Enterprise Switch

User Guide

Issue	01
Date	2025-04-25

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

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 a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Enterprise Switches

1.1 Buying an Enterprise Switch

Scenarios

This section describes how to buy an enterprise switch. An enterprise switch allows Layer 2 communication between an on-premises data center and a VPC based on VPN or Direct Connect.

Prerequisites

- You have planned the resources required both on the cloud and on premises. For details about resource planning, see **How Enterprise Switches Work**.
- An enterprise switch establishes a Layer 2 network based on a Layer 3 network between an on-premises data center and a VPC created by Direct Connect or VPN. You need to create a Direct Connect or VPN connection first by referring to **Step 1: Use Direct Connect or VPN to Communicate at Layer 3**.

Notes and Constraints

- The switch in an on-premises data center must support VXLAN because the enterprise switch needs to establish a VXLAN tunnel to the data center at Layer 2.
- The local tunnel subnet must have three IP addresses reserved for the enterprise switch.

Procedure

1. Go to the **Buy Enterprise Switch** page.
2. Configure the parameters as prompted. For details, see **Table 1-1**.

Table 1-1 Parameters for creating an enterprise switch

Parameter	Description	Example Value
Billing Mode	Mandatory Enterprise switches can be billed on a yearly/monthly or pay-per-use basis. • If you buy a yearly/monthly enterprise switch, you need to make a one-off payment for the enterprise switch in your selected period. • If you buy a pay-per-use enterprise switch, your enterprise switch is billed by the second but settled by the hour. If the usage is less than an hour, you are billed based on the actual duration consumed. **NOTE** The yearly/monthly billing mode is available only in regions **LA-Santiago** and **AF-Johannesburg**.	Pay-per-use
Region	Mandatory Select the region nearest to you to ensure the lowest latency possible.	LA-Santiago
Active AZ	Mandatory Enterprise switches are deployed in active/standby mode. Select the AZ where the active node is deployed. An active AZ carries traffic. You can set the AZ to the one where your ECSs that need to communicate with an on-premises data center are deployed to ensure quick and uninterrupted access to ECSs.	AZ1
Standby AZ	Mandatory Enterprise switches are deployed in active/standby mode. Select the AZ where the standby node is deployed. A standby AZ is used for backup and disaster recovery. The standby AZ must be different from the active AZ.	AZ2

Parameter	Description	Example Value
Specifications	Mandatory Currently, the following enterprise switch specifications are supported: • Small – Maximum Bandwidth: 3 Gbit/s – Maximum PPS: 500,000 – Connected Subnets: 1 • Medium – Maximum Bandwidth: 5 Gbit/s – Maximum PPS: 1,000,000 – Connected Subnets: 3 • Large – Maximum Bandwidth: 10 Gbit/s – Maximum PPS: 2,000,000 – Connected Subnets: 6 The specifications cannot be changed after the enterprise switch is created.	Large
VPC	Mandatory VPC that the enterprise switch belongs to. If **Tunnel Connection** is set to **Direct Connect** or **VPN**, the VPC is set to the one that the Direct Connect virtual gateway or VPN gateway belongs to by default.	vpc-01
Tunnel Subnet	Mandatory Subnet of the VPC that the enterprise switch belongs to. It is the local tunnel subnet. Local and remote tunnel subnets communicate with each other at Layer 3 over Direct Connect or VPN. Enterprise switches allow communications between cloud and on-premises networks at Layer 2 based on the Layer 3 network between tunnel subnets.	subnet-01

Parameter	Description	Example Value
Local Tunnel IP Address	Mandatory IP address in the local tunnel subnet, which can be automatically assigned or manually specified. If an enterprise switch establishes a VXLAN tunnel with an on-premises data center at Layer 2, each end of the VXLAN tunnel requires a tunnel IP address (the local and remote tunnel IP addresses). The two IP addresses must be different.	Automatically assign IP address
Name	Mandatory Enter the name of the enterprise switch. The name: • Must contain 1 to 64 characters. • Can contain letters, digits, underscores (_), hyphens (-), and periods (.).	esw-01
Description	Optional Enter the description of the enterprise switch in the text box as required.	-
Required Duration	Specifies how long an enterprise switch will be used. This parameter is mandatory in yearly/monthly subscriptions.	2 months

3. Click **Next**.
4. On the displayed page, confirm the enterprise switch information, read and select the *Enterprise Switch Service Statement*, and click **Submit**.

   This operation takes 3 to 6 minutes to complete. If the status is **Running**, the enterprise switch is created.

Follow-Up Operations

After an enterprise switch is created, you need to create a Layer 2 connection and configure a remote tunnel gateway. For details, see **Getting Started**.

1.2 Viewing Details of an Enterprise Switch

Scenarios

This section describes how to view basic information about an enterprise switch.

Procedure

1. Go to the **Enterprise Switch** page.

2. Locate the enterprise switch and view its details.

1.3 Modifying an Enterprise Switch

Scenarios

This section describes how to change the name and description of an enterprise switch.

Procedure

1. Go to the **Enterprise Switch** page.
   Locate the enterprise switch you want to modify.
2. Click  next to the enterprise switch name or description and enter the new name or description.
3. Click .

1.4 Deleting an Enterprise Switch

Scenarios

You can delete an enterprise switch to release resources and reduce costs if it is no longer required.

Notes and Constraints

An enterprise switch with Layer 2 connections associated cannot be deleted. To delete such an enterprise switch, delete the Layer 2 connections first. For details, see **Deleting a Layer 2 Connection**.

Procedure

1. Go to the **Enterprise Switch** page.
   Locate the enterprise switch you want to delete.
2. In the upper right corner of the enterprise switch details page, click **Delete**.
   A confirmation dialog box is displayed.
3. Click **OK**.
   This operation takes 10 to 30 seconds to complete.

2 Layer 2 Connections

2.1 Creating a Layer 2 Connection

Scenarios

After an enterprise switch is created, you need to create a Layer 2 connection to enable the local Layer 2 connection subnet and the remote VXLAN switch to communicate at Layer 2.

Notes and Constraints

- Each Layer 2 connection connects a local and a remote Layer 2 connection subnet. Each enterprise switch supports a maximum of six Layer 2 connections.
- The Layer 2 connections of an enterprise switch can share a tunnel IP address, but their tunnel VNIs must be unique. A tunnel VNI is the identifier of a tunnel.
- If a Layer 2 connection connects a local Layer 2 connection subnet to an enterprise switch, the local Layer 2 connection subnet must have two IP addresses reserved as active and standby interface IP addresses. The two IP addresses cannot be used by any local resources and must be different from the IP addresses in the remote Layer 2 connection subnet.

Procedure

1. Go to the **Enterprise Switch** page.

   Locate the enterprise switch that you want to create a Layer-2 connection.
2. In the lower right part of the enterprise switch details page, click **Create Connection**.

   The page for creating a Layer 2 connection is displayed.
3. Configure the parameters as prompted. For details, see **Table 2-1**.

Table 2-1 Parameters for creating a Layer-2 connection

Parameter	Description	Example Value
Enterprise Switch	Name of the enterprise switch. You do not need to set this parameter.	l2cg-01
VPC	VPC that is associated with the enterprise switch, which is the VPC that the local tunnel subnet belongs to. You do not need to set this parameter.	vpc-01
Layer 2 Connection Subnet	Mandatory Select the layer 2 connection subnet in the VPC. This Layer 2 connection subnet is used to communicate with the Layer 2 connection subnet in an on-premises data center at Layer 2. ● The local and remote Layer 2 connection subnets can overlap, but the IP addresses of the servers that need to communicate in the local and remote subnets must be different. Otherwise, the communication fails. ● A VPC subnet that has been used a Layer 2 connection cannot be used by any other Layer 2 connections or enterprise switches.	subnet-01
Interface IP Address	Mandatory IP addresses in the VPC subnet that are connected to the enterprise switch, including active and standby interface IP addresses. The IP addresses can be automatically assigned or manually specified.	Automatically assign
Remote Access Information > Tunnel VNI	Mandatory Network identifier of the VXLAN tunnel used by an on-premises data center to connect to an enterprise switch, which is used to uniquely identify the VXLAN. For the same VXLAN tunnel, the on-premises data center and the cloud must use the same tunnel VNI.	10001
Remote Access Information > Tunnel IP Address	Mandatory IP address of the VXLAN tunnel used by the on-premises data center to connect to the enterprise switch.	-

Parameter	Description	Example Value
Remote Access Information > Tunnel Port	Port number of the VXLAN tunnel used by the on-premises data center to connect to the enterprise switch. Port **4789** is used by default. You do not need to set this parameter.	4789
Name	Mandatory Enter the name of the Layer 2 connection. The name: • Must contain 1 to 64 characters. • Can contain letters, digits, underscores (_), hyphens (-), and periods (.).	l2conn-01

4. Click **Create**.

   This operation takes 20 to 60 seconds to complete. If the status is **Not connected** or **Connected**, the Layer 2 connection is created.

2.2 Viewing Details of a Layer 2 Connection

Scenarios

This section describes how to view the basic information and topology of a Layer 2 connection, including the local and remote Layer 2 connection subnets, and local and remote tunnel IP addresses.

Procedure

1. Go to the **Enterprise Switch** page.

   Locate the enterprise switch whose Layer-2 connection you want to view.
2. In the lower part of the enterprise switch details page, view the basic information and topology of a Layer 2 connection.

2.3 Modifying a Layer 2 Connection Name

Scenarios

This section describes how to change the name of a Layer 2 connection.

Procedure

1. Go to the **Enterprise Switch** page.

   Locate the enterprise switch whose Layer-2 connection you want to modify.
2. In the lower part of the enterprise switch details page, locate the Layer 2 connection.

3. Click  next to the Layer 2 connection name and enter a new name.
4. Click .

2.4 Deleting a Layer 2 Connection

Scenarios

You can delete a Layer 2 connection if it is not needed anymore.

Notes and Constraints

Layer 2 connections to be deleted cannot be in the **Creating** status.

Procedure

1. Go to the **Enterprise Switch** page.
   Locate the enterprise switch whose Layer-2 connection you want to delete.
2. In the lower part of the enterprise switch details page, locate the Layer 2 connection.
3. Click **Delete Connection**.
   A confirmation dialog box is displayed.
4. Click **OK**.
   This operation takes 10 to 30 seconds to complete.

3 Permissions Management

3.1 Creating a User and Granting Permissions

This section describes how to use IAM to implement fine-grained permissions control for your enterprise switch resources. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to enterprise switch resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust an account or a cloud service to perform professional and efficient O&M on your enterprise switch resources.

If your account does not require individual IAM users, skip over this section.

IAM can be used free of charge. You pay only for the resources in your account. For more information about IAM, see **IAM Service Overview**.

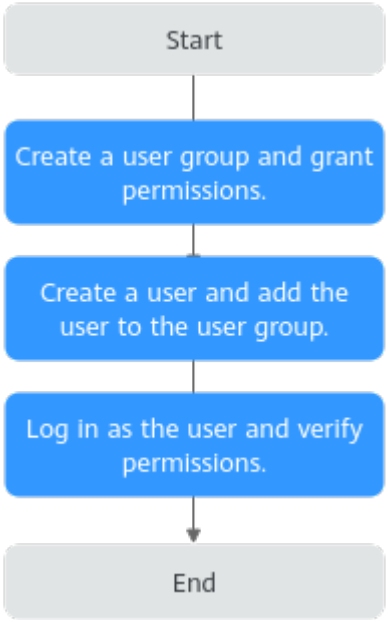
Figure 3-1 shows the procedure for granting permissions.

Prerequisites

You have learned about the permissions supported by Enterprise Switch and choose policies or roles according to your requirements. Enterprise Switch uses the same system permissions as VPC. For details, see **Permissions Management**. For permissions of other cloud services, see **System Permissions**.

Process Flow

Figure 3-1 Process for granting Enterprise Switch permissions



1. **Create a user group and assign permissions**.

   Create a user group on the IAM console, and assign the **VPC ReadOnlyAccess** policy to the group.

2. **Create a user and add the user to the user group**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify permissions.

   Log in to the Enterprise Switch console as the created user, switch to the authorized region, and verify the user permissions.

   - Click **Service List** and choose **Enterprise Switch**. Then click **Buy** in the upper right corner. If the enterprise switch fails to be created, the **VPC ReadOnlyAccess** permission has taken effect.
   - Choose any other service in the **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **VPC ReadOnlyAccess** policy has already taken effect.

4 Cloud Eye Monitoring

4.1 Supported Metrics

Description

This section describes metrics reported by enterprise switches to Cloud Eye as well as their namespaces, metrics, and dimensions. You can use the Cloud Eye management console or APIs to obtain the metrics and alarms generated for enterprise switches.

Namespace

SYS.ESW

Monitoring Metrics

With Cloud Eye, you can monitor the network status of enterprise switches.

- Table 4-1

Table 4-1 Enterprise switch metrics

ID	Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
up_bandwidth	Outbound Bandwidth	Network traffic per second going out of the enterprise switch	≥ 0	bit/s	1024 (IEC)	Enterprise switch	1 minute

ID	Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
down_bandwidth	Inbound bandwidth	Network traffic per second going into the enterprise switch	≥ 0	bit/s	1024 (IEC)	Enterprise switch	1 minute
up_stream	Outbound Traffic	Network traffic going out of the enterprise switch	≥ 0	byte	1024 (IEC)	Enterprise switch	1 minute
down_stream	Inbound Traffic	Network traffic going into the enterprise switch	≥ 0	byte	1024 (IEC)	Enterprise switch	1 minute
up_pps	Outbound PPS	Packets per second going out of the enterprise switch	≥ 0	pps	N/A	Enterprise switch	1 minute
down_pps	Inbound PPS	Packets per second going into the enterprise switch	≥ 0	pps	N/A	Enterprise switch	1 minute

Dimensions

The metric measurement dimension of an enterprise switch is **instance_id**.

Key	Value
instance_id	Enterprise switch

4.2 Viewing Metrics

Scenarios

This section describes how to view metrics for an enterprise switch.

Procedure

Step 1 Log in to the management console.

Step 2 In the upper left corner of the page, click , select a region, and choose **Management & Deployment** > **Cloud Eye**.

The **Cloud Eye** console is displayed.

Step 3 Click in the upper left corner and select the desired region and project.

Step 4 In the upper left corner of the page, click to open the service list and choose **Management & Deployment** > **Cloud Eye**.

Step 5 In the navigation pane on the left, choose **Cloud Service Monitoring** > **Enterprise Switch**.

Step 6 Locate the enterprise switch and click **View Metric** in the **Operation** column.

The metrics are displayed.

Step 7 View the metrics.

NOTE

For details about querying metrics, see **Querying Cloud Service Monitoring Metrics**.

----End

4.3 Creating an Alarm Rule

Scenarios

This section describes how to create alarm rules and notifications for enterprise switches.

You can create an alarm rule to configure the conditions that trigger an alarm and determine whether to send notifications when there is an alarm.

If you create an alarm rule for a metric, you can timely know metric exceptions and rectify the exceptions.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. In the upper left corner of the page, click to open the service list and choose **Management & Governance** > **Cloud Eye**.
4. In the left navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.
5. On the **Alarm Rules** page, click **Create Alarm Rule** and set required parameters, or modify an existing alarm rule.

6. After the parameters are set, click **Create**.

   After the alarm rule is set, the system notifies you when an alarm is triggered.

   NOTE

   For more information about alarm rules, see the **Cloud Eye User Guide**.

4.4 Storing Monitoring Data to OBS Buckets

Scenarios

This section describes how to configure OBS for enterprise switches to store their historical monitoring data.

Raw monitoring data of metrics is kept for only two days on Cloud Eye. For permanent data storage, enable Object Storage Service (OBS), and store raw monitoring data to OBS buckets.

Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner and select the desired region and project.

Step 3 In the upper left corner of the page, click  to open the service list and choose **Management & Deployment** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Cloud Service Monitoring** > **Enterprise Switch**.

Step 5 In the enterprise switch list, locate the row that contains the enterprise switch and click **Configure Storage** in the **Operation** column.

The **Configure Storage** page is displayed.

Step 6 On the **Configure Storage** page, configure parameters as prompted.

----End

