SDN AC Protocols
Introduction Practice Guide

Contents

SDN Commonly Used Protocols Integrated Practice Guide

Typical Application Scenarios of SDN Commonly Used Protocols

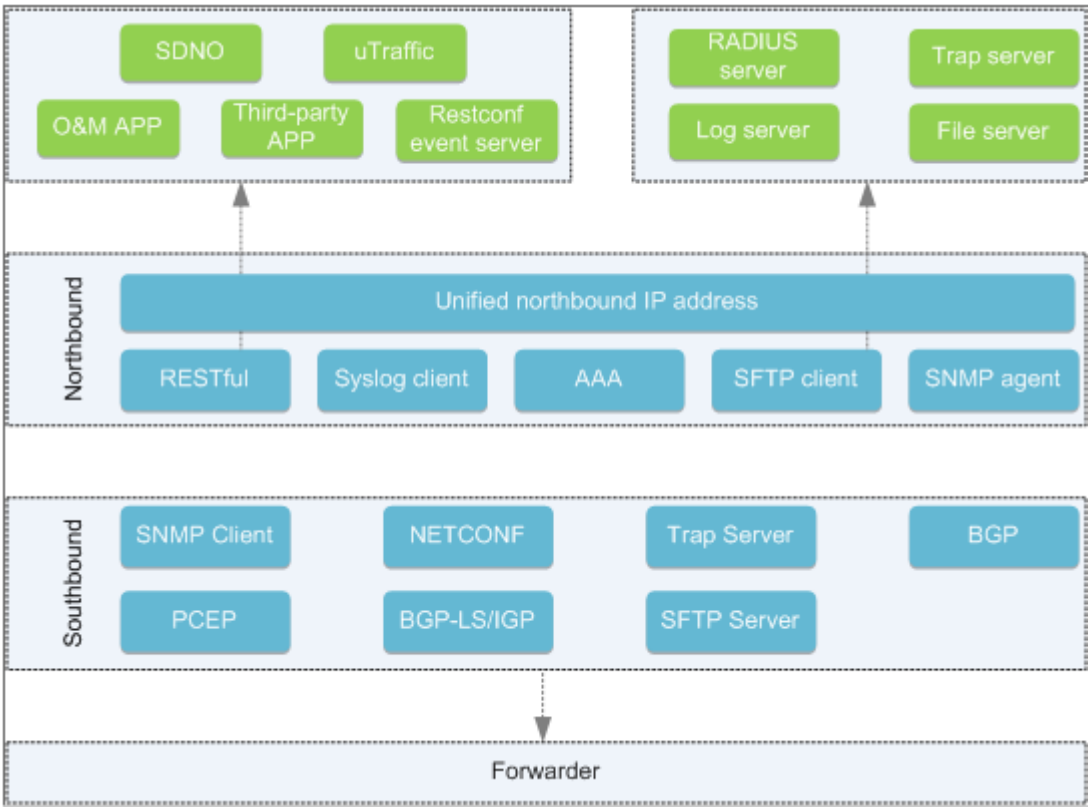
In conjunctions with the rapid growth and emergence of SDN networks, various types of protocols are deployed, which might vary based on different SDN solutions applied according to live network applications. This section generally describes the commonly used protocols in SDN applications, such as Openflow, SNMP, Netconf etc.

Diagrams below show the examples of a few types of Huawei SDN solutions. The similarities of each solution here is that all the SDN solutions will definitely comprise of two main SDN network elements such as the Agile Controller and the forwarding device(Network Elements), which is also known as forwarder. In certain solutions such as IP + Optical solution or TSDN solutions, there are some other additional SDN elements being deployed, which are the U2000 and utraffic. To allow all these elements to be able to communicate with each other, different communication protocols are deployed. SDN protocols can divided into Northbound and Southbound interface protocols. Northbound protocols are used during upper-level communication, between Apps/Cloud/Virtualization Platform to Controllers and southbound protocols used during communication between Agile controllers and Forwarding Devices.

Disclaimer:

After discussing the protocols briefly in the next section, this guide will focus on hands on practices of configuring some of the major protocols such as

Southbound and Northbound Protocols Supported by the AC-DCN



Northbound and Southbound Protocols

The AC-DCN supports a variety of standard northbound and southbound protocols.

The northbound layer uses the RESTCONF/RESTful management protocol to receive service information or policies from the orchestration layer or third-party apps. Communication protocols such as Syslog and SFTP are used to transfer and back up data between the AC-DCN and a third-party server.

Southbound protocols include the control protocol such as OpenFlow for multiple path detection, communication protocols such as SFTP for file transfer, and management protocols such as SNMP and NETCONF for configuration delivery or alarm collection.

The northbound layer provides a unified IP address, through which you can manage the AC-DCN regardless of the northbound protocol in use and without the need to monitor changes in the controller.

The following figure lists functions of the protocols.

Northbound Protocol	Description
RESTCONF/RESTful	Provides HTTP-based standard RESTCONF/RESTful interfaces, allowing you to configure, manage, and perform maintenance on the controller. Supports the WebSocket-based RESTful notification mechanism, which provides near-instantaneous notifications.
NETCONF	Receives configurations and optimization policies for scheduling IP network border traffic.
Syslog client	Enables you to upload Syslogs to log servers.
AAA	Supports login authorization and authentication, as well as remote RADIUS authentication.
SFTP client	Provides support for SFTP clients.
SNMP agent	Provides SNMP services and trap reporting.

Southbound Protocol	Description
SNMP client	Supports sending management information base (MIB) requests to forwarders and implementing operations such as device discovery. The AC-WAN actively attempts to connect to the target forwarder through the SNMP client (after the forwarder IP address, user name, and password are set on the controller). You can query device information after a connection is established.
NETCONF	Delivers and reconciles NE configurations. The NETCONF module of the AC-WAN acts as a NETCONF client at the southbound layer.
SFTP Server	Provides the SFTP server function.
Trap Server	Receives SNMP traps reported by forwarders.
PCEP	Communicates tunnel information between the controller (PCE) and forwarder (PCC). PCEP sessions can be used to configure tunnels and optimize traffic.
BGP/BGP Flowspec	Collects and controls routes on forwarders.
BGP-LS/IGP	Collects and advertises routes. It collects topology information from forwarders and sends it to the controller.

Configuring Northbound Protocols

Task Description

This lab practice will focus on configuration related to the Northbound protocols

Version Information

Equipment Type	Equipment Version
SDN Agile Controller	DCNV300R001C10

Objectives

Upon completion of this course, you will be able to:

- Configure RESTful Northbound Connection on SDN AC
- View RESTful Northbound Connection Statistics on SDN AC
- Configure SNMP Agent and Alarm Host protocol on SDN AC
- View SNMP Agent Statistics on SDN AC

Background

The northbound protocol, such as RESTCONF/RESTful, SNMP, SFTP, RADIUS, NETCONF and Syslogs, is the protocol used when an AC-DCN is communicating with the NMS.

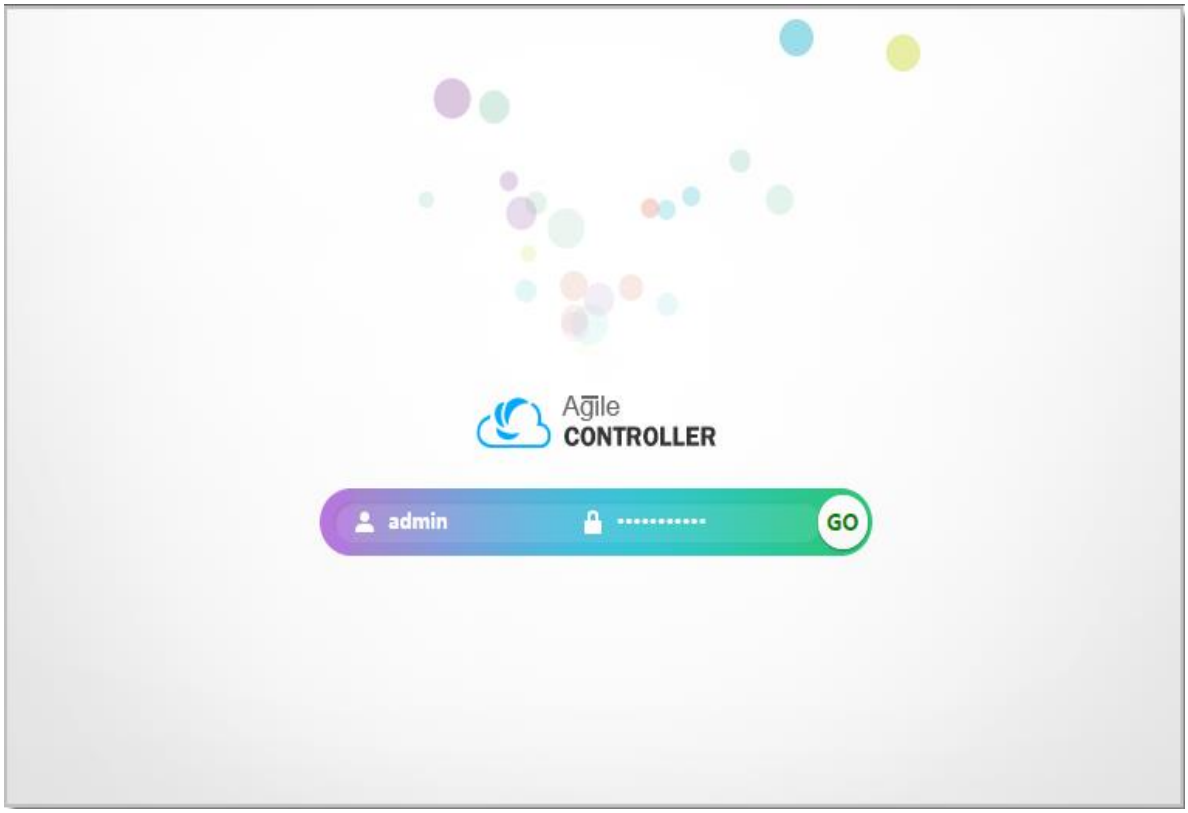
The AC-DCN unifies IP addresses and displays only one IP address to the NMS.

Configuration Tasks

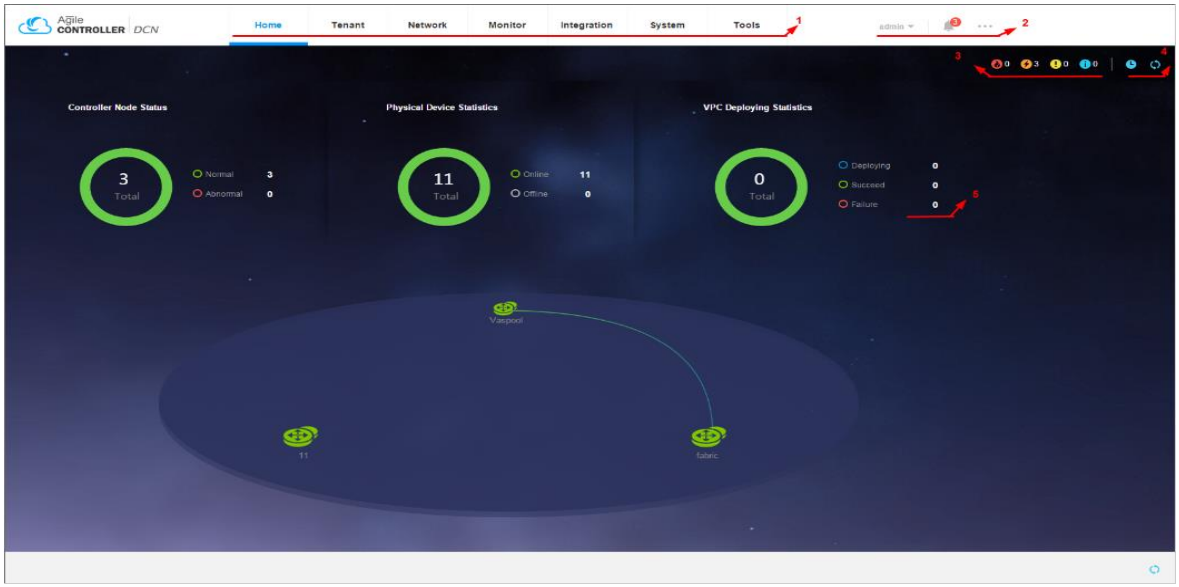
Login into AC controller

1. User Mozilla firefox to login into the AC controller via the management IP:
2. Enter **https://** AC-DCN *server IP address:***port number/index.html** in the address box, and press Enter. (example: https://100.0.100.40:18002)

3. Enter the default administrator name **admin** and password **Changeme123**, and click GO



4. After login, the system prompts you to the change the password.
5. After the password is modified, the system automatically jumps to the login page in 5 seconds. Log in to the AC-DCN using the new password to check whether the new password is correct
6. Below is the screenshot of the AC Homepage:



1)**Main menu area**-Function as a main entrance to different functions of the AC-DCN.

2)**General information area**-Displays the following common information about the AC-DCN from left to right:

User Name: Indicates the user name for logging in to the AC-DCN.

Logout: used for logging out of the AC-DCN or switching login account.

Notification Icon: Click the notification icon to display the AC-DCN alarms.

Others:

Language: Click the icon to switch the current language mode of the AC-DCN.

Oline Help: Click Oline Help to view help information if you encounter any problems when using the AC-DCN.

Config Guide: Click Config Guide to view the step-by-step guidance of configuring the AC-DCN services.

Website Map: Click Website Map to display a navigation page generated based on the structure, framework, and content of the AC-DCN. You can use Website Map to quickly locate the entries of functions of the AC-DCN.

About: Click About to display the AC-DCN version.

Visual Style: Click Visual Style to switch the view style.

3)Alarm indicator area -Shows severity and entries of uncleared alarms of the AC-DCN. They are critical alarm number, major alarm number, minor alarm number, and warning number, from left to right.

4)Statistics information fresh area-Displays refreshed device status and services on the statistic graph.

5)Statistics area-Shows device statuses and services, including measurement of network device statuses and physical network device statuses.

Northbound Protocols Setup

RESTful Northbound Connection

1. Choose **System > System Settings > Northbound Protocol** from the main menu.

2. Choose **RESTful** > **Northbound Connection** from the navigation tree on the left.The northbound connection page is displayed

3. The lock function prevents service configurations from being delivered to cluster nodes. Enable the lock function and click **Apply**. The Agile Controller-DCN rejects REST configurations and WebSocket connection requests

Northbound Connection Parameters	

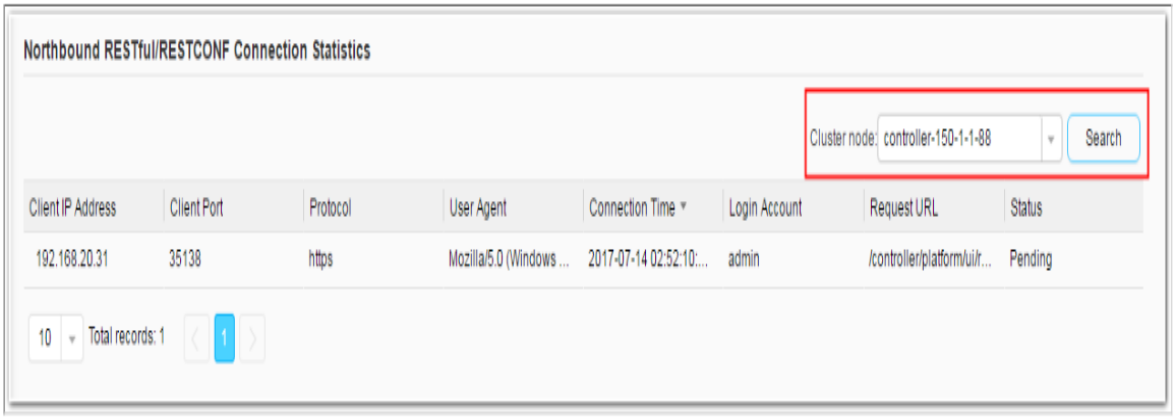
Northbound Lock	Indicates the status of the northbound lock
	
	During online upgrade, RESTful/RESTCONF requests and WebSocket connections must be locked.
	After the locking:
	• Northbound RESTful/RESTCONF POST/PUT/DELETE requests are denied, and POST requests with the query parameter **op=get** are processed as GET.
	• WebSocket connection requests are denied.
	You can perform the following operations to unlock some unexpected RESTful/RESTCONF POST/PUT requests:
	1. Access the directory where the configuration file is stored.
	`# /opt/controller/naas/naas-karaf-1.0.1-SNAPSHOT/configuration/rest-not-lock`
	2. Modify the lock.xml file as follows:
	`<not-allowed-locks`
	`<allow-rule url="/proxy/ui/test" method = "POST">`
	`</ allow-rule >`
	`</ not-allowed-locks >`
	Where:

	• **url**: indicates full match of request URLs. • **method**: indicates the request method. Save the modification.

4. On the **Northbound Websocket Connection Statistics** tab page, enter the node name in the search box, and click . The statistics result is displayed.

Northbound Websocket Connection Statistics	
Client IP	Indicates the IP address of a northbound application.
Node Name	Indicates the IP address of the service management node of the AC-DCN.
Connection Time	Indicates the time when a connection is established.
WSS URL	Indicates the uniform resource locator. A URL uniquely identifies the location of a resource.
Status	• connected • connecting

5. On the **Northbound RESTful/RESTCONF Connection Statistics** tab page, select a cluster node, and click **Search**. The statistics result is displayed in the list.



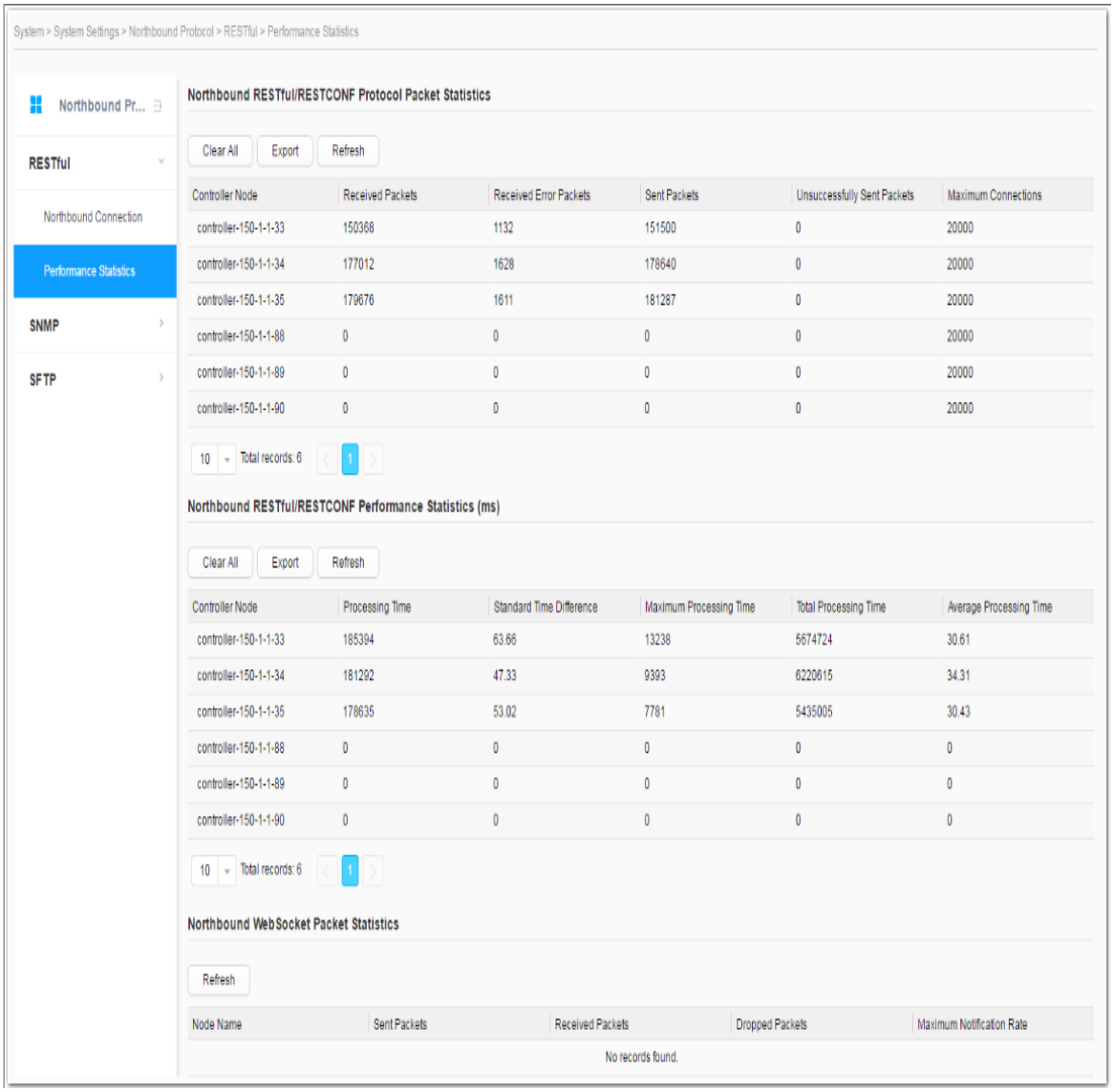
Northbound RESTful/RESTCONF Connection Statistics	
Client IP	Indicates the IP address of a northbound application.
Client Port	Indicates the northbound application port.
Protocol	• http: HTTP transfers hypertext messages in plain text. • https: HTTPS supports SSL encryption and has high security. • ws: WebSocket is a full-duplex technology enabling communications between the browser and server. • wss: Secure WebSocket supports SSL encryption.
User Agent	Indicates the client browser.
Connection Time	Indicates the time when a connection is established.
Login Account	Indicates the user name for logging in to the AC-DCN.
Request URL	Indicates the uniform resource locator. A URL uniquely identifies the location of a resource.
Status	• pending • processing

RESTful Performance Statistics

1. Choose **System > System Settings > Northbound Protocol** from the main menu.

2. Choose **RESTful > Performance Statistics** from the navigation tree on the left. The RESTful performance statistics page is displayed.

3. Information about **Northbound RESTful/RESTCONF Protocol Packet Statistics, Northbound RESTful/RESTCONF Performance Statistics (ms),** and **Northbound WebSocket Packet Statistics** is displayed on the performance statistics page. Users can export or clear the statistics result.

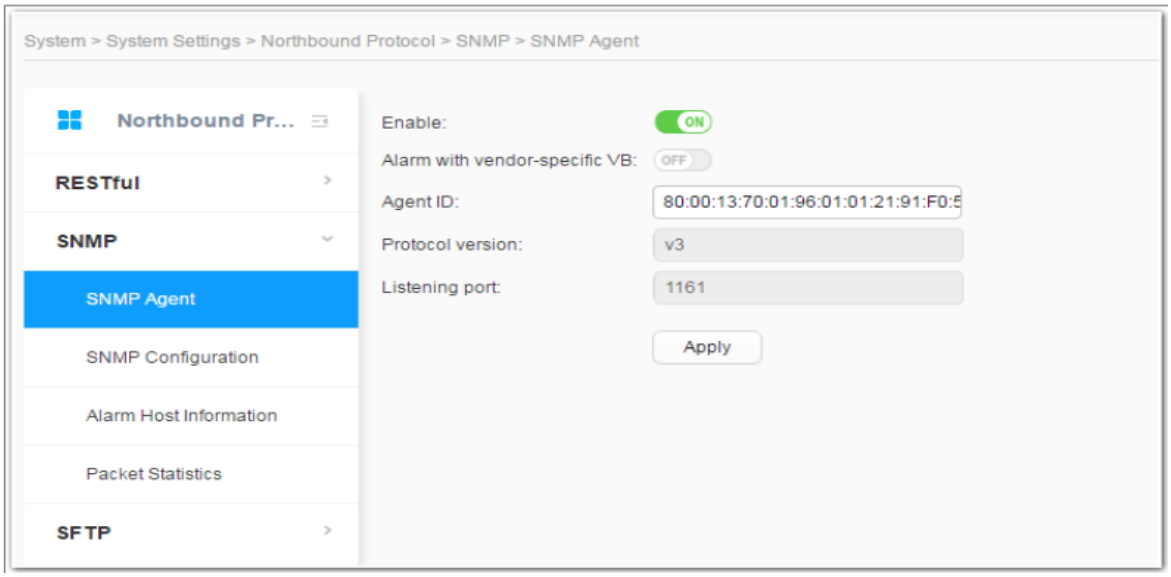


Parameter	Description
Northbound RESTful/RESTCONF Protocol Packet Statistics	
Controller Node	Indicates statistics on protocol packets of an AC-DCN node.
Max Connections	Indicates the maximum number of connections between the AC-DCN nodes and northbound applications.
Northbound RESTful/RESTCONF Performance Statistics (Time Unit: ms)	
Controller Node	Indicates the number of requests sent by northbound applications to the AC-DCN nodes.
Processing Time	Indicates the number of requests sent by northbound applications to the AC-DCN nodes.
Standard Time Difference	A smaller value indicates a more stable connection between the northbound application and AC-DCN.
Northbound WebSocket Packet Statistics	
Node Name	Indicates the AC-DCN node.
Sent/received/dropped packets	Indicates the number of WebSocket notification packets sent, received, and discarded by the AC-DCN.
Max Notification Rate	Indicates the rate at which WebSocket notification packets are reported.

SNMP Agent

1. Choose **System** > **System Settings** > **Northbound Protocol** from the main menu.

2. Choose **SNMP** > **SNMP Agent** from the navigation tree on the left. The SNMP agent page is displayed



3. Enable **SNMP Agent**, set **Alarm with vendor-specific VB** to **ON**, set **Agent ID**, and click **APPLY**.

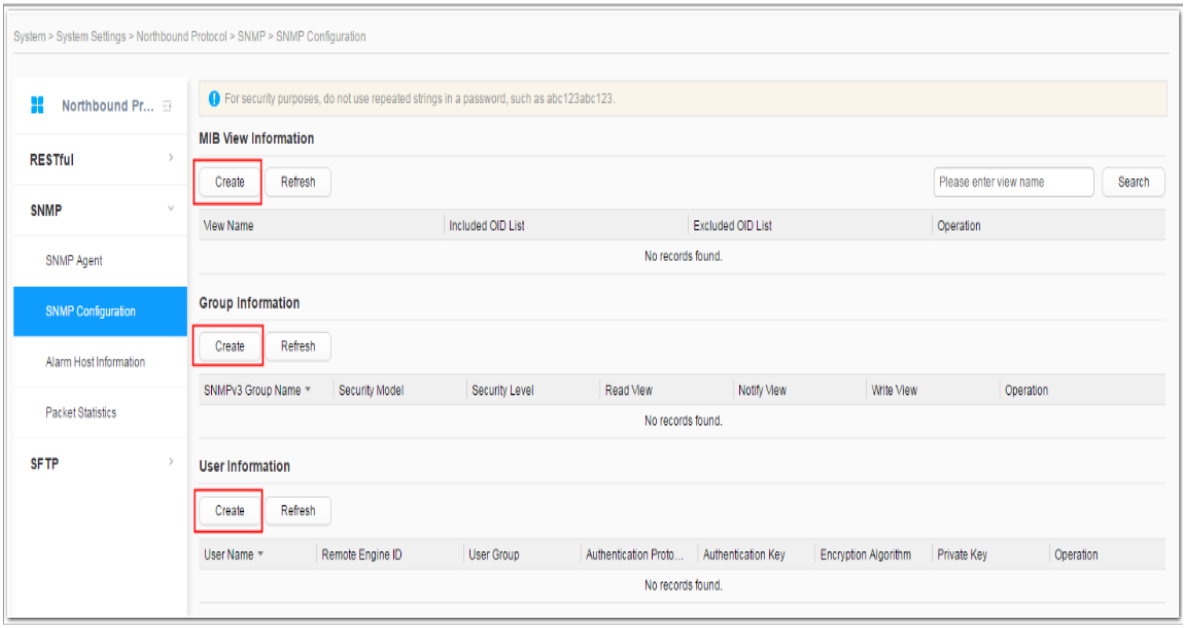
Parameter	Description
Enable	When you want to configure SNMP, switch this button to **ON**.
Alarm with vendor-specific VB	Specifies whether to receive the Trap packets carrying the extended private VBs.
Agent ID	Indicates the engine ID that uniquely identifies an SNMP agent. **NOTE:** If you set or change a local engine ID, the existing SNMPv3 user will be deleted.
Protocol version	The protocol supports only the SNMPv3 version.
Listening port	The listening port of the SNMP agent needs to be specified.

SNMP Configuration

1. Choose **System > System Settings > Northbound Protocol** from the main menu.

2. Choose **SNMP > SNMP Configuration** from the navigation tree on the left. The SNMP Configuration page is displayed.

3. You can create and view MIB view information, group Information, and user information on the **SNMP Configuration** page



Parameter		Description
MIB View Information	View name	Customization
	Include OID List	To filter the specified alarm in include mode, the OIDs of all variables bound to the alarm must be included. Otherwise, the filter will fail.
	Exclude OID List	To filter the specified alarm in exclude mode, the OID of the alarm or the OID of any variable bound to the alarm must be included.
Group Information	Group name	Customization
	Security level	There are three security levels: • auth-priv: authentication and encryption • auth-no-priv: authentication and non-encryption • no-auth-no-priv: non-authentication and non-encryption

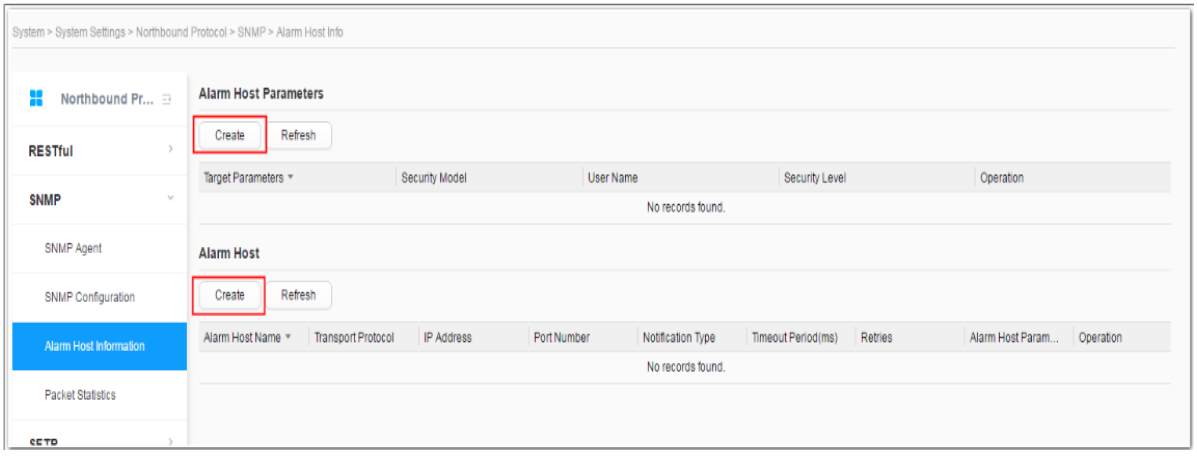
Parameter		Description
	Read view	The read-only view is specified, that is, the MIB nodes in read-only view can be read.
	Notification view	The notification view which has the permission to send alarms is specified. The MIB nodes in the view can send alarms to eSight.
	Write view	The write-only view is specified, that is, the MIB nodes in write-only view can be written.
User Information	User name	Customization
	Remote engine ID	The engine ID of an alarm host is specified.
	Group name	The SNMP user name defined by a user must join a valid SNMP user group.
	Authentication protocol	An authentication protocol such as SHA and MD5 is specified. SHA which is securer than MD5 is recommended. The authentication protocol can also be left empty.
	Authentication key	The authentication key is specified.
	Encryption algorithm	The encryption algorithm is specified. The northbound AES_256 and CES_DES are supported.
	Private key	The encryption key is specified.

Alarm Host Info

1. Choose **System > System Settings > Northbound Protocol** from the main menu.

2. Choose **SNMP > Alarm Host** Info from the navigation tree on the left. The Alarm Host Info page is displayed.

3. You can create and view alarm host parameters and alarm host on the **Alarm Host Information** page.



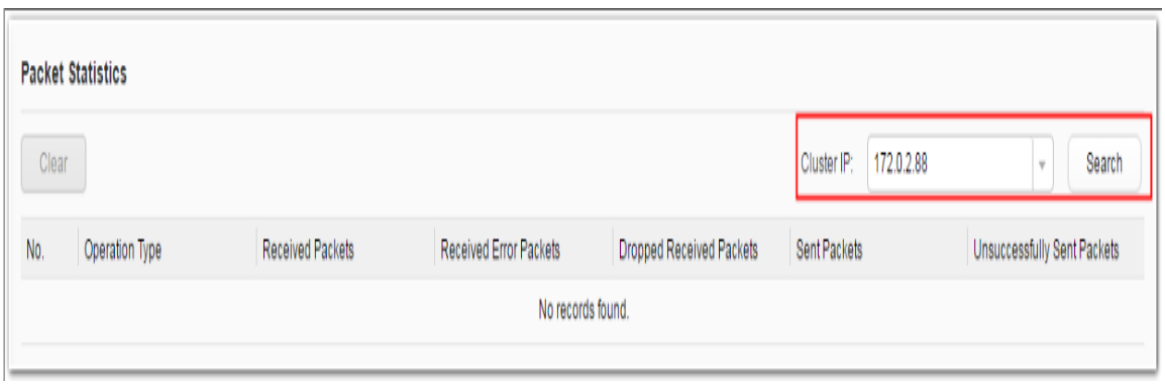
Parameter	Description
Alarm Host Parameters	
Target Parameters	Target parameter names.
Security Model	Indicates the SNMPv3 security model.
User Name	Select an existing user name.
Security Level	• auth-priv: authentication and encryption • auth-no-priv: authentication and non-encryption • no-auth-no-priv: non-authentication and non-encryption
Alarm Host	
Notification Type	• Trap message: Trap messages have poor reliability because senders cannot determine whether recipients have received the trap messages. • Inform message: Inform messages have high reliability because a mechanism is present for determining whether recipients have received the Inform messages.
Timeout Period (ms)	Indicates the timeout period of SNMP proxy packets sent by the AC-DCN to the SNMP agent.
Target parameters	Select one from existing target parameters to guarantee transmission security.

Packet Statistics

1. Choose **System > System Settings > Northbound Protocol** from the main menu.

2. Choose **SNMP > Packet Statistics** from the navigation tree on the left. The Packet Statistics page is displayed.

3. On the **Packet Statistics** tab page, select the IP address of the node from the **Cluster IP** drop-down list box and click **Search**. The packet statistics result is displayed in the list.



4. To clear the statistics result, click **Clear.**

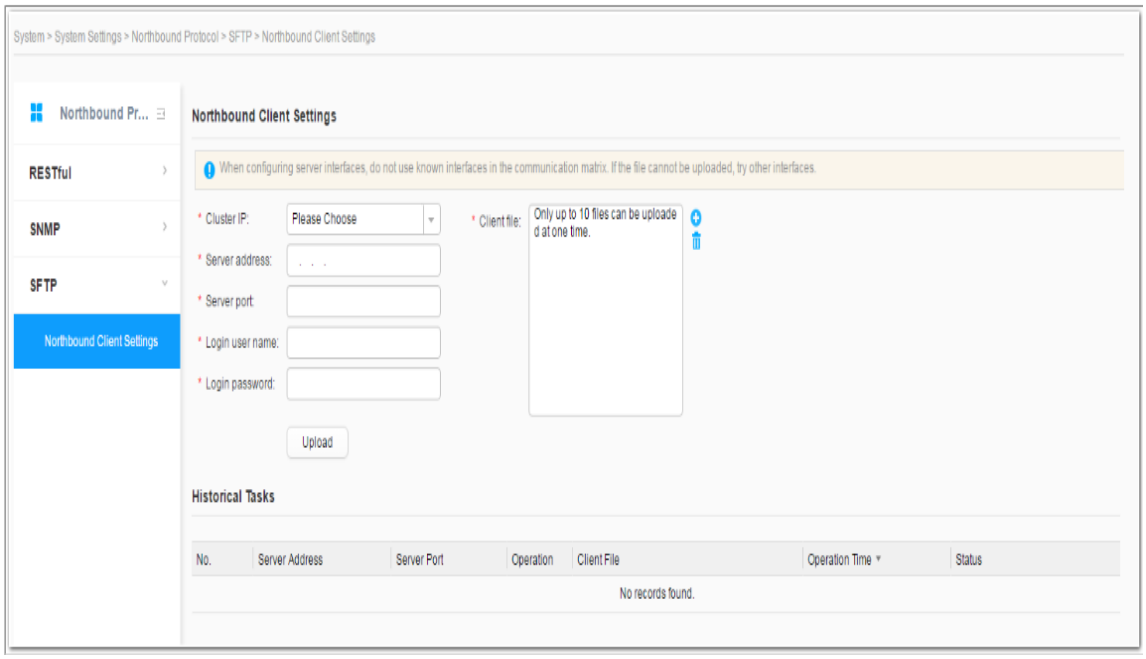
5. On the **Fault Records** page, select the IP address of the node from the **Cluster IP** drop-down list box and click **Search**. The fault records are displayed in the list.

6. To clear the fault records, click **Clear**.

SFTP

1. Choose **System > System Settings > Northbound Client Settings** from the main menu.

2. Choose **SFTP > Northbound Client Settings** from the navigation tree on the left. **The Northbound Client Settings** page is displayed.



3. Set **Cluster IP**, **Server address**, **Server port**, **Login user name**, and **Login password**, click to select a client file to be uploaded, and click **Upload**.

4. The historical client file records are displayed on the **Historical Tasks** tab page.

Parameter	Description
Cluster IP	Indicates the IP address of a node of the Agile Controller-DCN cluster whose log files need to be exported.
Server address	Indicates the SFTP server address.
Server port	Indicates a port on the SFTP server used to transfer log files.
Login user name	Indicates the user name for logging in to the SFTP server.
Login password	Indicates the password for logging in to the SFTP server.

Configuring Southbound Protocols

Task Description

This lab practice will focus on configuration related to the Southbound protocols

Version Information

Equipment Type	Equipment Version
SDN Agile Controller	DCNV300R001C10

Objectives

Upon completion of this course, you will be able to configure the following protocols for southbound communication:

- **NETCONF**
- **SNMP**
- **SFTP**
- **SOAP**
- **SFLOW**
- **OpenFlow**
- **OVSDB**
- **JSONRPC**
- **RESTful**

Background

The southbound protocol, such as NETCONF, SFTP, SNMP, Syslogs, and PCEP, is the protocol used when an Agile Controller-DCN is communicating with NEs.

Each controller node has a southbound IP address

Prerequisites

Forwarders have been added to the AC-DCN. This is done as part of the service commisoning practice

Configuration Tasks

SFTP

1. Choose **System > System Settings > Northbound Client Settings** from the main menu.

2. Choose **SFTP > Northbound Client Settings** from the navigation tree on the left. **The Northbound Client Settings** page is displayed.

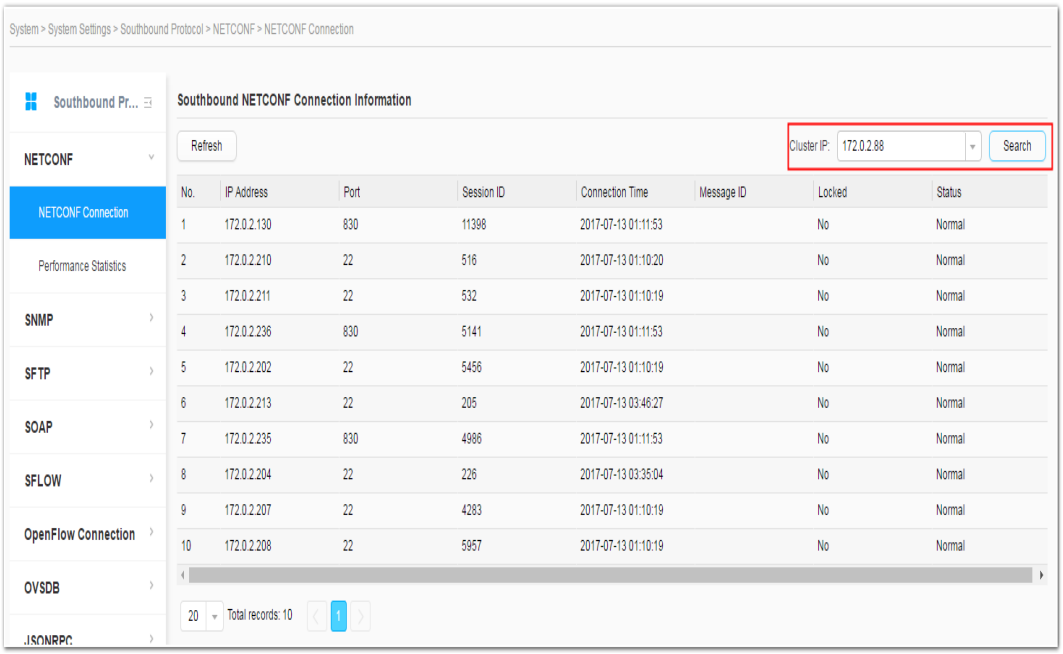
NETCONF

NETCONF Connection

1. Choose **System > System Settings > Southbound Protoco**l from the main menu.

2. Choose **NETCONF > NETCONF Connection** from the navigation tree on the left.

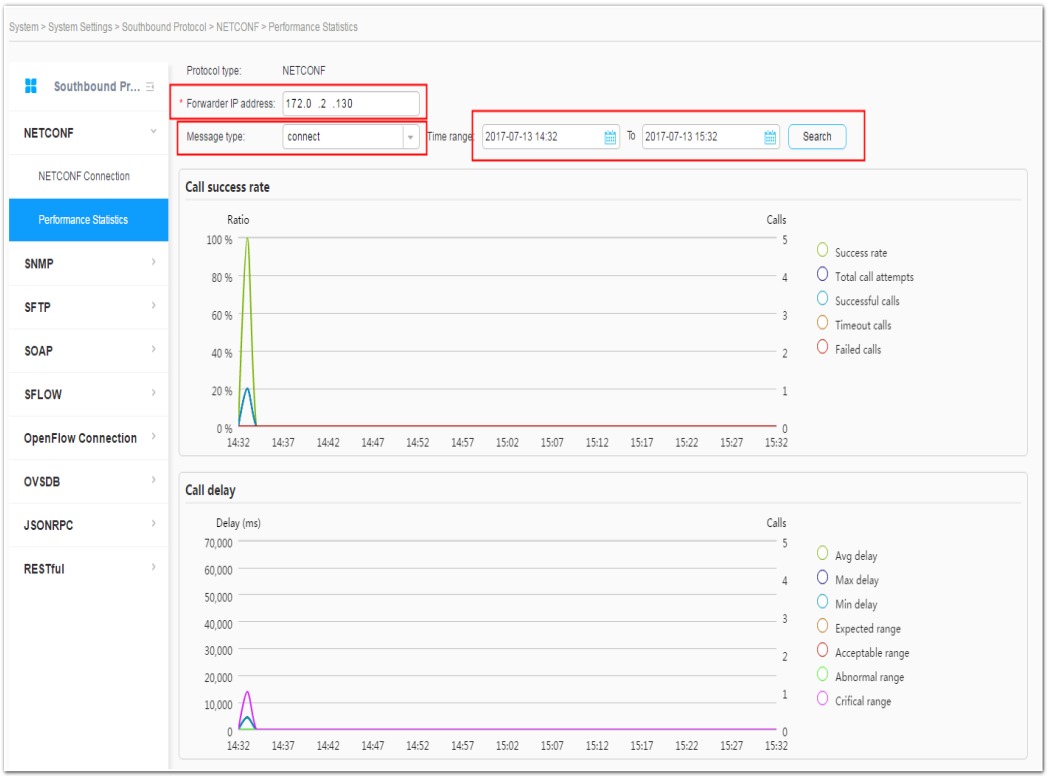
3. Select the IP address of the node from the **Cluster IP** drop-down list box and click **Search**. The NETCONF connections of the southbound devices managed by the node are displayed in the list.



Parameter	Description
IP Address	Forwarder IP address
(VMM) Port	Forwarder port number
Session ID	ID that uniquely identifies a connection between the controller and forwarder
Connection Time	NETCONF connection time
Locked	Whether the configuration database is locked: • **Yes**: The configuration database is locked to prevent operation conflicts. Other users cannot modify the data of this database. • **No**: The configuration database is not locked. Be sure to lock it before modifying its data.
Status	Connection status: • Normal • Disconnected

NETCONF Performance Statistics

1. Choose **System** > **System Settings** > **Southbound Protocol** from the main menu.
2. Choose **NETCONF** > **Performance Statistics** from the navigation tree on the left.
3. Set the IP address of the forwarder. Select a message type. Set the time range which needs to be less than one hour. Click **Search**. The statistics result is displayed.



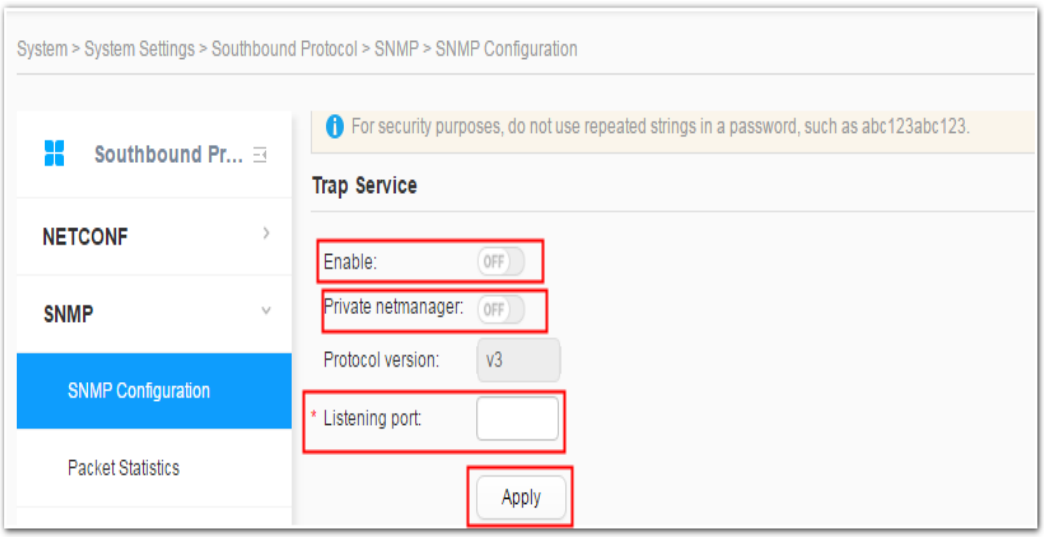
Parameter	Description
Forwarder IP address	Forwarder IP address
Message type	Message type for protocol operations: • **connect**: establishes a connection between the controller and forwarder. • **get**: obtains data from the running configuration database or device statistics. • **get-config**: obtains data from the running, candidate, or startup database. • **edit-config**: modifies a configuration database. • **notification:** indicates a notification message sent from the forwarder to the controller.
Time range	Duration for collecting performance statistics.

SNMP

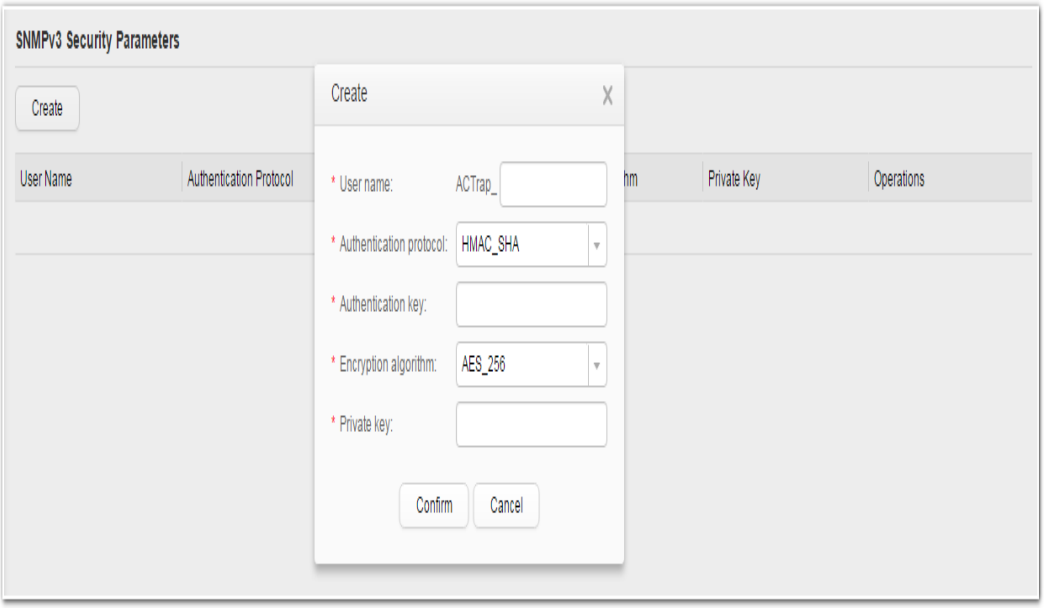
SNMP Configuration

1. Choose **System > System Settings > Southbound Protocol** from the main menu.
2. Choose **SNMP > SNMP Configuration** from the navigation tree on the left.

3. On the **Trap Service** page, set whether to enable **Trap Service** and **Private netmanager**, set **Listening port**, and click **Apply.**



4. On the **SNMPv3 Security Parameters** page, click **Create**, and set parameters.

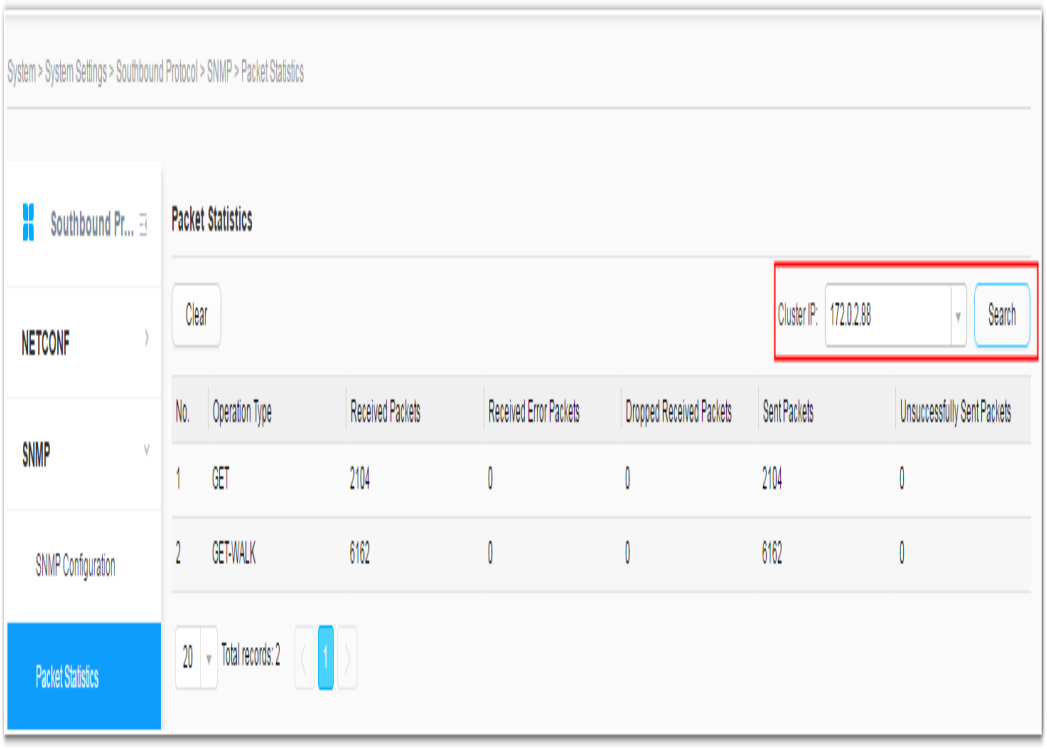


Parameter		Description
Trap Service	Enable	Select Enable.
	Private netmanager	When the network is unstable, this function can be enabled to prevent data loss. After this function is enabled, the Agile Controller-DCN will deliver an instruction to devices to modify the Private Net Management field of target hosts. After the modification, five VB tags will be automatically

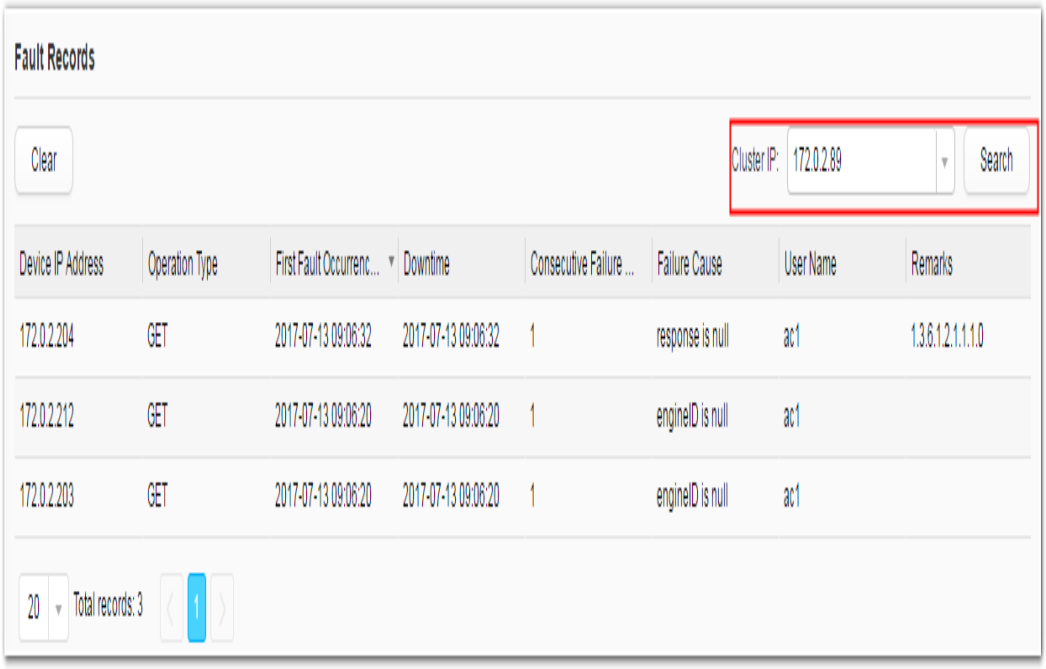
Parameter		Description
		added to alarms reported by devices and the tags are used as the credential for finding lost data packets.
	Protocol version	The trap service uses the SNMPv3 protocol by default.
	Listening port	Indicates the port used by the Agile Controller-DCN to receive device alarms.
SNMPv3 Security Parameters	User name	Indicates the user names delivered from the Agile Controller-DCN to devices.
	Authentication protocol	Indicates the authentication protocol delivered from the Agile Controller-DCN to devices to authenticate device alarms.
	Authentication key	Indicates the authentication key delivered from the Agile Controller-DCN to devices to authenticate device alarms.
	Encryption algorithm	Indicates the encryption algorithm delivered from the Agile Controller-DCN to devices to encrypt device alarms.
	Private key	Indicates the private key delivered from the Agile Controller-DCN to devices to encrypt device alarms.

SNMP Packet Statistics

1. Choose **System > System Settings > Southbound Protocol** from the main menu.
2. Choose **SNMP > Packet Statistics** from the navigation tree on the left.
3. On the **Packet Statistics** tab page, select the IP address of the node from the **Cluster IP** drop-down list box and click **Search**. The packet statistics result is displayed in the list.



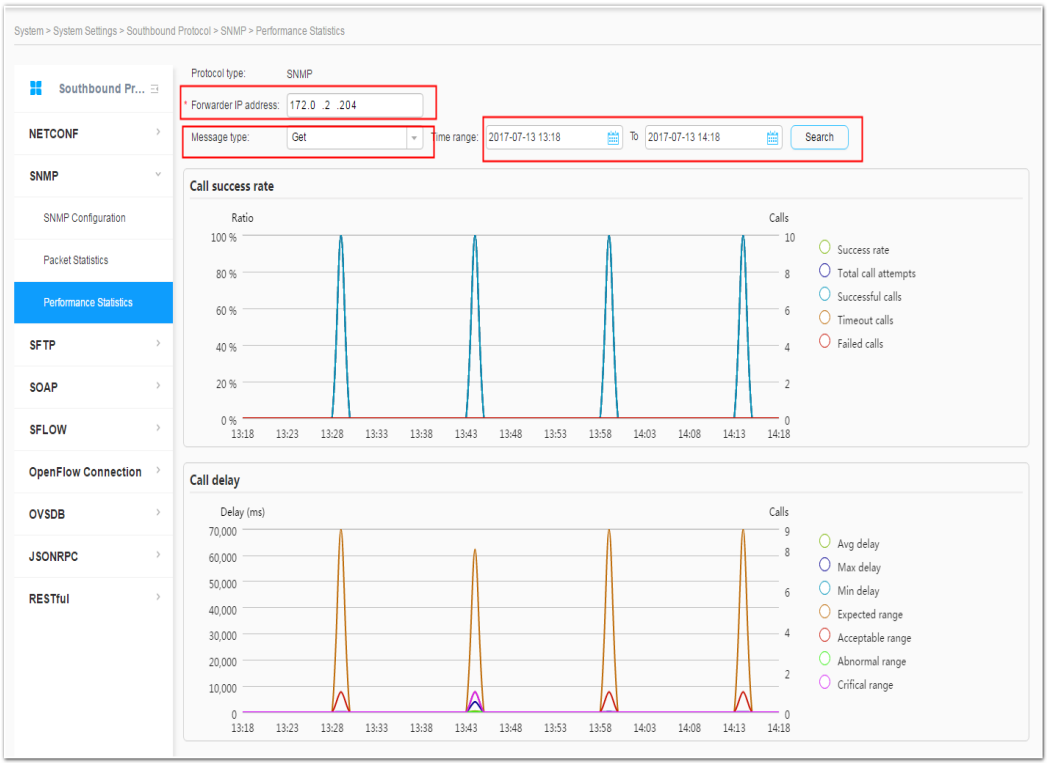
4. To clear the statistics result, click **Clear**.
5. On the **Fault Records** page, select the IP address of the node from the **Cluster IP** drop-down list box and click **Search**. The fault records are displayed in the list.



6. To clear the fault records, click **Clear**.

SNMP Performance Statistics

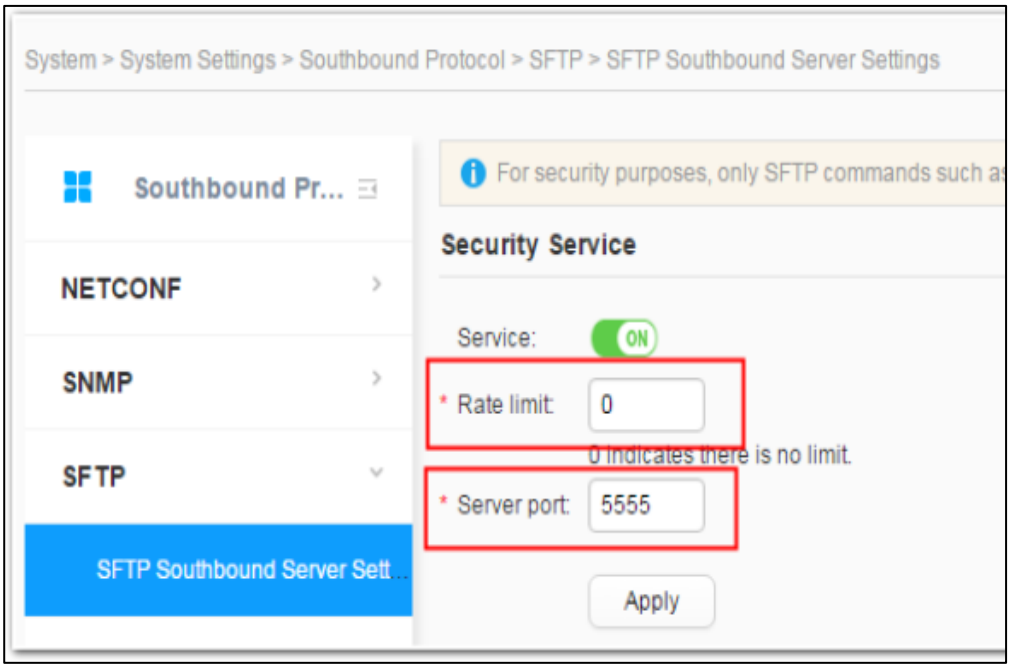
1. Choose System > System Settings > Southbound Protocol from the main menu.
2. Choose SNMP > Performance Statistics from the navigation tree on the left.
3. Set the IP address of the forwarder. Select a message type. Set the time range which needs to be less than one hour. Click Search. The statistics result is displayed.



Parameter	Description
Forwarder IP address	Forwarder IP address
Message type	Message type for protocol operations: • Get: value of the OID obtained from the MIB. • Get-Next: value of the next OID obtained from the MIB. • Trap: alarm sent from the Agent to the NMS.
Time range	Duration for collecting performance statistics.

SFTP

1. Choose **System > System Settings > Southbound Protocol** from the main menu.
2. Choose **SFTP > SFTP Southbound Server Settings** from the navigation tree on the left. The SFTP southbound server configuration page is displayed.



3. Set **Service**, **Rate limit**, and **Server port**, and click **Apply**.
4. On the **Southbound Server Settings** tab page, click **Create**, and set **Account Name** and **Password** of the SFTP server. You can delete an existing user or change the password.
5. On the **Task Overview** tab page, select the IP address of the node from the **Cluster IP** drop-down list box and click **Search**. Information about clients connected to the SFTP server is displayed.

Parameter		Description
Security Service	Service	• ON • OFF
	Rate limit	Indicates the maximum transmission rate of SFTP. The value cannot be empty, and the unit is kbps. The value ranges from 512 to 102400. Enter 0 if the value is not limited.
	Server port	Indicates the service port number of the southbound service NIC. The value ranges from 1025 to 65535.
Southbound Server Settings	Login user	Indicates an SFTP server user name.
	Password	Indicates the SFTP server password.

SOAP

1. Choose **System > System Settings > Southbound Protocol** from the main menu.
2. Choose **SOAP > VMM** from the navigation tree on the left.
3. Set the NE IP address and click Search. The VMM connection information under the NE is displayed.

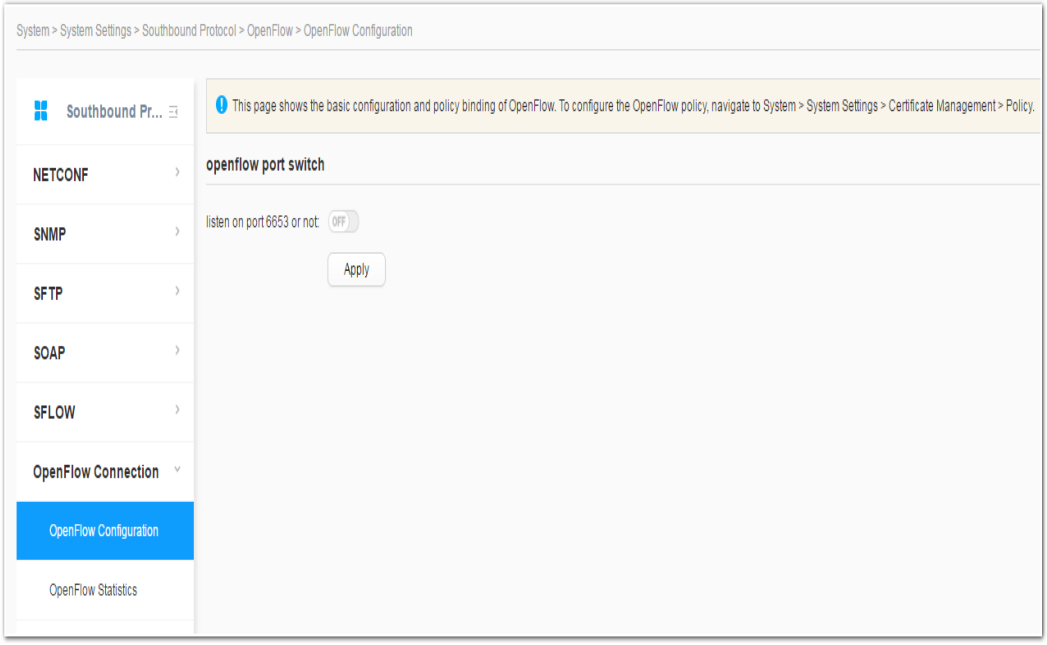
SFLOW

1. Choose **System > System Settings > Southbound Protocol** from the main menu.
2. Choose **SFLOW > Packet Statistics** from the navigation tree on the left. The sFlowProtocol Packet Statistics page is displayed.

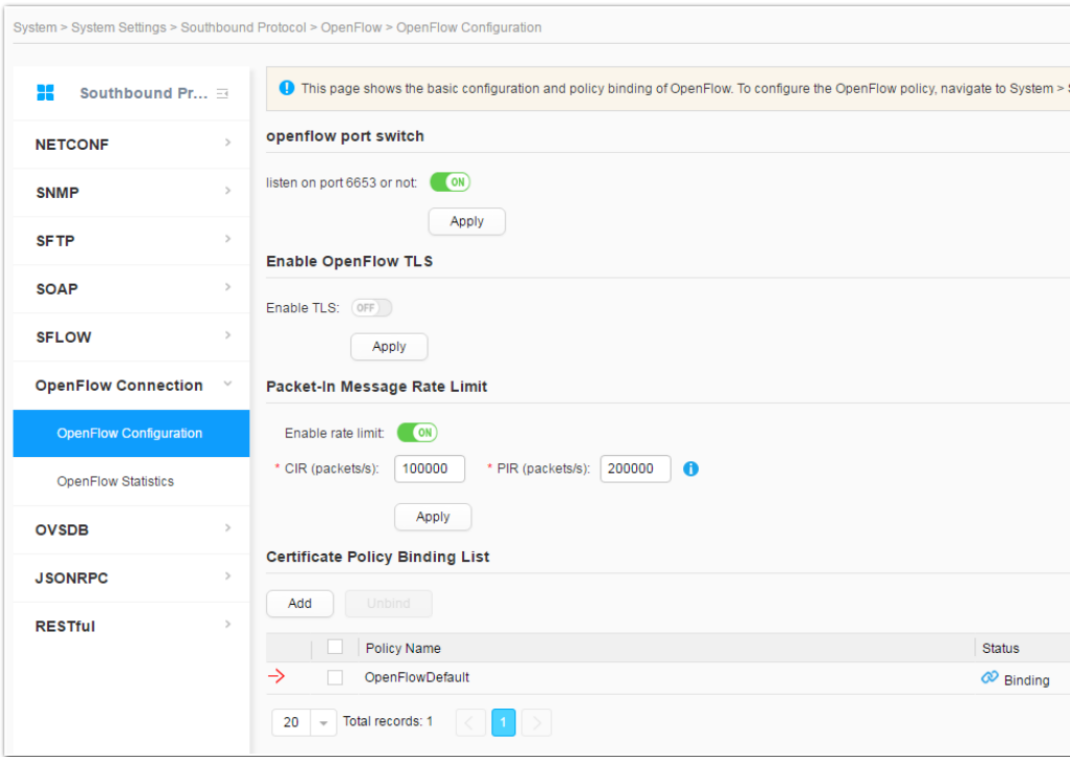
OpenFlow

OpenFlow Configuration

1. Choose **System > System Settings > Southbound Protocol** from the main menu.
2. Choose **OpenFlow > OpenFlow Configuration** from the navigation tree on the left.



3. Set **listen on port 6653 or not.**
4. If **listen on port 6653 or not** is set to **ON**, click **Apply**, and go to 4.

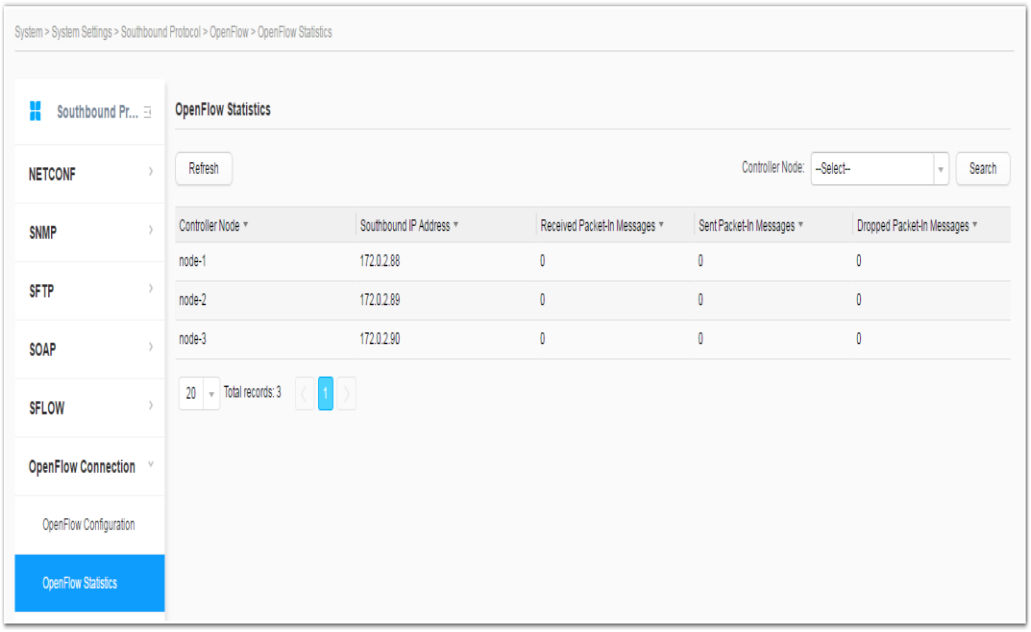


5. If **listen on port 6653 or not** is set to **OFF**, click **Apply**. The process ends.
6. Set **Enable TLS** and click **Apply**.
7. Set **Packet-In Message Rate Limit**. If the value is **ON**, set the CIR and PIR, and click **Apply**.
8. For details about creation and binding of the certificate policy, see refer to documentation

Parameter		Description
openflow port switch	listen on port 6653 or no	• ON:Yes • OFF:No
Enable TLS	Enable TLS	• ON:Enable • OFF:Disable
OpenFlow Packet-In Rate Limit Configuration	Enable rate limit	• ON:Enable • OFF:Disable
	CIR	Indicates the average rate at which the Agile Controller-DCN receives Packet-In packets from CE1800V switches. The value ranges from 1 to 200000, in PPS.
	PIR	Indicates the maximum rate at which the Agile Controller-DCN receives Packet-In packets from CE1800V switches. The value ranges from 1 to 400000, in PPS.

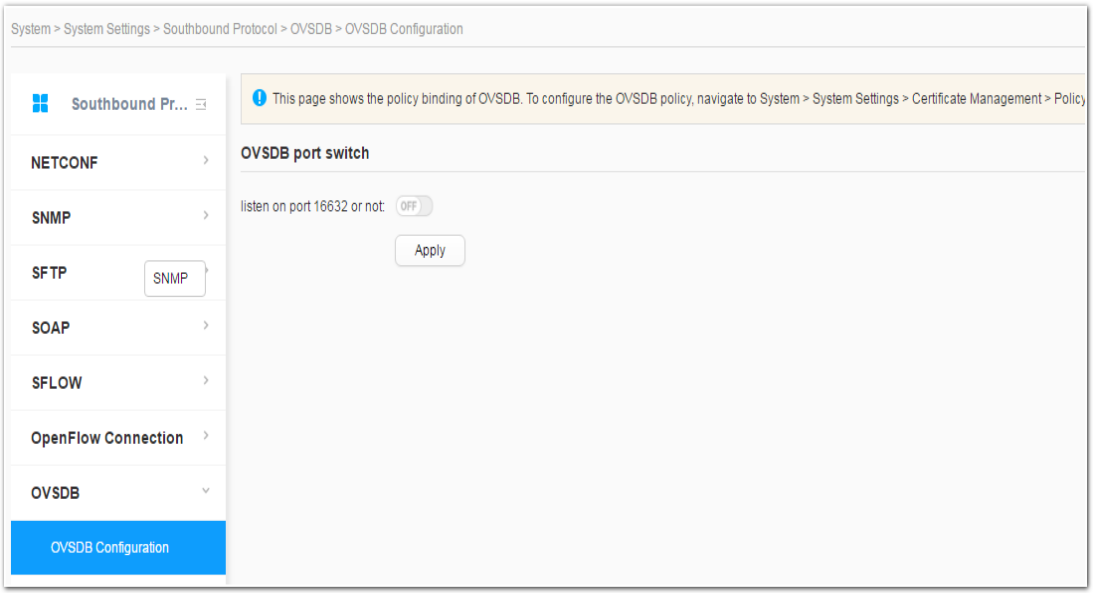
OpenFlow Statistics

1. Choose **System > System Settings > Southbound Protocol** from the main menu.
2. Choose **OpenFlow > OpenFlow Statistics** from the navigation tree on the left. The packet-in packet statistics page is displayed.

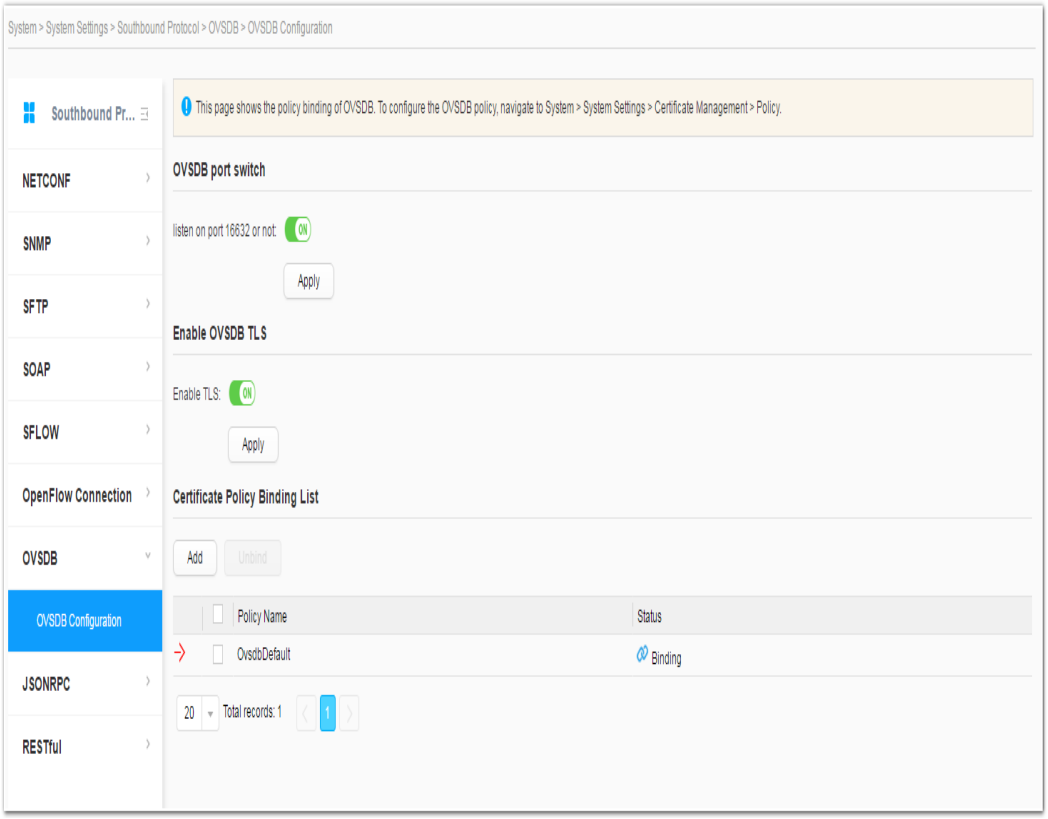


OVSDB

1. Choose **System > System Settings > Southbound Protocol** from the main menu.
2. Choose **OVSDB > OVSDB Configuration** from the navigation tree on the left. The **OVSDB Configuration** page is displayed.



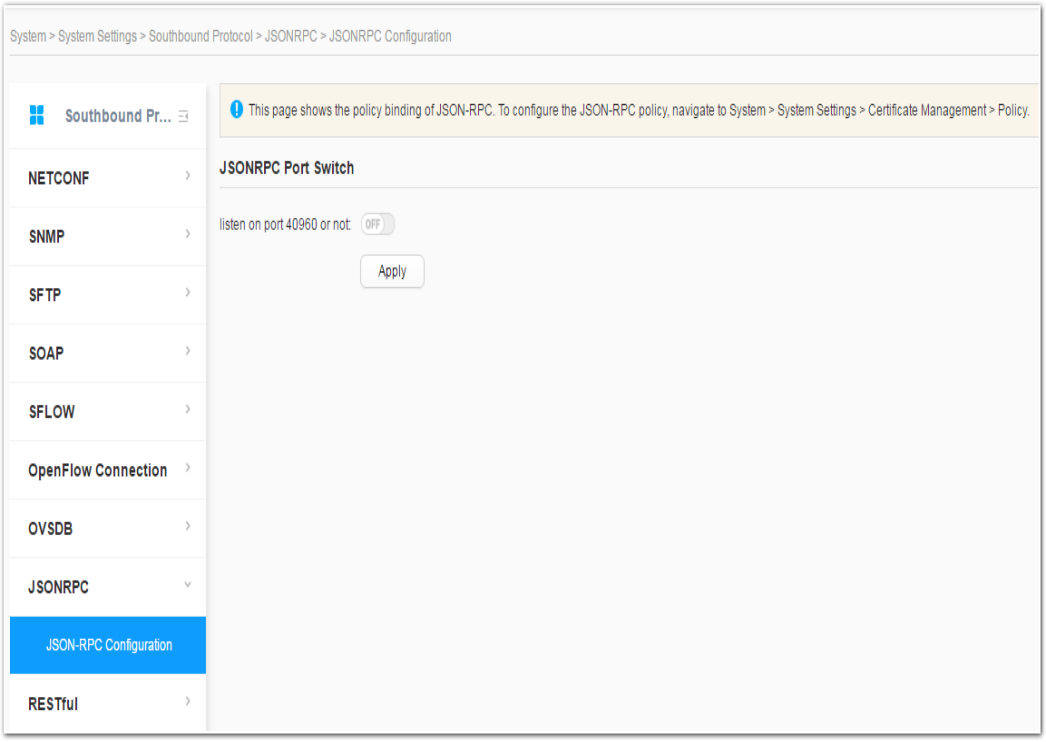
3. Set **listen on port 16632 or not**.
4. If **listen on port 16632 or not** is set to **ON**, click **Apply**, and go to 4.



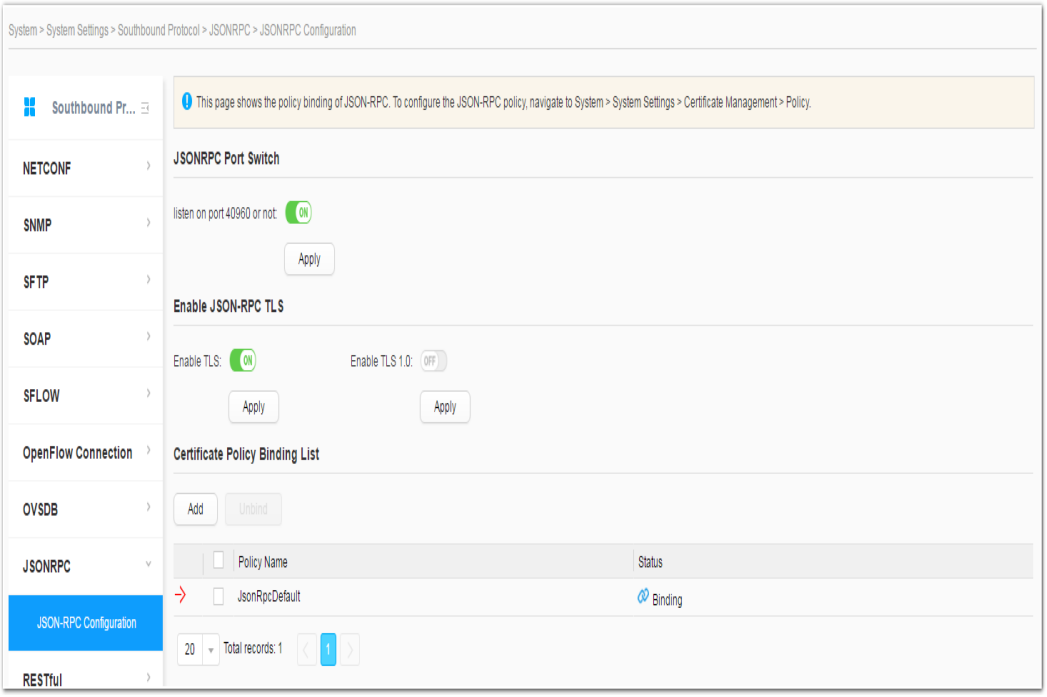
5. If **listen on port 16632 or not** is set to **OFF**, click **Apply**. The process ends.
6. Set **Enable TLS** and click **Apply**.
7. For details about creation and binding of the certificate policy, see Replacing the OVSDB Certificate Using the Certificate Management Tool.

JSONRPC

1. Choose **System > System Settings > Southbound Protocol** from the main menu.
2. Choose **JSONRPC > JSONRPC Configuration** from the navigation tree on the left. The JSONRPC configuration page is displayed.



3. Set **listen on port 40960 or not**.
4. If **listen on port 40960 or not** is set to **ON**, click **Apply**, and go to 4.



5. If **listen on port 40960 or not** is set to **OFF**, click **Apply**. The process ends.

6. Set **Enable TLS** and click **Apply**.
7. Set **Enable TLS 1.0** and click **Apply**.
8. For details about creation and binding of the certificate policy, see Replacing the jsonRPC Certificate Using the Certificate Management Tool.

RESTful

1. Choose System > System Settings > Southbound Protocol from the main menu.
2. Choose **RESTful > RESTful Configuration** from the navigation tree on the left.. The RESTful configuration page is displayed.
3. On the **Certificate Policy Binding List** tab page, click **Add**. On the **Policy List** page, click →. The certificate information is displayed. Select policies to be bound, and click **Bind**.