Direct Connect

FAQ

Issue 01

Date 2024-02-29

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 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 in the cloud. In addition, key parameters such as the LC, wavelength, and distance must be aligned with the Direct Connect location you select, for example, 1GE, LC, single-mode, 1310nm, 10 KM.

- Auto-negotiation for the port must be disabled. Port speed and full-duplex mode must be manually configured.

- 802.1Q VLAN encapsulation must be supported on the entire connection, including intermediate devices.

- Your device must support BGP and BGP MD5 authentication or static routing.

- (Optional) You can configure BFD on your network.

- The maximum transmission unit (MTU) supported at the physical layer cannot exceed 1,522 bytes (14-byte Ethernet header + 4-byte VLAN tag + 1,500-byte IP datagram + 4-byte frame check sequence). The recommended value is 1500.

- Private IP addresses are recommended both on and off the cloud, and the IP address ranges used for communications cannot overlap.

1.2 What Locations Are Available for Direct Connect?

A Direct Connect location provides access to Huawei Cloud in a region. Before using Direct Connect to access Huawei Cloud, you need to obtain the details about each location.

Direct Connect provides a number of locations for you to choose from. You can **request a port** when creating a connection.

For more information, **submit a service ticket** or contact your Direct Connect manager.

Table 1-1 Direct Connect locations

Geographic Region	City	Region	Location	IDC
Chinese mainland	Beijing	CN North-Beijing4	Langfang-Guangyang-Huawei	Huawei
			Beijing-Tongzhou-Huitian	Huitian
			Beijing-Yizhuang-Centrin	Centrin Data Systems
			Beijing-Yizhuang-Yatai	Yatai Zhongli
			Beijing-Chaoyang-Jiuxianqiao	Jiuxianqiao
			Langfang-GDS	Carrier-neutral data center
			Langfang-Runze-China Telecom	China Telecom
Chinese mainland	Shanghai	CN East-Shanghai2	Shanghai-Pudong-GDS	GDS
			Shanghai-Baoshan-Baoxin	Baoxin
			Shanghai-Jiading-Sinnet	Sinnet
	Suzhou	CN East-Shanghai1	Suzhou-Kunshan-GDS	GDS
			Suzhou-Wuzhong-Guoke	China Unicom
			Suzhou-Wujiang-Fenhu-China Mobile	China Mobile
			Hangzhou Research Center	Huawei
			Cloud data center of Hangzhou Iron & Steel Group	Carrier-neutral data center
			Shanghai-GDS	Carrier-neutral data center
			Shanghai-Baoxin	China Mobile

Geographic Region	City	Region	Location	IDC
			Suzhou-Kunshan-Kunhui	Kunshan Kunhui
			Suzhou-Wuzhong-Huawei Base	Huawei
			Shanghai-Sinnet	Sinnet
	Guangzhou	CN South-Guangzhou	Guangzhou-Huangpu-Huaxinyuan	Bigone
			Guangzhou-Fanyu-University town	Bigone
			Guangzhou-Mingmei-China Unicom	China Unicom
			Guangzhou-Hualong-China Unicom	China Unicom
			Guangzhou-Yunpu-China Telecom	China Telecom
			Shenzhen-Baode	Carrier-neutral data center
			Shenzhen-Nanshan	
			Shenzhen-Futian	
			Shenzhen-Yifeng	Yifeng
			Dongguan-Tuanbowa	Huawei
	Guiyang	CN Southwest-Guiyang1	Guiyang-Gui'an-China Mobile	China Mobile
			Guiyang–Gui'an–Qixinghu	Huawei
			Guiyang-Gui'an-High-end Park	Huawei
			Guiyang-Xi'an-Xigang	China Telecom
			Guiyang-Xi'an-21vianet	21vianet
Asia Pacific	Hong Kong	CN-Hong Kong	Hong Kong-Sha Tin-China Telecom	China Telecom

Geographic Region	City	Region	Location	IDC
			Hong Kong-Sai Kung-China Mobile	China Mobile
			Hong Kong-Sai Kung-Global Switch	GlobalSwitch
	Bangkok	AP-Bangkok	Bangkok-NTT	NTT
			Bangkok-TRUE	TRUE
	Singapore	AP-Singapore	Singapore-DataPro	Equinix
			Singapore-Global Switch	Global Switch
	Jakarta	AP-Jakarta	Jakarta-JK5	JK5
			Jakarta-EDGE	EDGE
Africa	Johannesburg	AF-Johannesburg	Kenya-Nairobi-Sameer Business Park	Nairobi Sameer Business Park
			Nigeria-Lagos-Medallion	Medallion
			Johannesburg-IS Parklands	Internet Solutions Parklands
			Johannesburg-Teraco	Teraco
Latin America	Mexico	LA-Mexico City1	Mexico City-COM Ixtlahuaca	COM Ixtlahuaca
			Mexico-KIO MEX 5	KIO MEX 5
		LA-Mexico City2	Mexico-Tultitlan	Carrier-neutral data center
			Bogota-Equinix	Equinix
	Sao Paulo	LA-Sao Paulo1	Sao Paulo-Equinix	Equinix
			Sao Paulo-ODATA	OData
	Lima	LA-Lima1	Lima-Telefonica	Telefonica
	Santiago	LA-Santiago	Santiago-Paine	Paine
			Santiago-Claro	Claro
Europe	Türkiye	TR-Istanbul	TR-Istanbul-Turkcell	Turkcell

Geographic Region	City	Region	Location	IDC
			TR-Istanbul-NGN	NGN
Other	Riyadh	ME-Riyadh	Riyadh-STC Khurais	STC Khurais
			Riyadh-Remal	Remal

1.3 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.

1.4 How Will I Be Billed for Direct Connect?

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

Billing Items

- **Standard connection**

  The following figure shows the fees that you need to pay for a standard connection.
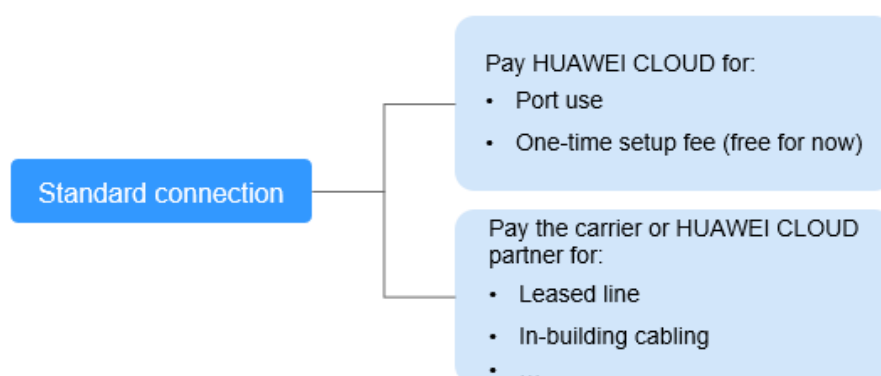
Table 1-2 Standard connection pricing

Payee	Billing Item	Description	Payment Method
Huawei Cloud	Port	The port is billed based on its specifications.	Prepaid (yearly/ monthly subscription)
	One-time setup	Currently, you are not be billed for the one-time setup.	N/A
Carrier or Huawei Cloud partner	Leased line	To connect your on-premises data center to the cloud, you need to lease a line from the carrier.	N/A
	In-building cabling	If you lease a line for a carrier, you also need to pay for the cabling inside the carrier's equipment room.	N/A

- **Hosted connection**

  If you buy a hosted connection from a Huawei Cloud partner, you share the port with other users and do not need to pay Huawei Cloud for one-time setup and the port.

  The following figure shows the fees that you need to pay for a hosted connection.

Table 1-3 Hosted connection billing details

Payee	Billing Item	Description	Payment Method
Carrier or Huawei Cloud partner	Leased line	Your partner has established network connectivity with Huawei Cloud. You need to pay the partner for the leased line.	N/A

For details, see **Product Pricing Details**.

Billing Mode

Only yearly/monthly subscription is available.

Changing Billing Mode

Currently, only **Yearly/Monthly** 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**.

1.5 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**.

Figure 1-1 Service Tickets
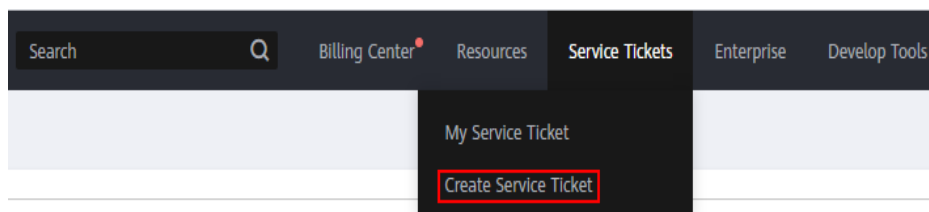
3. Choose **More Products**, and click **Direct Connect** under **Network**.

Figure 1-2 Direct Connect
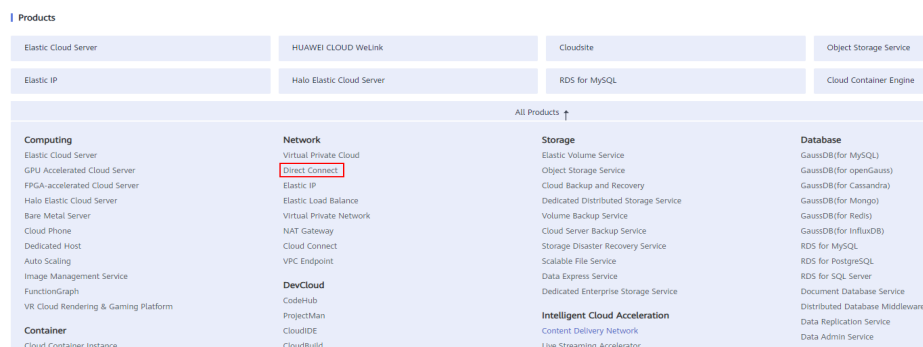
4. Select the service ticket type.

Figure 1-3 Select Subtype
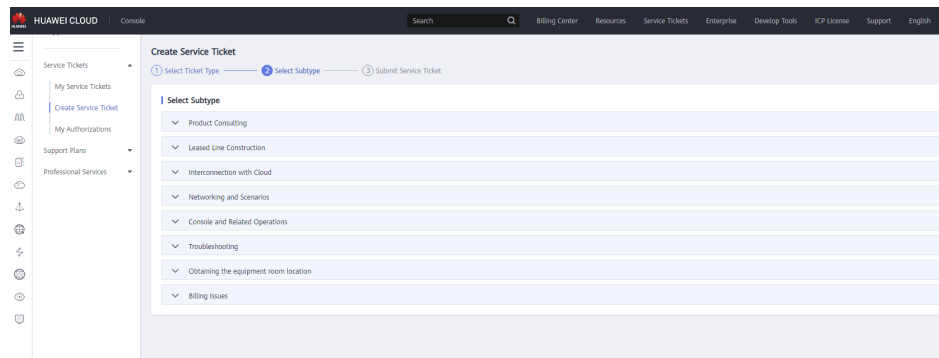
📖 **NOTE**

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

Figure 1-4 Ticket types

1.6 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.

1.7 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 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 in the cloud. In addition, key parameters such as the LC, wavelength, and distance must be aligned with the Direct Connect location. Examples of optical module parameters: 1 GE, LC single-mode, 1310 nm, and 10 km

- Auto-negotiation for the port must be disabled. Port speed and full-duplex mode must be manually configured.

- 802.1Q VLAN encapsulation must be supported on the entire connection, including intermediate devices.

- Your device must support BGP and BGP MD5 authentication or static routing.

- (Optional) You can configure BFD on your network.

- The maximum transmission unit (MTU) supported at the physical layer cannot exceed 1,522 bytes (14-byte Ethernet header + 4-byte VLAN tag + 1,500-byte IP datagram + 4-byte frame check sequence). The recommended value is 1500.

- Private IP addresses are recommended both on and off the cloud, and the IP address ranges used for communications cannot overlap.

2.2 What Are 1GE and 10GE?

GE is short for Gigabit Ethernet.

1GE indicates 1 Gbit/s bandwidth, and 10GE indicates 10 Gbit/s bandwidth. They are the maximum bandwidth supported by the ports.

2.3 What Locations Are Available for Direct Connect?

A Direct Connect location provides access to Huawei Cloud in a region. Before using Direct Connect to access Huawei Cloud, you need to obtain the details about each location.

Direct Connect provides a number of locations for you to choose from. You can **request a port** when creating a connection.

For more information, **submit a service ticket** or contact your Direct Connect manager.

Table 2-1 Direct Connect locations

Geographic Region	City	Region	Location	IDC
Chinese mainland	Beijing	CN North-Beijing4	Langfang-Guangyang-Huawei	Huawei
			Beijing-Tongzhou-Huitian	Huitian
			Beijing-Yizhuang-Centrin	Centrin Data Systems
			Beijing-Yizhuang-Yatai	Yatai Zhongli
			Beijing-Chaoyang-Jiuxianqiao	Jiuxianqiao
			Langfang-GDS	Carrier-neutral data center
			Langfang-Runze-China Telecom	China Telecom
Chinese mainland	Shanghai	CN East-Shanghai2	Shanghai-Pudong-GDS	GDS
			Shanghai-Baoshan-Baoxin	Baoxin
			Shanghai-Jiading-Sinnet	Sinnet
	Suzhou	CN East-Shanghai1	Suzhou-Kunshan-GDS	GDS
			Suzhou-Wuzhong-Guoke	China Unicom

Geographic Region	City	Region	Location	IDC
			Suzhou-Wujiang-Fenhu-China Mobile	China Mobile
			Hangzhou Research Center	Huawei
			Cloud data center of Hangzhou Iron & Steel Group	Carrier-neutral data center
			Shanghai-GDS	Carrier-neutral data center
			Shanghai-Baoxin	China Mobile
			Suzhou-Kunshan-Kunhui	Kunshan Kunhui
			Suzhou-Wuzhong-Huawei Base	Huawei
			Shanghai-Sinnet	Sinnet
	Guangzhou	CN South-Guangzhou	Guangzhou-Huangpu-Huaxinyuan	Bigone
			Guangzhou-Fanyu-University town	Bigone
			Guangzhou-Mingmei-China Unicom	China Unicom
			Guangzhou-Hualong-China Unicom	China Unicom
			Guangzhou-Yunpu-China Telecom	China Telecom
			Shenzhen-Baode	Carrier-neutral data center
			Shenzhen-Nanshan	
			Shenzhen-Futian	
			Shenzhen-Yifeng	Yifeng
			Dongguan-Tuanbowa	Huawei

Geographic Region	City	Region	Location	IDC
	Guiyang	CN Southwest-Guiyang1	Guiyang-Gui'an-China Mobile	China Mobile
			Guiyang–Gui'an–Qixinghu	Huawei
			Guiyang-Gui'an-High-end Park	Huawei
			Guiyang-Xi'an-Xigang	China Telecom
			Guiyang-Xi'an-21vianet	21vianet
Asia Pacific	Hong Kong	CN-Hong Kong	Hong Kong-Sha Tin-China Telecom	China Telecom
			Hong Kong-Sai Kung-China Mobile	China Mobile
			Hong Kong-Sai Kung-Global Switch	GlobalSwitch
	Bangkok	AP-Bangkok	Bangkok-NTT	NTT
			Bangkok-TRUE	TRUE
	Singapore	AP-Singapore	Singapore-DataPro	Equinix
			Singapore-Global Switch	Global Switch
	Jakarta	AP-Jakarta	Jakarta-JK5	JK5
			Jakarta-EDGE	EDGE
Africa	Johannesburg	AF-Johannesburg	Kenya-Nairobi-Sameer Business Park	Nairobi Sameer Business Park
			Nigeria-Lagos-Medallion	Medallion
			Johannesburg-IS Parklands	Internet Solutions Parklands
			Johannesburg-Teraco	Teraco
Latin America	Mexico	LA-Mexico City1	Mexico City-COM Ixtlahuaca	COM Ixtlahuaca

Geographic Region	City	Region	Location	IDC
			Mexico-KIO MEX 5	KIO MEX 5
		LA-Mexico City2	Mexico-Tultitlan	Carrier-neutral data center
			Bogota-Equinix	Equinix
	Sao Paulo	LA-Sao Paulo1	Sao Paulo-Equinix	Equinix
			Sao Paulo-ODATA	OData
	Lima	LA-Lima1	Lima-Telefonica	Telefonica
	Santiago	LA-Santiago	Santiago-Paine	Paine
			Santiago-Claro	Claro
Europe	Türkiye	TR-Istanbul	TR-Istanbul-Turkcell	Turkcell
			TR-Istanbul-NGN	NGN
Other	Riyadh	ME-Riyadh	Riyadh-STC Khurais	STC Khurais
			Riyadh-Remal	Remal

2.4 Is BGP Routing Supported in Direct Connect?

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

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

- **Accessing a VPC over a Connection Through BGP Routes**
- **Accessing a VPC over Two Connections Through BGP Routes**

2.5 What Is Full-Service Installation Statement?

Before creating a full-service connection, you need to read, have fully understood, and agreed to the content in the *Huawei Cloud Direct Connect Full-Service Installation Statement*.

The details are as follows:

1. **Definition**

   Full-service installation refers to the process where Huawei Cloud completes all work required to create a connection that links your premises to the cloud after you submit a request or pay for the order.

2. **Delivery and Acceptance**

   a. You are responsible for preparing the environment and completing in-building cabling (if any) in your on-premises data center to ensure that

Huawei Cloud can enter the site and complete all required work. You shall bear the cost of the in-building cabling. The delay of service provisioning caused due to your reason will not be counted in the delivery time, and Huawei Cloud will not be responsible for the delivery.

b. After the service is enabled, Huawei Cloud will notify you of commissioning and acceptance. After receiving the notification, you shall complete the acceptance within three (3) working days. If the criteria are met, you shall verify the functions on the console and confirm the billing information. If the commissioning does not meet acceptable standards, continue commissioning until the service meets acceptance criteria. If you fail to confirm or raise any objection in writing within three working days after receiving the notification from Huawei Cloud, you are deemed to have agreed that the service has been enabled as required and that Huawei Cloud can start charging you for using the service.

c. Acceptance criteria:

   i. No packets are lost when your CE device is pinged from the Direct Connect gateway in the data center at the location you selected and 5000 packets are sent with each containing 1400 bytes.

   ii. The port BER is less than ten to the negative seventh power (10^{-7}).

3. **Service Period and Termination**

   The service period of a full-service connection is one (1) year, starting from the date when billing starts. If you need to terminate the service in advance, Huawei Cloud will still charge you for the remaining service period.

4. **Availability**

   Huawei Cloud shall make reasonable commercial and technical efforts to ensure that the SLA of connections terminated at different locations reaches 99.95%. To ensure stable service running and high availability, you are advised to purchase multiple connections that are terminated at different locations. If you purchase a single Direct Connect connection or multiple Direct Connect connections terminated at one location, services may be affected due to a faulty connection, carrier cutover, or maintenance at the location. You must understand and accept the risk.

   For more details, see the **Huawei Cloud Service Level Agreement**.

2.6 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**.

   Figure 2-1 Service Tickets
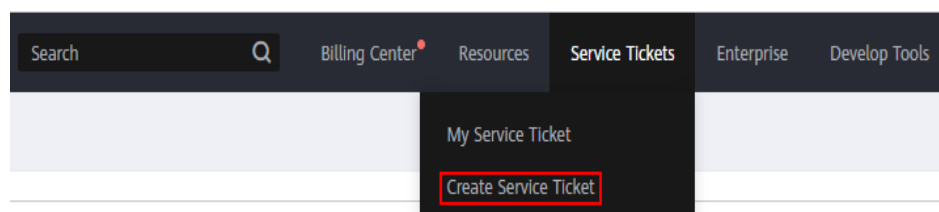
3. Choose **More Products**, and click **Direct Connect** under **Network**.

Figure 2-2 Direct Connect
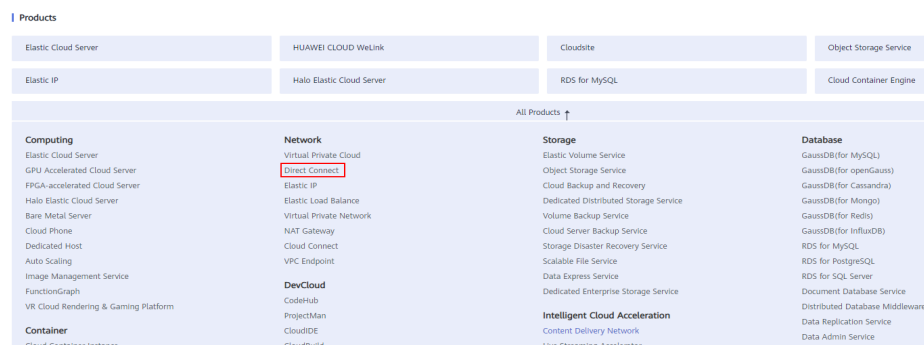
4. Select the service ticket type.

Figure 2-3 Select Subtype
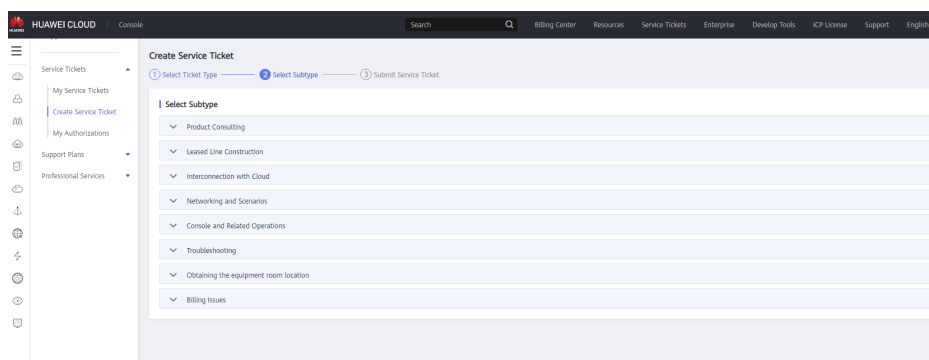
📖 **NOTE**

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

Figure 2-4 Ticket types
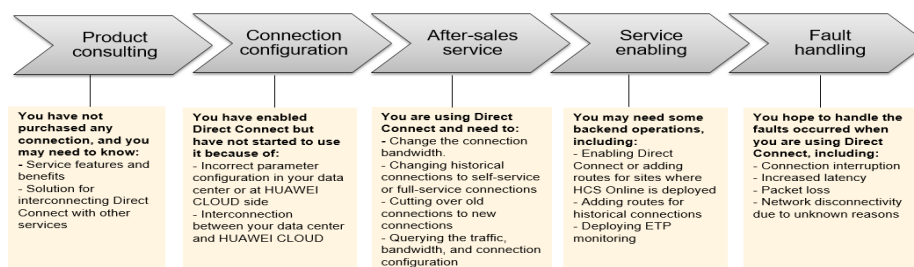
2.7 What Are the Network Latency and Packet Loss Rate of a Connection?

Huawei Cloud monitors the latency and packet loss rate from a VM to the Direct Connect gateway. To obtain the latency and packet loss rate from the Direct Connect gateway to your equipment room, contact the carrier from whom you leased the line.

2.8 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.

2.9 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.

2.10 How Can I Change the VPC Associated with My Connection?

Delete the virtual gateway and virtual interface associated with the old VPC, create a new virtual gateway and a new virtual interface, and associate them with the new VPC.

2.11 What Are IP Addresses for Interconnection in Direct Connect?

IP addresses for interconnection refer to the IP addresses of the local and remote gateways. The local gateway is the gateway on the Huawei Cloud network, and the remote gateway is on your on-premises network.

⚠ **CAUTION**

The local gateway and remote gateway must be in the same IP address range. Generally, a subnet with a 30-bit mask is recommended.

2.12 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 2-2 Default parameter settings

Parameter	Default Value
Global BFD	Disabled
Interval for sending BFD control packets	1000 ms
Interval for receiving BFD control packets	1000 ms
Local detection multiplier	3
WTR time	0
Delay before a BFD session becomes Up	0
Priority of BFD packets	7

BFD Support for Static Routing

Unlike dynamic routing protocols, 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 2-3** lists the BGP convergence speeds.

Table 2-3 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 2-5 BFD support for BGP
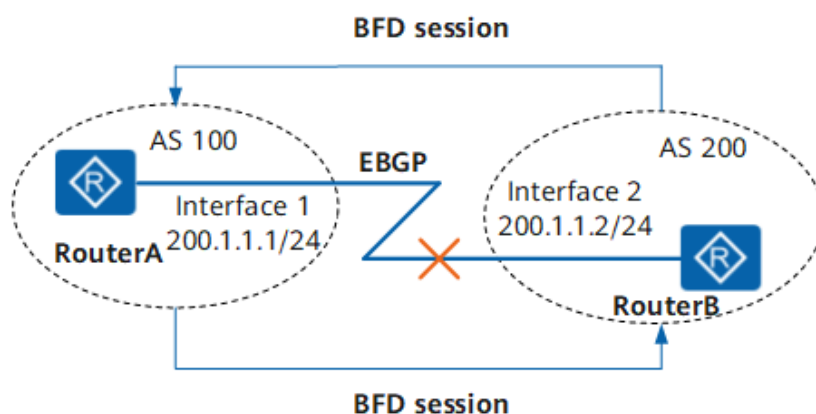
RouterA belongs to AS 100 and RouterB belongs to AS 200. An External Border Gateway Protocol (EBGP) connection is established between RouterA and RouterB. BFD monitors the status of the EBGP connection. When the link between RouterA and RouterB becomes faulty, BFD can quickly detect the fault and notify 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 Construction

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 Access Modes Does Direct Connect Support?

Huawei Cloud supports 1GE and 10GE single-mode optical ports. Single fiber access is not supported.

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 Can I Change the VPC Associated with My Connection?

Delete the virtual gateway and virtual interface associated with the old VPC, create a new virtual gateway and a new virtual interface, and associate them with the new VPC.

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**.

Figure 6-1 Service Tickets
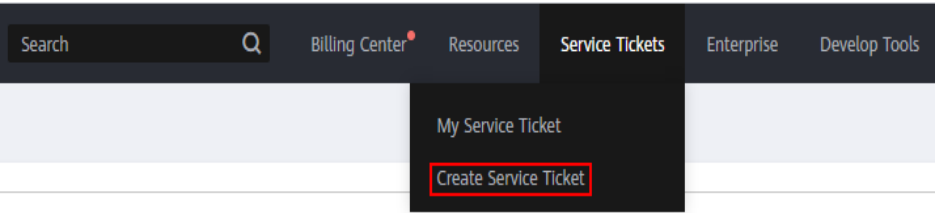
3. Choose **More Products**, and click **Direct Connect** under **Network**.

Figure 6-2 Direct Connect

4. Select the service ticket type.

Figure 6-3 Select Subtype
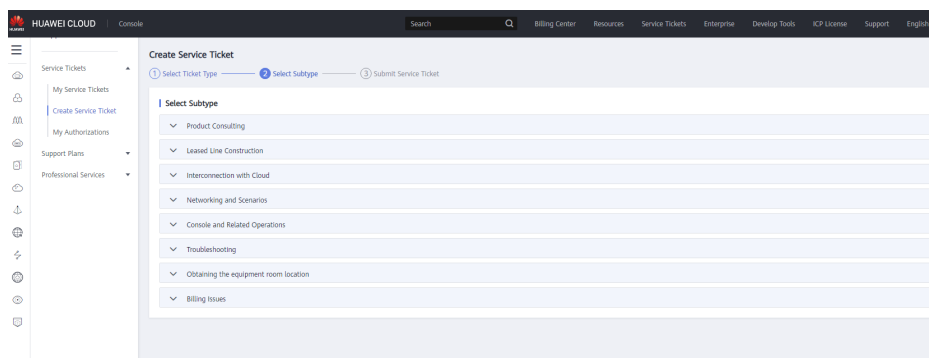
☐ **NOTE**

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

Figure 6-4 Ticket types
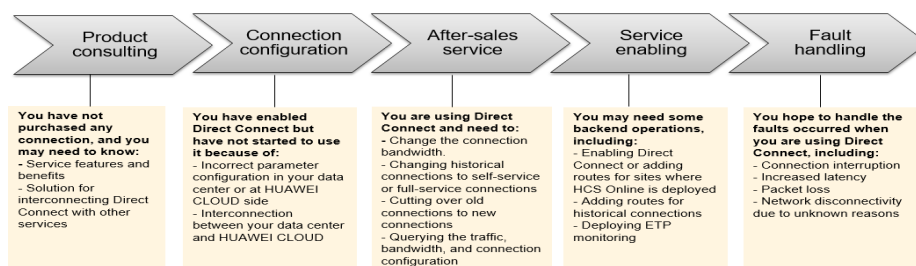
6.2 How Can I Unsubscribe from Direct Connect?

Scenarios

If you do not need to use a self-service connection any longer, you can unsubscribe from it.

☐ **NOTE**

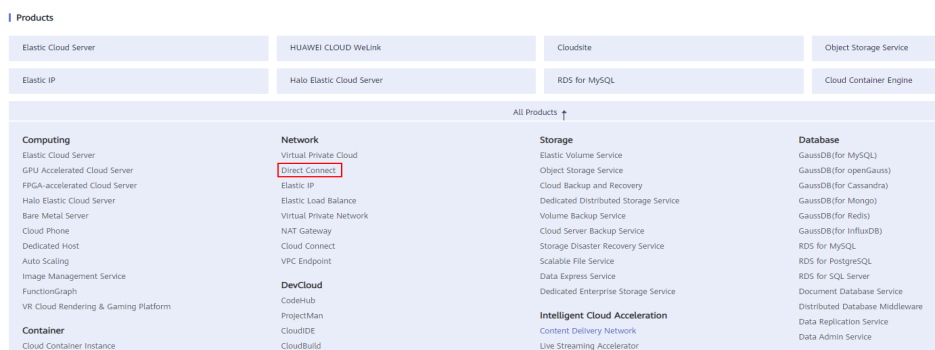You can only unsubscribe from connections that are in the **Normal** state. If a connection is being created, you can unsubscribe from it after the connection is created.

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?

To delete a hosted connection, contact the partner who created the hosted connection for you.

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.

For details, see **Table 6-1**.

Table 6-1 Default BGP ASNs in different Huawei Cloud regions

Region	Default Value
Direct Connect locations except some in the CN North-Beijing1 and AP-Bangkok regions	64512
CN North-Beijing1	65533

Region	Default Value
AP-Bangkok	The BGP ASN of some Direct Connect locations is 65535 by default. For details, contact the Direct Connect manager.

6.8 What Are IP Addresses for Interconnection in Direct Connect?

IP addresses for interconnection refer to the IP addresses of the local and remote gateways. The local gateway is the gateway on the Huawei Cloud network, and the remote gateway is on your on-premises network.

⚠ **CAUTION**

The local gateway and remote gateway must be in the same IP address range. 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 properly after you created a virtual interface to connect your on-premises network to Huawei 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:

1. Verify that the routes from your gateway to 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, and that BGP routes are used to route traffic to your on-premises network if you select 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.

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, or request a hosted connection from a partner and share the port.

Billing Items

- **Standard connection**

  The following figure shows the fees that you need to pay for a standard connection.
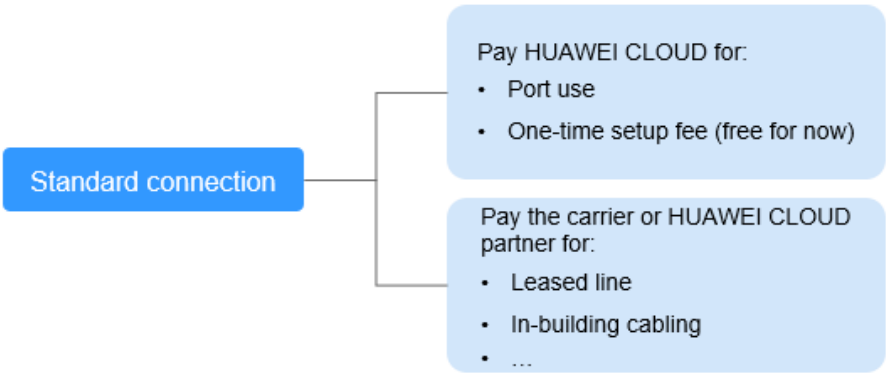

Table 8-1 Standard connection pricing

Payee	Billing Item	Description	Payment Method
Huawei Cloud	Port	The port is billed based on its specifications.	Prepaid (yearly/ monthly subscription)

Payee	Billing Item	Description	Payment Method
	One-time setup	Currently, you are not be billed for the one-time setup.	N/A
Carrier or Huawei Cloud partner	Leased line	To connect your on-premises data center to the cloud, you need to lease a line from the carrier.	N/A
	In-building cabling	If you lease a line for a carrier, you also need to pay for the cabling inside the carrier's equipment room.	N/A

- **Hosted connection**

  If you buy a hosted connection from a Huawei Cloud partner, you share the port with other users and do not need to pay Huawei Cloud for one-time setup and the port.

  The following figure shows the fees that you need to pay for a hosted connection.

Table 8-2 Hosted connection billing details

Payee	Billing Item	Description	Payment Method
Carrier or Huawei Cloud partner	Leased line	Your partner has established network connectivity with Huawei Cloud. You need to pay the partner for the leased line.	N/A

For details, see **Product Pricing Details**.

Billing Mode

Only yearly/monthly subscription is available.

Changing Billing Mode

Currently, only **Yearly/Monthly** 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. Hover on ≡ to display **Service List** and choose **Networking** > **Direct Connect**.

3. In the navigation pane on the left, choose **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?

1. Log in to the management console.

2. Hover on ≡ to display **Service List** and choose **Networking** > **Direct Connect**.

3. In the navigation pane on the left, choose **Direct Connect** > **Connections**.

4. Locate the connection that you want to unsubscribe from and choose **More** > **Unsubscribe** in the **Operation** column.

5. Locate the target connection and click **Unsubscribe from Resource** in the **Operation** column.

6. On the **Unsubscribe** page, select the reason for unsubscription, confirm the refund amount, and select **I understand a Handling fees will be charged for this unsubscription**.

7. Click **Confirm**.

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. If a connection is being created, you can unsubscribe from it after the creation is complete.

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

No. If you want to change the port type of a connection, you need to unsubscribe from the connection and create another 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.

The following are the two plug-ins:

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

For details, see **Installing 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 transmissio n over a connection Unit: Percentage	0–100%	Connection s and historical connection s	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_inc oming_bits_ rate	Networ k Incomi ng Bandwi dth	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_ou tgoing_bits_ rate	Networ k Outgoi ng Bandwi dth	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_conne ct_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 [icon] in the upper left corner and select the desired region and project.
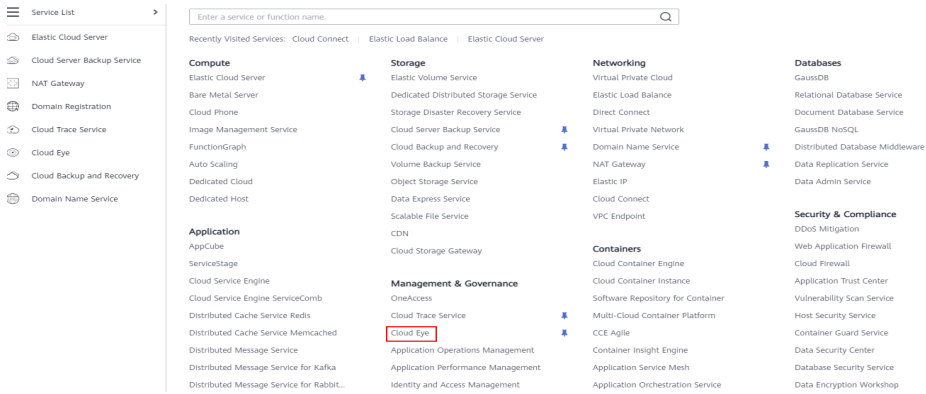
3. Hover on [icon] to display **Service List** and choose **Management & Governance** > **Cloud Eye**.

   Figure 9-1 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	Adjustable
Number of connections that can be created by an account in each region	10	**Submit a service ticket**.
Number of virtual 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 routes for BGP sessions on a virtual interface	100	**Submit a service ticket**.
Number of remote subnets on 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 a maximum of 1000 hosted connections on a single operations connection. The total bandwidth of all hosted connections cannot exceed the bandwidth of the operations connection.