminal**
2. **control-plane**
3. **[no] service-policy input** *policy-map-name*
4. **exit**
5. (Optional) **show running-config copp [all]**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	control-plane Example: switch(config)# control-plane switch(config-cp)#	Enters control plane configuration mode.
Step 3	[no] service-policy input <i>policy-map-name</i> Example: switch(config-cp)# service-policy input PolicyMapA	Specifies a policy map for the input traffic. Repeat this step if you have more than one policy map. You cannot disable CoPP. If you enter the no form of this command, packets are rate limited at 50 packets per seconds.
Step 4	exit Example: switch(config-cp)# exit switch(config)#	Exits control plane configuration mode.
Step 5	(Optional) show running-config copp [all] Example: switch(config)# show running-config copp	Displays the CoPP configuration.
Step 6	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

11.5.4 Configuring the CoPP Scale Factor Per Line Card

You can configure the CoPP scale factor per line card.

The scale factor configuration is used to scale the policer rate of the applied CoPP policy for a particular line card. The accepted value is from 0.10 to 2.00. You can increase or reduce the policer rate for a particular line card without changing the current CoPP policy. The changes are effective immediately, so you do not need to reapply the CoPP policy.

SUMMARY STEPS

1. **configure terminal**
2. **control-plane**
3. **scale-factor** *value* **module** *multiple-module-range*
4. (Optional) **show policy-map interface control-plane**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	control-plane Example: <pre>switch(config)# control-plane switch(config-cp)#</pre>	Enters control plane configuration mode.
Step 3	scale-factor <i>value</i> module <i>multiple-module-range</i> Example: <pre>switch(config-cp)# scale-factor 1.10 module 1-2</pre>	Configures the policer rate per line card. The allowed scale factor value is from 0.10 to 2.00. When the scale factor value is configured, the policing values are multiplied by the corresponding scale factor value of the module, and it is programmed in the particular module. To revert to the default scale factor value of 1.00, use the no scale-factor <i>value</i> module <i>multiple-module-range</i> command, or explicitly set the default scale factor value to 1.00 using the scale-factor 1 module <i>multiple-module-range</i> command.
Step 4	(Optional) show policy-map interface control-plane Example: <pre>switch(config-cp)# show policy-map interface</pre>	Displays the applied scale factor values when a CoPP policy is applied.

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

11.5.5 Changing or Reapplying the Default CoPP Policy

You can change to a different default CoPP policy, or you can reapply the same default CoPP policy.

SUMMARY STEPS

1. `[no] copp profile [strict | moderate | lenient | dense]`
2. (Optional) `show copp status`
3. (Optional) `show running-config copp`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>[no] copp profile [strict moderate lenient dense]</code> Example: <code>switch(config)# copp profile moderate</code>	Applies the CoPP best practice policy. You cannot disable CoPP. If you enter the no form of this command, packets are rate limited at 50 packets per seconds.
Step 2	(Optional) <code>show copp status</code> Example: <code>switch(config)# show copp status</code>	Displays the CoPP status, including the last configuration operation and its status. This command also enables you to verify that the CoPP best practice policy is attached to the control plane.
Step 3	(Optional) <code>show running-config copp</code> Example: <code>switch(config)# show running-config copp</code>	Displays the CoPP configuration in the running configuration.

11.5.6 Copying the CoPP Best Practice Policy

The CoPP best practice policy is read-only. If you want to modify its configuration, you must copy it.

SUMMARY STEPS

1. `copp copy profile {strict | moderate | lenient | dense} {prefix | suffix} string`
2. (Optional) `show copp status`
3. (Optional) `show running-config copp`

DETAILED STEPS

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

Step 1	copp copy profile {strict moderate lenient dense} {prefix suffix} <i>string</i> Example: switch# copp copy profile strict prefix abc	Creates a copy of the CoPP best practice policy. CoPP renames all class maps and policy maps with the specified prefix or suffix.
Step 2	(Optional) show copp status Example: switch# show copp status	Displays the CoPP status, including the last configuration operation and its status. This command also enables you to verify that the copied policy is not attached to the control plane.
Step 3	(Optional) show running-config copp Example: switch# show running-config copp	Displays the CoPP configuration in the running configuration, including the copied policy configuration.

11.6 Verifying the CoPP Configuration

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

Command	Purpose
show policy-map type control-plane [expand] [name] <i>policy-map-name</i>	Displays the control plane policy map with associated class maps and CIR and BC values.
show policy-map interface control-plane	Displays the policy values with associated class maps and drops per policy or class map. It also displays the scale factor values when a CoPP policy is applied. When the scale factor value is the default (1.00), it is not displayed. Note The scale factor changes the CIR and BC values internally on each module, but the display shows the configured CIR and BC values only. The actual applied value on a module is the scale factor multiplied by the configured value.
show class-map type control-plane [<i>class-map-name</i>]	Displays the control plane class

Command	Purpose
	map configuration, including the ACLs that are bound to this class map.
show copp diff profile {strict moderate lenient dense} [prior-ver] profile {strict moderate lenient dense} show copp diff profile	Displays the difference between two CoPP best practice policies. When you do not include the prior-ver option, this command displays the difference between two currently applied default CoPP best practice policies (such as the currently applied strict and currently applied moderate policies). When you include the prior-ver option, this command displays the difference between a currently applied default CoPP best practice policy and a previously applied default CoPP best practice policy (such as the currently applied strict and the previously applied lenient policies).
show copp profile {strict moderate lenient dense}	Displays the details of the CoPP best practice policy, along with the classes and policer values.
show running-config aclmgr [all]	Displays the user-configured access control lists (ACLs) in the running configuration. The all option displays both the default (CoPP-configured) and user-configured ACLs in the running configuration.
show running-config copp [all]	Displays the CoPP configuration in the running configuration.
show startup-config aclmgr [all]	Displays the user-configured access control lists (ACLs) in the startup configuration. The all option displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration.

11.7 Displaying the CoPP Configuration Status

SUMMARY STEPS

1. switch# **show copp status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# show copp status	Displays the configuration status for the CoPP feature.

Example

This example shows how to display the CoPP configuration status:

```
switch# show copp status
```

11.8 Monitoring CoPP

SUMMARY STEPS

1. switch# **show policy-map interface control-plane**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# show policy-map interface control-plane	Displays packet-level statistics for all classes that are part of the applied CoPP policy. Statistics are specified in terms of OutPackets (packets admitted to the control plane) and DropPackets (packets dropped because of rate limiting).

Example

This example shows how to monitor CoPP:

```
switch# show policy-map interface control-plane
Control Plane
  Service-policy   input: copp-system-p-policy-strict
    class-map copp-system-p-class-critical (match-
      any) set cos 7
      police cir 19000 pps , bc 128
      packets module 4 :
        transmitted 373977
        packets; dropped 0
        packets;
```

11.9 Clearing the CoPP Statistics

SUMMARY STEPS

1. (Optional) switch# **show policy-map interface control-plane**
2. switch# **clear copp statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) switch# show policy-map interface control-plane	Displays the currently applied CoPP policy and per-class statistics.
Step 2	switch# clear copp statistics	Clears the CoPP statistics.

Example

This example shows how to clear the CoPP statistics for your installation:

```
switch# show policy-map interface control-plane
switch# clear copp statistics
```

11.10 Configuration Examples for CoPP

This section includes example CoPP configurations.

11.10.1 CoPP Configuration Example

The following example shows how to configure CoPP using IP ACLs and MAC ACLs:

```
configure terminal
ip access-list copp-system-p-acl-igmp permit igmp any 10.0.0.0/24
ip access-list copp-system-p-acl-msdp permit tcp any any eq 639
mac access-list copp-system-p-acl-arp permit any any 0x0806
ip access-list copp-system-p-acl-tacas permit udp any any eq 49
ip access-list copp-system-p-acl-ntp permit udp any 10.0.1.1/23 eq 123
ip access-list copp-system-p-acl-icmp permit icmp any any
class-map type control-plane match-any copp-system-p-class-critical match access-group name copp-system-p-acl-igmp
match access-group name copp-system-p-acl-msdp
class-map type control-plane match-any copp-system-p-class-normal match access-group name copp-system-p-acl-icmp
match exception ip icmp redirect
match exception ip icmp unreachable
match exception ip option
policy-map type control-plane copp-system-p-policy
```

```
class copp-system-p-class-critical
police cir 19000 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-important
police cir 500 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-normal
police cir 300 pps bc 32 packets conform transmit violate drop
class class-default
police cir 50 pps bc 32 packets conform transmit violate drop
control-plane
service-policy input copp-system-p-policy
```

Create CoPP class and associate ACL:

```
class-map type control-plane copp-arp-
class match access-group name copp-arp-acl
```

Add the class to the CoPP policy:

```
policy-map type control-plane copp-system-
policy class copp-arp-class
police pps 500
```

11.10.2 Changing or Reapplying the Default CoPP Policy Using the Setup Utility

The following example shows how to change or reapply the default CoPP policy using the setup utility.

```
switch# setup

---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration
of the system. Setup configures only enough connectivity for
management of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes

Do you want to enforce secure password standard (yes/no) [y]: <CR>

Create another login account (yes/no) [n]: n

Configure read-only SNMP community string (yes/no) [n]: n

Configure read-write SNMP community string (yes/no) [n]: n
```

```

Enter the switch name : <CR>

Enable license grace period? (yes/no) [n]: n

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: n

Configure the default gateway? (yes/no) [y]: n

Configure advanced IP options? (yes/no) [n]: <CR>

Enable the telnet service? (yes/no) [n]: y

Enable the ssh service? (yes/no) [y]: <CR>

  Type of ssh key you would like to generate (dsa/rsa) : <CR>

Configure the ntp server? (yes/no) [n]: n

Configure default interface layer (L3/L2) [L3]: <CR>

Configure default switchport interface state (shut/noshut) [shut]: <CR>

Configure best practices CoPP profile (strict/moderate/lenient/dense/skip) [strict]:
strict

The following configuration will be applied:
password strength-check
no license grace-period
no telnet server enable
no system default switchport system
default switchport shutdown
policy-map type control-plane copp-system-p-policy

Would you like to edit the configuration? (yes/no) [n]: <CR>

Use this configuration and save it? (yes/no) [y]: y

switch#

```

11.11 Additional References for CoPP

This section provides additional information related to implementing CoPP.

Standards

Standards	Title
RFC 2698	A Two Rate Three Color Marker