



## Recommendations

- Huawei Learning Website
  - <http://learning.huawei.com/en>
- Huawei e-Learning
  - <https://ilearningx.huawei.com/portal/#/portal/ebg/51>
- Huawei Certification
  - [http://support.huawei.com/learning/NavigationAction!createNavi?navId=\\_31&lang=en](http://support.huawei.com/learning/NavigationAction!createNavi?navId=_31&lang=en)
- Find Training
  - [http://support.huawei.com/learning/NavigationAction!createNavi?navId=\\_trainingsearch&lang=en](http://support.huawei.com/learning/NavigationAction!createNavi?navId=_trainingsearch&lang=en)



## More Information

- Huawei learning APP



# **SDN AC Protocols**

## **Introduction Practice Guide**



Huawei Training & Certification Huawei Training & Certification

# Contents

<b>Typical Application Scenarios of SDN Commonly Used Protocols .....</b>	<b>1</b>
<b>Southbound and Northbound Protocols Supported by the AC-DCN .....</b>	<b>2</b>
<b>Configuring Northbound Protocols .....</b>	<b>4</b>
Task Description .....	4
Version Information.....	4
Objectives .....	4
Background.....	4
Configuration Tasks .....	5
Login into AC controller.....	5
Northbound Protocols Setup .....	7
<b>Configuring Southbound Protocols .....</b>	<b>18</b>
Task Description .....	18
Version Information.....	18
Objectives .....	18
Background.....	19
Prerequisites.....	19
Configuration Tasks .....	19

---

# SDN Commonly Used Protocols Integrated Practice Guide

## Typical Application Scenarios of SDN Commonly Used Protocols

---

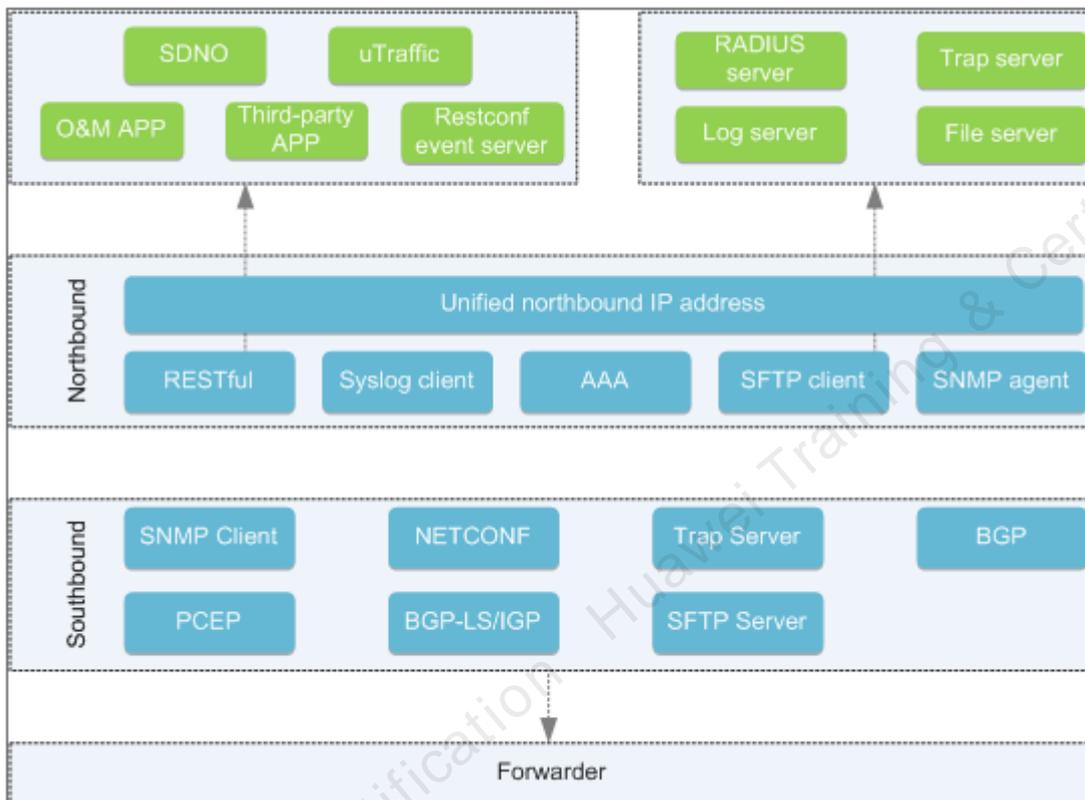
In conjunction with the rapid growth and emergence of SDN networks, various types of protocols are deployed, which might vary based on different SDN solutions applied according to live network applications. This section generally describes the commonly used protocols in SDN applications, such as Openflow,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

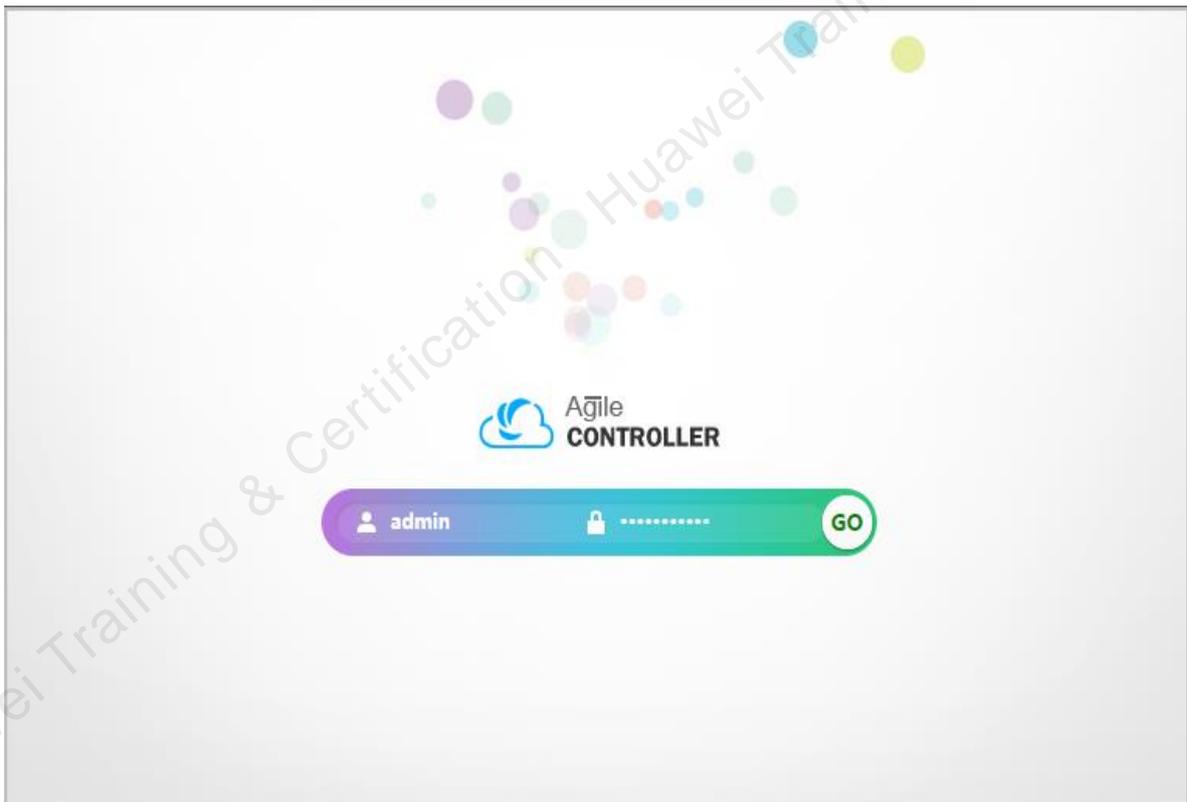
## Configuration Tasks

### Login into AC controller

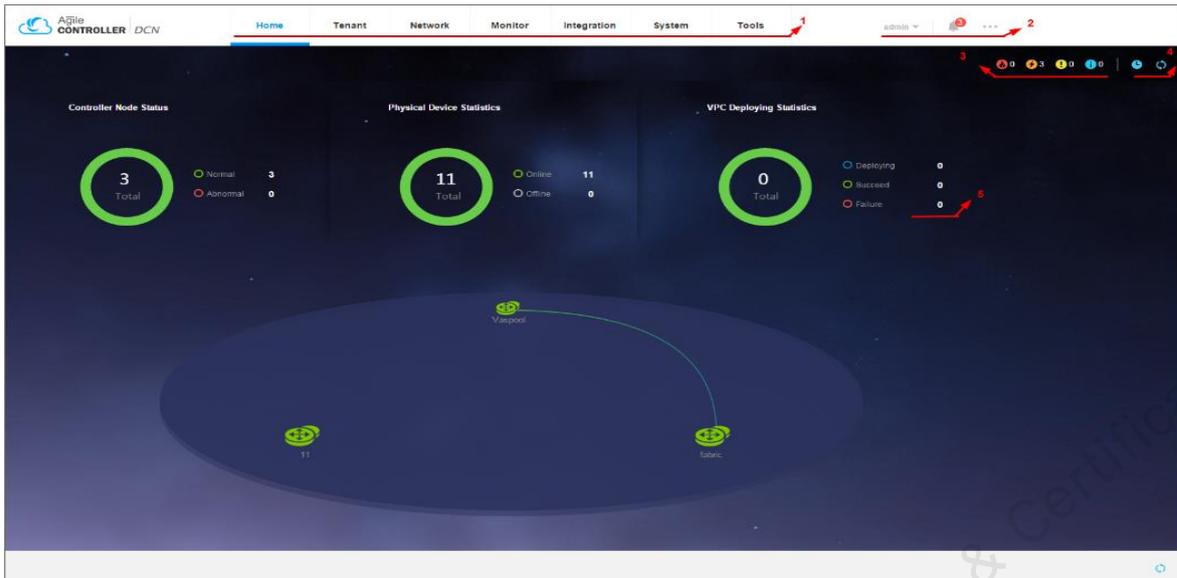
1. User Mozilla firefox to login into the AC controller via the management IP:
2. Enter **https:// AC-DCN server IP address:port number/index.html** in the address box, and press Enter. (example: https://100.0.100.40:18002)



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

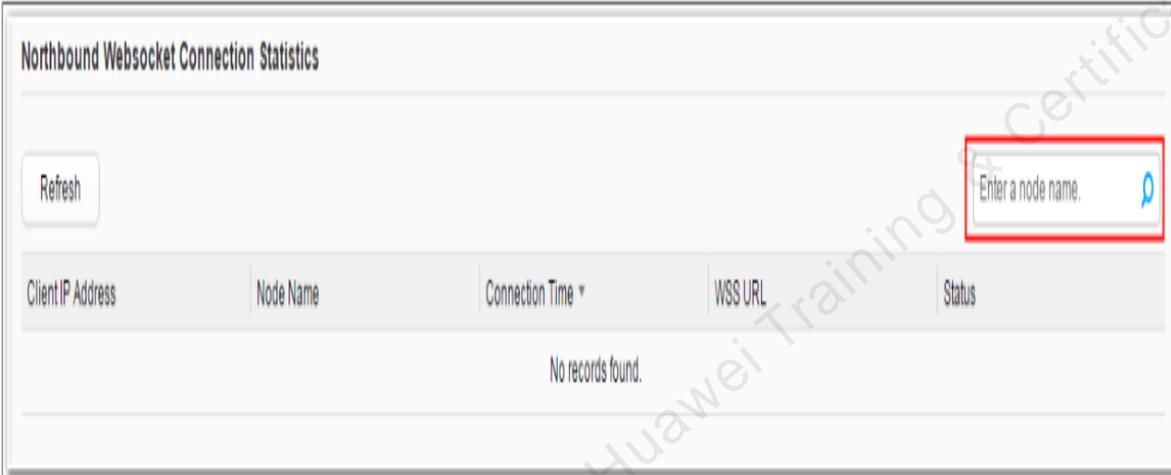


#### Northbound Connection Parameters

<p>Northbound Lock</p>	<p>Indicates the status of the northbound lock</p> <p>During online upgrade, RESTful/RESTCONF requests and WebSocket connections must be locked.</p> <p>After the locking:</p> <ul style="list-style-type: none"> <li>• Northbound RESTful/RESTCONF POST/PUT/DELETE requests are denied, and POST requests with the query parameter <b>op=get</b> are processed as GET.</li> <li>• WebSocket connection requests are denied.</li> </ul> <p>You can perform the following operations to unlock some unexpected RESTful/RESTCONF POST/PUT requests:</p> <ol style="list-style-type: none"> <li>1. Access the directory where the configuration file is stored. <pre># /opt/controller/naas/naas-karaf-1.0.1-SNAPSHOT/configuration/rest-not-lock</pre> </li> <li>2. Modify the lock.xml file as follows: <pre>&lt;not-allowed-locks &lt;allow-rule url="/proxy/ui/test" method = "POST"&gt; &lt;/ allow-rule &gt; &lt;/ not-allowed-locks &gt;</pre> </li> </ol> <p>Where:</p>
------------------------	--

	<ul style="list-style-type: none"> <li>• <b>url</b>: indicates full match of request URLs.</li> <li>• <b>method</b>: indicates the request method.</li> </ul> <p>Save the modification.</p>
--	---

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	<ul style="list-style-type: none"> <li>• connected</li> <li>• connecting</li> </ul>

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	<ul style="list-style-type: none"> <li>• http: HTTP transfers hypertext messages in plain text.</li> <li>• https: HTTPS supports SSL encryption and has high security.</li> <li>• ws: WebSocket is a full-duplex technology enabling communications between the browser and server.</li> <li>• wss: Secure WebSocket supports SSL encryption.</li> </ul>
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	<ul style="list-style-type: none"> <li>• pending</li> <li>• processing</li> </ul>

## 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.

System > System Settings > Northbound Protocol > RESTful > Performance Statistics

Northbound Pr...

RESTful

Northbound Connection

Performance Statistics

SNMP

SFTP

### Northbound RESTful/RESTCONF Protocol Packet Statistics

Clear All Export Refresh

Controller Node	Received Packets	Received Error Packets	Sent Packets	Unsuccessfully Sent Packets	Maximum Connections
controller-150-1-1-33	150368	1132	151500	0	20000
controller-150-1-1-34	177012	1628	178640	0	20000
controller-150-1-1-35	179676	1611	181287	0	20000
controller-150-1-1-88	0	0	0	0	20000
controller-150-1-1-89	0	0	0	0	20000
controller-150-1-1-90	0	0	0	0	20000

10 Total records: 6

### Northbound RESTful/RESTCONF Performance Statistics (ms)

Clear All Export Refresh

Controller Node	Processing Time	Standard Time Difference	Maximum Processing Time	Total Processing Time	Average Processing Time
controller-150-1-1-33	185394	63.66	13238	5674724	30.61
controller-150-1-1-34	181292	47.33	9393	6220615	34.31
controller-150-1-1-35	178635	53.02	7781	5435005	30.43
controller-150-1-1-88	0	0	0	0	0
controller-150-1-1-89	0	0	0	0	0
controller-150-1-1-90	0	0	0	0	0

10 Total records: 6

### Northbound WebSocket Packet Statistics

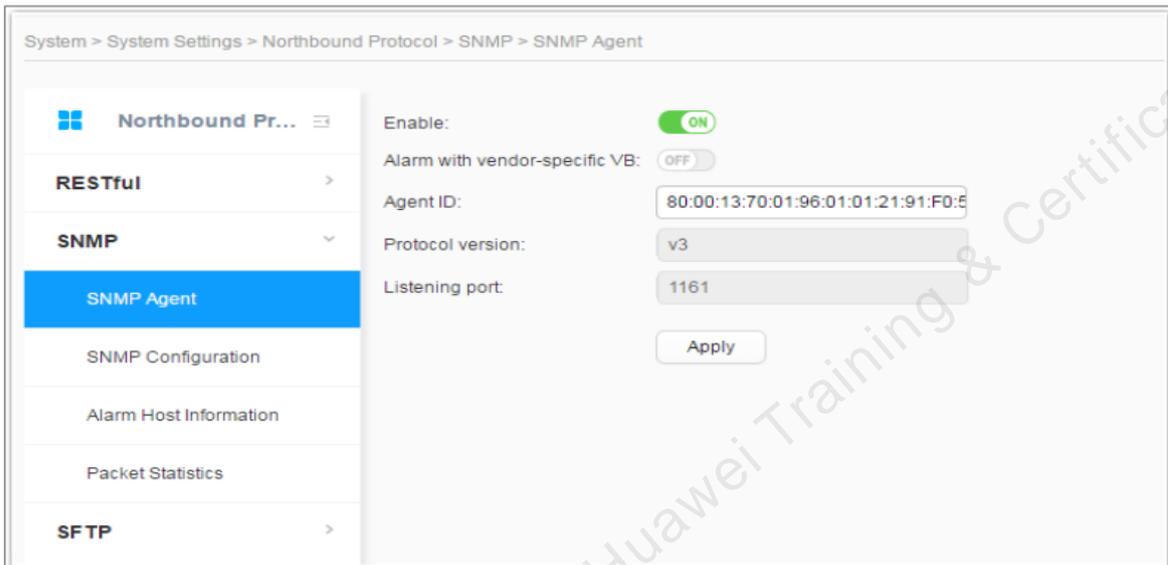
Refresh

Node Name	Sent Packets	Received Packets	Dropped Packets	Maximum Notification Rate
No records found.				

Parameter	Description
<b>Northbound RESTful/RESTCONF Protocol Packet Statistics</b>	
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.
<b>Northbound RESTful/RESTCONF Performance Statistics (Time Unit: ms)</b>	
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.
<b>Northbound WebSocket Packet Statistics</b>	
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 <b>ON</b> .
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. <b>NOTE:</b> 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

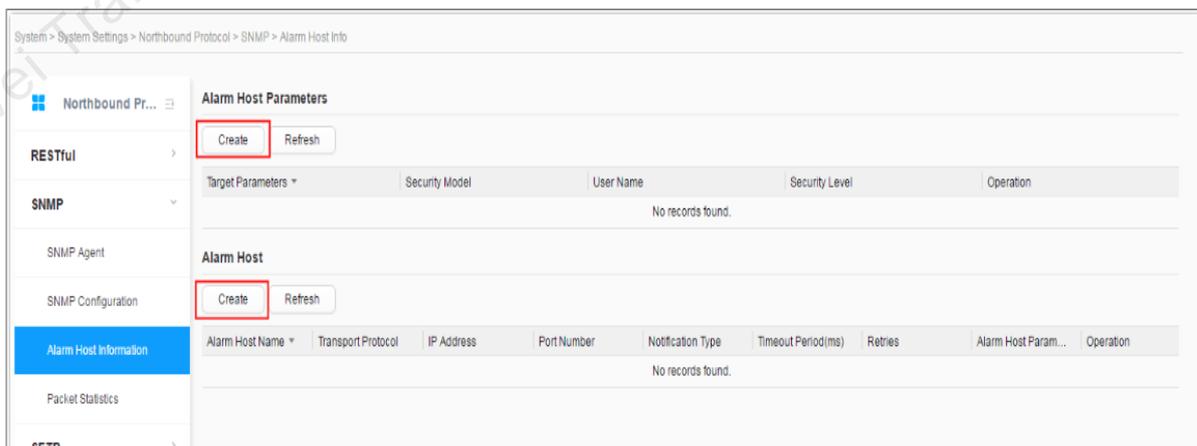
1. Choose **System > System Settings > Northbound Protocol** from the main menu.
2. Choose **SNMP > SNMP Configuration** from the navigation tree on the left. The SNMP Configuration page is displayed.
3. You can create and view MIB view information, group Information, and user information on the **SNMP 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: <ul style="list-style-type: none"> <li>• auth-priv: authentication and encryption</li> <li>• auth-no-priv: authentication and non-encryption</li> <li>• no-auth-no-priv: non-authentication and non-encryption</li> </ul>

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

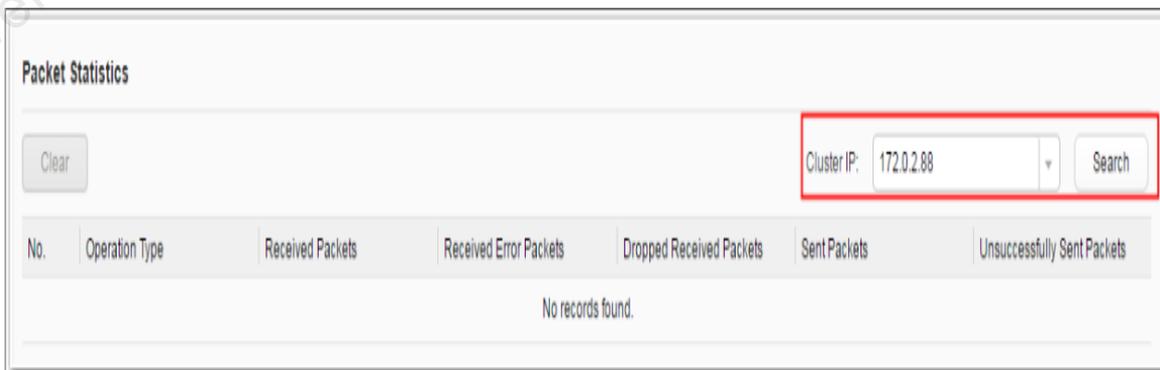
1. Choose **System > System Settings > Northbound Protocol** from the main menu.
2. Choose **SNMP > Alarm Host Info** from the navigation tree on the left. The Alarm Host Info page is displayed.
3. You can create and view alarm host parameters and alarm host on the **Alarm Host Information** page.



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	<ul style="list-style-type: none"> <li>• auth-priv: authentication and encryption</li> <li>• auth-no-priv: authentication and non-encryption</li> <li>• no-auth-no-priv: non-authentication and non-encryption</li> </ul>
Alarm Host	
Notification Type	<ul style="list-style-type: none"> <li>• Trap message: Trap messages have poor reliability because senders cannot determine whether recipients have received the trap messages.</li> <li>• Inform message: Inform messages have high reliability because a mechanism is present for determining whether recipients have received the Inform messages.</li> </ul>
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.



Packet Statistics

Clear

Cluster IP: 172.0.2.88 Search

No.	Operation Type	Received Packets	Received Error Packets	Dropped Received Packets	Sent Packets	Unsuccessfully Sent Packets
No records found.						

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

Fault Records

Clear

Cluster IP: 172.0.2.88 Search

Operation Type	First Fault Occurrence Ti...	Downtime	Consecutive Failure Times	Failure Cause	User Name	Remarks
No records found.						

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

## SFTP

- Choose **System > System Settings > Northbound Client Settings** from the main menu.
- Choose **SFTP > Northbound Client Settings** from the navigation tree on the left. **The Northbound Client Settings** page is displayed.

System > System Settings > Northbound Protocol > SFTP > Northbound Client Settings

**Northbound Client Settings**

When configuring server interfaces, do not use known interfaces in the communication matrix. If the file cannot be uploaded, try other interfaces.

\* Cluster IP:  \* Client file:

\* Server address:

\* Server port:

\* Login user name:

\* Login password:

**Historical Tasks**

No.	Server Address	Server Port	Operation	Client File	Operation Time	Status
No records found.						

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 commissioning 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 Protocol** 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.

System > System Settings > Southbound Protocol > NETCONF > NETCONF Connection

Southbound Pr... ▾

NETCONF ▾

NETCONF Connection

Performance Statistics

SNMP ▾

SFTP ▾

SOAP ▾

SFLOW ▾

OpenFlow Connection ▾

OVSDB ▾

.JSONRPC ▾

**Southbound NETCONF Connection Information**

Refresh

Cluster IP: 172.0.2.88 Search

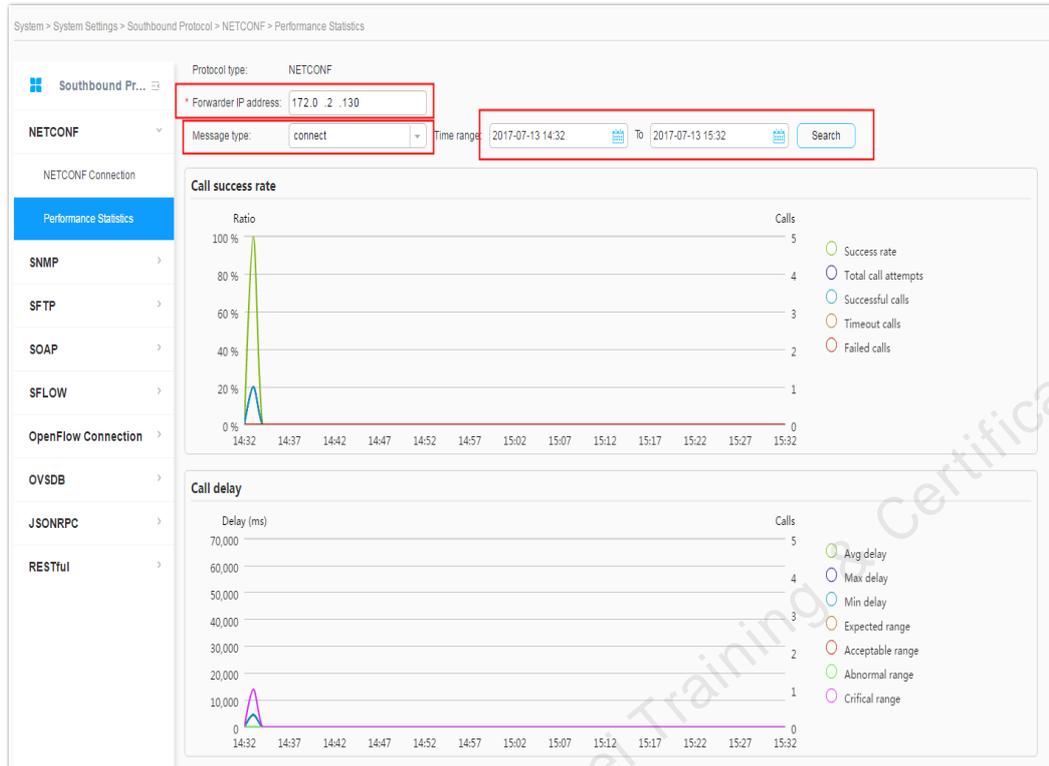
No.	IP Address	Port	Session ID	Connection Time	Message ID	Locked	Status
1	172.0.2.130	830	11398	2017-07-13 01:11:53		No	Normal
2	172.0.2.210	22	516	2017-07-13 01:10:20		No	Normal
3	172.0.2.211	22	532	2017-07-13 01:10:19		No	Normal
4	172.0.2.236	830	5141	2017-07-13 01:11:53		No	Normal
5	172.0.2.202	22	5456	2017-07-13 01:10:19		No	Normal
6	172.0.2.213	22	205	2017-07-13 03:46:27		No	Normal
7	172.0.2.235	830	4986	2017-07-13 01:11:53		No	Normal
8	172.0.2.204	22	226	2017-07-13 03:35:04		No	Normal
9	172.0.2.207	22	4283	2017-07-13 01:10:19		No	Normal
10	172.0.2.208	22	5957	2017-07-13 01:10:19		No	Normal

20 Total records: 10

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: <ul style="list-style-type: none"> <li><b>Yes:</b> The configuration database is locked to prevent operation conflicts. Other users cannot modify the data of this database.</li> <li><b>No:</b> The configuration database is not locked. Be sure to lock it before modifying its data.</li> </ul>
Status	Connection status: <ul style="list-style-type: none"> <li>Normal</li> <li>Disconnected</li> </ul>

## 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	<p>Message type for protocol operations:</p> <ul style="list-style-type: none"> <li><b>connect</b>: establishes a connection between the controller and forwarder.</li> <li><b>get</b>: obtains data from the running configuration database or device statistics.</li> <li><b>get-config</b>: obtains data from the running, candidate, or startup database.</li> <li><b>edit-config</b>: modifies a configuration database.</li> <li><b>notification</b>: indicates a notification message sent from the forwarder to the controller.</li> </ul>
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**.

System > System Settings > Southbound Protocol > SNMP > SNMP Configuration

For security purposes, do not use repeated strings in a password, such as abc123abc123.

**Trap Service**

Enable:  OFF

Private netmanager:  OFF

Protocol version: v3

\* Listening port:

Apply

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

SNMPv3 Security Parameters

Create

User Name | Authentication Protocol | Private Key | Operations

\* User name: ACTrap\_

\* Authentication protocol: HMAC\_SHA

\* Authentication key:

\* Encryption algorithm: AES\_256

\* Private key:

Confirm Cancel

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.

System > System Settings > Southbound Protocol > SNMP > Packet Statistics

Southbound Pr... Packet Statistics

Clear Cluster IP: 172.0.2.88 Search

No.	Operation Type	Received Packets	Received Error Packets	Dropped Received Packets	Sent Packets	Unsuccessfully Sent Packets
1	GET	2104	0	0	2104	0
2	GET-WALK	6162	0	0	6162	0

20 Total records: 2

Packet Statistics

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

Fault Records

Clear Cluster IP: 172.0.2.89 Search

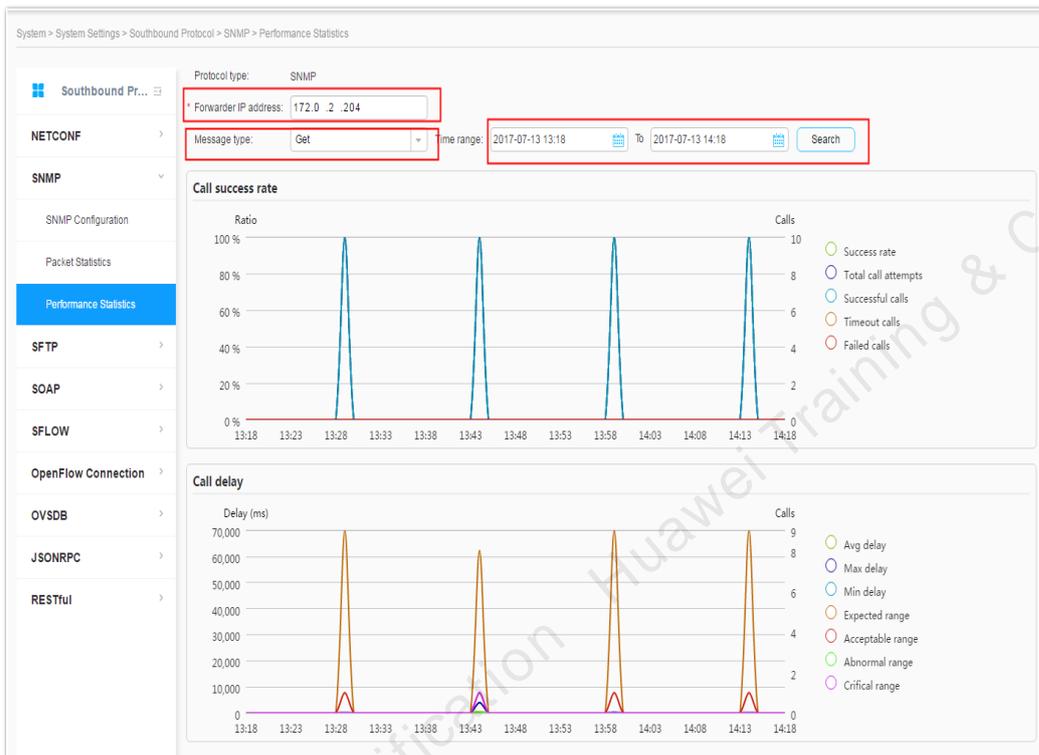
Device IP Address	Operation Type	First Fault Occurrence	Downtime	Consecutive Failure	Failure Cause	User Name	Remarks
172.0.2.204	GET	2017-07-13 09:06:32	2017-07-13 09:06:32	1	response is null	ac1	1.3.6.1.2.1.1.1.0
172.0.2.212	GET	2017-07-13 09:06:20	2017-07-13 09:06:20	1	engineID is null	ac1	
172.0.2.203	GET	2017-07-13 09:06:20	2017-07-13 09:06:20	1	engineID is null	ac1	

20 Total records: 3

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

## SNMP Performance Statistics

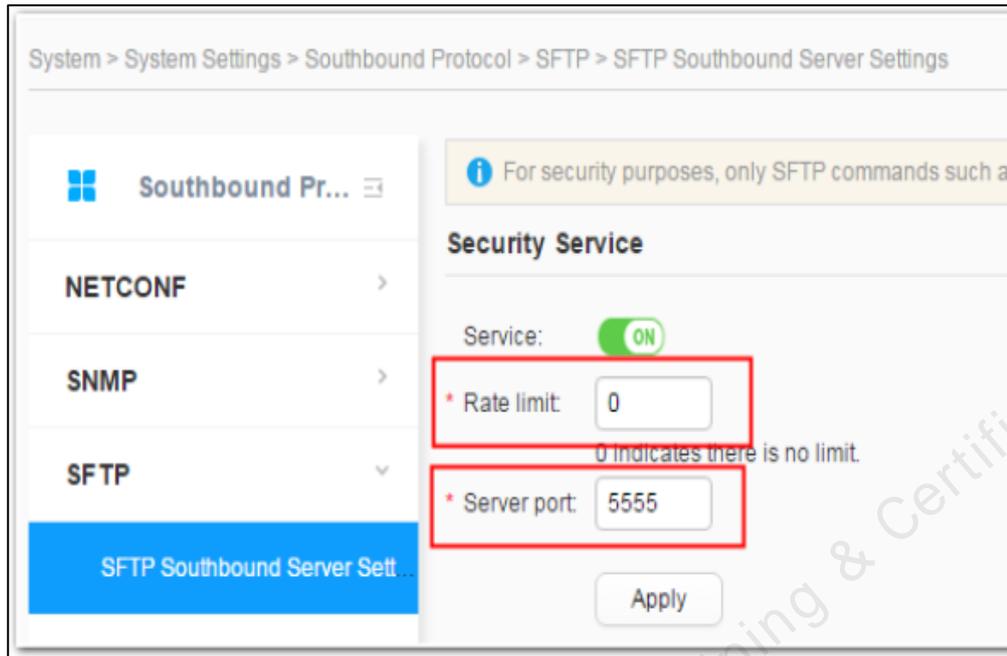
1. Choose System > System Settings > Southbound Protocol from the main menu.
2. Choose SNMP > Performance Statistics from the navigation tree on the left.
3. Set the IP address of the forwarder. Select a message type. Set the time range which needs to be less than one hour. Click Search. The statistics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



Parameter	Description
Forwarder IP address	Forwarder IP address
Message type	Message type for protocol operations: <ul style="list-style-type: none"> <li>• Get: value of the OID obtained from the MIB.</li> <li>• Get-Next: value of the next OID obtained from the MIB.</li> <li>• Trap: alarm sent from the Agent to the NMS.</li> </ul>
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** dropdown list box and click **Search**. Information about clients connected to the SFTP server is displayed.

Parameter		Description
Security Service	Service	<ul style="list-style-type: none"> <li>• ON</li> <li>• OFF</li> </ul>
	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.

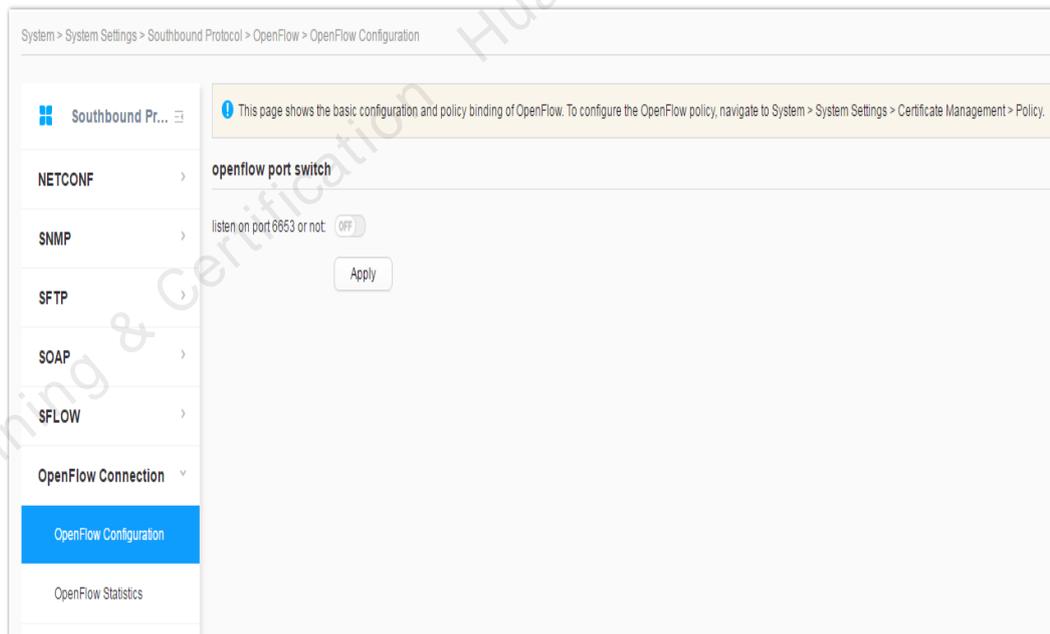
## SFLOW

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.

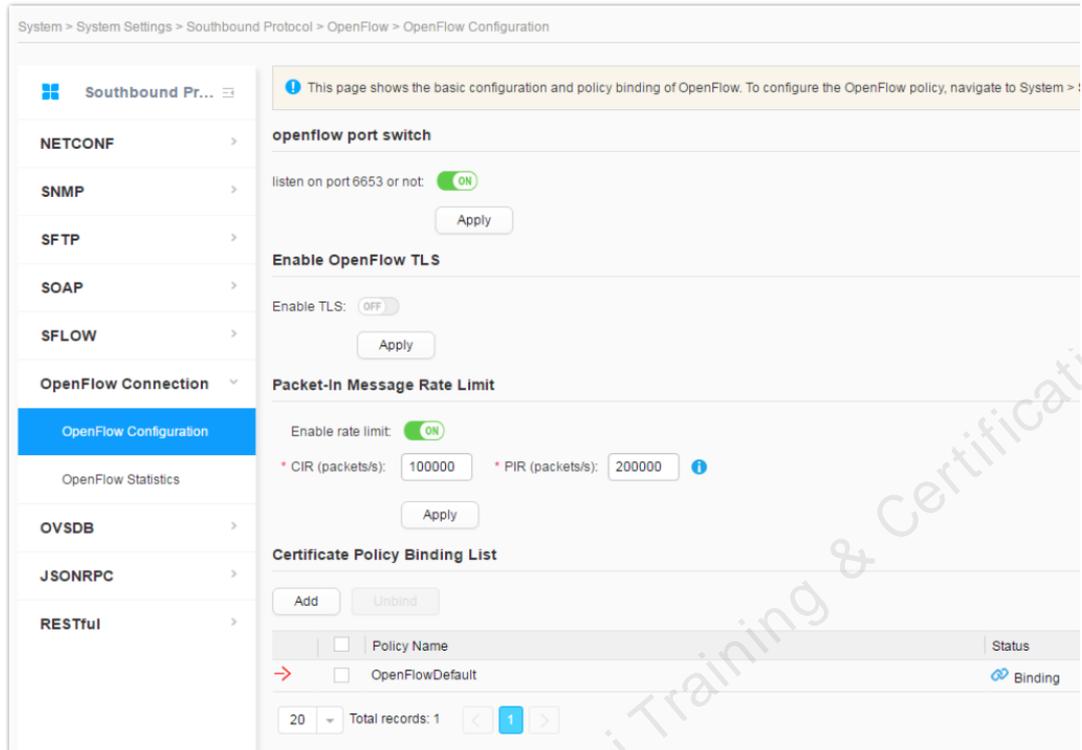
## OpenFlow

### 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	<ul style="list-style-type: none"> <li>• ON:Yes</li> <li>• OFF:No</li> </ul>
Enable TLS	Enable TLS	<ul style="list-style-type: none"> <li>• ON:Enable</li> <li>• OFF:Disable</li> </ul>
OpenFlow Packet-In Rate Limit Configuration	Enable rate limit	<ul style="list-style-type: none"> <li>• ON:Enable</li> <li>• OFF:Disable</li> </ul>
	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.

System > System Settings > Southbound Protocol > OpenFlow > OpenFlow Statistics

Southbound Pr... **OpenFlow Statistics**

Refresh Controller Node: --Select-- Search

Controller Node	Southbound IP Address	Received Packet-In Messages	Sent Packet-In Messages	Dropped Packet-In Messages
node-1	172.0.2.88	0	0	0
node-2	172.0.2.89	0	0	0
node-3	172.0.2.90	0	0	0

20 Total records: 3

OpenFlow Configuration

OpenFlow Statistics

## 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.

System > System Settings > Southbound Protocol > OVSDB > OVSDB Configuration

Southbound Pr... **OVSDB Configuration**

This page shows the policy binding of OVSDB. To configure the OVSDB policy, navigate to System > System Settings > Certificate Management > Policy

**OVSDB port switch**

listen on port 16632 or not: OFF

Apply

SNMP

OpenFlow Connection

OVSDB

OVSDB Configuration

# CE Switch VXLAN Feature Practice Guide



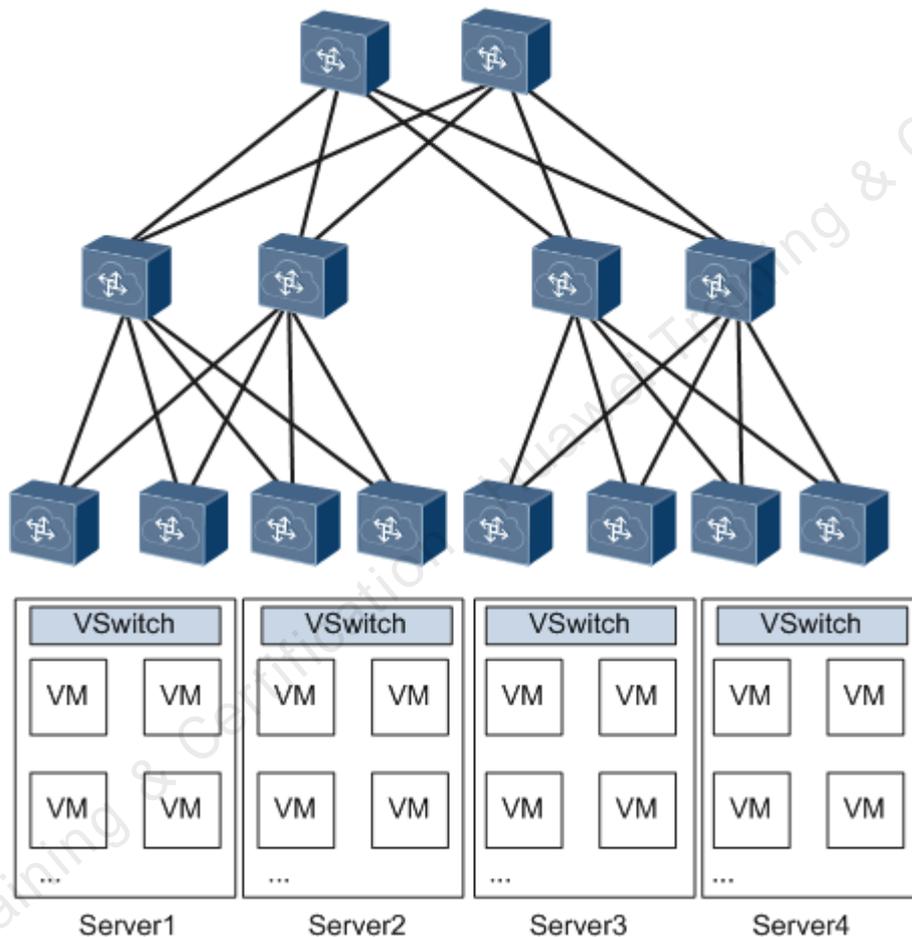
# Contents

<b>Typical Application Scenario of VXLAN .....</b>	<b>2</b>
<b>Example for VXLAN Feature Practice .....</b>	<b>4</b>
VXLAN Basic Operation Experimental Environment .....	4
Objectives .....	4
Topology .....	4
Reference .....	5
Practice Tasks .....	6
Data Preparation .....	6
Procedure chart .....	7
<b>Configuring User on the Same Network Segment VXLAN .....</b>	<b>8</b>
Step 1 Configure a routing protocol OSPF .....	8
Related Command Introduction .....	8
Configure Device 1 .....	8
Configure Device 2 .....	9
Configure Device 3 .....	9
Verification .....	10
Step 2 Configure VXLAN Tunnel Mode .....	11
Related Command Introduction .....	11
Configure Device 1 .....	11
Configure Device 3 .....	11
Step 3 Configure VXLAN Service Access Point .....	11
Related Command Introduction .....	11
Configure Device 1 .....	12
Configure Device 3 .....	12
Step 4 Configure VXLAN Tunnel .....	12
Related Command Introduction .....	12
Configure Device 1 .....	12
Configure Device 3 .....	13
Verification .....	13
FAQ .....	14
FAQ Answer .....	15

# Typical Application Scenario of VXLAN

As defined by RFC 7348, VXLAN is a Network Virtualization over Layer 3 (NVO) technology that uses MAC in User Datagram Protocol (MAC-in-UDP) to encapsulate packets.

Server virtualization is a critical cloud computing technology, and has been widely deployed because it significantly reduces IT and operation and maintenance (O&M) costs and facilitates more flexible service deployment.



**Figure 1** Server virtualization networking

On the network shown in Figure 1, one server is virtualized into multiple virtual machines (VMs), each of which acts as a host. However, the exponential increase in the number of hosts leads to the following problems on a virtual network:

- The number of VMs is limited by network performance.

On a large Layer 2 network, data packets are forwarded based on MAC address entries. Therefore, the number of VMs supported on the network depends on the MAC address table size.

- Network isolation capabilities are limited.

Most networks use VLANs or virtual private networks (VPNs) for network isolation. However, these two network isolation technologies have the following limitations on large-scale virtualized networks:

- The VLAN tag field, as defined in IEEE 802.1Q, has only 12 bits, and can only identify a maximum of 4096 VLANs, making it insufficient for identifying users on large Layer 2 networks.
- VLANs or VPNs cannot support dynamic network adjustment on traditional Layer 2 networks.
- VM migration scope is limited by the network architecture.

After VMs are started, they may need to be migrated from one server to another due to server resource problems (for example, CPU overload or insufficient memory). To ensure uninterrupted services during VM migration, the IP and MAC addresses of VMs must remain unchanged. To meet this requirement, the service network must be a Layer 2 network that provides multipath redundancy and reliability.

VXLAN addresses the above problems on large Layer 2 networks as follows:

- VM scale limitations imposed by network performance

VXLAN encapsulates data packets sent from VMs into UDP packets and encapsulates IP and MAC addresses used on the physical network into outer headers. The network is only aware of the encapsulated parameters. This greatly reduces the number of MAC address entries required on large Layer 2 networks.
- Limited network isolation capabilities

VXLAN uses a VXLAN network identifier (VNI) field similar to the VLAN ID field defined in IEEE 802.1Q. The VNI field has 24 bits and can identify a maximum of 16M  $[(2^{24}-1)/1024^2]$  VXLAN segments.
- VM migration scope limitations imposed by network architecture

When VXLAN is used to construct a large Layer 2 network, VM IP and MAC addresses can remain unchanged after VM migration.

When server virtualization is widely deployed in data centers based on physical network infrastructure, VXLAN offers the following benefits:

- Supports a maximum of 16M VXLAN segments with 24-bit VNIs, so a data center can accommodate a large number of tenants.
- Reduces the number of MAC addresses that network devices need to learn and enhances network performance because only devices at the edge of the VXLAN network need to identify VM MAC addresses.
- Extends Layer 2 networks using MAC-in-UDP encapsulation and decouples physical and virtual networks. Tenants can plan their own virtual networks, without being limited by the physical network IP addresses or broadcast domains. This greatly simplifies network management.

## Example for VXLAN Feature Practice

---

### VXLAN Basic Operation Experimental Environment

This practice guide describes configuration methods and process of basic operation of VXLAN Platform.

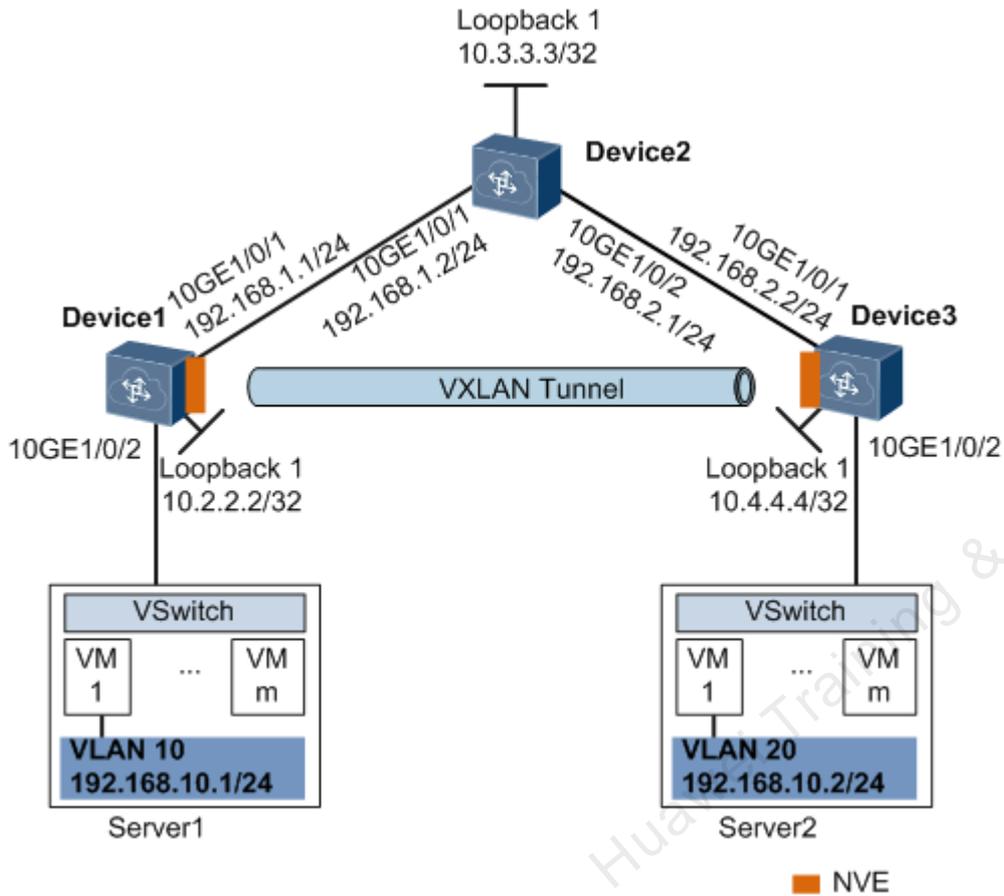
### Objectives

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

- Complete basic operation of configuring VXLAN tunnel on the same network segment.
- Troubleshooting VXLAN regular faults

### Topology

On the network shown in Figure 2, an enterprise has VMs deployed in different data centers. VM1 on Server1 belongs to VLAN10, and VM1 on Server2 belongs to VLAN20. VM1 on Server1 and VM1 on Server2 reside on the same network segment. To allow VM1s in different data centers to communicate with each other, configure a VXLAN tunnel between Device1 and Device3.



**Figure 2** Configuring users on the same network segment to communicate through a VXLAN tunnel

## Reference

- CloudEngine 12800 product documentation
- CloudEngine 7800&6800&5800 production documentation.

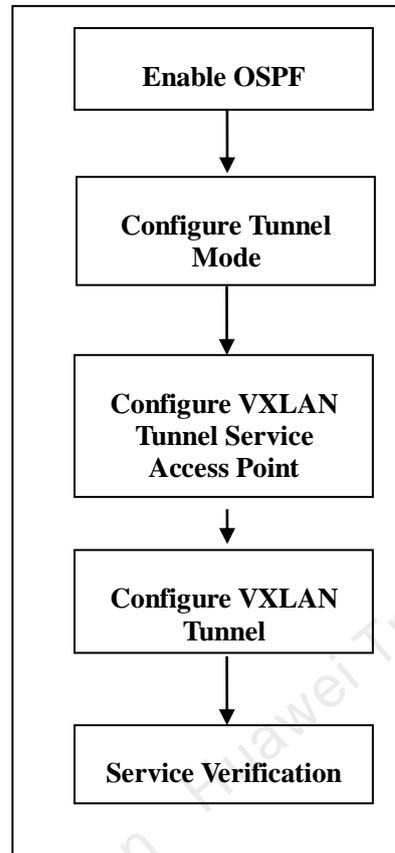
## Practice Tasks

Task	Description
1	Cabling the physical connection according to the topology
2	Configure a routing protocol on Device1, Device2, and Device3 to allow them to communicate at Layer 3.
3	Configure a service access point on Device1 and Device3 to differentiate service traffic.
4	Configure a VXLAN tunnel on Device1 and Device3 to forward service traffic.
5	Service verification

## Data Preparation

- VMs' VLAN IDs (10 and 20)
- Interface IP addresses for device interconnection
- Routing protocol: Open Shortest Path First (OSPF)
- BD ID (10)
- VNI ID (5010)

## Procedure chart



# Configuring User on the Same Network Segment VXLAN

## Step 1 Configure a routing protocol OSPF

### Related Command Introduction

Operation	Description	Commands
Setup OSPF process	[~Huawei]	ospf [process-id]
OSPF area	[~Huawei-ospf-1]	area [area-id]
Advertise the network	[~Huawei-ospf-1-area-0.0.0.1]	network-[ip-address-wildcard-mask]
Change the network Type of interface	[~Huawei-10GE1/0/1]	undo portswitch

### Configure Device 1

```

<HUAWEI> system-view
[~HUAWEI] sysname Device1
[*HUAWEI] commit
[~Device1] interface loopback 1
[*Device1-LoopBack1] ip address 10.2.2.2 32
[*Device1-LoopBack1] quit
[*Device1] interface 10ge 1/0/1
[*Device1-10GE1/0/1] undo portswitch
[*Device1-10GE1/0/1] ip address 192.168.1.1 24
[*Device1-10GE1/0/1] quit
[*Device1] ospf
[*Device1-ospf-1] area 0
[*Device1-ospf-1-area-0.0.0.0] network 10.2.2.2 0.0.0.0
[*Device1-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[*Device1-ospf-1-area-0.0.0.0] quit
[*Device1-ospf-1] quit
[*Device1] commit

```

## Configure Device 2

```
<HUAWEI> system-view
[~HUAWEI] sysname Device2
[*HUAWEI] commit
[~Device2] interface loopback 1
[*Device2-LoopBack1] ip address 10.3.3.3 32
[*Device2-LoopBack1] quit
[*Device2] interface 10ge 1/0/1
[*Device2-10GE1/0/1] undo portswitch
[*Device2-10GE1/0/1] ip address 192.168.1.2 24
[*Device2-10GE1/0/1] quit
[*Device2] interface 10ge 1/0/2
[*Device2-10GE1/0/1] undo portswitch
[*Device2-10GE1/0/1] ip address 192.168.2.1 24
[*Device2-10GE1/0/1] quit
[*Device2] ospf
[*Device2-ospf-1] area 0
[*Device2-ospf-1-area-0.0.0.0] network 10.3.3.3 0.0.0.0
[*Device2-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[*Device2-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[*Device2-ospf-1-area-0.0.0.0] quit
[*Device2-ospf-1] quit
[*Device2] commit
```

## Configure Device 3

```
<HUAWEI> system-view
[~HUAWEI] sysname Device3
[*HUAWEI] commit
[~Device3] interface loopback 1
[*Device3-LoopBack1] ip address 10.4.4.4 32
[*Device3-LoopBack1] quit
[*Device3] interface 10ge 1/0/1
[*Device3-10GE1/0/1] undo portswitch
[*Device3-10GE1/0/1] ip address 192.168.2.2 24
[*Device3-10GE1/0/1] quit
[*Device3] ospf
[*Device3-ospf-1] area 0
[*Device3-ospf-1-area-0.0.0.0] network 10.4.4.4 0.0.0.0
[*Device3-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
```

```
[*Device3-ospf-1-area-0.0.0.0] quit
[*Device3-ospf-1] quit
[*Device3] commit
```

## Verification

- 1) By using **display ospf 1 peer brief** to check whether the OSPF peer state is up or not. Take device 1 for example.

```
[Device 1]display ospf 1 peer brief
      OSPF Process 1 with Router ID 10.2.2.2
```

### Peer Statistic Information

Area Id	Interface	Neighbor id	State
0.0.0.0	10GE0/0/1	10.3.3.3	Full

- 2) We can use **display ospf routing** to examine the OSPF routing information.

```
[~Device1] display ospf routing
OSPF Process 1 with Router ID 10.1.1.1
Routing for Network
```

Destination	Cost	Type	NextHop	AdvRouter	Area
10.3.3.3/32	2	Transit	192.168.1.2	10.3.3.3	0.0.0.0
10.4.4.4/32	3	Transit	192.168.1.2	10.4.4.4	0.0.0.0
192.168.1.0/24	1	Direct	192.168.1.1	10.1.1.1	0.0.0.0
192.168.2.0/24	1	Transit	192.168.1.2	10.3.3.3	0.0.0.0
10.2.2.2/32	1	Direct	192.168.1.1	10.2.2.2	0.0.0.0

Total Nets: 5

Intra Area: 3 Inter Area: 0 ASE: 0 NSSA: 0

- 3) After OSPF is configured, the devices can use OSPF to learn the IP addresses of loopback interfaces of each other and successfully **ping** each other. The following example shows the command output on Device1 after it pings Device3:

```
[~Device1]ping 10.3.3.3
PING 10.3.3.3: 56 data bytes, press CTRL_C to break
  Reply from 10.3.3.3: bytes=56 Sequence=1 ttl=255 time=50 ms
  Reply from 10.3.3.3: bytes=56 Sequence=2 ttl=255 time=1 ms
  Reply from 10.3.3.3: bytes=56 Sequence=3 ttl=255 time=30 ms
  Reply from 10.3.3.3: bytes=56 Sequence=4 ttl=255 time=30 ms
```

```

Reply from 10.3.3.3: bytes=56 Sequence=5 ttl=255 time=60 ms
--- 1.1.1.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 1/34/60 ms

```

## Step 2 Configure VXLAN Tunnel Mode

### Related Command Introduction

Operation	Description	Commands
Setup OSPF process	[~Huawei]	ospf [process-id]
OSPF area	[~Huawei-ospf-1]	area [area-id]
Advertise the network	[~Huawei-ospf-1-area-0.0.0.1]	network- [ip-address-wildcard-mask]
Change the network Type of interface	[~Huawei-10GE1/0/1]	undo portswitch

### Configure Device 1

```

[~Device1] ip tunnel mode vxlan
[*Device1] commit

```

### Configure Device 3

```

[~Device3] ip tunnel mode vxlan
[*Device3] commit

```

## Step 3 Configure VXLAN Service Access Point

### Related Command Introduction

Operation	Description	Commands
Configure Bridge Domain	[~Huawei]	bridge-domain id

## Configure Device 1

```
[~Device1] bridge-domain 10
[*Device1-bd10] quit
[*Device1] interface 10ge 1/0/2.1 mode 12
[*Device1-10GE1/0/2.1] encapsulation dot1q vid 10
[*Device1-10GE1/0/2.1] bridge-domain 10
[*Device1-10GE1/0/2.1] quit
[*Device1] commit
```

## Configure Device 3

```
[~Device3] bridge-domain 10
[*Device3-bd10] quit
[*Device3] interface 10ge 1/0/2.1 mode 12
[*Device3-10GE1/0/2.1] encapsulation dot1q vid 10
[*Device3-10GE1/0/2.1] bridge-domain 10
[*Device3-10GE1/0/2.1] quit
[*Device3] commit
```

## Step 4 Configure VXLAN Tunnel

### Related Command Introduction

Operation	Description	Commands
Define VNI id	[~Huawei]	vxlan vni id
Define VNI interface	[*Huawei-Nve1]	vni id head-end peer-list ip-address

## Configure Device 1

```
[~Device1] bridge-domain 10
[~Device1-bd10] vxlan vni 5010
[*Device1-bd10] quit
[*Device1] interface nve 1
[*Device1-Nve1] source 10.2.2.2
[*Device1-Nve1] vni 5010 head-end peer-list 10.4.4.4
[*Device1-Nve1] quit
[*Device1] commit
```

## Configure Device 3

```
[~Device3] bridge-domain 10
[~Device3-bd10] vxlan vni 5010
[*Device3-bd10] quit
[*Device3] interface nve 1
[*Device3-Nve1] source 10.4.4.4
[*Device3-Nve1] vni 5010 head-end peer-list 10.2.2.2
[*Device3-Nve1] quit
[*Device3] commit
```

## Verification

1) After the VXLAN tunnel configuration, we can use **display vxlan vni** command to check the state of the VXLAN tunnel.

```
[~Device1] display vxlan vni
Number of vxlan vni : 1
VNI          BD-ID          State
-----
5010         10             up
```

```
[~Device1] display vxlan tunnel
Number of vxlan tunnel : 1
```

Tunnel ID	Source	Destination	State	Type
4026531841	10.2.2.2	10.4.4.4	up	static

2) Try to **ping** the IP address from one server to the opposite server in the VXLAN domain.

```
PING 192.168.10.2: 56 data bytes, press CTRL_C to break
  Reply from 192.168.10.2: bytes=56 Sequence=1 ttl=255 time=50 ms
  Reply from 192.168.10.2: bytes=56 Sequence=2 ttl=255 time=1 ms
  Reply from 192.168.10.2: bytes=56 Sequence=3 ttl=255 time=30 ms
  Reply from 192.168.10.2: bytes=56 Sequence=4 ttl=255 time=30 ms
  Reply from 192.168.10.2: bytes=56 Sequence=5 ttl=255 time=60 ms
--- 1.1.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/34/60 ms
```

## FAQ

1. How to verify the status of VXLAN tunnel?
2. Try to explain the concept VTEP、VNI、VAP in VXLAN.
3. What is the deployment of VXLAN?

Huawei Training & Certification Huawei Training & Certification

## FAQ Answer

1. display vxlan vni.
2. VXLAN tunnel endpoint (VTEP): A VXLAN tunnel endpoint that encapsulates and decapsulates VXLAN packets. It is represented by an NVE.
  - 1) A VTEP connects to a physical network and is assigned a physical network IP address. This IP address is irrelevant to virtual networks.
  - 2) In VXLAN packets, the source IP address is the local node's VTEP address, and the destination IP address is the remote node's VTEP address. This pair of VTEP addresses corresponds to a VXLAN tunnel.

VXLAN network identifier (VNI): A VXLAN segment identifier similar to a VLAN ID. VMs on different VXLAN segments cannot communicate directly at Layer 2.

- 1) A VNI identifies only one tenant. Even if multiple terminal users belong to the same VNI, they are considered one tenant. A VNI consists of 24 bits and supports a maximum of 16M  $[(2^{24}-1)/1024^2]$  tenants.

Virtual access point (VAP): A Layer 2 sub-interface used to transmit data packets.

- 1) Layer 2 sub-interfaces can have different encapsulation types configured to transmit various types of data packets.

3. Currently, you can deploy a VXLAN network in Single-node mode or Controller mode.

- 1) Single-node mode: In the traditional network deployment mode, you need to log in to each device to configure the devices according to the network plan. Collaboration with cloud platforms cannot be implemented in cloud computing data centers for automatic network deployment.
- 2) Controller mode: To help control and deploy a large Layer 2 network, a controller can be used. A controller is a unified network control platform that orchestrates and manages network resources and cooperates with the cloud platform to implement automatic service and network provisioning.



## Recommendations

- Huawei Learning Website
  - <http://learning.huawei.com/en>
- Huawei e-Learning
  - <https://ilearningx.huawei.com/portal/#/portal/ebg/51>
- Huawei Certification
  - [http://support.huawei.com/learning/NavigationAction!createNavi?navId=\\_31&lang=en](http://support.huawei.com/learning/NavigationAction!createNavi?navId=_31&lang=en)
- Find Training
  - [http://support.huawei.com/learning/NavigationAction!createNavi?navId=\\_trainingsearch&lang=en](http://support.huawei.com/learning/NavigationAction!createNavi?navId=_trainingsearch&lang=en)



## More Information

- Huawei learning APP

