Enterprise Switch

Best Practices

Issue	04
Date	2022-11-08

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 Enabling Communications Between an On-Premises Data Center and the Cloud Using an Enterprise Switch

1.1 Overview

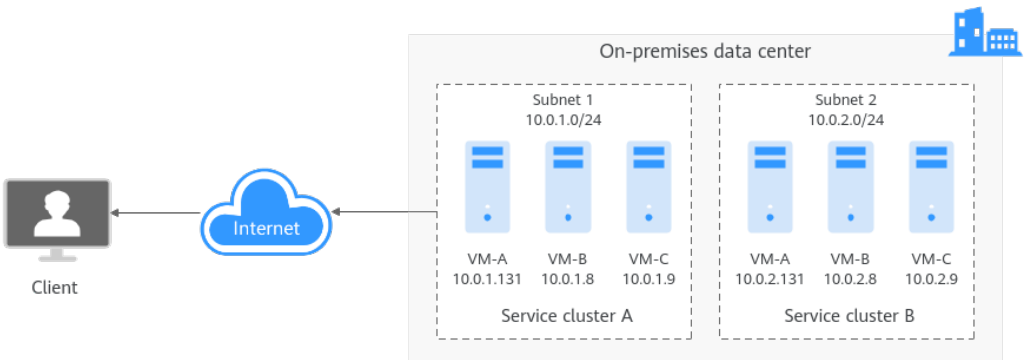
Application Scenario

A company wants to migrate some workloads from its on-premises data center to the cloud. The servers in the data center are deployed in the cluster mode. **Figure 1-1** shows the networking diagram.

During the migration to the cloud, the company has the following requirements:

- Workloads are migrated to the cloud by server and cannot be interrupted during the migration.
- The configuration files of the servers in the on-premises data center record domain names instead of actual IP addresses. Therefore, the IP addresses of servers cannot be changed after migration.

Figure 1-1 Service cluster architecture in the on-premises data center



Architecture

Enterprise switches allow cloud and on-premises networks to communicate at Layer 2. Servers can be migrated to the cloud one by one without interrupting workloads or changing IP addresses.

In **Figure 1-2**, VM-B in the on-premises data center is migrated to the cloud without IP address change using an enterprise switch. The migration process is as follows:

1. Use Direct Connect or VPN to allow the cloud and the on-premises tunnel subnets to communicate at Layer 3. The Layer 2 network used by an enterprise switch is based on the Layer 3 network between tunnel subnets.
2. Create an enterprise switch, establish Layer 2 connections, and configure the VXLAN switch to allow the cloud and the on-premises data center to communicate at Layer 2.
3. Migrate VM-B (10.0.1.8) to ECS-B (10.0.1.21), ensure that the VM-B and ECS-B can communicate with each other, and stop VM-B in the data center during off-peak hours.

   When VM-B is stopped for a short time, workloads are carried by VM-A (10.0.1.131) in the data center and are not interrupted.

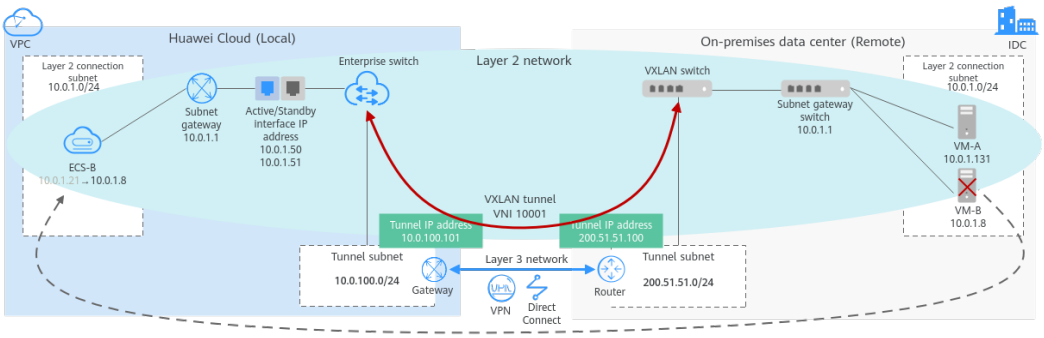
   NOTICE

   To verify the communication between VM-B and ECS-B, the IP address of ECS-B must be different from that of VM-B. Otherwise, the communication fails.

4. Change the IP address of ECS-B on the cloud from 10.0.1.21 to 10.0.1.8 after VM-B in the data center is stopped. In this case, traffic is forwarded to ECS-B on the cloud through the enterprise switch and the IP address is not changed after the migration.

   In addition, ECS-B on the cloud and VM-A in the data center can communicate with each other as if they were in the same subnet.

Figure 1-2 Networking of migration using enterprise switches



Advantages

- On-premises workloads communicate with each other using IP addresses instead of domain names. Reconstructing the on-premises network before cloud migration prolongs the cloud migration period, interrupts businesses, and increases O&M costs.

With enterprise switches, the on-premises IP addresses can remain unchanged, mitigating impacts on workloads and accelerating the cloud migration progress.

- 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.

  With enterprise switches, workloads can be seamlessly migrated to the cloud to prevent any loss caused by cloud migration.

Notes and Constraints

- 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 customer service.
- If you want to use a Direct Connect connection together with an enterprise switch, **submit a service ticket** to check whether your connection can interconnect with an enterprise switch. If your connection does not support this, contact customer service.
- If you use an enterprise switch to connect your on-premises data center to the cloud, the switch of your data center must support the VXLAN function. 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, Ruijie RG-S6250, and H3C S6520 series switches

1.2 Server-based Migration to the Cloud Without Business Interruption (VPN + Enterprise Switch)

Architecture

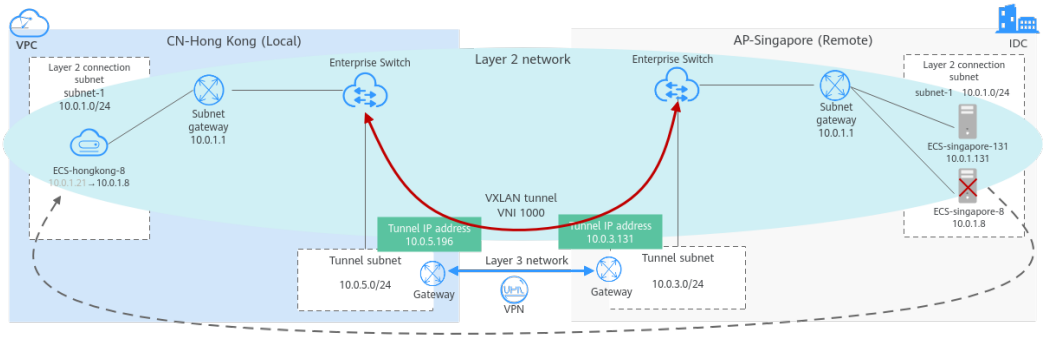
The simulated scenario is described as follows:

- AP-Singapore: is used to simulate an on-premises data center. Workloads of department A are running on the ECSs with IP addresses 10.0.1.131 and 10.0.1.8 in subnet-1. The two ECSs form a cluster to provide services.
- CN-Hong Kong: is used to simulate the cloud. On-premises workloads of department A will be migrated to the ECS with IP address 10.0.1.8 on the cloud.

The migration solution is as follows:

1. Use VPN and an enterprise switch to connect subnets in AP-Singapore and CN-Hong Kong at Layer 2 and migrate the ECS with IP address 10.0.1.8 from the on-premises subnet to the cloud subnet.
2. Delete the ECS with IP address 10.0.1.8 in the data center after the migration. The ECS with IP address 10.0.1.131 in the data center and the ECS with IP address 10.0.1.8 on the cloud can communicate with each other.

Figure 1-3 Networking of migration using enterprise switches (VPN + Enterprise Switch)



Resource and Cost Planning

Table 1-1 Resource and cost planning

Region	Resource	Resource Name	Description	Quantity
CN-Hong Kong: Huawei Cloud (Local)	VPC	vpc-hongkong	CIDR block: 10.0.0.0/16	1
	Subnet	subnet-1	CIDR block: 10.0.1.0/24 Layer 2 connection subnet on Huawei Cloud. ECS in the on-premises data center will be migrated to this subnet.	2
		subnet-5	CIDR block: 10.0.5.0/24 Tunnel subnet on Huawei Cloud. VPN is located in this subnet.	
	ECS	ecs-hongkong-8	Private IP address: 10.0.1.21 ECS on Huawei Cloud. Its IP address is changed from 10.0.1.21 to 10.0.1.8 after migration.	1
	VPN	vpn-hongkong	• Local subnet: subnet-5 • Remote gateway: 119.3.121.173. This is the local gateway of the VPN in AP-Singapore. • Remote subnet: 10.0.3.0/24. This is the subnet of the VPN in AP-Singapore.	1
	Enterprise switch	l2cg-hongkong	• Tunnel connection: VPN • Connection gateway: vpngw-hongkong • Tunnel subnet: subnet-5	1

Region	Resource	Resource Name	Description	Quantity
	Layer 2 connection	l2conn-hongkong	• Tunnel IP address: 10.0.5.196 • Tunnel VNI: 1000	1
AP-Singapore On-premises data center (Remote)	VPC	vpc-singapore	CIDR block: 10.0.0.0/16	1
	Subnet	subnet-1	CIDR block: 10.0.1.0/24 Layer 2 connection subnet that the ECS to be migrated in the on-premises data center is located.	2
		subnet-3	CIDR block: 10.0.3.0/24 Tunnel subnet in the on-premises data center. VPN is located in this subnet.	
	ECS	ecs-singapore-131	Private IP address: 10.0.1.131 ECS in the on-premises data center	2
		ecs-singapore-8	Private IP address: 10.0.1.8 ECS to be migrated in the on-premises data center	
	VPN	vpn-singapore	• Local subnet: subnet-3 • Remote gateway: 139.9.20.226. This is the local gateway of the VPN in CN-Hong Kong. • Remote subnet: 10.0.5.0/24. This is the subnet of the VPN in CN-Hong Kong.	1
	Enterprise switch	l2cg-singapore	• Tunnel connection: VPN • Connection gateway: vpngw-singapore • Tunnel subnet: subnet-3	1
	Layer 2 connection	l2conn-singapore	• Tunnel IP address: 10.0.3.131 • Tunnel VNI: 1000	1

Step 1: Create VPCs and Subnets

Step 1 Log in to the Huawei Cloud management console and select the **AP-Singapore** region.

Step 2 Choose **Networking** > **Virtual Private Cloud**, and click **Create VPC**.

Step 3 Configure a VPC in AP-Singapore based on **Resource and Cost Planning** and click Create Now.

- **Region**: AP-Singapore
- **Name**: vpc-singapore
- **IPv4 CIDR Block**: 10.0.0.0/16
- **Name**: subnet-1
- **IPv4 CIDR Block**: 10.0.1.0/24
- Click **Add Subnet**.
  - **Name**: subnet-3
  - **IPv4 CIDR Block**: 10.0.3.0/24
- For parameters not mentioned, retain their default values or configure them as prompted.

Step 4 View the created VPC.

Step 5 Click **Create VPC**, configure the VPC in CN-Hong Kong based on **Resource and Cost Planning**, and click **Create Now**.

- **Region**: CN-Hong Kong
- **Name**: vpc-hongkong
- **IPv4 CIDR Block**: 10.0.0.0/16
- **Name**: subnet-1
- **IPv4 CIDR Block**: 10.0.1.0/24
- Click **Add Subnet**.
  - **Name**: subnet-5
  - **IPv4 CIDR Block**: 10.0.5.0/24
- For parameters not mentioned, retain their default values or configure them as prompted.

Step 6 View the created VPC.

----End

Step 2: Create ECSs

Step 1 Under **Compute**, select **Elastic Cloud Server**. On the **Elastic Cloud Server** page displayed, click **Buy ECS**.

Step 2 Buy an ECS in AP-Singapore based on **Resource and Cost Planning** and click **Next: Configure Network**.

- **Billing Mode**: Pay-per-use
- **Region**: AP-Singapore
- **Specifications**: Select based on service requirements. This practice uses **c6.large.2** as an example.
- **Image**: Select **Public image**. This practice uses CentOS 8.0 as an example.

- For parameters not mentioned, retain their default values or configure them as prompted.

Step 3 Configure the ECS network and click **Next: Configure Advanced Settings**.

- **Network**: Select **vpc-singapore**, **Manually specify IP address**, and set the IP address.
- **Security Group**: Select **Sys-FullAccess**. This practice uses a security group that allows all inbound and outbound traffic. You can select a security group based on service requirements.
- **EIP**: Not required
- For parameters not mentioned, retain their default values or configure them as prompted.

Step 4 Set the ECS name and password, and click **Next: Confirm**.

- **ECS Name**: ecs-singapore-131
- **Login Mode**: Select **Password** and enter a password.
- For parameters not mentioned, retain their default values or configure them as prompted.

Step 5 Confirm the ECS information, agree to the agreement, and click **Submit**.

Step 6 In the ECS list, locate the row that contains the ECS and click **Remote Login** in the **Operation** column. In the displayed dialog box, click **Log In** under **Other Login Modes**.

Step 7 Log in to the ECS as user **root** and check whether the private IP address of the ECS is the one you planned:

ifconfig

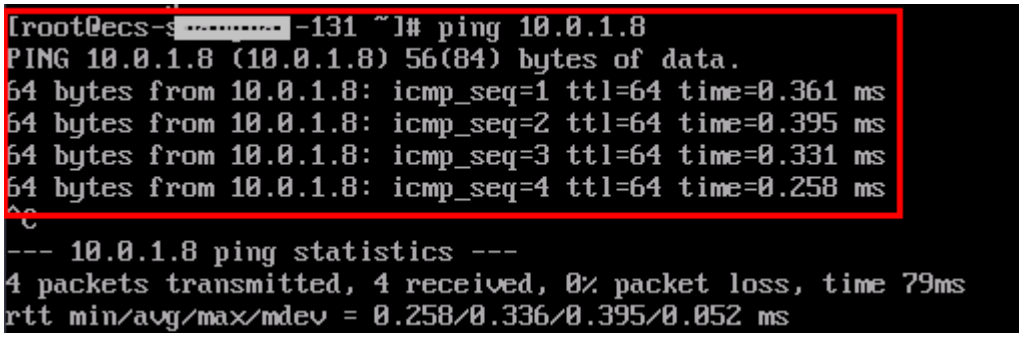
```
[root@ecs-[redacted]-131 ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.1.131  netmask 255.255.255.0  broadcast 10.0.1.255
        inet6 fe80::f816:3eff:fe98:e592  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:98:e5:92  txqueuelen 1000  (Ethernet)
        RX packets 158  bytes 29685 (28.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 245  bytes 25442 (24.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2  bytes 168 (168.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2  bytes 168 (168.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 8 Repeat **Step 1** to **Step 7** to create ecs-singapore-8 (10.0.1.8) in AP-Singapore and ecs-hongkong-8 (10.0.1.8) in CN-Hong Kong.

Step 9 Log in to ecs-singapore-131 as user **root** and run the following command to check whether the ECSs in the subnet can communicate with each other:

ping 10.0.1.8



----End

Step 3: Create VPN

Step 1 Choose **Networking** > **Virtual Private Network**, click **VPN Gateways** and then **Buy VPN Gateway**.

Step 2 Configure all required parameters based on **Resource and Cost Planning** and click **Buy Now**.

- VPN gateway
  - **Billing Mode**: Pay-per-use
  - **Region**: AP-Singapore
  - **VPC**: vpc-singapore
  - **Billed By**: Traffic
- VPN connection
  - **Name**: vpn-singapore
  - **Local Subnet**: subnet-3
  - **Remote Gateway**: Enter **1.1.1.1**. Change this value to that of the gateway in CN-Hong Kong after it is created.
  - **Remote Subnet**: Enter 10.0.5.0/24, the subnet in CN-Hong Kong.
  - **PSK**: Enter a PSK. Make a note of the PSK, which will be used when you create a VPN connection in CN-Hong Kong.
- For parameters not mentioned, retain their default values or configure them as prompted.

Step 3 Confirm the settings and click **Buy Now**.

Step 4 On the **VPN Connections** tab, make a note of the local gateway and local subnet, which will be used when creating a VPN gateway in CN-Hong Kong.

Step 5 Repeat **Step 1** to **Step 4** to create a VPN in CN-Hong Kong. The key parameters are as follows:

- VPN gateway
  - **Billing Mode**: Pay-per-use
  - **Region**: CN-Hong Kong
  - **VPC**: vpngw-hongkong

  - **Billed By**: Traffic
- VPN connection
  - **Name**: vpn-hongkong
  - **Local Subnet**: subnet-5
  - **Remote Gateway**: Enter 119.3.121.173, the gateway in AP-Singapore.
  - **Remote Subnet**: Enter 10.0.3.0/24, the local subnet in AP-Singapore.
  - **PSK**: Enter the PSK that is the same as the one when creating the VPN gateway in AP-Singapore.
- For parameters not mentioned, retain their default values or configure them as prompted.

Step 6 On the **VPN Connections** tab, make a note of the local gateway for changing the value of the remote gateway of the VPN gateway in AP-Singapore.

Step 7 Switch to the AP-Singapore region, go to the VPN console, locate the row that contains vpn-singapore, choose **More** > **Modify**, change the value of **Remote Gateway** to the value of **Local Gateway** of vpn-hongkong, and click **OK**.

Step 8 **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 the VPN service to enable the interconnection.

A VPN has been configured for the subnets in AP-Singapore and CN-Hong Kong and the VPN status is not connected. The VPN takes effect only when there are traffic requests between the two subnets.

----End

Step 4: Buy Enterprise Switch

Step 1 On the console homepage, choose **Networking** > **Enterprise Switch**.

The enterprise switch page is displayed.

Step 2 In the upper right corner of the page, click **Buy**.

The page for buying an enterprise switch is displayed.

Step 3 Configure parameters and click **Next**.

- **Region**: AP-Singapore
- **Tunnel Connection**: VPN
- **Connection Gateway**: vpngw-singapore
- **Tunnel Subnet**: subnet-3
- **Name**: l2cg-singapore
- For parameters not mentioned, retain their default values or configure them as prompted.

Step 4 This operation takes about 6 minutes. Make a note of the local tunnel IP address (10.0.3.131) of l2cg-singapore.

During the creation, refresh the page.

Step 5 Repeat **Step 1** to **Step 3** to create an enterprise switch in CN-Hong Kong. Configure the parameters as follows:

- **Region**: CN-Hong Kong
- **Tunnel Connection**: VPN
- **Connection Gateway**: vpngw-hongkong
- **Tunnel Subnet**: subnet-5
- **Name**: l2cg-hongkong
- For parameters not mentioned, retain their default values or configure them as prompted.

Step 6 This operation takes about 6 minutes. Make a note of the local tunnel IP address (10.0.5.196) of l2cg-hongkong.

During the creation, refresh the page.

Step 7 On the l2cg-hongkong tab, click **Create Connection**, configure **Remote Access Information**, and click **Create**.

- **Tunnel VNI**: 1000
- **Tunnel IP Address**: Enter 10.0.3.131, the local tunnel IP address of l2cg-singapore.
- **Name**: l2conn-hongkong
- For parameters not mentioned, retain their default values or configure them as prompted.

Step 8 This operation takes about 2 minutes. When the status changes to **Connected**, the Layer 2 connection in CN-Hong Kong is successfully created.

During the creation, refresh the page.

Step 9 On the l2cg-singapore tab, click **Create Connection**, configure **Remote Access Information**, and click **Create**.

- **Tunnel VNI**: 1000
- **Tunnel IP Address**: Enter 10.0.5.196, the local tunnel IP address of l2cg-hongkong.
- **Name**: l2conn-singapore
- For parameters not mentioned, retain their default values or configure them as prompted.

Step 10 This operation takes about 2 minutes. When the status changes to **Connected**, the Layer 2 connection in AP-Singapore is successfully created.

During the creation, refresh the page.

----End

Step 5: Migrate an On-Premises Server to the Cloud

Step 1 Migrate ecs-singapore-8 (10.0.1.8) from AP-Singapore to ecs-hongkong-8 (10.0.1.21) in CN-Hong Kong.

For details, see **Server Migration Service Quick Start**.

Step 2 Check whether ecs-singapore-131 (10.0.1.131) in AP-Singapore and ecs-hongkong-8 (10.0.1.21) in CN-Hong Kong can communicate at Layer 2.

1. Choose **Compute** > **Elastic Cloud Server** and switch to the AP-Singapore region.
2. Log in to ecs-singapore-131.

   Multiple methods are available for logging in to an ECS. For details, see **Logging In to an ECS**.

   In this example, use VNC provided on the management console to log in to an ECS.
3. Run the following command to check whether ecs-singapore-131 can access ecs-hongkong-8:

   ping 10.0.1.21
4. Choose **Compute** > **Elastic Cloud Server** and switch to the CN-Hong Kong region.
5. Log in to ecs-hongkong-8.

   Multiple methods are available for logging in to an ECS. For details, see **Logging In to an ECS**.

   In this example, use VNC provided on the management console to log in to an ECS.
6. Run the following command to check whether ecs-hongkong-8 can access ecs-singapore-131:

   ping 10.0.1.131

----End

Step 6: Changing the IP Address of the ECS on the Cloud

Step 1 Choose **Compute** > **Elastic Cloud Server** and switch to the AP-Singapore region.

Step 2 Locate the row that contains ecs-singapore-8 (10.0.1.8), click **More** in the **Operation** column, and click **Stop**.

Step 3 Choose **Compute** > **Elastic Cloud Server** and switch to the CN-Hong Kong region.

Step 4 Locate the row that contains ecs-hongkong-8 (10.0.1.21), click **More** in the **Operation** column, and click **Stop**.

Step 5 Stop ecs-hongkong-8 and choose **More** > **Manage Network** > **Modify Private IP**.

Change the private IP address of ecs-hongkong-8 from 10.0.1.21 to 10.0.1.8.

----End

Step 7: Verify Network Communication Between Cloud and On-premises Servers

Step 1 Choose **Compute** > **Elastic Cloud Server** and switch to the AP-Singapore region.

Step 2 Locate the row that contains ecs-singapore-8 (10.0.1.8), click **More** in the **Operation** column, choose **Delete** and release its EIP and data disks.

This is to delete the on-premises server after its workloads are migrated to the cloud.

Step 3 Log in to ecs-singapore-131 (10.0.1.131).

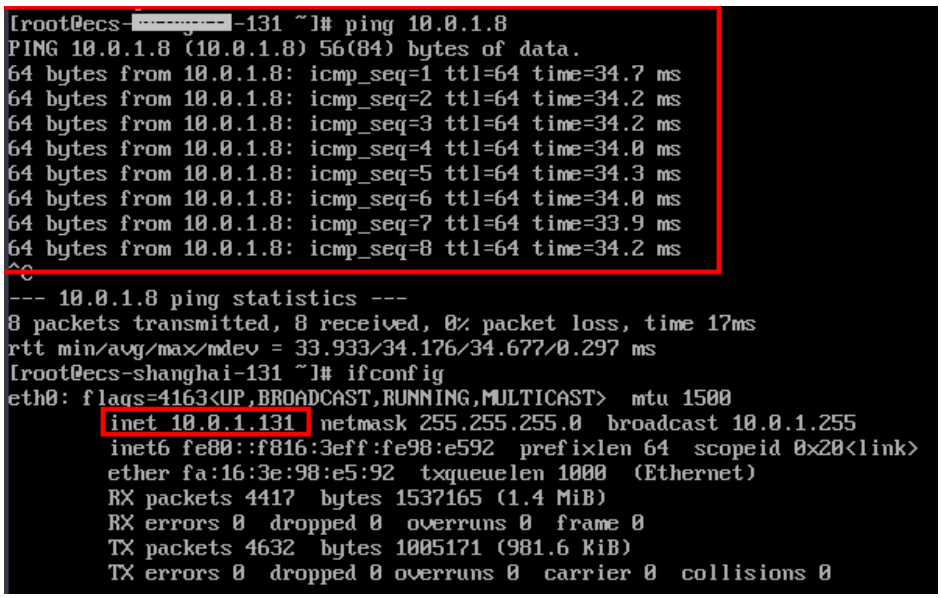
Multiple methods are available for logging in to an ECS. For details, see **Logging In to an ECS**.

In this example, use VNC provided on the management console to log in to an ECS.

Step 4 Run the following command to check whether ecs-singapore-131 can access ecs-hongkong-8:

ping 10.0.1.8

If information similar to the following is displayed, the two ECSs can communicate with each other.



Step 5 Choose **Compute** > **Elastic Cloud Server** and switch to the CN-Hong Kong region.

Step 6 Log in to ecs-hongkong-8 (10.0.1.8).

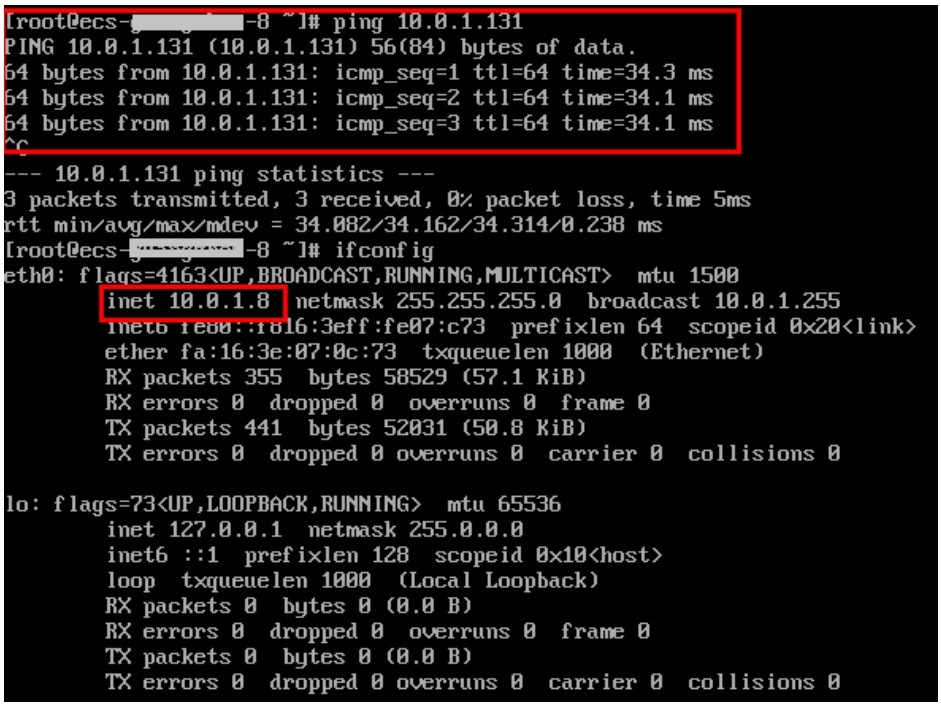
Multiple methods are available for logging in to an ECS. For details, see **Logging In to an ECS**.

In this example, use VNC provided on the management console to log in to an ECS.

Step 7 Run the following command to check whether ecs-hongkong-8 can access ecs-singapore-131:

ping 10.0.1.131

If information similar to the following is displayed, the two ECSs can communicate with each other.



Step 8 Choose **Networking** > **Virtual Private Network** and switch to the AP-Singapore or CN-Hong Kong region. The VPN connection status changes to normal.

On-premises and cloud servers can communicate at Layer 2 and workloads can be migrated on a server basis without interrupting services.

----End

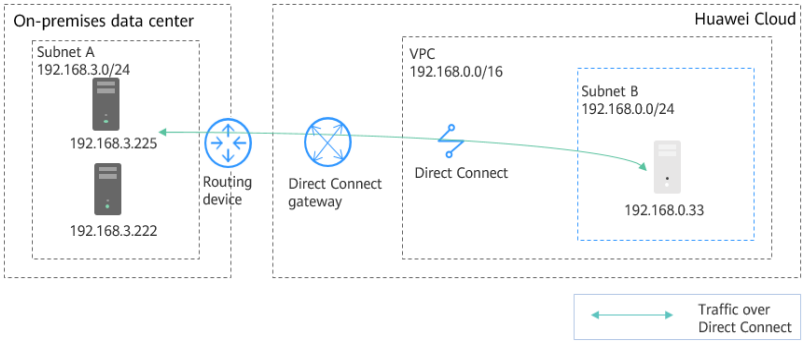
1.3 Server-based Migration to the Cloud Without Business Interruption (Direct Connect + Enterprise Switch)

Architecture

In **Figure 1-4**, the Subnet A in the on-premises data center connects to Subnet B on the cloud through Direct Connect. A customer wants to migrate some workloads in on-premises Subnet A to the cloud. The requirements are as follows:

- Servers migrated to the cloud can communicate with on-premises servers at Layer 2 even if their subnets are the same.
- The Layer 2 network extended to the cloud can communicate with the on-premises data center at Layer 3.
- The Layer 2 network reconstructed at the on-premises data center can communicate with the cloud at Layer 3.

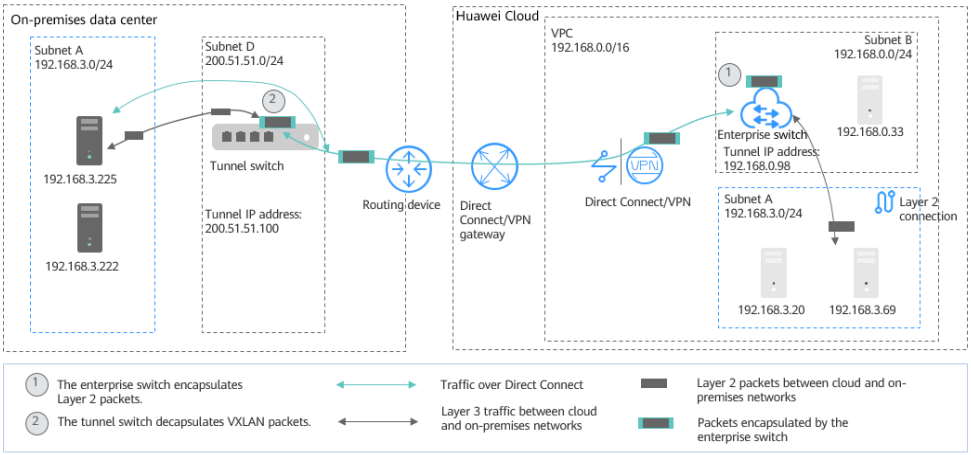
Figure 1-4 Networking diagram



The network deployment details are as follows:

1. Migrate Subnet A to the cloud at Layer 2. Use an enterprise switch to allow the cloud Subnet A and the on-premises Subnet A to communicate at Layer 2. **Figure 1-5** shows the networking diagram.
   a. Create Subnet D in the on-premises data center as the tunnel subnet required by the on-premises VXLAN switch.
   b. Create Subnet A in the VPC on the cloud and use it as the one that is migrated from the on-premises Subnet A.
   c. Use the Subnet B on the cloud as the tunnel subnet, create an enterprise switch and a Layer 2 connection in the subnet, and associate the subnet with a Direct Connect connection to allow cloud and on-premises networks to communicate at Layer 2.

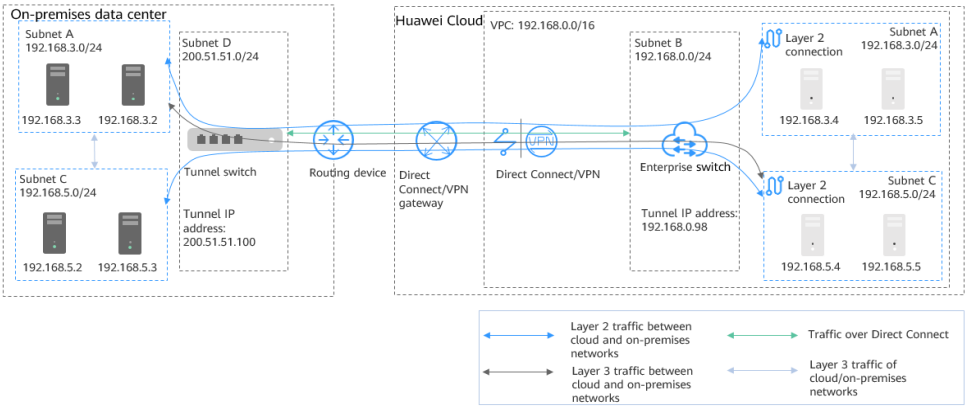
   Figure 1-5 Layer 2 communication between cloud Subnet A and on-premises Subnet A



2. Create a Subnet C both on the cloud and in the on-premises data center. Use an enterprise switch to allow the two subnets to communicate at Layer 2. Use Direct Connect to allow Layer 3 communication between on-premises Subnet A and cloud Subnet C, and between cloud Subnet A and on-premises Subnet C. **Figure 1-6** shows the networking diagram.
   a. Create a Subnet C both on the cloud and in the on-premises data center.
   b. Create a Layer 2 connection based on the existing tunnel subnets to connect the cloud Subnet C and on-premises Subnet C at Layer 2.

Subnets in the same VPC communicate at Layer 3. On-premises Subnet A and cloud Subnet C, cloud Subnet A and on-premises Subnet C communicate at Layer 3.

Figure 1-6 Communication between cloud and on-premises networks at Layer 3



Resource and Cost Planning

Table 1-2 Resource and cost planning

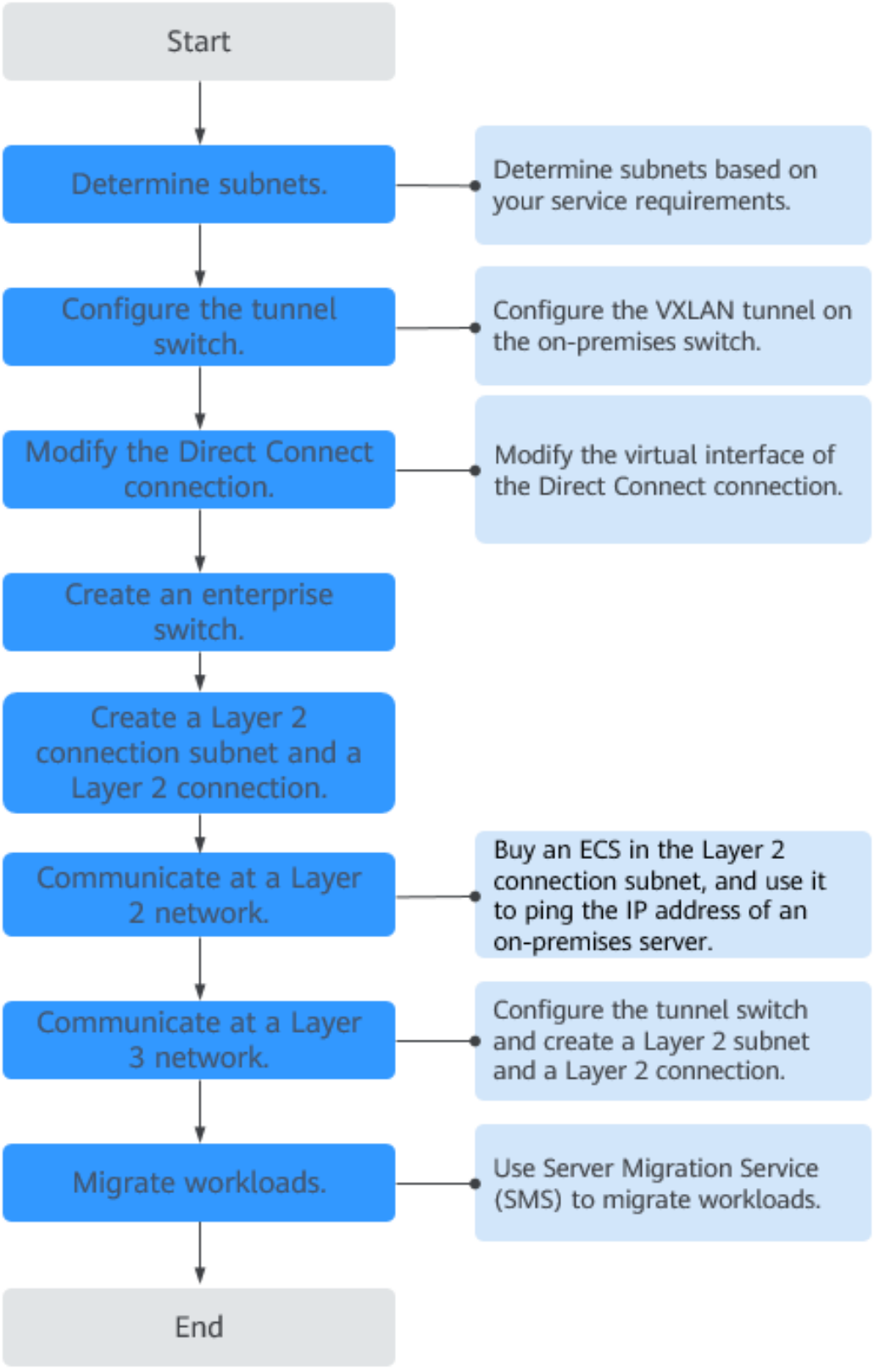
Region	Resource	Description	Quantity
Huawei Cloud (Local)	Subnet	Name: Subnet A CIDR block: 192.168.3.0/24 Subnet of the Layer 2 connection A. This is the subnet that the cloud ECSs reside.	3
		Name: Subnet C CIDR block: 192.168.5.0/24 Subnet of the Layer 2 connection C. This is the subnet that the cloud ECSs reside.	
		Name: Subnet B CIDR block: 192.168.0.0/24 Tunnel subnet on Huawei Cloud used by Direct Connect connection and the enterprise switch	

Region	Resource	Description	Quantity
	ECS	• ECSs in Subnet A. The two ECSs are used to deploy the workloads migrated from the on-premises data center. – Private IP address: 192.168.3.4 – Private IP address: 192.168.3.5 • ECSs in Subnet C: – Private IP address: 192.168.5.4 – Private IP address: 192.168.5.5	4
	Enterprise switch	• Tunnel connection: Direct Connect • Tunnel subnet: Subnet B	1
	Layer 2 connection	• Layer 2 connection A, connecting cloud Subnet A and on-premises Subnet A – Tunnel IP address: 192.168.0.98 – Tunnel VNI: 5530 • Layer 2 connection C, connecting cloud Subnet C and on-premises Subnet C – Tunnel IP address: 192.168.0.98 – Tunnel VNI: 5540 Layer 2 connections of the same enterprise switch must have the same tunnel IP address, but different tunnel VNIs.	2
On-premises data center (Remote)	Subnet	Name: Subnet A CIDR block: 192.168.3.0/24 Subnet of the Layer 2 connection A. This is the subnet that the on-premises clusters reside.	3
		Name: Subnet C CIDR block: 192.168.5.0/24 Subnet of the Layer 2 connection C. This is the subnet that the on-premises clusters reside.	
		Name: Subnet D CIDR block: 200.51.51.0/24 Tunnel subnet in the on-premises data center	

Region	Resource	Description	Quantity
	VXLAN tunnel corresponding to Layer 2 connection	• Layer 2 connection A, connecting cloud Subnet A and on-premises Subnet A – Tunnel IP address: 200.51.51.100 – Tunnel VNI: 5530 • Layer 2 connection C, connecting cloud Subnet C and on-premises Subnet C – Tunnel IP address: 200.51.51.100 – Tunnel VNI: 5540	2

Migration Process

Figure 1-7 Migration process



1. Plan resources and networks based on actual requirements.

   For details, see **Table 1-2**.

   NOTE

   - The subnets shown in the examples are for demonstration purposes. Adjust them according to actual subnets.
   - It is not recommended that the tunnel subnet be too large. The tunnel IP address is assigned from this tunnel subnet to establish a VXLAN tunnel with the enterprise switch on Huawei Cloud. For details, see **Figure 1-5**.

2. Configure the VXLAN tunnel on the on-premises tunnel switch.

   In this example, Subnet D is used by the tunnel switch.

   - Source address: Tunnel IP address (192.168.0.98) on the cloud
   - Destination address: On-premises tunnel IP address (200.51.51.100)
   - Tunnel VNI: 5530

   For details about how to configure on-premises switches, see **Configuring a Tunnel Gateway in Your Data Center**.

3. Modify the virtual interface of the Direct Connect connection and associate Subnet D (200.51.51.0/24) with the connection to enable the communication between the cloud and on-premises tunnel subnets.

   For details, see **Modifying a Virtual Interface**.

4. **Submit a service ticket** to check whether your Direct Connect connection supports VXLAN interconnection with an enterprise switch. If your connection does not support this, contact the Direct Connect service to enable the interconnection.

5. Buy an enterprise switch.

   For details, see **Buying an Enterprise Switch**.

   - **Tunnel Connection**: Select **Direct Connect**.
   - **Connection Gateway**: Select an existing Direct Connect gateway.
   - **Tunnel Subnet**: Select Subnet B (192.168.0.0/24).
   - **Tunnel IP Address**: Set it to the tunnel IP address (192.168.0.98) on the cloud.

   Click **Next** and then **Submit**. This operation takes 3 to 6 minutes to complete.

6. Create a Layer 2 connection subnet and Layer 2 connection to allow cloud Subnet A and on-premises Subnet A to communicate at Layer 2.

   CAUTION

   After a Layer 2 connection subnet is created, the cloud and on-premises subnets have the same CIDR block. As a result, there are conflicting routes used to forward traffic over the Direct Connect connection at Layer 3. Communication at Layer 3 over the connection will be restored only after Layer 2 connections are created.

   a. Create a Layer 2 connection subnet (Subnet A: 192.168.3.0/24) in the VPC.

For details about how to create a subnet, see **Creating a Subnet for the VPC**.

NOTE

- Subnet A, Subnet B, Subnet C and Subnet D cannot overlap.
- Subnet D is used as the tunnel subnet. Set its netmask to 28.
- The CIDR block of the VPC on the cloud depends on the number of required enterprise switches. Each enterprise switch needs three IP addresses from the tunnel subnet.

b. Create a Layer 2 connection A between cloud Subnet A and on-premises Subnet A.

For details, see **Creating a Layer 2 Connection**.

- Layer 2 connection subnet: Subnet A (192.168.3.0/24) on the cloud
- Remote Access Information
  - Tunnel VNI: 5530
  - Tunnel IP address: 200.51.51.100

c. Click **Create**. If the connection status changes to **Connected**, the Layer 2 connection is created successfully.

7. Check communication between cloud Subnet A and on-premises Subnet A at Layer 2.

a. Create two ECSs in the Layer 2 connection subnet (Subnet A) on the cloud.

The private IP addresses of the two ECSs are 192.168.3.20 and 192.168.3.69, respectively.

b. Log in to the two ECSs.

Multiple methods are available for logging in to an ECS. For details, see **Logging In to an ECS**.

In this example, use VNC provided on the management console to log in to an ECS.

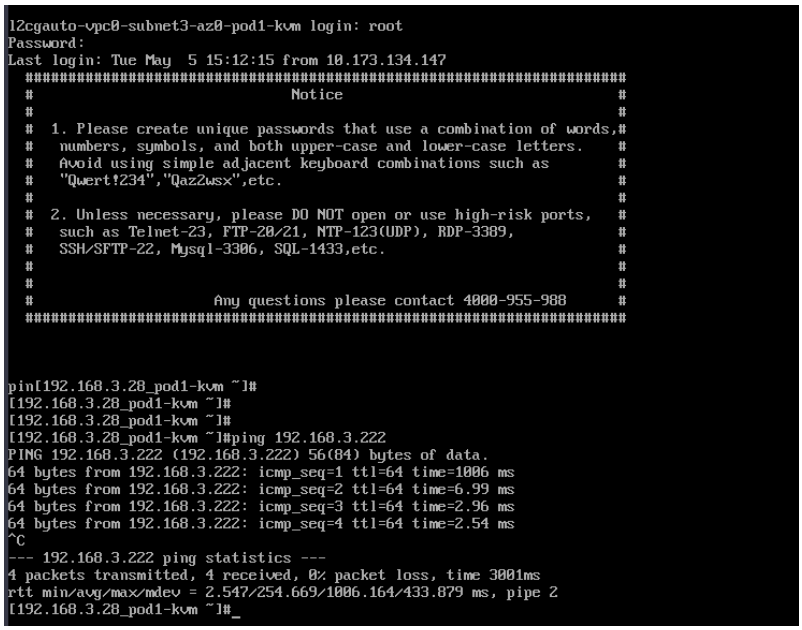
c. Check whether the ECSs can communicate with on-premises servers.

ping *IP address of an on-premises server in the on-premises Subnet A*

Example commands:

- **ping 192.168.3.255**
- **ping 192.168.3.222**

If information similar to the following is displayed, the cloud and on-premises subnets can communicate at Layer 2.



8. Create a Layer 2 connection subnet and a Layer 2 connection to allow on-premises and cloud subnets to communicate at Layer 3.
   a. Create a Layer 2 connection subnet (Subnet C: 192.168.5.0/24) in the VPC.

      For details about how to create a subnet, see **Creating a Subnet for the VPC**.

   b. Create a Layer 2 connection C between cloud Subnet C and on-premises Subnet C.

      For details, see **Creating a Layer 2 Connection**.

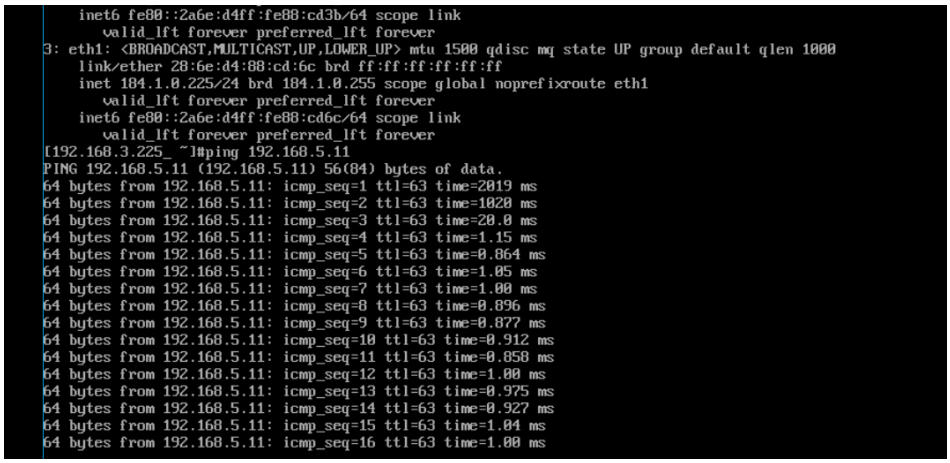
      - Layer 2 connection subnet: Subnet C (192.168.5.0/24) on the cloud
      - Remote Access Information
        - Tunnel VNI: 5540
        - Tunnel IP address: 200.51.51.100

   c. Click **Create**. If the connection status changes to **Connected**, the Layer 2 connection is created successfully. In this case, cloud and on-premises subnets can communicate with each other at Layer 3.

   d. Refer to **7** to check the communication between cloud Subnet C and on-premises Subnet C at Layer 2.

   e. Refer to **7** to check the communication between on-premises Subnet A and cloud Subnet C, and between on-premises Subnet A and cloud Subnet C at Layer 3.

      If information similar to the following is displayed, the subnets can communicate with each other at Layer 3.



9. **Migrate the workloads to the cloud.**
   a. Migrate on-premises workloads to the cloud at Layer 2.

      For details, see **Server Migration Service Quick Start**.
   b. Check the network communication between cloud and on-premises servers.
   c. If the communication is normal, stop the on-premises servers that their workloads are migrated to the cloud.
   d. Change the IP address of servers on the cloud to the IP address of the servers in the on-premises data center.

      For details, see **Modifying a Private IP Address**.
   e. Check the network communication between cloud and on-premises servers.

FAQs

If the subnets to be connected at Layer 2 are not on the same network, the VPC of the enterprise switch must have different CIDR blocks. In this case, you need to use a tool to create subnets across CIDR blocks. If you need help, **submit a service ticket**.

A Change History

Released On	Description
2022-11-08	This issue is the fourth official release. Modified the following content: • Added description about interconnecting Direct Connect or VPN connections with enterprise switches in **Overview**. • Added description about interconnecting VPN connections with enterprise switches in **Server-based Migration to the Cloud Without Business Interruption (VPN + Enterprise Switch)**. • Added description about interconnecting Direct Connect connections with enterprise switches in **Server-based Migration to the Cloud Without Business Interruption (Direct Connect + Enterprise Switch)**.
2022-06-20	This issue is the third official release. Modified the following content: • Changed the region name in the examples in **Server-based Migration to the Cloud Without Business Interruption (VPN + Enterprise Switch)**.

Released On	Description
2022-05-05	This issue is the second official release, which incorporates the following changes: • Added the solution architecture and advantages in **Overview**. • Added the solution architecture, resource and cost planning, and migration operations in **Server-based Migration to the Cloud Without Business Interruption (VPN + Enterprise Switch)**. • Added the solution architecture, resource and cost planning, and migration operations in **Server-based Migration to the Cloud Without Business Interruption (Direct Connect + Enterprise Switch)**.
2022-04-20	This issue is the first official release.