



Enterprise Router

Best Practices

Date **2023-12-30**

Contents

1 Overview.....	1
2 Using Enterprise Router to Isolate VPCs in the Same Region.....	4
2.1 Overview.....	4
2.2 Planning Networks and Resources.....	6
2.3 Creating Resources.....	11
2.3.1 Creating an Enterprise Router.....	11
2.3.2 Creating VPCs and ECSs.....	11
2.4 Configuring Networks.....	11
2.4.1 Creating VPC Attachments to the Enterprise Router.....	11
2.5 Verifying Network Isolation and Connectivity.....	12
3 Using Enterprise Router and a Transit VPC to Allow an On-premises Data Center to Access Service VPCs.....	14
3.1 Overview.....	14
3.2 Planning Networks and Resources.....	15
3.3 Process of Allowing an On-Premises Data Center to Access Service VPCs Using Enterprise Router and a Transit VPC.....	25
3.4 Building a Network Using an Enterprise Router and a Transit VPC.....	27
4 Using Enterprise Router and Direct Connect to Allow Communications Between an On-Premises Data Center and VPCs.....	32
4.1 Overview.....	32
4.2 Planning Networks and Resources.....	34
4.3 Creating Resources.....	39
4.3.1 Creating an Enterprise Router.....	39
4.3.2 Creating VPCs and ECSs.....	39
4.3.3 Creating a Direct Connect Connection.....	40
4.4 Configuring Networks.....	40
4.4.1 Creating VPC Attachments to the Enterprise Router.....	40
4.4.2 Configuring a Virtual Gateway Attachment in Enterprise Router.....	41
4.5 Verifying Connectivity Between the On-premises Data Center and VPCs.....	42
5 Allowing Direct Connect and VPN to Work in an Active and Standby Pair to Link Data Center to Cloud.....	44
5.1 Overview.....	44

5.2 Planning Networks and Resources.....	45
5.3 Construction Process.....	53
5.4 Construction Procedure.....	54
A Change History.....	60

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 public 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
Intra-region networking	Using Enterprise Router to Isolate VPCs in the Same Region	<ul style="list-style-type: none">Enterprise RouterVPCECS	<p>There are four VPCs in region A on public 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:</p> <ol style="list-style-type: none">VPC 1, VPC 2, and VPC 3 need to be isolated from each other.VPC 1, VPC 2, and VPC 3 need to communicate with VPC 4.

Networking	Scenario	Cloud Service	Description
Hybrid cloud networking	Using Enterprise Router and a Transit VPC to Allow an On-premises Data Center to Access Service VPCs	<ul style="list-style-type: none">• 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 networking	Using Enterprise Router and Direct Connect to Allow Communications Between an On-Premises Data Center and VPCs	<ul style="list-style-type: none">• Enterprise Router• Direct Connect• VPC• ECS	<p>There are two VPCs in region A. The two VPCs need to access each other and share the same Direct Connect connection to access an on-premises data center.</p> <p>To do this, we can create an enterprise router in region A, 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.</p>

Networking	Scenario	Cloud Service	Description
Hybrid cloud networking	<p>Allowing Direct Connect and VPN to Work in an Active and Standby Pair to Link Data Center to Cloud</p>	<ul style="list-style-type: none"> • Enterprise Router • Direct Connect • VPN • VPC • ECS 	<p>To improve the reliability of a hybrid cloud networking, an enterprise uses both Direct Connect and VPN connections to connect VPCs to the on-premises data center. 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.</p> <ul style="list-style-type: none"> • 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 data center through the VPN connection.

2 Using Enterprise Router to Isolate VPCs in the Same Region

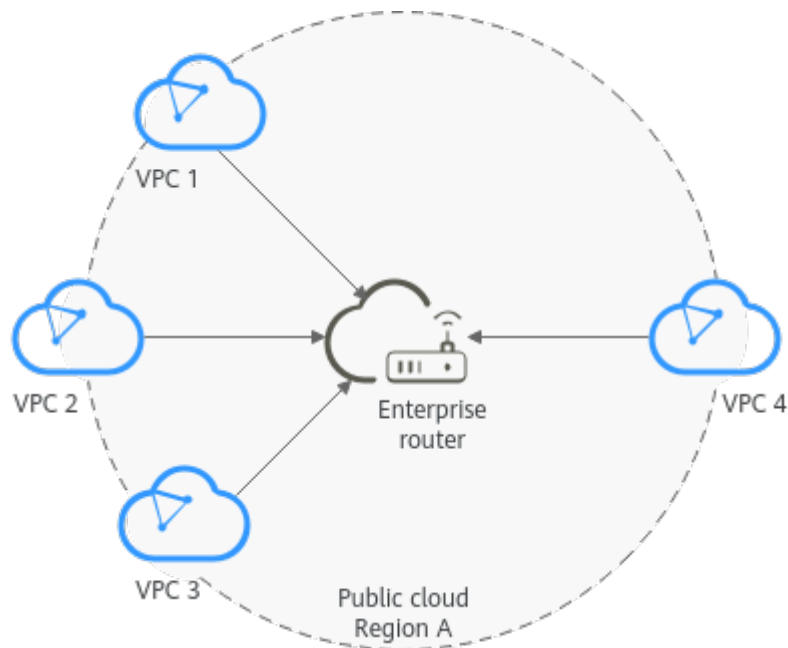
2.1 Overview

Background

There are four VPCs in region A on public 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 2-1 Isolation of VPCs in the same region



Operation Procedure

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

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

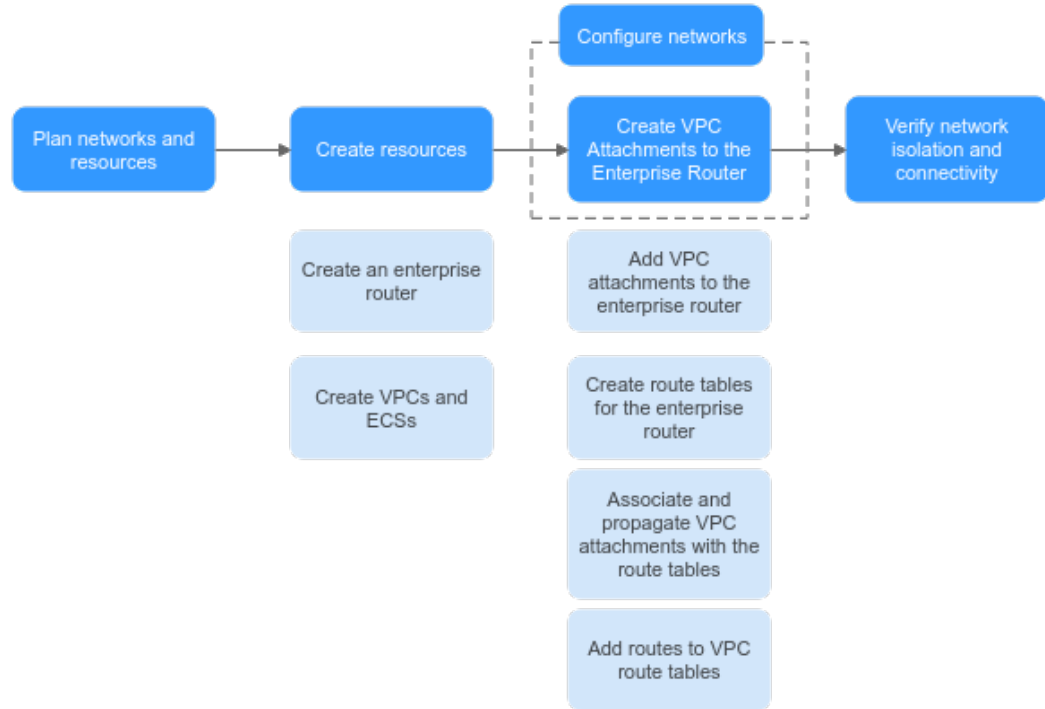


Table 2-1 Description of procedures for isolating VPCs in the same region

No.	Path	Description
1	Planning Networks and Resources	Plan required CIDR blocks and the number of resources.
2	Creating Resources	<ol style="list-style-type: none"> 1. Create an enterprise router. 2. Create four VPCs and four ECSs.
3	Creating VPC Attachments to the Enterprise Router	<ol style="list-style-type: none"> 1. Configure VPC attachments for the enterprise router: <ol style="list-style-type: none"> 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.

No.	Path	Description
4	Verifying Network Isolation and Connectivity	Log in to an ECS and run the ping command to verify the network isolation and connectivity.

2.2 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 2-3 and Table 2-3 show the network planning and its description for isolating VPCs in the same region.

Figure 2-3 Network planning for isolating VPCs in the same region

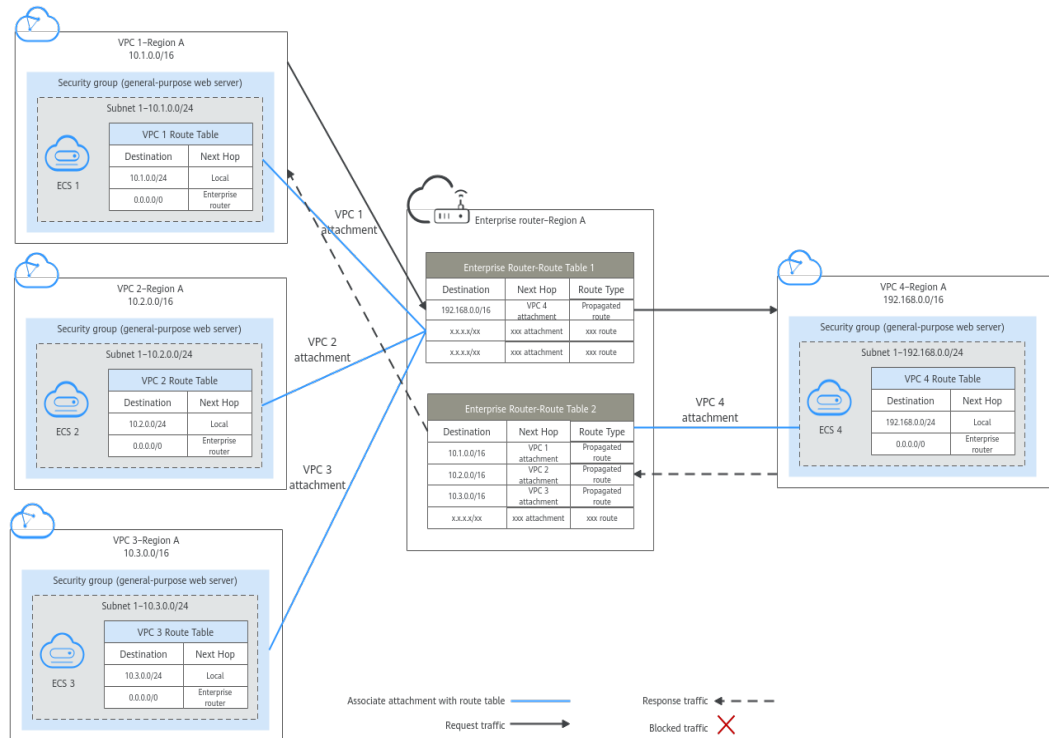


Table 2-2 Network traffic flows

Path	Description
Request from VPC 1 to VPC 4	<ol style="list-style-type: none">1. The route table of VPC 1 has routes with 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. The route table 1 of the enterprise router has a route with next hop set to VPC 4 attachment to forward traffic from the enterprise router to VPC 4.
Response from VPC 4 to VPC 1	<ol style="list-style-type: none">1. The route table of VPC 4 has routes with 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. The route table 2 of the enterprise router has a route with next hop set to VPC 1 attachment to forward traffic from the enterprise router to VPC 1.

Table 2-3 Description of network planning for isolating VPCs in the same region

Resource	Description
VPCs	<ul style="list-style-type: none">• 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:<ul style="list-style-type: none">– 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 2-4 for details.

Resource	Description
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: <ul style="list-style-type: none"> • 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 2-5. • Associate 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 2-6.
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 2-4 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 2-5 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 2-6 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 2-7](#).

Table 2-7 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: <ul style="list-style-type: none"> • er-rtb-isolation • er-rtb-share 	er-attach-isolation-01
					er-attach-isolation-02
					er-attach-isolation-03
					er-attach-share

Table 2-8 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 2-9 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 2-10](#).

Table 2-10 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-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 2-11](#).

Table 2-11 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

2.3 Creating Resources

2.3.1 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 section "Creating an Enterprise Router" in the *Enterprise Router User Guide*.

For enterprise router details, see [Table 2-7](#).

----End

2.3.2 Creating VPCs and ECSs

Scenarios

This section describes how to create VPCs and ECSs.

Procedure

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

For details, see [Creating a VPC](#).

For details, see [Creating an ECS](#).

- For details about VPC and subnet planning, see [Table 2-10](#).
- For details about ECS planning, see [Table 2-11](#).

----End

2.4 Configuring Networks

2.4.1 Creating VPC Attachments to 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 section "Creating VPC Attachments to the Enterprise Router" in the *Enterprise Router User Guide*.

Step 2 Create two route tables for the enterprise router.

For details, see section "Creating an Enterprise Router" in the *Enterprise Router User Guide*.

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

For details about creating an association, see section "Creating an Association" in the *Enterprise Router User Guide*.

For details about creating a propagation, see section "Creating a Propagation" in the *Enterprise Router User Guide*.

- For route table 1 details, see [Table 2-8](#).
- For route table 2 details, see [Table 2-9](#).

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

For details, see section "Adding Routes to VPC Route Tables" in the *Enterprise Router User Guide*.

----End

2.5 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

3 Using Enterprise Router and a Transit VPC to Allow an On-premises Data Center to Access Service VPCs

3.1 Overview

Application Scenarios

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 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 used by ELB, VPC Endpoint, NAT Gateway (private NAT gateways), or DCS, contact customer service to confirm the service compatibility and preferentially use a transit VPC for networking.
 - 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 ELB, NAT Gateway, VPC Endpoint, or DCS.
 - The VPC route table does not allow you to add a route whose destination address is 100.64.x.x and next hop is an enterprise router.

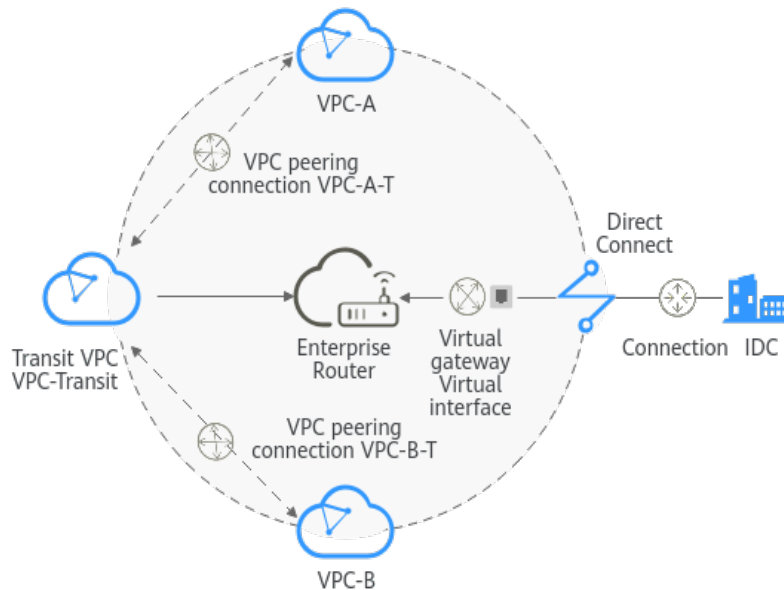
- If dedicated load balancers in the service VPCs have IP as backend enabled, the VPCs cannot communicate with each other using an enterprise router.
- If a VPC attached to an enterprise router has a NAT gateway associated and **Scenario** of the SNAT or DNAT rules is set to **Direct Connect/Cloud Connect**, 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 3-1](#) 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 3-1 Networking for allowing an on-premises data center to access two service VPCs over a transit VPC (scheme 2)



3.2 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:

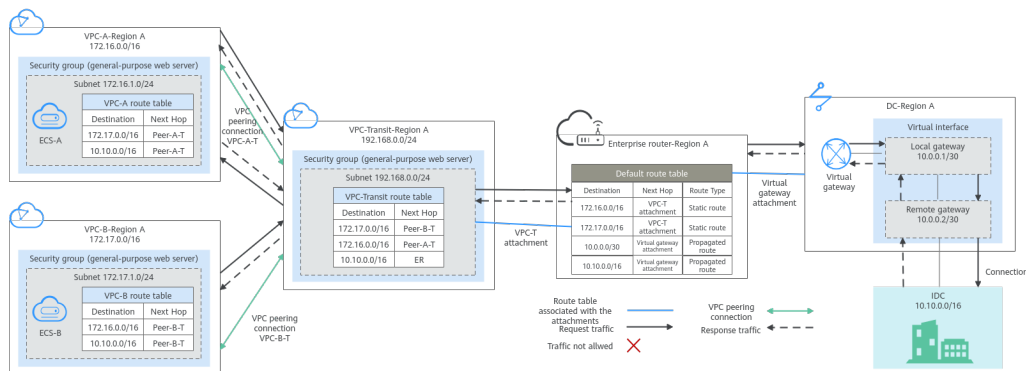
- **Network Planning:** Plan CIDR blocks of VPCs and their subnets, Direct Connect connection, and enterprise router, as well as the routes of these resources.

- **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 3-2 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 3-2** describes the resources for the networking.)

Figure 3-2 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 3-1**.
- 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 3-1**.

Table 3-1 Network traffic flows

No.	Path	Description
Path 1	Request traffic: from VPC-A to the on-premises data center	<ol style="list-style-type: none"> 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 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none">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 3-2 Networking with an enterprise router and a transit VPC

Cloud Service	Description
VPC	<p>Two service VPCs are required to run your workloads. In this example, the two VPCs are VPC-A and VPC-B.</p> <ul style="list-style-type: none">• 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:<ul style="list-style-type: none">- 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 3-3.- 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 3-3.

Cloud Service	Description
	<p>One transit VPC, which will be attached to the enterprise router. In this example, the transit VPC is VPC-Transit.</p> <ul style="list-style-type: none">• 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:<ul style="list-style-type: none">- 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	<ul style="list-style-type: none">• 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	<p>Add attachments to the enterprise router and configure the required routes.</p> <ul style="list-style-type: none"> • VPC <ul style="list-style-type: none"> - 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 3-4. • Direct Connect <ul style="list-style-type: none"> - 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 3-4.
ECS	<p>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.</p> <p>If you have multiple ECSs associated with different security groups, you need to add rules to the security groups to allow network access.</p>

Table 3-3 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 3-4 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 they can be in different AZs.

NOTE

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

Table 3-5 Resource details

Resource	Description
VPC	<p>Three VPCs are required. Table 3-6 describes the three VPCs and their settings.</p> <ul style="list-style-type: none"> • 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. <p>NOTICE</p> <ul style="list-style-type: none"> • 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.
VPC peering connection	Two VPC peering connections are required to connect VPC-A, VPC-B, and VPC-Transit. Table 3-7 describes the two VPC peering connections and their settings.
Direct Connect connection	A connection, a virtual gateway, and a virtual interface are required. Table 3-8 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 3-9 describes the enterprise router and its settings.
ECS	Two ECSs are required, with each in a service VPC. Table 3-10 describes the two ECSs and their settings.

Table 3-6 VPC details

VPC	VPC CIDR Block	Subnet	Subnet CIDR Block	Associated 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	Associated 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 3-7 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 3-8 Direct Connect resource details

Resource	Example Settings
Connection	Create a connection based on site requirements.
Virtual gateway	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none">• 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 3-9 Enterprise router details

Resource	Example Settings
Enterprise router	<ul style="list-style-type: none">• 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 .• Association/Propagation route table: default route table• Attachments:<ul style="list-style-type: none">– er-attach-VPctransit– er-attach-VGW

Resource	Example Settings
Attachments	<ul style="list-style-type: none"> • Attachment name: er-attach-VPctransit <ul style="list-style-type: none"> - 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 <ul style="list-style-type: none"> - Attachment type: virtual gateway attachment - Virtual gateway: vgw-demo

Table 3-10 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:	sg-demo (general	This ECS is used to run workloads.
ECS-B	VPC-B	subnet-B01	172.17.1.113	CentOS 8.2 64bit	- purpose web server)	This ECS is used to run workloads.

3.3 Process of Allowing an On-Premises Data Center to Access Service VPCs Using Enterprise Router and a Transit VPC

[Table 3-11](#) 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 3-11 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	<ol style="list-style-type: none"> 1. Create one 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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 CIDR block of the on-premises data center 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 CIDR block of the on-premises data center as the destination.
Step 4: Create a Virtual Gateway Attachment to the Enterprise Router	<ol style="list-style-type: none"> 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.

3.4 Building a Network Using an Enterprise Router and a Transit VPC

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 3-5](#).

Step 1 Create an enterprise router.

Disable **Default Route Table Propagation** when you create the enterprise router. For details, see [Table 3-9](#).

For details, see section "Creating an Enterprise Router" in the *Enterprise Router User Guide*.

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 [Creating an ECS](#).

----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 3-7](#).

- 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 section "Adding Routes to VPC Route Tables" in the *Enterprise Router User Guide*.

In this example, add the routes in [Table 3-3](#), and the next hop is the corresponding VPC peering connection.

- Add two routes in the route table of VPC-A with the 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 the 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 the 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 3-9](#).

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 section "Creating VPC Attachments to the Enterprise Router" in the *Enterprise Router User Guide*.

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

For details, see section "Adding Routes to VPC Route Tables" in the *Enterprise Router User Guide*.

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 3-4](#).

----End

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

For details about Direct Connect resources, see [Table 3-8](#).

Step 1 Create a connection.

For details, see section "Creating a Connection" in the *Direct Connect User Guide*.

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 section "Creating a Connection" in the *Direct Connect User Guide*.

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

For details, see section "Viewing Details About an Attachment" in the *Enterprise Router User Guide*.

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 with [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 section "Creating a Propagation" in the *Enterprise Router User Guide*.

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.

For details, see section "Creating a Connection" in the *Direct Connect User Guide*.

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

----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

4 Using Enterprise Router and Direct Connect to Allow Communications Between an On-Premises Data Center and VPCs

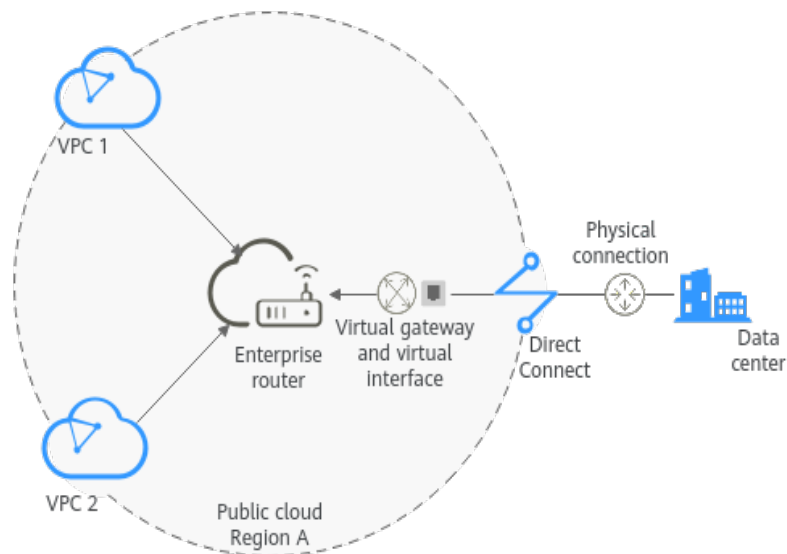
4.1 Overview

Background

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

To do this, we can create an enterprise router in region A, 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 4-1 Networking between an on-premises data center and VPCs



Operation Procedure

Figure 4-2 shows the procedure for using an enterprise router to connect an on-premises data center with VPCs.

Figure 4-2 Flowchart for connecting an on-premises data center with VPCs

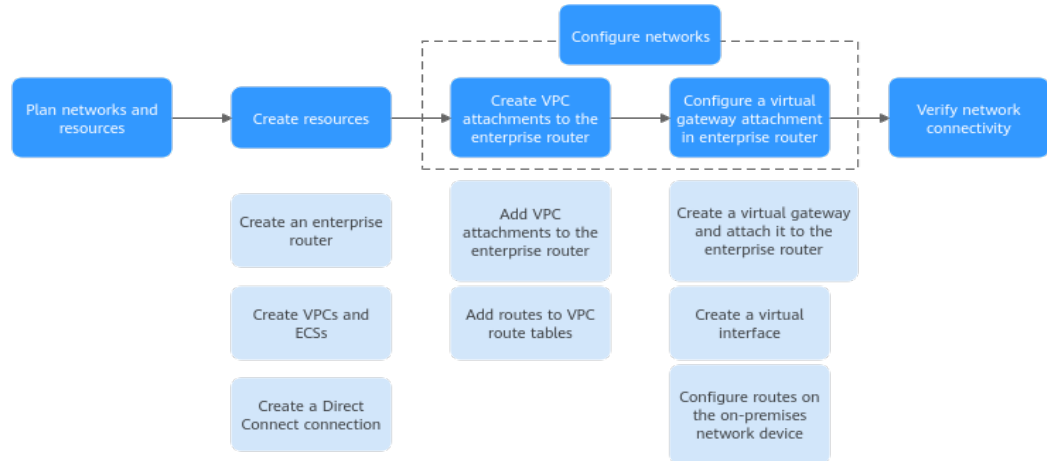


Table 4-1 Description of procedures for connecting an on-premises data center with VPCs

No.	Procedure	Description
1	Planning Networks and Resources	Plan required CIDR blocks and the number of resources.
2	Creating Resources	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none">1. Configure VPC attachments for the enterprise router:<ol style="list-style-type: none">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. Configure a virtual gateway attachment for the enterprise router:<ol style="list-style-type: none">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 of 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.

4.2 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 4-3 and **Table 4-3** show the network planning and its description for communications between on-premises data center and VPCs.

Figure 4-3 Network planning for communications between on-premises data center and VPCs

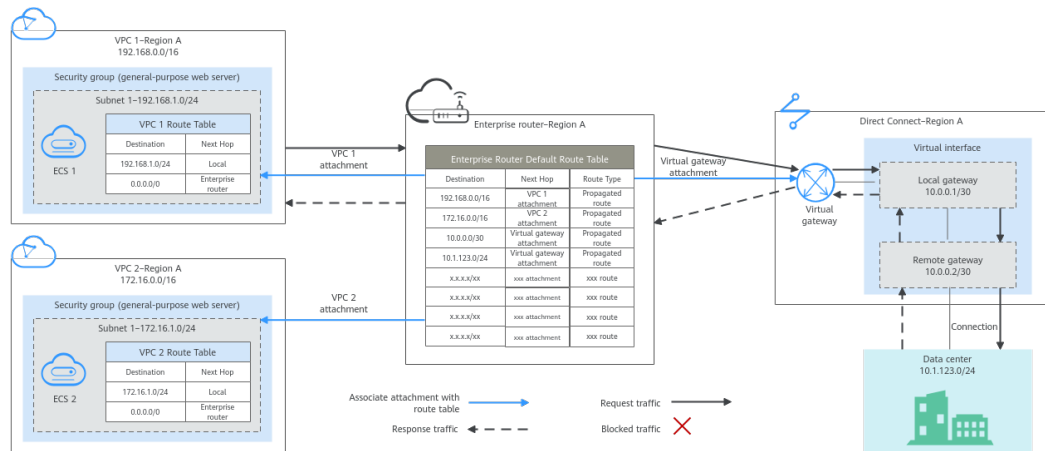


Table 4-2 Network traffic flows

Path	Description
Request from VPC 1 to the on-premises data center	<ol style="list-style-type: none"> The route table of VPC 1 has a route with next hop set to the enterprise router to forward traffic from VPC 1 to the enterprise router. The route table of the enterprise router has a route with next hop set to virtual gateway attachment to forward traffic from the enterprise router to the virtual gateway. 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 Traffic is sent to the on-premises data center over the connection.
Response from on-premises data center to VPC 1	<ol style="list-style-type: none"> Traffic is forwarded to the virtual interface through the connection. 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. Traffic is forwarded from the virtual gateway to enterprise router. The route table of the enterprise router has a route with next hop set to VPC 1 attachment to forward traffic from the enterprise router to the VPC 1.

Table 4-3 Description of network planning for communications between on-premises data center and VPCs

Resource	Description
VPCs	<ul style="list-style-type: none"> ● 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 the data center cannot overlap. ● Each VPC has a default route table. ● The routes in the default route table are described as follows: <ul style="list-style-type: none"> – 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 route details, see Table 4-4.
Direct Connect	<ul style="list-style-type: none"> ● One physical connection that you lease from a carrier to link 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	<p>After Default Route Table Association and Default Route Table Propagation are enabled and virtual gateway and VPC attachments are created, the system automatically:</p> <ul style="list-style-type: none"> ● Direct Connect <ul style="list-style-type: none"> – Associates the virtual gateway attachment with the default route table of the enterprise router. – Propagates the virtual gateway attachment to the default route table of the enterprise router. The route table automatically learns the local and remote gateways, and CIDR block of the data center as the destinations of routes. For details, see Table 4-5. ● VPC <ul style="list-style-type: none"> – Associates the two VPC attachments with the default route table of the enterprise router. – Propagates 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 4-5.

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 4-4 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 CIDR block of the on-premises data center 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 4-5 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 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 4-6](#).

Table 4-6 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 4-7](#).

Table 4-7 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 4-8](#).

Table 4-8 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 4-9](#).

Table 4-9 ECS details

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

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 section "Creating an Enterprise Router" in the *Enterprise Router User Guide*.

For enterprise router details, see [Table 4-6](#).

----End

4.3.2 Creating VPCs and ECSs

Scenarios

This section describes how to create VPCs and ECSs.

Procedure

Step 1 Create two VPCs and two ECSs in region A.

For details, see [Creating a VPC](#).

For details, see [Creating an ECS](#).

- For details about VPC and subnet planning, see [Table 4-8](#).
- For details about ECS planning, see [Table 4-9](#).

----End

4.3.3 Creating a Direct Connect Connection

Scenarios

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

Procedure

Step 1 Create a connection.

For details, see section "Creating a Connection" in the *Direct Connect User Guide*.

----End

4.4 Configuring Networks

4.4.1 Creating VPC Attachments to the Enterprise Router

Scenarios

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

Procedure

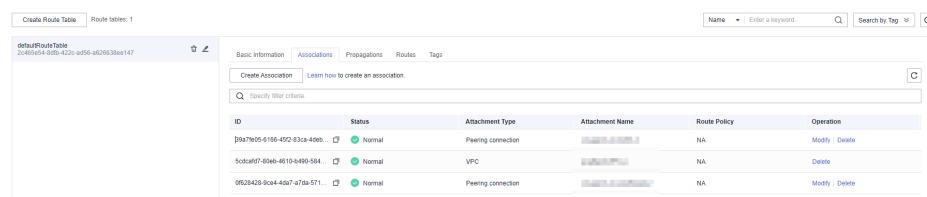
Step 1 Attach the two VPCs to the enterprise router.

For details, see section "Creating VPC Attachments to the Enterprise Router" in the *Enterprise Router User Guide*.

Default Route Table Association and **Default Route Table Propagation** are enabled when you create the enterprise router. Therefore, after you add VPC attachments to the enterprise router, the system automatically:

- Associates the VPC attachment with the default route table of the enterprise router.
- Propagates 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.

Figure 4-4 Viewing an association



ID	Status	Attachment Type	Attachment Name	Route Policy	Operation
19a7605-6166-452-832a-406b...	Normal	Peering connection	...	NA	Modify Delete
5cd4d7-0ba6-4610-8490-584...	Normal	VPC	...	NA	Delete
0f0242b-9aa4-46a7-a710a-571...	Normal	Peering connection	...	NA	Modify Delete

Figure 4-5 Viewing a propagation

ID	Status	Attachment Type	Attachment Name	Route Policy	Operation
7eed73b3-942-4811-9447-5813a74a4ce4	Normal	Peering connection		NA	Modify / Delete
8b81fa38-8465-4c77-a561-29226c51477a	Normal	VPC		NA	Delete
91a1c8b1-43d7-465b-851a-963a6f091354	Normal	Peering connection		NA	Modify / Delete

Figure 4-6 Viewing routes

Destination	Next Hop	Attachment Type	Attached Resource	Route Type	Operation
192.168.0.0/16		Peering connection		Propagated route	Modify / Delete
19.0.0.0/16		Peering connection		Propagated route	Modify / Delete
172.16.0.0/16		VPC		Propagated route	Modify / Delete

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

For details, see section "Adding Routes to VPC Route Tables" in the *Enterprise Router User Guide*.

----End

4.4.2 Configuring a Virtual Gateway Attachment in 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 section "Creating a Connection" in the *Direct Connect User Guide*.

2. On the enterprise router console, check whether the virtual gateway attachment exists.

For details, see section "Viewing Details About an Attachment" in the *Enterprise Router User Guide*.

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. Therefore, after you add the virtual gateway attachment to the enterprise router, the system automatically:

- Associates the virtual gateway attachment with the default route table of the enterprise router.

- Propagates 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 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.

For details, see section "Creating a Connection" in the *Direct Connect User Guide*.

For details about virtual interface planning, see [Table 4-7](#).

Step 3 Configure routes on the on-premises network device.

----End

4.5 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 (public 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 public 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 public 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

5 Allowing Direct Connect and VPN to Work in an Active and Standby Pair to Link Data Center to Cloud

5.1 Overview

Application Scenarios

Direct Connect establishes a dedicated, secure, and stable network connection between your on-premises data center and VPC. 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.

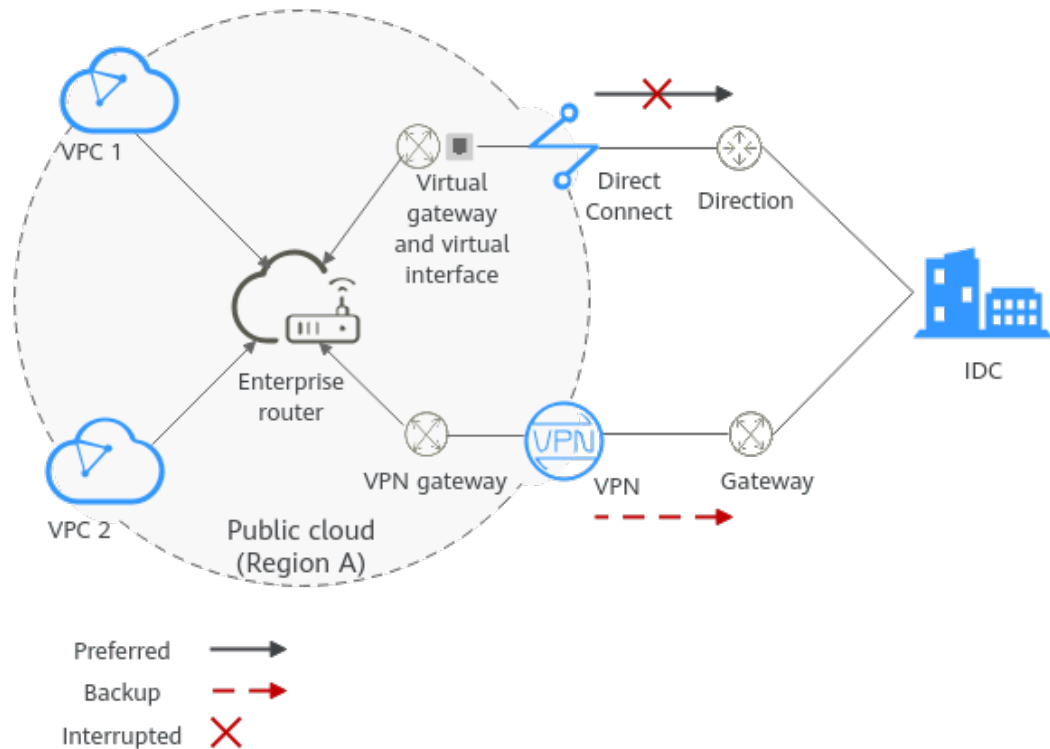
Architecture

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

Figure 5-1 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 VPCs and the data center cannot overlap.

5.2 Planning Networks and Resources

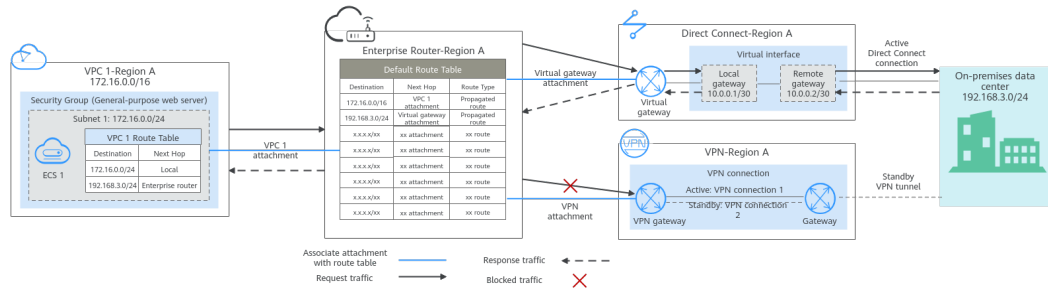
To attach both Direct Connect and VPN connections to an enterprise router to allow them to work in active/standby mode, you need to:

- **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 5-2 shows the network diagram of Direct Connect and VPN connections that work in the active/standby mode. **Table 5-2** describes the network planning.

Figure 5-2 Network diagram of Direct Connect and VPN connections working in an active/standby pair



Direct Connect and VPN connections work in the active/standby mode. 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 the data center. **Table 5-1** shows the details about the traffic flows in this example.

Table 5-1 Network traffic flows

Path	Description
Request from VPC 1 to the on-premises data center	<ol style="list-style-type: none"> 1. The route table of VPC 1 has routes with 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 route with next hop set to 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 physical connection through the remote gateway of the virtual interface. 4. Traffic is sent to the on-premises data center over the connection.

Path	Description
Response from the on-premises data center to VPC 1	<ol style="list-style-type: none"> 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 next hop set to VPC 1 attachment to forward traffic from the enterprise router to VPC 1.

Table 5-2 Description of network planning for Direct Connect and VPN connections that work in active/standby mode

Resource	Description
VPC	<p>VPC 1 (Service VPC) that your services are deployed:</p> <ul style="list-style-type: none"> • The CIDR blocks of the VPC and the data center cannot overlap. • The VPC has a default route table. • Routes in the default route table: <ul style="list-style-type: none"> – 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 subnet CIDR block of the data center. Table 5-3 shows the route. <p>A VPC that has a subnet used by the VPN gateway.</p> <p>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.</p>
Direct Connect	<ul style="list-style-type: none"> • One physical connection that you lease from a carrier to link 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	<ul style="list-style-type: none"> • 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.

Resource	Description
Enterprise router	<p>After Default Route Table Association and Default Route Table Propagation are enabled and an attachment is created, the system will automatically:</p> <ul style="list-style-type: none"> • VPC: <ul style="list-style-type: none"> - 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 5-4. • Direct Connect <ul style="list-style-type: none"> - 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. • VPN <ul style="list-style-type: none"> - 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 5-4.
ECS	<p>One ECS in the service VPC. The ECS is used to verify communications between the cloud and the on-premises data center.</p> <p>If you have multiple ECSs associated with different security groups, you need to add rules to the security groups to allow network access.</p>

Table 5-3 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 CIDR block of the on-premises data center and next hop set to enterprise router.

Table 5-4 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 they can be in different AZs.

 NOTE

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

Table 5-5 Details of required resources

Resource	Quantity	Description
VPC	2	<p>Service VPC that your services are deployed and needs to be attached to the enterprise router</p> <ul style="list-style-type: none"> • 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 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 data center. Set it based on site requirements. In this example, 172.16.0.0/24 is used. <p>A VPC that has a subnet used by the VPN gateway.</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
Enterprise router	1	<ul style="list-style-type: none"> • Name: Set it based on site requirements. In this example, er-test-01 is used. • ASN: Specify a different ASN from that of the 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: <ul style="list-style-type: none"> – VPC attachment: er-attach-VPC – Virtual gateway attachment: er-attach-VGW – VPN gateway attachment: er-attach-VPN

Resource	Quantity	Description
Direct Connect	1	<p>Connection: Create one based on site requirements.</p>
		<p>Virtual gateway</p> <ul style="list-style-type: none"> • 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.
		<p>Virtual interface</p> <ul style="list-style-type: none"> • 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 data center, which must be different from the ASN of the virtual gateway on the cloud. In this example, 65525 is used.
VPN	1	<p>VPN gateway</p> <ul style="list-style-type: none"> • 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.

Resource	Quantity	Description
		<p>Customer gateway</p> <ul style="list-style-type: none"> • Name: Set it based on site requirements. In this example, cgw-demo is used. • Routing Mode: Select Dynamic (BGP). • BGP ASN: ASN of the 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.
		<p>Two VPN connections that work in active/standby mode:</p> <ul style="list-style-type: none"> • 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).
ECS	1	<ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> – 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 data center must be different from that of the cloud. Set this ASN of the data center based on site requirements. In this example, 65525 is used.

5.3 Construction Process

Table 5-6 describes the overall process of building the hybrid cloud network using Direct Connect and VPN connections that work in the active/standby mode and an enterprise router.

Table 5-6 Process description of constructing the hybrid cloud network

Procedure	Description
Step 1: Create Cloud Resources	<ol style="list-style-type: none">1. Create one 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.
Step 2: Create a Virtual Gateway Attachment to the Enterprise Router	<ol style="list-style-type: none">1. Create a Direct Connect connection. The connection is dedicated to connect an on-premises data center to the public 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	<ol style="list-style-type: none">1. Attach the service VPC to the enterprise router.2. Add a route with the enterprise router as the next hop and the CIDR block of the data center 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.

Procedure	Description
Step 5: Create a VPN Attachment to the Enterprise Router	<ol style="list-style-type: none">1. Create a VPN gateway and attach it to the enterprise router.2. Create a customer gateway, that is the gateway of the 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	<p>Log in to the ECS and run the ping command to verify the network connectivity through the VPN connections.</p> <p>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.</p>

5.4 Construction Procedure

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 5-5](#).

Step 1 Create an enterprise router.

For details, see section "Creating an Enterprise Router" in the *Enterprise Router User Guide*.

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 data center. The ECS quantity and configuration are for reference only.

For details, see [Creating an ECS](#).

----End

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

For details about Direct Connect resources, see [Table 5-5](#).

Step 1 Create a connection.

For details, see section "Creating a Connection" in the *Direct Connect User Guide*.

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 section "Creating a Connection" in the *Direct Connect User Guide*.
2. On the enterprise router console, check whether the virtual gateway attachment has been added to the enterprise router.
For details, see section "Viewing Details About an Attachment" in the *Enterprise Router User Guide*.

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. Therefore, after you add the virtual gateway attachment 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 data center in the route table of the enterprise router only after performing the following steps.

Step 3 Create a virtual interface.

For details, see section "Creating a Connection" in the *Direct Connect User Guide*.

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 CIDR block of the on-premises data center and next hop set to enterprise router.

For details, see section "Creating VPC Attachments to the Enterprise Router" in the *Enterprise Router User Guide*.

- 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 the system automatically adds routes with destinations set to VPC CIDR blocks when you attach the VPCs to the enterprise router.

For VPC route details, see [Table 5-2](#) and [Table 5-4](#).

Check the routes of the enterprise router. For details, see section "Viewing Routes" in the *Enterprise Router User Guide*.

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

For VPC route details, see [Table 5-3](#).

For details, see "Adding Routes to VPC Route Tables" in the quick start of the *Enterprise Router User Guide*.

----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 data center through the enterprise router.

ping *IP address of the data center*

Example command:

ping 192.168.3.10

If information similar to the following is displayed, vpc-for-er can communicate with the 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 5-5](#).

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" in the *Virtual Private Network User Guide*.
2. On the enterprise router console, check whether the VPN gateway attachment has been added to the enterprise router.

For details, see section "Viewing Details About an Attachment" in the *Enterprise Router User Guide*.

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. Therefore, after you add the VPN gateway attachment 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 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" in the *Virtual Private Network User Guide*.

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

1. Create a VPN connection. For details, see section "Creating VPN Connection 1" in the *Virtual Private Network User Guide*.
2. Create another VPN connection. For details, see section "Creating VPN Connection 2" in the *Virtual Private Network User Guide*.

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 data center over the connection.

NOTICE

Simulate a fault only when no service is running on 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 data center through the enterprise router.

ping *IP address of the data center*

Example command:

ping 192.168.3.10

If information similar to the following is displayed, vpc-for-er can communicate with the 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

A Change History

Released On	Description
2023-12-30	This release incorporates the following changes: Added the transit VPC scenario in Overview and Building a Network Using an Enterprise Router and a Transit VPC .
2023-06-30	This release incorporates the following changes: Added content about backup between Direct Connect and VPN connections in Overview to Construction Procedure .
2022-12-30	This release incorporates the following changes: Added interconnection with Direct Connect in Overview to Verifying Connectivity Between the On-premises Data Center and VPCs .
2022-07-30	This issue is the first official release.