Enterprise Router

Best Practices

Issue	07
Date	2023-12-26

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property 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 Cloud 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 Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Overview

An enterprise router is a high-specification, high-bandwidth, and high-performance router that connects virtual private clouds (VPCs) and on-premises networks to build a central hub network. Enterprise routers use the Border Gateway Protocol (BGP) to learn, dynamically select, or switch between routes, thereby significantly improving the network scalability and O&M efficiency and ensuring the service continuity.

You can use enterprise routers together with other Huawei Cloud services to flexibly construct different networks. This document provides best practices of typical networking for your reference.

Table 1-1 Scenario description

Networking	Scenario	Cloud Service	Description
Cross-region network	**Using Enterprise Router and Cloud Connect Central Network to Allow Communications Among VPCs Across Regions**	• Enterprise Router • Cloud Connect center network • VPC • Elastic Cloud Server (ECS)	For nearby access, an enterprise runs workloads in regions A, B, and C. The VPCs in each region need to communicate with each other. To achieve this, you can: 1. Create an enterprise router in each region: ER-A in region A, ER-B in region B, and ER-C in region C. 2. Create a central network and add ER-A, ER-B, and ER-C to the central network as attachments so that the three enterprise routers can communicate with each other. 3. In region A, attach VPC-A01 and VPC-A02 to ER-A so that the two VPCs can communicate with each other. Perform the same operations in regions B and C. In this way, the VPCs in the three regions can communicate with each other over the central network.
Intra-region network	**Using Enterprise Router to Isolate VPCs in the Same Region**	• Enterprise Router • VPC • ECS	There are four VPCs in a region of Huawei Cloud, with service A, service B, and service C respectively in VPC 1, VPC 2, and VPC 3, and common service in VPC 4. The network requirements are as follows: 1. VPC 1, VPC 2, and VPC 3 need to be isolated from each other. 2. VPC 1, VPC 2, and VPC 3 need to communicate with VPC 4.
Intra-region network	**Using a Third-Party Firewall to Protect VPCs Connected by Enterprise Routers**	• Enterprise Router • VPC • ECS	There are three VPCs in a region of Huawei Cloud, with service A and service B respectively in VPC 1 and VPC 2, and the third-party firewall in VPC 3. For security purposes, the traffic to service A and service B must be filtered by the firewall in VPC 3.

Networking	Scenario	Cloud Service	Description
Hybrid cloud network	**Using Enterprise Router and a Transit VPC to Allow an On-Premises Data Center to Access Service VPCs**	• Enterprise Router • Direct Connect • VPN • VPC • ECS	You can use enterprise routers to build a central network and to simplify the network architecture. There are two typical networking schemes. One is to attach the service VPCs to the enterprise router. The other is to use a transit VPC to build a network, together with VPC Peering and Enterprise Router. Compared with scheme 1, scheme 2 costs less and eliminates some restrictions.
Hybrid cloud network	**Using Enterprise Router and Direct Connect (Virtual Gateway) to Connect an On-Premises Data Center to the Cloud**	• Enterprise Router • Direct Connect (virtual gateway) • VPC • ECS	There are two VPCs in a region. The two VPCs need to access each other and share the same Direct Connect connection to communicate with an on-premises data center. For this to work, you can create an enterprise router in the region, and attach the two VPCs and the virtual gateway of the Direct Connect connection to the enterprise router. The enterprise router can forward traffic among the attached VPCs and the virtual gateway, and the two VPCs can share the Direct Connect connection.

Networking	Scenario	Cloud Service	Description
Hybrid cloud network	**Allowing Direct Connect (Virtual Gateway) and VPN to Work in an Active and Standby Pair to Connect an On-Premises Data Center to the Cloud**	• Enterprise Router • Direct Connect (virtual gateway) • VPN • VPC • ECS	To improve the reliability of a hybrid cloud networking, your enterprise uses both Direct Connect and VPN connections to connect your on-premises data center to the VPCs. The Direct Connect connection works as the active connection and the VPN connection works as the standby one. If the active connection is faulty, services are automatically switched to the standby one, reducing the impact of network interruptions on services. • VPC 1, VPC 2, and the Direct Connect connection are attached to the enterprise router. VPC1 and VPC 2 can communicate with each other. They communicate with the on-premises data center through the Direct Connect connection. • The VPN connection is also attached to the enterprise router. If the Direct Connect connection is faulty, VPC 1 and VPC 2 can communicate with the on-premises data center through the VPN connection.

Networking	Scenario	Cloud Service	Description
Hybrid cloud network	**Allowing a Pair of Direct Connect Connections (Virtual Gateway) to Connect an On-Premises Data Center to the Cloud**	• Enterprise Router • Direct Connect (virtual gateway) • VPC • ECS	To improve the performance and reliability of hybrid cloud networking, your enterprise uses two Direct Connect connections to connect your on-premises data center to the VPCs. Two Direct Connect connections work in load balancing mode. When both connections are working normally, network transmission is greatly improved. If one connection is faulty, the other connection ensures the normal running of the hybrid cloud network and thereby prevents service interruption caused by a single point of failure. • VPC1 and VPC2 can communicate with each other and communicate with the on-premises data center over two Direct Connect connections and an enterprise router. • When one Direct Connect connection is faulty, VPC1 and VPC2 can communicate with the on-premises data center over the normal connection.
Access to the public network from the cloud network	**Using Enterprise Router and NAT Gateway to Allow VPCs to Share an EIP to Access the Internet**	• Enterprise Router • NAT Gateway • Elastic IP • VPC • ECS	There are four VPCs in region A on Huawei Cloud. VPC 1, VPC 2, and VPC 3 need to communicate with each other, and share an EIP through an SNAT rule of a NAT gateway in VPC 4 to access the Internet.
Network migration	**Using an Enterprise Router to Replace VPC Peering Connections**	• Enterprise Router • VPC • ECS	VPC-A, VPC-B, and VPC-C are in region A and connected over VPC peering connections. To improve network scalability and reduce O&M costs, you can use an enterprise router to connect the three VPCs.

Networking	Scenario	Cloud Service	Description
Network migration	**Using Enterprise Router to Reconstruct a Network Connected Through Direct Connect**	• Enterprise Router • Direct Connect • VPC • ECS	Your on-premises data center can access VPC-X in region A over a Direct Connect connection that has a virtual gateway (VGW-A) and two virtual interfaces (VIF-A01 and VIF-A02). To improve the reliability of your hybrid cloud network and reduce O&M costs, you can migrate the network by replacing Direct Connect with Enterprise Router.

2 Using Enterprise Router and Cloud Connect Central Network to Allow Communications Among VPCs Across Regions

2.1 Overview

Scenario

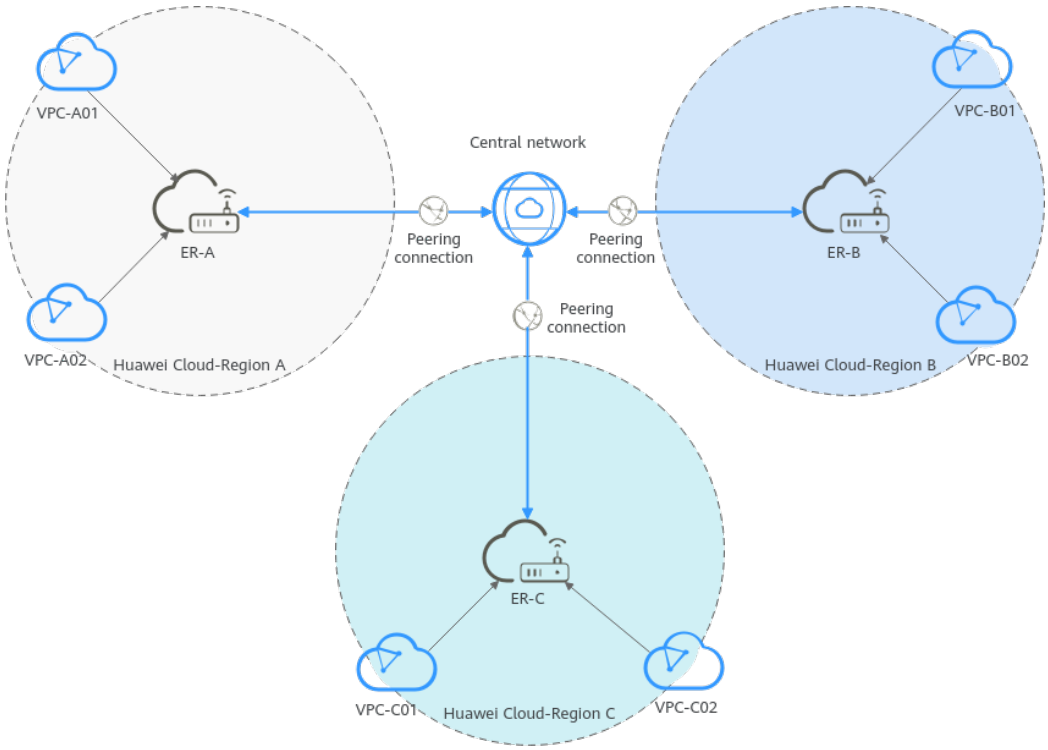
Relying on the Huawei Cloud backbone network, Cloud Connect allows you to build a central network to easily and securely create and manage global network resources on premises and on the cloud. You can connect enterprise routers in two or more regions to a central network, so that VPCs attached to these enterprise routers can communicate with each other across regions.

Architecture

For nearby access, an enterprise runs workloads in regions A, B, and C. The VPCs in each region need to communicate with each other. To achieve this, you can:

1. Create an enterprise router in each region: ER-A in region A, ER-B in region B, and ER-C in region C.
2. Create a central network and add ER-A, ER-B, and ER-C to the central network as attachments so that the three enterprise routers can communicate with each other.
3. In region A, attach VPC-A01 and VPC-A02 to ER-A so that the two VPCs can communicate with each other. Perform the same operations in regions B and C. In this way, the VPCs in the three regions can communicate with each other over the central network.

Figure 2-1 Cross-region VPC network



NOTE

You can **share an enterprise router** with different accounts to attach VPCs of these accounts to the same enterprise router for communications.

Constraints

The CIDR blocks of the VPCs must be unique. If CIDR blocks overlap, the VPCs may fail to communicate with each other.

2.2 Planning Networks and Resources

To use enterprise routers and a central network to connect VPCs across regions, you need:

- **Network Planning**: Plan the central network, VPCs and their subnets, VPC route tables, and enterprise router route tables.
- **Resource Planning**: Plan the quantity, names, and other parameters of the central network, VPCs, ECSs, and enterprise routers.

Network Planning

Figure 2-2 and **Table 2-2** show the network planning and its description for communications among VPCs across regions.

NOTE

In this example, one VPC is created and attached to an enterprise router in each region. Make the plan based on your service requirements.

Figure 2-2 Cross-region VPC network planning

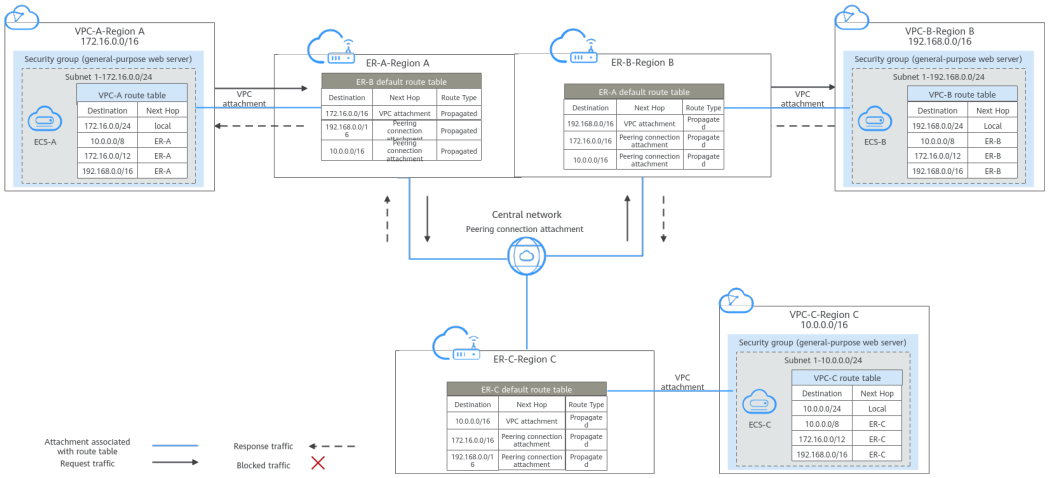


Table 2-1 Network traffic flows

Path	Description
Request traffic: from VPC-A to VPC-B	1. The route table of VPC-A has routes with the next hop set to enterprise router ER-A to forward traffic from VPC-A to ER-A. 2. The route table of enterprise router ER-A has a route with the next hop set to the peering connection attachment and destination to 192.168.0.0/16 to forward traffic from ER-A to enterprise router ER-B. 3. The route table of enterprise router ER-B has a route with the next hop set to the VPC-B attachment to forward traffic from ER-B to the VPC-B.
Response traffic: from VPC-B to VPC-A	1. The route table of VPC-B has routes with the next hop set to enterprise router ER-B to forward traffic from VPC-B to ER-B. 2. The route table of enterprise router ER-B has a route with the next hop set to the peering connection attachment and destination set to 172.16.0.0/16 to forward traffic from ER-B to enterprise router ER-A. 3. The route table of enterprise router ER-A has a route with the next hop set to the VPC-A attachment to forward traffic from ER-A to VPC-A.

Table 2-2 Description for cross-region VPC communications

Resource	Description
VPCs	• The CIDR blocks of the VPCs to be connected cannot overlap with each other. In this example, the CIDR blocks of the VPCs are propagated to the enterprise router route table as the destination in routes. The CIDR blocks cannot be modified and overlapping CIDR blocks may cause route conflicts. If your existing VPCs have overlapping CIDR blocks, do not use propagated routes. Instead, you need to manually add static routes to the route table of the enterprise router. The destination can be VPC subnet CIDR blocks or smaller ones. • Each VPC has a default route table. • The routes in the default route table are described as follows: – Local: a system route for communications between subnets in a VPC. – Enterprise Router: automatically added routes with 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations for routing traffic from a VPC subnet to the enterprise router. See **Table 2-3** for details.
Central network	• Enterprise routers in different regions are added to the central network as attachments. • Global private bandwidths are required for assigning cross-site connection bandwidths to communicate across regions.
Enterprise routers	The network configuration for the enterprise router in the three regions is the same. The following uses region A as an example. If **Default Route Table Association** and **Default Route Table Propagation** are enabled and a VPC is attached to the enterprise router, Enterprise Router will automatically: • Associate the VPC attachment with the default route table of the enterprise router. • Propagate the VPC attachment to the default route table of the enterprise router. The route table automatically learns the VPC CIDR block as the destination of routes. For details, see **Table 2-4**.
ECSs	An ECS is created in each VPC. If the ECSs are in different security groups, add rules to the security groups to allow access to each other.

Table 2-3 VPC route table

Destination	Next Hop	Route Type
10.0.0.0/8	Enterprise router	Static route: Custom

Destination	Next Hop	Route Type
172.16.0.0/12	Enterprise Router	Static route: Custom
192.168.0.0/16	Enterprise Router	Static route: Custom

NOTE

- If you enable **Auto Add Routes** when creating a VPC attachment, you do not need to manually add static routes to the VPC route table. Instead, the system automatically adds routes (with this enterprise router as the next hop and 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations) to all route tables of the VPC.
- If an existing route in the VPC route tables has a destination to 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16, the routes will fail to be added. In this case, do not to enable **Auto Add Routes**. After the attachment is created, manually add routes.
- Do not set the destination of a route (with an enterprise router as the next hop) to 0.0.0.0/0 in the VPC route table. If an ECS in the VPC has an EIP bound, the VPC route table will have a policy-based route with 0.0.0.0/0 as the destination, which has a higher priority than the route with the enterprise router as the next hop. In this case, traffic is forwarded to the EIP and cannot reach the enterprise router.

Table 2-4 Enterprise router route table

Enterprise Router	Destination	Next Hop	Route Type
Region A: ER-A	VPC-A CIDR block: 172.16.0.0/16	VPC attachment: er-attach-VPC-A	Propagated route
	VPC-B CIDR block: 192.168.0.0/16	Peering connection attachment: region-A-region-B	Propagated route
	VPC-C CIDR block: 10.0.0.0/16	Peering connection attachment: region-A-region-C	Propagated route
Region B: ER-B	VPC-B CIDR block: 192.168.0.0/16	VPC-B attachment: er-attach-VPC-B	Propagated route
	VPC-A CIDR block: 172.16.0.0/16	Peering connection attachment: region-B-region-A	Propagated route
	VPC-C CIDR block: 10.0.0.0/16	Peering connection attachment: region-B-region-C	Propagated route
Region C: ER-C	VPC-C CIDR block: 10.0.0.0/16	VPC-C attachment: er-attach-VPC-C	Propagated route
	VPC-A CIDR block: 172.16.0.0/16	Peering connection attachment: region-C-region-A	Propagated route

Enterprise Router	Destination	Next Hop	Route Type
	VPC-B CIDR block: 192.168.0.0/16	Peering connection attachment: region-C-region-B	Propagated route

Resource Planning

Each region has an enterprise router, VPCs, and ECSs. They can be in different availability zones (AZs).

NOTE

The following resource planning is only for your reference.

Table 2-5 Resource planning for cross-region VPC communications

Resource	Quantity	Description
VPC	3	A service VPC is created in each region for running workloads. • **Name**: Set it based on site requirements. In this example, the names are as follows: – Region A: VPC-A – Region B: VPC-B – Region C: VPC-C • **IPv4 CIDR block**: The CIDR blocks of VPCs must be unique. Plan the CIDR blocks based on site requirements. In this example, the CIDR blocks are as follows: – VPC-A: 172.16.0.0/16 – VPC-B: 192.168.0.0/16 – VPC-C: 10.0.0.0/16 • **Subnet**: The subnet CIDR blocks that need to communicate with each other must be unique. Plan the subnets based on site requirements. In this example, the subnets are as follows: – subnet-A01: 172.16.0.0/24 – subnet-B01: 192.168.0.0/24 – subnet-C01: 10.0.0.0/24

Resource	Quantity	Description
Enterprise router	3	An enterprise router is in each region. The VPC in each region is attached to the enterprise router, and a peering connection attachment is created between every two enterprise routers. • **Name**: Set it based on site requirements. – Region A: ER-A – Region B: ER-B – Region C: ER-C • **ASN**: Set different ASNs for enterprise routers. In this example, the ASNs are as follows: – ER-A: 64512 – ER-B: 64513 – ER-C: 64514 • **Default Route Table Association**: Enable • **Default Route Table Propagation**: Enable • **Auto Accept Shared Attachments**: Set it based on site requirements. In this example, **Enable** is selected. • **Attachment**: Three attachments are required for each enterprise router. In this example, the attachments are as follows: ER-A: – VPC attachment er-attach-VPC-A: connects the network between VPC-A and ER-A. – Peering connection attachment region-A-region-B: connects the network between ER-A and ER-B. – Peering connection attachment region-A-region-C: connects the network between ER-A and ER-C. ER-B: – VPC attachment er-attach-VPC-B: connects the network between VPC-B and ER-B. – Peering connection attachment region-B-region-A: connects the network between ER-B and ER-A. – Peering connection attachment region-B-region-C: connects the network between ER-B and ER-C. ER-C: – VPC attachment er-attach-VPC-C: connects the network between VPC-C and ER-C. – Peering connection attachment region-C-region-A: connects the network between ER-C and ER-A. – Peering connection attachment region-C-region-A: connects the network between ER-C and ER-B.

Resource	Quantity	Description
Central network	1	A central network is required, with all enterprise routers are added to it as attachments. • **Name**: Set it based on site requirements. In this example, the name is gcn-A-B-C. • **Policy**: – Region A: enterprise router ER-A – Region B: enterprise router ER-B – Region C: enterprise router ER-C • **Cross-region connection bandwidths**: – Region A-Region B: 10 Mbit/s – Region A-Region C: 5 Mbit/s – Region B-Region C: 20 Mbit/s
Global private bandwidth	3	In this example, you need to purchase three global private bandwidths to connect the cloud backbone networks in different regions. • **Name**: Set it based on site requirements. In this example, the names are as follows: – Global private bandwidth for communications between region A and region B: bandwidth-A-B – Global private bandwidth for communications between region A and region C: bandwidth-A-C – Global private bandwidth for communications between region B and region C: bandwidth-B-C • **Bandwidth type**: Set it based on site requirements. In this example, select **Geographic-region** because regions A, B, and C are in the same geographic region. • **Geographic region**: Set it based on site requirements. In this example, select **Chinese Mainland**. • **Connect regions**: Select the regions based on site requirements.

Resource	Quantity	Description
ECS	3	Create an ECS in each region to verify network connectivity. • **Name**: Set it based on site requirements. In this example, the names are as follows: – Region A: ECS-A – Region B: ECS-B – Region C: ECS-C • **Image**: Select an image based on site requirements. In this example, a public image (CentOS 8.2 64bit) is used. • **Network**: Select the VPC and subnet based on site requirements. In this example, the VPCs and subnets are as follows: – ECS-A: VPC-A, subnet-A01 – ECS-B: VPC-B, subnet-B01 – ECS-C: VPC-C, subnet-C01 • **Security Group**: Select a security group based on site requirements. In this example, the security group is named sg-demo and uses a general-purpose web server template. • Private IP addresses: – ECS-A: 172.16.0.91 – ECS-B: 192.168.0.5 – ECS-C: 10.0.0.29

2.3 Enabling Cross-Region VPC Communications over a Central Network

Table 2-6 shows the process of enabling VPCs in different regions to communicate with each other through enterprise routers and a central network.

Table 2-6 Description of the steps for connecting VPCs across regions

No.	Step	Description
1	**Creating Cloud Resources**	1. Create three enterprise routers with one in each region. 2. Create a service VPC and its subnet in each region. 3. Create an ECS in the subnet of the service VPC. 4. Create a central network. When creating the central network, create a policy and add the enterprise routers in different regions to the policy. 5. Purchase three global private bandwidths to connect networks in different regions.
2	**Creating VPC Attachments for Enterprise Routers**	Create a VPC attachment to each enterprise router.
3	**Assigning Cross-Site Connection Bandwidths**	Assign cross-site connection bandwidths on the central network based on service requirements.
4	**Verifying Network Connectivity**	Log in to the ECS in each region and run the **ping** command to verify the network connectivity.

2.4 Procedure for Enabling Cross-Region VPC Communications over a Central Network

2.4.1 Creating Cloud Resources

In this example, you need to create a central network, three enterprise routers, three VPCs, and three ECSs based on **Table 2-5**.

Step 1 Create an enterprise router in each of the three regions.

For details, see **Creating an Enterprise Router**.

NOTE

Specify a unique ASN for each enterprise router.

Step 2 Create a VPC in each of the three regions.

For details, see **Creating a VPC**.

Step 3 Create an ECS in each of the three regions.

For details, see **Overview**.

Step 4 Create a central network and add the enterprise routers to the central network as attachments.

1. Create a central network and add the enterprise routers to the policy.

   For details, see **Creating a Central Network**.

2. On the Enterprise Router console, view the peering connection attachments.

   For details, see **Viewing Details About an Attachment**.

   If the status of the peering connection attachments is **Normal**, the attachments are available.

   Default Route Table Association and **Default Route Table Propagation** are enabled when you create enterprise routers. After peering connection attachments are created for the enterprise routers, the system will automatically:

   - Associate the peering connection attachment with the default route table of each enterprise router.
   - Propagate the peering connection attachment to the default route table of each enterprise router. The route tables automatically learn routes from each other.

Step 5 Purchase three global private bandwidths to connect networks in different regions.

For details, see **Purchasing a Global Private Bandwidth**.

----End

2.4.2 Creating VPC Attachments for Enterprise Routers

Create a VPC attachment to each enterprise router. For details about resource planning, see **Table 2-5**.

Step 1 In region A, attach VPC-A to enterprise router ER-A.

1. Attach the VPC to the enterprise router.

   In this example, enable **Auto Add Routes** to save you from manually configuring routes in the VPC route table.

   For details, see **Creating VPC Attachments to the Enterprise Router**.

   Default Route Table Association and **Default Route Table Propagation** are enabled when you create the enterprise router. After VPCs are attached to the enterprise router, the system will automatically:

   - Associate the VPC attachment with the default route table of the enterprise router.
   - Propagate the VPC attachment to the default route table of the enterprise router. The route table automatically learns the VPC CIDR block as the destination of routes.

2. (Optional) Add routes to the VPC route table for traffic to route through the enterprise router.

   Skip this step if you have enabled **Auto Add Routes** in the previous step. For details about routes, see **Table 2-3**.

   For details, see **Adding Routes to VPC Route Tables**.

Step 2 In region B, attach VPC-B to enterprise router ER-B by referring to **Step 1**.

Step 3 In region C, attach VPC-C to enterprise router ER-C by referring to **Step 1**.

----End

2.4.3 Assigning Cross-Site Connection Bandwidths

To allow cross-region VPC communications, you need to assign cross-region connection bandwidths on the central network based on service requirements by referring to **Table 2-5**.

NOTE

By default, Cloud Connect allocates 10 kbit/s of bandwidth for testing connectivity between regions. After the peering connection attachments are created, you can verify the network connectivity between VPCs. For details, see **Verifying Network Connectivity**.

To ensure your workloads run normally, you need to purchase global private bandwidths and assign cross-site connection bandwidths.

Step 1 Assign bandwidth from the purchased global private bandwidth for the communications between region A and region B.

For details, see **Assigning a Cross-Site Connection Bandwidth**.

Step 2 Assign bandwidth from the purchased global private bandwidth for the communications between region A and region C.

Step 3 Assign bandwidth from the purchased global private bandwidth for the communications between region B and region B.

----End

2.4.4 Verifying Network Connectivity

Step 1 Log in to the ECS.

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 2 Verify the network connectivity between every two VPCs.

1. Verify the network connectivity between VPCs.

   ping *IP address of the ECS*

   Use ECS-A as an example to verify the network connectivity between VPC-A and VPC-B:

   ping 192.168.0.5

   If information similar to the following is displayed, the communications between VPC-A and VPC-B are normal:

```
[root@ECS-A ~]# ping 192.168.0.5
PING 192.168.0.5 (192.168.0.5) 56(84) bytes of data.
64 bytes from 192.168.0.5: icmp_seq=1 ttl=62 time=30.6 ms
64 bytes from 192.168.0.5: icmp_seq=2 ttl=62 time=30.2 ms
64 bytes from 192.168.0.5: icmp_seq=3 ttl=62 time=30.1 ms
64 bytes from 192.168.0.5: icmp_seq=4 ttl=62 time=30.1 ms
...
--- 192.168.0.5 ping statistics ---
```


2. Verify the network connectivity between VPCs.

   ping *IP address of the ECS*

   Use ECS-A as an example to verify the network connectivity between VPC-A and VPC-C:

   ping 10.0.0.29

   If information similar to the following is displayed, the communications between VPC-A and VPC-C are normal:

```
[root@ECS-A ~]# ping 10.0.0.29
PING 10.0.0.29 (10.0.0.29) 56(84) bytes of data.
64 bytes from 10.0.0.29: icmp_seq=1 ttl=62 time=27.4 ms
64 bytes from 10.0.0.29: icmp_seq=2 ttl=62 time=27.0 ms
64 bytes from 10.0.0.29: icmp_seq=3 ttl=62 time=26.10 ms
64 bytes from 10.0.0.29: icmp_seq=4 ttl=62 time=26.9 ms
...
--- 10.0.0.29 ping statistics ---
```

Step 3 Repeat **Step 1** to **Step 2** to verify the network connectivity between VPC-B and VPC-C.

----End

3 Using Enterprise Router to Isolate VPCs in the Same Region

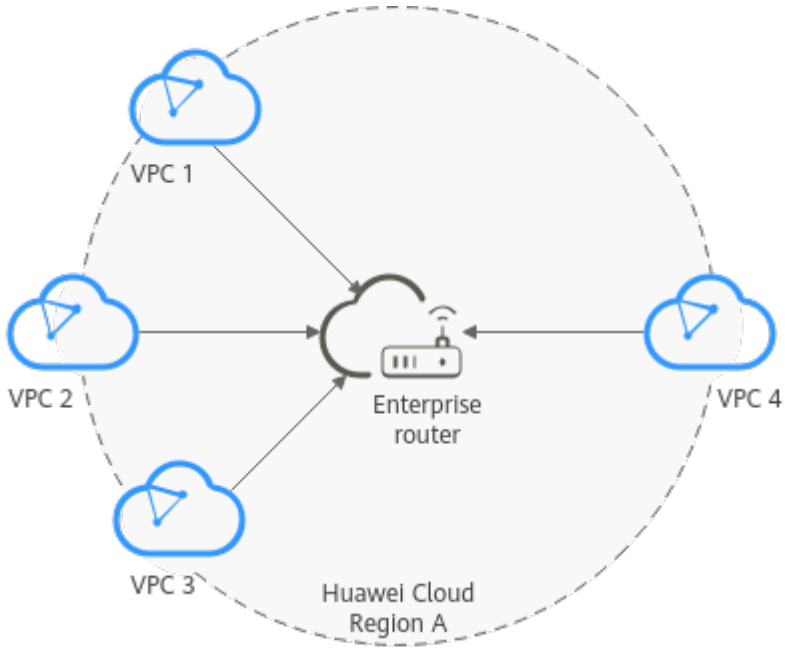
3.1 Overview

Background

There are four VPCs in a region of Huawei Cloud, with service A, service B, and service C respectively in VPC 1, VPC 2, and VPC 3, and common service in VPC 4. The network requirements are as follows:

1. VPC 1, VPC 2, and VPC 3 need to be isolated from each other.
2. VPC 1, VPC 2, and VPC 3 need to communicate with VPC 4.

Figure 3-1 Isolation of VPCs in the same region



NOTE

You can **share an enterprise router** with different accounts to attach VPCs of these accounts to the same enterprise router for communications.

Operation Procedure

Figure 3-2 shows the procedure for using an enterprise router to isolate VPCs in the same region.

Figure 3-2 Flowchart for isolating VPCs in the same region

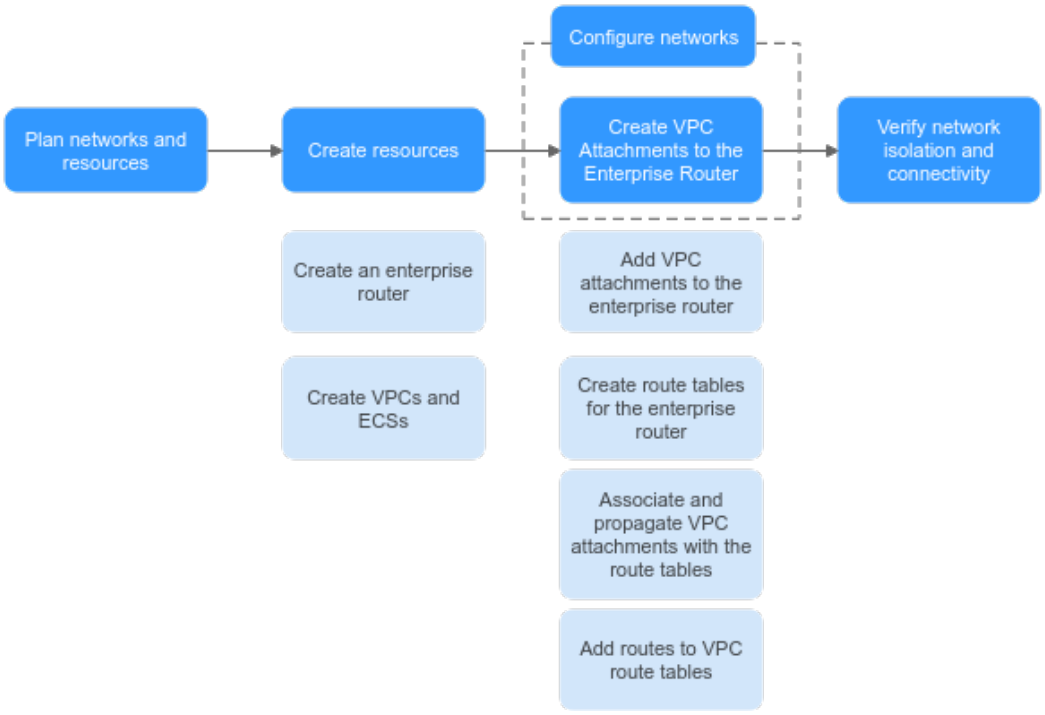


Table 3-1 Description of procedures for isolating VPCs in the same region

No.	Path	Description
1	**Planning Networks and Resources**	Plan required CIDR blocks and the number of resources.
2	**Creating Resources**	1. **Create an enterprise router**. 2. **Create four VPCs and four ECSs**.

No.	Path	Description
3	Creating VPC Attachments for the Enterprise Router	1. Create VPC attachments for the enterprise router: a. Attach the four VPCs to the enterprise router. b. Create two custom route tables for the enterprise router. c. Associate and propagate VPC attachments with the route tables of the enterprise router. d. Add routes to the route tables of the VPCs for traffic to route through the enterprise router.
4	Verifying Network Isolation and Connectivity	Log in to an ECS and run the **ping** command to verify the network isolation and connectivity.

3.2 Planning Networks and Resources

To use an enterprise router to isolate VPCs in the same region, you need to:

- **Network Planning**: Plan CIDR blocks of VPCs and their subnets, and route tables of VPCs and the enterprise router.
- **Resource Planning**: Plan the quantity, names, and other parameters of cloud resources, including VPCs, ECSs, and the enterprise router.

Network Planning

Figure 3-3 and **Table 3-3** show the network planning and its description for isolating VPCs in the same region.

Figure 3-3 Network planning for isolating VPCs in the same region

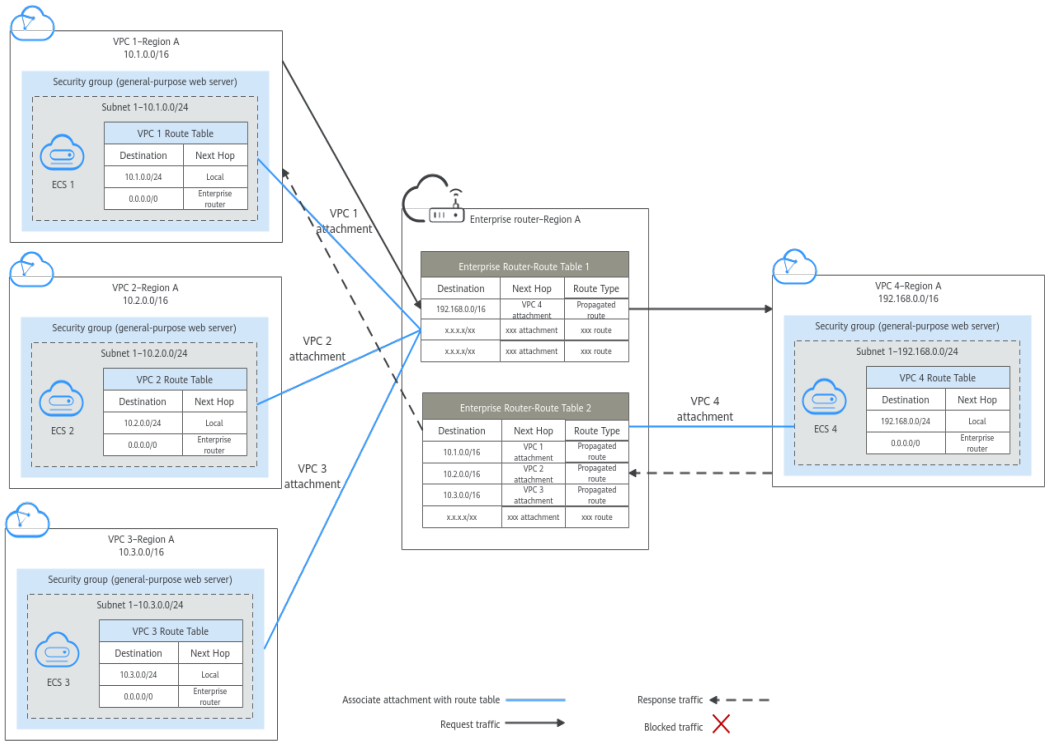


Table 3-2 Network traffic flows

Path	Description
Request traffic: from VPC 1 to VPC 4	1. The route table of VPC 1 has routes with the next hop set to the enterprise router to forward traffic from VPC 1 to the enterprise router. 2. VPC 1 is associated with route table 1 of the enterprise router. This route table has a route with the next hop set to VPC 4 attachment to forward traffic from the enterprise router to VPC 4.
Response traffic: from VPC 4 to VPC 1	1. The route table of VPC 4 has routes with the next hop set to the enterprise router to forward traffic from VPC 4 to the enterprise router. 2. VPC 4 is associated with route table 2 of the enterprise router. This route table has a route with the next hop set to VPC 1 attachment to forward traffic from the enterprise router to VPC 1.

Table 3-3 Description of network planning for isolating VPCs in the same region

Resource	Description
VPCs	• VPC 1, VPC 2, and VPC 3 need to be isolated from each other, but all of them need to communicate with VPC 4. • The CIDR blocks of the VPCs to be connected cannot overlap with each other. In this example, the CIDR blocks of the VPCs are propagated to the enterprise router route table as the destination in routes. The CIDR blocks cannot be modified and overlapping CIDR blocks may cause route conflicts. If your existing VPCs have overlapping CIDR blocks, do not use propagated routes. Instead, you need to manually add static routes to the route table of the enterprise router. The destination can be VPC subnet CIDR blocks or smaller ones. • Each VPC has a default route table. • The routes in the default route table are described as follows: – Local: a system route for communications between subnets in a VPC. – Enterprise Router: custom routes with 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations for routing traffic from a VPC subnet to the enterprise router. See **Table 3-4** for details.
Enterprise router	Disable the **Default Route Table Association** and **Default Route Table Propagation**, create two route tables, attach the four VPCs to the enterprise router, and configure the route tables as follows: • Associate VPC 1, VPC 2, and VPC 3 attachments with the route table 1. Propagate VPC 4 attachment to the route table 1. The route table automatically learns the VPC CIDR blocks as the destination of routes. For details, see **Table 3-5**. • Associate the VPC 4 attachment with the route table 2. Propagate VPC 1, VPC 2, and VPC 3 attachments to the route table 2. The route table automatically learns the VPC CIDR blocks as the destination of routes. For details, see **Table 3-6**.
ECSs	The four ECSs are in different VPCs. If the ECSs are in different security groups, add rules to the security groups to allow access to each other.

Table 3-4 VPC route table

Destination	Next Hop	Route Type
10.0.0.0/8	Enterprise router	Static route: Custom
172.16.0.0/12	Enterprise Router	Static route: Custom
192.168.0.0/16	Enterprise Router	Static route: Custom

NOTE

- If you enable **Auto Add Routes** when creating a VPC attachment, you do not need to manually add static routes to the VPC route table. Instead, the system automatically adds routes (with this enterprise router as the next hop and 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations) to all route tables of the VPC.
- If an existing route in the VPC route tables has a destination to 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16, the routes will fail to be added. In this case, do not to enable **Auto Add Routes**. After the attachment is created, manually add routes.
- Do not set the destination of a route (with an enterprise router as the next hop) to 0.0.0.0/0 in the VPC route table. If an ECS in the VPC has an EIP bound, the VPC route table will have a policy-based route with 0.0.0.0/0 as the destination, which has a higher priority than the route with the enterprise router as the next hop. In this case, traffic is forwarded to the EIP and cannot reach the enterprise router.

Table 3-5 Enterprise router route table 1

Destination	Next Hop	Route Type
VPC 4 CIDR block: 192.168.0.0/16	VPC 4 attachment: er-attach-share	Propagated route

Table 3-6 Enterprise router route table 2

Destination	Next Hop	Route Type
VPC 1 CIDR block: 10.1.0.0/16	VPC 1 attachment: er-attach-isolation-01	Propagated route
VPC 2 CIDR block: 10.2.0.0/16	VPC 2 attachment: er-attach-isolation-02	Propagated route
VPC 3 CIDR block: 10.3.0.0/16	VPC 3 attachment: er-attach-isolation-03	Propagated route

Resource Planning

Each region has an enterprise router, VPCs, and ECSs. They can be in different AZs.

NOTE

The following resource details are only examples. You can modify them as required.

- One enterprise router. See details in **Table 3-7**.

Table 3-7 Enterprise router details

Enterprise Router Name	ASN	Default Route Table Association	Default Route Table Propagation	Route Table	Attachment
er-test-01	64512	Disabled	Disabled	Two route tables: • er-rtb-isolation • er-rtb-share	er-attach-isolation-01
					er-attach-isolation-02
					er-attach-isolation-03
					er-attach-share

Table 3-8 Enterprise router route table 1 details

Name	Associated Attachment	Propagated Attachment
er-rtb-isolation	er-attach-isolation-01	er-attach-share
	er-attach-isolation-02	
	er-attach-isolation-03	

Table 3-9 Enterprise router route table 2 details

Name	Associated Attachment	Propagated Attachment
er-rtb-share	er-attach-share	er-attach-isolation-01
		er-attach-isolation-02
		er-attach-isolation-03

- Four VPCs that do not overlap with each other. See details in **Table 3-10**.

Table 3-10 VPC details

VPC Name	VPC CIDR Block	Subnet Name	Subnet CIDR Block	Association Route Table
vpc-isolation-01	10.1.0.0/16	subnet-isolation-01	10.1.0.0/24	Default route table

VPC Name	VPC CIDR Block	Subnet Name	Subnet CIDR Block	Association Route Table
vpc-isolation-02	10.2.0.0/16	subnet-isolation-02	10.2.0.0/24	Default route table
vpc-isolation-03	10.3.0.0/16	subnet-isolation-03	10.3.0.0/24	Default route table
vpc-share	192.168.0.0/16	subnet-share	192.168.0.0/24	Default route table

- Four ECSs, respectively, in four VPCs. See details in **Table 3-11**.

Table 3-11 ECS details

ECS Name	Image	VPC Name	Subnet Name	Security Group	Private IP Address
ecs-isolation-01	Public image: CentOS 7.5 64-bit	vpc-isolation-01	subnet-isolation-01	sg-demo (general-purpose web server)	10.1.0.134
ecs-isolation-02		vpc-isolation-02	subnet-isolation-02		10.2.0.215
ecs-isolation-03		vpc-isolation-03	subnet-isolation-03		10.3.0.14
ecs-share		vpc-share	subnet-share		192.168.0.130

3.3 Creating Resources

3.3.1 Creating an Enterprise Router

Scenarios

This section describes how to create an enterprise router.

Procedure

Step 1 Create an enterprise router in region A.

For details, see **Creating an Enterprise Router**.

For enterprise router details, see **Table 3-7**.

----End

3.3.2 Creating VPCs and ECSs

Scenarios

This section describes how to create VPCs and ECSs.

Procedure

Step 1 Create four VPCs in region A and an ECS in each VPC.

For details, see **Creating a VPC**.

For details, see **Overview**.

- For details about VPC and subnet planning, see **Table 3-10**.
- For details about ECS planning, see **Table 3-11**.

----End

3.4 Configuring Networks

3.4.1 Creating VPC Attachments for the Enterprise Router

Scenarios

This section describes how to attach VPCs to the enterprise router and configure routes for the VPCs and enterprise router.

Procedure

Step 1 Attach the four VPCs to the enterprise router.

For details, see **Creating VPC Attachments to the Enterprise Router**.

Step 2 Create two route tables for the enterprise router.

For details, see **Creating a Route Table**.

Step 3 Associate and propagate VPC attachments with the route tables of the enterprise router.

For details about creating an association, see **Creating an Association**.

For details about creating a propagation, see **Creating a Propagation**.

- For route table 1 details, see **Table 3-8**.
- For route table 2 details, see **Table 3-9**.

Step 4 Add routes to VPC route tables for traffic to route through the enterprise router.

For details, see **Adding Routes to VPC Route Tables**.

----End

3.5 Verifying Network Isolation and Connectivity

Scenarios

This section describes how to log in to ECSs and verify the connectivity between VPCs.

Procedure

Step 1 Log in to the ECS.

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 2 Verify whether the VPCs are isolated or connected from each other.

1. Verify whether the VPCs are isolated from each other.

   ping *IP address of the ECS*

   To verify whether vpc-isolation-01 is isolated from vpc-isolation-02 and vpc-isolation-03, log in to ecs-isolation-01 and run the following commands:

   ping 10.2.0.215

   ping 10.3.0.14

   If information similar to the following is displayed, vpc-isolation-01 is isolated from vpc-isolation-02 and vpc-isolation-03.

   ```
   PING 10.2.0.215 (10.2.0.215) 56(84) bytes of data.
   ^C
   --- 10.2.0.215 ping statistics ---
   6 packets transmitted, 0 received, 100% packet loss, time 4999ms
   ```

   ```
   PING 10.3.0.14 (10.3.0.14) 56(84) bytes of data.
   ^C
   --- 10.3.0.14 ping statistics ---
   3 packets transmitted, 0 received, 100% packet loss, time 1999ms
   ```

2. Verify the network connectivity between VPCs.

   ping *IP address of the ECS*

   To verify the network connectivity between vpc-isolation-01 and vpc-share, log in to ecs-isolation-01 and run the following command:

   ping 192.168.0.130

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


```
PING 192.168.0.130 (192.168.0.130) 56(84) bytes of data.
64 bytes from 192.168.0.130: icmp_seq=1 ttl=64 time=0.455 ms
64 bytes from 192.168.0.130: icmp_seq=2 ttl=64 time=0.340 ms
64 bytes from 192.168.0.130: icmp_seq=3 ttl=64 time=0.310 ms
64 bytes from 192.168.0.130: icmp_seq=4 ttl=64 time=0.232 ms
64 bytes from 192.168.0.130: icmp_seq=5 ttl=64 time=0.275 ms
^C
--- 192.168.0.130 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.275/0.578/1.131/0.345 ms
```

Step 3 Repeat **Step 1** to **Step 2** to verify isolation and connectivity between other VPCs.

----End

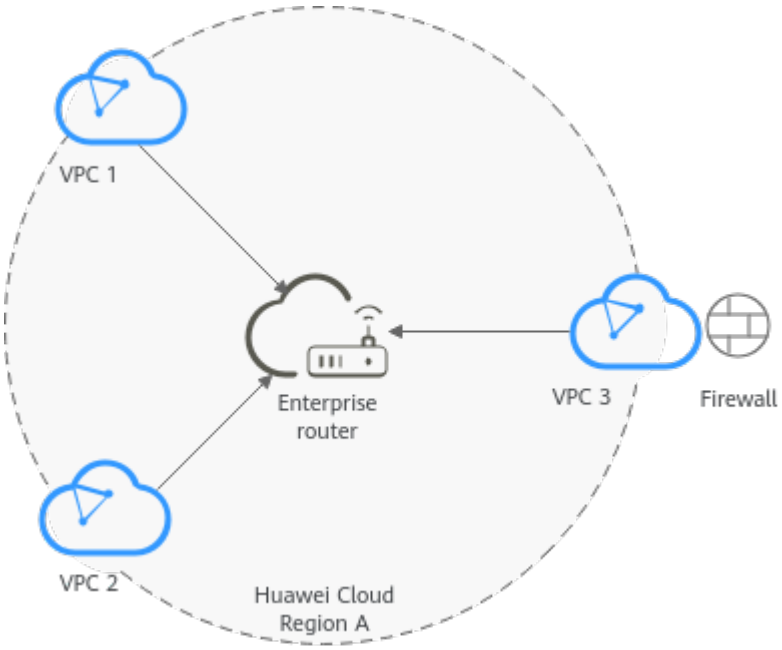
4 Using a Third-Party Firewall to Protect VPCs Connected by Enterprise Routers

4.1 Overview

Background

There are three VPCs in a region of Huawei Cloud, with service A and service B respectively in VPC 1 and VPC 2, and the third-party firewall in VPC 3. For security purposes, the traffic to service A and service B must be filtered by the firewall in VPC 3.

Figure 4-1 Traffic scrubbing for VPCs in the same region



NOTE

You can **share an enterprise router** with different accounts to attach VPCs of these accounts to the same enterprise router for communications.

Operation Procedure

Figure 4-2 shows the procedure for using an enterprise router to scrub traffic for VPCs in the same region.

Figure 4-2 Flowchart for scrubbing traffic between VPCs in the same region

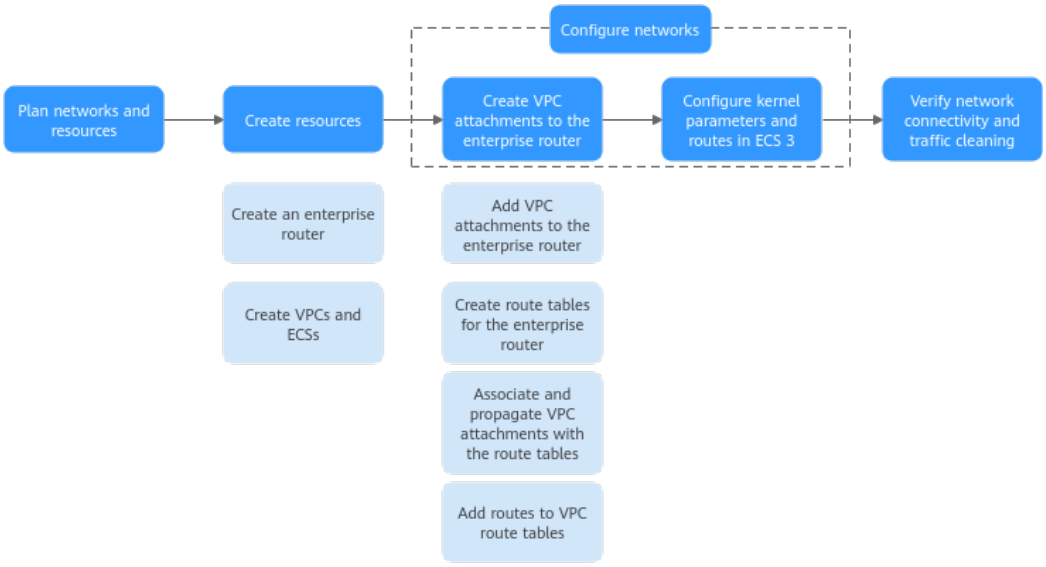


Table 4-1 Description of procedures for scrubbing traffic for VPCs in the same region

No.	Procedure	Description
1	**Planning Networks and Resources**	Plan required CIDR blocks and the number of resources.
2	**Creating Resources**	1. **Create an enterprise router**. 2. **Create three VPCs and three ECSs**.

No.	Procedure	Description
3	Configuring Networks	1. Create VPC attachments for the enterprise router: a. Attach the three VPCs to the enterprise router. b. Create two custom route tables for the enterprise router. c. Associate and propagate VPC attachments with the route tables of the enterprise router. d. Add routes to the route tables of the VPCs for traffic to route through the enterprise router. 2. Configure kernel parameters and routes for ECS 3 to allow communications between NICs eth0 and eth1.
4	Verifying Network Connectivity and Traffic Scrubbing	Log in to an ECS and run the **ping** command to verify the network connectivity.

4.2 Planning Networks and Resources

To use an enterprise router to scrub traffic for VPCs in the same region, you need:

- **Network Planning**: Plan CIDR blocks of VPCs and their subnets, and route tables of VPCs and the enterprise router.
- **Resource Planning**: Plan the quantity, names, and other parameters of cloud resources, including VPCs, ECSs, and the enterprise router.

Network Planning

Figure 4-3 and **Table 4-3** show the network planning and its description for scrubbing traffic for VPCs in the same region.

Figure 4-3 Networking planning for traffic scrubbing for VPCs in the same region

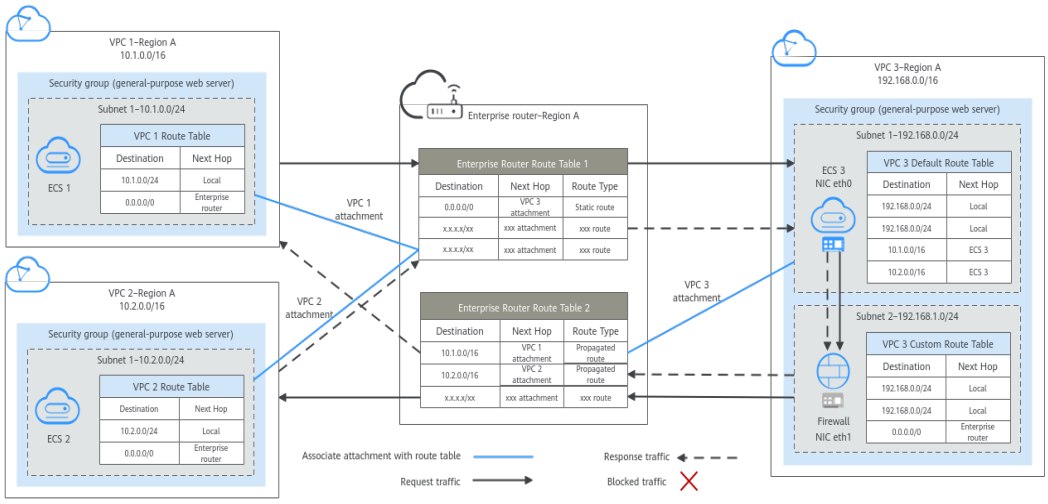


Table 4-2 Network traffic flows

Path	Description
Request traffic: from VPC 1 to VPC 2	1. The route table of VPC 1 has routes with the next hop set to the enterprise router to forward traffic from VPC 1 to the enterprise router. 2. VPC 1 is associated with the route table 1 of the enterprise router. This route table has a static route with the next hop set to the VPC 3 attachment to forward traffic from the enterprise router to VPC 3. 3. Two NICs of ECS 3 are in the two subnets of VPC 3, respectively. a. The NIC eth0 in subnet 1 receives traffic. The default route table of VPC 3 has a route with the next hop set to ECS 3 to forward traffic from eth0 to eth1. b. The NIC eth1 in subnet 2 forwards the traffic scrubbed by firewall. The custom route table of VPC 3 has routes with the next hop set to the enterprise router to forward scrubbed traffic from VPC 3 to the enterprise router. 4. VPC 3 is associated with the route table 2 of the enterprise router. This route table has a propagated route with the next hop set to the VPC 2 attachment to forward traffic from the enterprise router to VPC 2.

Path	Description
Response traffic: from VPC 2 to VPC 1	1. The route table of VPC 2 has routes with the next hop set to the enterprise router to forward traffic from VPC 2 to the enterprise router. 2. VPC 2 is associated with the route table 1 of the enterprise route. This route table has a static route with the next hop set to the VPC 3 attachment to forward traffic from the enterprise router to VPC 3. 3. Two NICs of ECS 3 are in the two subnets of VPC 3, respectively. a. The NIC eth0 in subnet 1 receives traffic. The default route table of VPC 3 has a route with the next hop set to ECS 3 to forward traffic from eth0 to eth1. b. The NIC eth1 in subnet 2 forwards the traffic scrubbed by firewall. The custom route table of VPC 3 has routes with the next hop set to the enterprise router to forward scrubbed traffic from VPC 3 to the enterprise router. 4. VPC 3 is associated with the route table 2 of the enterprise router. This route table has a propagated route with the next hop set to the VPC 1 attachment to forward traffic from the enterprise router to VPC 1.

Table 4-3 Description for traffic scrubbing for VPCs in the same region

Resource	Description
VPCs	• The traffic to VPC 1 and VPC 2 needs to be scrubbed by the firewall deployed in VPC 3. • The CIDR blocks of the VPCs to be connected cannot overlap with each other. In this example, the CIDR blocks of the VPCs are propagated to the enterprise router route table as the destination in routes. The CIDR blocks cannot be modified and overlapping CIDR blocks may cause route conflicts. If your existing VPCs have overlapping CIDR blocks, do not use propagated routes. Instead, you need to manually add static routes to the route table of the enterprise router. The destination can be VPC subnet CIDR blocks or smaller ones. • VPC 1 and VPC 2 each have a default route table. • VPC 3 has two subnets. Subnet 1 is associated with the default route table, and subnet 2 is associated with the custom route table. • The routes in the default route table are described as follows: – Local: a system route for communications between subnets in a VPC. – Enterprise router: a custom route with destination set to 0.0.0.0/0 for routing traffic from a VPC subnet to the enterprise router. For details, see **Table 4-4**. – ECS 3: a custom route for routing traffic from a VPC subnet to ECS 3. For details, see **Table 4-5**.
Enterprise router	Disable the **Default Route Table Association** and **Default Route Table Propagation**, create two route tables, attach the three VPCs to the enterprise router, and configure the route tables as follows: • Associate the VPC 1 and VPC 2 attachments with route table 1, and add a static route to route table 1 with the next hop set to the VPC 3 attachment. For details, see **Table 4-6**. • Associate the VPC 3 attachment with route table 2. Propagate VPC 1 and VPC 2 attachments to route table 2. The route table 2 automatically learns the VPC CIDR blocks as the destination of routes. For details, see **Table 4-7**.
ECS	• The three ECSs are in different VPCs. If the ECSs are in different security groups, add rules to the security groups to allow access to each other. • A third-party firewall is deployed on ECS 3. The ECS 3 has two NICs that are in the two subnets of VPC 3, respectively.

Table 4-4 Route table for VPC 1, VPC 2, and VPC 3

Destination	Next Hop	Route Type
10.0.0.0/8	Enterprise router	Static route (custom)
172.16.0.0/12	Enterprise router	Static route (custom)
192.168.0.0/16	Enterprise router	Static route (custom)

NOTE

- If you enable **Auto Add Routes** when creating a VPC attachment, you do not need to manually add static routes to the VPC route table. Instead, the system automatically adds routes (with this enterprise router as the next hop and 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations) to all route tables of the VPC.
- If an existing route in the VPC route tables has a destination to 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16, the routes will fail to be added. In this case, do not to enable **Auto Add Routes**. After the attachment is created, manually add routes.
- Do not add a route with the next hop set to the enterprise router to the default route table of VPC 3. Do not enable **Auto Add Routes** when creating the VPC 3 attachment.
- Do not set the destination of a route (with an enterprise router as the next hop) to 0.0.0.0/0 in the VPC route table. If an ECS in the VPC has an EIP bound, the VPC route table will have a policy-based route with 0.0.0.0/0 as the destination, which has a higher priority than the route with the enterprise router as the next hop. In this case, traffic is forwarded to the EIP and cannot reach the enterprise router.

Table 4-5 VPC 3 default route table

Destination	Next Hop	Route Type
10.1.0.0/16	ECS	Static route (custom)
10.2.0.0/16	ECS	Static route (custom)

Table 4-6 Enterprise router route table 1

Destination	Next Hop	Route Type
0.0.0.0/0	VPC 3 attachment: er-attach-inspection	Static route

Table 4-7 Enterprise router route table 2

Destination	Next Hop	Route Type
VPC 1 CIDR block: 10.1.0.0/16	VPC 1 attachment: er-attach-01	Propagated route

Destination	Next Hop	Route Type
VPC 2 CIDR block: 10.2.0.0/16	VPC 2 attachment: er-attach-02	Propagated route

Resource Planning

Each region has an enterprise router, VPCs, and ECSs. They can be in different AZs.

NOTE

The following resource details are only examples. You can modify them as required.

- One enterprise router. See details in **Table 4-8**.

Table 4-8 Enterprise router details

Enterprise Router Name	ASN	Default Route Table Association	Default Route Table Propagation	Route Table	Attachment
er-test-01	64512	Disabled	Disabled	Two route tables: • **er-rtb-01** • **er-rtb-02**	er-attach-01
					er-attach-02
					er-attach-inspection

Table 4-9 Enterprise router route table 1 details

Name	Associated Attachment	Static Route
er-rtb-01	er-attach-01	er-attach-inspection
	er-attach-02	

Table 4-10 Enterprise router route table 2 details

Name	Associated Attachment	Propagated Attachment
er-rtb-02	er-attach-inspection	er-attach-01
		er-attach-02

- Three VPCs that do not overlap with each other. See details in **Table 4-11**.

Table 4-11 VPC details

VPC Name	VPC CIDR Block	Subnet Name	Subnet CIDR Block	Association Route Table
vpc-demo-01	10.1.0.0/16	subnet-demo-01	10.1.0.0/24	Default route table
vpc-demo-02	10.2.0.0/16	subnet-demo-02	10.2.0.0/24	Default route table
vpc-inspection	192.168.0.0/16	subnet-inspection-01	192.168.0.0/24	Default route table
		subnet-inspection-02	192.168.1.0/24	Custom route table

- Three ECSs, respectively, in three VPCs. See details in **Table 4-12** and **Table 4-13**.

Table 4-12 ECS 1 and ECS 2 details

ECS Name	Image	VPC Name	Subnet Name	Security Group	Private IP Address
ecs-demo-01	Public image: CentOS 8.0 64-bit	vpc-demo-01	subnet-demo-01	sg-demo (general-purpose web server)	10.1.0.113
ecs-demo-02		vpc-demo-02	subnet-demo-02		10.2.0.175

Table 4-13 ECS 3 details

ECS Name	Image	NIC	VPC Name	Subnet Name	Security Group	Private IP Address
ecs-inspection	Public image: CentOS 8.0 64-bit	eth0	vpc-inspection	subnet-inspection-01	sg-demo (general-purpose web server)	192.168.0.21
		eth1		subnet-inspection-02		192.168.1.22

4.3 Creating Resources

4.3.1 Creating an Enterprise Router

Scenarios

This section describes how to create an enterprise router.

Procedure

Step 1 Create an enterprise router in region A.

For details, see **Creating an Enterprise Router**.

For enterprise router details, see **Table 4-8**.

----End

4.3.2 Creating VPCs and ECSs

Scenarios

This section describes how to create VPCs and ECSs. A third-party firewall needs to be installed on one of the ECSs.

Procedure

Step 1 Create three VPCs in region A.

For details, see **Creating a VPC**.

For details about VPC and subnet planning, see **Table 4-11**.

Step 2 Create three ECSs in region A.

For details, see **Overview**.

- For details about resource planning of ECS 1 and ECS 2, see **Table 4-12**.
- Two NICs need to be installed on ECS 3. For details about resource planning of ECS 3, see **Table 4-13**.

  After ECS 3 is created, go to the ECS 3 details page. On the **NICs** tab, disable **Source/Destination Check** for the NIC eth1 to ensure that the traffic from eth1 is not blocked.

Step 3 Install a third-party firewall on ECS 3.

----End

4.4 Configuring Networks

4.4.1 Creating VPC Attachments for the Enterprise Router

Scenarios

This section describes how to attach VPCs to the enterprise router and configure routes for the VPCs and the enterprise router.

Procedure

Step 1 Attach the three VPCs to the enterprise router.

For details, see **Creating VPC Attachments to the Enterprise Router**.

Step 2 Create two route tables for the enterprise router.

For details, see **Creating a Route Table**.

Step 3 Associate VPC attachments with route table 1 of the enterprise router, and add a static route to the route table 1 with the next hop set to the VPC attachment.

For route table 1 details, see **Table 4-9**.

1. Associate VPC 1 and VPC 2 attachments with route table 1.
   For details about creating an association, see **Creating an Association**.
2. Add a static route to route table 1 with the next hop set to the VPC 3 attachment and destination to 0.0.0.0/0.
   For details, see **Creating a Static Route**.

Step 4 Associate and propagate VPC attachments with the route table 2.

For route table 2 details, see **Table 3-9**.

1. Associate VPC 3 attachment with route table 2.
   For details about creating an association, see **Creating an Association**.
2. Propagate VPC 1 and VPC 2 attachments to route table 2.
   For details about creating a propagation, see **Creating a Propagation**.

Step 5 Add routes to the route tables of the VPCs.

For details, see **Adding Routes to VPC Route Tables**.

1. Add routes for traffic to route from the VPCs to the enterprise router.
   For details, see **Table 4-4**.
2. Add a route to default route table of VPC 3 for traffic to route from the VPC 3 to the ECS.
   For details, see **Table 4-5**.

----End

4.4.2 Configuring Kernel Parameters and Routes for ECS 3

Scenarios

ECS 3 has two NICs, eth0 and eth1. You need to configure kernel parameters and add routes for ECS 3 to allow communications between eth0 and eth1.

NOTICE

ECS 3 runs CentOS 8.0 64-bit. The configuration commands may vary by the OS.

Procedure

Step 1 Log in to the ECS.

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 2 Disable the verification on the source address of the data packet:

1. Run the following command to open the **/etc/sysctl.conf** file:

   vim /etc/sysctl.conf
2. Press **i** to enter the editing mode.
3. Add the following content to the end of the file:

   ```
   net.ipv4.conf.default.rp_filter = 0
   net.ipv4.conf.all.rp_filter = 0
   ```
4. Press **Esc** to exit and enter **:wq!** to save the configuration.
5. Run the following command for the configuration to take effect:

   sysctl -p
6. Run the following command to check whether verifying data packet source address is disabled:

   sysctl -a | grep rp_filter

   If the value of **net.ipv4.conf.all.rp_filter** and **net.ipv4.conf.default.rp_filter** is **0**, verifying data packet source address is disabled.

   ```
   [root@ecs-inspection ~]# sysctl -a | grep rp_filter
   net.ipv4.conf.all.arp_filter = 0
   net.ipv4.conf.all.rp_filter = 0
   net.ipv4.conf.default.arp_filter = 0
   net.ipv4.conf.default.rp_filter = 0
   net.ipv4.conf.eth0.arp_filter = 0
   net.ipv4.conf.eth0.rp_filter = 0
   net.ipv4.conf.eth1.arp_filter = 0
   net.ipv4.conf.eth1.rp_filter = 0
   net.ipv4.conf.lo.arp_filter = 0
   net.ipv4.conf.lo.rp_filter = 0
   ```

Step 3 Enable the forwarding function.

1. Run the following command to open the **/etc/sysctl.conf** file:

   vim /etc/sysctl.conf
2. Press **i** to enter the editing mode.
3. Add the following content to the end of the file:

   ```
   net.ipv4.ip_forward = 1
   ```
4. Press **Esc** to exit and enter **:wq!** to save the configuration.
5. Run the following command for the configuration to take effect:

sysctl -p

6. Run the following command to verify that the forwarding function is enabled.

   sysctl -a | grep ip_forward

   If the value of **net.ipv4.ip_forward** is **1**, the forwarding function is enabled.

```
[root@ecs-inspection ~]# sysctl -a | grep ip_forward
net.ipv4.ip_forward = 1
net.ipv4.ip_forward_update_priority = 1
net.ipv4.ip_forward_use_pmtu = 0
```

Step 4 Add routes.

The routes are for forwarding scrubbed traffic from eth1 to VPC 1 and VPC 2.

To add routes for ECSs running CentOS 8.0 or CentOS 7.4, perform the following:

- CentOS 8.0:
  a. Run the following command to open the NIC configuration file:

     vi /etc/sysconfig/network-scripts/route-eth1

  b. Press **i** to enter the editing mode.
  c. Add the following content to the end of the file:

```
10.1.0.0/16 via 192.168.1.1
10.2.0.0/16 via 192.168.1.1
```

     10.1.0.0/16 is the CIDR block of VPC 1, 10.2.0.0/16 is that of VPC 2, and 192.168.1.1 is the gateway address of eth1.
  d. Press **Esc** to exit and enter **:wq!** to save the configuration.
  e. Restart ECS 3 for the routes to take effect.
  f. After the restart is complete, run the following command to verify that the routes are added successfully:

     route -n

     If information similar to the following is displayed, the two routes have been added.

```
[root@ecs-inspection ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.0.1     0.0.0.0         UG    100    0        0 eth0
10.1.0.0        192.168.1.1     255.255.0.0     UG    0      0        0 eth1
10.2.0.0        192.168.1.1     255.255.0.0     UG    0      0        0 eth1
169.254.169.254 192.168.0.254   255.255.255.255 UGH   100    0        0 eth0
192.168.0.0     0.0.0.0         255.255.255.0   U     100    0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     101    0        0 eth1
```

- CentOS 7.4:
  a. Run the following command to open the NIC configuration file:

     vi /etc/sysconfig/static-routes

  b. Press **i** to enter the editing mode.
  c. Add the following content to the end of the file:

```
any net 10.1.0.0/16 gw 192.168.1.1
any net 10.2.0.0/16 gw 192.168.1.1
```

     10.1.0.0/16 is the CIDR block of VPC 1, 10.2.0.0/16 is that of VPC 2, and 192.168.1.1 is the gateway address of eth1.
  d. Press **Esc** to exit and enter **:wq!** to save the configuration.
  e. Run the following command to restart the network service for the configuration to take effect:

service network restart

f. After the restart is complete, run the following command to verify that the routes are added successfully:

route -n

If information similar to the following is displayed, the two routes have been added.

```
[root@ecs-inspection ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.0.1     0.0.0.0         UG    100    0        0 eth0
10.1.0.0        192.168.1.1     255.255.0.0     UG    0      0        0 eth1
10.2.0.0        192.168.1.1     255.255.0.0     UG    0      0        0 eth1
169.254.169.254 192.168.0.254   255.255.255.255 UGH   100    0        0 eth0
192.168.0.0     0.0.0.0         255.255.255.0   U     100    0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     101    0        0 eth1
```

----End

4.5 Verifying Network Connectivity and Traffic Scrubbing

Scenarios

This section describes how to log in to ECSs and verify the connectivity between VPCs.

Procedure

Step 1 Log in to the ECS.

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 2 Verify the network connectivity between VPCs.

1. The command is in the following format:

   ping *IP address of the ECS*

   To verify the network connectivity between vpc-demo-01 and vpc-demo-02, log in to ecs-demo-01 and run the following command:

   ping 10.2.0.175

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

```
[root@ecs-demo-01 ~]# ping 10.2.0.175
PING 10.2.0.175 (10.2.0.175) 56(84) bytes of data.
64 bytes from 10.2.0.175: icmp_seq=1 ttl=63 time=1.78 ms
64 bytes from 10.2.0.175: icmp_seq=2 ttl=63 time=1.03 ms
64 bytes from 10.2.0.175: icmp_seq=3 ttl=63 time=0.951 ms
64 bytes from 10.2.0.175: icmp_seq=4 ttl=63 time=0.963 ms
64 bytes from 10.2.0.175: icmp_seq=5 ttl=63 time=0.965 ms
64 bytes from 10.2.0.175: icmp_seq=6 ttl=63 time=0.943 ms
^C
--- 10.2.0.175 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 12ms
rtt min/avg/max/mdev = 0.943/1.105/1.784/0.307 ms
```


2. Keep the network connectivity between vpc-demo-01 and vpc-demo-02 in **Step 2.1** and log in to ecs-inspection to verify whether the traffic from vpc-demo-01 to vpc-demo-02 flows through ecs-inspection.

   a. Run the following command at least twice consecutively to check whether the value of RX packets increases:

      ifconfig eth0

   b. Run the following command at least twice consecutively to check whether the value of TX packets increases:

      ifconfig eth1

   If the values increase, the traffic flows through ecs-inspection:

```
[                ~]#ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.21  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::34c8:d0f7:a82f:ceb7  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:5a:ea:be  txqueuelen 1000  (Ethernet)
        RX packets 520241  bytes 50982241 (48.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 422285  bytes 41557376 (39.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[                 ~]#ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.21  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::34c8:d0f7:a82f:ceb7  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:5a:ea:be  txqueuelen 1000  (Ethernet)
        RX packets 520267  bytes 50984789 (48.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 422285  bytes 41557376 (39.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[                 ~]#ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.22  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::dd1f:e122:7899:5611  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:db:2d:b2  txqueuelen 1000  (Ethernet)
        RX packets 379  bytes 21854 (21.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 98891  bytes 9670654 (9.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[                 ]#ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.22  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::dd1f:e122:7899:5611  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:db:2d:b2  txqueuelen 1000  (Ethernet)
        RX packets 380  bytes 21910 (21.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 98924  bytes 9673832 (9.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 3 Repeat **Step 1** to **Step 2** to log in to ecs-demo-02 and verify whether the traffic from vpc-demo-02 to vpc-demo-01 flows through ecs-inspection.

----End

5 Using an Enterprise Router and a Transit VPC to Enable an On-Premises Data Center to Access Service VPCs

5.1 Overview

Scenario

You can use enterprise routers to build a central network and to simplify the network architecture. There are two typical networking schemes. One is to attach the service VPCs to the enterprise router. The other is to use a transit VPC to build a network, together with VPC Peering and Enterprise Router. Compared with scheme 1, scheme 2 costs less and eliminates some restrictions, as detailed below:

- Scheme 2 uses less traffic and fewer attachments.
  - Traffic between service VPCs is routed through VPC peering connections instead of enterprise routers, reducing traffic costs.
  - Only the transit VPC is attached to the enterprise router. You can pay less for the attachments.
- Scheme 2 frees you from the following constraints that scheme 1 has on attaching service VPCs to an enterprise router:
  - If a service VPC is used by ELB, VPC Endpoint, NAT Gateway (private NAT gateways), or DCS, **submit a service ticket** to confirm the service compatibility and preferentially use a transit VPC for networking.

    If you attach a service VPC to an enterprise router when Elastic Load Balance (ELB), VPC Endpoint, or DCS is being used together with Enterprise Router, persistent connections may be intermittently interrupted during service reliability assurance, such as a DR switchover, an upgrade, or elastic scaling. Ensure that the clients are capable of automatic reconnection in case of intermittent disconnection.
  - Traffic cannot be forwarded from a VPC to the enterprise router if you set the destination of a route in the VPC route table to 0.0.0.0/0 and:

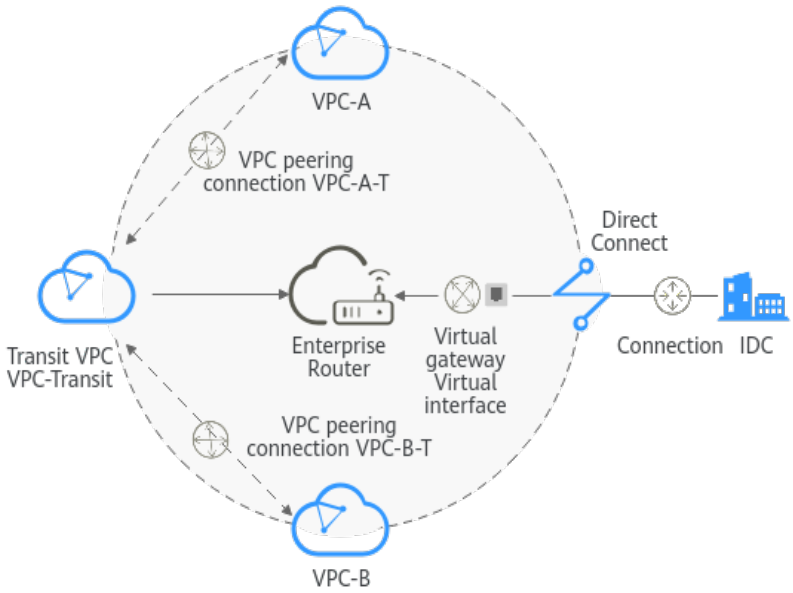
  - An ECS in the VPC has an EIP bound.
  - The VPC is being used by the ELB (either dedicated or shared load balancers), NAT Gateway, VPCEP, and DCS services.
- If a VPC attached to an enterprise router has a NAT gateway associated and **Scenario** of the SNAT or DNAT rules is set to **Direct Connect/Cloud Connect**, the network from the on-premises data center to the VPC is disconnected.

Architecture

In scheme 2, service VPCs communicate with each other over VPC peering connections and with the on-premises data center using an enterprise router. **Figure 5-1** shows the networking architecture.

1. Create a VPC peering connection between VPC-A and VPC-Transit, and between VPC-B and VPC-Transit. Traffic between VPC-A and VPC-B is forwarded through VPC-Transit and the two VPC peering connections.
2. VPC-Transit is connected to the enterprise router. Traffic from VPC-A and VPC-B to the on-premises data center is forwarded to the enterprise router through the transit VPC, and then to the on-premises data center over the Direct Connect connection.

Figure 5-1 Networking for allowing an on-premises data center to access two service VPCs over a transit VPC (scheme 2)



5.2 Planning Networks and Resources

To use Enterprise Router and a transit VPC to build a central network and allow an on-premises data center to access the VPCs over Direct Connect, you need:

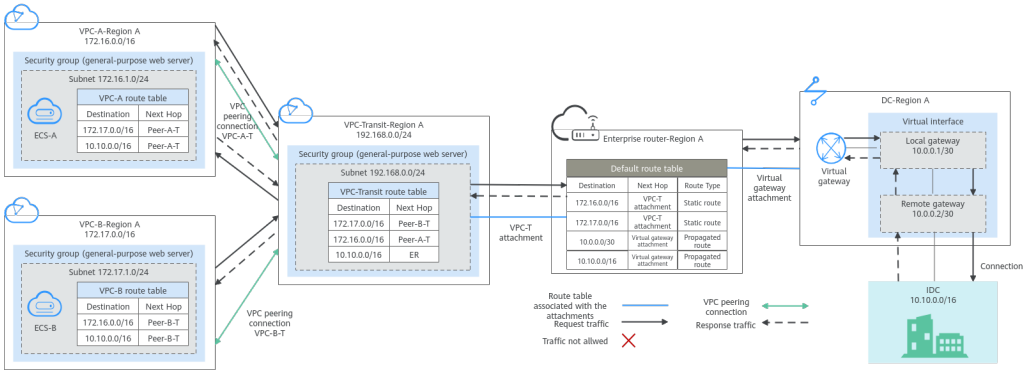
- **Network Planning**: Plan CIDR blocks of VPCs and their subnets, Direct Connect connection, and enterprise router, as well as the routes of these resources.

- **Resource Planning**: Plan the quantity, names, and settings of cloud resources, including VPCs, VPC peering connections, Direct Connect resources, and enterprise router.

Network Planning

Figure 5-2 shows the networking of allowing an on-premises data center to access the cloud by using an enterprise router, a transit VPC, and a Direct Connect connection. The VPCs communicate with each other over VPC peering connections. (**Table 5-2** describes the resources for the networking.)

Figure 5-2 Networking with an enterprise router and a transit VPC



In this networking scheme, the service VPCs are connected over VPC Peering, and the on-premises data center accesses the services VPCs over Direct Connect and Enterprise Router.

- A VPC peering connection connects each service VPC to the transit VPC, so that the service VPCs can communicate with each other. For details, see Path 1 in **Table 5-1**.
- The on-premises data center accesses the service VPCs over a Direct Connect connection and an enterprise router. For details, see Path 2 in **Table 5-1**.

Table 5-1 Network traffic flows

No.	Path	Description
Path 1	Request traffic: from VPC-A to the on-premises data center	1. In the route table of VPC-A, there is a route with the next hop set to Peer-A-T to forward the traffic to VPC-Transit. 2. In the route table of VPC-Transit, there is a route with the next hop set to the enterprise router to forward traffic from VPC-Transit to the enterprise router. 3. In the route table of the enterprise router, there is a route with the next hop set to the virtual gateway attachment to forward traffic from the enterprise router to the virtual gateway. 4. The virtual gateway is associated with the virtual interface. Traffic from the virtual gateway is forwarded to the Direct Connect connection through the remote gateway of the virtual interface. 5. Traffic is sent to the on-premises data center over the Direct Connect connection.
	Response traffic: from the on-premises data center to VPC-A	1. Traffic is forwarded to the virtual interface over the Direct Connect connection. 2. The virtual interface is connected to the virtual gateway. Traffic from the virtual interface is forwarded to the virtual gateway through the local gateway of the virtual interface. 3. Traffic is forwarded from the virtual gateway attachment to the enterprise router. 4. In the route table of the enterprise router, there is a route with the next hop set to peering connection attachment VPC-T to forward the traffic to VPC-Transit. 5. In the route table of VPC-Transit, there is a route with the next hop set to Peer-A-T to forward the traffic to VPC-A.
Path 2	Request traffic: from VPC-B to VPC-A	1. In the route table of VPC-B, there is a route with the next hop set to Peer-B-T to forward the traffic to VPC-Transit. 2. In the route table of VPC-Transit, there is a route with the next hop set to Peer-A-T to forward the traffic to VPC-A.

No.	Path	Description
	Response traffic: from VPC-A to VPC-B	1. In the route table of VPC-A, there is a route with the next hop set to Peer-A-T to forward the traffic to VPC-Transit. 2. In the route table of VPC-Transit, there is a route with the next hop set to Peer-B-T to forward the traffic to VPC-B.

Table 5-2 Networking with an enterprise router and a transit VPC

Cloud Service	Description
VPC	Two service VPCs are required to run your workloads. In this example, the two VPCs are VPC-A and VPC-B. • The CIDR block of each service VPC cannot be the same as the CIDR block of the on-premises network. • The CIDR blocks of VPC subnets connected over a VPC peering connection cannot overlap. In this example, the subnet CIDR blocks of VPC-A, VPC-B, and VPC-Transit must be different. • Each VPC has a default route table. • The routes in the default route tables are described as follows: – VPC-A: The traffic is forwarded from VPC-A to VPC-Transit over the VPC peering connection Peer-A-T. Two routes are required, and the destination of one route is the CIDR block of VPC-B and that of the other route is the CIDR block of the on-premises network. For details, see **Table 5-3**. – VPC-B: The traffic is forwarded from VPC-B to VPC-Transit over the VPC peering connection Peer-B-T. Two routes are required, and the destination of one route is the CIDR block of VPC-A and that of the other route is the CIDR block of the on-premises network. For details, see **Table 5-3**.

Cloud Service	Description
	One transit VPC, which will be attached to the enterprise router. In this example, the transit VPC is VPC-Transit. ● A transit VPC is used to forward traffic between service VPCs and between each service VPC and the on-premises data center. No workloads are running in this VPC. ● The CIDR block of the transit VPC cannot be the same as the CIDR block of the on-premises network. ● The CIDR blocks of VPC subnets connected over a VPC peering connection cannot overlap. In this example, the subnet CIDR blocks of VPC-A, VPC-B, and VPC-Transit must be different. ● The VPC has a default route table. ● The routes in the default route table of the VPC are described as follows: – Two routes are required with the next hop set to each VPC peering connection (Peer-A-T and Peer-B-T) and destination set to the CIDR block of each service VPC to forward the traffic between VPC-A and VPC-B. – One route is required with the next hop set to the enterprise router and destination set to the CIDR block of the on-premises network to forward the traffic from VPC-A and VPC-B to the virtual gateway and then to the on-premises data center.
Direct Connect	● One connection links your on-premises data center to the cloud. ● One virtual gateway is attached to the enterprise router. ● One virtual interface connects the virtual gateway with the connection.

Cloud Service	Description
Enterprise Router	Add attachments to the enterprise router and configure the required routes. • VPC – Associate the transit VPC with the default route table of the enterprise router. You need to manually add routes to the default route table of the enterprise router because **Auto Add Routes** is not enabled. – Manually add static routes to the default route table of the enterprise router because **Default Route Table Propagation** is not enabled. For details about the route, see **Table 5-4**. • Direct Connect – Associate the virtual gateway attachment with the default route table of the enterprise router. – Propagate the virtual gateway attachment to the default route table of the enterprise router. The route table automatically learns the route information of the virtual gateway attachment. For details, see **Table 5-4**.
ECS	There is an ECS in each service VPC. In this example, the two ECSs are used to verify network connectivity between service VPCs and between service VPCs and the on-premises data center. If you have multiple ECSs associated with different security groups, you need to add rules to the security groups to allow network access.

Table 5-3 VPC route table

VPC	Destination	Next Hop	Route Type
VPC-A	172.17.0.0/16	VPC peering connection: Peer-A-T	Static route (custom)
	10.10.0.0/16	VPC peering connection: Peer-A-T	Static route (custom)
VPC-B	172.16.0.0/16	VPC peering connection: Peer-B-T	Static route (custom)
	10.10.0.0/16	VPC peering connection: Peer-B-T	Static route (custom)

VPC	Destination	Next Hop	Route Type
VPC-Transit	172.17.0.0/16	VPC peering connection: Peer-B-T	Static route (custom)
	172.16.0.0/16	VPC peering connection: Peer-A-T	Static route (custom)
	10.10.0.0/16	Enterprise router	Static route (custom)

NOTICE

When attaching a VPC to an enterprise router, do not enable **Auto Add Routes**. You need to manually add routes in the route table of VPC-Transit.

Table 5-4 Enterprise router route table

Destination	Next Hop	Route Type
VPC-A CIDR block: 172.16.0.0/16	VPC-Transit attachment: er-attach-VPCtransit	Static route
VPC-B CIDR block: 172.17.0.0/16	VPC-Transit attachment: er-attach-VPCtransit	Static route
Local and remote gateways: 10.0.0.0/30	Virtual gateway attachment: vgw-demo	Propagated route
CIDR block of the on-premises network: 10.10.0.0/16	Virtual gateway attachment: vgw-demo	Propagated route

Resource Planning

An enterprise router, a Direct Connect connection, VPCs, and ECSs are in the same region but can be in different AZs.

NOTE

The following resource details are only examples. You can modify them as required.

Table 5-5 Resource details

Resource	Description
VPC	Three VPCs are required. **Table 5-6** describes the three VPCs and their settings. • Service VPCs: Two VPCs are used to run workloads. Each service VPC is connected to the transit VPC over a VPC peering connection and is not attached to the enterprise router. • Transit VPC: One transit VPC is attached to the enterprise router and used to forward traffic between service VPCs and between each service VPC and the on-premises data center. No workloads are running in this VPC. **NOTICE** • The CIDR block of each service VPC and that of the transit VPC cannot be the same as the CIDR block of the on-premises network. • The CIDR block of each service VPC and that of the transit VPC cannot overlap. • The transit VPC is attached to the enterprise router. There are some **constraints** on attaching a VPC to an enterprise router.
VPC peering connection	Two VPC peering connections are required to connect VPC-A, VPC-B, and VPC-Transit. **Table 5-7** describes the two VPC peering connections and their settings.
Direct Connect connection	A connection, a virtual gateway, and a virtual interface are required. **Table 5-8** describes the required Direct Connect resources and their settings.
Enterprise router	An enterprise router is required and two network instances will be attached to the enterprise router. **Table 5-9** describes the enterprise router and its settings.
ECS	Two ECSs are required, with each in a service VPC. **Table 5-10** describes the two ECSs and their settings.

Table 5-6 VPC details

VPC	VPC CIDR Block	Subnet	Subnet CIDR Block	Association Route Table	VPC Description
VPC-A	172.16.0.0/16	subnet-A01	172.16.1.0/24	Default route table	Service VPC, not connected to the enterprise router

VPC	VPC CIDR Block	Subnet	Subnet CIDR Block	Association Route Table	VPC Description
VPC-B	172.17.0.0/16	subnet-B01	172.17.1.0/24	Default route table	Service VPC, not connected to the enterprise router
VPC-Transit	192.168.0.0/24	subnet-Transit	192.168.0.0/24	Default route table	Transit VPC, connected to the enterprise router

Table 5-7 VPC peering connection details

VPC Peering Connection	Local VPC	Peer VPC	Description
Peer-A-T	VPC-A	VPC-Transit	Connects VPC-A and VPC-Transit.
Peer-B-T	VPC-B	VPC-Transit	Connects VPC-B and VPC-Transit.

Table 5-8 Direct Connect resource details

Resource	Example Settings
Connection	Create a connection based on site requirements.
Virtual gateway	• **Name**: **vgw-demo** • **Attach To**: enterprise router • **BGP ASN**: The ASN is the same as or different from that of the enterprise router. In this example, retain the default value 64512.

Resource	Example Settings
Virtual interface	• **Name**: **vif-demo** • **Virtual Gateway**: **vgw-demo** • **Local Gateway**: 10.0.0.1/30 • **Remote Gateway**: 10.0.0.2/30 • **Remote Subnet**: 10.10.0.0/16 • **Routing Mode**: BGP • **BGP ASN**: ASN of the on-premises data center, which must be different from the ASN of the virtual gateway on the cloud. In this example, 65525 is used.

Table 5-9 Enterprise router details

Resource	Example Settings
Enterprise router	• **Name**: **er-demo** • **ASN**: 64512 • **Default Route Table Association**: Enable • **Default Route Table Propagation**: Disable You need to manually add a route for the VPC attachment in the route table of the enterprise router. There is no need to enable this option. • **Auto Accept Shared Attachments**: Enable If you want to connect VPCs of different accounts using an enterprise router, enable this function. For details, see **Sharing Overview**. • Association/Propagation route table: default route table • Attachments: – er-attach-VPCtransit – er-attach-VGW

Resource	Example Settings
Attachments	• Attachment name: **er-attach-VPCtransit** – Attachment type: VPC attachment – VPC: VPC-Transit – Subnet: subnet-Transit – **Auto Add Routes**: There is no need to enable this option. If this option is enabled, Enterprise Router automatically adds routes (with this enterprise router as the next hop and 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations) to all route tables of the VPC. In this example, the CIDR block of each service VPC needs to be added as the route destination. • Attachment name: **er-attach-VGW** – Attachment type: virtual gateway attachment – Virtual gateway: vgw-demo

Table 5-10 ECS details

ECS	VPC	Subnet	Private IP Address	Image	Security Group	ECS Description
ECS-A	VPC-A	subnet-A01	172.16.1.25	Public image: CentOS 8.2 64bit	sg-demo (general-purpose web server)	This ECS is used to run workloads.
ECS-B	VPC-B	subnet-B01	172.17.1.113			This ECS is used to run workloads.

5.3 Enabling Communications Between an On-Premises Data Center and Service VPCs

Table 5-11 describes the overall process of building a network using an enterprise router and a transit VPC to allow an on-premises data center to access the cloud over a Direct Connect connection.

Table 5-11 Process of allowing an on-premises data center to access service VPCs using an enterprise router, a transit VPC, and a Direct Connect connection

Procedure	Detailed Steps
Step 1: Create Cloud Resources	1. Create an enterprise router for connecting VPCs in the same region. 2. Create VPCs and subnets. In this example, create two service VPCs and one transit VPC. 3. Create an ECS in each service VPC.
Step 2: Create VPC Peering Connections and Configure Routes	1. Create a VPC peering connection between VPC-A and VPC-Transit, and add routes for this VPC peering connection. 2. Create a VPC peering connection between VPC-B and VPC-Transit, and add routes for this VPC peering connection. 3. Verify the connectivity between VPC-A and VPC-B.
Step 3: Create a VPC Attachment to the Enterprise Router	1. Attach the transit VPC to the enterprise router. 2. Add routes in the route table of VPC-Transit with the enterprise router as the next hop and the on-premises CIDR block as the destination. 3. Add a route in the route table of the enterprise router with the VPC attachment as the next hop and the on-premises CIDR block as the destination.
Step 4: Create a Virtual Gateway Attachment to the Enterprise Router	1. Create a Direct Connect connection to connect the on-premises data center to the cloud over a line you lease from a carrier. 2. Create a virtual gateway and attach it to the enterprise router. 3. Create a propagation for the virtual gateway attachment in the route table of the enterprise router to automatically learn the routes of the on-premises data center. 4. Create a virtual interface to associate the virtual gateway with the Direct Connect connection. 5. Configure routes on the router in the on-premises data center.
Step 5: Verify Network Connectivity Between the Service VPCs and On-Premises Data Center	Log in to an ECS and run the **ping** command to verify the network connectivity.

5.4 Procedure for Enabling Communications Between an On-Premises Data Center and Service VPCs

Step 1: Create Cloud Resources

Create an enterprise router, two service VPCs, a transit VPC, and two ECSs. For details about these resources, see **Table 5-5**.

Step 1 Create an enterprise router.

Disable **Default Route Table Propagation** when you create the enterprise router. For details, see **Table 5-9**.

For details, see **Creating an Enterprise Router**.

Step 2 Create two service VPCs and a transit VPC.

For details, see **Creating a VPC**.

Step 3 Create two ECSs.

In this example, ECSs are used to verify network connectivity. The quantity and configuration are for reference only.

For details, see **Overview**.

----End

Step 2: Create VPC Peering Connections and Configure Routes

Step 1 Create a VPC peering connection between each service VPC and the transit VPC.

1. Create VPC peering connection Peer-A-T to connect VPC-A and VPC-Transit.
2. Create VPC peering connection Peer-B-T to connect VPC-B and VPC-Transit.

For details about the VPC peering connections, see **Table 5-7**.

- If the service VPC and transit VPC are in the same account, create a VPC peering connection by following the instructions provided in **Creating a VPC Peering Connection with Another VPC in Your Account**.
- If the service VPC and transit VPC are in different accounts, create a VPC peering connection by following the instructions provided in **Creating a VPC Peering Connection with a VPC in Another Account**

Step 2 In the route tables of VPC-A, VPC-B, and VPC-Transit, add routes with the next hop being the corresponding VPC peering connection.

For details, see **Adding Routes to VPC Route Tables**.

In this example, add the routes in **Table 5-3**, and the next hop is the corresponding VPC peering connection.

- Add two routes in the route table of VPC-A with destination set to 172.17.0.0/16 and 10.10.0.0/16.

- Add two routes in the route table of VPC-B with destination set to 172.16.0.0/16 and 10.10.0.0/16.
- Add two routes to the route table of VPC-Transit with destination set to 172.17.0.0/16 and 172.16.0.0/16.

Step 3 Verify network connectivity between VPC-A and VPC-B.

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 the ECSs.

1. Log in to ECS-A and verify that VPC-A and VPC-B can communicate with each other over the VPC peering connections.

   ping *Private IP address of ECS-B*

   Example command:

   ping 172.17.1.113

   If information similar to the following is displayed, the communications between VPC-A and VPC-B are normal:

   ```
   [root@ECS-A ~]# ping 172.17.1.113
   PING 172.17.1.113 (172.17.1.113) 56(84) bytes of data.
   64 bytes from 172.17.1.113: icmp_seq=1 ttl=64 time=0.849 ms
   64 bytes from 172.17.1.113: icmp_seq=2 ttl=64 time=0.455 ms
   64 bytes from 172.17.1.113: icmp_seq=3 ttl=64 time=0.385 ms
   64 bytes from 172.17.1.113: icmp_seq=4 ttl=64 time=0.372 ms
   ...
   --- 172.17.1.113 ping statistics ---
   ```

2. Log in to ECS-B and verify that VPC-B can communicate with VPC-A over the VPC peering connections.

   ping *Private IP address of ECS-A*

   Example command:

   ping 172.16.1.25

   If information similar to the following is displayed, the communications between VPC-B and VPC-A are normal:

   ```
   [root@ECS-B ~]# ping 172.16.1.25
   PING 172.16.1.25 (172.16.1.25) 56(84) bytes of data.
   64 bytes from 172.16.1.25: icmp_seq=1 ttl=64 time=0.849 ms
   64 bytes from 172.16.1.25: icmp_seq=2 ttl=64 time=0.455 ms
   64 bytes from 172.16.1.25: icmp_seq=3 ttl=64 time=0.385 ms
   64 bytes from 172.16.1.25: icmp_seq=4 ttl=64 time=0.372 ms
   ...
   --- 172.16.1.25 ping statistics ---
   ```

----End

Step 3: Create a VPC Attachment to the Enterprise Router

Step 1 Attach the transit VPC to the enterprise router.

Do not enable **Auto Add Routes** when creating the attachment. For more resource details, see **Table 5-9**.

NOTICE

If this option is enabled, Enterprise Router automatically adds routes (with this enterprise router as the next hop and 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations) to all route tables of the VPC. In this example, the CIDR block of each service VPC needs to be added as the route destination.

For details, see **Creating VPC Attachments to the Enterprise Router**.

Step 2 In the route table of the transit VPC, add a route with the next hop as the enterprise router.

For details, see **Adding Routes to VPC Route Tables**.

In this example, add a route in the route table of VPC-Transit, with the next hop as the enterprise router and destination as 10.10.0.0/16.

Step 3 In the route table of the enterprise router, add static routes with the next hop as the VPC attachment.

For details, see **Creating a Static Route**.

In this example, add routes in the route table of the enterprise router, with the next hop as the VPC-Transit attachment. The destination of one route is 172.16.0.0/16, and that of the other is 172.17.0.0/16. For details, see **Table 5-4**.

----End

Step 4: Create a Virtual Gateway Attachment to the Enterprise Router

For details about Direct Connect resources, see **Table 5-8**.

Step 1 Create a connection.

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

Step 2 Create a virtual gateway and attach it to the enterprise router.

1. On the Direct Connect console, create a virtual gateway.

   For details, see **Step 2: Create a Virtual Gateway**.

2. On the Enterprise Router console, check whether the virtual gateway attachment has been added to the enterprise router.

   For details, see **Viewing Details About an Attachment**.

   If the status of the virtual gateway attachment is **Normal**, the attachment has been added.

   In this example, **Default Route Table Association** was enabled but **Default Route Table Propagation** was disabled during the creation of the enterprise router. After the virtual gateway attachment is added:

   - An association is automatically created in the default route table of the enterprise router.
   - You need to manually create a propagation to proceed to **Step 3**.

Step 3 In the route table of the enterprise router, create a propagation for the virtual gateway attachment to automatically learn the routes of the on-premises data center.

For details about creating a propagation, see **Creating a Propagation**.

You can view routes to the on-premises data center in the route table of the enterprise router only after performing the following steps.

Step 4 Create a virtual interface.

Create a virtual interface to connect the virtual gateway with the on-premises data center. For details, see **Step 3: Create a Virtual Interface**.

Step 5 Configure routes on the on-premises network device to point to Huawei Cloud.

The following uses Huawei network devices as an example to describe how to configure a BGP route.

bgp *65525*

peer *10.0.0.1* **as-number 64512**

peer *10.0.0.1* **password simple** *12345678*

network *10.10.0.0 255.255.0.0*

Table 5-12 BGP route

Command	Description
bgp *65525*	Enable BGP. 65525 is the ASN used by the on-premises data center.
peer *10.0.0.1* **as-number 64512**	Create a BGP peer. • 10.0.0.1 is the gateway on Huawei Cloud. • 64512 is the ASN used by Huawei Cloud. The value must be 64512.
peer *10.0.0.1* **password simple** *12345678*	Perform MD5 authentication on BGP messages when a TCP connection is established between BGP peers. 12345678 is the BGP MD5 authentication password.
network *10.10.0.0 255.255.0.0*	Add routes in the IP route table to the BGP route table. • 10.10.0.0 is the network used by the on-premises data center. • 255.255.0.0 is the subnet mask of the on-premises network.

----End

Step 5: Verify Network Connectivity Between the Service VPCs and On-Premises Data Center

Step 1 Log in to the ECSs and verify the communications between each service VPC and the on-premises data center.

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 the ECSs.

1. Log in to ECS-A and run the following command to check whether VPC-A can communicate with the on-premises data center through the enterprise router:

   ping *IP address of the on-premises data center*

   Example command:

   ping 10.10.0.27

   If information similar to the following is displayed, VPC-A can communicate with the on-premises data center through the enterprise router.

   ```
   [root@ECS-A ~]# ping 10.10.0.27
   PING 10.10.0.27 (10.10.0.27) 56(84) bytes of data.
   64 bytes from 10.10.0.27: icmp_seq=1 ttl=64 time=0.849 ms
   64 bytes from 10.10.0.27: icmp_seq=2 ttl=64 time=0.455 ms
   64 bytes from 10.10.0.27: icmp_seq=3 ttl=64 time=0.385 ms
   64 bytes from 10.10.0.27: icmp_seq=4 ttl=64 time=0.372 ms
   ...
   --- 10.10.0.27 ping statistics ---
   ```

2. Log in to ECS-B and run the following command to check whether VPC-B can communicate with the on-premises data center through the enterprise router:

   ping *IP address of the on-premises data center*

   Example command:

   ping 10.10.0.30

   If information similar to the following is displayed, VPC-B can communicate with the on-premises data center through the enterprise router.

   ```
   [root@ECS-B ~]# ping 10.10.0.30
   PING 10.10.0.30 (10.10.0.30) 56(84) bytes of data.
   64 bytes from 10.10.0.30: icmp_seq=1 ttl=64 time=0.849 ms
   64 bytes from 10.10.0.30: icmp_seq=2 ttl=64 time=0.455 ms
   64 bytes from 10.10.0.30: icmp_seq=3 ttl=64 time=0.385 ms
   64 bytes from 10.10.0.30: icmp_seq=4 ttl=64 time=0.372 ms
   ...
   --- 10.10.0.30 ping statistics ---
   ```

Step 2 Log in to the ECSs and verify the communications between service VPCs.

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 the ECSs.

1. Log in to ECS-A and verify that VPC-A and VPC-B can communicate with each other over the VPC peering connections.

   ping *Private IP address of ECS-B*

   Example command:

   ping 172.17.1.113

If information similar to the following is displayed, the communications between VPC-A and VPC-B are normal:

```
[root@ECS-A ~]# ping 172.17.1.113
PING 172.17.1.113 (172.17.1.113) 56(84) bytes of data.
64 bytes from 172.17.1.113: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.17.1.113: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.17.1.113: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.17.1.113: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.17.1.113 ping statistics ---
```

2. Log in to ECS-B and verify that VPC-B can communicate with VPC-A over the VPC peering connections.

   ping *Private IP address of ECS-A*

   Example command:

   ping 172.16.1.25

   If information similar to the following is displayed, the communications between VPC-B and VPC-A are normal:

```
[root@ECS-B ~]# ping 172.16.1.25
PING 172.16.1.25 (172.16.1.25) 56(84) bytes of data.
64 bytes from 172.16.1.25: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.16.1.25: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.16.1.25: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.16.1.25: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.16.1.25 ping statistics ---
```

----End

6 Using Enterprise Router and Direct Connect (Virtual Gateway) to Connect an On-Premises Data Center to the Cloud

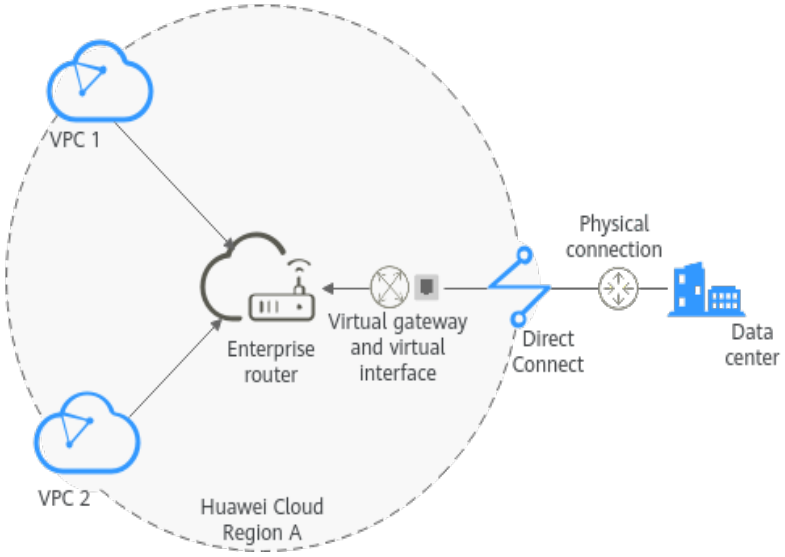
6.1 Overview

Background

There are two VPCs in a region. The two VPCs need to access each other and share the same Direct Connect connection to communicate with an on-premises data center.

For this to work, you can create an enterprise router in the region, and attach the two VPCs and the virtual gateway of the Direct Connect connection to the enterprise router. The enterprise router can forward traffic among the attached VPCs and the virtual gateway, and the two VPCs can share the Direct Connect connection.

Figure 6-1 Networking between an on-premises data center and VPCs



NOTE

You can **share an enterprise router** with different accounts to attach VPCs of these accounts to the same enterprise router for communications.

Virtual gateways can be attached to enterprise routers in the following regions: CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN-Hong Kong, AP-Bangkok, and AP-Singapore.

Operation Procedure

Figure 6-2 shows the procedure for using an enterprise router to connect an on-premises data center with VPCs.

Figure 6-2 Flowchart for connecting an on-premises data center with VPCs

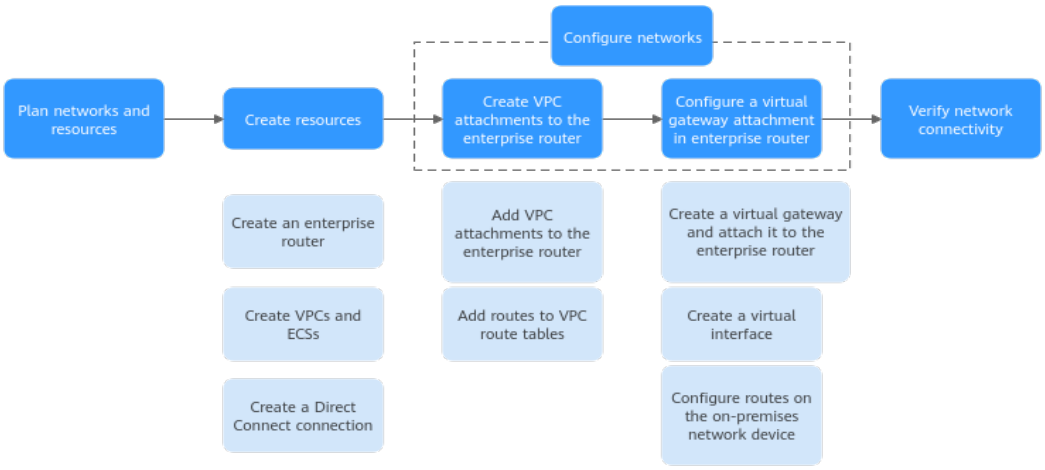


Table 6-1 Description of procedures for connecting an on-premises data center with VPCs

No.	Procedure	Description
1	**Planning Networks and Resources**	Plan required CIDR blocks and the number of resources.
2	**Creating Resources**	1. **Create an enterprise router**. 2. **Create two VPCs and two ECSs**. 3. **Create a Direct Connect connection**. The connection is dedicated to connect an on-premises data center to the cloud over a line you lease from a carrier.

No.	Procedure	Description
3	Configuring Networks	1. Create VPC attachments for the enterprise router: a. Attach the two VPCs to the enterprise router. b. Add routes to the route tables of the VPCs for traffic to route through the enterprise router. 2. Create a virtual gateway attachment for the enterprise router: a. Create a virtual gateway that is associated with the enterprise router. The **virtual gateway** attachment is automatically added to the enterprise router. b. Create a virtual interface to associate the virtual gateway with the Direct Connect connection. c. Configure routes on the router in the on-premises data center.
4	Verifying Connectivity Between the On-premises Data Center and VPCs	Log in to an ECS and run the **ping** command to verify the network connectivity between the on-premises data center and VPCs.

6.2 Planning Networks and Resources

To use an enterprise router to connect an on-premises data center with VPCs, you need to:

- **Network Planning**: Plan CIDR blocks of VPCs and their subnets, virtual gateway and virtual interface of the Direct Connect connection, VPC route tables, and enterprise router route tables.
- **Resource Planning**: Plan the quantity, names, and other parameters of cloud resources, including VPCs, Direct Connect connection, ECSs, and enterprise router.

Network Planning

Figure 6-3 and **Table 6-3** show the network planning and its description for communications between on-premises data center and VPCs.

Figure 6-3 Network planning for communications between on-premises data center and VPCs

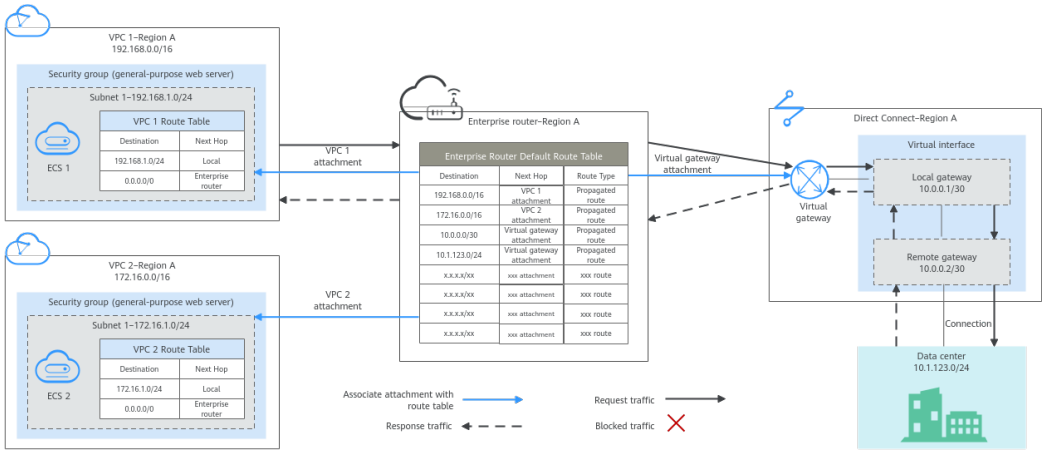


Table 6-2 Network traffic flows

Path	Description
Request traffic: from VPC 1 to the on-premises data center	1. The route table of VPC 1 has a route with the next hop set to the enterprise router to forward traffic from VPC 1 to the enterprise router. 2. In the route table of the enterprise router, there are two routes with the next hop set to the virtual gateway attachment to forward traffic from the enterprise router to the virtual gateway. 3. The virtual gateway is associated with the virtual interface. Traffic from the virtual gateway is forwarded to the Direct Connect connection through the remote gateway of the virtual interface 4. Traffic is sent to the on-premises data center over the connection.
Response traffic: from the on-premises data center to VPC 1	1. Traffic is forwarded to the virtual interface through the connection. 2. The virtual interface connects to the virtual gateway. Traffic from the virtual interface is forwarded to the virtual gateway through the local gateway of the virtual interface. 3. Traffic is forwarded from the virtual gateway to enterprise router. 4. The route table of the enterprise router has a route with the next hop set to the VPC 1 attachment to forward traffic from the enterprise router to VPC 1.

Table 6-3 Description of network planning for communications between on-premises data center and VPCs

Resource	Description
VPCs	• The CIDR blocks of the VPCs to be connected cannot overlap with each other. In this example, the CIDR blocks of the VPCs are propagated to the enterprise router route table as the destination in routes. The CIDR blocks cannot be modified and overlapping CIDR blocks may cause route conflicts. If your existing VPCs have overlapping CIDR blocks, do not use propagated routes. Instead, you need to manually add static routes to the route table of the enterprise router. The destination can be VPC subnet CIDR blocks or smaller ones. • The CIDR blocks of VPCs and of the on-premises data center cannot overlap. • Each VPC has a default route table. • The routes in the default route table are described as follows: – Local: a system route for communications between subnets in a VPC. – Enterprise router: a custom route with destination set to 0.0.0.0/0 for routing traffic from a VPC subnet to the enterprise router. For details, see **Table 6-4**.
Direct Connect	• One connection links your on-premises data center to the cloud. • One virtual gateway that is attached to the enterprise router. • One virtual interface that connects the virtual gateway with the connection.
Enterprise router	After **Default Route Table Association** and **Default Route Table Propagation** are enabled and virtual gateway and VPC attachments are created, the system will automatically: • Direct Connect – Associate the virtual gateway attachment with the default route table of the enterprise router. – Propagate the virtual gateway attachment to the default route table of the enterprise router. The route table automatically learns the local and remote gateways, and the on-premises CIDR block as the destinations of routes. For details, see **Table 6-5**. • VPC – Associate the two VPC attachments with the default route table of the enterprise router. – Propagate the VPC attachments to the default route table of the enterprise router. The route table automatically learns the VPC CIDR blocks as the destination of routes. For details, see **Table 6-5**.

Resource	Description
ECSs	The two ECSs are in different VPCs. If the ECSs are in different security groups, add rules to the security groups to allow access to each other.

Table 6-4 VPC route table

Destination	Next Hop	Route Type
0.0.0.0/0	Enterprise router	Static route (custom)

NOTE

- If you enable **Auto Add Routes** when creating a VPC attachment, you do not need to manually add static routes to the VPC route table. Instead, the system automatically adds routes (with this enterprise router as the next hop and 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations) to all route tables of the VPC.
- If an existing route in the VPC route tables has a destination to 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16, the routes will fail to be added. In this case, do not to enable **Auto Add Routes**. After the attachment is created, manually add routes.
- You need to add a route to VPC route tables with destination set to the on-premises CIDR block and next hop set to enterprise router.
- To reduce the number of routes, you can set the destination of a route (with an enterprise router as the next hop) to 0.0.0.0/0 in the VPC route table. However, in this case, ECSs in VPCs cannot be bound with EIPs. If an ECS in the VPC has an EIP bound, the VPC route table will have a policy-based route with 0.0.0.0/0 as the destination, which has a higher priority than the route with the enterprise router as the next hop. In this case, traffic is forwarded to the EIP and cannot reach the enterprise router.

Table 6-5 Enterprise router route table

Destination	Next Hop	Route Type
VPC 1 CIDR block: 192.168.0.0/16	VPC 1 attachment: er-attach-01	Propagated route
VPC 2 CIDR block: 172.16.0.0/16	VPC 2 attachment: er-attach-02	Propagated route
Local and remote gateways: 10.0.0.0/30	Virtual gateway attachment: vgw-demo	Propagated route
Data center CIDR block: 10.1.123.0/24	Virtual gateway attachment: vgw-demo	Propagated route

Resource Planning

An enterprise router, a Direct Connect connection, VPCs, and ECSs are in the same region but can be in different AZs.

NOTE

The following resource details are only examples. You can modify them as required.

- One enterprise router. See details in **Table 6-6**.

Table 6-6 Enterprise router details

Enterprise Router Name	ASN	Default Route Table Association	Default Route Table Propagation	Association Route Table	Propagation Route Table	Attachment
er-test-01	64512	Enabled	Enabled	Default route table	Default route table	er-attach-01
						er-attach-02

- Direct Connect connection: see details in **Table 6-7**.

Table 6-7 Direct Connect connection details

Virtual Gateway	Virtual Interface	Local Gateway (Cloud)	Remote Gateway (On-premises)	Remote Subnet	Routing and BGP Peer ASN
vgw-demo	vif-demo	10.0.0.1/30	10.0.0.2/30	10.1.123.0/24	Routing: BGP
					BGP peer ASN: 64510

- Two VPCs that do not overlap with each other. See details in **Table 6-8**.

Table 6-8 VPC details

VPC Name	VPC CIDR Block	Subnet Name	Subnet CIDR Block	Association Route Table
vpc-demo-01	192.168.0.0/16	subnet-demo-01	192.168.1.0/24	Default route table
vpc-demo-02	172.16.0.0/16	subnet-demo-02	172.16.1.0/24	Default route table

- Two ECSs, respectively, in two VPCs. See details in **Table 6-9**.

Table 6-9 ECS details

ECS Name	Image	VPC Name	Subnet Name	Security Group	Private IP Address
ecs-demo-01	Public image: EulerOS 2.5 64-bit	vpc-demo-01	subnet-demo-01	sg-demo (general-purpose web server)	192.168.1.99
ecs-demo-02		vpc-demo-02	subnet-demo-02		172.16.1.137

6.3 Creating Resources

6.3.1 Creating an Enterprise Router

Scenarios

This section describes how to create an enterprise router.

Procedure

Step 1 Create an enterprise router in region A.

For details, see **Creating an Enterprise Router**.

For enterprise router details, see **Table 6-6**.

----End

6.3.2 Creating VPCs and ECSs

Scenarios

This section describes how to create VPCs and ECSs.

Procedure

Step 1 Create two VPCs in region A and an ECS in each VPC.

For details, see **Creating a VPC**.

For details, see **Overview**.

- For details about VPC and subnet planning, see **Table 6-8**.
- For details about ECS planning, see **Table 6-9**.

----End

6.3.3 Creating a Direct Connect Connection

Scenarios

This section describes how to create a Direct Connect connection to link an on-premises data center to Huawei Cloud.

Procedure

Step 1 Create a connection.

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

----End

6.4 Configuring Networks

6.4.1 Creating VPC Attachments for the Enterprise Router

Scenarios

This section describes how to attach VPCs to the enterprise router and configure routes.

Procedure

Step 1 Attach the two VPCs to the enterprise router.

For details, see **Creating VPC Attachments to the Enterprise Router**.

Default Route Table Association and **Default Route Table Propagation** are enabled when you create the enterprise router. After VPCs are attached to the enterprise router, the system will automatically:

- Associate the VPC attachment with the default route table of the enterprise router.
- Propagate the VPC attachment to the default route table of the enterprise router. The route table automatically learns the VPC CIDR block as the destination of routes.

Step 2 Add routes to VPC route tables for traffic to route through the enterprise router.

For details, see **Adding Routes to VPC Route Tables**.

----End

6.4.2 Creating a Virtual Gateway Attachment for the Enterprise Router

Scenarios

This section describes how to attach a Direct Connect connection to the enterprise router and configure a route.

Procedure

Step 1 Create a virtual gateway and attach it to an enterprise router.

1. On the Direct Connect console, create a virtual gateway.

   For details, see **Step 2: Create a Virtual Gateway**.

2. On the Enterprise Router console, check whether the virtual gateway attachment has been added to the enterprise router.

   For details, see **Viewing Details About an Attachment**.

   If the status of the virtual gateway attachment is **Normal**, the attachment has been added.

   Default Route Table Association and **Default Route Table Propagation** are enabled when you create the enterprise router. After the virtual gateway is attached to the enterprise router, the system will automatically:

   - Associate the virtual gateway attachment with the default route table of the enterprise router.
   - Propagate the virtual gateway attachment to the default route table of the enterprise router. The routes to the on-premises data center are propagated to the route table.

     You can view routes to the on-premises data center in the route table of the enterprise router only after creating a virtual interface by performing **Step 2**.

Step 2 Create a virtual interface.

Create a virtual interface to connect the virtual gateway with the on-premises data center. For details, see **Step 3: Create a Virtual Interface**.

For details about virtual interface planning, see **Table 6-7**.

Step 3 Configure routes on the on-premises network device to point to Huawei Cloud.

The following uses Huawei network devices as an example to describe how to configure a BGP route.

bgp *64510*

peer *10.0.0.1* **as-number 64512**

peer *10.0.0.1* **password simple** *12345678*

network *10.1.123.0 255.255.255.0*

Table 6-10 BGP route

Command	Description
bgp *64510*	Enable BGP. 64510 is the ASN used by the on-premises data center.
peer *10.0.0.1* **as-number 64512**	Create a BGP peer. • 10.0.0.1 is the gateway on Huawei Cloud. • 64512 is the ASN used by Huawei Cloud. The value must be 64512.
peer *10.0.0.1* **password simple** *12345678*	Perform MD5 authentication on BGP messages when a TCP connection is established between BGP peers. 12345678 is the BGP MD5 authentication password.
network *10.1.123.0 255.255.255.0*	Add routes in the IP route table to the BGP route table. • 10.1.123.0 is the subnet used by the on-premises data center. • 255.255.255.0 is the subnet mask of the on-premises network.

----End

6.5 Verifying Connectivity Between the On-premises Data Center and VPCs

Scenarios

This section describes how to log in to ECSs and verify the connectivity between VPCs.

Procedure

Step 1 Log in to the ECS.

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 2 Verify the network connectivity.

1. Verify the network connectivity between VPCs.

   ping *IP address of the ECS*

To verify the network connectivity between vpc-demo-01 and vpc-demo-02, log in to ecs-demo-01 and run the following command:

ping 172.16.1.137

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

```
[root@ecs-demo-01 ~]# ping 172.16.1.137
PING 172.16.1.137 (172.16.1.137) 56(84) bytes of data.
64 bytes from 172.16.1.137: icmp_seq=1 ttl=64 time=0.455 ms
64 bytes from 172.16.1.137: icmp_seq=2 ttl=64 time=0.299 ms
64 bytes from 172.16.1.137: icmp_seq=3 ttl=64 time=0.232 ms
64 bytes from 172.16.1.137: icmp_seq=4 ttl=64 time=0.236 ms
^C
--- 172.16.1.137 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 92ms
rtt min/avg/max/mdev = 0.232/0.305/0.455/0.091 ms
```

2. Verify the network connectivity between a VPC and the Direct Connect connection.

   ping *IP address of the local gateway (Huawei Cloud)*

   ping *IP address of the remote gateway (on-premises)*

   ping *IP address (on-premises)*

   To verify the network connectivity between vpc-demo-01 and the local gateway on Huawei Cloud, log in to ecs-demo-01 and run the following command:

   ping 10.0.0.1

   If information similar to the following is displayed, the network between the VPC and the local gateway on Huawei Cloud is connected.

```
[root@ecs-demo-01 ~]# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=255 time=7.90 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=255 time=3.72 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=255 time=3.22 ms
^C
--- 10.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.228/4.952/7.907/2.099 ms
[root@ecs-demo-01 ~]#
```

Step 3 Repeat **Step 1** to **Step 2** to verify the network connectivity between the other VPC and the Direct Connect connection.

----End

7 Allowing Direct Connect (Virtual Gateway) and VPN to Work in an Active and Standby Pair to Connect an On-Premises Data Center to the Cloud

7.1 Overview

Scenario

Direct Connect establishes a dedicated, secure, and stable network connection between your on-premises data center and VPCs. It can work together with an enterprise router to build a large-scale hybrid cloud network.

VPN establishes a secure, encrypted communications tunnel between your on-premises data center and your VPC. Compared with Direct Connect, VPN is cost-effective and can be quickly deployed.

To achieve high reliability of hybrid cloud networking and control costs, you can attach both Direct Connect and VPN connections to an enterprise router to enable the connections to work in an active and standby way. If the active connection is faulty, services are automatically switched to the standby one, reducing the risk of service interruptions.

NOTE

You can **share an enterprise router** with different accounts to attach VPCs of these accounts to the same enterprise router for communications.

Virtual gateways can be attached to enterprise routers in the following regions: CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN-Hong Kong, AP-Bangkok, and AP-Singapore.

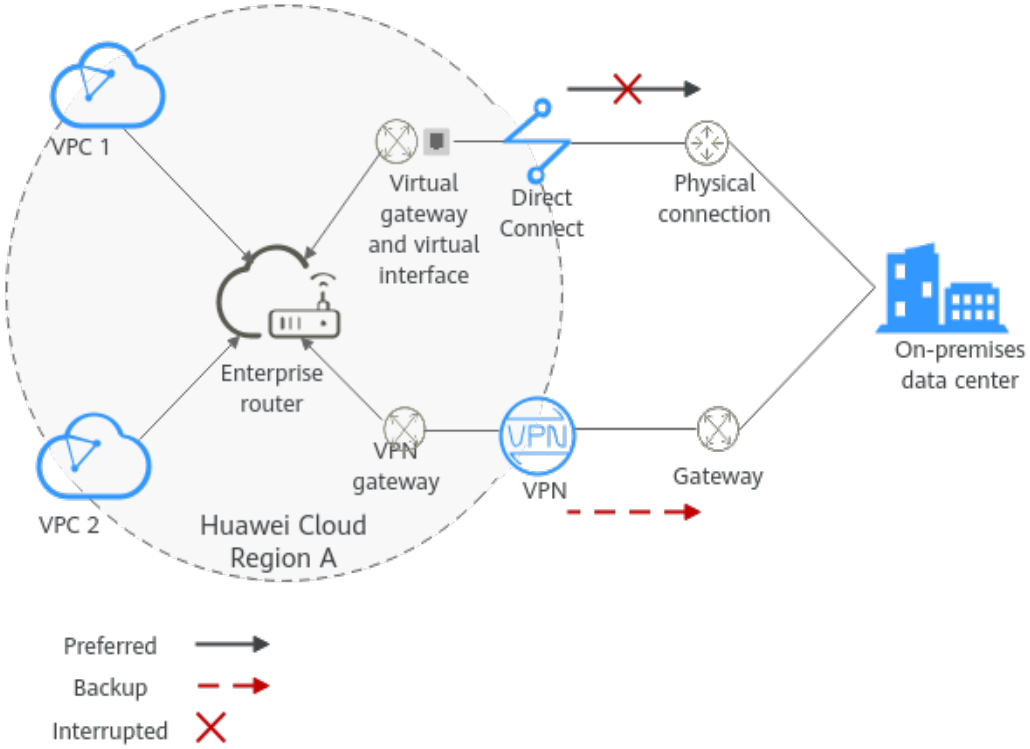
Architecture

To improve the reliability of a hybrid cloud networking, your enterprise uses both Direct Connect and VPN connections to connect your on-premises data center to

the VPCs. The Direct Connect connection works as the active connection and the VPN connection works as the standby one. If the active connection is faulty, services are automatically switched to the standby one, reducing the impact of network interruptions on services.

- VPC 1, VPC 2, and the Direct Connect connection are attached to the enterprise router. VPC1 and VPC 2 can communicate with each other. They communicate with the on-premises data center through the Direct Connect connection.
- The VPN connection is also attached to the enterprise router. If the Direct Connect connection is faulty, VPC 1 and VPC 2 can communicate with the on-premises data center through the VPN connection.

Figure 7-1 Network diagram of Direct Connect and VPN connections working in an active/standby pair



Advantages

An enterprise router allows automatic switchover between active and standby Direct Connect and VPN connections. You do not need to manually switch between them. This prevents service loss and reduces maintenance costs.

Notes and Constraints

The subnet CIDR blocks of the VPCs and of the on-premises data center cannot overlap.

7.2 Planning Networks and Resources

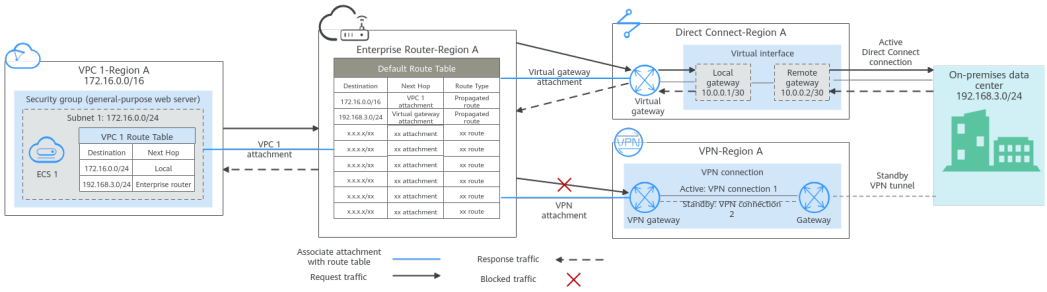
To attach both Direct Connect and VPN connections to an enterprise router to allow them to work in an active/standby pair, you need:

- **Network Planning**: Plan CIDR blocks of VPCs and their subnets, Direct Connect connection, VPN connection, enterprise router, and routes.
- **Resource Planning**: Plan the quantity, names, and other parameters of cloud resources, including VPCs, Direct Connect connection, VPN connection, and enterprise router.

Network Planning

Figure 7-2 shows the network diagram of Direct Connect and VPN connections that work in an active/standby pair. **Table 7-2** describes the network planning.

Figure 7-2 Network diagram of Direct Connect and VPN connections working in an active/standby pair



Direct Connect and VPN connections work in an active/standby pair. If the Direct Connect connection is normal, it is preferentially selected for traffic forwarding.

- Only preferred routes are displayed in the enterprise router route table. The routes of a virtual gateway attachment have a higher priority than those of a VPN gateway attachment. Therefore, routes of the VPN gateway attachment will not be displayed in the route table.
- By default, the Direct Connect connection is used for communications between the VPCs and on-premises data center. **Table 7-1** shows the details about the traffic flows in this example.

Table 7-1 Network traffic flows

Path	Description
Request traffic: from VPC 1 to the on-premises data center	1. The route table of VPC 1 has routes with the next hop set to the enterprise router to forward traffic from VPC 1 to the enterprise router. 2. In the route table of the enterprise router, there is a route with the next hop set to the virtual gateway attachment to forward traffic from the enterprise router to the virtual gateway. 3. The virtual gateway is associated with the virtual interface. Traffic from the virtual gateway is forwarded to the connection through the remote gateway of the virtual interface. 4. Traffic is sent to the on-premises data center over the connection.
Response traffic: from the on-premises data center to VPC 1	1. Traffic is forwarded to the virtual interface through the connection. 2. The virtual interface is connected to the virtual gateway. Traffic from the virtual interface is forwarded to the virtual gateway through the local gateway of the virtual interface. 3. Traffic is forwarded from the virtual gateway to the enterprise router. 4. The route table of the enterprise router has a route with the next hop set to the VPC 1 attachment to forward traffic from the enterprise router to VPC 1.

Table 7-2 Description of network planning for Direct Connect and VPN connections that work in active/standby mode

Resource	Description
VPC	VPC 1 (Service VPC) where your services are deployed: • The CIDR blocks of the VPC and of the on-premises data center cannot overlap. • The VPC has a default route table. • Routes in the default route table: – Local: a system route for communications between subnets in a VPC. – Enterprise router: traffic from a VPC subnet can be forwarded to the enterprise router. The destination is set to the on-premises CIDR block. **Table 7-3** shows the route.
	A VPC that has a subnet used by the VPN gateway. When you create the VPN gateway, you need to enter the subnet CIDR block. The subnet used by the VPN gateway cannot overlap with existing subnets in the VPC.

Resource	Description
Direct Connect	• One connection links your on-premises data center to the cloud. • One virtual gateway that is attached to the enterprise router. • One virtual interface that connects the virtual gateway with the connection.
VPN	• One VPN gateway that is attached to the enterprise router. • One customer gateway that is the gateway of the on-premises data center. • Two VPN connections that connect the VPN gateway and the customer gateway and work in active/standby mode.
Enterprise router	After **Default Route Table Association** and **Default Route Table Propagation** are enabled and an attachment is created, Enterprise Router will automatically: • VPC: – Associate the VPC attachment with the default route table of the enterprise router. – Propagate the VPC attachment to the default route table of the enterprise router. The route table automatically learns the VPC CIDR block as the destination of a route. For details, see **Table 7-4**. • Direct Connect – Associate the virtual gateway attachment with the default route table of the enterprise router. – Propagate the virtual gateway attachment to the default route table of the enterprise router. The route table automatically learns the route information of the virtual gateway attachment. For details, see **Table 7-4**. • VPN – Associate the VPN gateway attachment with the default route table of the enterprise router. – Propagate the VPN gateway attachment to the default route table of the enterprise router. The route table automatically learns the route information of the VPN gateway attachment. For details, see **Table 7-4**.
ECS	One ECS in the service VPC. The ECS is used to verify communications between the cloud and the on-premises data center. If you have multiple ECSs associated with different security groups, you need to add rules to the security groups to allow network access.

Table 7-3 VPC route table

Destination	Next Hop	Route Type
192.168.3.0/24	Enterprise router	Static route (custom)

NOTE

- If you enable **Auto Add Routes** when creating a VPC attachment, you do not need to manually add static routes to the VPC route table. Instead, the system automatically adds routes (with this enterprise router as the next hop and 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations) to all route tables of the VPC.
- If an existing route in the VPC route tables has a destination to 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16, the routes will fail to be added. In this case, do not to enable **Auto Add Routes**. After the attachment is created, manually add routes.
- You need to add a route to the VPC route table with destination set to the on-premises CIDR block and next hop set to enterprise router.

Table 7-4 Enterprise router route table

Destination	Next Hop	Route Type
VPC 1 CIDR block: 172.16.0.0/16	VPC 1 attachment: er-attach-01	Propagated route
Data center CIDR block: 192.168.3.0/24	Virtual gateway attachment: vgw-demo	Propagated route
Data center CIDR block: 192.168.3.0/24	VPN gateway attachment: vpngw-demo	Propagated route

NOTICE

- Only preferred routes are displayed in the enterprise router route table. If both the Direct Connect and VPN connections are working normally, the routes of the virtual gateway attachment take priority and can be viewed in the enterprise router route table. Routes (including routes that are not preferred) of the VPN gateway attachment cannot be viewed.
- If the Direct Connect connection is faulty and services are switched to the VPN connection, you can view the propagated routes of the VPN gateway attachment in the enterprise router route table on the management console.

Resource Planning

An enterprise router, a Direct Connect connection, VPN resources, two VPCs, and an ECS are in the same region but can be in different AZs.

NOTE

The following resource details are only examples. You can modify them as required.

Table 7-5 Details of required resources

Resource	Quantity	Description
VPC	2	A service VPC that is used to run your services and needs to be attached to the enterprise router • VPC name: Set it based on site requirements. In this example, **vpc-for-er** is used. • VPC IPv4 CIDR block: The CIDR block must be different from that of the on-premises data center. Set it based on site requirements. In this example, 172.16.0.0/16 is used. • Subnet name: Set it based on site requirements. In this example, **subnet-for-er** is used. • Subnet IPv4 CIDR block: The CIDR block must be different from that of the on-premises data center. Set it based on site requirements. In this example, 172.16.0.0/24 is used.
		A VPC that has a subnet used by the VPN gateway • VPC name: Set it based on site requirements. In this example, **vpc-for-vpn** is used. • VPC IPv4 CIDR block: Set it based on site requirements. In this example, 10.0.0.0/16 is used. • Subnet name: A default subnet is created together with a VPC. Set it based on site requirements. In this example, **subnet-01** is used. • Subnet IPv4 CIDR block: The default subnet is not used in this example. Set it based on site requirements. In this example, 10.0.0.0/24 is used. **NOTICE** When you create a VPN gateway, you need to select the VPC and set **Interconnection Subnet** to a subnet that is not used by any resource in the VPC. The subnet CIDR block cannot overlap with existing subnet CIDR blocks in the VPC. In this example, the CIDR block of the interconnection subnet cannot be the same as that of the default subnet **subnet-01**.

Resource	Quantity	Description
Enterprise router	1	• **Name**: Set it based on site requirements. In this example, **er-test-01** is used. • **ASN**: Set a different ASN from that of the on-premises data center. In this example, retain the default value **64512**. • **Default Route Table Association**: Enable • **Default Route Table Propagation**: Enable • **Auto Accept Shared Attachments**: Set it based on site requirements. In this example, enable this option. • Three attachments on the enterprise router: – VPC attachment: **er-attach-VPC** – Virtual gateway attachment: **er-attach-VGW** – VPN gateway attachment: **er-attach-VPN**
Direct Connect	1	Connection: Create one based on site requirements.
		Virtual gateway • **Name**: Set it based on site requirements. In this example, **vgw-demo** is used. • **Attachment**: Select **Enterprise Router**. • **Enterprise Router**: Select your enterprise router. In this example, the router is **er-test-01**. • **BGP ASN**: The ASN is the same as or different from that of the enterprise router. In this example, retain the default value 64512.
		Virtual interface • **Name**: Set it based on site requirements. In this example, **vif-demo** is used. • **Virtual Gateway**: Select your virtual gateway. In this example, the virtual gateway is **vgw-demo**. • **Local Gateway**: Set it based on site requirements. In this example, 10.0.0.1/30 is used. • **Remote Gateway**: Set it based on site requirements. In this example, 10.0.0.2/30 is used. • **Remote Subnet**: Set it based on site requirements. In this example, 192.168.3.0/24 is used. • **Routing Mode**: Select **BGP**. • **BGP ASN**: ASN of the on-premises data center, which must be different from the ASN of the virtual gateway on the cloud. In this example, **65525** is used.

Resource	Quantity	Description
VPN	1	VPN gateway • **Name**: Set it based on site requirements. In this example, **vpngw-demo** is used. • **Associate With**: Select **Enterprise Router**. • **Enterprise Router**: Select your enterprise router. In this example, the router is **er-test-01**. • **BGP ASN**: The ASN must be the same as that of the virtual gateway because the Direct Connect and VPN connections back up each other. In this example, 64512 is used. • **VPC**: Select your VPC. In this example, select **vpc-for-vpn**. • **Interconnection Subnet**: Subnet used by the VPN gateway. The subnet cannot overlap with existing subnets in the VPC. Set it based on site requirements. In this example, 10.0.5.0/24 is used.
		Customer gateway • **Name**: Set it based on site requirements. In this example, **cgw-demo** is used. • **Routing Mode**: Select **Dynamic (BGP)**. • **BGP ASN**: ASN of the on-premises data center. The ASN must be the same as that of the virtual gateway because the Direct Connect and VPN connections back up each other. In this example, **65525** is used.
		Two VPN connections that work in active/standby mode: • **Name**: Set it based on site requirements. In this example, the active VPN connection is **vpn-demo-01**, and the standby VPN connection is **vpn-demo-02**. • **VPN Gateway**: Select your VPN gateway. In this example, the VPN gateway is **vpngw-demo**. • **EIP**: Set it based on site requirements. Select the active EIP for the active VPN connection and the standby EIP for the standby VPN connection. • **VPN Type**: Select **Route-based**. • **Customer Gateway**: Select your customer gateway. In this example, the customer gateway is **cgw-demo**. • **Interface IP Address Assignment**: In this example, **Automatically assign** is selected. • **Routing Mode**: Select **Dynamic (BGP)**.

Resource	Quantity	Description
ECS	1	• **ECS Name**: Set it based on site requirements. In this example, **ecs-demo** is used. • **Image**: Select an image based on site requirements. In this example, a public image (CentOS 8.2 64bit) is used. • **Network** – **VPC**: Select your VPC. In this example, select **vpc-for-er**. – **Subnet**: Select a subnet. In this example, select **subnet-for-er**. • **Security Group**: Select a security group based on site requirements. In this example, the security group uses a general-purpose web server template and its name is **sg-demo**. • Private IP address: 172.16.1.137

NOTICE

- The virtual gateway and the VPN gateway must use the same ASN to prevent network loops because the Direct Connect and VPN connections back up each other. In this example, 64512 is used.
- The ASN of the enterprise router can be the same as or different from that of the virtual gateway and the VPN gateway. In this example, 64512 is used.
- The ASN of the on-premises data center must be different from that used on the cloud. Set this ASN of the on-premises data center based on site requirements. In this example, 65525 is used.

7.3 Building a Hybrid Cloud Network Through Direct Connect and VPN Working in an Active/Standby Pair

Table 7-6 describes the overall process of building a hybrid cloud network using an enterprise router and Direct Connect and VPN connections that work in an active/standby pair.

Table 7-6 Process description of constructing the hybrid cloud network

Procedure	Description
Step 1: Create Cloud Resources	1. Create an enterprise router for connecting VPCs in the same region. 2. Create a service VPC with a subnet. 3. Create an ECS in the service VPC subnet.

Procedure	Description
Step 2: Create a Virtual Gateway Attachment to the Enterprise Router	1. Create a Direct Connect connection. The connection is dedicated to connect an on-premises data center to Huawei Cloud over a line you lease from a carrier. 2. Create a virtual gateway and attach it to the enterprise router. 3. Create a virtual interface to associate the virtual gateway with the Direct Connect connection. 4. Configure routes on the router in the on-premises data center.
Step 3: Create a VPC Attachment to the Enterprise Router	1. Attach the service VPC to the enterprise router. 2. Add a route with the enterprise router as the next hop and the on-premises CIDR block as the destination to the VPC route table.
Step 4: Verify the Network Connectivity Over the Direct Connect Connection	Log in to the ECS and run the **ping** command to verify the network connectivity through the Direct Connect connection.
Step 5: Create a VPN Attachment to the Enterprise Router	1. Create a VPN gateway and attach it to the enterprise router. 2. Create a customer gateway, that is the gateway of the on-premises data center. 3. Create two VPN connections that connect the VPN gateway and the customer gateway and work in active/standby mode. 4. Configure routes on the router in the on-premises data center.
Step 6: Verify the Network Connectivity Over the VPN Connection	Log in to the ECS and run the **ping** command to verify the network connectivity through the VPN connections. A VPN connection is a standby one. If you need to verify the network connectivity through a VPN connection, you need to simulate a fault on the active connection, that is the Direct Connect connection.

7.4 Procedure for Communications Between an On-Premises Data Center and the Cloud Through Direct Connect and VPN

Step 1: Create Cloud Resources

This step describes how to create the service VPC, ECS, and enterprise router. For details about these resources, see **Table 7-5**.

Step 1 Create an enterprise router.

For details, see **Creating an Enterprise Router**.

Step 2 Create a service VPC.

For details, see **Creating a VPC**.

Step 3 Create an ECS.

In this example, the ECS is used to verify the communications between the VPC and the on-premises data center. The ECS quantity and configuration are for reference only.

For details, see **Overview**.

----End

Step 2: Create a Virtual Gateway Attachment to the Enterprise Router

For details about Direct Connect resources, see **Table 7-5**.

Step 1 Create a connection.

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

Step 2 Create a virtual gateway and attach it to the enterprise router.

1. On the Direct Connect console, create a virtual gateway.

   For details, see **Step 2: Create a Virtual Gateway**.

2. On the Enterprise Router console, check whether the virtual gateway attachment has been added to the enterprise router.

   For details, see **Viewing Details About an Attachment**.

   If the status of the virtual gateway attachment is **Normal**, the attachment has been added.

   Default Route Table Association and **Default Route Table Propagation** are enabled when you create the enterprise router. After the virtual gateway is attached to the enterprise router, the system will automatically:

   - Associate the virtual gateway attachment with the default route table of the enterprise router.
   - Propagate the virtual gateway attachment to the default route table of the enterprise router. The routes to the on-premises data center are propagated to the route table.

You can view routes to the on-premises data center in the route table of the enterprise router only after performing the following steps.

Step 3 Create a virtual interface.

Create a virtual interface to connect the virtual gateway with the on-premises data center. For details, see **Step 3: Create a Virtual Interface**.

Step 4 Configure routes on the on-premises network device.

Direct Connect and VPN connections back up each other. Note the following when configuring routes:

- The route type of the Direct Connect connection must be the same as that of the VPN connection. BGP routes must be configured for dual-link mutual backup.
- The route priority of the Direct Connect connection must be higher than that of the VPN connection.
- The amount of time that the disconnection of Direct Connect and VPN connections is detected should be the same as that of the cloud network.

----End

Step 3: Create a VPC Attachment to the Enterprise Router

Step 1 Attach the service VPC to the enterprise router.

When creating the VPC attachment, do not enable **Auto Add Routes**.

NOTICE

If this option is enabled, Enterprise Router automatically adds routes (with this enterprise router as the next hop and 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations) to all route tables of the VPC. In this example, you need to add a route to the VPC route table with destination set to the on-premises CIDR block and next hop set to enterprise router.

For details, see **Creating VPC Attachments to the Enterprise Router**.

Step 2 Check the route with destination set to the VPC CIDR block in the enterprise router route table.

In this example, **Default Route Table Association** and **Default Route Table Propagation** are enabled for the enterprise router, and routes with destinations set to VPC CIDR blocks are automatically added when you attach the VPCs to the enterprise router.

For VPC route details, see **Table 7-2** and **Table 7-4**.

To view enterprise routes, see **Viewing Routes**.

Step 3 In the route table of the service VPC, add a route with the next hop set to the enterprise router.

For VPC route details, see **Table 7-3**.

For details, see **Adding Routes to VPC Route Tables**.

----End

Step 4: Verify the Network Connectivity Over the Direct Connect Connection

Step 1 Log in to ecs-demo.

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 the ECS.

Step 2 Check whether the service VPC can communicate with the on-premises data center through the enterprise router.

ping *IP address of the on-premises data center*

Example command:

ping 192.168.3.10

If information similar to the following is displayed, the VPC can communicate with the on-premises data center through the enterprise router.

```
[root@ecs-demo ~]# ping 192.168.3.10
PING 192.168.3.10 (192.168.3.10) 56(84) bytes of data.
64 bytes from 192.168.3.10: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 192.168.3.10: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 192.168.3.10: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 192.168.3.10: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 192.168.3.10 ping statistics ---
```

----End

Step 5: Create a VPN Attachment to the Enterprise Router

For details about the VPC used by VPN, see **Table 7-5**.

Step 1 Create a VPC for the VPN gateway.

For details, see **Creating a VPC**.

NOTICE

When you create a VPN gateway, you need to select the VPC and set **Interconnection Subnet** to a subnet that is not used by any resource in the VPC. The subnet CIDR block cannot overlap with existing subnet CIDR blocks in the VPC. In this example, the CIDR block of the interconnection subnet cannot be the same as that of the default subnet **subnet-01**.

Step 2 Create a VPN gateway and attach it to the enterprise router.

1. On the VPN management console, create a VPN gateway.

   For details, see **Creating a VPN Gateway**.

2. On the Enterprise Router console, view the VPN gateway attachment created for the enterprise router.

For details, see **Viewing Details About an Attachment**.

If the status of the VPN gateway attachment is **Normal**, the attachment has been added.

Default Route Table Association and **Default Route Table Propagation** are enabled when you create the enterprise router. After the VPN gateway is attached to the enterprise router, the system will automatically:

- Associate the VPN gateway attachment with the default route table of the enterprise router.
- Propagate the VPN gateway attachment to the default route table of the enterprise router. The routes to the on-premises data center are propagated to the route table.

  You can view routes to the on-premises data center in the route table of the enterprise router only after performing the following steps.

Step 3 Create a customer gateway.

For details, see **Creating a Customer Gateway**.

Step 4 Create two VPN connections that will work in active/standby mode.

1. **Create VPN connection 1**.
2. **Create VPN connection 2**.

Step 5 Configure routes on the on-premises network device.

Direct Connect and VPN connections back up each other. Note the following when configuring routes:

- The route type of the Direct Connect connection must be the same as that of the VPN connection. BGP routes must be configured for dual-link mutual backup.
- The route priority of the Direct Connect connection must be higher than that of the VPN connection.
- The amount of time that the disconnection of Direct Connect and VPN connections is detected should be the same as that of the cloud network.

----End

Step 6: Verify the Network Connectivity Over the VPN Connection

A VPN connection is a standby one. If you need to verify the network connectivity through a VPN connection, you need to simulate a fault on the active connection, that is the Direct Connect connection.

Step 1 Simulate a fault on the Direct Connect connection to ensure that the service VPC cannot communicate with the on-premises data center over the connection.

NOTICE

Simulate a fault only when no packets are transmitted over the Direct Connect connection to prevent service interruptions.

Step 2 Log in to ecs-demo.

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 the ECS.

Step 3 Check whether the service VPC can communicate with the on-premises data center through the enterprise router.

ping *IP address of the on-premises data center*

Example command:

ping 192.168.3.10

If information similar to the following is displayed, the VPC can communicate with the on-premises data center through the enterprise router.

```
[root@ecs-demo ~]# ping 192.168.3.10
PING 192.168.3.10 (192.168.3.10) 56(84) bytes of data.
64 bytes from 192.168.3.10: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 192.168.3.10: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 192.168.3.10: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 192.168.3.10: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 192.168.3.10 ping statistics ---
```

----End

8 Allowing a Pair of Direct Connect Connections (Virtual Gateway) to Connect an On-Premises Data Center to the Cloud

8.1 Overview

Scenario

Direct Connect establishes a dedicated, secure, stable, and high-speed network connection between your on-premises data center and VPCs. It works together with an enterprise router to build a large-scale hybrid cloud network.

Enterprise Router makes it possible for dynamic route selection and switchover of Direct Connect connections. Load is balanced among multiple connections, and the network bandwidth is fully used, which increases network throughput, improves network performance, and ensures high reliability.

In this example, we use an enterprise router and two Direct Connect connections to build a hybrid cloud network.

NOTE

You can **share an enterprise router** with different accounts to attach VPCs of these accounts to the same enterprise router for communications.

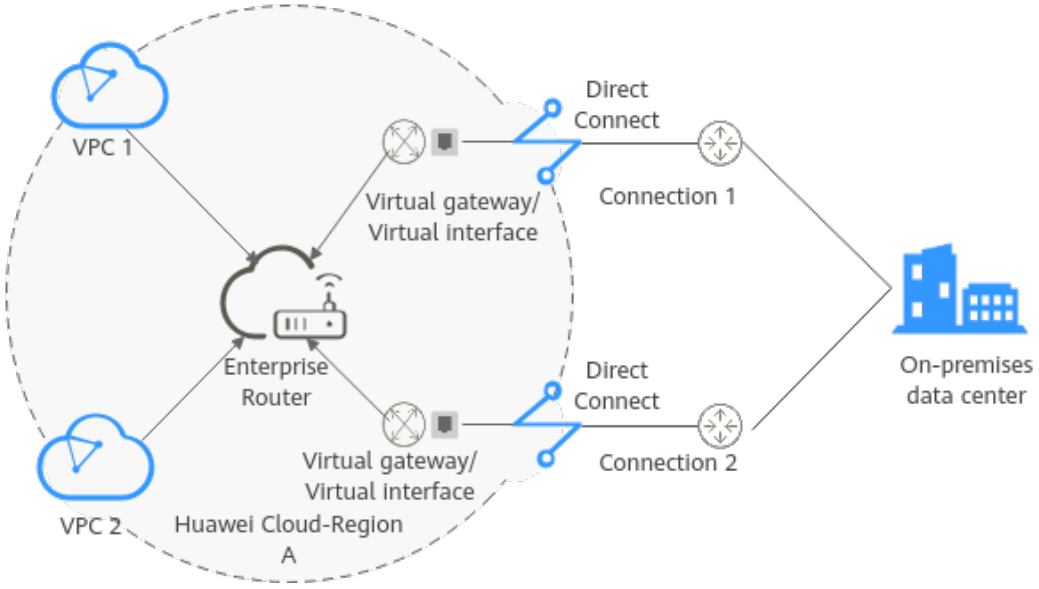
Virtual gateways can be attached to enterprise routers in the following regions: CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN-Hong Kong, AP-Bangkok, and AP-Singapore.

Architecture

To improve the performance and reliability of hybrid cloud networking, your enterprise uses two Direct Connect connections to connect your on-premises data center to the VPCs. Two Direct Connect connections work in load balancing mode. When both connections are working normally, network transmission is greatly improved. If one connection is faulty, the other connection ensures the normal running of the hybrid cloud network and thereby prevents service interruption caused by a single point of failure.

- VPC1 and VPC2 can communicate with each other and communicate with the on-premises data center over two Direct Connect connections and an enterprise router.
- When one Direct Connect connection is faulty, VPC1 and VPC2 can communicate with the on-premises data center over the normal connection.

Figure 8-1 A hybrid cloud network built using an enterprise router and a pair of Direct Connect connections



Advantages

Enterprise Router makes it possible for two Direct Connect connections to work in load balancing mode. This improves the network performance and reliability of hybrid cloud networking and prevents service interruptions caused by a single point of failure.

Constraints

The subnet CIDR blocks of the VPCs and of the on-premises data center cannot overlap.

8.2 Planning Networks and Resources

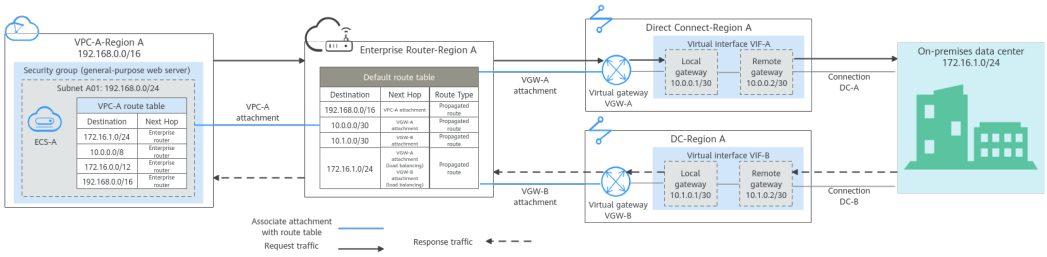
To attach both Direct Connect connections to an enterprise router to allow them to work in load balancing mode, you need to:

- **Network Planning**: Plan CIDR blocks of VPCs and their subnets, Direct Connect connections, and enterprise router, as well as the routes of these resources.
- **Resource Planning**: Plan the quantity, names, and other parameters of cloud resources, including VPCs, Direct Connect connections, and enterprise router.

Network Planning

Figure 8-2 shows the network diagram of Direct Connect connections that work in load balancing mode. Table 8-2 describes the network planning.

Figure 8-2 Network diagram of two Direct Connect connections



Two Direct Connect connections work in load balancing mode and connect the on-premises data center to the VPCs. Table 8-1 describes the network traffic flows in detail.

Table 8-1 Network traffic flows

Path	Description
Request traffic: from VPC-A to the on-premises data center	1. In the route table of VPC-A, there are routes with the next hop set to the enterprise router to forward traffic from VPC-A to the enterprise router. 2. In the route table of the enterprise router, there is a route with next hop set to virtual gateway VGW-A attachment to forward traffic from the enterprise router to virtual gateway VGW-A. • The next hop is VGW-A. 172.16.1.0/24 is the CIDR block used by the on-premises data center, and 10.0.0.0/30 is the IP address range for assigning gateway addresses to virtual interface VIF-A. • The next hops of the routes destined for 172.16.1.0/24 are VGW-A and VGW-B. The two routes are equal-cost routes for load balancing. The traffic selects a network connection based on the hash algorithm. In this example, connection DC-A with virtual gateway VGW-A is selected. 3. Virtual interface VIF-A is connected to virtual gateway VGW-A. Traffic from the virtual gateway is forwarded to the connection through the remote gateway of the virtual interface. 4. Traffic is forwarded to the on-premises data center over connection DC-A.

Path	Description
Response traffic: from the on-premises data center to VPC-A	1. Traffic is forwarded to virtual interface VIF-B over connection DC-B. In the on-premises data center, there are also two equal-cost routes that point to the cloud and are used for load balancing. Traffic is returned over a connection selected based on the hash algorithm. In this example, DC-B with virtual gateway VGW-B is selected. 2. Virtual interface VIF-B is connected to virtual gateway VGW-B. Traffic from the virtual interface is forwarded to the virtual gateway through the local gateway of the virtual interface. 3. Traffic is forwarded from virtual gateway VGW-B attachment to the enterprise router. 4. In the route table of the enterprise router, there is a route with the next hop set to the VPC-A attachment to forward traffic from the enterprise router to VPC-A.

Table 8-2 Network planning using two Direct Connect connections

Cloud Service/ Resource	Description
VPC	A VPC that is used to run your services and needs to be attached to the enterprise router. • The CIDR blocks of the VPC and of the on-premises data center cannot overlap. • The VPC has a default route table. • **Table 8-3** lists the routes in the default VPC route table. – Three routes to fixed CIDR blocks: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. If **Auto Add Routes** is enabled when the VPC is attached to the enterprise router, static routes will be automatically configured in the VPC route table. If more than one VPC is attached to an enterprise router, traffic from one VPC to the other VPCs can be forwarded to the enterprise router over these routes, and is then to the next-hop network instance through the enterprise router. – A route to the on-premises CIDR block: In addition to the three automatically-added VPC CIDR blocks, you need to add a route whose destination is the on-premises CIDR block (172.16.1.0/24 in this example) and next hop is enterprise router to the VPC route table. Traffic from the VPC is forwarded to the enterprise router and then to the next-hop network instance through the enterprise router. **NOTICE** If an existing route in the VPC route table has a destination to 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16, the route that points to each CIDR block will fail to be added. In this case, do not enable **Auto Add Routes**. After the attachment is created, manually add the routes.
Direct Connect	Two connections that work in load balancing mode. • Both connections link your on-premises data center to the cloud. • Each connection has a virtual gateway associated, and both virtual gateways are attached to the enterprise router. • A virtual interface is required for connecting each virtual gateway to the connection. The two virtual interfaces work in load balancing mode.

Cloud Service/ Resource	Description
Enterprise Router	After **Default Route Table Association** and **Default Route Table Propagation** are enabled and an attachment is created, Enterprise Router will automatically: • VPC – Associate the VPC attachment with the default route table of the enterprise router. – Propagate the VPC attachment to the default route table of the enterprise router. The route table automatically learns the VPC CIDR block as the destination of a route. For details, see **Table 8-4**. • Direct Connect – Associate the two virtual gateway attachments with the default route table of the enterprise router. – Propagate the virtual gateway attachments to the default route table of the enterprise router. The route table automatically learns the route information of the virtual gateway attachments. For details, see **Table 8-4**.
Route policy	• If the on-premises BGP routes learned by the enterprise router through two virtual gateway attachments are equal-cost routes, load balancing is automatically implemented, and you do not need to create a route policy. In this example, the two routes with 172.16.1.0/24 as the destination and VGW-A and VGW-B as the next hops are equal-cost routes. • If the on-premises BGP routes learned by the enterprise router through two virtual gateway attachments are not equal-cost routes, load balancing cannot be implemented. In this case, you need to associate a route policy with the propagation of the two virtual gateway attachments. After the AS_Path are replaced, the routes from the enterprise router to the on-premises data center through the two virtual gateways will work as equal-cost routes. For this to work, you need to add two nodes to the route policy: – Node 1 has a higher priority and matches BGP routes. The AS_Path of matched BGP routes is replaced with the BGP ASNs of the virtual gateways. – Node 2 has a lower priority and matches all routes, ensuring normal communication through non-BGP routes. For details, see **Route Policies**. **NOTICE** Configuring a route policy to replace the AS_Path of a route may cause network loops. Before configuring a route policy, check your network plan.

Cloud Service/ Resource	Description
ECS	An ECS deployed in the service VPC. The ECS is used to verify communications between the cloud and the on-premises data center. If you have multiple ECSs associated with different security groups, you need to add rules to the security groups to allow network access.
On-premises data center	Two equal-cost routes from the on-premises data center to the enterprise router for load balancing.

Table 8-3 VPC route table

Destination	Next Hop	Route Type
Fixed CIDR block: 10.0.0.0/8	Enterprise router	Static route (custom)
Fixed CIDR block: 172.16.0.0/12	Enterprise router	Static route (custom)
Fixed CIDR block: 192.168.0.0/16	Enterprise router	Static route (custom)
On-premises CIDR block: 172.16.1.0/24	Enterprise router	Static route (custom)

Table 8-4 Enterprise router route table

Destination	Next Hop	Route Type
VPC-A CIDR block: 192.168.0.0/16	VPC-A attachment: er-attach-vpc-A	Propagated route
VIF-A gateway: 10.0.0.0/30	VGW-A attachment: er-attach-vgw-A	Propagated route
VIF-B gateway: 10.1.0.0/30	VGW-B attachment: er-attach-vgw-B	Propagated route

Destination	Next Hop	Route Type
On-premises CIDR block: 172.16.1.0/24On-premises data center CIDR block	Two equal-cost routes for the two connections to work in load balancing mode: • VGW-A attachment: er-attach-vgw-A • VGW-B attachment: er-attach-vgw-B	Propagated route

Resource Planning

An enterprise router, two Direct Connect connections, a VPC, and an ECS are in the same region but can be in different AZs.

NOTE

The following resource details are only examples. You can modify them as required.

Table 8-5 Details of required resources

Resource	Quantity	Description
VPC	1	A VPC that is used to run your services and needs to be attached to the enterprise router. • VPC name: Set it based on site requirements. In this example, **VPC-A** is used. • VPC IPv4 CIDR block: The CIDR block must be different from that of the on-premises data center. Set it based on site requirements. In this example, **192.168.0.0/16** is used. • Subnet name: Set it based on site requirements. In this example, **subnet-A01** is used. • Subnet IPv4 CIDR block: The CIDR block must be different from that of the on-premises data center. Set it based on site requirements. In this example, **192.168.0.0/24** is used.

Resource	Quantity	Description
Enterprise Router	1	• **Name**: Set it based on site requirements. In this example, **ER-X** is used. • **ASN**: Set an ASN that is different from that of the on-premises data center. In this example, the ASN is **64512**. • **Default Route Table Association**: Enable • **Default Route Table Propagation**: Enable • **Auto Accept Shared Attachments**: Set it based on site requirements. In this example, enable this option. • Three attachments on the enterprise router: – VPC-A attachment: **er-attach-vpc-A** – VGW-A attachment: **er-attach-vgw-A** – VGW-B attachment: **er-attach-vgw-B**
Route policy	1	If the on-premises BGP routes learned by the enterprise router through two virtual gateway attachments are not equal-cost routes, load balancing cannot be implemented. If this happens, you need to configure a route policy to associate it with two virtual gateway attachments. For this to work, you need to add two nodes to the route policy. • Node 1 has a higher priority. The AS_Path of BGP routes is replaced, so the routes learned by the enterprise router through the two virtual gateway attachments can work as equal-cost routes. – **Node Number**: A node with a smaller node number is executed first. The node number of node 1 must be smaller than that of node 2. Set it to **10**. – **Action**: Set it to **Allow**. – **Match Condition**: Select **Route type** and then **BGP**. – **Policy Value** 1: Select **AS_Path**. – **Action**: Select **Replace**. The value of **Replace** must be the same as the BGP ASN of the virtual gateway. In this example, the value is **64513**. • Node 2 has a lower priority and matches all routes, ensuring normal communication through non-BGP routes. – **Node Number**: Set a value greater than that of node 1. In this example, set it to **20**. – **Action**: Set it to **Allow**. Leave other parameters blank, indicating that other routes that do not match node 1 can match node 2. This ensures that the route policy allows all routes.

Resource	Quantity	Description
Direct Connect	2	Two connections are required. In this example, the two connections are DC-A and DC-B.
		Two virtual gateways are required. • **Name**: Set it based on site requirements. In this example, **VGW-A** and **VGW-B** are used. • **Associate With**: Select **Enterprise Router**. • **Enterprise Router**: Select your enterprise router. In this example, **ER-X** is used. • **BGP ASN**: The ASNs of the two virtual gateways must be the same and can be the same as or different from that of the enterprise router. In this example, the ASNs of the two virtual gateways are **64513**.
		Two virtual interfaces are required. • **Name**: In this example, the two virtual interfaces are **VIF-A** and **VIF-B**. • **Virtual Interface Priority**: Select **Preferred** for both virtual interfaces, indicating that load balancing will be implemented. • **Connection**: In this example, virtual interface VIF-A is associated with connection DC-A, and virtual interface VIF-B is associated with connection DC-B. • **Virtual Gateway**: In this example, virtual interface VIF-A is associated with virtual gateway VGW-A, and virtual interface VIF-B is associated with virtual gateway VGW-B. • **Local Gateway**: In this example, the local gateway IP address range for virtual interface VIF-A is **10.0.0.1/30**, and that for VIF-B is **10.1.0.1/30**. • **Remote Gateway**: In this example, the remote gateway IP address range for virtual interface VIF-A is **10.0.0.2/30**, and that for VIF-B is **10.1.0.2/30**. • **Remote Subnet**: In this example, the on-premises CIDR block is **172.16.1.0/24**. • **Routing Mode**: Select **BGP**. • **BGP ASN**: ASN of the on-premises data center, which must be different from the ASNs of the virtual gateways on the cloud. In this example, **64555** is used.

Resource	Quantity	Description
ECS	1	An ECS is used to verify connectivity. • **ECS Name**: Set it based on site requirements. In this example, **ecs-A** is used. • **Image**: Select an image based on site requirements. In this example, a public image (CentOS 8.2 64bit) is used. • **Network** – **VPC**: Select the service VPC. In this example, select **VPC-A**. – **Subnet**: Select the subnet that communicates with the on-premises data center. In this example, the subnet is **subnet-A01**. • **Security Group**: Select a security group based on site requirements. In this example, the security group uses a general-purpose web server template and its name is **sg-demo**. • Private IP address: 192.168.0.137

NOTICE

- The two Direct Connect connections work in load balancing mode. To prevent network loops and form equal-cost routes, the ASNs of the two virtual gateways must be the same. In this example, the ASN is **64513**.
- The ASN of the enterprise router can be the same as or different from that of the virtual gateways. In this example, **64512** is used.
- The ASN of the on-premises data center must be different from that used on the cloud. Set this ASN of the on-premises data center based on site requirements. In this example, **64555** is used.

8.3 Building a Hybrid Network Using an Enterprise Router and Two Direct Connect Connections

Table 8-6 describes the overall process of building a hybrid cloud network using an enterprise router and a pair of Direct Connect connections that work in load balancing mode.

Table 8-6 Process for building a hybrid cloud network

Step	Description
Step 1: Create Cloud Resources	1. Create an enterprise router. 2. Create a service VPC with a subnet. 3. Create an ECS in the subnet of the service VPC.
Step 2: Add a VPC Attachment for the Enterprise Router	1. Attach the service VPC to the enterprise router. 2. In the VPC route table, add a route with the enterprise router as the next hop and the on-premises CIDR block as destination.
Step 3: Create Virtual Gateway Attachments to the Enterprise Router	1. Establish connectivity using one connection and verify connectivity. a. Create a Direct Connect connection to connect the on-premises data center to the cloud over a line you lease from a carrier. b. Create a virtual gateway and attach it to the enterprise router. c. Create a virtual interface to connect the virtual gateway to the connection. d. Configure routes on the router in the on-premises data center. e. Log in to the ECS and run the **ping** command to verify connectivity. 2. Establish connectivity using the other connection and verify connectivity.

Step	Description
Step 4: Configure Equal-Cost Routes on the Enterprise Router and the On-Premises Network	1. In the enterprise router route table, check whether load balancing is implemented among the BGP routes learned by the enterprise router through the virtual gateway attachments. a. If load balancing is implemented, no route policy is required. b. If load balancing is not implemented, configure a route policy and perform 2 to configure equal-cost routes on the enterprise router. 2. (Optional) Configure equal-cost routes on the enterprise router. Replace the AS_Path of the routes, which may cause network loops. Before configuring a route policy, check your network plan. a. Create a route policy that contains two nodes. b. Associate the route policy with the two virtual gateway attachments so that the BGP routes learned by the enterprise router through the two attachments can work as equal-cost routes. 3. Log in to the on-premises network device and configure equal-cost routes.

8.4 Procedure for Building a Hybrid Network Using an Enterprise Router and Two Direct Connect Connections

Step 1: Create Cloud Resources

Create an enterprise router, a service VPC, an ECS, as described in **Table 8-5**.

Step 1 Create an enterprise router.

For details, see **Creating an Enterprise Router**.

Step 2 Create a service VPC.

For details, see **Creating a VPC**.

Step 3 Create an ECS.

In this example, the ECS is used to verify the communications between the VPC and the on-premises data center. The ECS quantity and configuration are for reference only.

For details, see **Overview**.

----End

Step 2: Add a VPC Attachment for the Enterprise Router

Step 1 Attach the service VPC to the enterprise router.

When creating the VPC attachment, enable **Auto Add Routes**.

NOTICE

If this option is enabled, Enterprise Router automatically adds routes (with this enterprise router as the next hop and 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations) to all route tables of the VPC.

For details, see **Creating VPC Attachments to the Enterprise Router**.

Step 2 Check the routes with destinations set to the VPC CIDR blocks in the enterprise router route table.

In this example, **Default Route Table Association** and **Default Route Table Propagation** are enabled for the enterprise router, and routes with destinations set to VPC CIDR blocks are automatically added when you attach the VPCs to the enterprise router.

For VPC route details, see **Table 8-2** and **Table 8-4**.

In this example, the route whose destination is **192.168.0.0/16** and next hop is the VPC-A attachment is automatically added.

To view enterprise routes, see **Viewing Routes**.

Step 3 In the route table of the service VPC, add a route with the next hop set to the enterprise router.

For VPC route details, see **Table 8-3**.

In this example, the route destination is **172.16.1.0/24**, which is the CIDR block used in the on-premises data center.

For details, see **Adding Routes to VPC Route Tables**.

----End

Step 3: Create Virtual Gateway Attachments to the Enterprise Router

For details about Direct Connect resources, see **Table 8-5**.

Step 1 Use one Direct Connect connection to link the on-premises data center to the cloud.

1. Create a connection.

   For details, see **Creating a Connection**.
2. Create a virtual gateway and attach it to the enterprise router.
   a. On the Direct Connect console, create a virtual gateway.

      For details, see **Step 2: Create a Virtual Gateway**.
   b. On the Enterprise Router console, check whether the virtual gateway attachment has been added to the enterprise router.

For details, see **Viewing Details About an Attachment**.

If the status of the virtual gateway attachment is **Normal**, the attachment has been added.

Default Route Table Association and **Default Route Table Propagation** are enabled when you create the enterprise router. After the virtual gateway is attached to the enterprise router, the system will automatically:

- Associate the virtual gateway attachment with the default route table of the enterprise router.
- Propagate the virtual gateway attachment to the default route table of the enterprise router. The routes to the on-premises data center are propagated to the route table.

  You can view routes to the on-premises data center in the route table of the enterprise router only after performing the following steps.

3. Create a virtual interface.

   Create a virtual interface to connect the virtual gateway with the on-premises data center. For details, see **Step 3: Create a Virtual Interface**.

4. Configure routes on the on-premises network device to point to the cloud.

   The following uses Huawei network devices as an example to describe how to configure a BGP route.

   bgp *64555*

   peer *10.0.0.1* **as-number 64512**

   peer *10.0.0.1* **password simple** *12345678*

   network *172.16.1.0 255.255.255.0*

Table 8-7 BGP route

Command	Description
bgp *64555*	Enable BGP. **64555** is the ASN used by the on-premises data center.
peer *10.0.0.1* **as-number 64512**	Create a BGP peer. – **10.0.0.1** is the gateway on the cloud. – **64512** is the ASN used by the cloud.
peer *10.0.0.1* **password simple** *12345678*	Perform MD5 authentication on BGP messages when a TCP connection is established between BGP peers. **12345678** is the BGP MD5 authentication password.

Command	Description
network *172.16.1.0 255.255.255.0*	Add routes in the IP route table to the BGP route table. – **172.16.1.0** is the network used by the on-premises data center. – **255.255.255.0** is the subnet mask of the on-premises network.

5. Log in to ecs-A.

   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 the ECS.

6. Run the following command to verify the connectivity over one Direct Connect connection:

   ping *IP address of the on-premises data center*

   Example command:

   ping 172.16.1.10

   If information similar to the following is displayed, VPC-A can communicate with the on-premises data center over the Direct Connect connection:

```
[root@ecs-A ~]# ping 172.16.1.10
PING 172.16.1.10 (172.16.1.10) 56(84) bytes of data.
64 bytes from 172.16.1.10: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.16.1.10: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.16.1.10 ping statistics ---
```

Step 2 Use the other Direct Connect connection to link the on-premises data center to the cloud.

1. Repeat **Step 1.1** to **Step 1.4** set up the other Direct Connect connection.
2. Simulate a fault on one Direct Connect connection to ensure that the service VPC cannot communicate with the on-premises data center over this connection.

   NOTICE

   Simulate a fault only when no packets are transmitted over the Direct Connect connection to prevent service interruptions.

3. Repeat **Step 1.5** to **Step 1.6** to verify the connectivity over the other Direct Connect connection.

----End

Step 4: Configure Equal-Cost Routes on the Enterprise Router and the On-Premises Network

Step 1 In the enterprise router route table, check whether load balancing is implemented among the BGP routes learned by the enterprise router through the virtual gateway attachments.

To view enterprise routes, see **Viewing Routes**.

- If load balancing is implemented, no route policy is required.
- If load balancing is not implemented, configure a route policy and perform **Step 2** to configure equal-cost routes on the enterprise router.

  If the next hop of the route to 172.16.1.0/24 is the two virtual gateways, the load balancing mode is used.

Step 2 (Optional) Configure equal-cost routes on the enterprise router.

1. Create a route policy that contains two nodes.

   For details about the overview planning of the policy, see **Table 8-5**.

   For details about how to create a route policy, see **Creating a Route Policy**.
2. Associate the route policy with the propagation of each virtual gateway attachment to enable the BGP routes learned by the enterprise router through the virtual gateway attachments to work as equal-cost routes.

   For details, see **Associating a Route Policy with the Propagation of an Attachment**.
3. Perform **Step 1** again to verify that load balancing is implemented among routes.

NOTICE

Configuring a route policy to replace the AS_Path of a route may cause network loops. Before configuring a route policy, check your network plan.

Step 3 Log in to the on-premises network device and configure the routes from the on-premises data center to the enterprise router as equal-cost routes based on your network plan for load balancing.

----End

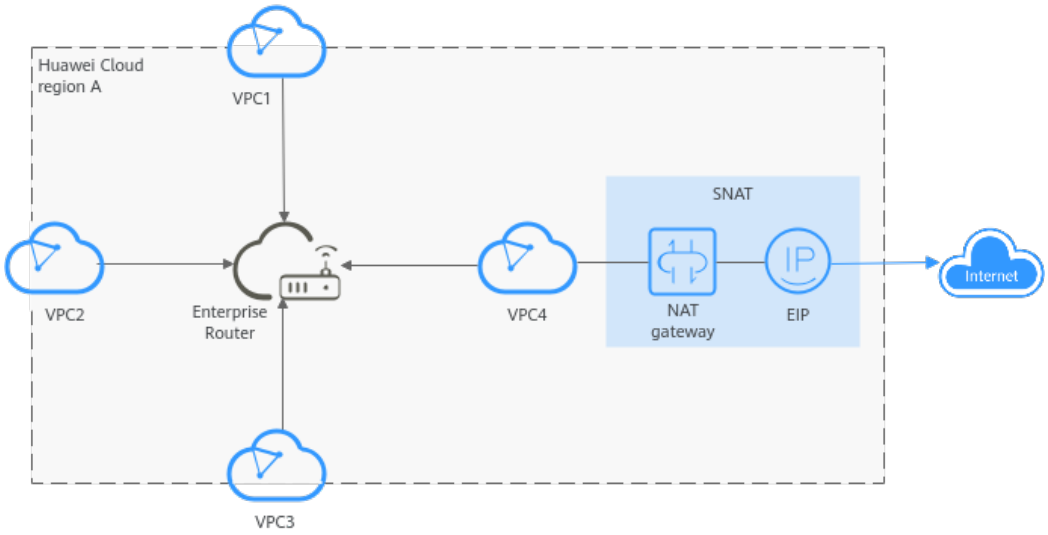
9 Using Enterprise Router and NAT Gateway to Allow VPCs to Share an EIP to Access the Internet

9.1 Overview

Background

There are four VPCs in region A on Huawei Cloud. VPC 1, VPC 2, and VPC 3 need to communicate with each other, and share an EIP through an SNAT rule of a NAT gateway in VPC 4 to access the Internet.

Figure 9-1 VPCs sharing an EIP through an SNAT rule



NOTE

You can **share an enterprise router** with different accounts to attach VPCs of these accounts to the same enterprise router for communications.

Operation Procedure

Figure 9-2 shows the procedure for using an enterprise router and a NAT gateway to allow VPCs in the same region to share an EIP to access the Internet.

Figure 9-2 Flowchart for enabling VPCs in the same region to share an EIP to access the Internet

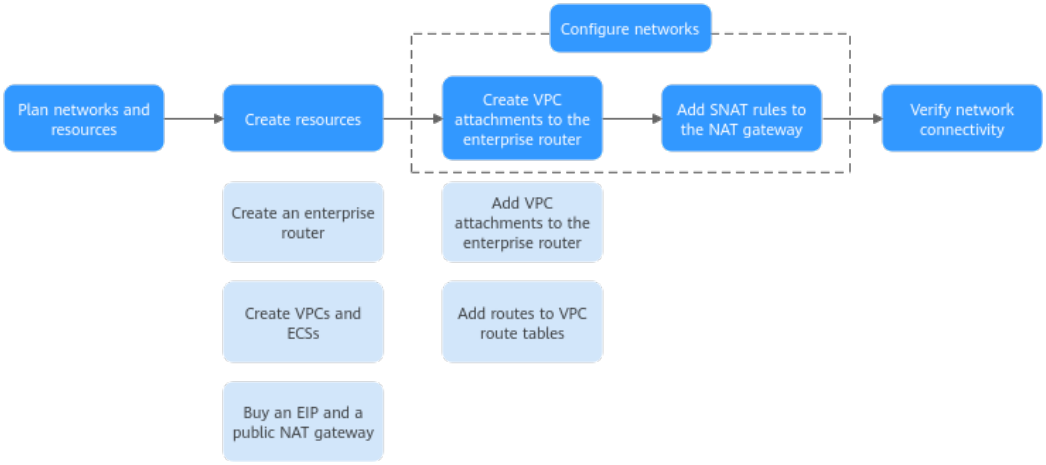


Table 9-1 Description of procedures for enabling VPCs in the same region to share an EIP to access the Internet

No.	Procedure	Description
1	Planning Networks and Resources	Plan required CIDR blocks and the number of resources.
2	Creating Resources	1. Create an enterprise router. 2. Create four VPCs and three ECSs. One of the VPCs will be used to host a NAT gateway 3. Assign an EIP and create a public NAT gateway in VPC 4.
3	Configuring Networks	1. Create VPC attachments for the enterprise router: a. Attach the four VPCs to the enterprise router. b. Add routes to the route tables of the VPCs for traffic to route through the enterprise router. 2. Add SNAT rules for the VPCs to the NAT gateway.
4	Verifying Network Connectivity	Log in to an ECS and run the **ping** command to verify the network connectivity.

9.2 Planning Networks and Resources

To use an enterprise router and a NAT gateway to allow VPCs in the same region to share an EIP to access the Internet, you need:

- **Network Planning**: Plan CIDR blocks of VPCs and their subnets, EIP, public NAT gateway, and route tables of VPCs and the enterprise router.
- **Resource Planning**: Plan the quantity, names, and other parameters of cloud resources, including VPCs, EIP, NAT gateway, ECSs, and enterprise router.

Network Planning

Figure 9-3 and **Table 9-3** show the network planning and its description for enabling VPCs in the same region to share an EIP to access the Internet.

Figure 9-3 Network planning for enabling VPCs in the same region to share an EIP to access the Internet

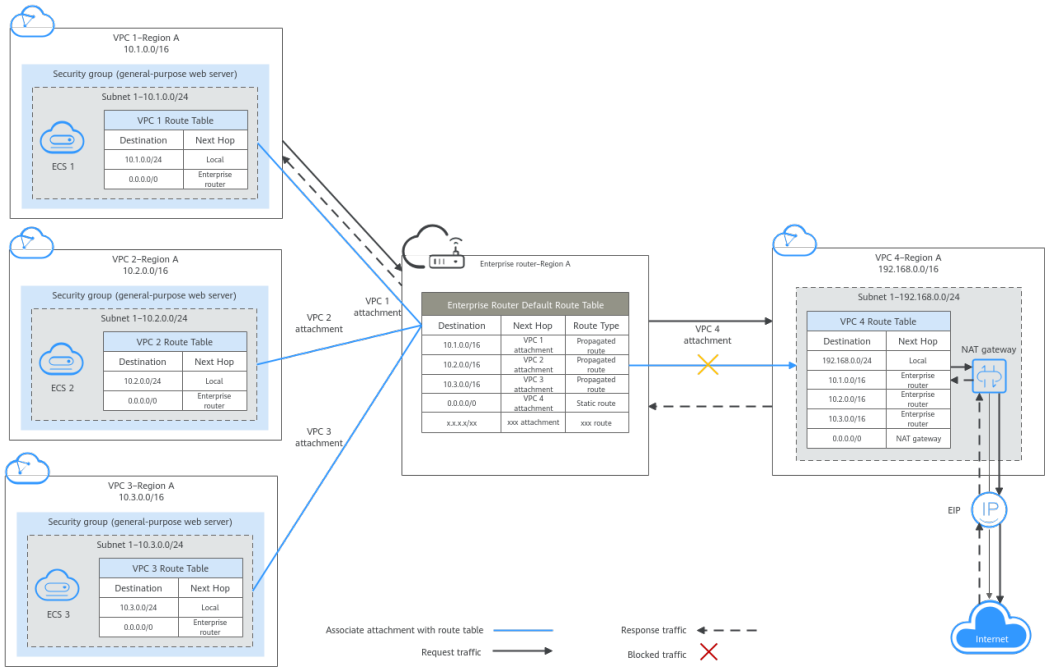


Table 9-2 Network traffic flows

Path	Description
Request traffic: from VPC 1 to Internet	1. The route table of VPC 1 has a route with the next hop set to the enterprise router to forward traffic from VPC 1 to the enterprise router. 2. The route table of the enterprise router has a static route with the next hop set to the VPC 4 attachment to forward traffic from the enterprise router to VPC 4. 3. The route table of VPC 4 has a route with the next hop set to the NAT gateway to forward traffic from VPC 4 to the NAT gateway. 4. The NAT gateway forwards the traffic to a destination on the Internet through the EIP configured in an SNAT rule.
Response traffic: from Internet to VPC 1	1. The destination on the Internet forwards the traffic to the NAT gateway through the EIP configured in the SNAT rule. 2. The NAT gateway forwards the traffic to VPC 4 based on the SNAT rule. 3. The route table of VPC 4 has routes with the next hop set to the enterprise router to forward traffic from VPC 4 to the enterprise router. 4. The route table of the enterprise router has a propagated route with the next hop set to the VPC 1 attachment to forward traffic from the enterprise router to VPC 1.

Table 9-3 Description of network planning for enabling VPCs in the same region to share an EIP to access the Internet

Resource	Description
VPCs	• The CIDR blocks of the VPCs to be connected cannot overlap with each other. In this example, the CIDR blocks of the VPCs are propagated to the enterprise router route table as the destination in routes. The CIDR blocks cannot be modified and overlapping CIDR blocks may cause route conflicts. If your existing VPCs have overlapping CIDR blocks, do not use propagated routes. Instead, you need to manually add static routes to the route table of the enterprise router. The destination can be VPC subnet CIDR blocks or smaller ones. • Each VPC has a default route table. • The routes in the default route table are described as follows: – Local: a system route for communications between subnets in a VPC. – Enterprise Router: a custom route for routing traffic from a VPC subnet to the enterprise router. In order to keep route configuration simple, VPC 1, VPC 2 and VPC 3 each have such a route with destination set to 0.0.0.0/0. For route details, see **Table 9-4**. The route table of VPC 4 has a route with NAT gateway as the next hop and 0.0.0.0/0 as the destination. To prevent conflicts with this route, set the destinations to CIDR blocks of the other three VPCs for routes with enterprise router as the next hop in this route table. For route details, see **Table 9-5**. – NAT gateway: a route configured by the system for routing traffic from the VPC subnet to the NAT gateway.
NAT gateway	Create a public NAT gateway in VPC 4, and add an SNAT rule with an EIP associated.
Enterprise router	• After **Default Route Table Association** and **Default Route Table Propagation** are enabled and VPC attachments are created, Enterprise Router will automatically: – Associate VPC attachments with the default route table of the enterprise router. – Propagate VPC attachments to the default route table of the enterprise router. The route table automatically learns the VPC CIDR blocks as the destination of routes. For details, see **Table 9-6**. • Add a static route to enterprise router route table with destination set to 0.0.0.0/0 for routing traffic for accessing the Internet through VPC 4.

Resource	Description
ECSs	The three ECSs are in different VPCs. If the ECSs are in different security groups, add rules to the security groups to allow access to each other.

Table 9-4 Route table for VPC 1, VPC 2, and VPC 3

Destination	Next Hop	Route Type
0.0.0.0/0	Enterprise router	Static route (custom)

NOTE

- If you enable **Auto Add Routes** when creating a VPC attachment, you do not need to manually add static routes to the VPC route table. Instead, the system automatically adds routes (with this enterprise router as the next hop and 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations) to all route tables of the VPC.
- If an existing route in the VPC route tables has a destination to 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16, the routes will fail to be added. In this case, do not to enable **Auto Add Routes**. After the attachment is created, manually add routes.
- You need to add a route to VPC route tables with destination set to a CIDR block on the Internet and next hop set to enterprise router.
- To reduce the number of routes, you can set the destination of a route (with an enterprise router as the next hop) to 0.0.0.0/0 in the VPC route table. However, in this case, ECSs in VPCs cannot be bound with EIPs. If an ECS in the VPC has an EIP bound, the VPC route table will have a policy-based route with 0.0.0.0/0 as the destination, which has a higher priority than the route with the enterprise router as the next hop. In this case, traffic is forwarded to the EIP and cannot reach the enterprise router.

Table 9-5 VPC 4 route table

Destination	Next Hop	Route Type
VPC 1 CIDR block: 10.1.0.0/16	Enterprise router	Static route (custom)
VPC 2 CIDR block: 10.2.0.0/16	Enterprise router	Static route (custom)
VPC 3 CIDR block: 10.3.0.0/16	Enterprise router	Static route (custom)
0.0.0.0/0	NAT gateway	Static route (custom)

NOTE

- Do not enable **Auto Add Routes** when creating attachments. Manually add routes to VPC route tables after the attachments are created.
- Do not bind an EIP to an ECS in VPCs. If you do that, policy-based routes with destination set to 0.0.0.0/0 are added to ECS route tables. The priority of the routes is higher than that of the route with destination to the NAT gateway. As a result, the traffic will be forwarded to the EIP of the ECS instead of the NAT gateway.

Table 9-6 Enterprise router route table

Destination	Next Hop	Route Type
VPC 1 CIDR block: 10.1.0.0/16	VPC 1 attachment: er-attach-business-01	Propagated route
VPC 2 CIDR block: 10.2.0.0/16	VPC 2 attachment: er-attach-business-02	Propagated route
VPC 3 CIDR block: 10.3.0.0/16	VPC 3 attachment: er-attach-business-03	Propagated route
0.0.0.0/0	VPC 4 attachment: er-attach-nat	Static route

Resource Planning

An enterprise router, a NAT gateway, an EIP, four VPCs, and three ECSs are in the same region but can be in different AZs.

NOTE

The following resource details are only examples. You can modify them as required.

- One enterprise router. See details in **Table 9-7**.

Table 9-7 Enterprise router details

Enterprise Router Name	ASN	Default Route Table Association	Default Route Table Propagation	Association Route Table	Propagation Route Table	Attachment
er-test-01	64512	Enabled	Enabled	Default route table	Default route table	er-attach-business-01
						er-attach-business-02

Enterprise Router Name	ASN	Default Route Table Association	Default Route Table Propagation	Association Route Table	Propagation Route Table	Attachment
						er-attach-business-03
						er-attach-nat

- One EIP. Set the EIP type and bandwidth size as required. In this practice, the EIP is 123.60.73.78.
- One public NAT gateway. See details in **Table 9-8**.

Table 9-8 Public NAT gateway details

Public NAT Gateway Name	VPC Name	Subnet Name	SNAT Rule Scenario	SNAT Rule CIDR Block
nat-demo	vpc-nat	subnet-nat	VPC	Custom: 0.0.0.0/0

- Four VPCs that do not overlap with each other. See details in **Table 9-9**.

Table 9-9 VPC details

VPC Name	VPC CIDR Block	Subnet Name	Subnet CIDR Block	Association Route Table
vpc-business-01	10.1.0.0/16	subnet-business-01	10.1.0.0/24	Default route table
vpc-business-02	10.2.0.0/16	subnet-business-02	10.2.0.0/24	Default route table
vpc-business-03	10.3.0.0/16	subnet-business-03	10.3.0.0/24	Default route table
vpc-nat	192.168.0.0/16	subnet-nat	192.168.0.0/24	Default route table

- Three ECSs, respectively, in three VPCs. See details in **Table 9-10**.

Table 9-10 ECS details

ECS Name	Image	VPC Name	Subnet Name	Security Group	Private IP Address
ecs-business-01	Public image: CentOS 7.5 64-bit	vpc-business-01	subnet-business-01	sg-demo (general-purpose web server)	10.1.0.134
ecs-business-02		vpc-business-02	subnet-business-02		10.2.0.215
ecs-business-03		vpc-business-03	subnet-business-03		10.3.0.14

9.3 Creating Resources

9.3.1 Creating an Enterprise Router

Scenarios

This section describes how to create an enterprise router.

Procedure

Step 1 Create an enterprise router in region A.

For details, see **Creating an Enterprise Router**.

For enterprise router details, see **Table 9-7**.

----End

9.3.2 Creating VPCs and ECSs

Scenarios

This section describes how to create VPCs and ECSs.

Procedure

Step 1 Create four VPCs and three ECSs in region A.

For details, see **Creating a VPC**.

For details, see **Overview**.

- For details about VPC and subnet planning, see **Table 9-9**.

- For details about ECS planning, see **Table 9-10**.

----End

9.3.3 Assigning an EIP and Creating a Public NAT Gateway

Scenarios

This section describes how to assign an EIP and create a public NAT gateway.

Procedure

Step 1 Assign an EIP in region A.

For details, see **Assigning an EIP**.

Step 2 Create a public NAT gateway in region A.

For details, see **Buying a Public NAT Gateway**.

For public NAT gateway planning, see **Table 9-8**.

----End

9.4 Configuring Networks

9.4.1 Creating VPC Attachments for the Enterprise Router

Scenarios

This section describes how to attach VPCs to the enterprise router and configure routes for the VPCs and enterprise router.

Procedure

Step 1 Attach the four VPCs to the enterprise router.

For details, see **Creating VPC Attachments to the Enterprise Router**.

Default Route Table Association and **Default Route Table Propagation** are enabled when you create the enterprise router. After VPCs are attached to the enterprise router, the system will automatically:

- Associate the VPC attachments with the default route table of the enterprise router.
- Propagate the VPC attachments to the default route table of the enterprise router. The route table automatically learns the VPC CIDR blocks as the destination of routes.

Step 2 Add a static route to enterprise router route table with the next hop set to the VPC 4 attachment and destination to 0.0.0.0/0 for accessing the Internet through VPC 4.

For details, see **Creating a Static Route**.

After the static route with the next hop set to VPC 4 is created, you can delete the propagated route. For details, see **Deleting a Propagation**.

Step 3 Add routes to VPC route tables for traffic to route through the enterprise router.

For details, see **Adding Routes to VPC Route Tables**.

- For route details, see **Table 9-4**.
- For VPC 4 route details, see **Table 9-5**.

----End

9.4.2 Adding an SNAT Rule to the NAT Gateway

Scenarios

This section describes how to add an SNAT rule to the public NAT gateway.

Procedure

Step 1 Add an SNAT rule to the public NAT gateway.

For details, see **Adding an SNAT Rule**.

For SNAT rule details, see **Table 9-8**.

----End

9.5 Verifying Network Connectivity

Scenarios

This section describes how to log in to ECSs and verify the connectivity between VPCs.

Procedure

Step 1 Log in to the ECS.

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 2 Verify the network connectivity.

1. Verify the network connectivity between VPCs.

   ping *IP address of the ECS*

   To verify whether vpc-business-01 can communicate with vpc-business-02 and vpc-business-03, log in to ecs-business-01 and run the following commands:

   ping 10.2.0.215

   ping 10.3.0.14

If information similar to the following is displayed, vpc-business-01 can communicate with vpc-business-02 and vpc-business-03.

```
PING 10.2.0.215 (10.2.0.215) 56(84) bytes of data.
64 bytes from 10.2.0.215: icmp_seq=1 ttl=64 time=0.460 ms
64 bytes from 10.2.0.215: icmp_seq=2 ttl=64 time=0.358 ms
64 bytes from 10.2.0.215: icmp_seq=3 ttl=64 time=0.345 ms
64 bytes from 10.2.0.215: icmp_seq=4 ttl=64 time=0.303 ms
64 bytes from 10.2.0.215: icmp_seq=5 ttl=64 time=0.289 ms
64 bytes from 10.2.0.215: icmp_seq=6 ttl=64 time=0.262 ms
64 bytes from 10.2.0.215: icmp_seq=7 ttl=64 time=0.297 ms
^C
--- 10.2.0.215 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 0.262/0.330/0.460/0.064 ms
```

```
PING 10.3.0.14 (10.3.0.14) 56(84) bytes of data.
64 bytes from 10.3.0.14: icmp_seq=1 ttl=64 time=0.900 ms
64 bytes from 10.3.0.14: icmp_seq=2 ttl=64 time=1.87 ms
64 bytes from 10.3.0.14: icmp_seq=3 ttl=64 time=0.323 ms
64 bytes from 10.3.0.14: icmp_seq=4 ttl=64 time=0.315 ms
64 bytes from 10.3.0.14: icmp_seq=5 ttl=64 time=0.296 ms
64 bytes from 10.3.0.14: icmp_seq=6 ttl=64 time=0.286 ms
64 bytes from 10.3.0.14: icmp_seq=7 ttl=64 time=0.281 ms
^C
--- 10.3.0.14 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 0.281/0.610/1.874/0.556 ms
```

2. Verify whether a VPC can access the Internet.

   ping *public IP address or domain name*

   To verify that the vpc-business-01 can communicate with the Internet, log in to ecs-isolation-01 and run the following command:

   ping support.huaweicloud.com

   If information similar to the following is displayed, vpc-business-01 can communicate with the Internet.

```
[root@ecs-[redacted] ~]$ ping support.huaweicloud.com
PING cdn-p1mz674n.sched.s2.tdnsv5.com (117.41.241.211) 56(84) bytes of data.
64 bytes from 117.41.241.211 (117.41.241.211): icmp_seq=1 ttl=52 time=17.10 ms
64 bytes from 117.41.241.211 (117.41.241.211): icmp_seq=2 ttl=52 time=17.7 ms
64 bytes from 117.41.241.211 (117.41.241.211): icmp_seq=3 ttl=52 time=17.6 ms
64 bytes from 117.41.241.211 (117.41.241.211): icmp_seq=4 ttl=52 time=17.8 ms
64 bytes from 117.41.241.211 (117.41.241.211): icmp_seq=5 ttl=52 time=17.7 ms
64 bytes from 117.41.241.211 (117.41.241.211): icmp_seq=6 ttl=52 time=17.6 ms
64 bytes from 117.41.241.211 (117.41.241.211): icmp_seq=7 ttl=52 time=17.7 ms
^C
--- cdn-p1mz674n.sched.s2.tdnsv5.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 8ms
rtt min/avg/max/mdev = 17.636/17.716/17.951/0.144 ms
```

Step 3 Repeat **Step 1** to **Step 2** to verify the network connectivity of other VPCs.

----End

10 Using an Enterprise Router to Replace VPC Peering Connections

10.1 Overview

Scenario

Before enterprise routers are available, VPC peering connections are used to connect different VPCs in the same region. VPC peering connections are suitable for simple networks because every two VPCs need a VPC peering connection. In a complex network, a large number of VPC peering connections are required, which is inconvenient for network expansion and increases O&M costs.

As a high-performance centralized router on the cloud, an enterprise router can connect multiple VPCs in the same region, making network expansion and O&M easier.

If you have a lot of VPCs that are connected by VPC peering connections, you can use an enterprise router to replace the VPC peering connections.

NOTE

For details, see **Enterprise Router Service Overview**.

Architecture

VPC-A, VPC-B, and VPC-C are in region A and connected over VPC peering connections. To improve network scalability and reduce O&M costs, you can use an enterprise router to connect the three VPCs.

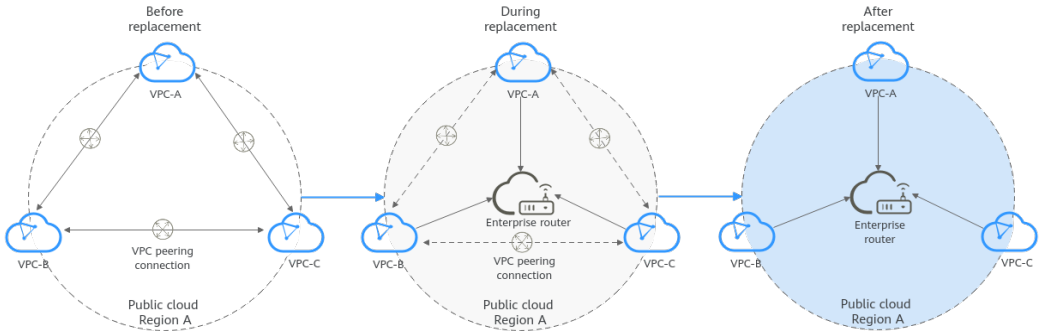
This process consists of three phases: before replacement, during replacement, and after replacement. The details are as follows:

1. Before the replacement, VPC-A, VPC-B, and VPC-C are connected through VPC peering connections.
2. During the replacement, VPC-A, VPC-B, and VPC-C will be connected through both VPC peering connections and an enterprise router. Large and small CIDR

blocks are used to ensure that the routes of VPC peering connections and the enterprise router do not conflict.

3. After the replacement, VPC-A, VPC-B, and VPC-C can communicate with each other through the enterprise router and you can delete the VPC peering connections.

Figure 10-1 Replacing VPC peering connections with an enterprise router

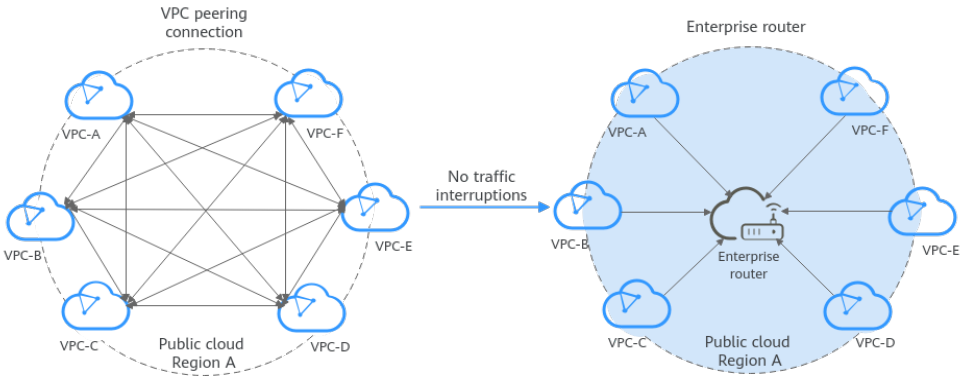


Advantages

Simplified networking structure, improved scalability, and reduced O&M costs

As shown in **Figure 10-2**, the networking of VPCs connected by VPC peering connections is more complex than that of an enterprise router. For example, if you have six VPCs, you need to create 15 VPC peering connections. But if you use an enterprise router, one router can connect all of your VPCs. The networking is simple and clear, making O&M and network expansion easier.

Figure 10-2 Networking using VPC peering connections and an enterprise router



Notes and Constraints

- If the VPCs connected by VPC peering connections are from different accounts, you can use **the sharing function of the enterprise router** to connect the VPCs of different accounts through one enterprise router.
- Replacing VPC peering connections with an enterprise router may interrupt services. **Submit a service ticket** and contact customer service to evaluate the replacement solution. Here are some example scenarios that services may be interrupted.

- If resources in a service VPC have virtual IP addresses bound, the service VPC cannot be attached to an enterprise router.
- If a service VPC is being used by ELB, VPC Endpoint, NAT Gateway (private NAT gateway), Distributed Cache Service (DCS), or hybrid DNS, this VPC cannot be attached to an enterprise router.

For details about constraints on enterprise routers, see **Notes and Constraints**.

10.2 Planning Networks and Resources

Plan required resources and networking before, during, and after the replacement.

- **Network Planning**: Plan CIDR blocks of VPCs and their subnets, and route tables of VPCs and the enterprise router.
- **Resource Planning**: Plan the quantity, names, and other parameters of cloud resources, including VPCs, ECSs, and the enterprise router.

Network Planning

During the replacement, in addition to adding routes for communications among enterprise router and VPCs, you also need to add routes for verification and temporary communications. After the replacement is complete, you can delete unnecessary routes. For details about the networking planning, see **Table 10-1**.

The following figures show the networking in different replacement phases.

- **Figure 10-3**
- **Figure 10-4**
- **Figure 10-5**

NOTE

The routes in the figures are only examples for your reference. You need to plan routes based on service requirements.

Figure 10-3 Networking topology before replacement

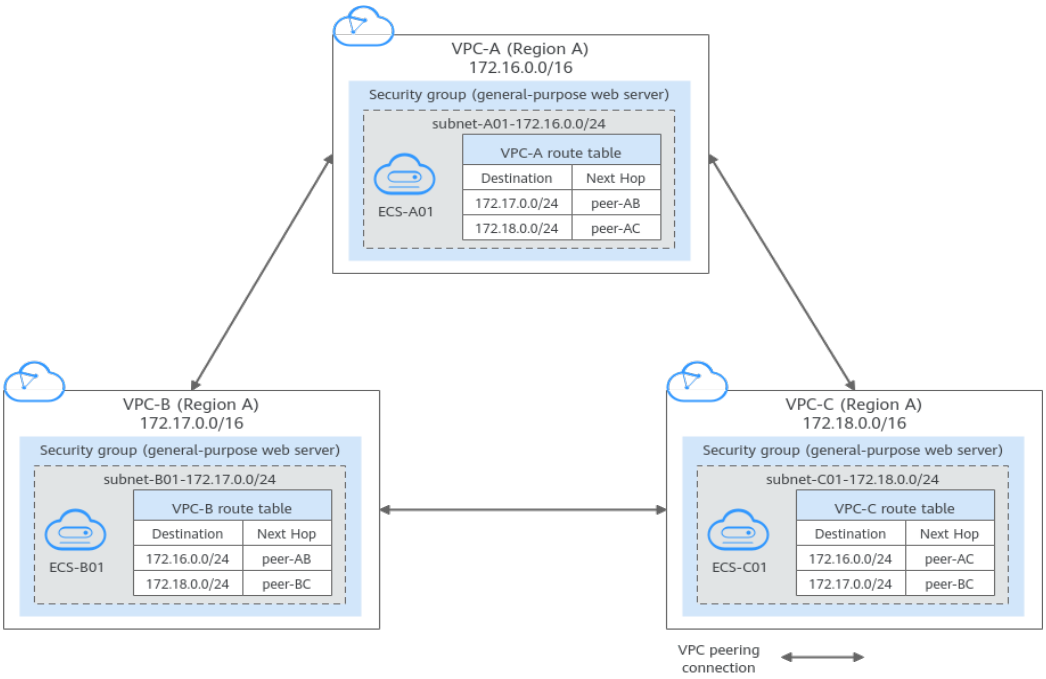


Figure 10-4 Networking topology during replacement

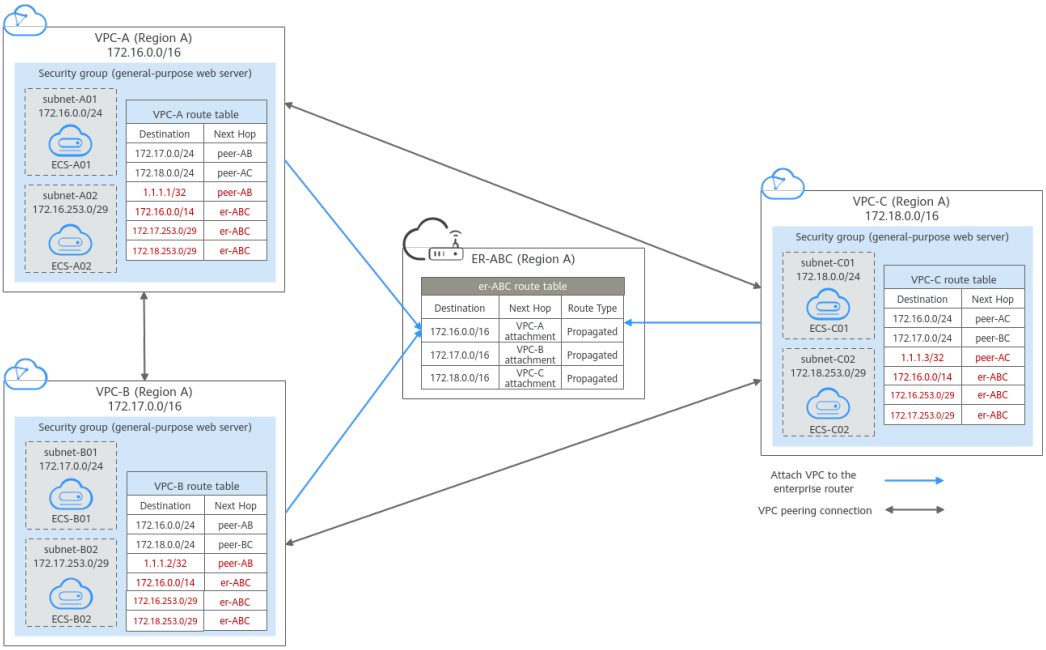


Figure 10-5 Networking topology after replacement

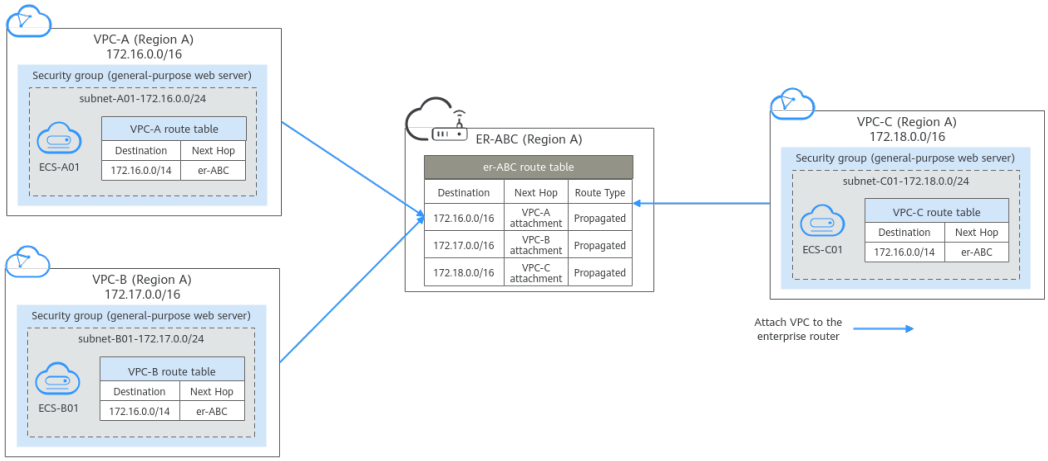


Table 10-1 Networking planning for replacing VPC peering connections with an enterprise router

Route Table	Description
VPC route table	Table 10-2 lists the routes in this route table. 1. Before the replacement, the destination of the route with next hop set to VPC peering connection is a CIDR block of a VPC subnet. This only connects specific subnets of VPCs. 2. During the replacement, add routes as follows: • The routes for temporary communications ensure that traffic is not interrupted when original routes added for VPC peering connections are deleted. The next hop of the routes can be any VPC peering connection of the VPC. The route destinations cannot be used by any other services. You can set the destinations to those that are rarely used. In this example, the destinations are 1.1.1.1/32, 1.1.1.2/32, and 1.1.1.3/32. • The routes with destination set to a large CIDR block and next hop to the enterprise router is used for communications between the VPCs and enterprise router. The route destination must contain CIDR blocks of all VPCs that need to communicate with each other and cannot be used by any other services. In this example, the destination is 172.16.0.0/14, containing three VPC CIDR blocks, 172.16.0.0/16, 172.17.0.0/16, and 172.18.0.0/16. • The routes with next hop set to the enterprise router are used for communications between the VPCs and enterprise router. The route destinations cannot contain CIDR blocks configured for VPC peering connections and are not used to allow communications through VPC peering connections. In this example, the destinations are 172.16.253.0/29, 172.17.253.0/29, and 172.18.253.0/29. **NOTICE** • The routes for temporary communications are necessary to ensure that traffic is not interrupted when original routes added for VPC peering connections are deleted. Traffic is not interrupted only for the replacement solution described in this document. Before your actual replacement, traffic may be interrupted. Contact customer service to evaluate the replacement solution. • The routes with destination set to a large CIDR block must contain CIDR blocks of all VPCs that need to communicate with each other. If one large CIDR block cannot contain all VPC CIDR blocks, you can configure more large CIDR blocks.

Route Table	Description
	3. After the replacement, delete the routes for verification and temporary communications. **NOTICE** After the replacement, you can continue to use the routes with destinations of large CIDR blocks or add routes with destinations that are the same as those of the original routes and then delete the routes with destinations of large CIDR blocks.
Enterprise router route table	Table 10-3 lists the routes in this route table. During the replacement, add routes that with destinations set to VPC CIDR blocks to allow communications among the enterprise router and VPCs. If **Default Route Table Association** and **Default Route Table Propagation** are enabled for the enterprise router, routes with destinations set to VPC CIDR blocks are automatically added when you attach the VPCs to the enterprise router. **CAUTION** If the CIDR blocks of VPCs connected by a VPC peering connection overlap, do not enable **Default Route Table Propagation** for the enterprise router. This function adds routes with entire VPC CIDR blocks as destinations. If VPC CIDR blocks overlap, there will be route conflicts. In this case, you need to manually add routes with next hop set to VPC attachment to the route table of the enterprise router.

Table 10-2 VPC route table details

VPC	VPC Route Table	Destination	Next Hop Type	Next Hop	Route Type	Route Function	Required
VPC-A	rtb-vpc-A	172.17.0.0/24	VPC peering connection	peer-AB	Custom	• Destination: subnet-B01 in VPC-B • Connects subnet-A01 to subnet-B01	Before/During replacement
		172.18.0.0/24	VPC peering connection	peer-AC	Custom	• Destination: subnet-C01 in VPC-C • Connects subnet-A01 to subnet-C01	Before/During replacement

VPC	VPC Route Table	Destination	Next Hop Type	Next Hop	Route Type	Route Function	Required
		1.1.1.1/32	VPC peering connection	peer-AB	Custom	• Destination: Any IP address that is not used by other services • Ensures that traffic flowing through VPC peering connections is not interrupted during the replacement.	During replacement
		172.16.0.0/14	Enterprise router	er-ABC	Custom	• Destination: A large CIDR block that can contain CIDR blocks of the three VPCs • Connects VPC-A to er-ABC	During/After replacement
		172.17.253.0/29	Enterprise router	er-ABC	Custom	• Destination: subnet-B02 in VPC-B • Connects subnet-B02 to er-ABC	During replacement
		172.18.253.0/29	Enterprise router	er-ABC	Custom	• Destination: subnet-C02 in VPC-C • Connects subnet-C02 to er-ABC	During replacement
VPC-B	rtb-vpc-B	172.16.0.0/24	VPC peering connection	peer-AB	Custom	• Destination: subnet-A01 in VPC-A • Connects subnet-A01 to subnet-B01	Before/During replacement

VPC	VPC Route Table	Destination	Next Hop Type	Next Hop	Route Type	Route Function	Required
		172.18.0.0/24	VPC peering connection	peer-BC	Custom	• Destination: subnet-C01 in VPC-C • Connects subnet-B01 to subnet-C01	Before/During replacement
		1.1.1.2/32	VPC peering connection	peer-AB	Custom	• Destination: Any IP address that is not used by other services • Ensures that traffic flowing through VPC peering connections is not interrupted during the replacement.	During replacement
		172.16.0.0/14	Enterprise router	er-ABC	Custom	• Destination: A large CIDR block that can contain CIDR blocks of the three VPCs • Connects VPC-B to er-ABC	During/After replacement
		172.16.253.0/29	Enterprise router	er-ABC	Custom	• Destination: subnet-A02 in VPC-A • Connects subnet-A02 to er-ABC	During replacement
		172.18.253.0/29	Enterprise router	er-ABC	Custom	• Destination: subnet-C02 in VPC-C • Connects subnet-C02 to er-ABC	During replacement

VPC	VPC Route Table	Destination	Next Hop Type	Next Hop	Route Type	Route Function	Required
VPC-C	rtb-vpc-C	172.16.0.0/24	VPC peering connection	peer-AC	Custom	• Destination: subnet-A01 in VPC-A • Connects subnet-A01 to subnet-C01	Before/During replacement
		172.17.0.0/24	VPC peering connection	peer-BC	Custom	• Destination: subnet-B01 in VPC-B • Connects subnet-B01 to subnet-C01	Before/During replacement
		1.1.1.3/32	VPC peering connection	peer-AC	Custom	• Destination: Any IP address that is not used by other services • Ensures that traffic flowing through VPC peering connections is not interrupted during the replacement.	During replacement
		172.16.0.0/14	Enterprise router	er-ABC	Custom	• Destination: A large CIDR block that can contain CIDR blocks of the three VPCs • Connects VPC-C to er-ABC	During/After replacement
		172.16.253.0/29	Enterprise router	er-ABC	Custom	• Destination: subnet-A02 in VPC-A • Connects subnet-A02 to er-ABC	During replacement

VPC	VPC Route Table	Destination	Next Hop Type	Next Hop	Route Type	Route Function	Required
		172.17.253.0/29	Enterprise router	er-ABC	Custom	• Destination: subnet-B02 in VPC-B • Connects subnet-B02 to er-ABC	During replacement

Table 10-3 Details of the enterprise router route table

Enterprise Router	Route Table	Destination	Next Hop	Attached Resource	Route Type	Route Function	Required
er-ABC	defaultRouteTable	172.16.0.0/16	er-attach-A	VPC-A	Propagated	• Destination: VPC-A • Connects VPC-A to er-ABC	During/After replacement
		172.17.0.0/16	er-attach-B	VPC-B	Propagated	• Destination: VPC-B • Connects VPC-B to er-ABC	During/After replacement
		172.18.0.0/16	er-attach-C	VPC-C	Propagated	• Destination: VPC-C • Connects VPC-C to er-ABC	During/After replacement

Resource Planning

Table 10-4 lists the enterprise router and also resources that are temporarily required and can be deleted after the replacement.

NOTE

The following resource planning details are only examples for your reference. You need to plan resources based on service requirements.

Table 10-4 Resource planning for replacing VPC peering connections with an enterprise router

Resource	Description
VPC	Table 10-5 shows details about the required VPCs. • Before the replacement, there are three VPCs. Each VPC has a subnet that is associated with the default VPC route table. • During the replacement, create one more subnet that is not used by any services in each VPC. These subnets cannot communicate with each other through VPC peering connections and are used for communications between the VPCs and enterprise router. • After the replacement, delete the subnets that are used for verifying communications.
VPC peering connection	Table 10-6 shows details about the required VPC peering connections. After the replacement, delete the VPC peering connections.
ECS	Table 10-7 shows details about the required ECSs. • Before the replacement, there are three ECSs that are running services. • During the replacement, create one more ECS in each verification subnet for communications between the VPCs and enterprise router. • After the replacement, delete the ECSs in verification subnets.
Enterprise router	The enterprise router and the VPC peering connections are in the same region. Table 10-8 shows details about the enterprise router. During the replacement, create an enterprise router and three VPC attachments. Table 10-9 shows details about the VPC attachments. • Enable **Default Route Table Association** and **Default Route Table Propagation** when you create the enterprise router to automatically add routes. **CAUTION** If the CIDR blocks of VPCs connected by a VPC peering connection overlap, do not enable **Default Route Table Propagation** for the enterprise router. This function adds routes with entire VPC CIDR blocks as destinations. If VPC CIDR blocks overlap, there will be route conflicts. In this case, you need to manually add routes with next hop set to VPC attachment to the route table of the enterprise router. • Do not enable **Auto Add Routes** when you create the three VPC attachments. If this option is enabled, Enterprise Router automatically adds routes (with this enterprise router as the next hop and 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations) to all route tables of the VPC. During the replacement, manually add routes with destinations set to the large CIDR block to the VPC route tables.

Table 10-5 VPC details

VPC Name	VPC CIDR Block	Subnet Name	Subnet CIDR Block	Association Route Table	Subnet Is Used to	Required
VPC-A	172.16.0.0/16	subnet-A01	172.16.0.0/24	Default route table	Deploy services.	During/After replacement
		subnet-A02	172.16.253.0/29	Default route table	Verify the communications between the VPC and the enterprise router.	During replacement
VPC-B	172.17.0.0/16	subnet-B01	172.17.0.0/24	Default route table	Deploy services.	During/After replacement
		subnet-B02	172.17.253.0/29	Default route table	Verify the communications between the VPC and the enterprise router.	During replacement
VPC-C	172.18.0.0/16	subnet-C01	172.18.0.0/24	Default route table	Deploy services.	During/After replacement
		subnet-C02	172.18.253.0/29	Default route table	Verify the communications between the VPC and the enterprise router.	During replacement

Table 10-6 VPC peering connection details

Connection Name	Local VPC	Peer VPC	Connection Is Used to	Required
peer-AB	VPC-A	VPC-B	Connect subnet-A01 in VPC-A to subnet-B01 in VPC-B.	Before/During replacement

Connection Name	Local VPC	Peer VPC	Connection Is Used to	Required
peer-AC	VPC-A	VPC-C	Connect subnet-A01 in VPC-A to subnet-C01 in VPC-C.	Before/During replacement
peer-BC	VPC-B	VPC-C	Connect subnet-B01 in VPC-B to subnet-C01 in VPC-C.	Before/During replacement

Table 10-7 ECS details

ECS	VPC	Subnet	Private IP Address	Image	Security Group	ECS Is Used to	Required
ecs-A01	VPC-A	subnet-A01	172.16.0.139	Public image: CentOS 8.2 64bit	sg-demo (general-purpose web server)	Run services.	Before/During/After replacement
ecs-A02	VPC-A	subnet-A02	172.16.253.3			Verify the communications between the VPC and the enterprise router.	During replacement
ecs-B01	VPC-B	subnet-B01	172.17.0.93			Run services.	Before/During/After replacement
ecs-B02	VPC-B	subnet-B02	172.17.253.4			Verify the communications between the VPC and the enterprise router.	During replacement
ecs-C01	VPC-C	subnet-C01	172.18.0.220			Run services.	Before/During/After replacement
ecs-C02	VPC-C	subnet-C02	172.18.253.5			Verify the communications between the VPC and the enterprise router.	During replacement

Table 10-8 Enterprise router details

Name	ASN	Default Route Table Association	Default Route Table Propagation	Auto Accept Shared Attachments	Association Route Table	Attachment	Required
er-ABC	64512	Enabled	Enabled If your VPC CIDR blocks overlap, do not enable this function.	Disabled If you want to connect VPCs of different accounts using an enterprise router, enable this function. For details, see **Sharing Overview**.	Default route table	er-attach-A	During/After replacement
						er-attach-B	
						er-attach-C	

Table 10-9 VPC attachment details

Name	Type	VPC	Subnet	Auto Add Routes	Required
er-attach-A	VPC	VPC-A	subnet-A01	Disabled	During/After replacement
er-attach-B		VPC-B	subnet-B01		
er-attach-C		VPC-C	subnet-C01		

10.3 Replacing VPC Peering with Enterprise Router

Table 10-10 describes the overall process of replacing VPC peering connections with an enterprise router.

Table 10-10 Process of replacing VPC peering connections with an enterprise router

Step	Description
Step 1: Create Cloud Resources	1. Create an enterprise router for connecting VPCs in the same region. 2. Create a verification subnet in each VPC. These subnets cannot communicate with each other through VPC peering connections, but can communicate through the enterprise router to verify the communications between the VPCs and enterprise router during the replacement. 3. Create an ECS in each verification subnet. Log in to the ECS and use **ping** to verify communications between the VPCs and enterprise router.
Step 2: Create VPC Attachments and Add Routes	1. Create VPC attachments to attach the three VPCs to the enterprise router. Do not enable **Auto Add Routes** and manually add routes with destinations set to large CIDR blocks to the VPC route tables. 2. Check the routes in the enterprise router route table. In this example, **Default Route Table Association** and **Default Route Table Propagation** are enabled for the enterprise router, and routes with destinations set to VPC CIDR blocks are automatically added when you attach the VPCs to the enterprise router.
Step 3: Verify communications Between the VPCs and Enterprise Router	1. Add routes with the next hop set to the enterprise router in the VPC route tables. These routes are used to verify communications between the VPCs and enterprise router. 2. Log in to each verification ECS and use **ping** to verify communications between the VPCs and enterprise router. 3. After the verification, delete the routes, ECSs, and subnets that are used for verifying communications.
Step 4: Add Routes to VPC Route Tables	1. Add routes for temporary communications to the VPC route tables. These routes ensure that traffic is not interrupted when original routes added for VPC peering connections are deleted. 2. Add routes with the next hop set to the enterprise router in the VPC route tables. These routes are used to verify communications between the VPCs and enterprise router.
Step 5: Perform the Replacement	Delete the original routes with the next hop set to the VPC peering connection from the VPC route tables. During the replacement, check the service traffic in real time. If traffic is interrupted, add the deleted routes immediately.

Step	Description
Step 6: Delete the Original VPC Peering Connections	After you have deleted original routes and verified that services are running properly, delete the VPC peering connections. This will also delete the routes for temporary communications from the VPC route tables.

10.4 Replacement Steps

Step 1: Create Cloud Resources

Table 10-4 lists all required cloud resources in this example.

Step 1 Create a subnet in each VPC.

The subnets are used to verify communications between the VPCs and enterprise router during the replacement. In this example, three verification subnets are required. For more resource details, see Table 10-5.

For details, see Creating a VPC.

Step 2 Create an ECS in each verification subnet.

In this example, three verification ECSs are required. For more resource details, see Table 10-7.

For details, see Overview.

Step 3 Create an enterprise router.

In this example, the CIDR blocks of VPCs connected by VPC peering connections do not overlap. Therefore, enable both **Default Route Table Association** and **Default Route Table Propagation** when creating the enterprise router. For more resource details, see Table 10-3.

CAUTION

If the CIDR blocks of VPCs connected by a VPC peering connection overlap, do not enable **Default Route Table Propagation** for the enterprise router. This function adds routes with entire VPC CIDR blocks as destinations. If VPC CIDR blocks overlap, there will be route conflicts. In this case, you need to manually add routes with next hop set to VPC attachment to the route table of the enterprise router.

For details, see Creating an Enterprise Router.

----End

Step 2: Create VPC Attachments and Add Routes

Step 1 Create three VPC attachments to attach the VPCs to the enterprise router.

Do not enable **Auto Add Routes** when creating the attachments. For more resource details, see Table 10-3.

NOTICE

If this option is enabled, Enterprise Router automatically adds routes (with this enterprise router as the next hop and 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations) to all route tables of the VPC. During the replacement, manually add routes with destinations set to the large CIDR block to the VPC route tables.

For details, see **Creating VPC Attachments to the Enterprise Router**.

Step 2 Check the routes with destinations set to the VPC CIDR blocks in the enterprise router route table.

In this example, **Default Route Table Association** and **Default Route Table Propagation** are enabled for the enterprise router, and routes with destinations set to VPC CIDR blocks are automatically added when you attach the VPCs to the enterprise router.

NOTICE

If **Default Route Table Propagation** is not enabled when creating the enterprise router, you need to manually add routes with destinations set to the VPC CIDR blocks to the enterprise router route table. For details, see **Creating a Static Route**.

Table 10-1 and **Table 10-3** lists the routes required.

To view enterprise routes, see **Viewing Routes**.

----End

Step 3: Verify communications Between the VPCs and Enterprise Router

Step 1 Add routes with the next hop set to the enterprise router in the VPC route tables.

For VPC route details, see **Table 10-1**.

For details, see **Adding Routes to VPC Route Tables**.

In this example, the routes to be added are required during the replacement in **Table 10-2** and have next hop set to the enterprise router.

- Add routes with destinations set to 172.17.253.0/29 and 172.18.253.0/29 to the route table of VPC-A.
- Add routes with destinations set to 172.16.253.0/29 and 172.18.253.0/29 to the route table of VPC-B.
- Add routes with destinations set to 172.16.253.0/29 and 172.17.253.0/29 to the route table of VPC-C.

Step 2 Verify communications between the VPCs and enterprise router.

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 the ECSs.

1. Log in to ecs-A02 to check whether VPC-A can communicate with VPC-B through the enterprise router.

   ping *Private IP address of ecs-B02*

   Example command:

   ping 172.17.253.4

   If information similar to the following is displayed, VPC-A can communicate with VPC-B through the enterprise router.

   ```
   [root@ecs-A02 ~]# ping 172.17.253.4
   PING 172.17.253.4 (172.17.253.4) 56(84) bytes of data.
   64 bytes from 172.17.253.4: icmp_seq=1 ttl=64 time=0.849 ms
   64 bytes from 172.17.253.4: icmp_seq=2 ttl=64 time=0.455 ms
   64 bytes from 172.17.253.4: icmp_seq=3 ttl=64 time=0.385 ms
   64 bytes from 172.17.253.4: icmp_seq=4 ttl=64 time=0.372 ms
   ...
   --- 172.17.253.4 ping statistics ---
   ```

2. Log in to ecs-A02 to check whether VPC-A can communicate with VPC-C through the enterprise router.

   ping *Private IP address of ecs-C02*

   Example command:

   ping 172.18.253.5

   If information similar to the following is displayed, VPC-A can communicate with VPC-C through the enterprise router.

   ```
   [root@ecs-A02 ~]# ping 172.18.253.5
   PING 172.18.253.5 (172.18.253.5) 56(84) bytes of data.
   64 bytes from 172.18.253.5: icmp_seq=1 ttl=64 time=0.849 ms
   64 bytes from 172.18.253.5: icmp_seq=2 ttl=64 time=0.455 ms
   64 bytes from 172.18.253.5: icmp_seq=3 ttl=64 time=0.385 ms
   64 bytes from 172.18.253.5: icmp_seq=4 ttl=64 time=0.372 ms
   ...
   --- 172.18.253.5 ping statistics ---
   ```

3. Log in to ecs-B02 to check whether VPC-B can communicate with VPC-C through the enterprise router.

   ping *Private IP address of ecs-C02*

   Example command:

   ping 172.18.253.5

   If information similar to the following is displayed, VPC-B can communicate with VPC-C through the enterprise router.

   ```
   [root@ecs-B02 ~]# ping 172.18.253.5
   PING 172.18.253.5 (172.18.253.5) 56(84) bytes of data.
   64 bytes from 172.18.253.5: icmp_seq=1 ttl=64 time=0.849 ms
   64 bytes from 172.18.253.5: icmp_seq=2 ttl=64 time=0.455 ms
   64 bytes from 172.18.253.5: icmp_seq=3 ttl=64 time=0.385 ms
   64 bytes from 172.18.253.5: icmp_seq=4 ttl=64 time=0.372 ms
   ...
   --- 172.18.253.5 ping statistics ---
   ```

Step 3 After the verification, delete the routes, ECSs, and subnets that are used for verifying communications.

1. Delete the routes that are used for verifying communications from the three VPC route tables.

   In this example, the routes to be deleted are the ones required during the replacement in **Table 10-2** and have next hop set to the enterprise router.

- Delete routes with destinations set to 172.17.253.0/29 and 172.18.253.0/29 from the route table of VPC-A.
- Delete routes with destinations set to 172.16.253.0/29 and 172.18.253.0/29 from the route table of VPC-B.
- Delete routes with destinations set to 172.16.253.0/29 and 172.17.253.0/29 from the route table of VPC-C.

To delete a route, refer to **Deleting a Route**.

2. Delete the ECSs deployed in the three verification subnets.

   In this example, delete ecs-A02, ecs-B02, and ecs-C02 that are listed in **Table 10-7**.

   To delete an ECS, refer to **How Can I Delete or Restart an ECS?**

3. Delete the three verification subnets.

   In this example, delete subnet-A02, subnet-B02, and subnet-C02 that are listed in **Table 10-5**.

   To delete a subnet, see **Deleting a Subnet**.

NOTICE

Before deleting a subnet, delete the ECSs in the subnet. Otherwise, the subnet cannot be deleted.

----End

Step 4: Add Routes to VPC Route Tables

For VPC route details, see **Table 10-1**.

Step 1 Add routes to the route tables of VPC-A, VPC-B, and VPC-C.

For details, see **Adding Routes to VPC Route Tables**.

1. Add routes that are used for temporary communications and have next hop set to VPC peering connection.

   These routes ensure that traffic is not interrupted when original routes added for VPC peering connections are deleted.

   In this example, the routes to be added are required during the replacement in **Table 10-2** and have next hop set to VPC peering connection.

   - Add a route with destination set to 1.1.1.1/32 to the route table of VPC-A.
   - Add a route with destination set to 1.1.1.2/32 to the route table of VPC-B.
   - Add a route with destination set to 1.1.1.3/32 to the route table of VPC-C.

2. Add routes with destination set to a large CIDR block and next hop set to enterprise router.

   The route destination must contain CIDR blocks of all VPCs that need to communicate with each other and cannot be used by any other services.

   In this example, the routes to be added are required during and after the replacement in **Table 10-2** and have next hop set to the enterprise router.

   - Add a route with destination set to 172.16.0.0/14 to the route table of VPC-A.

- Add a route with destination set to 172.16.0.0/14 to the route table of VPC-B.
- Add a route with destination set to 172.16.0.0/14 to the route table of VPC-C.

----End

Step 5: Perform the Replacement

Step 1 Delete the original routes with the next hop set to the VPC peering connection from the three VPC route tables.

In this example, the routes to be deleted are required before and during the replacement in **Table 10-2**.

- Delete routes with destinations set to 172.17.0.0/24 and 172.18.0.0/24 from the route table of VPC-A.
- Delete routes with destinations set to 172.16.0.0/24 and 172.18.0.0/24 from the route table of VPC-B.
- Delete routes with destinations set to 172.16.0.0/24 and 172.17.0.0/24 from the route table of VPC-C.

To delete a route, refer to **Deleting a Route**.

CAUTION

Log in to the ECSs where services are running and use **ping** to check whether the traffic is interrupted. If traffic is interrupted, add the deleted routes immediately.

----End

Step 6: Delete the Original VPC Peering Connections

NOTICE

After the replacement is complete and you have verified that services are running properly, delete the VPC peering connections.

Step 1 Delete the three VPC peering connections.

Deleting the VPC peering connections will also delete the routes for temporary communications in the VPC route tables.

- **Table 10-6** lists the details about the VPC peering connections to be deleted.
- Deleting the VPC peering connections will also delete the routes whose next hop is VPC peering connection and that are required during the replacement in **Table 10-2**.
  - Delete the route with destination set to 1.1.1.1/32 from the route table of VPC-A.
  - Delete the route with destination set to 1.1.1.2/32 from the route table of VPC-B.

- Delete the route with destination set to 1.1.1.3/32 from the route table of VPC-C.

To delete a VPC peering connection, see **Deleting a VPC Peering Connection**.

----End

11 Using Enterprise Router to Reconstruct a Network Connected Through Direct Connect

11.1 Overview

Scenario

Before Enterprise Router is launched, you can use Direct Connect to build a hybrid cloud network. If your on-premises data center needs to access multiple VPCs, you may need more than one Direct Connect connection to improve network reliability, which may result in the following problems:

- Multiple connections may lead to complex networking and incur higher O&M costs.
- Connections are independent of each other and cannot work in load balancing or active/standby mode.

To improve the reliability of your hybrid cloud network and reduce O&M costs, you can use an enterprise router to reconstruct the network.

NOTE

For details, see **Enterprise Router Service Overview**.

Architecture

Your on-premises data center can access VPC-X in region A over a Direct Connect connection that has a virtual gateway (VGW-A) and two virtual interfaces (VIF-A01 and VIF-A02). To improve the reliability of your hybrid cloud network and reduce O&M costs, you can migrate the network by replacing Direct Connect with Enterprise Router.

This process consists of three phases: before migration, during migration, and after migration.

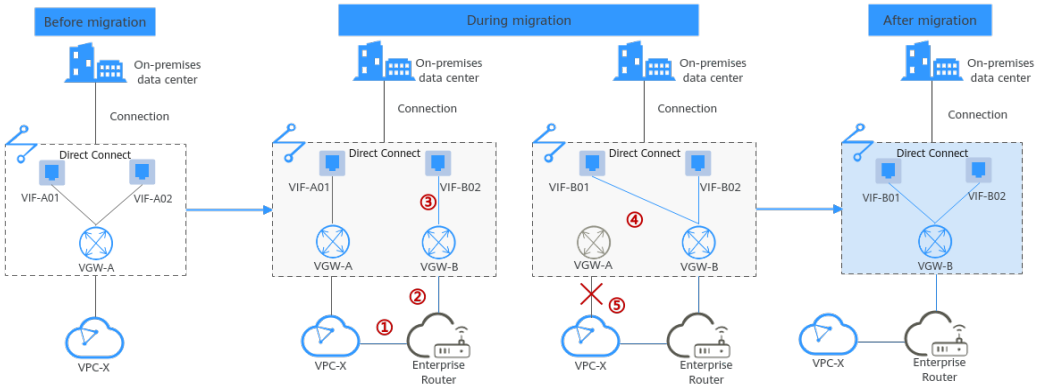
1. Before the migration, virtual gateway VGW-A directly connects to VPC-X and works with virtual interfaces VIF-A01 and VIF-A02 to allow the on-premises data center to access VPC-X.
2. During migration
   a. Attach VPC-X and virtual gateway VGW-A to an enterprise router. In the route table of VPC-X, ensure that the routes of the virtual gateway and the enterprise router do not conflict with each other. A CIDR block larger than the on-premises CIDR block will be used to avoid route conflicts.
   b. Create a virtual gateway VGW-B and attach it to the enterprise router.

      VGW-B is used to replace VGW-A after the migration.
   c. Delete virtual interface VIF-A02 associated with virtual gateway VGW-A and create virtual interface VIF-B02 for virtual gateway VGW-B.

      VIF-B02 is used to replace VIF-A02 after the migration. The on-premises data center can access VPC-X through the enterprise router.
   d. Delete virtual interface VIF-A01 associated with virtual gateway VGW-A and create virtual interface VIF-B01 for virtual gateway VGW-B.

      VIF-B01 is used to replace VIF-A01 after the migration.
3. When the on-premises data center can access the VPC through the enterprise router, delete virtual gateway VGW-A.

Figure 11-1 Architecture diagram



Advantages

As a high-performance central hub on the cloud, an enterprise router can connect multiple network instances. For example, if multiple VPCs and Direct Connect virtual gateways are attached to an enterprise router, the VPCs can share one Direct Connect connection to connect the on-premises data center.

- Enterprise routers support route learning, which frees you from complex configurations and simplifies O&M.
- Enterprise routers make it possible for multiple connections to work in load balancing or active/standby mode.

NOTE

Enterprise Router and Direct Connect can work together to build a highly reliable hybrid cloud network. For details, see **Allowing Direct Connect (Virtual Gateway) and VPN to Work in an Active and Standby Pair to Connect an On-Premises Data Center to the Cloud**.

Constraints

Migrating the network from Direct Connect to Enterprise Router may cause intermittent disconnections. **Submit a service ticket** and contact customer service to evaluate the migration solution. Here are some example scenarios that connectivity may be interrupted.

- If resources in a service VPC have virtual IP addresses bound, the service VPC cannot be attached to an enterprise router.
- If a service VPC is being used by ELB, VPC Endpoint, NAT Gateway (private NAT gateway), Distributed Cache Service (DCS), or hybrid DNS, this VPC cannot be attached to an enterprise router.

For details about constraints on enterprise routers, see **Notes and Constraints**.

11.2 Planning Networks and Resources

Plan required resources and networking before, during, and after the migration.

- **Network Planning**: Plan the VPC route table and enterprise router route table.
- **Resource Planning**: Plan the quantity, names, and main parameters of cloud resources: virtual gateways and virtual interfaces, VPC, ECSs, and enterprise router.

Network Planning

During the migration, you need to add routes to the VPC and enterprise router route tables. For details, see **Table 11-1**.

The following figures show the networking in different phases.

- **Figure 11-2**
- **Figure 11-3**
- **Figure 11-4**

NOTE

The routes in the figures are only examples for your reference. You need to plan routes based on service requirements.

Figure 11-2 Networking topology before the migration

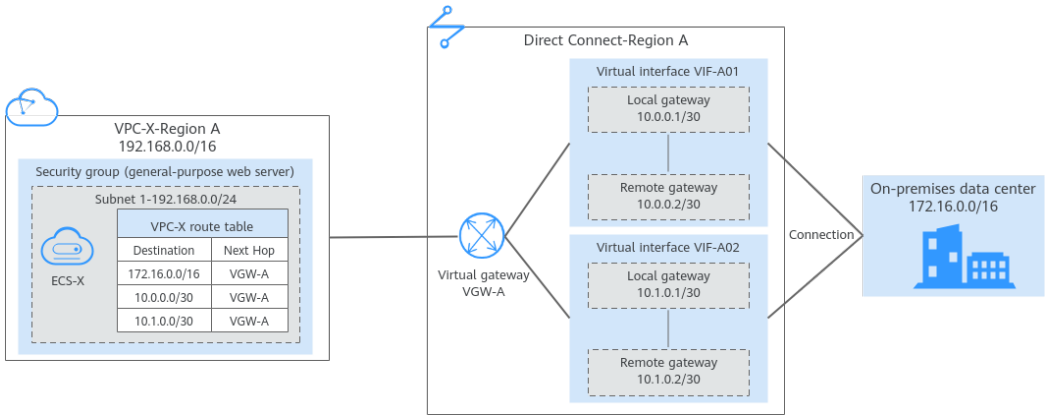


Figure 11-3 Networking topology during the migration

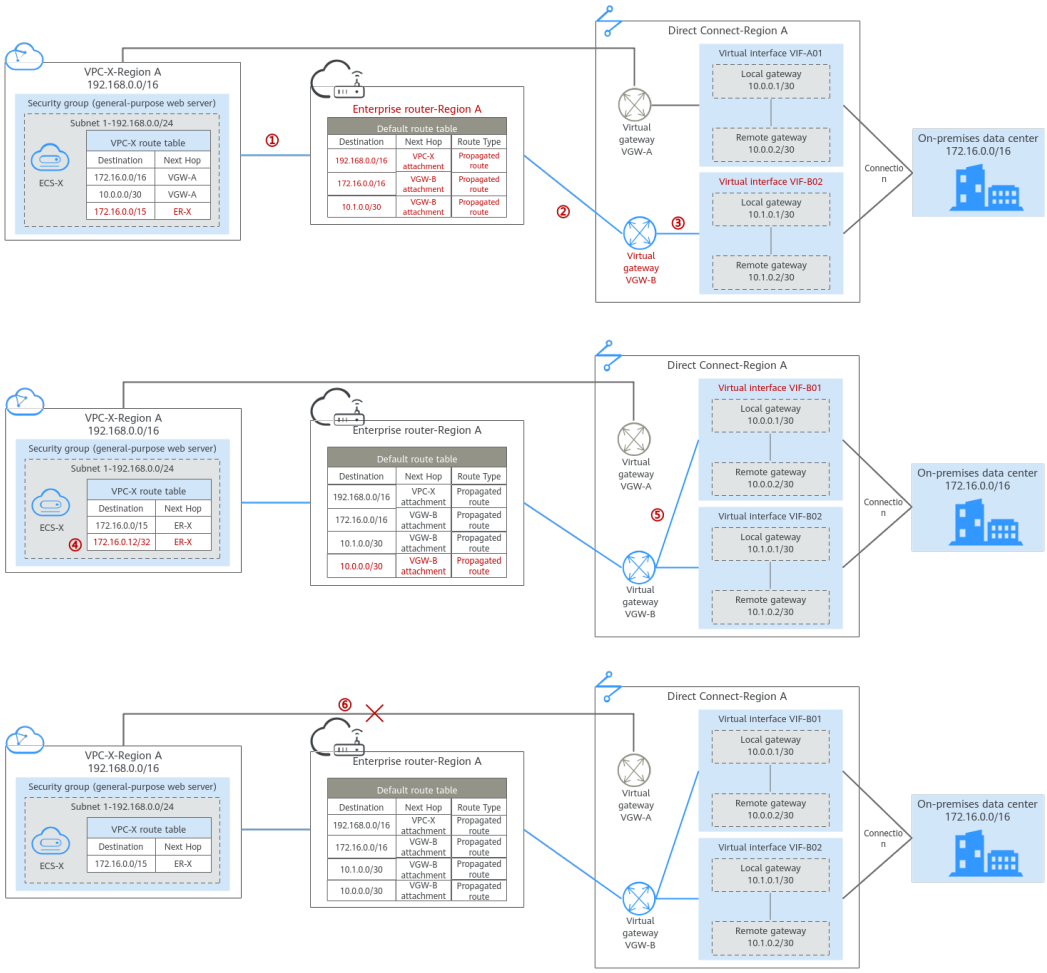


Figure 11-4 Networking topology after the migration

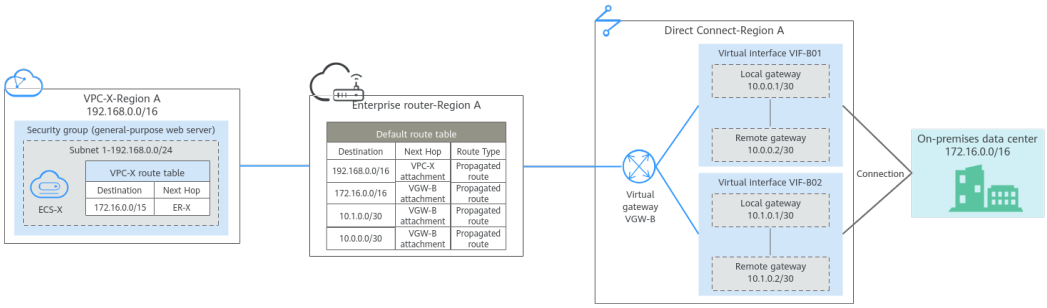


Table 11-1 Overall planning for migrating the network from Direct Connect to Enterprise Router

Route Table	Description
VPC route table	Table 11-2 lists the routes in this route table. 1. Before the migration, the VPC route table contains three routes pointing to the on-premises CIDR block and IP address ranges of the local and remote gateways over the virtual gateway. In this example, the CIDR block is 172.16.0.0/16, and the IP address ranges are 10.0.0.0/30 and 10.1.0.0/30. 2. During the migration, to prevent route conflicts, you need to add two routes in the VPC route table. a. A route with destination set to a larger CIDR block and next hop to the enterprise router is used for communications between the VPC and the enterprise router. The route destination must contain the on-premises CIDR block and cannot be used by other services. In this example, the destination is 172.16.0.0/15, which is larger than 172.16.0.0/16. **NOTICE** The route with destination set to a larger CIDR block must contain the on-premises CIDR block. If one larger CIDR block cannot contain the on-premises CIDR block, you can configure more larger CIDR blocks. b. A route pointing to the enterprise router is used to verify communications between the on-premises data center and VPC. The route can be deleted after the verification. The route destination can be the IP address of any on-premises server. In this example, the destination is 172.16.0.12/32. 3. When you delete the original virtual interfaces and virtual gateway during or after the migration, the routes related to the virtual gateway are also deleted. In this example, routes with destinations set to 172.16.0.0/16, 10.0.0.0/30, and 10.1.0.0/30 are deleted. **NOTICE** After the migration, you can continue to use the routes with a destination of the larger CIDR block or add routes with destinations that are the same as those of the original routes and then delete the routes with destination of the larger CIDR block.

Route Table	Description
Enterprise router route table	Table 11-3 lists the routes in this route table. During the migration, add routes pointing to the VPC CIDR block and virtual gateway to forward the traffic between the VPC and Direct Connect connection through the enterprise router. If **Default Route Table Association** and **Default Route Table Propagation** are enabled for the enterprise router, routes with destinations set to the attachments are automatically added when you attach the VPC and virtual gateways to the enterprise router. • In this example, when you attach the VPC to the enterprise router, there will be a propagated route destined for 192.168.0.0/16. • In this example, when you attach the virtual gateway to the enterprise router, there will be three propagated routes destinations set to 172.16.0.0/16, 10.0.0.0/30, and 10.1.0.0/30.

Table 11-2 VPC route table details

VPC	Route Table	Destination	Next Hop Type	Next Hop	Route Type	Description	Phase
VPC-X	rtb-vpc-X	172.16.0.0/16	Virtual gateway	vgw-A	System	Destined for the on-premises CIDR block	• Before migration • During migration
		10.0.0.0/30	Virtual gateway	vgw-A	System	Destined for the local and remote gateways of VIF-A01.	• Before migration • During migration

VPC	Route Table	Destination	Next Hop Type	Next Hop	Route Type	Description	Phase
		10.1.0.0/30	Virtual gateway	vgw-A	System	Destined for the local and remote gateways of VIF-A02.	• Before migration • During migration
		172.16.0.0/15	Enterprise router	ER-X	Custom	Destined for the larger CIDR block	• During migration • After migration
		172.16.0.12/32	Enterprise router	ER-X	Custom	Destined for any on-premises server to verify communications	During migration

Table 11-3 Details of the enterprise router route table

Enterprise Router	Route Table	Destination	Next Hop	Attached Resource	Route Type	Description	Phase
ER-X	defaultRouteTable	192.168.0.0/16	er-attach-VPC-X	VPC-X	Propagated route	Destination: VPC-X	• During migration • After migration
		172.16.0.0/16	er-attach-VGW-B	VGW-B	Propagated	Destination: on-premises CIDR block	• During migration • After migration

Enterprise Router	Route Table	Destination	Next Hop	Attached Resource	Route Type	Description	Phase
		10.0.0.0/30	er-attach-VGW-B	VGW-B	Propagated	Destination: local and remote gateways of VIF-B01	• During migration • After migration
		10.1.0.0/30	er-attach-VGW-B	VGW-B	Propagated route	Destination: local and remote gateways of VIF-B02.	• During migration • After migration

Resource Planning

During the migration, you need to create the required number of enterprise routers, virtual gateways, and virtual interfaces. After the migration is complete, the original resources can be released. **Table 11-4** describes the required resources.

NOTE

The following resource planning details are only examples for your reference. You need to plan resources based on service requirements.

Table 11-4 Resources planning for migrating the network from Direct Connect to Enterprise Router

Resource	Quantity	Description	Phase
VPC	1	A VPC for running your services. • VPC name: In this example, VPC-X is used. • IPv4 CIDR block: The VPC CIDR block must be different from the on-premises CIDR block. In this example, the VPC CIDR block is 192.168.0.0/16. • Subnet name: **subnet-X01** is used in this example. • Subnet IPv4 CIDR block: The subnet CIDR block cannot overlap with the on-premises CIDR block. In this example, the subnet CIDR block is 192.168.0.0/24.	• Before migration • During migration • After migration
Direct Connect connection	1	One connection	• Before migration • During migration • After migration
	2	The virtual gateway connected to the VPC. • **Name**: In this example, set it to **VGW-A**. • **Associate With**: Select **VPC**. The virtual gateway is connected to the VPC. • **VPC**: Select the service VPC. In this example, select **VPC-X**. • **BGP ASN**: In this example, set it to **64512**.	• Before migration • During migration
		The virtual gateway used to replace VGW-A. • **Name**: Set it based on site requirements. In this example, **VGW-B** is used. • **Associate With**: Select **Enterprise Router**. • **Enterprise Router**: Select your enterprise router. In this example, **ER-X** is used. • **BGP ASN**: Set it based on site requirements. In this example, the ASN is **64512**.	• During migration • After migration

Resource	Quantity	Description	Phase
	4	The virtual interfaces before the migration. • **Name**: In this example, the two virtual interfaces are **VIF-A01** and **VIF-A02**. • **Virtual Gateway**: In this example, the virtual gateway associated with the two virtual interfaces is VGW-A. • **Local Gateway**: In this example, the local gateway IP address range for virtual interface VIF-A01 is 10.0.0.1/30, and that for VIF-A02 is 10.1.0.1/30. • **Remote Gateway**: In this example, the remote gateway IP address range for virtual interface VIF-A01 is 10.0.0.2/30, and that for VIF-A02 is 10.1.0.2/30. • **Remote Subnet**: In this example, the on-premises CIDR block is 172.16.0.0/16. • **Routing Mode**: Select **BGP**. • **BGP ASN**: ASN of the on-premises data center, which must be different from the ASN of the virtual gateway on the cloud. In this example, **65525** is used.	• Before migration • During migration

Resource	Quantity	Description	Phase
		The virtual interfaces after the migration. They are used to replace VIF-A01 and VIF-A02. • **Name**: Set it based on site requirements. In this example, the two virtual interfaces are named **VIF-B01** and **VIF-B02**. • **Virtual Gateway**: Set it based on site requirements. In this example, the virtual gateway associated with the two virtual interfaces is VGW-B. • **Local Gateway**: Set it the same as that of the virtual interface before the migration. In this example, the local gateway for VIF-B01 is 10.0.0.1/30, and that for VIF-B02 is 10.1.0.1/30. • **Remote Gateway**: Set it the same as that of the virtual interface before the migration. In this example, the remote gateway for VIF-B01 is 10.0.0.2/30, and that for VIF-B02 is 10.1.0.2/30. • **Remote Subnet**: In this example, the on-premises CIDR block is 172.16.0.0/16. • **Routing Mode**: Select **BGP**. • **BGP ASN**: ASN of the on-premises data center, which must be different from the ASN of the virtual gateway on the cloud. In this example, **65525** is used.	• During migration • After migration

Resource	Quantity	Description	Phase
Enterprise Router	1	The enterprise router that is in the same region as the service VPC. • **Name**: Set it based on site requirements. In this example, **ER-X** is used. • **ASN**: Set an ASN that is different from that of the on-premises data center. In this example, the ASN is **64512**. • **Default Route Table Association**: Enable • **Default Route Table Propagation**: Enable • **Auto Accept Shared Attachments**: Set it based on site requirements. In this example, enable this option. • Two attachments on the enterprise router: – VPC attachment: **er-attach-VPC-X** – Virtual gateway attachment: **er-attach-VGW-B** **NOTICE** Do not enable **Auto Add Routes** when you create the VPC attachment. If this option is enabled, Enterprise Router automatically adds routes (with this enterprise router as the next hop and 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations) to all route tables of the VPC. During the migration, manually add routes with destinations set to the larger CIDR block in the VPC route table.	• During migration • After migration
ECS	1	An ECS used to verify connectivity. • **ECS Name**: Set it based on site requirements. In this example, **ecs-X** is used. • **Image**: Select an image based on site requirements. In this example, a public image (CentOS 8.2 64bit) is used. • **Network** – **VPC**: Select the service VPC. In this example, select **VPC-X**. – **Subnet**: Select the subnet that communicates with the on-premises data center. In this example, the subnet is **subnet-X01**. • **Security Group**: Select a security group based on site requirements. In this example, the security group uses a general-purpose web server template and its name is **sg-demo**. • Private IP address: 192.168.0.137	• Before migration • During migration • After migration

11.3 Reconstructing the Network with Enterprise Router

Table 11-5 describes the process of migrating a hybrid cloud network by replacing Direct Connect with Enterprise Router.

Table 11-5 Process of migrating a network from Direct Connect to Enterprise Router

Step	Description
Step 1: Create an Enterprise Router and a VPC Attachment	1. Create an enterprise router ER-X in the same region as the service VPC. 2. Create a VPC attachment er-attach-VPC-X to attach the service VPC to the enterprise router. 3. Verify that routes are automatically added to the enterprise router route table. 4. In the VPC route table, add a route destined for the larger CIDR block through the enterprise router.
Step 2: Create a Virtual Gateway Attachment	1. Create a virtual gateway VGW-B and attach it to the enterprise router. VGW-B is used to replace VGW-A after the migration. 2. Delete virtual interface VIF-A02 associated with virtual gateway VGW-A. Before deleting virtual interface VIF-A02, complete configuration on the on-premises network device to ensure that traffic does not pass through this virtual interface. 3. Create virtual interface VIF-B02 for virtual gateway VGW-B. VIF-B02 is used to replace VIF-A02 after the migration. 4. Complete configuration on the on-premises network device to ensure that traffic can pass through virtual interface VIF-B02.
Step 3: Verify Communications Between the VPC and On-Premises Data Center Through the Enterprise Router	1. In the VPC route table, add a route destined for any on-premises server to verify communications between the VPC and on-premises data center. 2. Create an ECS in the VPC subnet that needs to communicate with the on-premises data center, log in to the ECS, and run the **ping** command. 3. Delete the route and ECS used for verifying communications.

Step	Description
Step 4: Complete Migration	1. Delete virtual interface VIF-A01 associated with virtual gateway VGW-A. Before deleting virtual interface VIF-A01, complete configuration on the on-premises network device to ensure that traffic does not pass through this virtual interface. 2. Create virtual interface VIF-B01 for virtual gateway VGW-B. VIF-B01 is used to replace VIF-A01 after the migration. 3. Complete configuration on the on-premises network device to ensure that traffic can pass through virtual interface VIF-B01.
Step 5: Delete the Original Virtual Gateway	When the on-premises data center can access VPC-X using the enterprise router, delete virtual gateway VGW-A.

11.4 Procedure for Reconstructing the Network Using Enterprise Router

Step 1: Create an Enterprise Router and a VPC Attachment

Step 1 Create an enterprise router ER-X in the same region as the service VPC.

When creating the enterprise router, enable **Default Route Table Association** and **Default Route Table Propagation**. For details, see **Table 11-4**.

For details, see **Creating an Enterprise Router**.

Step 2 Create a VPC attachment er-attach-VPC-X to attach the service VPC to the enterprise router.

Do not enable **Auto Add Routes** and manually add routes with destinations set to the larger CIDR block to the VPC route table.

For details, see **Creating VPC Attachments to the Enterprise Router**.

Step 3 In the enterprise router route table, verify that the route points to the VPC attachment.

In this example, **Default Route Table Association** and **Default Route Table Propagation** are enabled for the enterprise router, and routes with destinations set to VPC CIDR blocks are automatically added when you attach the VPCs to the enterprise router.

NOTICE

If **Default Route Table Propagation** is not enabled when creating the enterprise router, you need to manually add routes with destinations set to the VPC CIDR blocks to the enterprise router route table. For details, see **Creating a Static Route**.

For enterprise router route details, see **Table 11-1** and **Table 11-3**.

To view enterprise routes, see **Viewing Routes**.

Step 4 In the VPC route table, add a route destined for the larger CIDR block through the enterprise router.

For VPC route details, see **Table 11-1** and **Table 11-2**.

In this example, the larger CIDR block is 172.16.0.0/15, and the next hop is the enterprise router.

For details, see **Adding Routes to VPC Route Tables**.

----End

Step 2: Create a Virtual Gateway Attachment

Step 1 Create a virtual gateway VGW-B and attach it to the enterprise router.

VGW-B is used to replace VGW-A after the migration.

1. On the Direct Connect console, create a virtual gateway.

   For details, see **Step 2: Create a Virtual Gateway**.

2. On the Enterprise Router console, check whether the virtual gateway attachment has been added to the enterprise router.

   For details, see **Viewing Details About an Attachment**.

   If the status of the virtual gateway attachment is **Normal**, the attachment has been added.

   Default Route Table Association and **Default Route Table Propagation** are enabled when you create the enterprise router. After the virtual gateway is attached to the enterprise router, the system will automatically:

   - Associate the virtual gateway attachment with the default route table of the enterprise router.
   - Propagate the virtual gateway attachment to the default route table of the enterprise router. The routes destined for the on-premises CIDR block are propagated to the route table.

     You can view routes destined for the on-premises CIDR block in the route table of the enterprise router only after creating a virtual interface by performing **Step 3**.

Step 2 Delete virtual interface VIF-A02 on the on-premises network device and the Direct Connect console in sequence:

1. Log in to the on-premises network device and delete the configuration of VIF-A02.

Before deleting virtual interface VIF-A02 on the Direct Connect console, complete configuration on the on-premises network device to ensure that traffic does not pass through this virtual interface.

2. Delete virtual interface VIF-A02 on the Direct Connect console.

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

   After the virtual interface is deleted, the system route pointing to VGW-A and destined for the local and remote gateways of VIF-A02 will be deleted from the VPC route table. For VPC route details, see **Table 11-2**.

   In this example, the route whose destination is 10.1.0.0/30 and next hop is the virtual gateway will be automatically deleted.

Step 3 Create virtual interface VIF-B02 for virtual gateway VGW-B.

VIF-B02 is used to replace VIF-A02 after the migration.

Create a virtual interface to connect the virtual gateway with the on-premises data center. For details, see **Step 3: Create a Virtual Interface**.

In the enterprise router route table, two routes pointing to VGW-B are automatically added. One route is destined for the on-premises CIDR block, and the other route for the local and remote gateways of VIF-B02. For enterprise router route details, see **Table 11-3**.

In this example, the route destinations are 172.16.0.0/16 and 10.1.0.0/30 and next hops are the virtual gateway.

Step 4 Complete configuration on the on-premises network device to ensure that traffic can pass through virtual interface VIF-B02.

----End

Step 3: Verify Communications Between the VPC and On-Premises Data Center Through the Enterprise Router

Step 1 In the VPC route table, add a route destined for any on-premises server to verify communications between the VPC and on-premises data center.

For VPC route details, see **Table 11-2**.

In this example, the route destination is 172.16.0.12/32 and next hop is the enterprise router.

For details, see **Adding Routes to VPC Route Tables**.

Step 2 Create an ECS in the VPC subnet that needs to communicate with the on-premises data center.

For more resource details, see **Table 11-4**.

For details, see **Overview**.

Step 3 Verify communications between the VPC and enterprise router.

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

ping *IP address of an on-premises server*

Add the IP address of an on-premises server to the VPC route table and run the following command:

ping 172.16.0.12

If information similar to the following is displayed, VPC-X can communicate with the on-premises data center through the enterprise router:

```
[root@ecs-X ~]# ping 172.16.0.12
PING 172.16.0.12 (172.16.0.12) 56(84) bytes of data.
64 bytes from 172.16.0.12: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.16.0.12: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.16.0.12: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.16.0.12: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.16.0.12 ping statistics ---
```

Step 4 Delete the route and ECS used for verifying communications.

1. Delete the route from the VPC route table.

   To delete a route, refer to **Deleting a Route**.

2. Delete the ECS.

   To delete an ECS, refer to **How Can I Delete or Restart an ECS?**

----End

Step 4: Complete Migration

Step 1 Delete virtual interface VIF-A01 on the on-premises network device and the Direct Connect console in sequence:

1. Log in to the on-premises network device and delete the configuration of VIF-A01.

   Before deleting VIF-A01 on the Direct Connect console, complete configuration on the on-premises network device to ensure that traffic does not pass through this virtual interface.

2. Delete virtual interface VIF-A01 on the Direct Connect console.

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

   After the virtual interface is deleted, the two routes pointing to virtual gateway VGW-A are deleted from the VPC route table. For VPC route details, **Table 11-2**.

   - The system route whose destination is the local and remote gateways of virtual interface VIF-A01.

     In this example, the route whose destination is 10.0.0.0/30 and next hop is the virtual gateway will be automatically deleted.

   - The system route destined for the on-premises data center.

     In this example, the route whose destination is 172.16.0.0/16 and next hop is the virtual gateway will be automatically deleted.

Step 2 Create virtual interface VIF-B01 for virtual gateway VGW-B.

VIF-B01 is used to replace VIF-A01 after the migration.

Create a virtual interface to connect the virtual gateway with the on-premises data center. For details, see **Step 3: Create a Virtual Interface**.

In the enterprise router route table, a route pointing to VGW-B is automatically added. The route destination is the local and remote gateways of virtual interface VIF-B02. For enterprise router route details, see **Table 11-3**.

In this example, the route destination is 10.0.0.0/30 and next hop is the virtual gateway attachment.

Step 3 Complete configuration on the on-premises network device to ensure that traffic can pass through virtual interface VIF-B01.

----End

Step 5: Delete the Original Virtual Gateway

NOTICE

After the migration is complete, ensure that VPC-X and the on-premises data center can communicate with each other through the enterprise router. After services run for a period of time, delete the original virtual gateway.

Step 1 Delete virtual gateway VGW-A.

For details, see **Deleting a Virtual Gateway**.

----End

A Change History

Released On	Description
2023-12-26	This issue is the seventh official release. Updated the following content: Added **Overview** to **Procedure for Building a Hybrid Network Using an Enterprise Router and Two Direct Connect Connections**.
2023-12-07	This issue is the sixth official release. Updated the following content: Added **Overview** to **Procedure for Reconstructing the Network Using Enterprise Router**.
2023-10-25	This issue is the fifth official release. Updated the following content: Added the description and steps of central networks in **Overview** to **Verifying Network Connectivity**.
2023-06-01	This issue is the fourth official release. Updated the following content: Added the transit VPC scenario in **Overview** and **Procedure for Enabling Communications Between an On-Premises Data Center and Service VPCs**.
2023-01-29	This issue is the third official release. Updated the following content: Added content about backup between Direct Connect and VPN connections in **Overview** to **Procedure for Communications Between an On-Premises Data Center and the Cloud Through Direct Connect and VPN**.

Released On	Description
2022-10-30	This issue is the second official release. Added the following content: Added **Overview** to **Replacement Steps**.
2022-08-25	This issue is the first official release.

