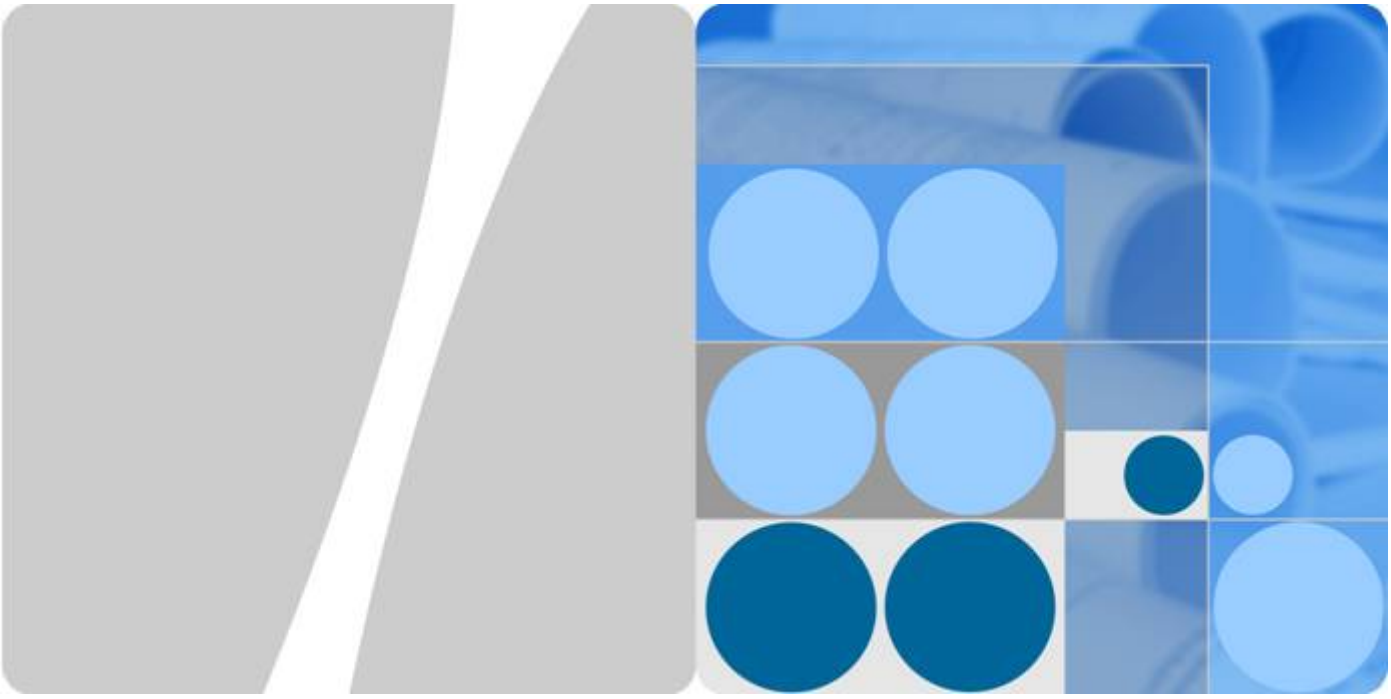


Cloud Connect

Best Practices

Date **2026-03-09**

Contents

1 Connecting Multiple On-Premises Networks Across Regions Through Enterprise Routers on a Central Network....1
1.1 Overview....1
1.2 Network and Resource Planning....2
1.3 Process of Connecting Multiple On-Premises Data Centers Across Regions....8
1.4 Procedure of Connecting Multiple On-Premises Data Centers Across Regions....9

1 Connecting Multiple On-Premises Networks Across Regions Through Enterprise Routers on a Central Network

1.1 Overview

Scenarios

Direct Connect establishes a dedicated, secure, stable, and high-speed network connection between your on-premises data center and VPCs. You can attach Direct Connect global DC gateways to enterprise routers to build a large-scale hybrid cloud network globally.

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

The following describes how to use Enterprise Router, Direct Connect, and Cloud Connect central networks to connect on-premises networks in different regions.

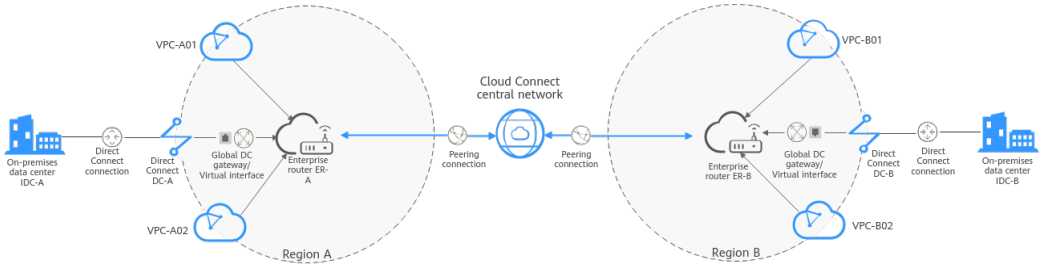
Architecture

An enterprise deployed services in the on-premises data centers in region A and region B. To quickly connect the two on-premises networks in different regions, you need to:

1. Create enterprise router ER-A in region A and enterprise router ER-B in region B.
2. Create a Cloud Connect central network and add the two enterprise routers (ER-A and ER-B) from different regions to this network.
3. In region A, connect IDC-A to ER-A through Direct Connect (global DC gateway). In region B, connect IDC-B to ER-B through Direct Connect (global DC gateway).

After the preceding steps are complete, the on-premises networks from different regions can communicate with each other.

Figure 1-1 Communications between multiple on-premises networks from different regions



Advantages

You can use Cloud Connect central networks and enterprise routers to flexibly build a global network for communications.

Constraints

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

1.2 Network and Resource Planning

To use enterprise routers and a Cloud Connect central network to allow on-premises networks from different regions to communicate with each other, you need to:

- **Network Planning**: Plan the required Direct Connect global DC gateways, virtual interfaces, and enterprise router route tables.
- **Resource Planning**: Plan the quantity, names, and other parameters of the Cloud Connect central network, Direct Connect resources, and enterprise routers.

Network Planning

Figure 1-2 shows the network planning for communications between on-premises networks across regions. Each on-premises data center is connected to an enterprise router through Direct Connect, and then the enterprise routers are connected to a Cloud Connect central network. **Table 1-2** describes the details.

Figure 1-2 Communications between multiple on-premises data centers from different regions

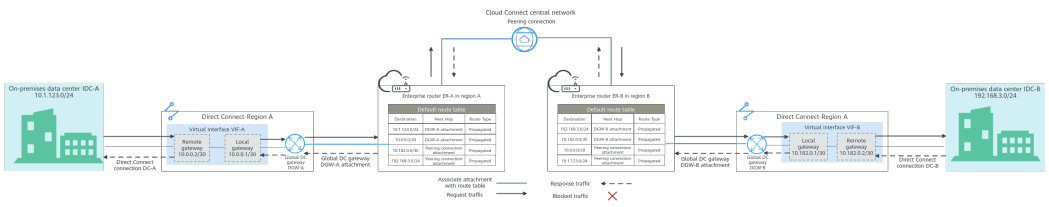


Table 1-1 Network traffic flows (Communications between multiple on-premises data centers across regions)

Path	Description
Request traffic: from IDC A, ER-A, ER-B, to IDC B	1. In the route table of ER-A, there is route with peering connection attachment as the next hop and 192.168.3.0/24 as the destination to route traffic to ER-B through a Cloud Connect central network. 2. In the route table of ER-B, there are two routes with DGW-B attachment as the next hop to forward traffic to global DC gateway DGW-B. The destination of one route is 192.168.3.0/24, which is the CIDR block of IDC-B. The destination of the other route is 10.182.0.0/30, which is the gateway address of virtual interface VIF-B. 3. Virtual interface VIF-B is connected to global DC gateway DGW-B to forward traffic from the remote gateway to the Direct Connect connection DC-B. 4. The traffic is then sent to IDC-B through Direct Connect connection DC-B.
Response traffic: from IDC-B, ER-B, ER-A, to IDC-A	1. In the route table of ER-B, there is route with peering connection attachment as the next hop and 10.1.123.0/24 as the destination to route traffic to ER-A through a Cloud Connect central network. 2. In the route table of ER-A, there are two routes with DGW-A attachment as the next hop to forward traffic to global DC gateway DGW-A. The destination of one route is 10.1.123.0/24, which is the CIDR block of IDC-A. The destination of the other route is 10.0.0.0/30, which is the gateway address of virtual interface VIF-A. 3. Virtual interface VIF-A is connected to global DC gateway DGW-A to forward traffic from the remote gateway to the Direct Connect connection DC-A. 4. The traffic is then sent to IDC-A through Direct Connect connection DC-A.

Table 1-2 Network planning description for communications between multiple on-premises data centers across regions

Resource	Quantity	Description
Enterprise router	2	The network configuration for the enterprise routers in region A and region B is the same. **Table 1-3** lists all routes required by the enterprise routers. When a central network is set up to connect the enterprise routers, you must enable **Default Route Table Association** and **Default Route Table Propagation** for the enterprise routers. In this way, when you create an attachment to such an enterprise router, a route pointing to the attachment will be automatically added for the enterprise router.
Direct Connect	2	The required resources in region A and region B are as follows: • There are two connections. Each links an on-premises data center to the cloud. In this example, there are connections DC-A in region A and DC-B in region B. • There are two global DC gateways. Each is attached to an enterprise router. In this example, global DC gateway DGW-A in region A is attached to enterprise router ER-A, and DGW-B in region B is attached to ER-B. • There are two virtual interfaces. Each connects a global DC gateway to a connection. In this example, there are virtual interfaces VIF-A in region A and VIF-B in region B.
Central network	1	• Enterprise routers in different regions are added to the central network as attachments. • A global connection bandwidth is required for assigning cross-site connection bandwidths to communicate across regions.

Table 1-3 Enterprise router route tables

Enterprise Router	Destination	Next Hop	Route Type
ER-A in region A	CIDR block of IDC-A: 10.1.123.0/24	DGW-A attachment: er-attach-dgw-A	Propagated
	Gateway of virtual interface VIF-A: 10.0.0.0/30	DGW-A attachment: er-attach-dgw-A	Propagated
	Gateway of virtual interface VIF-B: 10.182.0.0/30	Peering connection attachment: region-A-region-B	Propagated

Enterprise Router	Destination	Next Hop	Route Type
	CIDR block of IDC-B: 192.168.3.0/24	Peering connection attachment: region-A-region-B	Propagated
ER-B in region B	CIDR block of IDC-B: 192.168.3.0/24	DGW-B attachment: er-attach-dgw-B	Propagated
	Gateway of virtual interface VIF-B: 10.182.0.0/30	DGW-B attachment: er-attach-dgw-B	Propagated
	Gateway of virtual interface VIF-A: 10.0.0.0/30	Peering connection attachment: region-B-region-A	Propagated
	CIDR block of IDC-A: 10.1.123.0/24	Peering connection attachment: region-B-region-A	Propagated

Resource Planning

An enterprise router and its Direct Connect connection must be in the same region but can be in different AZs.

The following resource details are only for your reference. You can modify them if needed.

Table 1-4 Resource planning for communications between multiple on-premises data centers across regions

Resource	Quantity	Description
Enterprise router	2	An enterprise router is required in each of the two regions. Each enterprise router has a global DC gateway attachment from the same region and a peering connection attachment that is created between the two enterprise routers. • **Name**: Set it based on site requirements. In this example, the names are as follows: – Region A: ER-A – Region B: ER-B • **ASN**: Set different ASNs for the enterprise routers. In this example, the ASNs are as follows: – ER-A: 64522 – ER-B: 64523 • **Default Route Table Association**: This function must be enabled if a central network is used to connect the two enterprise routers. • **Default Route Table Propagation**: This function must be enabled if a central network is used to connect the two enterprise routers. • **Auto Accept Shared Attachments**: Set it based on site requirements. In this example, this option is enabled. • Attachment: Two attachments are created for each enterprise router. In this example, the attachments are as follows: **ER-A:** – Peering connection attachment region-A-region-B: connects enterprise routers ER-A to ER-B. – Global DC gateway attachment er-attach-dgw-A: connects on-premises data center IDC-A and enterprise router ER-A. **ER-B:** – Peering connection attachment region-B-region-A: connects enterprise routers ER-B to ER-A. – Global DC gateway attachment er-attach-dgw-B: connects on-premises data center IDC-B and enterprise router ER-B.
Direct Connect	2	Two connections are required. In this example, create connection DC-A in region A and DC-B in region B.

Resource	Quantity	Description
		Create two global DC gateways. • **Name**: Enter a name as required. In this example, the name of the global DC gateway in region A is DGW-A, and that in region B is DGW-B. • **BGP ASN**: It is recommended that the ASN of a global DC gateway be different from that of its enterprise router. In this example, the ASN of the global DC gateway in region A is 64512, and that of the global DC gateway in region B is 64513. • **IP Address Family**: Set this parameter based on site requirements. In this example, **IPv4** is used.
		Create two virtual interfaces. • **Name**: In this example, the name of the virtual interface in region A is VIF-A, and that in region B is VIF-B. • **Virtual Interface Priority**: In this example, **Preferred** is selected. • **Connection**: In this example, virtual interface VIF-A is associated with connection DC-A, and VIF-B is associated with DC-B. • **Global DC Gateway**: In this example, virtual interface VIF-A is associated with global DC gateway DGW-A, and VIF-B associated with DGW-B. • **Local Gateway**: In this example, the local gateway IP address range for virtual interface VIF-A is 10.0.0.1/30, and that for VIF-B is 10.182.0.1/30. • **Remote Gateway**: In this example, the remote gateway IP address range for virtual interface VIF-A is 10.0.0.2/30, and that for VIF-B is 10.182.0.2/30. • **Remote Subnet**: Specify the subnets of your on-premises data center. In this example, this value is set to 10.1.123.0/24 for virtual interface VIF-A and 192.168.3.0/24 for VIF-B. • **Routing Mode**: In this example, **BGP** is selected. • **BGP ASN**: ASN of the on-premises data center, which must be different from that used on the cloud (such as ASN of the global DC gateway or the enterprise router). In this example, the ASN of virtual interface VIF-A is 64855 and that of VIF-B is 64856.

Resource	Quantity	Description
		Attach global DC gateways to enterprise routers. • **Resource Type**: In this example, **Peer link** is selected. • **Peer Link Name**: Enter a name as required. In this example, the link name of DGW-A is **er-attach-dgw-A**, and that of DGW-B is **er-attach-dgw-B**. • **Peer Link Type**: In this example, **Enterprise Router** is selected. • **Link To**: Select the enterprise router that the global DC gateway to be attached to. In this example, global DC gateway DGW-A is attached to enterprise router ER-A, and DGW-B is attached to ER-B.
Cloud Connect central network	1	Create a central network, and add the two enterprise routers to it as attachments. • **Name**: Enter a name as required. In this example, the name is gcn-A-B. • Policies: – Region: Region A; Enterprise Router: ER-A – Region: Region B; Enterprise Router: ER-B • Cross-site connection bandwidth: Connects region A and region B. In this example, the bandwidth is 10 Mbit/s.
Global connection bandwidth	1	One global connection bandwidth is required to connect the cloud backbone networks in different regions. • **Bandwidth Name**: Enter a name as required. In this example, the bandwidth name is bandwidth-A-B to connect networks in region A and region B. • **Bandwidth Type**: Set it based on site requirements. In this example, **Geographic-region** is selected because region A and region B are in the same geographic region. • **Geographic Region**: Set it based on site requirements. In this example, **Chinese Mainland** is selected because region A and region B are in Chinese Mainland. • **Connect Regions**: Select the regions based on site requirements.

1.3 Process of Connecting Multiple On-Premises Data Centers Across Regions

Table 1-5 describes the overall process of using enterprise routers to connect on-premises data centers across regions.

Table 1-5 Steps for connecting multiple on-premises data centers across regions

Step	Description
Step 1: Create an Enterprise Router	1. Create an enterprise router in each region. 2. Create a central network. When creating the central network, create a policy and add the enterprise routers in different regions to the policy. 3. Create a global connection bandwidth to connect on-premises networks from different regions.
Step 2: Attach Global DC Gateways to Enterprise Routers	1. Create a Direct Connect connection in region A and verify the connectivity. a. Create a Direct Connect connection to connect the on-premises data center to the cloud over a line you lease from a carrier. b. Create a global DC gateway. c. Create a virtual interface to connect the global DC gateway to the connection. d. Attach the global DC gateway to the enterprise router and view the global DC gateway attachment in the attachment list of the enterprise router. e. Configure routes on the network device of the on-premises data center. f. Log in to the ECS and use **ping** to verify connectivity through the Direct Connect connection. 2. Create a Direct Connect connection in region B and verify the connectivity by referring to **1**.
Step 3: Assign Cross-Site Connection Bandwidths on the Central Network	Assign cross-site connection bandwidths on the central network based on service requirements.
Step 4: Verify Network Connectivity	Log in to a server in each of the on-premises data center and use **ping** to verify the network connectivity.

1.4 Procedure of Connecting Multiple On-Premises Data Centers Across Regions

Step 1: Create an Enterprise Router

The following describes how to create cloud resources, such as enterprise routers and Cloud Connect central networks. For details about the overall planning of cloud resources, see **Table 1-4**.

Step 1 Create two enterprise routers with one in each region.

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

Step 2 Create a central network and add the enterprise routers to the central network as attachments.

1. Create a central network and add the enterprise routers to the central network as attachments.
2. On the Enterprise Router console, view the peering connection attachments.

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

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

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

Step 3 Create a global connection bandwidth to connect on-premises networks from different regions.

----End

Step 2: Attach Global DC Gateways to Enterprise Routers

For details about Direct Connect resources used in this example, see **Table 1-4**.

Step 1 Create a Direct Connect connection in region A to link the on-premises data center to the cloud.

1. Create a connection.

   For details, see **Creating a Connection**.
2. Create a global DC gateway attachment for the enterprise router.
   a. On the Direct Connect console, perform the following operations:
      i. Create a global DC gateway.
      ii. Create a virtual interface.
      iii. Attach the global DC gateway to the enterprise router.

      For details, see **Creating a Global DC Gateway**.
   b. On the Enterprise Router console, view the global DC gateway attachment created for the enterprise router.

      If the status of the global DC gateway attachment is **Normal**, the attachment has been created.

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

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

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

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

   The following uses a Huawei network device as an example to describe how to configure a BGP route:

   bgp *64855*

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

   peer *10.0.0.1* **password simple** *Qaz12345678*

   network *10.1.123.0 255.255.255.0*

   Table 1-6 BGP route

Command	Description
bgp *64855*	Enables BGP. 64855: ASN of IDC-A
peer *10.0.0.1* **as-number 64512**	Creates a BGP peer. – 10.0.0.1: the gateway address on Huawei Cloud – 64512: BGP ASN of the global DC gateway
peer *10.0.0.1* **password simple** *Qaz12345678*	Performs MD5 authentication on BGP messages when a TCP connection is established between BGP peers. Qaz12345678: BGP MD5 authentication password
network *10.1.123.0 255.255.255.0*	Adds routes in the IP route table to the BGP route table. – 10.1.123.0: network used by the on-premises data center – 255.255.255.0: subnet mask of the on-premises network

4. Log in to an ECS of the enterprise router.

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

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

5. Verify the connectivity over the Direct Connect connection in region A:

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

Example command:

ping 10.1.123.5

If information similar to the following is displayed, the cloud network is connected to the on-premises network.

```
[root@ecs-A ~]# ping 10.1.123.5
PING 10.1.123.5 (10.1.123.5) 56(84) bytes of data.
64 bytes from 10.1.123.5: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 10.1.123.5: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 10.1.123.5: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 10.1.123.5: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 10.1.123.5 ping statistics ---
```

Step 2 Create a Direct Connect connection in region B and verify the connectivity by referring to **Step 1**.

----End

Step 3: Assign Cross-Site Connection Bandwidths on the Central Network

To allow cross-region communications, you need to assign cross-site connection bandwidths on the central network based on service requirements by referring to **Table 1-4**.

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

----End

Step 4: Verify Network Connectivity

Step 1 Log in to a server in on-premises data center IDC-A.

Step 2 Check whether IDC-A can access a server in IDC-B:

ping *IP address in IDC-B*

Example command:

ping 192.168.3.5

If information similar to the following is displayed, IDC-A can access IDC-B.

```
[root@idc-A ~]# ping 192.168.3.5
PING 192.168.3.5 (192.168.3.5) 56(84) bytes of data.
64 bytes from 192.168.3.5: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 192.168.3.5: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 192.168.3.5: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 192.168.3.5: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 192.168.3.5 ping statistics ---
```

Step 3 Log in to a server in on-premises data center IDC-B.

Step 4 Check whether IDC-B can access a server in IDC-A:

ping *IP address in IDC-A*

Example command:

ping 10.1.123.6

If information similar to the following is displayed, IDC-B can access IDC-A.

```
[root@idc-B ~]# ping 10.1.123.6
PING 10.1.123.6 (10.1.123.6) 56(84) bytes of data.
64 bytes from 10.1.123.6: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 10.1.123.6: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 10.1.123.6: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 10.1.123.6: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 10.1.123.6 ping statistics ---
```

----End