ALIBABA CLOUD

Alibaba Cloud

智能接入网关

Troubleshooting

Document Version: 20220331

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

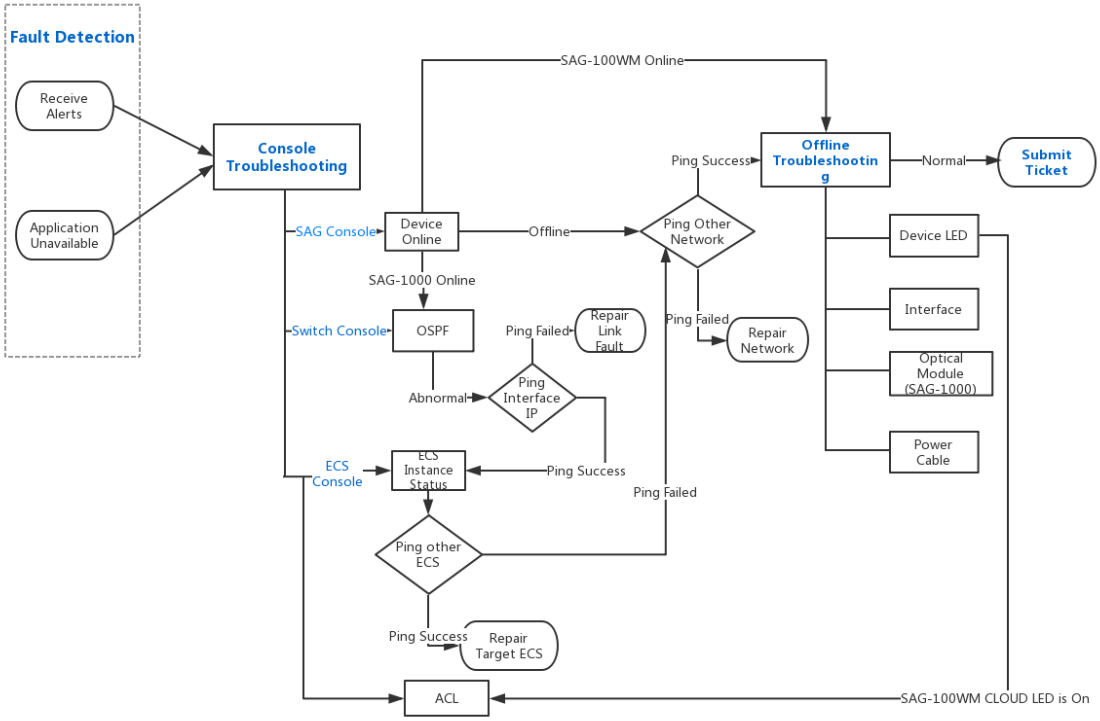
Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Handle device faults

This topic describes how to observe the symptoms, collect relevant information, analyze the situation, and handle the faults when Smart Access Gateway (SAG) device faults occur.

The following figure shows the procedure of handling SAG device faults.



Handle SAG-100WM faults

Take the following steps to handle SAG-100WM faults. For more information, see Handle failures of pinging Alibaba Cloud resources through SAG-100WM.

1. You receive alerts or find that you have trouble connecting to Alibaba Cloud.
2. Log on to the SAG console to view the status of the SAG-100WM device.
3. Make an attempt to access other public websites to check whether the status of the ISP connection is normal.
4. Check the SAG-100WM device.
5. Check the security group rules.
6. Submit a ticket.

Handle SAG-1000 faults

Take the following steps to handle SAG-1000 faults. For more information, see Handle failures of pinging an ECS instance through SAG-1000 and Handle connection failures to a local terminal.

1. You receive alerts or find that you have trouble connecting to Alibaba Cloud.
2. Log on to the SAG console to view the status of the SAG-1000 device.

3. Log on to the switch console to view the status of the Open Shortest Path First (OSPF) connections.
4. Log on to the ECS console to view the status of the target instance.
5. Make an attempt to access other public websites to check whether the status of the ISP connection is normal.
6. Check the SAG-1000 device.
7. Submit a ticket.

2.View and query the device status

2.1. Indicators

Different indicator colors and blinking states represent different states of a Smart Access Gateway (SAG) device.

Device	LED indicator	Description
SAG-100WM	LTE	Indicates the communication status of the device: • On or off: abnormal communication. • Blinking: device communicating as expected.
	Signal indicator	The number of bars indicates the strength of the 4G LTE signal. Three bars indicate the strongest signal.
	WAN	Indicates the Ethernet usage status: • On or off: abnormal Ethernet connection. • Blinking: transferring data over the Ethernet.
	WIFI	Indicates the Wi-Fi connection status: • On or off: abnormal Wi-Fi connection. • Blinking: transferring data over Wi-Fi.
	RUN/SYS	Indicates the system status: • On or off: system not working as expected. • Blinking: system working as expected.
	CLOUD	Indicates whether the device is connected to Alibaba Cloud: • On: connected to Alibaba Cloud. • Blinking: restoring the system or restoring to default settings. • Off: not connected to Alibaba Cloud.
	PWR	Indicates whether the device is powered on. On: device powered on. Off: device powered off.
	RJ45 yellow light	Indicates the connection status and speed of the network interface controller (NIC): • On: Ethernet port working in 1000Base-T mode. • Off: Ethernet port working in 10/100Base-T mode.
	RJ45 green light	Indicates the connection status and speed of the NIC: • On: Ethernet connected. • Blinking: transferring data. • Off: Ethernet not connected.

Device	LED indicator	Description
SAG-1000	LTE	Indicates the communication status of the device: • On or off: abnormal communication. • Blinking: device communicating as expected.
	Signal indicator	The number of bars indicates the strength of the 4G LTE signal. Three bars indicate the strongest signal.
	SYS	Indicates the system status: • On or off: system not working as expected. • Blinking: system working as expected.
	CLOUD	Indicates whether the device is connected to Alibaba Cloud: • On: connected to Alibaba Cloud. • Blinking: restoring the system or restoring to default settings. • Off: not connected to Alibaba Cloud.
	PWR	Indicates whether the device is powered on. On: device powered on. Off: device powered off.
	RJ45 yellow light	Indicates the connection status and speed of the NIC: • On: Ethernet port working in 1000Base-T mode. • Off: Ethernet port working in 10/100Base-T mode.
	RJ45 green light	Indicates the connection status and speed of the NIC: • On: Ethernet connected. • Blinking: transferring data. • Off: Ethernet not connected.
	Some SAG devices use the following indicators:	
	⏻	Indicates whether the device is powered on. On: device powered on. Off: device powered off.
	⚠	Indicates whether the device is working as expected: • Green: device working as expected. • Yellow: device having faults.
	☁	Indicates whether the device is connected to Alibaba Cloud: • Green: device connected to Alibaba Cloud. • Yellow: device not connected to Alibaba Cloud.

2.2. View the device status

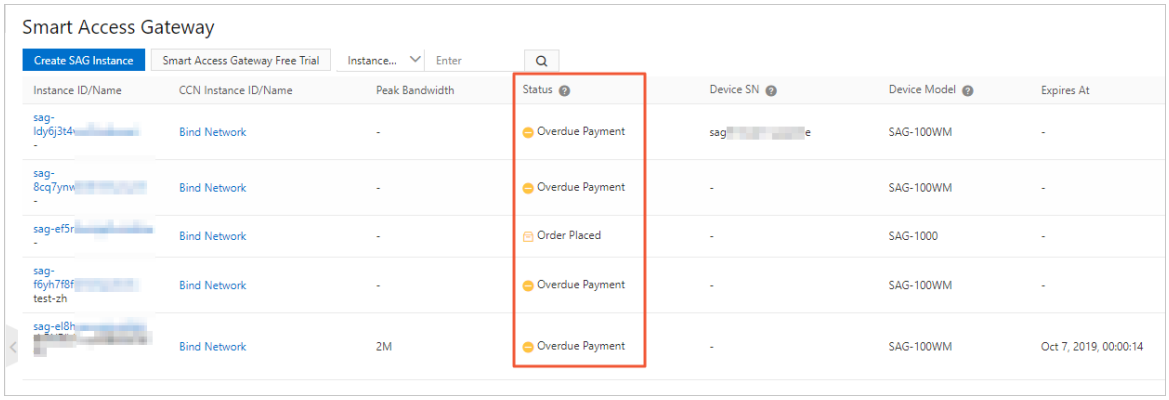
You can log on to the Smart Access Gateway (SAG) console to view the status of an SAG device.

Procedure

1. Log on to the SAG console.
2. In the **Status** column, you can view the status of an SAG device.

   Different states include:

   - Ready: The SAG device is ready for use.
   - Disconnected: The SAG device is not connected to Alibaba Cloud.
   - Not Associated: The SAG device is not associated with a Cloud Connect Network (CCN) instance or a virtual border router (VBR).
   - Order Placed: The order has been placed and the package is not dispatched.
   - Order Shipped: The package has been dispatched. After you receive the package, sign for it.
   - Overdue Payment: The SAG device is unavailable due to overdue payments.



2.3. View the connection status

You can log on to the Smart Access Gateway (SAG) console to view the connection status of an SAG device. When a system fault occurs, switch to another connection.

Procedure

1. Log on to the SAG console.
2. On the **Smart Access Gateway** page, click the ID of a target instance.
3. On the page that appears, click **Configure High Availability** to view the connection status of the SAG device.
   - Green: The connection is normal.
   - Red: The connection has faults.

2.4. Query the OSPF status

If your service is unavailable and the Open Shortest Path First routing protocol is used, you can use a switch to test the connectivity between the switch and a Smart Access Gateway (SAG) device.

Procedure

1. Run the following command to log on to the web console of the switch.

   ```
   telnet The IP address of the switch
   ```

> **Note** The command may vary based on the switch. For more information, see the manual provided by the manufacturer. A certain type of switch is used in this example.

2. Run the following command to query the status of a neighbor connection.

```
show ip ospf neighbor
```

You can view the values in the State column, as shown in the following sample code.

```
OSPF process 1, 8 Neighbors, 8 is Full:
Neighbor ID     Pri   State           BFD State  Dead Time   Address         Inter
face
10.10.**.**       0   Full/ -         -          00:00:10    192.168.**.**    Giga
bitEthernet 0/13
10.10.**.**       0   Full/ -         -          00:00:10    192.168.**.**   Gigab
itEthernet 0/46
```

3. Run the following commands to query the OSPF configurations.

```
configure terminal
router ospf
show this
```

You can view the IP addresses in the area and network rows, as shown in the following sample code.

```
Building configuration...
 !
 router-id 1.1.**.**
 area 1 nssa translator always default-information-originate no-summary
 area 2 nssa translator always default-information-originate no-summary
 area 3 nssa translator always default-information-originate no-summary
 area 17 nssa translator always default-information-originate no-summary
 area 18 nssa translator always default-information-originate no-summary
 area 81 nssa translator always default-information-originate no-summary
 area 90 nssa translator always default-information-originate no-summary
 area 91 nssa translator always default-information-originate no-summary
 network 192.168.**.** 0.0.**.** area 1
 network 192.168.**.** 0.0.**.** area 1
 network 192.168.**.** 0.0.**.** area 1
 network 192.168.**.** 0.0.**.** area 2
 network 192.168.**.** 0.0.**.** area 2
 network 192.168.**.** 0.0.**.** area 0
 network 192.168.**.** 0.0.**.** area 81
 network 192.168.**.** 0.0.**.** area 81
 network 192.168.**.** 0.0.**.** area 81
 network 192.168.**.** 0.0.**.** area 81
 network 192.168.**.** 0.0.**.** area 90
 network 192.168.**.** 0.0.**.** area 90
 network 192.168.**.** 0.0.**.** area 91
 network 192.168.**.** 0.0.**.** area 91
 network 192.169.**.** 0.0.**.** area 17
 network 192.169.**.** 0.0.**.** area 17
 network 192.169.**.** 0.0.**.** area 18
 network 192.169.**.** 0.0.**.** area 18
 !
end
```

4. Run the following command to query the port status of an SAG device.

   ```
   show ip interface brief
   ```

   - up: The port is working as expected.
   - administratively down: The port is manually disabled. You can run the **no shutdown** command to enable the port.
   - down: The network cable is not connected to the port. Check the network cable.

   Sample output:

```
Interface                      IP-Address(Pri)      IP-Address(Sec)      Status
Protocol
GigabitEthernet 0/2            no address           no address           down
down
GigabitEthernet 0/7            192.168.**.**/24       no address           up
up
GigabitEthernet 0/11           9.9.**.**/24           no address           down
down
GigabitEthernet 0/12           192.168.**.**/24     no address           up
up
GigabitEthernet 0/13           192.168.**.**/30     no address           up
up
```

```
GigabitEthernet 0/15            192.168.**.**/24      no address          down
down
GigabitEthernet 0/20            192.168.**.**/30      no address          up
up
GigabitEthernet 0/22            192.168.**.**/30      192.169.**.**/30     up
up
                                                      192.168.**.**/24
GigabitEthernet 0/23            192.168.**.**/30      192.169.**.**/30     up
up
GigabitEthernet 0/27            192.169.**.**/30      no address          up
up
GigabitEthernet 0/28            192.169.**.**/30      no address          up
up
GigabitEthernet 0/29            192.169.**.**/30      192.168.**.**/30     up
up
                                                      192.169.**.**/30
GigabitEthernet 0/30            192.169.**.**/30      no address          up
up
GigabitEthernet 0/33            192.168.**.**/30      192.168.68.6/30     down
down
GigabitEthernet 0/35            192.169.**.**/30      no address          up
up
GigabitEthernet 0/36            192.169.**.**/30      no address          up
up
GigabitEthernet 0/37            192.168.**.**/30      192.169.**.**/30     down
down
                                                      192.168.**.**/30
GigabitEthernet 0/38            192.168.**.**/30      192.169.**.**/30     down
down
GigabitEthernet 0/39            192.168.**.**/30      192.169.**.**/30     administra
tively down  down
                                                      192.168.**.**/30
GigabitEthernet 0/40            192.168.**.**/30      192.169.**.**/30     up
up
GigabitEthernet 0/43            192.168.**.**/24     no address          up
up
GigabitEthernet 0/45            192.168.**.**/30     no address          down
down
GigabitEthernet 0/46            192.168.**.**/30     no address          up
up
GigabitEthernet 0/48            192.168.**.**/30    no address          down
down
Loopback 0                      no address           no address          up
down
VLAN 1                          no address           no address          up
down
VLAN 4                          192.168.**.**/24      no address          up
down
VLAN 19                         192.168.**.**/30      no address          up
down
VLAN 47                         192.168.**.**/24     no address          up
down
VLAN 148                        172.16.**.**/24       no address          up
up
```

5. Run the following commands to check whether the OSPF negotiation time and authentication parameter values are the same as those configured on the SAG device.

```
interface GigabitEthernet 0/39
show this
```

Check whether the values of the ospf authentication and ospf message-digest-key parameters are the same as those configured on the SAG device. If not, the SAG device fails the authentication and cannot establish neighbor relationship with the switch.

Sample output:

```
Building configuration...
 !
 poe enable
 no switchport
 ip ospf network point-to-point
 ip ospf authentication message-digest
 ip ospf message-digest-key 23 md5 888
 ip ospf hello-interval 3
 ip ospf dead-interval 10
 ip ospf priority 0
 no ip proxy-arp
 ip address 192.168.**.** 255.255.255.252
 ip address 192.169.**.** 255.255.255.252 secondary
 ip address 192.168.**.** 255.255.255.252 secondary
 !
end2 secondary
```

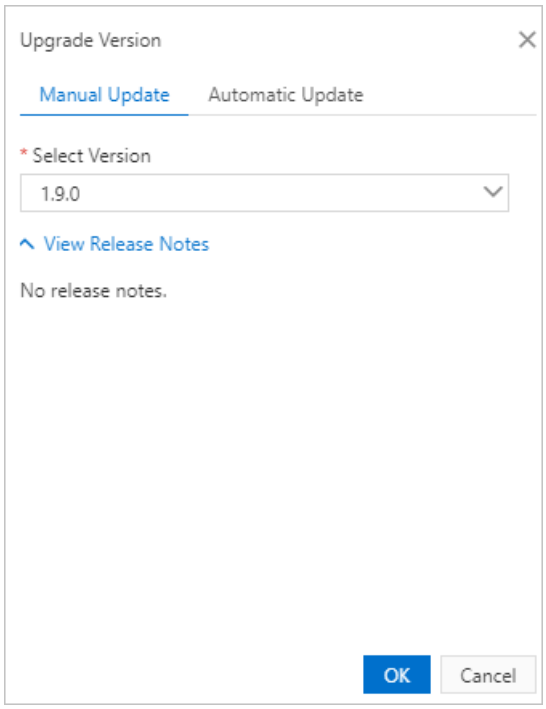
3.Maintain the system

3.1. Update an SAG device

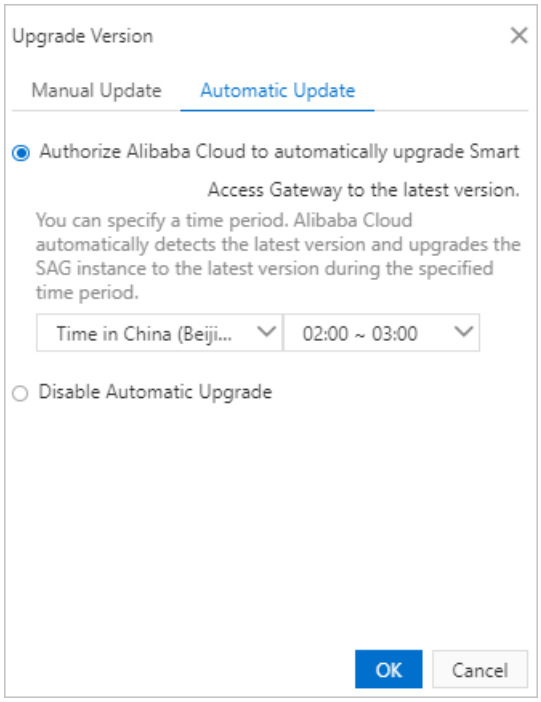
In the Smart Access Gateway (SAG) console, you can update the software version of an SAG device.

Procedure

1. Log on to the Smart Access Gateway console.
2. Use one of the following methods to open the **Device Management** tab.
   - Click the ID of the target SAG instance. On the instance details page that appears, click the **Device Management** tab.
   - Find the target SAG instance and choose > **Device Management** in the **Actions** column.
3. If both the active and standby devices are associated with the SAG instance, select the target device and click **Upgrade Version**.
4. In the **Upgrade Version** dialog box that appears, select one of the following methods to perform an upgrade.
   - Click the **Manual Update** tab, select the target version, and then click **OK**. Your device is upgraded to the selected version.



   - Click the **Automatic Update** tab, select the **Authorize Alibaba Cloud to automatically upgrade Smart Access Gateway to the latest version** check box, select a time zone and time period, and then click **OK**. The device is upgrade to the latest version during the specified time period.



Note You can also choose to **Disable Automatic Upgrade**.

3.2. Restart an SAG device

Restarting a Smart Access Gateway (SAG) device can solve some network faults.

Context

Choose one of the following methods to restart an SAG device:

- Power off the SAG device and then power it on. We recommend that you save the current configurations before you power off the SAG device.
- Log on to the SAG console to remotely restart the SAG device.

Power off and then power on an SAG device

After you power off an SAG device, power it on.

In this case, you restart the SAG device by turning off and on the power switch.

Remote restart

To remotely restart an SAG device in the SAG console, follow these steps:

1. Log on to the SAG console.
2. On the Smart Access Gateway page, click the ID of the target instance.
3. Click **Device Management**.
4. Select the target SAG device that you want to restart, and click **Remote Restart**.
5. In the **Remote Restart** dialog box that appears, click **OK** to restart the target SAG device.

4.Handle device faults

4.1. Handle optical module faults

This topic explains the possible causes of optical module faults and provides solutions.

Symptoms

After you insert an optical module into a Smart Access Gateway (SAG) device, the indicator does not turn green.

Possible causes

The optical module is incompatible or damaged.

For more information about the optical module models supported by SAG devices, see Optical module models.

> **Note** Currently, you can only insert optical modules into SAG-1000 devices.

Procedure

1. A multi-mode optical module emits visible light. If you can see a red laser on the left of the sending port, the module is working normally. Do not look directly into the sending port.

   A single-mode optical module emits invisible light. You can use a jumper to connect the sending port and the receiving port. If the indicator turns green, the module is working normally.

2. If the indicator still does not turn green, check whether the optical module is compatible with the device.

4.2. Handle Ethernet connection failures

This topic explains why Ethernet connection failures occur and offers solutions.

Symptoms

The Ethernet port is not connected.

Possible causes

- The Smart Access Gateway (SAG) device or the neighbor device is not powered on, or the cable are not correctly connected.
- The twisted pair cable or optical fiber is too long, or the cable attenuation is too high.
- The port, port module, SAG device, or neighbor device is faulty.

Procedure

1. Check whether both the SAG and neighbor devices are powered on and whether the cable and port module are correctly connected.
2. Check whether the cable or port module of both devices is faulty.

   If the SAG and neighbor devices are connected through a twisted pair cable, check the items described in the following table.

Check item	Criteria	Solution
Use a tester to test whether the twisted pair cable is faulty.	The tester shows that the twisted pair cable is working as expected.	If the twisted pair cable is faulty, replace it.
Measure whether the length of the twisted pair cable meets the requirement.	The length of the twisted pair cable must be less than 100 meters. **Note** 10/100/1000 Mbit/s electrical ports use RJ45 connectors. Category 5 or later cables support a maximum transmission distance of 100 meters.	If the length of the twisted pair cable is more than 100 meters, choose one of the following solutions: ○ Shorten the distance between the SAG and neighbor devices to shorten the length of the twisted pair cable. ○ If you cannot change the distance, you can use a repeater, hub, or switch to connect the SAG and neighbor devices in series.
Check whether you are using the correct type of twisted pair cable.	Twisted pair cables are classified into two types: crossover and straight-through cables. A straight-through cable is used to connect Ethernet ports of the following devices: ○ A router and a hub. ○ A router and an Ethernet switch. ○ A computer and an Ethernet switch. ○ A computer and a hub. A crossover cable is used to connect Ethernet ports of the following devices: ○ Two routers. ○ A router and a computer. ○ Two hubs. ○ A hub and a switch. ○ Two switches. ○ Two computers.	Use the correct type of twisted pair cable.

If the SAG and neighbor devices are connected through an optical fiber, check the items described in the following table.

Check item	Criteria	Solution

Check item	Criteria	Solution
Check whether the optical module matches the optical fiber.	Check whether the optical module matches the optical fiber based on the following descriptions. ○ A multi-mode optical fiber works with a multi-mode optical module. ○ A single-mode optical fiber only works with a single-mode optical module, and does not work with a multi-mode optical module. A single-mode optical fiber is typically yellow, whereas a multi-mode optical fiber is typically orange. ○ The wavelength of two connected optical modules must be the same.	Use an optical module and optical fiber that match each other.
Check whether the length of the optical fiber falls into the transmission distance range supported by the optical module.	The length of the optical fiber must be less than the transmission distance supported by the optical module.	Shorten the length of the optical fiber or use an optical module that supports a longer transmission distance.
Use a tester to test whether the signal attenuation falls into the allowed range.	The range of optical signal attenuation.	If the attenuation exceeds the allowed range, replace the optical fiber. If the issue persists after you replace the optical fiber, shorten the length of the optical fiber.
Use a tester or physical loopback testing to check whether the cable is faulty.	When you use a tester, the result shows that the cable is working as expected. To perform physical loopback testing, connect both ends of the cable to the same optical module. If the port is enabled, the cable is functioning.	If the cable is faulty, replace it. If the issue persists after you replace the cable, replace the optical module.

3. Check whether the SAG or neighbor device is faulty.

4.3. Handle frequent switches of the Ethernet port status

This topic explains why the Ethernet port is frequently enabled or disabled and provides solutions.

Symptoms

The Ethernet port is frequently enabled or disabled.

Possible causes

- The cable is not correctly connected.
- The twisted pair cable or optical fiber is too long, or the cable attenuation is too high.
- The port, port module, SAG device, or neighbor device is faulty.

Procedure

1. Check whether the cable and module of the SAG and neighbor devices are correctly connected.
2. Check whether the links and interface modules of the devices are faulty.

   If the devices are connected by a twisted pair, check the items listed in the following table.

Check item	Criteria	Action
Check whether the twisted pair is faulty.	The twisted pair is normal.	Replace the twisted pair if it is faulty.
Check whether the length of the twisted pair between the two devices meets requirements.	The length of the cable between the two devices is less than 100 meters. **Note** For 10/100/1000-M electrical interfaces, RJ45 connectors and category 5 twisted pair cables (or higher) are used, with a transmission distance of 100 meters.	If the cable is longer than 100 meters, use the following methods: ○ Shorten the distance between the devices to shorten the length of the twisted pair. ○ If the distance between the devices cannot be changed, the devices can be connected in series through a repeater, hub, or switch.
Check whether the twisted pair is used correctly.	Twisted pairs are classified into straight-through twisted pairs and crossover twisted pairs. Straight-through twisted pairs are used to connect Ethernet interfaces between the following devices: ○ A router and a hub ○ A router and an Ethernet switch ○ A computer and an Ethernet switch ○ A computer and a hub Crossover twisted pairs are used to connect Ethernet interfaces between the following devices: ○ Two routers ○ A router and a computer ○ A hub and a hub ○ A hub and a switch ○ Two switches ○ Two computers	If the type of twisted pair used is incorrect, change it to the correct type.

If the devices are connected through an optical fiber, check the items listed in the following table.

Check item	Criteria	Action
Check whether the optical module corresponds to the optical fiber.	Check whether the optical module matches the optical fiber according to the following information: ○ A multi-mode optical fiber can be used with a multi-mode optical module. ○ A single-mode optical fiber can be used with a single-mode optical module, but cannot be used with a multi-mode optical module. Single-mode optical fibers are yellow and multi-mode optical fibers are orange. ○ The wave length of two connected optical modules must be consistent.	If the optical fiber and the optical module do not match, replace the optical module or the optical fiber as needed.
Check whether the length of the optical fiber matches the transmission distance supported by the optical module.	The length of the optical fiber must be shorter than the transmission distance supported by the optical module.	Shorten the length of the optical fiber or use an optical module that supports greater transmission distance.
Check whether the signal attenuation is within the allowed range.	The range of optical signal attenuation is less than - 28 dB.	If the attenuation exceeds the allowed range, replace the optical fiber. If the problem persists, shorten the length of the optical fiber.
Check whether the two ends of the link are faulty by using the loopback method or a tester.	If you use a tester, the results indicate that the sending and the receiving data flows are normal. If you use the loopback method, the interface is in the up state after you connect the two ends of the optical fiber to an optical module.	If a cable is faulty, replace the cable. If the fault persists, replace the optical modules at the two ends.

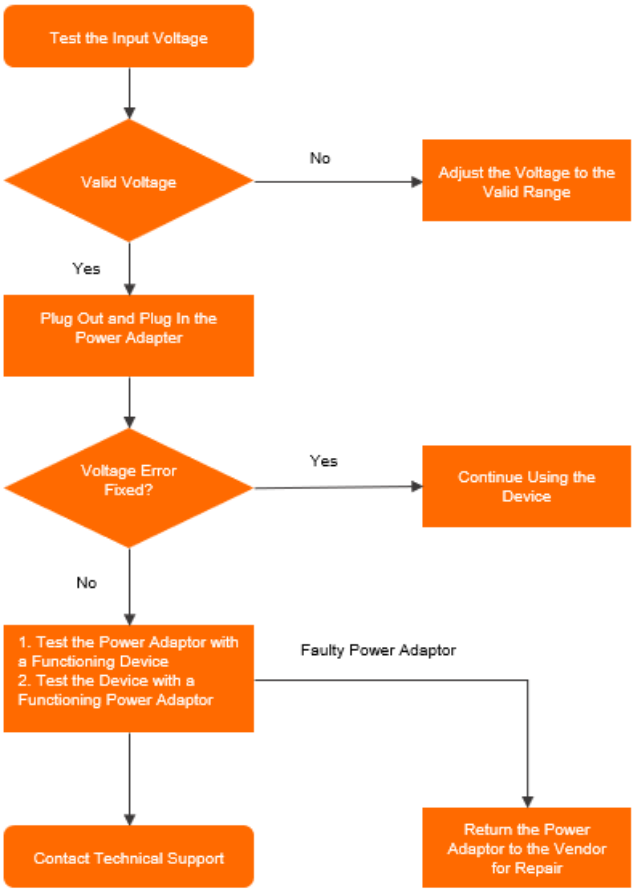
3. Check whether the SAG or neighbor device is faulty.

4.4. Locate power failures

To locate and handle power failures, follow the procedure as described below.

Flowchart

The flowchart is shown in the following figure.



Procedure

1. Measure the input voltage. Use a multimeter to measure the input voltage, and assess whether the input voltage falls outside the working voltage range.
2. Connect and disconnect the power adapter. Connect and disconnect the power adapter and the power cable to exclude loose connections.
3. Cross-check the power adapter and the Smart Access Gateway (SAG) device. Connect the current power adapter to a functioning SAG device, or connect a functioning power adapter to the current SAG device.
   - If power failures occur after you connect the current power adapter to a functioning SAG device, repair the current power adapter.
   - If power failures occur after you connect a functioning power adapter to the current SAG device, submit a ticket to repair the current SAG device.

5.Handle power failures

Symptoms

The SYS and PWR indicators of the Smart Access Gateway (SAG) device are off.

Possible causes

- The power switch of the SAG device is not turned on.
- The power cable is not firmly connected.
- The power supply is faulty.
- The power adapter is faulty.

Procedure

1. Check whether the power switch is on.
2. Check whether the power cable is firmly connected.
3. Check whether the power supply is faulty.

   Connect the current power adapter to a functioning power supply. If the SAG device is powered on, the current power supply is faulty.
4. Check whether the power adapter is faulty.

   Connect a functioning power adapter to the current power supply. If the SAG device is powered on, the current power adapter is faulty.
5. If power failures continue to occur after you complete the preceding four steps, the SAG device is faulty. Submit a ticket to repair the SAG device.

6.Handle connectivity failures

6.1. Handle SAG device disconnections

This topic explains why a Smart Access Gateway (SAG) device is disconnected from Alibaba Cloud and provides solutions.

Symptoms

Log on to the SAG console, the status of an SAG device is **Disconnected**.

Possible causes

- The SAG device is faulty.
- The SAG device fails to connect to Alibaba Cloud.

Procedure

1. Ping other public websites through the current Internet service provider (ISP) network to check whether the ISP network is functioning.
   - If the ISP network is abnormal, contact the ISP.
   - If the ISP network is working as expected, go to step 2.
2. Check whether the SAG device is powered on.
   - Check whether the PWR indicator is green.
   - Check whether the green light of the connected port is on.
   - If the SAG device cannot be powered on, see Handle power failures.
   - If the SAG device is powered on, go to step 3.
3. Log on to the switch console to view the connectivity between the SAG device and switch.
   - If static routing is configured in the SAG device and the switch, ping the IP address of each port of the SAG device through the switch. If you cannot ping the IP address of a port, see Handle connection failures between an SAG device and a switch to solve port interconnection issues.
   - If the SAG device is not connected to a switch, check whether the second and third indicators on the right of the SAG device are yellow or continuously blinking.
     - If the second indicator is yellow or continuously blinking, the SAG device is faulty. Submit a ticket.
     - If the third indicator is yellow or continuously blinking, the VPN tunnel between the SAG device and Alibaba Cloud is unavailable. Submit a ticket.

     For more information about indicators, see Indicators.
4. The software of the SAG device may be faulty. Restart the SAG device or submit a ticket.

6.2. Handle failures of pinging an ECS instance through SAG-1000

This topic explains why you cannot ping an Elastic Compute Service (ECS) instance through an SAG-1000 device and provides solutions.

Symptoms

A local terminal cannot connect to Alibaba Cloud. For example, you fail to ping from an SAG device an ECS instance that is associated with the same CEN instance as the SAG device.

Possible causes

- The connection between the local terminal and the SAG-1000 device is faulty.
- The VPN tunnel between the SAG-1000 device and Alibaba Cloud is faulty.
- The target ECS instance is faulty.
- The Internet service provider (ISP) network is faulty.

Procedure

1. Log on to the Smart Access Gateway (SAG) console.
2. Click the ID of the target SAG instance, check whether the status is **Ready**.
   - If the status is Disconnected, see Handle SAG device disconnections.
   - If the status is Ready, go to step 3.
3. Log on to the switch console to check the connectivity between the SAG-1000 device and the switch.
   - If static routing is configured in the SAG-1000 device and the switch, ping the IP address of each port of the SAG-1000 device through the switch. If you cannot ping the IP address of a port, see Handle connection failures between an SAG device and a switch to solve port interconnection issues.
   - If you use the SAG device without a switch, check whether the second and third indicators on the right of the SAG-1000 device are yellow or continuously blinking.
     - If the second indicator is yellow or continuously blinking, the SAG device is faulty. Submit a ticket.
     - If the third indicator is yellow or continuously blinking, the VPN tunnel between the SAG device and Alibaba Cloud is unavailable. Submit a ticket.
     - If both the second and third indicators are green, go to step 4.

     For more information about indicators, see Indicators.
4. Check the status of the current ECS instance. Ping the ECS instances deployed in other Virtual Private Cloud (VPC) networks or configure Elastic IP addresses for the target ECS instances in the Alibaba Cloud console.
   - If you can ping other ECS instances, the current ECS instance is faulty. Handle the faults of the current ECS instance.
   - If you cannot ping other ECS instances, go to step 5.
5. Ping other public websites through the current Internet service provider (ISP) network. If you cannot ping other public websites, check whether the ISP network is functioning.

6.3. Handle failures of pinging Alibaba Cloud resources through SAG-100WM

This topic explains why you cannot `ping` Alibaba Cloud resources through an SAG-100WM device and provides solutions.

Symptoms

A local terminal cannot connect to Alibaba Cloud, for example, you cannot `ping` Elastic Compute Service (ECS) instances deployed in Cloud Enterprise Network (CEN), or other local terminals deployed in Cloud Connect Network (CCN).

Possible causes

- The connection between the local terminal and the SAG-100WM device is faulty.
- The VPN tunnel between the SAG-100WM device and Alibaba Cloud is faulty.
- The target ECS instance is faulty.
- The Internet service provider (ISP) network is faulty.

Procedure

1. Log on to the Smart Access Gateway (SAG) console.
2. Click the ID of the target SAG instance, check whether the status is **Ready**.
   - If the status is Disconnected, see Handle SAG device disconnections.
   - If the status is Ready, go to .
3. Check whether the CLOUD indicator of the SAG-100WM device is on.
   - If the CLOUD indicator is on, the VPN tunnel between the SAG-100WM device and Alibaba Cloud is functioning. Log on to the ECS console to check whether the rules of the security group allows access from the local terminal.
   - If the CLOUD indicator is off, the VPN tunnel between the SAG-100WM device and Alibaba Cloud is not established. Go to .
4. Check the intermediary device such as a router.
   - Configure PPPoE for the WAN port and connect the WAN port to the ISP network without a router.
   - If the CLOUD indicator is still off, go to .
5. The software of the SAG-100WM device may be faulty. Restart the SAG-100WM device or submit a ticket.

6.4. Handle connection failures to a local terminal

This topic explains why an SAG-1000 device cannot connect to a local terminal associated with the same Cloud Connect Network (CCN) instance and provides solutions.

Symptoms

An SAG-1000 device cannot connect to a local terminal deployed in the same CCN instance.

Possible causes

- The connection between the local terminal and the SAG-1000 device is faulty.
- The VPN tunnel between the SAG-1000 device and Alibaba Cloud is faulty.

- The network environment of the target local terminal is faulty.
- The Internet service provider (ISP) network is faulty.

Procedure

1. Log on to the Smart Access Gateway (SAG) console.
2. Click the ID of the target SAG instance, check whether the status is **Ready**.
   - If the status is Disconnected, see Handle SAG device disconnections.
   - If the status is Ready, go to step 3.
3. Log on to the switch console to check the connectivity between the SAG-1000 device and the switch.
   - If static routing is configured in the SAG-1000 device and the switch, `ping` the IP address of each port of the SAG-1000 device through the switch. If you cannot `ping` the IP address of a port, see Handle connection failures between an SAG device and a switch to solve port interconnection issues.
   - If you use the SAG device without a switch, check whether the second and third indicators on the right of the SAG-1000 device are yellow or continuously blinking.
     - If the second indicator is yellow or continuously blinking, the SAG-1000 device is faulty. Submit a ticket.
     - If the third indicator is yellow or continuously blinking, the VPN tunnel between the SAG-1000 device and Alibaba Cloud is unavailable. Submit a ticket.

     For more information about indicators, see Indicators.
4. Repeat the preceding steps to check the environment of the target local terminal. If the issue persists, submit a ticket.

6.5. Handle connection failures between an SAG device and a switch

This topic explains why connection failures occur between a Smart Access Gateway (SAG) device and a switch, and provides solutions.

Symptoms

- You cannot ping the ports of the SAG device through a switch.
- On the Port Alloc page of the web console, the indicators are red.
- When the Open Shortest Path First (OSPF) protocol is configured for dynamic routing, the indicators are red on the configuration page of the web console.
- On the Home page of the web console, no route type is configured for the target CIDR block.
- The cable that connects the SAG device to the switch is faulty.
- The port of the switch is disabled.
- IP address configurations of the SAG device and the switch are incorrect.

Procedure

1. Check whether the cable that connects the SAG device and the switch is faulty. Make sure that the

indicators of the ports are on.

2. Check whether the port of the switch is enabled.
3. Check whether the IP address of the switch port and the SAG device port fall into the same CIDR block.
4. If the OSPF protocol is configured, check whether the configurations of the OSPF port and the SAG device port are the same.

   The parameters include: Area ID, Hello Time, Dead Time, Authentication Type, Router ID, Area Type. Make sure that all directly connected CIDR blocks have advertised routes.

7.FAQ

7.1. What should I do if my workloads are interrupted?

This topic provides solutions on how to manage workload interruption. The solutions vary depending on the device type.

- SAG-100WM: See Handle failures of pinging Alibaba Cloud resources through SAG-100WM.
- SAG-1000: See Handle failures of pinging an ECS instance through SAG-1000 and Handle connection failures to a local terminal.

7.2. What should I do if the SAG device is disconnected from Alibaba Cloud?

See Handle SAG device disconnections.

7.3. What should I do if I forget the password used to log on to the web console?

- SAG-100WM: After you power on the device, press the reset button on the device to delete the current password. Then, log on to the web console to set a new password.
- SAG-1000: After you power on the device, press and hold the reset button with a pointed object for 1 second to delete the current password. Then, log on to the web console to set a new password.

7.4. What is the default Wi-Fi password?

The default Wi-Fi password of a SAG-100WM device is the serial number.