Direct Connect

FAQ

Issue 01

Date 2026-01-09

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Popular Questions

1.1 What Are the Network Requirements for Connections?

- Your on-premises network must use a single-mode fiber with a 1GE, 10GE, 40GE, or 100GE optical module to connect to the access device on Huawei Cloud. In addition, key parameters such as the LC, wavelength, and distance must be consistent with those of the access device on Huawei Cloud. Examples of optical module parameters: 1 GE, LC single-mode, 1,310 nm, and 10 km
- Auto-negotiation for the ports must be disabled. Port speed and full-duplex mode must be manually configured.
- 802.1Q VLAN encapsulation must be supported on all devices of the entire connection, including intermediate devices.
- Your device must support Border Gateway Protocol (BGP) and BGP MD5 authentication or static routing.
- (Optional) You can configure Bidirectional Forwarding Detection (BFD) on the network.
- A physical connection supports jumbo frames with a default maximum transmission unit (MTU) size of 8,500 bytes. If you need to configure a larger MTU, contact the Direct Connect manager.

  If you ping the IP address of the local gateway of a Direct Connect connection for connectivity test, the MTU is 1,500 bytes.
- Private IP addresses are recommended for cloud and on-premises servers, and the IP address ranges used for communications cannot overlap.

1.2 How Do I Select a Carrier When Purchasing a Connection?

1. Confirm which carriers are available at the Direct Connect location you select. Different locations may have different carriers available.

2. Select the one that best meets your requirements based on their price, network performance, and other features.

1.3 How Will I Be Billed for Direct Connect?

You can create a standard connection, which will give you exclusive access to the port. You can also request a hosted connection from a partner and share the port with other users.

Billed Items

This section describes the billed items of self-service connections, full-service connections, and hosted connections.

Billed Items of a Self-Service Connection

Billed items of a standard connection include the port, one-time setup, leased line, and in-building cabling. Huawei Cloud billed items include the port and one-time setup. Non-Huawei Cloud billed items include the leased line and in-building cabling.

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

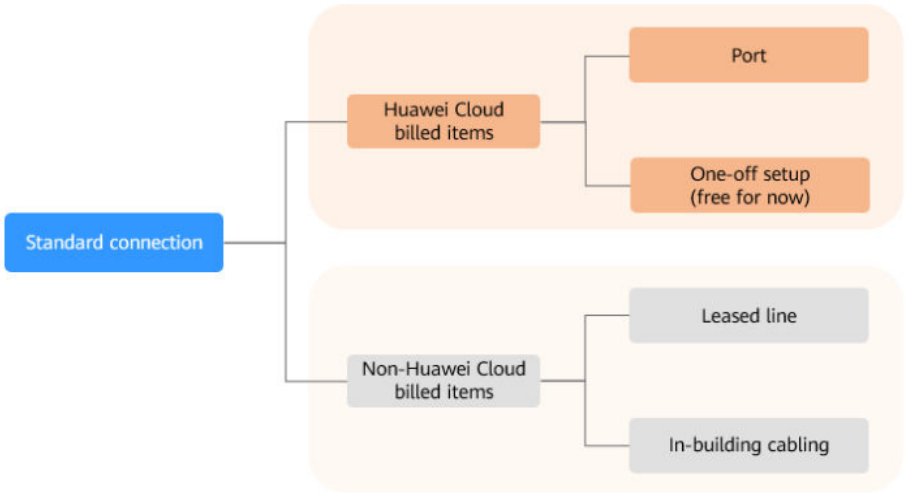


Table 1-1 Billed items of a self-service connection

Billed Items	Description	Billing Mode	Formula
Port	The port is billed based on its specifications.	Yearly/ Monthly (prepaid)	Unit price × Duration For port prices, see **Direct Connect Pricing Details**.

Billed Items	Description	Billing Mode	Formula
One-time setup	Currently, the one-time setup is free.	Free	Free
Leased line	You need to pay to the carrier for the line that is used to connect your on-premises data center to the Direct Connect location you select.	Pay for the leased line to the carrier.	Consult the carrier.
In-building cabling	A fiber may be required for connecting your leased line to the equipment room at the Direct Connect location you select if the data center at the Direct Connect location is a carrier-neutral data center.	You pay for the property of the data center for in-building cabling.	Consult the property of the data center.

Billed Items of a Full-Service Connection

Billed items of a full-service connection include port, one-time setup, leased line, and in-building cabling. You pay for all these items to Huawei Cloud.

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

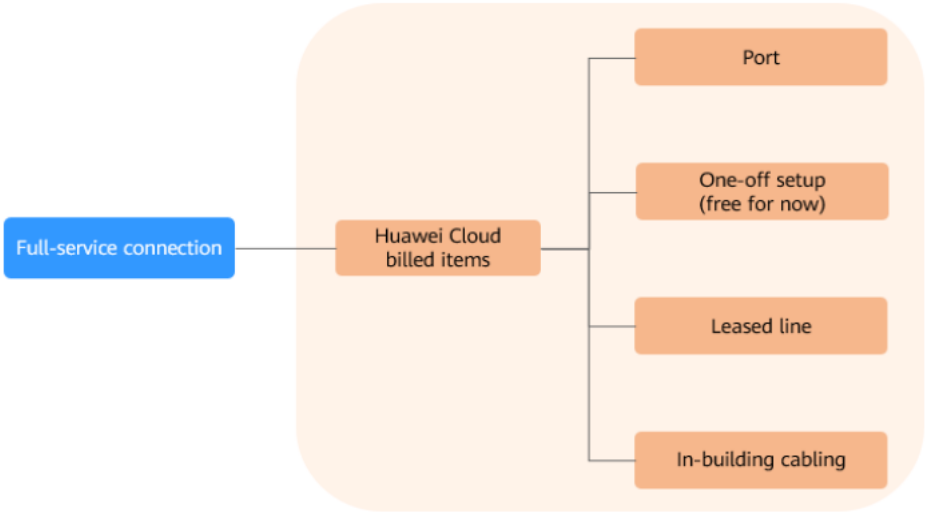


Table 1-2 Billed items of a full-service connection

Billed Items	Description	Billing Mode	Formula
Port	The port is billed based on its specifications.	Yearly/Monthly (prepaid)	Unit price × Duration For port prices, see **Direct Connect Pricing Details**.
One-time setup	Currently, the one-time setup is free.	Free	Free
Leased line	You need to pay to the carrier for the line that is used to connect your on-premises data center to the Direct Connect location you select.	Pay for it to Huawei Cloud.	-
In-building cabling	A fiber may be required for connecting your leased line to the equipment room at the Direct Connect location you select if the data center at the Direct Connect location is a carrier-neutral data center.		-

Billed Items of a Hosted Connection

To use a hosted connection, you only need to pay the partner for the leased line.

For details, see **Table 1-3**.

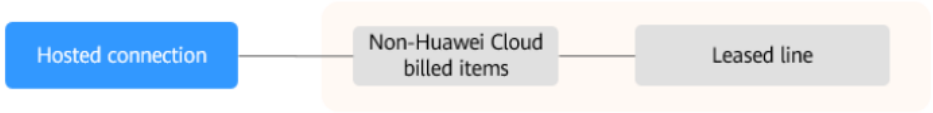


Table 1-3 Billing items of a hosted connection

Billed Items	Description	Billing Mode	Formula
Leased line	You need to pay to the carrier for the line that is used to connect your on-premises data center to the Direct Connect location you select.	Pay the partner for the leased line.	Consult the partner.

Billing Mode

Yearly/Monthly

Changing Billing Mode

Only Yearly/Monthly billing is supported, and it cannot be changed.

Renewal

For details, see **Renewal Management**.

Expiration and Overdue Payment

For details, see **Service Suspension and Resource Release** and **Payment and Repayment**.

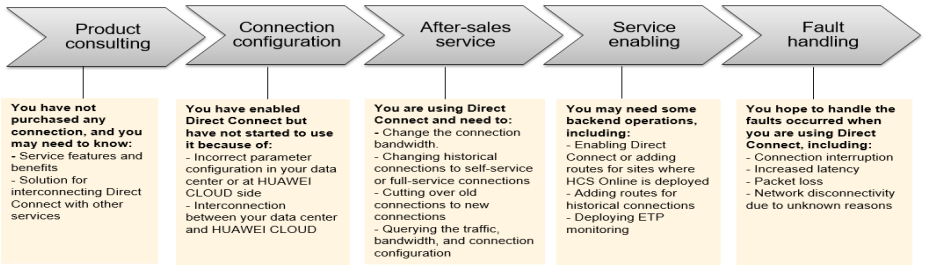
1.4 How Do I Submit a Service Ticket?

1. Log in to the management console.
2. In the upper right corner, choose **Service Tickets** > **Create Service Ticket**.
3. Choose **More Products**, and click **Direct Connect** under **Network**.
4. Select the service ticket type.

NOTE

When you **submit a service ticket**, selecting a ticket type can accelerate problem handling.

Figure 1-1 Ticket types



1.5 How Do I Test the Network Connectivity Between a Location and the Cloud?

To test network connectivity between the location you select and the cloud, add the CIDR block where the local and remote gateways reside to the remote subnet you configure when creating the virtual interface, and then ping the IP address of the local gateway from a VM on the cloud.

If the test fails, check whether:

- The VM is in the VPC associated with the virtual gateway.

- The VM IP address is within the local subnet configured when you create the virtual gateway.
- Security group rules and network ACL rules of the VM allow traffic from the VM to the local gateway configured for the virtual interface.

1.6 What Do I Do If I Select the Wrong Carrier When Creating a Connection?

Your selection for the carrier does not affect the establishment of network connectivity.

If you want to change the carrier, you can unsubscribe from the created connection, create another one, and select the desired carrier.

2 Product Consultation

2.1 What Are the Network Requirements for Connections?

- Your on-premises network must use a single-mode fiber with a 1GE, 10GE, 40GE, or 100GE optical module to connect to the access device on Huawei Cloud. In addition, key parameters such as the LC, wavelength, and distance must be consistent with those of the access device on Huawei Cloud. Examples of optical module parameters: 1 GE, LC single-mode, 1,310 nm, and 10 km
- Auto-negotiation for the ports must be disabled. Port speed and full-duplex mode must be manually configured.
- 802.1Q VLAN encapsulation must be supported on all devices of the entire connection, including intermediate devices.
- Your device must support Border Gateway Protocol (BGP) and BGP MD5 authentication or static routing.
- (Optional) You can configure Bidirectional Forwarding Detection (BFD) on the network.
- A physical connection supports jumbo frames with a default maximum transmission unit (MTU) size of 8,500 bytes. If you need to configure a larger MTU, contact the Direct Connect manager.

  If you ping the IP address of the local gateway of a Direct Connect connection for connectivity test, the MTU is 1,500 bytes.
- Private IP addresses are recommended for cloud and on-premises servers, and the IP address ranges used for communications cannot overlap.

2.2 What Are 1GE and 10GE?

GE is short for Gigabit Ethernet, which indicates the bandwidth supported by a port.

- 1GE: supports data transmission at a speed of 1 Gbit/s.

- 10GE: supports data transmission at a speed of 10 Gbit/s.

2.3 Is BGP Routing Supported by Direct Connect?

Yes. Direct Connect allows you to use BGP for routing traffic.

You can refer to the following best practices to see where BGP routing is required:

- **Connecting an On-Premises Data Center to a VPC over a Single Connection and Using BGP Routing to Route Traffic**
- **Connecting an On-Premises Data Center to a VPC over Two Connections in an Active/Standby Pair (Virtual Gateway)**

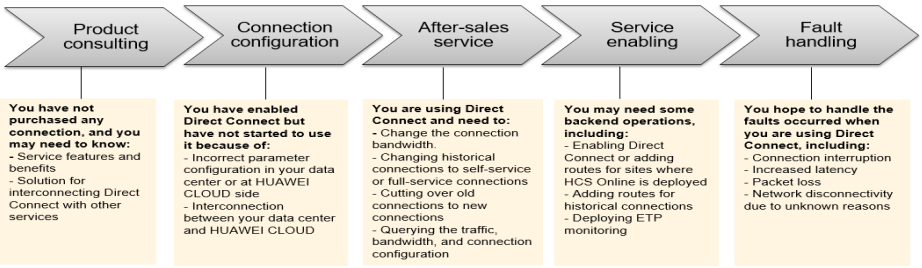
2.4 How Do I Submit a Service Ticket?

1. Log in to the management console.
2. In the upper right corner, choose **Service Tickets** > **Create Service Ticket**.
3. Choose **More Products**, and click **Direct Connect** under **Network**.
4. Select the service ticket type.

   NOTE

   When you **submit a service ticket**, selecting a ticket type can accelerate problem handling.

   Figure 2-1 Ticket types



2.5 What Are the Network Latency and Packet Loss Rate of a Connection?

- You can install Direct Connect monitoring plug-ins to monitor the network quality of connections. There are two metrics: network latency and packet loss rate.

  Direct Connect provides two monitoring plug-ins:

  – dc-nqa-collector: monitors the connections requested on the Direct Connect console.

  – history-dc-nqa-collector: monitors historical connections.

  For details, see **Installing the Direct Connect Metric Collection Plug-ins**.

NOTE

- Automated connections are requested using the console and can be self-service or full-service connections. Each connection has at least a virtual gateway and a virtual interface, and their routes are automatically advertised. Connections in most regions are automated connections.
- Historical connections are requested by email or phone. They do not have virtual gateways and virtual interfaces, and their routes must be configured manually. Historical connections exist only in some regions.

- Contact the leased line provider to learn more about the network latency and packet loss rate of the line from the Direct Connect gateway to your on-premises data center.

The provided data is theoretical values. The actual values vary depending on the monitoring results.

2.6 Are the Uplink and Downlink Bandwidths of a Direct Connect Connection the Same?

Yes.

If you set the bandwidth to 100 Mbit/s, the uplink and downlink bandwidths are both 100 Mbit/s.

2.7 What Do I Do If I Select the Wrong Carrier When Creating a Connection?

Your selection for the carrier does not affect the establishment of network connectivity.

If you want to change the carrier, you can unsubscribe from the created connection, create another one, and select the desired carrier.

2.8 How Do I Plan the VPCs for a New Connection?

You have already connected your on-premises network to a VPC using a connection. To connect to a new VPC using a new connection, you need to perform the following operations:

1. Delete the virtual interface and virtual gateway created for the VPC in sequence.
   a. **Delete the virtual interface**.
   b. **Delete the virtual gateway**.
2. To connect to the new VPC, you need to create a virtual gateway and virtual interface for this VPC, and associate them with the new connection.
   a. **Create a virtual gateway**.
   b. **Create a virtual interface**.

CAUTION

The preceding operations will interrupt network connectivity.

2.9 What Are Local and Remote Gateways (Interconnection IP Addresses)?

- The local gateway provides an IP address used by the cloud to connect to your on-premises network. After you configure **Local Gateway** on the console, the IP address will be automatically delivered to the gateway used by the cloud.
- The remote gateway provides an IP address used by the on-premises data center to connect to the cloud. After you configure **Remote Gateway** on the console, you need to configure the IP address on the interface of the on-premises device.

CAUTION

The local and remote gateways must be in the same IP address range. You need to plan this IP address range by yourself. This IP address range cannot conflict with that used by your on-premises network. Generally, a subnet with a 30-bit mask is recommended.

2.10 How Do I Configure BFD for a Connection?

What Is BFD?

Bidirectional Forwarding Detection (BFD) is a network protocol designed to detect faults between two forwarding devices connected by a link.

Default BFD Configuration

Table 2-1 Default parameter settings

Parameter	Default Value
Global BFD	Disabled
Interval for sending BFD control packets	1,000 ms
Interval for receiving BFD control packets	1,000 ms
Local detection multiplier	3
WTR time	0

Parameter	Default Value
Delay before a BFD session becomes Up	0
Priority of BFD packets	7

BFD Support for Static Routing

Unlike dynamic routing, static routes do not have a dedicated detection mechanism. If a fault occurs, static routes cannot detect the fault, and network administrators must delete the static route. With BFD, faults on static routes can be detected.

Each static route can be bound to a BFD session. When a BFD session bound to a static route detects a fault (for example, the link changes from Up to Down), BFD reports the fault to the routing management (RM) module, which then configures the route as inactive to indicate that the route is unavailable and will be deleted from the route table. When the BFD session bound to the static route is established or the link changes from Down to Up, BFD reports the event to the RM module, which then configures the static route as active to indicate that the route is available and will be added back to the route table.

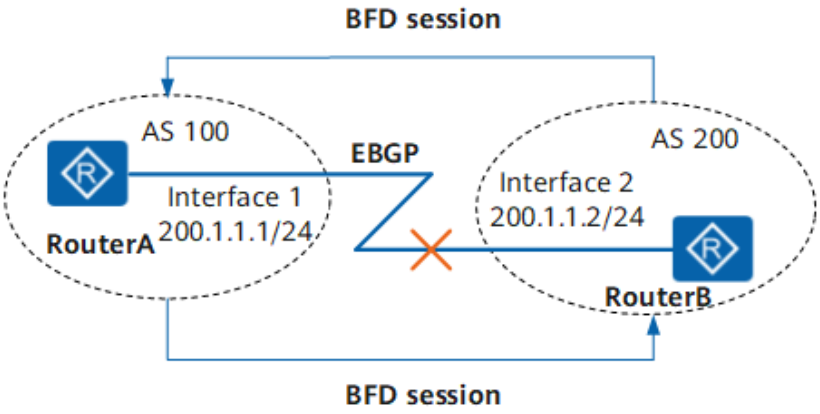
BFD Support for BGP Routing

BGP periodically sends Keepalive packets to its peers to detect faults. Detecting a fault using this mechanism takes more than 1 second. If traffic is transmitted at gigabit rates, a large number of packets will be lost. To avoid packet loss, BFD can be configured for BGP to rapidly detect faults on links between BGP peers and report the faults to BGP for fast BGP route convergence. **Table 2-2** lists the BGP convergence speeds.

Table 2-2 BGP convergence speeds

BFD Session Bound	Link Fault Detection Mechanism	Convergence Speed
Not bound	Keepalive packets	Within seconds
Bound	BFD session in the Down state	Within milliseconds

Figure 2-2 BFD support for BGP



RouterA belongs to AS 100 and RouterB belongs to AS 200. An External Border Gateway Protocol (EBGP) connection is established between RouterA and RouterB. BFD monitors the status of the EBGP connection. When the link between RouterA and RouterB becomes faulty, BFD can quickly detect the fault and notify BGP.

Verifying the BFD Configuration

You can run the following commands to view information about the configured BFD session.

- **display bfd interface** *[interface-type interface-number]*: Check the BFD-enabled interface.
- **display bfd session** {**all** | **static** | **discriminator** *discr-value* | **dynamic** | **peer-ip { default-ip** | *peer-ip* **[vpn-instance** *vpn-instance-name]* **}** | **static-auto }** **[verbose]** : View information about the BFD session.
- **display bfd statistics**: Check global BFD statistics.
- **display bfd statistics session { all** | **static** | **dynamic** | **discriminator** *discr-value* | **peer-ip default-ip** | **peer-ip** *peer-ip* **[vpn-instance** *vpn-name* **]** | **static-auto }**: Check BFD session statistics.

Troubleshooting

- **BFD Session Cannot Become Up**

  Common causes

  Common causes are as follows:

  – The link detected by the BFD session is faulty. As a result, BFD packets cannot be exchanged.

  – The BFD session frequently flaps.

  Procedure

  a. Run **display current-configuration configuration bfd** to check whether the local and remote discriminators at both ends of the BFD session match.

  ▪ If local and remote discriminators at both ends match, go to **b**.

- If the local and remote discriminators at both ends do not match, run **discriminator** to configure the local and remote discriminators of the BFD session, and then run **display bfd session all** to check whether the BFD session is Up.
  - If the value of the **State** field is **Up**, the BFD session has been established.
  - If the value of the **State** field is not **Up**, go to **b**.

b. Run **display current-configuration configuration bfd** to check whether the BFD detection time is longer than the delay before the BFD session becomes Up.

Detection time = Received Detect Multi of the remote system x Max (Local RMRI/Received DMTI)

Detect Multi is the local detection multiplier, which is configured by running the **detect-multiplier** command. The **Required Min Rx Interval (RMRI)** is the minimum interval for receiving BFD packets, which is configured by running the **min-rx-interval** command. The **Desired Min Tx Interval (DMTI)** is the minimum interval for sending BFD packets, which is configured by running the **min-tx-interval** command.

The link delay can be obtained using the **ping** or **tracert** command.

If the BFD detection time is shorter than the delay before the BFD session becomes Up, run **detect-multiplier**, **min-rx-interval**, and **min-tx-interval** to increase the BFD detection time to be longer than the delay.

- **BFD Detection Result Affects Forwarding on an Interface**

  Common causes

  The BFD session is associated with the interface status.

  Procedure

  a. Run **display interface interface-type interface-number** to check the status of the interface bound to the BFD session.

  - If the value of **Line protocol current state** is **UP**, the interface status is affected by the BFD session status. When the BFD session detects a link fault, the interface enters the **BFD status down** state. Go to **2**.
  - If the value of **Line protocol current state** is **Up** but the interface cannot forward packets, the forwarding module is working normally.

  b. Run **display bfd session all** to view the BFD session status.

  If the BFD session is **Down**, go to **3**.

  c. Run **display current-configuration configuration bfd-session** to check the BFD session configuration and check whether the **process-interface-status** command is configured.

  If the **process-interface-status** command is configured, the interface enters the **DOWN (BFD status down)** state when the BFD session detects a link fault and enters the **Down** state. As a result, the interface cannot forward packets.

- **Modified BFD Parameters Do Not Take Effect**

  Common causes

The configuration is not committed after BFD session parameters are modified.

NOTE

Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide Huawei technical support personnel.

Procedure

Run **display current-configuration configuration bfd-session** to check the BFD session configuration and check whether the **commit** command is configured.

If the **commit** command is configured, the modified BFD parameters are committed.

If the **commit** command is not used, the modified BFD parameters are not committed. Run **commit** to commit the configuration.

3 Leased Line

3.1 How Long Does It Take to Establish Connectivity Between an On-premises Data Center and the Cloud?

Generally, this depends on how long it takes the carrier to deploy the leased line, which depends where your on-premises data center is located and on the Direct Connect location you select.

- If your on-premises data center and location are in different cities, it will take three to four months.
- If your on-premises data center and location are in the same city, it will take two to three months.

3.2 How Do I Select a Carrier When Purchasing a Connection?

1. Confirm which carriers are available at the Direct Connect location you select. Different locations may have different carriers available.
2. Select the one that best meets your requirements based on their price, network performance, and other features.

3.3 What Should I Consider When Connecting My On-Premises Data Center to the Cloud Using Direct Connect?

Consider the following when you connect your on-premises data center to the cloud using Direct Connect:

- **Port speed**: Direct Connect supports 1GE, 10GE, 40GE, and 100GE single-mode optical ports. (Single fiber access is not supported.)
- **Connection type**: You can create standard connections or request hosted connections.

  - A standard connection has a dedicated port for your exclusive use and can be associated with multiple virtual interfaces.
  - If you request a hosted connection from a partner, you share a port with other users, and you can create only one virtual interface for your connection. The partner allocates the required VLAN and bandwidth for your connection.
- **How a port is ordered**: You can request a self-service connection or a full-service connection.
  - Self-service connection: Huawei Cloud only provides the port. You need to create a connection on the console, lease a line from a carrier, and use the line to connect your on-premises data center to the Direct Connect location you have selected.
  - Full-service connection: You only need to create a connection on the console, and Huawei Cloud will complete all operations required for network connectivity.
- **Routing mode**: There are static routing and BGP routing.
  - Static routes are configured for access to the cloud over the connection.
  - BGP is used for more flexible and efficient access.

4 Interconnection with the Cloud

4.1 Can I Access the Same VPC over Multiple Connections?

Yes.

To do so, you need to create multiple virtual interfaces, and select the same virtual gateway but different connections for each virtual interface.

4.2 How Do I Plan the CIDR Blocks for a Connection?

- The CIDR block of the VPC, the CIDR block of the local and remote gateways, and the CIDR block used by the on-premises network cannot conflict with each other.
- To avoid conflicts with cloud service addresses, do not use 127.0.0.0/8, 169.254.0.0/16, 224.0.0.0/3 or 100.64.0.0/10 for your on-premises network.

4.3 What Should I Consider When I Use Direct Connect to Access the Cloud?

- Connection reliability: At least two connections are terminated at different locations to work as backup for each other.
- Bandwidth and port specifications: Select a 1GE port if the bandwidth of the leased line is 1 Gbit/s or lower. Select a 10GE, 40GE, or 100GE port if the bandwidth ranges from 1 Gbit/s to 100 Gbit/s.
- Port type: You can use an optical port or an electrical port. If you want to use an optical port, consider compatibility with optical modules at both ends, including the transmission distance and device brand.

4.4 Does Direct Connect Support NAT?

No.

During hybrid cloud networking, plan different IP address ranges for the cloud and your premises. If IP address ranges conflict, use NAT for your on-premises network.

4.5 Can the VLAN of the On-premises Network Be Used in the VPC Through Direct Connect?

No.

On-premises networks can only communicate with the cloud at Layer 3.

4.6 Can My On-Premises Data Center Access Multiple VPCs Through One Connection?

Yes. You can use either of the following methods to access multiple VPCs, depending on the type of your connection:

- If you use a standard connection, you can create multiple virtual gateways and virtual interfaces to access different VPCs.
- If you have a hosted connection, you can only create one virtual interface and virtual gateway, and you can set up VPC Peering connections to connect the VPC associated with your virtual gateway to the VPCs you want to access.

4.7 Can Direct Connect Be Used with Similar Services of Other Cloud Service Providers?

Yes.

Direct Connect can be used together with similar services provided by other cloud service providers.

5 Networking and Scenarios

5.1 Can Multiple Connections Access the Same VPC?

Yes.

To do so, you need to create multiple virtual interfaces, and select the same virtual gateway but different connections for each virtual interface.

5.2 Can My On-Premises Data Center Access Multiple VPCs Through One Connection?

Yes. You can use either of the following methods to access multiple VPCs, depending on the type of your connection:

- Standard connection: You can create multiple virtual gateways and virtual interfaces to associate with different VPCs.
- If you have a hosted connection, you can only create one virtual interface and virtual gateway, and you can set up VPC Peering connections to connect the VPC associated with your virtual gateway to the VPCs you want to access.

5.3 Can Direct Connect Be Used with Similar Services of Other Cloud Service Providers?

Yes.

Direct Connect can be used together with similar services provided by other cloud service providers.

5.4 Can I Limit the Bandwidth Available on Each Hosted Connection?

Yes.

Hosted connections share the bandwidth of an operations connection, and the rate can be limited on your end or on the end user's device.

5.5 How Do I Plan the VPCs for a New Connection?

You have already connected your on-premises network to a VPC using a connection. To connect to a new VPC using a new connection, you need to perform the following operations:

1. Delete the virtual interface and virtual gateway created for the VPC in sequence.
   a. **Delete the virtual interface**.
   b. **Delete the virtual gateway**.
2. To connect to the new VPC, you need to create a virtual gateway and virtual interface for this VPC, and associate them with the new connection.
   a. **Create a virtual gateway**.
   b. **Create a virtual interface**.

CAUTION

The preceding operations will interrupt network connectivity.

5.6 How Do I Plan the ASN for Interconnection Between Direct Connect and Enterprise Router?

To ensure the stable running and efficient management of Direct Connect connections, you are advised to comply with the following ASN planning principles:

- Do not use reserved ASNs.

  Do not use 64512 as the ASN of the on-premises data center or enterprise router. This ASN is reserved for Direct Connect. If this ASN is used, there may be route conflicts or configuration exceptions.
- Plan independent ASNs.

  If a connection is used to access multiple VPCs in different regions, you are advised to plan independent ASNs for the global DC gateway and enterprise router in each region to:
  - Prevent BGP route learning conflicts between regions.
  - Ensure the routes that direct traffic to or from instances in each region are independent and secure.
  - Help with network management and troubleshooting.

Good ASN planning improves connection reliability and management, keeping networks stable when a connection is used to access multiple VPCs across regions.

6 Related Console Operations

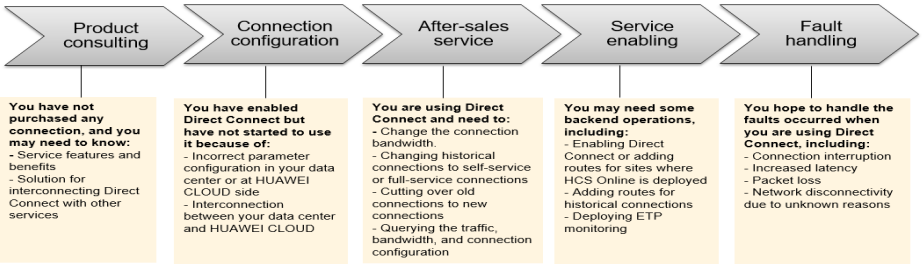
6.1 How Do I Submit a Service Ticket?

1. Log in to the management console.
2. In the upper right corner, choose **Service Tickets** > **Create Service Ticket**.
3. Choose **More Products**, and click **Direct Connect** under **Network**.
4. Select the service ticket type.

NOTE

When you **submit a service ticket**, selecting a ticket type can accelerate problem handling.

Figure 6-1 Ticket types



6.2 How Can I Unsubscribe from Direct Connect?

Unsubscribing from a Self-Service Connection

You can only unsubscribe from connections that are in the **Normal** state.

1. Go to the **Connections** page.
2. In the upper left corner of the page, click  and select a region and project.
3. Locate the connection that you want to unsubscribe from and click **Unsubscribe** in the **Operation** column.

4. Locate the target connection and click **Unsubscribe from Resource** in the **Operation** column.
5. On the displayed page, select the reason for unsubscription, confirm the refund amount, and select **I understand a handling fee will be charged for this unsubscription.**
6. Click **Confirm**.

Unsubscribing from a Full-Service Connection

Currently, self-service connections cannot be unsubscribed from on the console. Contact your customer manager to unsubscribe from your connection.

6.3 What Parameters Can Be Modified After I Have Created a Virtual Interface?

You can modify the name, bandwidth, remote subnet, and description.

To modify the VLAN, local gateway, and remote gateway, you need to delete the virtual interface and create a new one.

6.4 Do I Need to Delete the Virtual Gateway and Virtual Interface Before Deleting a Hosted Connection?

Yes. You need to delete the virtual interface associated with the hosted connection before deleting the hosted connection.

However, you can keep the virtual gateway and associate it with other hosted connections later.

6.5 How Do I Change the Routing Mode of a Connection?

Delete the virtual interface associated with the connection and create another virtual interface. Select the routing mode you want when you create the virtual interface.

CAUTION

Deleting the original virtual interface will interrupt network connectivity of the connection, which will be resumed after you associate the new virtual interface with the connection.

6.6 How Do I Delete a Hosted Connection?

Scenario

If you do not need a hosted connection, contact your partner to delete it.

Procedure

1. Go to the **Connections** page.
2. In the upper left corner of the page, click  and select a region and project.
3. In the operations connection list, locate the operations connection that the hosted connection is hosted on and click **Manage Hosted Connection** in the **Operation** column.
4. In the hosted connection list, locate the hosted connection you want to delete and click **Delete** in the **Operation** column.
5. Click **OK**.

6.7 What Is the BGP ASN Used by Huawei Cloud?

The BGP ASN of Huawei Cloud ranges from 1 to 4294967295. Generally, the BGP ASN of Huawei Cloud is 64512 by default.

6.8 What Are Local and Remote Gateways (Interconnection IP Addresses)?

- The local gateway provides an IP address used by the cloud to connect to your on-premises network. After you configure **Local Gateway** on the console, the IP address will be automatically delivered to the gateway used by the cloud.
- The remote gateway provides an IP address used by the on-premises data center to connect to the cloud. After you configure **Remote Gateway** on the console, you need to configure the IP address on the interface of the on-premises device.

CAUTION

The local and remote gateways must be in the same IP address range. You need to plan this IP address range by yourself. This IP address range cannot conflict with that used by your on-premises network. Generally, a subnet with a 30-bit mask is recommended.

7 Troubleshooting

7.1 What Are Common Troubleshooting Methods for Direct Connect?

Connectivity Issues

If network connectivity is abnormal after you have connected the leased line to the endpoint device, perform the following steps to locate the fault:

1. Verify that the network device is connected correctly, auto-negotiation is disabled for the optical port, and the port speed and full-duplex mode are configured correctly.
2. Verify that optical signals can be normally transmitted and received.

Network Issues

If the connection fails to work normally after you created a virtual interface to connect your on-premises network to the cloud, perform the following steps to locate the fault:

1. Verify that the local gateway can be pinged from the remote gateway and that the VLAN of the intermediate device is configured correctly.
2. Verify that IP addresses of the local and remote gateways are in the same CIDR block and are configured on the VLAN sub-interfaces.
3. If static routing is used, verify that the next hop or outbound interface of the static route is configured correctly.
4. If BGP routing is used, verify that:
   - BGP ASN, BGP MD5 authentication key, and BGP peer IP address are configured correctly.
   - BGP ASNs on both gateways are different.
   - There are no more than 100 BGP routes propagated through the virtual interface.
   - There are no rules for prohibiting TCP port 179 or dynamic TCP ports.

Routing Issues

If static routes have been delivered for the virtual interface or a BGP peer relationship has been established, perform the following steps to locate the fault:

Accessing a VPC through Direct Connect

1. Verify that the routes between your gateway and your on-premises network are reachable.
2. Verify that the routes to your on-premises network are propagated and correctly configured in the remote subnet of the virtual interface if static routing is configured for the virtual interface, or BGP is used to route traffic to your on-premises network if you have selected BGP routing.
3. Verify that the VPC CIDR block is correctly configured on the virtual gateway.
4. Verify that the security group and network ACL rules allow inbound and outbound traffic.

Accessing a VPC Through Direct Connect and Enterprise Router

1. Verify that the routes between your gateway and your on-premises network are reachable.
2. Verify that the routes to your on-premises network are propagated and correctly configured in the remote subnet of the virtual interface if static routing is configured for the virtual interface, or BGP is used to route traffic to your on-premises network if you have selected BGP routing.
3. Verify that the enterprise router route table contains the association and propagation of the global DC gateway attachment, the routes destined for your on-premises network (with the next hop set to the global DC gateway), and the routes destined for the VPC you want to access (with the next hop set to the VPC).
4. Verify that routes whose destination is your on-premises network and next hop is the enterprise router are added to your VPC route table.
5. Verify that the security group and network ACL rules allow inbound and outbound traffic.

7.2 How Do I Test the Network Connectivity Between a Location and the Cloud?

To test network connectivity between the location you select and the cloud, add the CIDR block where the local and remote gateways reside to the remote subnet you configure when creating the virtual interface, and then ping the IP address of the local gateway from a VM on the cloud.

If the test fails, check whether:

- The VM is in the VPC associated with the virtual gateway.
- The VM IP address is within the local subnet configured when you create the virtual gateway.
- Security group rules and network ACL rules of the VM allow traffic from the VM to the local gateway configured for the virtual interface.

8 Billing

8.1 How Will I Be Billed for Direct Connect?

You can create a standard connection, which will give you exclusive access to the port. You can also request a hosted connection from a partner and share the port with other users.

Billed Items

This section describes the billed items of self-service connections, full-service connections, and hosted connections.

Billed Items of a Self-Service Connection

Billed items of a standard connection include the port, one-time setup, leased line, and in-building cabling. Huawei Cloud billed items include the port and one-time setup. Non-Huawei Cloud billed items include the leased line and in-building cabling.

For details, see **Table 8-1**.

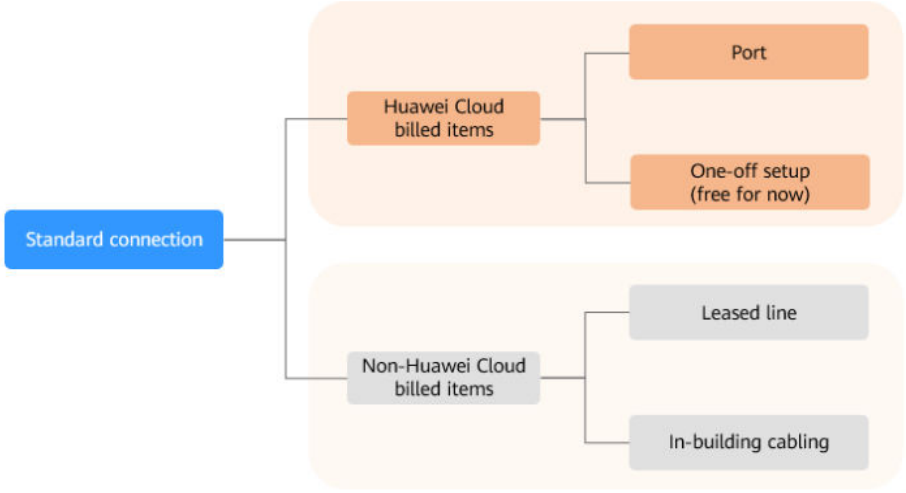


Table 8-1 Billed items of a self-service connection

Billed Items	Description	Billing Mode	Formula
Port	The port is billed based on its specifications.	Yearly/ Monthly (prepaid)	Unit price × Duration For port prices, see **Direct Connect Pricing Details**.
One-time setup	Currently, the one-time setup is free.	Free	Free
Leased line	You need to pay to the carrier for the line that is used to connect your on-premises data center to the Direct Connect location you select.	Pay for the leased line to the carrier.	Consult the carrier.
In-building cabling	A fiber may be required for connecting your leased line to the equipment room at the Direct Connect location you select if the data center at the Direct Connect location is a carrier-neutral data center.	You pay for the property of the data center for in-building cabling.	Consult the property of the data center.

Billed Items of a Full-Service Connection

Billed items of a full-service connection include port, one-time setup, leased line, and in-building cabling. You pay for all these items to Huawei Cloud.

For details, see **Table 8-2**.

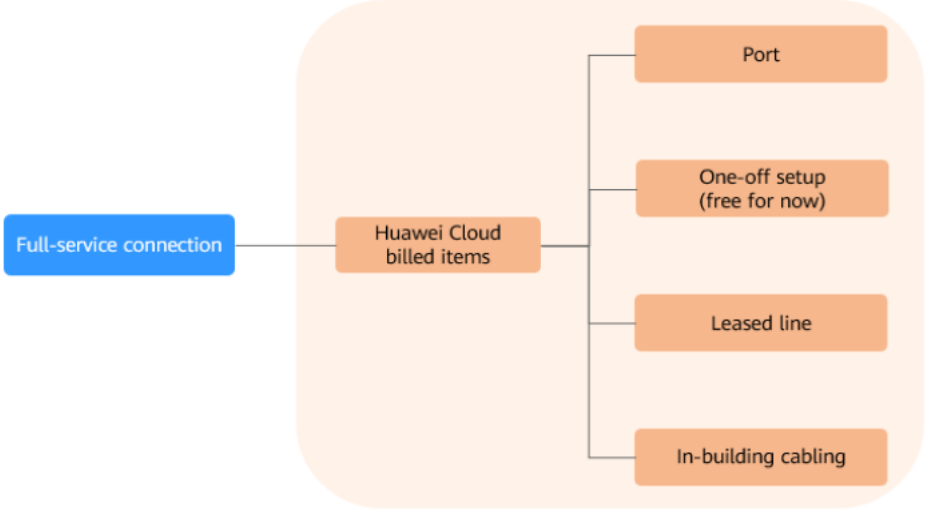


Table 8-2 Billed items of a full-service connection

Billed Items	Description	Billing Mode	Formula
Port	The port is billed based on its specifications.	Yearly/Monthly (prepaid)	Unit price × Duration For port prices, see **Direct Connect Pricing Details**.
One-time setup	Currently, the one-time setup is free.	Free	Free
Leased line	You need to pay to the carrier for the line that is used to connect your on-premises data center to the Direct Connect location you select.	Pay for it to Huawei Cloud.	-
In-building cabling	A fiber may be required for connecting your leased line to the equipment room at the Direct Connect location you select if the data center at the Direct Connect location is a carrier-neutral data center.		-

Billed Items of a Hosted Connection

To use a hosted connection, you only need to pay the partner for the leased line.

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

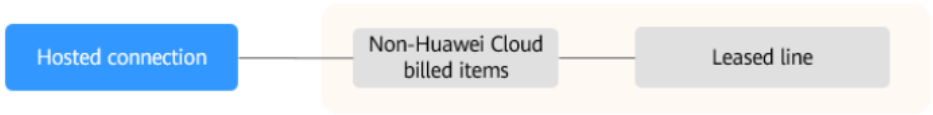


Table 8-3 Billing items of a hosted connection

Billed Items	Description	Billing Mode	Formula
Leased line	You need to pay to the carrier for the line that is used to connect your on-premises data center to the Direct Connect location you select.	Pay the partner for the leased line.	Consult the partner.

Billing Mode

Yearly/Monthly

Changing Billing Mode

Only Yearly/Monthly billing is supported, and it cannot be changed.

Renewal

For details, see **Renewal Management**.

Expiration and Overdue Payment

For details, see **Service Suspension and Resource Release** and **Payment and Repayment**.

8.2 Can I Renew My Connections?

Yes. You can perform the following operations to renew a connection:

1. Log in to the management console.
2. In the service list, choose **Networking** > **Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect** > **Connections**.
4. Locate the connection you want to renew and choose **More** > **Renew** in the **Operation** column.
5. Set the duration that you want to renew the connection and click **Pay**. Then pay the order as prompted.

8.3 How Can I Unsubscribe from Direct Connect?

Unsubscribing from a Self-Service Connection

You can only unsubscribe from connections that are in the **Normal** state.

1. Go to the **Connections** page.
2. In the upper left corner of the page, click  and select a region and project.
3. Locate the connection that you want to unsubscribe from and click **Unsubscribe** in the **Operation** column.
4. Locate the target connection and click **Unsubscribe from Resource** in the **Operation** column.
5. On the displayed page, select the reason for unsubscription, confirm the refund amount, and select **I understand a handling fee will be charged for this unsubscription.**
6. Click **Confirm**.

Unsubscribing from a Full-Service Connection

Currently, self-service connections cannot be unsubscribed from on the console. Contact your customer manager to unsubscribe from your connection.

8.4 Is a Connection Still Available After Being Frozen?

After a connection expires, it is frozen and cannot be used. If you renew a frozen connection, it will become available again.

If you do not renew the connection within a certain amount of time, it will be deleted, and can no longer be renewed.

8.5 Can I Unsubscribe from a Connection in the Creating State?

No.

You can only unsubscribe from connections that are in the **Normal** state.

8.6 Can I Change the Port Type After a Connection Is Created?

No. The port type cannot be changed after a connection is created.

There are four port types: 1GE, 10GE, 40GE, and 100GE. If you expand or reduce the capacity of a port, the connection price will be changed. In this case, you need to unsubscribe from the connection and request a new one.

Helpful Links

- **Creating a Connection**
- **Unsubscribing from a Connection**

9 Resource Monitoring

9.1 How Do I Monitor the Network Quality of a Direct Connect Connection?

The network quality of connections is monitored using two plug-ins, and there are two key metrics: network latency and packet loss rate.

Direct Connect provides two monitoring plug-ins:

- dc-nqa-collector: monitors the connections requested on the Direct Connect console.
- history-dc-nqa-collector: monitors historical connections.

For details, see **Installing the Direct Connect Metric Collection Plug-ins**.

Table 9-1 Network quality metrics

Metric	Metric Name	Meaning	Value Range	Monitored Object	Monitoring Interval
latency	Latency	Network latency of data transmission over a connection Unit: ms	≥ 0 ms	Connections and historical connections	1 minute

Metric	Metric Name	Meaning	Value Range	Monitored Object	Monitoring Interval
packet_loss_rate	Packet Loss Rate	Rate of packets lost during data transmission over a connection Unit: Percentage	0–100%	Connections and historical connections	1 minute

9.2 What Are Direct Connect Metrics?

Function

Use the management console or call APIs provided by Cloud Eye to query the metrics of the monitored objects and alarms generated for Direct Connect.

Namespace

SYS.DCAAS

Metrics

Table 9-2 Direct Connect metrics

Metric	Metric Name	Meaning	Value Range	Monitored Object	Monitoring Interval
network_incoming_bits_rate	Network Incoming Bandwidth	Bit rate for inbound data to the Direct Connect side of a connection Unit: bit/s	≥ 0 bits/s	Connections and historical connections	1 minute
network_outgoing_bits_rate	Network Outgoing Bandwidth	Bit rate for outbound data from the Direct Connect side of a connection Unit: bit/s	≥ 0 bits/s	Connections and historical connections	1 minute

Metric	Metric Name	Meaning	Value Range	Monitored Object	Monitoring Interval
network_incoming_bytes	Network Incoming Traffic	Number of bytes for inbound data to the Direct Connect side of a connection Unit: byte	≥ 0 bytes	Connections and historical connections	1 minute
network_outgoing_bytes	Network Outgoing Traffic	Number of bytes for outbound data from the Direct Connect side of a connection Unit: byte	≥ 0 bytes	Connections and historical connections	1 minute
network_incoming_packets_rate	Network Incoming Packet Rate	Packet rate for inbound data to the Direct Connect side of a connection Unit: Packet/s	≥ 0 packets/s	Connections and historical connections	1 minute
network_outgoing_packets_rate	Network Outgoing Packet Rate	Packet rate for outbound data from the Direct Connect side of a connection Unit: Packet/s	≥ 0 packets/s	Connections and historical connections	1 minute
network_incoming_packets	Network Incoming Packets	Number of packets for inbound data to the Direct Connect side of a connection Unit: Packet	≥ 0 packets	Connections and historical connections	1 minute
network_outgoing_packets	Network Outgoing Packets	Number of packets for outbound data from the Direct Connect side of a connection Unit: Packet	≥ 0 packets	Connections and historical connections	1 minute

Dimensions

Key	Value
direct_connect_id	Connection
history_direct_connect_id	Historical connection

9.3 How Can I View Direct Connect Metrics?

1. Log in to the management console.
2. On the console homepage, click  in the upper left corner and select the desired region and project.
3. In the service list, choose **Management & Governance** > **Cloud Eye**.
4. In the navigation pane on the left, choose **Cloud Service Monitoring** > **Direct Connect**.
5. Click **View Metric** in the **Operation** column.

   You can view data of the last 1, 3, 12, or 24 hours, or last 7 days.

10 Quota

10.1 What Are Resource Quotas of Direct Connect?

The following table lists the quotas of connections, virtual gateways, and virtual interfaces.

Resource	Default Quota	How to Increase Quota
Number of connections that can be created by an account in each region	10	**Submit a service ticket**.
Number of global DC gateways that can be created by an account in each region	5	**Submit a service ticket**.
Number of virtual interfaces that can be created by an account in each region	50	**Submit a service ticket**.
Number of local subnets for a virtual gateway	50	Increasing the quota is not allowed.
Number of routes for BGP sessions on a virtual interface	100	**Submit a service ticket**.
Number of remote subnets for a virtual interface	50	**Submit a service ticket**.

NOTE

For details about how to view or increase the quota, see **Quotas**.

10.2 How Many Hosted Connections Can a Partner Create on an Operations Connection?

A partner can create up to 1,000 hosted connections on an operations connection.

NOTE

The bandwidth of all hosted connections cannot exceed that of the operations connection.

Helpful Links

- Operations Connections
- Hosted Connections

