

Enterprise Switch

User Guide

Issue 01
Date 2024-12-04



Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI 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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <https://www.huawei.com>

Email: support@huawei.com

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 Service Overview	1
1.1 What Is an Enterprise Switch?	1
1.2 Why Using Enterprise Switches	2
1.3 How Enterprise Switches Work	4
1.4 Permissions Management	7
1.5 Notes and Constraints	8
1.6 Region and AZ	9
1.7 Working with Other Services	10
2 Getting Started	12
2.1 Quick Start	12
2.2 Step 1: Use VPN to Communicate at Layer 3	13
2.3 Step 2: Create an Enterprise Switch	13
2.4 Step 3: Create a Layer 2 Connection	16
2.5 Step 4: Configure a Tunnel Gateway in Your Data Center	18
3 Enterprise Switches	24
3.1 Creating an Enterprise Switch	24
3.2 Viewing Details of an Enterprise Switch	26
3.3 Modifying an Enterprise Switch	27
3.4 Deleting an Enterprise Switch	27
4 Layer 2 Connections	29
4.1 Creating a Layer 2 Connection	29
4.2 Viewing Details of a Layer 2 Connection	31
4.3 Modifying a Layer 2 Connection Name	31
4.4 Deleting a Layer 2 Connection	32
5 Permissions Management	33
5.1 Creating a User and Granting Permissions	33
6 FAQs	35
6.1 What Switches Can Connect to Enterprise Switches?	35
6.2 Why Is the Layer 2 Connection in the Not Connected State Even After Its Configuration Is Complete?	35
6.3 Why Is Communication Between the Cloud and On-premises Servers Unavailable Even When the Layer 2 Connection Status Is Connected?	35

A Change History..... 37

1 Service Overview

1.1 What Is an Enterprise Switch?

Enterprise switches enable Layer 2 networking for VPCs, helping you to connect cloud and on-premises networks that are highly reliable, in a large scale, and of high performance.

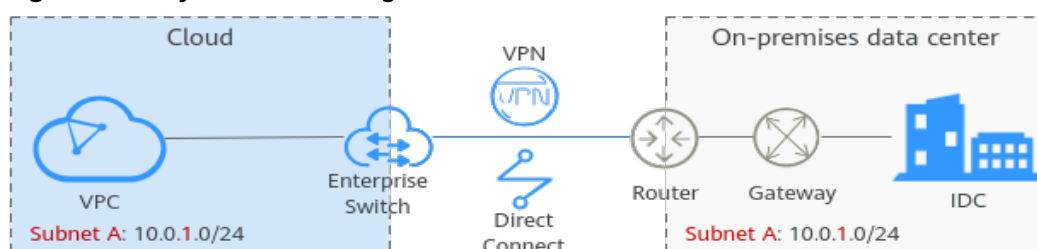
Currently, enterprise switches only support Layer 2 connection gateways (L2CGs). An L2CG is a virtual tunnel gateway that can work with VPN to establish network communications between cloud and on-premises networks at Layer 2. The gateway allows you to migrate workloads in data centers or private clouds to the cloud without changing subnets and IP addresses.

VPN only allows cloud and on-premises networks to communicate at Layer 3 and the CIDR blocks of the networks that are used for communication cannot overlap.

If the cloud and on-premises networks overlap and need to communicate with each other, you can use an enterprise switch to enable communication between them at Layer 2.

An enterprise switch is a tunnel gateway of a VPC and corresponds to the tunnel gateway of your data center. It can work together with VPN to enable communications between a VPC and your data center at Layer 2. [Figure 1-1](#) shows the networking diagram. You need to connect a VPC subnet to the enterprise switch and specify the enterprise switch to establish a connection with the tunnel gateway of your on-premises data center so that the VPC subnet can communicate with the data center subnet at Layer 2.

Figure 1-1 Layer 2 networking



1.2 Why Using Enterprise Switches

VPN allows communications between on-premises data centers and VPCs at Layer 3. However, this may require network reconstruction, long cloud migration period, and service interruptions. For details, see [Constraints on Communication at Layer 3](#).

Enterprise switches allow communications between on-premises data centers and VPCs at Layer 2, helping you dynamically and smoothly migrate workloads to the cloud. For details, see [Advantages on Communication at Layer 2](#).

Constraints on Communication at Layer 3

[Figure 1-2](#) shows the Layer 3 network between on-premises data centers and VPCs using VPN. [Table 1-1](#) describes the pain points.

Figure 1-2 Layer 3 networking diagram

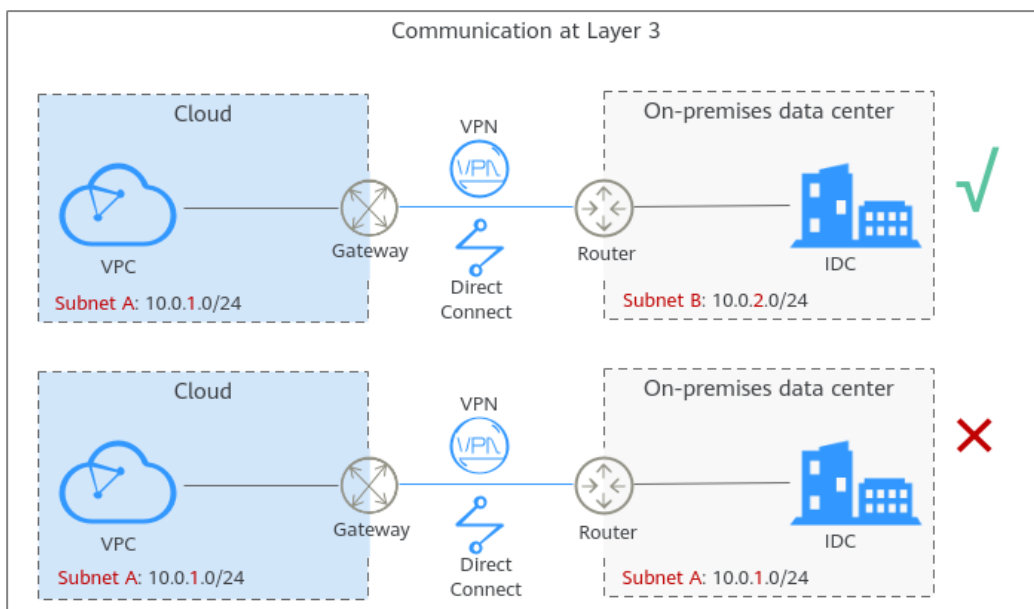


Table 1-1 Layer 3 networking description

Description	VPN allows the communication between on-premises data centers and VPCs at Layer 3 through routes.
--------------------	---

Pain Points	<ul style="list-style-type: none"> The CIDR blocks of the on-premises data center and the VPC that are used for communication cannot overlap. On-premises workloads communicate with each other using IP addresses instead of domain names. If the CIDR blocks of the on-premises data center and the VPC that are used for communication overlap, the on-premises network needs to be reconstructed before the cloud migration, which prolongs the cloud migration period, interrupts businesses, and increases O&M costs. Workloads in a subnet have to be migrated together, and cloud and on-premises workloads in the same subnet cannot communicate with each other. Dozens of different workloads are deployed on each subnet of the on-premises data center. If workloads are migrated by subnet, business continuity cannot be ensured.
--------------------	--

Advantages on Communication at Layer 2

To handle the pain points of cloud migration at Layer 3, you can use enterprise switches to allow the communication between on-premises data centers and VPCs at Layer 2. For details about the advantages of enterprise switches, see [Table 1-2](#).

Figure 1-3 Layer 2 networking diagram

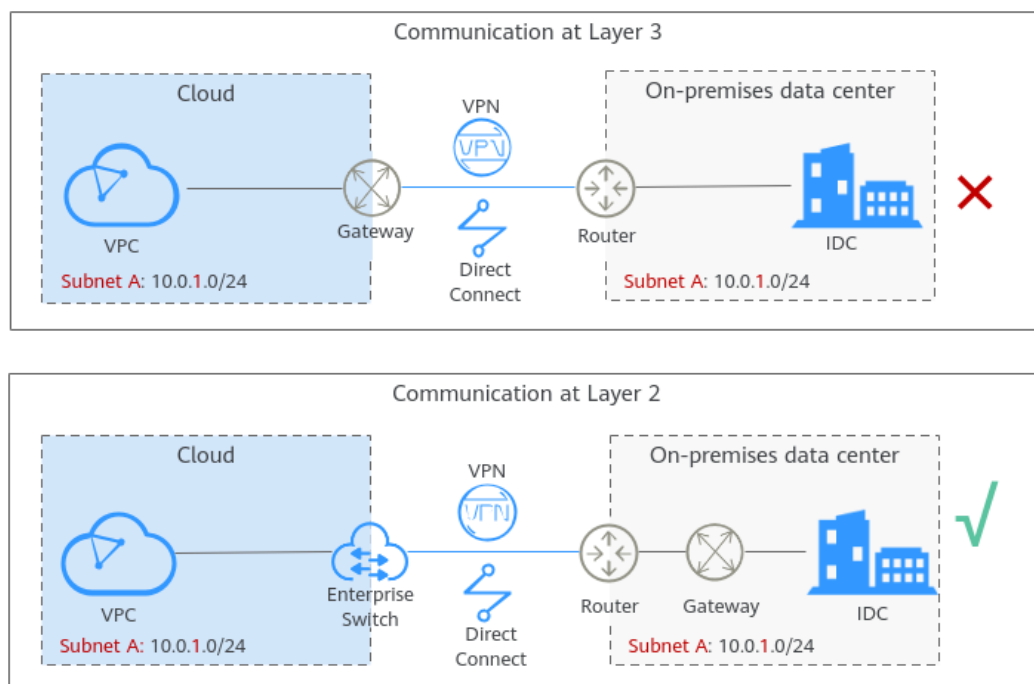
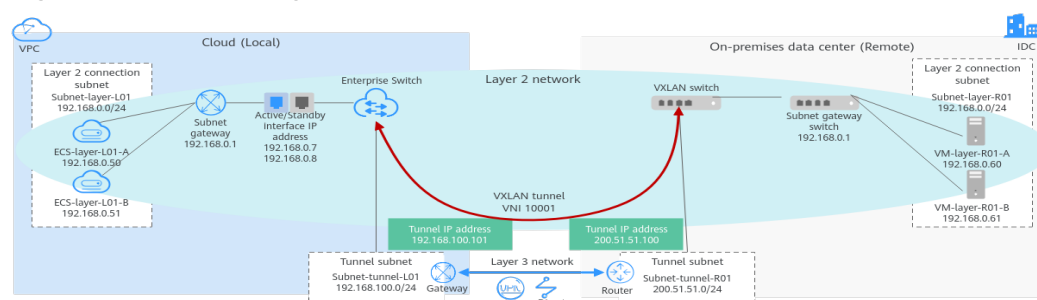


Table 1-2 Layer 2 networking description

Description	Enterprise switches establish a Layer 2 network between on-premises data centers and VPCs based on the Layer 3 network established by VPN.
Advantages	<ul style="list-style-type: none"> The CIDR blocks of the on-premises data center and the VPC that are used for communication can overlap. An enterprise switch allows the network of the on-premises data center to remain unchanged even if the data center and the VPC have overlapping CIDR blocks. Workloads can be migrated to the cloud on a server basis, and cloud and on-premises workloads in the same subnet can communicate with each other. Workloads can be seamlessly migrated to the cloud to prevent any loss caused by cloud migration.

1.3 How Enterprise Switches Work

Figure 1-4 illustrates how an enterprise switch works. **Table 1-3** describes the working principles in more detail.

Figure 1-4 Networking**Table 1-3** Working principles

No.	Action	Description
1	Enable the local and remote tunnel subnets to communicate at Layer 3.	<ul style="list-style-type: none"> Plan resources on and off the cloud. For details, see Table 1-4. Use VPN to enable the local (Subnet-tunnel-L01) and remote (Subnet-tunnel-R01) tunnel subnets to communicate at Layer 3.
2	Create an enterprise switch and specify a tunnel subnet .	Create an enterprise switch, set the local tunnel subnet to Subnet-tunnel-L01 , and the local tunnel IP address to 192.168.100.101 .

No.	Action	Description
3	Create a Layer 2 connection .	Create a Layer 2 connection to enable the local Layer 2 connection subnet (Subnet-layer-L01) and the remote VXLAN switch to communicate at Layer 2. Configure the following parameters: <ul style="list-style-type: none"> Active and standby interface IP addresses: They can be automatically assigned or manually specified. Remote tunnel IP address (200.51.51.100) and tunnel VNI (10001)
4	Configure a tunnel gateway in the on-premises data center.	Configure a tunnel gateway on the remote VXLAN switch to establish a VXLAN tunnel for the remote Layer 2 connection subnet (Subnet-layer-R01).

Table 1-4 Resource details

Resource	Cloud (Local)		On Premises (Remote)	
Layer 2 connection subnet	VPC subnet	Subnet-layer-L01: 192.168.0.0/24	On-premises subnet	Subnet-layer-R01: 192.168.0.0/24
	ECS	<ul style="list-style-type: none"> ECS-layer-L01-A: 192.168.0.50 ECS-layer-L01-B: 192.168.0.51 	On-premises server	<ul style="list-style-type: none"> VM-layer-R01-A: 192.168.0.60 VM-layer-R01-B: 192.168.0.61
	Active and standby interface IP addresses	<ul style="list-style-type: none"> Active interface IP address: 192.168.0.7 Standby interface IP address: 192.168.0.8 	-	-
Tunnel subnet	VPC subnet	Subnet-tunnel-L01: 192.168.100.0/24	On-premises subnet	Subnet-tunnel-R01: 200.51.51.0/24
	Tunnel IP address	192.168.100.101	Tunnel IP address	200.51.51.100
Tunnel VNI	10001			

Layer 2 Connection Subnets

A local Layer 2 connection subnet is on the cloud and a remote one is in an on-premises data center. They are used to communicate at Layer 2.

- Local Layer 2 connection subnet: a VPC subnet, for example, Subnet-layer-L01
- Remote Layer 2 connection subnet: an on-premises subnet, for example, Subnet-layer-R01

Constraints

- 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.

Tunnel Subnets

Local and remote tunnel subnets communicate with each other at Layer 3 over VPN. Enterprise switches allow communications between cloud and on-premises networks at Layer 2 based on the Layer 3 network between tunnel subnets.

- Local tunnel subnet: a VPC subnet, for example, Subnet-tunnel-L01
- Remote tunnel subnet: an on-premises subnet, for example, Subnet-tunnel-R01

Constraints

- Ensure that the local and remote tunnel subnets can communicate at Layer 3 over VPN before you use an enterprise switch to allow communication at Layer 2.
- 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.

Layer 2 Connections

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.

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.

Active and Standby Interface IP Addresses

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.

Tunnel IP Addresses

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.

- Local tunnel IP address: in the local tunnel subnet. In this example, the local tunnel subnet is Subnet-tunnel-L01, and the tunnel IP address is 192.168.100.101.
- Remote tunnel IP address: in the remote tunnel subnet. In this example, the remote tunnel subnet is Subnet-tunnel-R01, and the tunnel IP address is 200.51.51.100.

Tunnel VNIs

Tunnel VNIs are used to uniquely identify the VXLAN tunnels between an on-premises data center and an enterprise switch.

For the same VXLAN tunnel, the on-premises data center and the cloud must use the same tunnel VNI.

1.4 Permissions Management

If you need to assign different permissions to employees in your enterprise to control their access to your cloud resources, you can use Identity and Access Management (IAM) for fine-grained permissions management. IAM provides functions such as identity authentication, permissions management, and access control.

With IAM, you can create IAM users and assign permissions to the users to control their access to specific resources.

If your account does not need individual IAM users for permissions management, skip this section.

Enterprise Switch Permissions

By default, new IAM users do not have any permissions assigned. You need to add them to one or more groups and attach roles to these groups so that these users can inherit permissions from the groups and perform specified operations on cloud services.

Enterprise Switch is a project-level service deployed and accessed in specific physical regions. You need to select a project for which the permissions will be granted. If you select **All projects**, the permissions will be granted for all the

projects. You need to switch to the authorized region before accessing Enterprise Switch.

Enterprise Switch uses the same system permissions as VPC. [Table 1-5](#) lists all the system-defined roles and policies supported by VPC. This VPC role is dependent on other roles. When assigning VPC roles to users, you need to also assign dependent roles for the VPC permissions to take effect.

Table 1-5 System-defined permissions for VPC

Policy Name	Description	Policy Type	Dependencies
VPC FullAccess	Full permissions for VPC.	System-defined policy	To use the VPC flow log function, users must also have the LTS ReadOnlyAccess permission.
VPC ReadOnlyAccess	Read-only permissions on VPC.	System-defined policy	None
VPC Administrator	Most permissions on VPC, excluding creating, modifying, deleting, and viewing security groups and security group rules. To be granted this permission, users must also have the Tenant Guest and Server Administrator permission.	System-defined role	Tenant Guest and Server Administrator policies, which must be attached in the same project as VPC Administrator .

1.5 Notes and Constraints

Constraints

- Enterprise switches cannot forward unknown unicast, broadcast, and multicast (except VRRP) packets from your data center to the cloud or IPv6 packets.
- On-premises servers cannot use advanced network functions on the cloud, such as VPC Peering, Route Table, ELB, and NAT Gateway.
- If you want to use a VPN connection together with an enterprise switch, submit a service ticket to check whether your connection supports VXLAN interconnection with an enterprise switch. If your connection does not support this, contact technical support.
- Only classic VPNs can be used together with enterprise switches.
- If cloud and on-premises networks communicate with each other at Layer 2, the cloud subnet gateway address must be the same as the on-premises

subnet gateway address. Otherwise, the on-premises subnet gateway address may conflict with the IP address of a cloud server, causing communication exceptions.

- Each enterprise switch allows up to 10,000 IP addresses to communicate at Layer 2, including a maximum of 1,000 on-premises IP addresses.
- To use an enterprise switch to connect cloud and on-premises networks at Layer 2, you are responsible for constructing the VXLAN network in your data center, such as preparing VXLAN switches, connecting physical networks, and connecting to VPN.
- Generally, a server determines the destination MAC address of a reply packet through ARP. However, some hosts or hardware devices (such as F5 load balancers) are configured to use the source MAC address of a request packet as the destination MAC address of its reply packet. If an enterprise switch is used for cloud and on-premises communications at Layer 3 in this case, a network disconnection may occur.

For example, an enterprise switch allows cloud and on-premises networks to communicate on 192.168.3.0/24. If the cloud server 192.168.2.2/24 accesses the on-premises server 192.168.3.3/24, the request packet on the cloud is sent to the on-premises server through the VPC route and then the enterprise switch. The reply packet from the on-premises server is sent back to the cloud through the route and VPN. If the on-premises server is configured to use the source MAC address of a request packet as the destination MAC address of its reply packet, the destination MAC address of the reply packet is not the MAC address of gateway 192.168.3.0/24, but the source MAC address of the request packet, that is, the MAC address of the enterprise switch. In this case, the destination MAC address of the reply packet is incorrect and the network is disconnected.

- If an enterprise switch uses the VXLAN protocol, the VXLAN protocol has a header of 50 bytes and the packet length increases. Your on-premises network devices that allow VXLAN packets should support jumbo frames (Ethernet frames whose MTU is greater than 1500 bytes). Otherwise, such packets cannot be transmitted.
- If you use an enterprise switch to connect your on-premises data center to the cloud, the switches of your data center must support the VXLAN function. The following lists some switches that support the VXLAN function.

1.6 Region and AZ

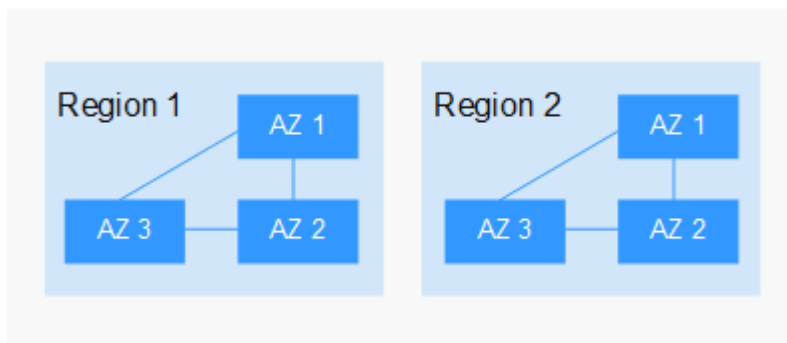
Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- A region is a physical data center, which is completely isolated to improve fault tolerance and stability. The region that is selected during resource creation cannot be changed after the resource is created.
- An AZ is a physical location where resources use independent power supplies and networks. A region contains one or more AZs that are physically isolated but interconnected through internal networks. Because AZs are isolated from each other, any fault that occurs in one AZ will not affect others.

Figure 1-5 shows the relationship between regions and AZs.

Figure 1-5 Regions and AZs



Selecting a Region

Select a region closest to your target users for lower network latency and quick access.

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see [Regions and Endpoints](#).

1.7 Working with Other Services

Figure 1-6 illustrates how an enterprise switch works with other cloud services.

Figure 1-6 Interactions between an enterprise switch and other cloud services

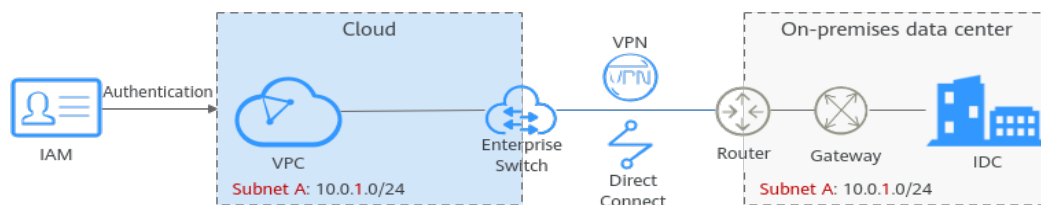


Table 1-6 Interactions between an enterprise switch and other cloud services

Service	Interaction
Virtual Private Cloud (VPC)	VPCs can use enterprise switches to communicate with on-premises data centers at Layer 2.
Virtual Private Network (VPN)	VPN allows the communication between on-premises data centers and VPCs at Layer 3. Based on the Layer 3 network, enterprise switches establish a Layer 2 network between on-premises data centers and VPCs.
Identity and Access Management (IAM)	On IAM, you can assign different permissions to different users to control their access to enterprise switch resources.

2 Getting Started

2.1 Quick Start

Enterprise switches establish a Layer 2 network between on-premises data centers and VPCs based on the Layer 3 network established by VPN.

Table 2-1 Process description

No.	Step	Description
1	Step 1: Use VPN to Communicate at Layer 3	An enterprise switch establishes a Layer 2 network based on a Layer 3 network between an on-premises data center and a VPC. This section describes how to create a VPN connection between an on-premises data center and a VPC at Layer 3.
2	Step 2: Create an Enterprise Switch	This section describes how to create an enterprise switch. An enterprise switch allows Layer 2 communication between an on-premises data center and a VPC based on VPN.
3	Step 3: Create a Layer 2 Connection	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.
4	Step 4: Configure a Tunnel Gateway in Your Data Center	This section describes how to configure the tunnel gateway on a VXLAN tunnel switch of an on-premises data center.

2.2 Step 1: Use VPN to Communicate at Layer 3

Scenarios

An enterprise switch establishes a Layer 2 network based on a Layer 3 network between an on-premises data center and a VPC. This section describes how to create a VPN connection between an on-premises data center and a VPC at Layer 3.

Prerequisites

You have planned the resources required both on the cloud and on premises. For details about resource planning, see [How Enterprise Switches Work](#).

Procedure

1. Create a VPN connection.
For details, see the *Virtual Private Network User Guide*.

NOTE

- Only classic VPNs can be used together with enterprise switches.
2. Submit a service ticket to check whether your VPN connection supports VXLAN interconnection with an enterprise switch. If your connection does not support this, contact technical support.

2.3 Step 2: Create an Enterprise Switch

Scenarios

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

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 VPN. You need to create a VPN connection first by referring to [Step 1: Use 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. Log in to the management console.
2. On the console homepage, choose **Network > Enterprise Switch**.
The **Enterprise Switch** page is displayed.
3. In the upper right corner of the page, click **Create**.
The page for creating an enterprise switch is displayed.
4. Configure the parameters as prompted. For details, see [Table 2-2](#).

Table 2-2 Parameters for creating an enterprise switch

Parameter	Description
Region	Mandatory Select the region nearest to you to ensure the lowest latency possible.
Active AZ	Mandatory Select the AZ where the active node is deployed. Enterprise switches are deployed in active/standby mode. 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.
Standby AZ	Mandatory Select the AZ where the standby node is deployed. Set the standby AZ to be different from the active AZ. A standby AZ is used for backup and disaster recovery.
Specifications	Mandatory Currently, standard enterprise switches are supported.
Tunnel Connection	Mandatory Tunnel connection between the enterprise switch and the on-premises data center at Layer 3. Select a connection type based on your needs. <ul style="list-style-type: none">• VPN: allows an on-premises data center and a VPC to communicate at Layer 3.• Custom: Select another type of connection to allow an on-premises data center and a VPC to communicate at Layer 3.
Connection Gateway	This parameter is mandatory if Tunnel Connection is set to VPN . Select a virtual gateway if you set Tunnel Connection to a VPN gateway if you set Tunnel Connection to VPN .

Parameter	Description
VPC	Mandatory VPC that the enterprise switch belongs to. If Tunnel Connection is set to VPN , the VPC is set to the one that the VPN gateway belongs to by default.
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 VPN. Enterprise switches allow communications between cloud and on-premises networks at Layer 2 based on the Layer 3 network between tunnel subnets.
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.
Name	Mandatory Enter the name of the enterprise switch. The name: <ul style="list-style-type: none">• Must contain 1 to 64 characters.• Can contain letters, digits, underscores (_), hyphens (-), and periods (.).
Description	Optional Enter the description of the enterprise switch in the text box as required.

5. Click **Create Now**.

6. Confirm the enterprise switch information 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](#).

2.4 Step 3: Create 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. Log in to the management console.
2. On the console homepage, choose **Network > Enterprise Switch**.
The **Enterprise Switch** page is displayed.
3. Click the name of the target enterprise switch.
The enterprise switch details page is displayed.
4. In the lower right part of the enterprise switch details page, click **Create Connection**.
The page for creating a Layer 2 connection is displayed.
5. Configure the parameters as prompted. For details, see [Table 2-3](#).

Table 2-3 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, that is, the VPC that the local tunnel subnet belongs to. You do not need to set this parameter.	vpc-01

Parameter	Description	Example Value
Layer 2 Connection Subnet	<p>Mandatory</p> <p>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.</p> <ul style="list-style-type: none">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	<p>Mandatory</p> <p>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.</p>	Automatically assign
Remote Access Information > Tunnel VNI	<p>Mandatory</p> <p>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.</p>	10001
Remote Access Information > Tunnel IP Address	<p>Mandatory</p> <p>IP address of the VXLAN tunnel used by the on-premises data center to connect to the enterprise switch.</p>	-
Remote Access Information > Tunnel Port	<p>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.</p>	4789

Parameter	Description	Example Value
Name	Mandatory Enter the name of the Layer 2 connection. The name: <ul style="list-style-type: none">• Must contain 1 to 64 characters.• Can contain letters, digits, underscores (_), hyphens (-), and periods (.).	l2conn-01

6. 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.

2.5 Step 4: Configure a Tunnel Gateway in Your Data Center

Scenarios

This section describes how to configure the tunnel gateway on a VXLAN tunnel switch of an on-premises data center.

The following uses CE6850 and H3C S6520 series switches as examples. To check more configurations, see the product documentation of the corresponding switch.

- [Procedure \(CE6850 Switches\)](#)
- [Procedure \(H3C S6520 Switches\)](#)

Notes and Constraints

If you use an enterprise switch to connect your on-premises data center to the cloud, the switches of your data center must support the VXLAN function. If high reliability is required, the VXLAN switches need to be deployed in disaster recovery mode.

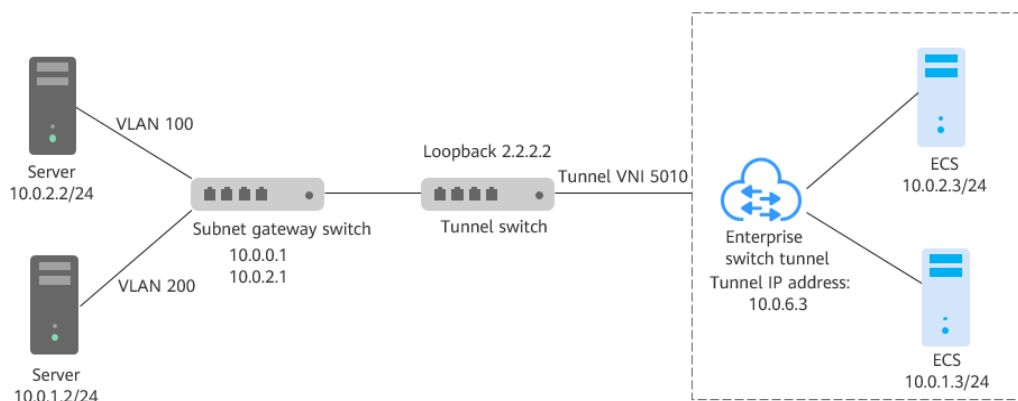
The following lists some switches that support the VXLAN function.

- Huawei switches: Huawei CE58, CE68, CE78, and CE88 series switches, such as CE6870, CE6875, CE6881, CE6863, and CE12800 switches
- Switches of other vendors: Cisco Nexus 9300 and H3C S6520 series switches

Networking Example

In this example, the Layer 2 subnet gateway and the VXLAN tunnel are on different switches.

The tunnel IP address on the cloud is 10.0.6.3, the tunnel IP address of the tunnel switch on the on-premises data center is 2.2.2.2, and the tunnel VNI is 5010.

Figure 2-1 Layer 2 subnet gateway and VXLAN tunnel on different switches

Procedure (CE6850 Switches)

Configure the tunnel switch of your data center to divert the traffic of the VLAN corresponding to the Layer 2 subnet to the tunnel.

NOTICE

Currently, most CE series switches do not support forwarding of encapsulated VXLAN packets through Layer 3 sub-interfaces. Layer 3 sub-interfaces cannot be used by VXLAN uplinks (connected to enterprise switches). Instead, VLAN interfaces can be used.

1. Log in to the tunnel switch and run the **system-view** command to switch to the system view.
2. Switch to the loopback 0 interface view and configure the tunnel IP address.
Example:
interface loopback 0
ip address 2.2.2.2 255.255.255.255
3. Use the **quit** command to exit the interface view and return to the system view.
4. Switch to the bridge domain (BD) view and configure the VXLAN VNI for the BD.
Example:
bridge-domain 10
vxlan vni 5010
5. Use the **quit** command to exit the BD view and return to the system view.
6. Create a Layer 2 sub-interface and use the sub-interface to divert traffic from the VLAN at Layer 2 to the tunnel.
Example:
interface 10ge 1/0/2.1 mode l2
encapsulation dot1q vid 100
bridge-domain 10

7. Use the **interface nve** command to create an NVE interface, switch to the NVE interface view, and configure the IP address (2.2.2.2) for the source VTEP of the VXLAN tunnel.

Example:

```
interface nve1  
source 2.2.2.2
```

8. Use the **vni** command in the NVE interface view to configure an ingress replication list for VNI 5010.

Example:

```
vni 5010 head-end peer-list 10.0.6.3
```

9. Check the VXLAN configuration status in the system view:

```
display vxlan vni 5010 verbose
```

Figure 2-2 VXLAN configuration status

```
[~B0706-172.30.192.3-core-new-gateway]display vxlan vni 5010 verbose  
BD ID           : 10  
State           : up  
NVE             : 1  
Source Address  : 2.2.2.2  
Source IPv6 Address : -  
UDP Port        : 4789  
BUM Mode        : head-end  
Group Address   : -  
Peer List       : 10.0.6.3  
IPv6 Peer List  : -
```

If the value of **State** is **up**, the tunnel status is normal.

Procedure (H3C S6520 Switches)

Establish a VXLAN tunnel between a VXLAN switch and an enterprise switch, associate the VXLAN tunnel with a VXLAN, so that Layer 2 packets from VMs can be encapsulated into IP packets and then sent to the enterprise switch. Configure Ethernet service instances and matching rules on downlink interfaces of a VXLAN switch to identify the VXLAN that packets belong to.

1. Configure the switch to work in VXLAN mode.

Save the configuration, and restart the switch. (Skip this step if the switch is already working in VXLAN mode.)

Example:

```
<SwitchA> system-view
```

```
[SwitchA] switch-mode 1
```

Reboot device to make the configuration take effect.

```
[SwitchA] quit
```

```
<SwitchA> reboot
```

Start to check configuration with next startup configuration file, please wait..

.....DONE!

Current configuration may be lost after the reboot, save current configuration?

[Y/N]:y

This command will reboot the device. Continue? [Y/N]:y

2. Create a tunnel interface and configure an IP address for the interface.
Create a loopback interface and configure an IP address for the loopback interface as the remote IP address of the VXLAN tunnel.

Example:

```
[SwitchA] interface loopback 0  
[SwitchA-LoopBack0] ip address 2.2.2.2 32
```

NOTICE

For a new interface IP address (including the loopback interface IP address) of the VXLAN switch, check whether there is a route to direct traffic from the IP address to the tunnel subnet of the enterprise switch. If there is no such a route, configure one on the VXLAN switch. The VXLAN switch can be an aggregation switch or a core switch. Select a switch based on the network plan.

3. Create a VXLAN.
 - a. Enable L2VPN.
Example:
<SwitchA> **system-view**
[SwitchA] **l2vpn enable**
 - b. Enable Layer 2 forwarding for the VXLAN tunnel.
Example:
[SwitchA] **undo vxlan ip-forwarding**
 - c. Create the VSI **vpna** and VXLAN 5010.
Example:

```
[SwitchA] vsi vpna  
[SwitchA-vsi-vpna] vxlan 5010  
[SwitchA-vsi-vpna-vxlan5010] quit  
[SwitchA-vsi-vpna] quit
```

NOTICE

The VXLAN ID must be the same as the tunnel VNI in remote access information configured during Layer 2 connection creation in [Table 2-3](#).

4. Create a VXLAN tunnel.
Create a VXLAN tunnel (Tunnel1) to the enterprise switch.
Example:
[SwitchA] **interface tunnel 1 mode vxlan**
[SwitchA-Tunnel1] **source 2.2.2.2**
[SwitchA-Tunnel1] **destination 10.0.6.3**
[SwitchA-Tunnel1] **quit**

5. Associate the VXLAN with the VXLAN tunnel.

On the VXLAN switch, associate the VXLAN tunnel (Tunnel1) with VXLAN 5010.

Example:

```
[SwitchA] vsi vpna
[SwitchA-vsi-vpna] vxlan 5010
[SwitchA-vsi-vpna-vxlan5010] tunnel 1
[SwitchA-vsi-vpna-vxlan5010] quit
[SwitchA-vsi-vpna] quit
```

NOTICE

- A maximum of six Layer 2 connections can be created on an enterprise switch. Each connection corresponds to a VXLAN. Multiple VXLANs can be associated with the same VXLAN tunnel, such as, Tunnel1.
- A VXLAN switch can connect to multiple enterprise switches. In this case, you can associate multiple VXLAN tunnels, for example, Tunnel1 and Tunnel2, with the same VXLAN.

6. Configure an Ethernet service instance to match frames and associate the instance with the VSI.

Create Ethernet service instance 1000 on Bridge-Aggregation1 of the VXLAN switch to match frames of VLAN 100 and associate the instance with VSI **vpna** (VXLAN 5010).

Example:

```
[SwitchA] Bridge-Aggregation 1
[SwitchA-Bridge-Aggregation1] port link-type trunk
[SwitchA-Bridge-Aggregation1] service-instance 1000
[SwitchA-Bridge-Aggregation1-srv1000] encapsulation s-vid 100
[SwitchA-Bridge-Aggregation1-srv1000] xconnect vsi vpna
[SwitchA-Bridge-Aggregation1-srv1000] quit
[SwitchA-Bridge-Aggregation1] quit
```

NOTICE

The method for creating Ethernet service instances on physical Ethernet interfaces of switches is similar.

7. Check the status of the VXLAN tunnel interface.

- The status of the VXLAN tunnel interface is **Up**.

Example:

```
[SwitchA] display interface Tunnel 1
```

```
Tunnel1
Current state: UP
Line protocol state: UP
```

```
Description: Tunnel1 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1464
Internet protocol processing: Disabled
Last clearing of counters: 17:19:44 Fri 01/18/2013
Tunnel source 2.2.2.2, destination 10.0.6.3
Tunnel protocol/transport UDP_VXLAN/IP
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 4 drops
Output: 0 packets, 0 bytes, 0 drops
```

- Check the VSI information. The VXLAN tunnel associated with the VXLAN and the Ethernet service instance associated with the VSI are in **Up** status.

Example:

[SwitchA]display l2vpn vsi verbose

```
VSI Name: vnpa
VSI Index      : 1
VSI State      : Up
MTU            : 1500
Bandwidth      : -
Broadcast Restrain : -
Multicast Restrain : -
Unknown Unicast Restrain: -
MAC Learning   : Enabled
MAC Table Limit : -
MAC Learning rate : -
Drop Unknown   : -
Flooding       : Enabled
Statistics     : Disabled
VXLAN ID       : 5010
Tunnels:
Tunnel Name    Link ID  State  Type    Flood proxy
Tunnel1        0x5000001 UP      Manual  Disabled
ACs:
AC             Link ID  State  Type
BAGG1 srv1000 0        Up     Manual
```

3 Enterprise Switches

3.1 Creating an Enterprise Switch

Scenarios

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

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 VPN. You need to create a VPN connection first by referring to [Step 1: Use 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. Log in to the management console.
2. On the console homepage, choose **Network > Enterprise Switch**. The **Enterprise Switch** page is displayed.
3. In the upper right corner of the page, click **Create**. The page for creating an enterprise switch is displayed.
4. Configure the parameters as prompted. For details, see [Table 3-1](#).

Table 3-1 Parameters for creating an enterprise switch

Parameter	Description
Region	Mandatory Select the region nearest to you to ensure the lowest latency possible.
Active AZ	Mandatory Select the AZ where the active node is deployed. Enterprise switches are deployed in active/standby mode. 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.
Standby AZ	Mandatory Select the AZ where the standby node is deployed. Set the standby AZ to be different from the active AZ. A standby AZ is used for backup and disaster recovery.
Specifications	Mandatory Currently, standard enterprise switches are supported.
Tunnel Connection	Mandatory Tunnel connection between the enterprise switch and the on-premises data center at Layer 3. Select a connection type based on your needs. <ul style="list-style-type: none">• VPN: allows an on-premises data center and a VPC to communicate at Layer 3.• Custom: Select another type of connection to allow an on-premises data center and a VPC to communicate at Layer 3.
Connection Gateway	This parameter is mandatory if Tunnel Connection is set to VPN . Select a virtual gateway if you set Tunnel Connection to a VPN gateway if you set Tunnel Connection to VPN .
VPC	Mandatory VPC that the enterprise switch belongs to. If Tunnel Connection is set to VPN , the VPC is set to the one that the VPN gateway belongs to by default.

Parameter	Description
Tunnel Subnet	<p>Mandatory</p> <p>Subnet of the VPC that the enterprise switch belongs to. It is the local tunnel subnet.</p> <p>Local and remote tunnel subnets communicate with each other at Layer 3 over VPN. Enterprise switches allow communications between cloud and on-premises networks at Layer 2 based on the Layer 3 network between tunnel subnets.</p>
Tunnel IP Address	<p>Mandatory</p> <p>IP address in the local tunnel subnet, which can be automatically assigned or manually specified.</p> <p>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.</p>
Name	<p>Mandatory</p> <p>Enter the name of the enterprise switch. The name:</p> <ul style="list-style-type: none">• Must contain 1 to 64 characters.• Can contain letters, digits, underscores (_), hyphens (-), and periods (.).
Description	<p>Optional</p> <p>Enter the description of the enterprise switch in the text box as required.</p>

5. Click **Create Now**.
6. Confirm the enterprise switch information 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](#).

3.2 Viewing Details of an Enterprise Switch

Scenarios

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

Procedure



1. Log in to the management console.
2. On the console homepage, choose **Network > Enterprise Switch**.
The **Enterprise Switch** page is displayed.
3. Click the name of the target enterprise switch.
You can view the basic information about the enterprise switch.

3.3 Modifying an Enterprise Switch

Scenarios

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

Procedure

1. Log in to the management console.
2. On the console homepage, choose **Network > Enterprise Switch**.
The **Enterprise Switch** page is displayed.
3. Click the name of the target enterprise switch.
The enterprise switch details page is displayed.
4. Click  next to the enterprise switch name or description and enter the new name or description.
5. Click .

3.4 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. Log in to the management console.
2. On the console homepage, choose **Network > Enterprise Switch**.
The **Enterprise Switch** page is displayed.
3. Click the name of the target enterprise switch.

The enterprise switch details page is displayed.

4. In the upper right corner of the enterprise switch details page, click **Delete**.
A confirmation dialog box is displayed.
5. Click **OK**.
This operation takes 10 to 30 seconds to complete.

4 Layer 2 Connections

4.1 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. Log in to the management console.
2. On the console homepage, choose **Network > Enterprise Switch**.
The **Enterprise Switch** page is displayed.
3. Click the name of the target enterprise switch.
The enterprise switch details page is displayed.
4. In the lower right part of the enterprise switch details page, click **Create Connection**.
The page for creating a Layer 2 connection is displayed.

5. Configure the parameters as prompted. For details, see [Table 4-1](#).

Table 4-1 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, that is, the VPC that the local tunnel subnet belongs to. You do not need to set this parameter.	vpc-01
Layer 2 Connection Subnet	<p>Mandatory</p> <p>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.</p> <ul style="list-style-type: none">• 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	<p>Mandatory</p> <p>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.</p>	Automatically assign
Remote Access Information > Tunnel VNI	<p>Mandatory</p> <p>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.</p>	10001
Remote Access Information > Tunnel IP Address	<p>Mandatory</p> <p>IP address of the VXLAN tunnel used by the on-premises data center to connect to the enterprise switch.</p>	-

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: <ul style="list-style-type: none">• Must contain 1 to 64 characters.• Can contain letters, digits, underscores (_), hyphens (-), and periods (.).	l2conn-01

6. 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.

4.2 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. Log in to the management console.
2. On the console homepage, choose **Network > Enterprise Switch**.
The **Enterprise Switch** page is displayed.
3. Click the name of the target enterprise switch.
The enterprise switch details page is displayed.
4. In the lower part of the enterprise switch details page, view the basic information and topology of a Layer 2 connection.



4.3 Modifying a Layer 2 Connection Name

Scenarios

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

Procedure

1. Log in to the management console.

2. On the console homepage, choose **Network > Enterprise Switch**.
The **Enterprise Switch** page is displayed.
3. Click the name of the target enterprise switch.
The enterprise switch details page is displayed.
4. In the lower part of the enterprise switch details page, locate the Layer 2 connection.
5. Click  next to the Layer 2 connection name and enter a new name.
6. Click .

4.4 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. Log in to the management console.
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.

5 Permissions Management

5.1 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 "Service Overview" in the *Identity and Access Management User Guide*.

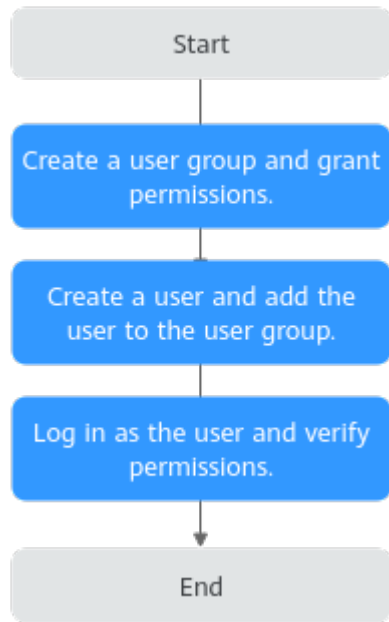
[Figure 5-1](#) shows the procedure for granting permissions.

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](#).

Process Flow

Figure 5-1 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.

6 FAQs

6.1 What Switches Can Connect to Enterprise Switches?

The following lists some switches that support the VXLAN function.

- Huawei switches: Huawei CE58, CE68, CE78, and CE88 series switches, such as CE6870, CE6875, CE6881, CE6863, and CE12800 switches
- Switches of other vendors: Cisco Nexus 9300 and H3C S6520 series switches

6.2 Why Is the Layer 2 Connection in the Not Connected State Even After Its Configuration Is Complete?

Possible causes and solutions:

1. The VXLAN tunnel of your data center is not properly configured.
Log in to the switch of your data center and check its tunnel configurations. For details, see [Step 4: Configure a Tunnel Gateway in Your Data Center](#).
2. The VPN connection fails.
Check the VPN connection configurations.

6.3 Why Is Communication Between the Cloud and On-premises Servers Unavailable Even When the Layer 2 Connection Status Is Connected?

Possible cause: The VXLAN tunnel of your data center is not properly configured.

Solution:

Log in to the switch of your data center and check its tunnel configurations. For details, see [Step 4: Configure a Tunnel Gateway in Your Data Center](#).

A Change History

Released on	Description
2024-12-04	This issue is the first official release.