

Alibaba Cloud Smart Access Gateway

Best Practices

Issue: 20190814

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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK.
<code>Courier font</code>	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is a optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>switch {stand slave}</code>

Contents

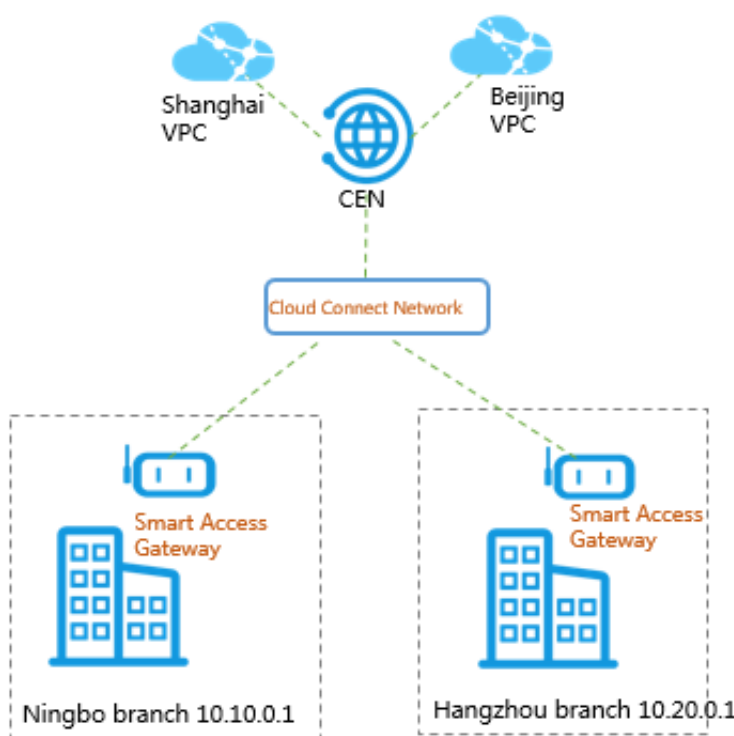
Legal disclaimer.....	I
Generic conventions.....	I
1 SAG-100WM inline mode configuration tutorial.....	1
2 SAG-1000 stand-alone one-arm static-routing configuration tutorial.....	7
2.1 Configuration overview.....	7
2.2 Step 1: Purchase a Smart Access Gateway device.....	9
2.3 Step 2: Configure the Smart Access Gateway device and its peer switches...	10
2.4 Step 3: Console configuration.....	14
3 SAG-1000 dual-device one-arm dynamic-routing hot-backup configuration tutorial.....	17
3.1 Configuration overview.....	17
3.2 Step 1: Purchase a Smart Access Gateway device.....	20
3.3 Step 2: Configure the SAG device (device 1) and its peer switches.....	21
3.4 Step 3: Configure the SAG device (device 2) and its peer switches.....	29
3.5 Step 4: Console configuration.....	37
4 Configure Smart Access Gateway as the backup of a physical connection.....	41
4.1 Configuration overview.....	41
4.2 Step 1: Purchase a Smart Access Gateway device.....	43
4.3 Step 2: Configure the SAG device and Layer-3 switches.....	44
4.4 Step 3: Console configuration.....	51
5 Tutorial for configuring local branches or headquarters with multiple CIDR blocks.....	54
5.1 Configuration overview.....	54
5.2 Step 1: Purchase a Smart Access Gateway device.....	56
5.3 Step 2: Configure the SAG device and the peer switches.....	56
5.4 Step 3: Console configuration.....	59
6 Cross-region access to VPC.....	61

1 SAG-100WM inline mode configuration tutorial

This tutorial uses a Ningbo branch and a Hangzhou branch as an example to describe how to use a Smart Access Gateway (SAG) device to connect two local branches to VPCs located in Shanghai and Beijing. The clients of the local branches as a result can directly access the VPCs through the SAG device.

Scenarios

In this tutorial, a company wants to connect local branches in Hangzhou and Ningbo to VPCs hosted in Shanghai and Beijing. Given that the branches and VPCs are all in the same SAG area, you only need to attach the Cloud Connect Network (CCN) instance associated with the SAG instances to the Cloud Enterprise Network (CEN) instance.



To connect the local branches to the VPCs, you need to complete the following tasks:

1. Purchase an SAG device.
2. Connect the SAG device.
3. Activate the SAG device.
4. Configure the network connection.

5. Configure the security group.

6. Perform an access test.

Prerequisites

- A CEN instance is created.
- A VPC is created in Shanghai and another VPC is created in Beijing. In addition, the VPCs are added to the same CEN instance. If you have not completed this step, complete the following instructions:

1. Log on to the [Smart Access Gateway console](#).
2. Choose Quick Links > VPC.
3. Select the China (Beijing) region and click the ID of the target VPC.
4. On the VPC Details page, click Attach to CEN, and then select the target CEN instance.
5. Repeat the preceding steps to add the VPC in Shanghai to the same CEN instance.

The screenshot shows the 'CEN' (Cloud Enterprise Network) instance details page. At the top, there's a notification bar. Below it, the 'Basic Settings' section shows the instance ID, name, description, and status (Ready). The 'Overlapping Routing Function' is set to 'Disable'. The 'Networks' tab is selected, showing a table of attached VPCs. Two VPCs are listed: one in China (Hangzhou) and one in US (Silicon Valley), both with a status of 'Attached'.

Instance ID/Name	Region	Network Type	Account ID	attach time	Status	Actions
vpc-d...	China (Hangzhou)	VPC	12...	10/16/2018, 16:46:00	Attached	Detach
vpc-d...	US (Silicon Valley)	VPC	1...	10/16/2018, 16:47:00	Attached	Detach

- A CCN instance is created. For more information, see [Create a CCN instance](#).

Step 1: Buy an SAG device

After you buy an SAG device on the console, Alibaba Cloud delivers the device to you and creates an SAG instance for you to manage.

To buy an SAG device, follow these steps:

1. Log on to the [Smart Access Gateway console](#).
2. Click Create SmartAG.

3. Configure the SAG device and click Buy Now.

For more information, see [Buy a Smart Access Gateway](#).



Note:

In this tutorial, the SAG-100WM specification and the Stand-alone usage method are selected.

4. Confirm the order information, and then click Buy Now.

5. On the displayed Address dialog box, enter the shipping address of the gateway device and click Order Now.

You can check whether the order is successfully placed on the SAG page. The system will deliver the device within 48 hours after the order is placed. If you do not receive the device within 48 hours, you can open a ticket to check the delivery status.

Create SmartAG

Instance ID

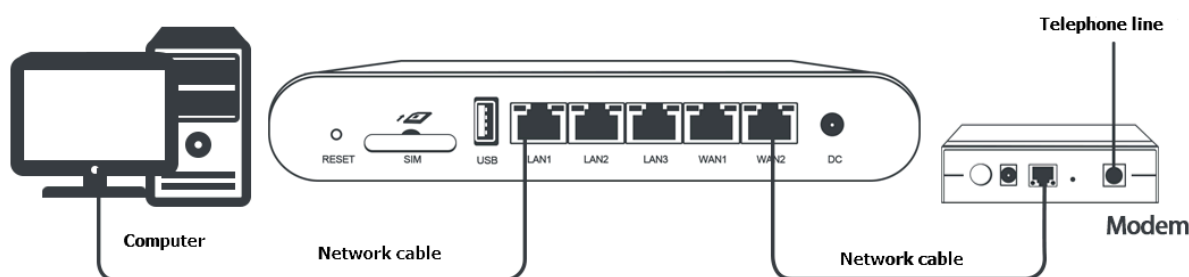
Enter

Instance ID/Name	CCN Instance ID/Name	Peak Bandwidth	Status	Private CIDR Block	Expires At	Actions
sag-ke3k-connectN		1Mbps Change Specification	Ordered			Configure Network Notify Delivery Renew ...

Step 2: Connect the SAG device

After receiving an SAG device, follow [SAG-100WM user manual](#) to check that all accessories are included, and then power on the device. After you start the SAG device, connect the WAN port to the network cable and connect the LAN ports to local clients.

In this tutorial, the clients in the Hangzhou and Ningbo branches can be directly connected to Alibaba Cloud through the SAG devices, so you can use the default gateway configuration. If you need to configure the WAN port and LAN ports, see [Configuration guide](#).



Step 3: Activate the SAG device

After receiving an SAG device, you must activate it.

To activate the SAG device, follow these steps:

1. Log on to the [Smart Access Gateway console](#).
2. On the SmartAG page, find the target gateway instance.
3. Click Activate in the Actions column.

Step 4: Configure the network connection

After activating the SAG device, you need to attach it to a CCN instance and then attach the CCN instance to a CEN instance, so that local branches can be connected to Alibaba Cloud.

Complete these steps to configure the network:

1. Log on to the [Smart Access Gateway console](#).
2. On the Smart Access Gateway page, find the target SAG instance.
3. Click Configure Network in the Actions column.
4. On the Configure Network page, follow these steps:
 - a. **Private CIDR Block:** Configure the private CIDR blocks used by the local clients to access Alibaba Cloud. Make sure all private CIDR blocks do not conflict with one another.

In this tutorial, enter 172.16.0.0/12. In this tutorial, each local branch uses the default gateway configuration, so the IP address used by the local client to access Alibaba Cloud is allocated from the 10.10.0.0/12 CIDR block.



Note:

Configuring a 32-bit mask is not supported.

- b. **CCN Instance ID/Name:** Add the SAG instance to the CCN instance. Then, SAG devices in the CCN instance can communicate with one another.

In this tutorial, the default CCN is used. For more information.

5. **Bind CEN Instance:** Select the CEN instance to attach. After the CCN instance is attached to the CEN instance, SAG devices in the CCN instance can communicate with networks (VPCs and VBRs) attached to the CEN instance.

In this tutorial, the CEN instance associated with the Shanghai VPC and Beijing VPC is selected.

6. Click OK.
7. Repeat the preceding steps to configure the network for the SAG instance of the other branch.

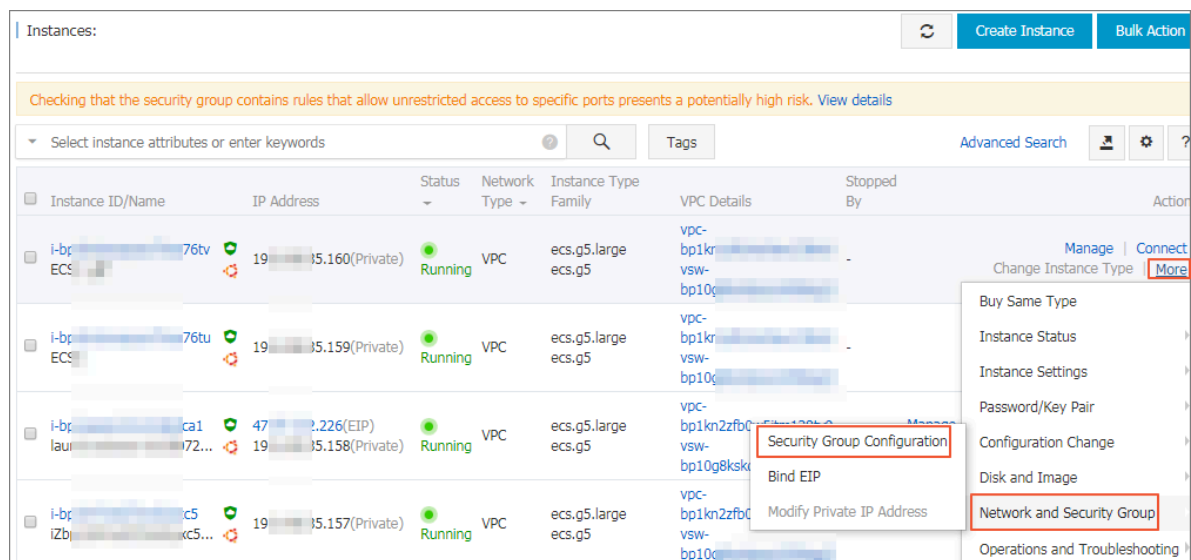
Make sure the two SAG instances are attached to the same CCN instance and the same CEN instance.

Step 5: Configure a security group

Configure a security group to allow the branches to access VPC.

To configure the security groups, complete these steps:

1. Log on to the [ECS Console](#).
2. In the left-side navigation pane, click Instances.
3. Find the target ECS instance in the target VPC, and then choose More > Network and Security Group > Configure Security Group.



4. Click Add Rules and click Add Security Group Rule.
5. Configure a security group rule that allows access from local branches.

The following figure shows the security group configurations in this tutorial. You need to set the authorization object as the private CIDR block of the local branch.

Step 6: Test the access

After completing the preceding configurations, you can use local clients to access cloud resources deployed in the connected VPCs to check if the configurations take effect.

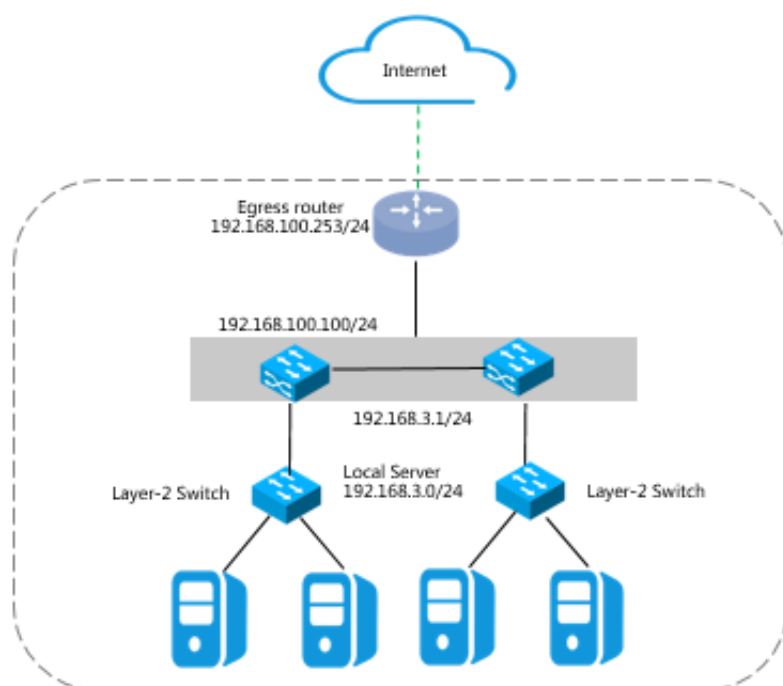
2 SAG-1000 stand-alone one-arm static-routing configuration tutorial

2.1 Configuration overview

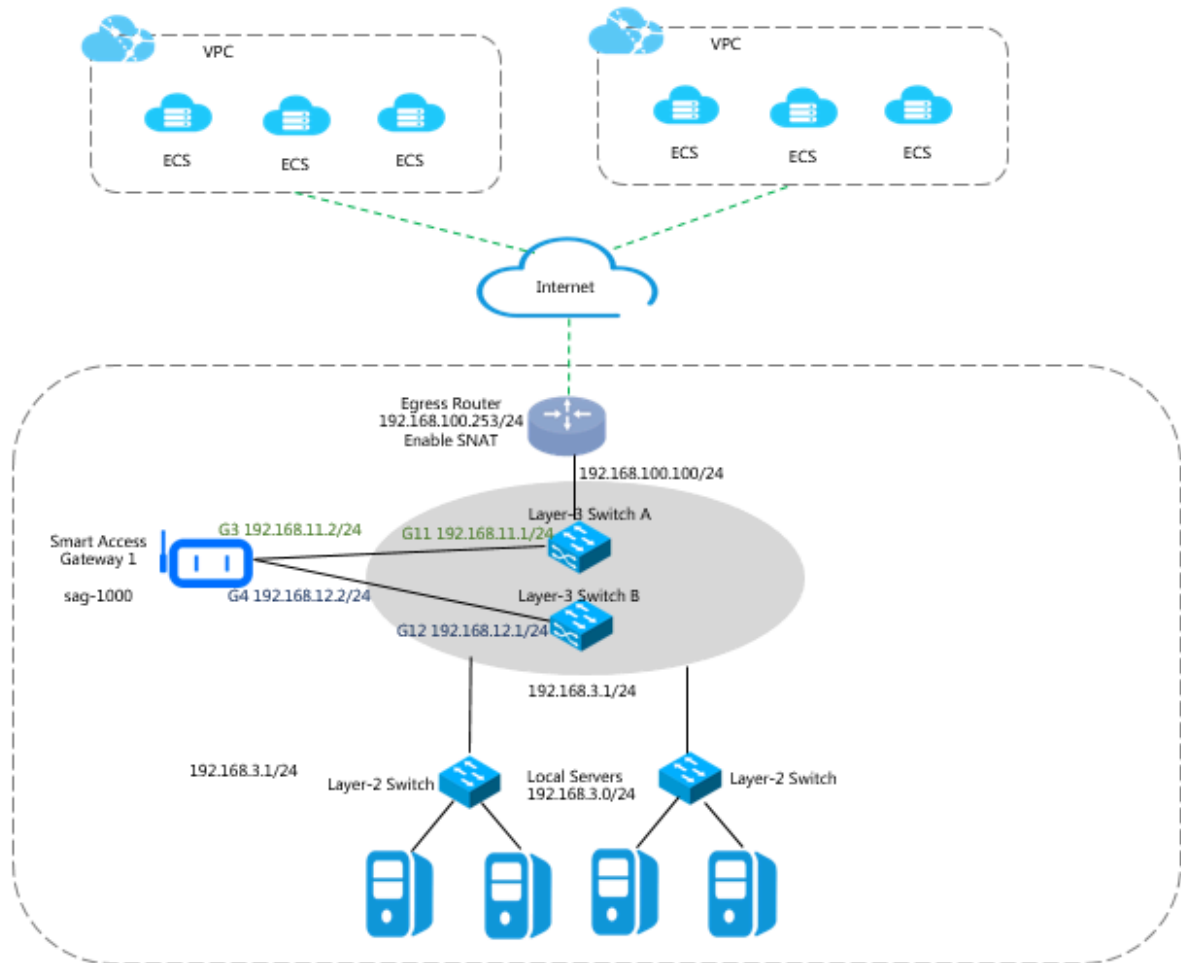
This tutorial guides you to connect your headquarters or branches to Alibaba Cloud through SAG-1000 Smart Access Gateway (SAG).

Scenarios

This tutorial takes the network architecture in the following figure as an example. Two Layer-3 switches form a switch stack and are connected to two Layer-2 switches. Local clients access the Internet through Layer-2 switches.



As shown in the following figure, one SAG-1000 Smart Access Gateway is connected to Layer-3 switches through one-arm mode to connect local servers to Alibaba Cloud.



Network planning

Before you begin, you must plan the following network configurations and ensure that the CIDR blocks do not conflict with one another:

- The CIDR blocks of the VPCs to connect. In this tutorial, the CIDR blocks of the two VPCs are 192.168.0.0/24 and 10.0.0.0/24.
- IP addresses of local servers/clients

Plan the IP addresses of the local servers/clients according to your needs. In this tutorial, the IP address 192.168.3.0/24 is used.

- IP addresses used by the device to communicate with the Layer-3 switches

Plan the IP addresses of the ports used by the SAG device to communicate with the Layer-3 switches. We recommend that you set the mask to /30. In this tutorial, the port IP addresses used by the device are 192.168.11.2/24 and 192.168.12.2/24.

- Service IP address

Plan the service IP address of the SAG device. In this tutorial, the service port IP address 192.168.101.1 is used.

- Management port IP address

Plan the management port IP address of the SAG device. You can use an independent management port IP address or use the service port IP address as the management port IP address. In this tutorial, 192.168.0.1/24 is used as the management port IP address. In this tutorial, 192.168.0.1/24 is used as the management port IP address.

Table 2-1: Example values in this tutorial

Configuration	Example value
CIDR blocks of the VPCs	VPC1: 192.168.0.0/24 VPC2: 10.0.0.0/24
The CIDR block of the egress router	192.168.100.253/24
The CIDR block used by the Layer-3 switches to communicate with Alibaba Cloud	192.168.100.100/24
The CIDR block used by the Layer-3 switches to communicate with the SAG device	192.168.3.1/24
IP addresses of the ports of the SAG device	G3 192.168.11.2/24 G4 192.168.12.2/24
IP addresses of the ports on the peer switches of the SAG device	G11 192.168.11.1/24 G12 192.168.12.1/24
The CIDR block of local servers	192.168.3.0/24

2.2 Step 1: Purchase a Smart Access Gateway device

After you buy a Smart Access Gateway (SAG) device in the console, Alibaba Cloud delivers the device to you and creates an SAG instance for you to manage.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. On the SAG page, click Create SmartAG.
3. Configure the SAG device and click Buy Now.

For more information, see [Buy a Smart Access Gateway](#).



Note:

In this tutorial, the SAG-1000 specification and the Standby usage method are selected.

4. Confirm the order information, and then click Pay.
5. On the Address dialog box, enter the shipping address of the gateway device and click Order Now.

You can check whether the order is successfully placed on the status page of the Smart Access Gateway instance. The system will deliver the device within two days after the order is placed. If you do not receive the device within two days, you can open a ticket to check the delivery status.

Smart Access Gateway Hardware

Usage CapacityDocumentationProduct Updates

Create SmartAG

Instance ID

Enter

Instance ID/Name	CCN Instance ID/Name	Peak Bandwidth	Status	Private CIDR Block	Expires At	Actions
		5Mbps Change Specification	Offline		Dec 22, 2019, 18:07:30	Configure NetworkView HelpRenew
		1Mbps Change Specification	Ordered			Configure NetworkNotify DeliveryRenew

2.3 Step 2: Configure the Smart Access Gateway device and its peer switches

This tutorial shows you how to configure the Smart Access Gateway(SAG) device and its peer switches.

Configure the SAG device

To configure the SAG device, follow these steps:

1. After receiving the SAG device, follow [SAG-1000 user manual](#) to check if all accessories are provided and then power on the SAG device.
2. Connect port G3 of the Smart Access Gateway to port G11 of switch A, and connect port G4 of the Smart Access Gateway to port G12 of switch B.
3. Connect the network card of the PC to port 2 of the SAG device, and set the IP address of the network card to 192.168.0.100/24.

4. Enter the web configuration address of the SAG device in the browser.

The default address is `https://192.168.0.1`. For more information, see [Log on to the web configuration page](#).

5. Configure the service IP address and the management port.

In this tutorial, enter 192.168.101.1 as the service IP address, enter 192.168.20.1/24 as the management IP address, and enter 192.168.20.4 as the next hop.



Notice:

The specified service IP address must be able to access the Internet. For one-arm mode, if the service IP address is a private CIDR block, you must enable NAT mapping at the Internet egress or firewall.

Service IP

* Configure Service IP :

* Management Interface : Port 2

* Isolate or not :


☒ Yes ☐ NO

* Management port IP :

* Next Hop :

OK

Cancel

Configuration	Description
Configure Service IP:	<p>The service IP address is used to establish the VPN tunnel.</p> <div> Notice: Make sure that the specified service IP address can access the Internet.</div>
Management Interface:	<p>The management port is used for local clients to access the Web console. By default, port 2 is the management port.</p>

Configuration	Description
Isolate or not:	<p>Select whether to isolate the service port from the management port:</p> <ul style="list-style-type: none"> · Yes: This port can only be used as a local Web management port and cannot be used as a service port. <p>In the isolation mode, the service traffic and the management traffic do not communicate with each other, achieving a high level of security.</p> <ul style="list-style-type: none"> · No: This port is used as both the local Web management port and the service port.
Management port IP:	The management IP address is used for Web access of the local client.
Next Hop:	If you choose to isolate the service port from the management port, specify the next hop of the management port.

6. Configure the ports used to communicate with the switches:

- **Connection Mode:** Select to use static routes.
- **Port:** Click the Edit option in the Configuration Information area.

The specified ports are 192.168.11.2/24 and 192.168.12.2/24.

Configure the peer switches

Add route configurations for the peer switches of the device according to the following configurations. Here a Ruijie switch is taken as an example. For devices of other manufacturers, see the device manuals for specific configurations.

Route configurations of the peer switches.

```

interface GigabitEth ernet 0 / 11
no switchport
ip address 192 . 168 . 11 . 1 255 . 255 . 255 . 0 The IP
address of the port on the peer switch of the SAG
device

interface GigabitEth ernet 0 / 12
no switchport
ip address 192 . 168 . 12 . 1 255 . 255 . 255 . 0 The IP
address of the port on the peer switch of the
SAG device

ip route 192 . 168 . 101 . 2 255 . 255 . 255 . 255 192 . 168
. 11 . 2 The route from the switch to the service
IP address
ip route 192 . 168 . 101 . 1 255 . 255 . 255 . 255 192 . 168
. 12 . 2

```

```

ip route 192 . 168 . 0 . 0 255 . 255 . 255 . 0 192 . 168 . 11
. 2 The route from the switch to VPC1
ip route 192 . 168 . 0 . 0 255 . 255 . 255 . 0 192 . 168 . 12
. 2

ip route 10 . 0 . 0 . 0 255 . 255 . 255 . 0 192 . 168 . 11 .
2 The route from the switch to VPC2
ip route 10 . 0 . 0 . 0 255 . 255 . 255 . 0 192 . 168 . 12 .
2

```

2.4 Step 3: Console configuration

After you configure the Smart Access Gateway (SAG) device, you must activate it in the Smart Access Gateway console and complete the network configuration.

Step 1: Configure the network configuration

After activating the SAG device, you must attach the SAG instance to the CCN instance and attach the CCN instance to the CEN instance to which the target VPCs belong.

To configure the network, follow these steps:

1. Log on to the [Smart Access Gateway console](#).
2. On the SAG page, find the target gateway instance.
3. Click Configure Network in the Actions column.
4. On the Configure Network page, set the following configurations:
 - a. **Private CIDR Block:** Configure the private CIDR blocks used by the local clients to access Alibaba Cloud. Make sure all private CIDR blocks do not conflict with one another.

In this tutorial, enter 192.168.3.0/24. Configuring a CIDR block with a 32-bit mask is not supported.

- b. **CCN Instance ID/Name:** Add the gateway instance to the CCN instance. Then gateway devices in the CCN instance can communicate with one another.

In this tutorial, the default CCN is used. For more information, see [Cloud Connect Network](#).

5. **Bind CEN Instance:** Select the CEN instance to attach. After the CCN instance is attached to the CEN instance, gateway devices in the CCN instance can communicate with networks (VPCs and VBRs) attached to the CEN instance.
 6. Click OK.

Step 2: Activate the SAG device

After configuring the network connection, you must activate the SAG device:

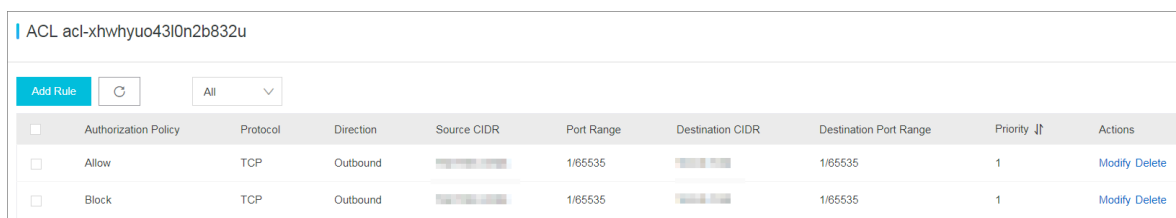
To activate the SAG device, follow these steps:

1. Log on to the [Smart Access Gateway console](#).
2. On the SmartAG page, find the target gateway instance.
3. Click Activate in the Actions column.

Step 3: Configure an ACL

To configure an access control list (ACL), follow these steps:

1. Log on to the [Smart Access Gateway console](#).
2. Click ACL and configure an ACL rule for the SAG device. For more information, see [Configure an access control list](#).



<input type="checkbox"/>	Authorization Policy	Protocol	Direction	Source CIDR	Port Range	Destination CIDR	Destination Port Range	Priority	Actions
<input type="checkbox"/>	Allow	TCP	Outbound		1/65535		1/65535	1	Modify Delete
<input type="checkbox"/>	Block	TCP	Outbound		1/65535		1/65535	1	Modify Delete

Step 4: Configure a security group

Configure a security group to allow local branches to access the VPCs.

To configure the security group, follow these steps:

1. Log on to the [ECS Console](#).
2. In the left-side navigation pane, click Instances.
3. Find the target ECS instance in the target VPC, and then choose More > Network and Security Group > Configure Security Group.
4. Click Add Rules and click Add Security Group Rule.

5. Configure a security group rule that allows access from local branches.

The following figure shows the security group configurations in this tutorial. You must enter the private CIDR blocks of the local branches as the authorization objects.

Add Security Group Rule

NIC: Intranet

Rule Direction: Ingress

Action: Allow

Protocol Type: Customized TCP

* Port Range: 1/65535

Priority: 1

Authorization Type: CIDR

* Authorization Objects: 172.16.0.0/12

Description:

It can be 2 to 256 characters in length and cannot start with http:// or https://.

OK Cancel

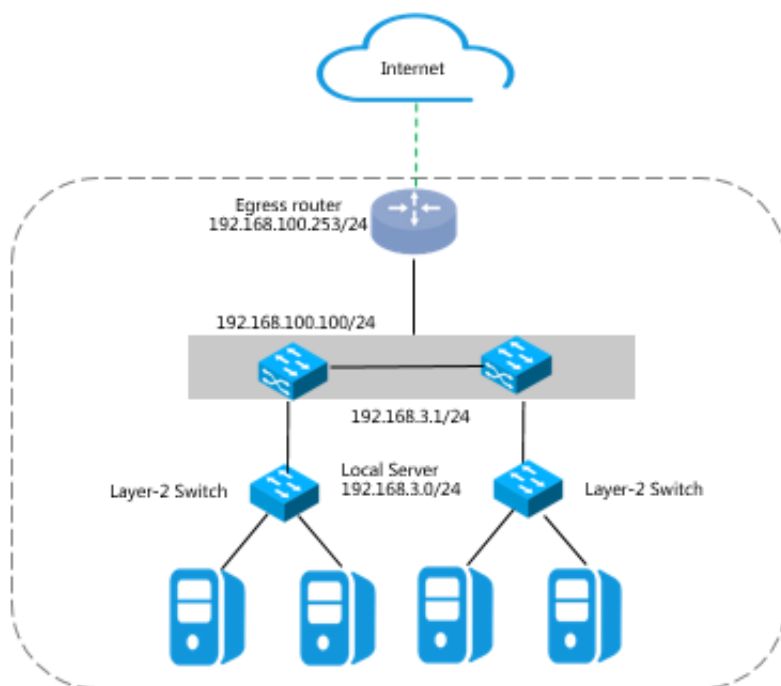
3 SAG-1000 dual-device one-arm dynamic-routing hot-backup configuration tutorial

3.1 Configuration overview

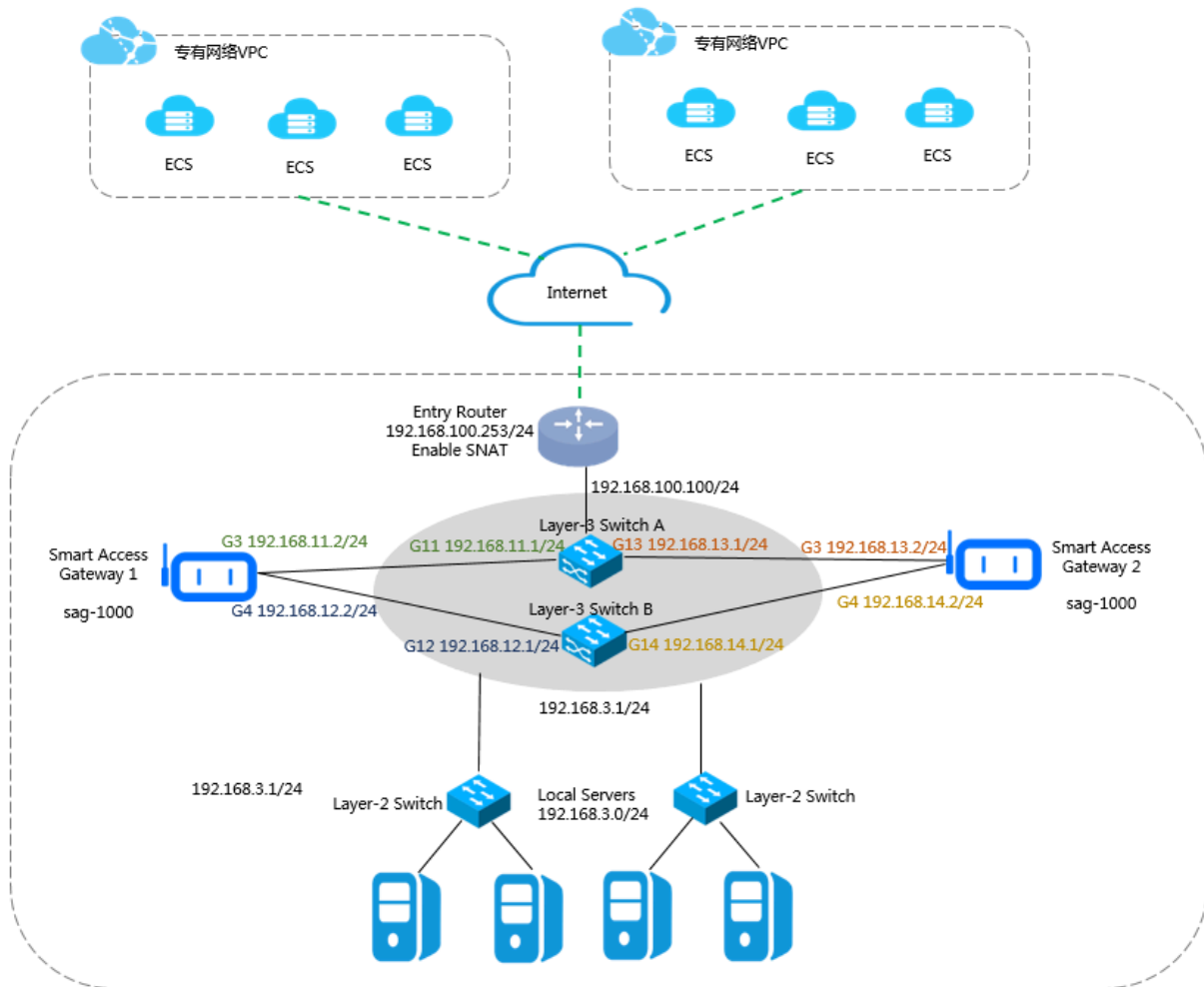
This tutorial guides you to connect your headquarters or branches to Alibaba Cloud through the SAG-1000 Smart Access Gateway.

Scenarios

This tutorial takes the network architecture in the following figure as an example. Two Layer-3 switches form a switch stack and are connected to two Layer-2 switches. Local clients access the Internet through Layer-2 switches.



As shown in the following figure, two SAG-1000 Smart Access Gateways access Layer-3 switches through one-arm mode to connect local servers to Alibaba Cloud.



Network planning

Before you begin, you must plan the following network configurations and ensure that the CIDR blocks do not conflict with one another:

- The CIDR blocks of the VPCs to connect. In this tutorial, the CIDR blocks of the two VPCs are 192.168.0.0/24 and 10.0.0.0/24.
- IP addresses of local servers/clients

Plan the IP addresses of the local servers/clients according to your needs. In this tutorial, the IP address 192.168.3.0/24 is used.

- IP addresses used by the devices to communicate with the Layer-3 switches

Plan the IP addresses of the ports used by the Smart Access Gateway devices to connect the Layer-3 switches. We recommend that you set the mask to /30. In this tutorial, the IP addresses of the ports used by device 1 are 192.168.11.2/24 and 192.168.12.2/24, and those of the ports used by device 2 are 192.168.13.2/24 and 192.168.14.2/24.

- Service IP addresses

Plan the service IP addresses of the Smart Access Gateway devices. In this tutorial, the service port IP addresses used by the devices are 192.168.101.1 and 192.168.101.2.

- Management port IP addresses

Plan the management port IP addresses of the Smart Access Gateway devices. You can use an independent management port IP address or use the service IP address as the in-band management port IP address. In this tutorial, the management port IP address used by device 1 is 192.168.20.1/24, and the one used by device 2 is 192.168.20.2/24.

Table 3-1: Example values in this tutorial

Configuration	Example value
CIDR blocks of the VPCs	VPC1: 192.168.0.0/24 VPC2: 10.0.0.0/24
The CIDR block of the egress router	192.168.100.253/24
The CIDR block used by the Layer-3 switches to communicate with Alibaba Cloud	192.168.100.100/24
The CIDR block used by the Layer-3 switches to communicate with the Smart Access Gateway devices	192.168.3.1/24
IP addresses of the ports used by Smart Access Gateway device 1	G3 192.168.11.2/24 G4 192.168.12.2/24
IP addresses of the ports used by Smart Access Gateway device 2	G3 192.168.13.2/24 G4 192.168.14.2/24
IP addresses of the ports used by the peer switches of the Smart Access Gateway devices	G11 192.168.11.1/24 G12 192.168.12.1/24 G13 192.168.13.1/24 G14 192.168.14.1/24

Configuration	Example value
The CIDR block of local servers	192.168.3.0/24

3.2 Step 1: Purchase a Smart Access Gateway device

After you buy a Smart Access Gateway device in the console, Alibaba Cloud delivers the device to you and creates a Smart Access Gateway instance for you to manage.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. On the SAG page, click Create SmartAG.
3. Configure the Smart Access Gateway device and click Buy Now.

For more information, see [Buy a Smart Access Gateway](#).



Note:

In this tutorial, the SAG-1000 specification and the Standby usage method are selected.

4. Confirm the order information, and then click Pay.
5. On the Address dialog box, enter the shipping address of the gateway device and click Order Now.

You can check whether the order is successfully placed on the status page of the Smart Access Gateway instance. The system will deliver the device within two days after the order is placed. If you do not receive the device within two days, you can open a ticket to check the delivery status.

Smart Access Gateway Hardware

[Usage Capacity](#)
[Documentation](#)
[Product Updates](#)

Create SmartAG

Instance ID

Enter

Instance ID/Name	CCN Instance ID/Name	Peak Bandwidth	Status	Private CIDR Block	Expires At	Actions
...	...	5Mbps Change Specification	Offline		Dec 22, 2019, 18:07:30	Configure Network View Help Renew
...	...	1Mbps Change Specification	Ordered			Configure Network Notify Delivery Renew

3.3 Step 2: Configure the SAG device (device 1) and its peer switches

This tutorial describes how to configure the routes of Smart Access Gateway (SAG) device (known as device 1 in this topic) and its peer switches.

Configure the SAG device

To configure device 1, follow these steps:

1. After receiving device 1, follow the instructions in the [SAG-1000 user manual](#) to check that all accessories are provided, and then power on the SAG device.
2. Connect Port G3 of device 1 to Port G11 of switch A, and connect Port G4 of device 1 to Port G12 of switch B.
3. Connect the network card of the PC to port 2 of device 1 and set the IP address of the network card to 192.168.0.100/24.
4. Enter the web configuration address of device 1 in your browser.

The default address is `https://192.168.0.1`. For more information, see [Log on to the web configuration page](#).

5. Configure the service IP address and the management port.

In this tutorial, enter 192.168.101.1 as the service IP address, enter 192.168.20.1/24 as the management IP address, and enter 192.168.20.4 as the next hop.

Service IP

* Configure Service IP :

192.168.101.1

* Management Interface : Port 2

* Isolate or not :

☒ Yes ☐ NO

* Management port IP :

192.168.20.1/24

* Next Hop :

192.168.20.4

OK

Cancel

Configuration	Description
Configure Service IP:	The service IP address is used to establish the VPN tunnel.
Management Interface:	The management port is used for local web access. Port 2 is the management port by default.
Management port IP:	The management IP address is used for the local client to access the Web console.

Configuration	Description
Isolate or not:	<p>Select whether to isolate the service port from the management port:</p> <ul style="list-style-type: none">· Yes: This port can only be used as a local web management port and cannot be used as a service port. <p>In the isolation mode, the service traffic and the management traffic do not communicate with each other, thus achieving a higher level of security.</p> <ul style="list-style-type: none">· No: This port is used as both the local web management port and the service port.
Next Hop	If you choose to isolate the service port from the management port, specify the next hop of the management port.

6. Configure the ports used to communicate with the switches:

- **Connection Type:** Select static or dynamic routing. In this tutorial, select **Dynamic Route**.
- **Port:** Click the **Edit** option in the **Configurations** area, enter the IP addresses of the ports used for communication and select whether to enable **Open Shortest Path First (OSPF)**.

In this tutorial, OSPF is enabled, and the IP addresses of the ports used for communicating with the switches are 192.168.11.2/24 and 192.168.12.2/24.

Port Management

Connection Type

☐ Static Route ☒ Dynamic Route

☒ OSPF ☐ BGP

Configurations [Edit](#)

Port	Whether to enable OSPF	IP address
• Port0	NO	-
• Port1	NO	-
• Port2 (Used for management port)	NO	-
• Port3	NO	-
• Port4	NO	-

7. Configure OSPF.

In this tutorial, MD5 authentication is selected. Enter the service IP 192.168.101.1 as the RouterId.

OSPF global configuration :

* Area ID :

1

* Hello_time :

3

* Dead_time :

10

* Authentication

☐ Not

☐ Plain Text

☒ MD5

Method :

certified

Authentication

certification

* MD5 key ID :

7

* MD5 key :


1234

* Routerid :

192.168.101.1

* Area Type :

nssa

Configuration	Description
Connection method	<div>Choose to access the switch using static or dynamic routing.</div> <div> Notice: When dual-device one-arm mode is used, only dynamic routing is supported.</div>

Configuration	Description
Port	Click the Edit option in the Configuration Information area, enter the IP address of the port used for communication and select whether to enable OSPF. Port 2 is the default management port.
OSPF routing configuration	
Area ID	The ID of the area. Make sure that area IDs of SAG device 1 and SAG device 2 are different and the area ID of each SAG device is the same as that of the corresponding peer switch.
Hello_time	The interval at which hello packets are sent, in seconds. Default value: 3 seconds.
Dead_time	The dead interval of OSPF neighbor, in seconds. The neighbor relation stops if no hello packet is received during the dead time. Default value: 10 seconds.
Authentication method	Select an authentication method. <ul style="list-style-type: none">· Do not authenticate: Do not perform authentication.· Clear Text Authentication: Enter a clear text password.· MD5 Authentication: Use the MD5 method to perform authentication. Enter the MD5 key ID and the MD5 key.
Routerid	The ID of the OSPF router. We recommend that you directly use the service IP address.
Area Type	The area type is nssa by default.

Configure the peer switches (Ruijie)

Add route configurations for the peer switches of device 1 according to the following configurations. For switches of other manufacturers, see the device manuals.

- Route configurations of the peer switches.



Note:

You must configure the network type of the interfaces using the OSPF protocol on the same Smart Access Gateway device to P2P, otherwise the routes cannot be correctly calculated.

```

interface GigabitEthernet 0 / 11
no switchport
ip ospf network point-to-point The network
type must be p2p
ip ospf authentication message-digest
ip ospf message-digest-key 7 md5 1234
ip ospf hello-interval 3
ip ospf dead-interval 10
ip address 192.168.11.1 255.255.255.0 The IP
address of the port on the peer switch of the
SAG device

interface GigabitEthernet 0 / 12
no switchport
ip ospf network point-to-point The network
type must be p2p
ip ospf authentication message-digest
ip ospf message-digest-key 7 md5 1234
ip ospf hello-interval 3
ip ospf dead-interval 10
ip address 192.168.12.1 255.255.255.0 The
IP address of the port on the peer switch of
the SAG device

```

- Configure the loopback address of the switch.



Note:

You must configure OSPF to be in the NSSA area and to automatically generate default routes and advertise them to Smart Access Gateway.

```

interface Loopback 0
ip address 192.168.101.3 255.255.255.255
The loopback address of the switch

router ospf 1
router-id 192.168.101.3
The router ID of the switch

area 0
area 1
area 2
area 1 nssa translator always default-information-
originate
area 1 nssa translator always default-information-
originate
network 192.168.3.0 0.0.0.255 area 0
The CIDR block of the local PC
network 192.168.11.0 0.0.0.255 area 1
The CIDR block of the switch
network 192.168.12.0 0.0.0.255 area 1
network 192.168.13.0 0.0.0.255 area 1
network 192.168.14.0 0.0.0.255 area 1
network 192.168.100.0 0.0.0.255 area 0
The CIDR block used for communicating
with the uplink router

```

```

network 192 . 168 . 101 . 3 0 . 0 . 0 . 0 area 0
The loopback address of the switch
default - information originate always
Advertise default routes to the SAG device

```

Configure the peer switches (Cisco)

Add route configurations for the peer switches of device 1 according to the following configurations. For switches of other manufacturers, see the device manuals for specific configurations.

- Route configurations of the peer switches.



Note:

You must configure the network type of the interfaces using the OSPF protocol on the same Smart Access Gateway device to P2P, otherwise the routes cannot be correctly calculated.

```

interface GigabitEthernet 0 / 11
no switchport
ip address 192 . 168 . 11 . 1 255 . 255 . 255 . 0 The
IP address of the port on the peer switch of
the SAG device
ip ospf network point - to - point The network
type must be p2p
ip ospf authentication message - digest
ip ospf message - digest - key 7 md5 1234
ip ospf dead - interval 10
ip ospf hello - interval 3
!
interface GigabitEthernet 0 / 12
no switchport
ip address 192 . 168 . 12 . 1 255 . 255 . 255 . 0 The
IP address of the port on the peer switch of
the SAG device
ip ospf network point - to - point The network
type must be p2p
ip ospf authentication message - digest
ip ospf message - digest - key 7 md5 1234
ip ospf dead - interval 10
ip ospf hello - interval 3
!

```

- Configure the loopback address of the switch.



Note:

You must configure OSPF to be in the NSSA area and to automatically generate default routes and advertise them to the SAG device.

```

interface Loopback 0
ip address 192 . 168 . 101 . 3 255 . 255 . 255 . 255
The loopback address of the switch
!

```

```

router ospf 1
router - id 192 . 168 . 101 . 3
The router ID of the switch
area 2 nssa default - informatio n - originate no -
summary Advertise default routes to the SAG
device
network 192 . 168 . 3 . 0 0 . 0 . 0 . 255 area 0
The CIDR block of the local PC
network 192 . 168 . 11 . 0 0 . 0 . 0 . 255 area 1
The CIDR block of the switch
network 192 . 168 . 11 . 0 0 . 0 . 0 . 255 area 1
The CIDR block of the switch
network 192 . 168 . 100 . 0 0 . 0 . 0 . 255 area 0
The CIDR block used for communicat ing
with the uplink router
network 192 . 168 . 101 . 3 0 . 0 . 0 . 0 area 0
The loopback address of the switch
network 192 . 168 . 11 . 0 0 . 0 . 0 . 255 area 1
The CIDR block of the switch
network 192 . 168 . 14 . 0 0 . 0 . 0 . 255 area 1
default - informatio n originate always
!
```

3.4 Step 3: Configure the SAG device (device 2) and its peer switches

This tutorial describes how to configure the routes of Smart Access Gateway (SAG) device 2 (known as device 2 in this topic) and its peer switches.

Configure the SAG device

To configure device 2, follow these steps:

1. After receiving device 2, follow [SAG-1000 user manual](#) to check that all accessories are provided and then power on the device.
2. Connect port G3 of device 2 to port G13 of switch A, and connect port G4 of device 2 to port G14 of switch B.
3. Connect the network card of the PC to port 2 of device 2 and set the IP address of the network card to 192.168.0.100/24.
4. Enter the web configuration address of device 2 in your browser.

The default address is <https://192.168.0.1>. For more information, see [Log on to the web configuration page](#).

5. Configure the service IP address and the management port.

In this tutorial, set the service IP address to 192.168.101.2, set the management IP address to 192.168.20.2/24, and set the next hop to 192.168.20.4.

Service IP

* Configure Service IP :

192.168.101.2

* Management Interface : Port 2

* Isolate or not :

☒ Yes ☐ NO

* Management port IP :

192.168.20.2/24

* Next Hop :

192.168.20.4

OK

Cancel

Configuration	Description
Configure Service IP:	The service IP address is used to establish the VPN tunnel.
Management Interface:	The management port that the local client uses to access the Web console. Port 2 is the management port by default.

Configuration	Description
Management port IP:	The management IP address that the local client uses to access the Web console.
Isolate or not:	<p>Select whether to isolate the service port from the management port:</p> <ul style="list-style-type: none">· Yes: This port can only be used as a local Web management port and cannot be used as a service port. <p>In the isolation mode, the service traffic and the management traffic do not communicate with each other, achieving a high level of security.</p> <ul style="list-style-type: none">· No: This port is used as both the local Web management port and the service port.
Next Hop	If you choose to isolate the service port from the management port, you must specify the next hop of the management port.

6. Configure the ports used to communicate with the switches:

- **Connection Type:** Select static or dynamic routes. In this tutorial, select **Dynamic Route**.
- **Port:** Click the **Edit** option in the **Configurations** area, enter the IP addresses of the ports used for communication and select whether to enable OSPF.

In this tutorial, OSPF is enabled and the ports used for communicating with the switches are 192.168.13.2/24 and 192.168.14.2/24.

Port Management

Connection Type

☐ Static Route ☒ Dynamic Route

☒ OSPF ☐ BGP

Configurations Edit

Port	Whether to enable OSPF	IP address
• Port0	NO	-
• Port1	NO	-
• Port2 (Used for management port)	NO	-
• Port3	NO	-
• Port4	NO	-

7. Configure OSPF.

In this tutorial, MD5 authentication is selected. Enter the service IP address 192.168.101.2 as the RouterId.

OSPF global configuration :

* Area ID :

2

* Hello_time :

3

* Dead_time :

10

* Authentication

☐ Not

☐ Plain Text

☒ MD5

Method :

certified

Authentication

certification

* MD5 key ID :

7

* MD5 key :


1234

* Routerid :

192.168.101.2

* Area Type :

nssa

Configuration	Description
Connection method	<div>Choose to access the switch using static or dynamic routing.</div> <div> Notice: When dual-device one-arm mode is used, only dynamic routing is supported.</div>

Configuration	Description
Port	Click the Edit option in the Configuration Information area, enter the IP address of the port used for communication and select whether to enable OSPF. Port 2 is the default management port.
OSPF routing configuration	
Area ID	The ID of the area. Make sure that area IDs of SAG device 1 and SAG device 2 are different and the area ID of each SAG device is the same as that of the corresponding peer switch.
Hello_time	The interval at which hello packets are sent, in seconds. Default value: 3 seconds.
Dead_time	The dead interval of OSPF neighbor, in seconds. The neighbor relation stops if no hello packet is received during the dead time. Default value: 10 seconds.
Authentication method	Select an authentication method. <ul style="list-style-type: none">· Do not authenticate: Do not perform authentication.· Clear Text Authentication: Enter a clear text password.· MD5 Authentication: Use the MD5 method to perform authentication. Enter the MD5 key ID and the MD5 key.
Routerid	The ID of the OSPF router. We recommend that you directly use the service IP address.
Area Type	The area type is nssa by default.

Configure the peer switches (Ruijie)

After you have configured device 2, you need to add route configurations for the peer switches of device 2 according to the following configurations. For switches of different manufacturers, see the device manuals for specific configurations.

- Route configurations of the peer switches.



Note:

You must configure the network type of the interfaces using the OSPF protocol on the same Smart Access Gateway device to p2p, otherwise the routes cannot be correctly calculated.

```

interface GigabitEthernet 0 / 13
no switchport
ip ospf network point-to-point The network type
must be p2p
ip ospf authentication message-digest
ip ospf message-digest-key 7 md5 1234
ip ospf hello-interval 3
ip ospf dead-interval 10
ip address 192.168.13.1 255.255.255.0 The
IP address of port on the peer switch of the
SAG device

interface GigabitEthernet 0 / 14
no switchport
ip ospf network point-to-point The network type
must be p2p
ip ospf authentication message-digest
ip ospf message-digest-key 7 md5 1234
ip ospf hello-interval 3
ip ospf dead-interval 10
ip address 192.168.14.1 255.255.255.0 The
IP address of the port on the peer switch of
the SAG device

```

- Configure the loopback address of the switch.



Note:

You must configure OSPF to be in the NSSA area and to automatically generate default routes and advertise the routes to the SAG device.

```

interface Loopback 0
ip address 192.168.101.3 255.255.255.255
The loopback address of the switch

router ospf 1
router-id 192.168.101.4
The router ID of the switch

area 0
area 1
area 2
area 2 nssa translator always default-information-
originate
area 1 nssa translator always default-information-
originate
network 192.168.3.0 0.0.0.255 area 0
The CIDR block of the local PC
network 192.168.11.0 0.0.0.255 area 1
The CIDR block of the switch
network 192.168.12.0 0.0.0.255 area 1
network 192.168.13.0 0.0.0.255 area 2
network 192.168.14.0 0.0.0.255 area 2
network 192.168.100.0 0.0.0.255 area 0
The CIDR block used for communicating
with the uplink router

```

```
network 192 . 168 . 101 . 3 0 . 0 . 0 . 0 area 0
The loopback address of the switch
default - information originate always
Advertise default routes to the SAG device
```

Configure the peer switches (Cisco)

After you have configured device 2, you need to add route configurations for the peer switches of device 2 according to the following configurations. For switches of different manufacturers, see the device manuals for specific configurations.

- Route configurations of the peer switches.



Note:

You must configure the network type of the interfaces using the OSPF protocol on the same Smart Access Gateway device to p2p, otherwise the routes cannot be correctly calculated.

```
interface GigabitEthernet 0 / 13
no switchport
ip address 192 . 168 . 11 . 1 255 . 255 . 255 . 0 The IP
address of the port on the peer switch of the
Smart Access Gateway device
ip ospf network point-to-point The network type
must be p2p
ip ospf authentication message-digest
ip ospf message-digest-key 7 md5 1234
ip ospf dead-interval 10
ip ospf hello-interval 3
!
interface GigabitEthernet 0 / 14
no switchport
ip address 192 . 168 . 11 . 1 255 . 255 . 255 . 0 The IP
address of the port on the peer switch of the
Smart Access Gateway device
ip ospf network point-to-point The network type
must be p2p
ip ospf authentication message-digest
ip ospf message-digest-key 7 md5 1234
ip ospf dead-interval 10
ip ospf hello-interval 3
!
```

- Configure the loopback address of the switch.



Note:

You must configure OSPF to be in the NSSA area and to automatically generate default routes and advertise the routes to the Smart Access Gateway device.

```
interface Loopback 0
ip address 192 . 168 . 101 . 3 255 . 255 . 255 . 255
The loopback address of the switch
!
```

```

router ospf 1
router - id 192 . 168 . 101 . 3
The router ID of the switch
area 2 nssa default - informatio n - originate no -
summary Advertise default routes to the Smart
Access Gateway device
network 192 . 168 . 3 . 0 0 . 0 . 0 . 255 area 0
The CIDR block of the local PC
network 192 . 168 . 11 . 0 0 . 0 . 0 . 255 area 1
The CIDR block of the switch
network 192 . 168 . 12 . 0 0 . 0 . 0 . 255 area 1
network 192 . 168 . 100 . 0 0 . 0 . 0 . 255 area 0
The CIDR block used for communicat ing
with the uplink router
network 192 . 168 . 101 . 3 0 . 0 . 0 . 0 area 0
The loopback address of the switch
network 192 . 168 . 11 . 0 0 . 0 . 0 . 255 area 2
The CIDR block of the switch
network 192 . 168 . 14 . 0 0 . 0 . 0 . 255 area 2
default - informatio n originate always
!
```

3.5 Step 4: Console configuration

After you have configured the Smart Access Gateway (SAG) device, you need to activate the SAG device on the Smart Access Gateway console and complete the network configurations.

Step 1: Configure the network configuration

After activating the SAG device, you must attach the SAG instance to the CCN instance and attach the CCN instance to the CEN instance to which the target VPCs belong.

To configure the network, follow these steps:

1. Log on to the [Smart Access Gateway console](#).
2. On the SAG page, find the target gateway instance.
3. Click Configure Network in the Actions column.

4. On the Configure Network page, configure the following parameters:

- a. **Private CIDR Block:** Configure the private CIDR blocks used by the local clients to access Alibaba Cloud. Make sure all private CIDR blocks do not conflict with one another.

In this tutorial, enter 192.168.3.0/24. Configuring a CIDR block with a 32-bit mask is not supported.

- b. **CCN Instance ID/Name:** Add the gateway instance to the CCN instance. Then gateway devices in the CCN instance can communicate with one another.

In this tutorial, the default CCN is used. For more information, see [Cloud Connect Network](#).

5. **Bind CEN Instance:** Select the CEN instance to attach. After the CCN instance is attached to the CEN instance, gateway devices in the CCN instance can communicate with networks (VPCs and VBRs) attached to the CEN instance.
6. Click OK.

Step 2: Activate the SAG device

After configuring the network connection, you must activate the SAG device:

To activate the SAG device, follow these steps:

1. Log on to the [Smart Access Gateway console](#).
2. On the SmartAG page, find the target gateway instance.
3. Click Activate in the Actions column.

Step 3: Configure an ACL

To configure an access control list (ACL), follow these steps:

1. Log on to the [Smart Access Gateway console](#).
2. Click ACL and configure an ACL rule for the SAG device. For more information, see [Configure an ACL rule](#).

	Authorization Policy	Protocol	Direction	Source CIDR	Port Range	Destination CIDR	Destination Port Range	Priority	Actions
<input type="checkbox"/>	Allow	TCP	Outbound		1/65535		1/65535	1	Modify Delete
<input type="checkbox"/>	Block	TCP	Outbound		1/65535		1/65535	1	Modify Delete

Step 4: Configure a security group

Configure a security group to allow local branches to access the VPCs.

To configure the security group, follow these steps:

1. Log on to the [ECS Console](#).
2. In the left-side navigation pane, click Instances.
3. Find the target ECS instance in the target VPC, and then choose More > Network and Security Group > Configure Security Group.
4. Click Add Rules and click Add Security Group Rule.

5. Configure a security group rule that allows access from local branches.

The following figure shows the security group configurations in this tutorial. You must enter the private CIDR blocks of the local branches as the authorization objects.

Add Security Group Rule

NIC:

Intranet

Rule Direction:

Ingress

Action:

Allow

Protocol Type:

Customized TCP

* Port Range:

1/65535

i

Priority:

1

i

Authorization Type:

CIDR

* Authorization Objects:

172.16.0.0/12

i Tutorial

Description:

It can be 2 to 256 characters in length and cannot start with http:// or https://.

OK

Cancel

4 Configure Smart Access Gateway as the backup of a physical connection

4.1 Configuration overview

This tutorial shows you how to use the Smart Access Gateway (SAG) device as the backup link of an existing physical connection to access Alibaba Cloud and build a high-availability hybrid cloud.

Scenarios

This tutorial uses the network architecture shown in the following figure as an example. In the example, the on-premises data center is already connected to Alibaba Cloud through a physical connection by using Express Connect. To ensure high service availability and avoid unnecessary changes to the network architecture, the Smart Access Gateway (SAG-1000) device is connected to a Layer-3 switch by using the one-arm mode and connected to Alibaba Cloud as a backup to the existing physical connection.



Note:

- Only an SAG-1000 device can form active and standby links with a leased line.
- Only access through the physical connection of Cloud Enterprise Network (CEN) is supported. Access through Express Connect is not supported.
- Make sure that Border Gateway Protocol (BGP) has been configured for the Virtual Border Router (VBR) of the leased line. If a static route is configured for the VBR, the VBR cannot be used as a backup leased line.

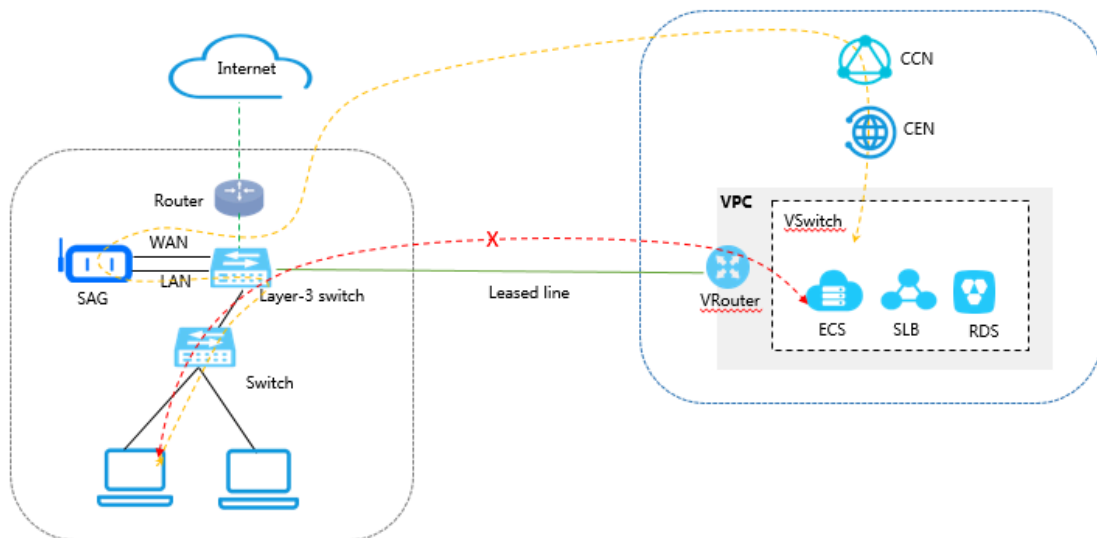
The flow direction of network traffic in this tutorial is as follows:

- To Alibaba Cloud:

By default, the routing priority is configured on the core switch of your on-premises data center, and traffic is distributed to Alibaba Cloud through the physical connection. If the physical connection fails, traffic is encrypted and then distributed to Alibaba Cloud over the Internet.

- To the on-premises data center:

By default, the CEN gives higher priority to routing through the physical connection, rather than through the CCN. More specifically, the traffic is distributed to your on-premises data center through the physical connection. If the physical connection fails, traffic is encrypted and then distributed to Alibaba Cloud (to the CCN instance) over the Internet.



Network planning

Before you begin, you must plan the following network configurations and ensure that the CIDR blocks do not conflict with one another:

- The CIDR block of the VPC to connect. In this tutorial, the CIDR block of the VPC is 192.168.0.0/24.
- Local server/client IP address

Plan the IP address of the local server/client as needed. In this tutorial, the IP address 192.168.3.0/24 is used.

- The IP address used by the device to connect to the Layer-3 switches

Plan the IP address of the port used by the SAG device to communicate with the Layer-3 switches. In this tutorial, the IP address of service port 3 used by the device is 192.168.11.2/24.

- The IP address used by the Layer-3 switches to connect to Alibaba Cloud

Make sure that the IP address used by the Layer-3 switches to connect to Alibaba Cloud and the IP address of the WAN port are in the same CIDR block. In this

tutorial, the Layer-3 switches use the IP address 172.16.0.254 to access Alibaba Cloud.

Table 4-1: Example values in this tutorial

Configuration	Example value
The CIDR block of the VPC	192.168.0.0/24
The CIDR block of the egress router	192.168.100.253/24
The CIDR block used by the Layer-3 switches to communicate with Alibaba Cloud	192.168.100.100/24
The CIDR block used by the Layer-3 switches to communicate with the SAG device	192.168.3.1/24
IP addresses of the ports used by SAG device 1	G3 192.168.11.2/24 G4 192.168.12.2/24
IP addresses of the ports used by SAG device 2	G3 192.168.13.2/24 G4 192.168.14.2/24
IP addresses of the ports used by the peer switches of the SAG devices	G11 192.168.11.1/24 G12 192.168.12.1/24 G13 192.168.13.1/24 G14 192.168.14.1/24
The CIDR block of local servers	192.168.3.0/24

4.2 Step 1: Purchase a Smart Access Gateway device

After you buy a Smart Access Gateway (SAG) device in the console, Alibaba Cloud delivers the device to you and creates an SAG instance for you to manage.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. On the SAG page, click Create SmartAG.

3. Configure the SAG device and click Buy Now.

For more information, see [Buy a Smart Access Gateway](#).



Note:

In this tutorial, the SAG-1000 specification and the Standby usage method are selected.

4. Confirm the order information, and then click Pay.

5. On the Address dialog box, enter the shipping address of the gateway device and click Order Now.

You can check whether the order is successfully placed on the status page of the Smart Access Gateway instance. The system will deliver the device within two days after the order is placed. If you do not receive the device within two days, you can open a ticket to check the delivery status.

Instance ID/Name	CCN Instance ID/Name	Peak Bandwidth	Status	Private CIDR Block	Expires At	Actions
...	...	5Mbps Change Specification	Offline ⓘ		Dec 22, 2019, 18:07:30	Configure Network View Help Renew
...	...	1Mbps Change Specification	Ordered		Dec 22, 2019, 18:07:30	Configure Network Notify Delivery Renew

4.3 Step 2: Configure the SAG device and Layer-3 switches

This tutorial shows you how to configure the routes of the Smart Access Gateway (SAG) device and its peer switches.

Configure the SAG device

To configure the SAG device, follow these steps:

1. After receiving the SAG device, follow [SAG-1000 user manual](#) to check if all the accessories are provided, and then power on the SAG device.
2. Connect port G3 of the SAG device to port G11 of switch A, and connect port G4 of the device to port G12 of switch B.
3. Connect the network card of the PC to port 2 of the SAG device, and set the IP address of the network card to 192.168.0.100/24.
4. Open your browser and enter the web configuration address of the SAG device.

The default IP address is `https://192.168.0.1`. For more information, see [Log on to the web configuration page](#).

5. Configure the service IP address and the management port.

In this tutorial, set the service IP address to 192.168.101.1, set the management IP address to 192.168.20.1/24, and set the next hop to 192.168.20.4.

Service IP

* Configure Service IP :

192.168.101.1

* Management Interface : Port 2

* Isolate or not :

☒ Yes ☐ NO

* Management port IP :

192.168.20.1/24

* Next Hop :

192.168.20.4

OK

Cancel

Configuration	Description
Configure Service IP:	The service IP address is used to establish the VPN tunnel.
Management Interface:	The management port is used for the local client to access the Web console. Port 2 is the management port by default.
Management port IP:	The management IP address is used for the local client to access the Web console.

Configuration	Description
Isolate or not:	<p>Select whether to isolate the service port from the management port:</p> <ul style="list-style-type: none">· Yes: This port can only be used as a local Web management port and cannot be used as a service port. <p>In the isolation mode, the service traffic and the management traffic do not communicate with each other, thus achieving a higher level of security.</p> <ul style="list-style-type: none">· No: This port is used as both the local Web management port and the service port.
Next Hop	If you choose to isolate the service port from the management port, specify the next hop of the management port.

6. Configure the ports used to communicate with the switches:

- **Connection Type:** Select static or dynamic routing. In this tutorial, select Dynamic Route.
- **Port:** Click the Edit option in the Configurations area, enter the IP addresses of the ports used for communication and select whether to enable Open Shortest Path First (OSPF).

In this tutorial, OSPF is enabled. The IP addresses of the ports used for communicating with the switches are 192.168.11.2/24 and 192.168.12.2/24.

Port Management

Connection Type

☐ Static Route ☒ Dynamic Route

☒ OSPF ☐ BGP

Configurations [Edit](#)

Port	Whether to enable OSPF	IP address
• Port0	NO	-
• Port1	NO	-
• Port2 (Used for management port)	NO	-
• Port3	NO	-
• Port4	NO	-

7. Configure OSPF.

In this tutorial, MD5 authentication is selected, and the service IP address used by the RouterID is 192.168.101.1.

OSPF global configuration :

* Area ID :

1

* Hello_time :

3

* Dead_time :

10

* Authentication

☐ Not

☐ Plain Text

☒ MD5

Method :

certified

Authentication

certification

* MD5 key ID :

7

* MD5 key :


1234

* Routerid :

192.168.101.1

* Area Type :

nssa

Configuration	Description
Connection method	<div>Choose to access the switch using static or dynamic routing.</div> <div> Notice: When dual-device one-arm mode is used, only dynamic routing is supported.</div>

Configuration	Description
Port	<p>Click the Edit option in the Configuration Information area, enter the IP address of the port used for communication and select whether to enable OSPF.</p> <p>Port 2 is the default management port.</p>
OSPF routing configuration	
Area ID	<p>The ID of the area.</p> <p>Make sure that area IDs of SAG device 1 and SAG device 2 are different and the area ID of each SAG device is the same as that of the corresponding peer switch.</p>
Hello_time	<p>The interval at which hello packets are sent, in seconds.</p> <p>Default value: 3 seconds.</p>
Dead_time	<p>The dead interval of OSPF neighbor, in seconds. The neighbor relation stops if no hello packet is received during the dead time.</p> <p>Default value: 10 seconds.</p>
Authentication method	<p>Select an authentication method.</p> <ul style="list-style-type: none">· Do not authenticate: Do not perform authentication.· Clear Text Authentication: Enter a clear text password.· MD5 Authentication: Use the MD5 method to perform authentication. Enter the MD5 key ID and the MD5 key.
Routerid	<p>The ID of the OSPF router. We recommend that you directly use the service IP address.</p>
Area Type	<p>The area type is nssa by default.</p>

Configure the peer switches

Add route configurations for the peer switches of the device according to the following configurations. Here a switch is taken as an example. For switches of other manufacturers, see the device manuals for specific configurations.

- Route configurations of the peer switches.



Note:

You must configure the network type of the interfaces using the OSPF protocol on the same Smart Access Gateway device to p2p, otherwise the routes cannot be correctly calculated.

```

interface GigabitEthernet 0 / 11
no switchport
ip ospf network point-to-point
ip ospf authentication message-digest
ip ospf message-digest-key 7 md5 1234
ip ospf hello-interval 3
ip ospf dead-interval 10
ip address 192.168.11.1 255.255.255.0 The
IP address of the port on the peer switch of
the SAG device

interface GigabitEthernet 0 / 12
no switchport
ip ospf network point-to-point
ip ospf authentication message-digest
ip ospf message-digest-key 7 md5 1234
ip ospf hello-interval 3
ip ospf dead-interval 10
ip address 192.168.12.1 255.255.255.0 The
IP address of the port on the peer switch of
the SAG device

```

- Configure the loopback address of the switch.



Note:

You must configure OSPF to be in the NSSA area and to automatically generate default routes and advertise them to the SAG device.

```

interface Loopback 0
ip address 192.168.101.3 255.255.255.255
The loopback address of the switch

router ospf 1
router-id 192.168.101.3
The router ID of the switch

area 0
area 1
area 1 nssa translator always default-information-originate
network 192.168.3.0 0.0.0.255 area 0
The CIDR block of the local PC
network 192.168.11.0 0.0.0.255 area 1
The CIDR block of the switch
network 192.168.12.0 0.0.0.255 area 1
network 192.168.13.0 0.0.0.255 area 1
network 192.168.14.0 0.0.0.255 area 1
network 192.168.100.0 0.0.0.255 area 0
The CIDR block used for communicating
with the uplink router
network 192.168.101.3 0.0.0.0 area 0
The loopback address of the switch

```

```
default - informatio n originate always
Advertise default routes to the SAG device
```

4.4 Step 3: Console configuration

After you have configured the Smart Access Gateway (SAG) device, you need to activate it on the console and attach the Cloud Connect Network (CCN) instance where the SAG device belongs to the Cloud Enterprise Network (CEN) instance where the physical connection belongs.

Step 1: Activate the SAG device

To activate the SAG device, follow these steps:

1. Log on to the [Smart Access Gateway console](#).
2. On the SmartAG page, find the target gateway instance.
3. Click Activate in the Actions column.

Step 2: Configure active/standby links

To configure active/standby links, follow these steps:

1. Log on to the [Smart Access Gateway console](#).
2. On the SAG page, find the target gateway instance.
3. Click the ID of the target instance, and then in the High-Availability Configurations area, enable link-level backup.
4. Complete the following configuration, and then click OK:
 - High Availability Mode: Select Leased line.
 - Main Link: Select the established physical connection.



Notice:

Make sure the selected physical connection does not use Express Connect to establish a peering connection and that the corresponding Virtual Border Router (VBR) has configured Border Gateway Protocol (BGP) routing. If the physical connection is used to synchronize BGP routes for the VBR, check that the routes do not conflict with the CIDR block used by Smart Access Gateway to communicate with the switch.

Step 3: Configure the network connection

After activating the SAG device, you must attach the SAG instance to the CCN and attach the CCN to the CEN where the target VPC belongs.



Notice:

Make sure that the SAG instance and the VBR to which the physical connection belongs are in the same CEN instance.

To configure the network, follow these steps:

1. Log on to the [Smart Access Gateway console](#).
2. On the SAG page, find the target gateway instance.
3. Click Configure Network in the Actions column.
4. On the Configure Network page, configure the following parameters:
 - a. **Private CIDR Block:** Configure the private CIDR blocks used by the local clients to access Alibaba Cloud. Make sure all private CIDR blocks do not conflict with each other.

In this tutorial, enter 192.168.3.0/24.

- b. **CCN Instance ID/Name:** Add the gateway instance to the CCN instance. Then gateway devices in the CCN instance can communicate with one another.

In this tutorial, the default CCN is used. For more information, see [Cloud Connect Network](#).

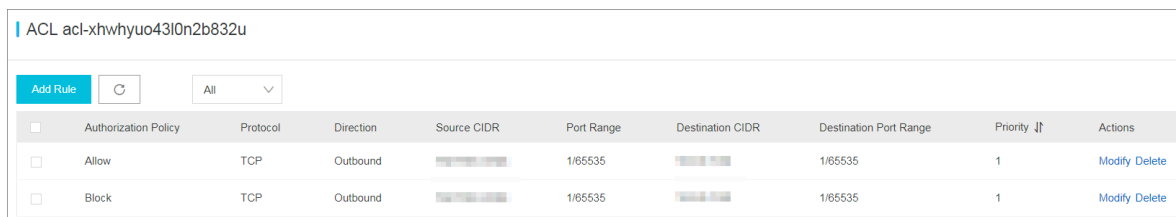
5. **Bind CEN Instance:** Select the CEN instance to attach. After the CCN instance is attached to the CEN instance, gateway devices in the CCN instance can communicate with networks (VPCs and VBRs) attached to the CEN instance.
6. Click OK.

Step 4: Configure an ACL

To configure an access control list (ACL), follow these steps:

1. Log on to the [Smart Access Gateway console](#).

2. Click ACL and configure an ACL rule for the SAG device. For more information, see [Configure an access control list](#).



The screenshot shows the ACL configuration page for an ACL named 'acl-xhwhyuo43l0n2b832u'. It features a table with columns for Authorization Policy, Protocol, Direction, Source CIDR, Port Range, Destination CIDR, Destination Port Range, Priority, and Actions. Two rules are listed: 'Allow' and 'Block', both for TCP protocol and Outbound direction, with Source CIDR 192.168.3.0/24 and Destination Port Range 1/65535.

<input type="checkbox"/>	Authorization Policy	Protocol	Direction	Source CIDR	Port Range	Destination CIDR	Destination Port Range	Priority	Actions
<input type="checkbox"/>	Allow	TCP	Outbound	192.168.3.0/24	1/65535	192.168.3.0/24	1/65535	1	Modify Delete
<input type="checkbox"/>	Block	TCP	Outbound	192.168.3.0/24	1/65535	192.168.3.0/24	1/65535	1	Modify Delete

Step 5: Configure a security group

Configure a security group to allow the local branches to access VPC.

To configure the security group, follow these steps:

1. Log on to the [ECS Console](#).
2. In the left-side navigation pane, click Instances.
3. Find the target ECS instance in the target VPC, and then choose More > Network and Security Group > Configure Security Group.
4. Click Add Rules and click Add Security Group Rule.
5. Configure a security group rule that allows access from local branches.

You must enter the private CIDR blocks of local branches as the authorization objects. In this case, enter 192.168.3.0/24.

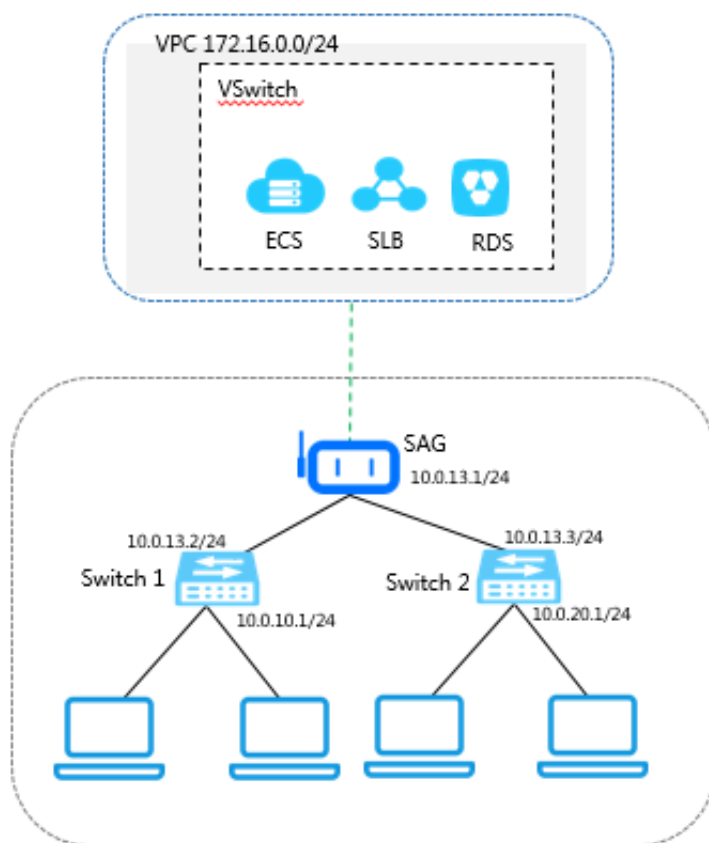
5 Tutorial for configuring local branches or headquarters with multiple CIDR blocks

5.1 Configuration overview

This tutorial guides you to connect local branches or headquarters with multiple private CIDR blocks to Alibaba Cloud.

Scenario

This tutorial takes the network architecture in the following figure as an example. Clients of the local branches are connected to two different switches, and the two switches are connected to Alibaba Cloud directly through the Smart Access Gateway (SAG).



Network planning

Before you begin, you must plan the following network configurations and ensure that the CIDR blocks do not conflict with one another:

- The CIDR block of the VPC to connect. In this tutorial, the CIDR block of the VPC is 172.16.0.0/24.

- Local client IP address

Plan the IP address of each local client according to your needs. In this tutorial, the CIDR blocks 10.0.10.0/24 and 10.0.20.0/24 are used.

- The IP addresses of the ports on the SAG device

Plan the IP addresses of the ports used by the SAG device to communicate with the Layer-3 switch. In this tutorial, the static IP address of the LAN port used by the SAG device is 10.0.13.1, and the WAN port of the SAG device accesses the Internet through DHCP.

- The IP address of the switch

Plan the IP addresses used by each switch to communicate with the SAG device and the IP addresses used by each switch to communicate with Alibaba Cloud.

Table 5-1: Example values in this tutorial

Configuration	Example value
The CIDR block of the VPC	172.16.0.0/24
The IP addresses of the ports on the SAG device	WAN port: Enable DHCP The static IP address used by the LAN port: 10.0.13.1/24
The CIDR blocks of switch 1	The IP address used for connecting to Alibaba Cloud: 10.0.13.2/24 The IP address used for connecting to the SAG device: 10.0.10.1/24
The CIDR blocks of switch 2	The IP address used for connecting to Alibaba Cloud: 10.0.13.3/24 The IP address used for connecting to the SAG device: 10.0.20.1/24

5.2 Step 1: Purchase a Smart Access Gateway device

After you buy a Smart Access Gateway (SAG) device in the console, Alibaba Cloud delivers the device to you and creates an SAG instance for you to manage.

Procedure

1. Log on to the [Smart Access Gateway console](#).
2. On the SAG page, click Create SmartAG.
3. Configure the SAG device and click Buy Now.

For more information, see [Gateway device configurations](#).



Note:

In this tutorial, the SAG-100WM specification and the Stand-alone usage method are selected.

4. Confirm the order information, and then click Pay.
5. On the Address dialog box, enter the shipping address of the gateway device and click Order Now.

You can check whether the order is successfully placed on the status page of the Smart Access Gateway instance. The system will deliver the device within two days after the order is placed. If you do not receive the device within two days, you can open a ticket to check the delivery status.

Smart Access Gateway Hardware

Usage CapacityDocumentationProduct Updates

Create SmartAG

Instance ID

Enter

Instance ID/Name	CCN Instance ID/Name	Peak Bandwidth	Status	Private CIDR Block	Expires At	Actions
		5Mbps Change Specification	● Offline ⓘ		Dec 22, 2019, 18:07:30	Configure Network View Help Renew ⋮
		1Mbps Change Specification	● Ordered			Configure Network Notify Delivery Renew ⋮

5.3 Step 2: Configure the SAG device and the peer switches

After receiving the Smart Access Gateway (SAG) device, you need to configure its WAN and LAN ports and add related routing configurations to the switch.

Configure the SAG device

To configure the SAG device, follow these steps:

1. After receiving the SAG device, follow [SAG-100WM overview](#) to check if all accessories are provided and then power on the device.

2. Connect the WAN port of the SAG device to the network cable and connect a LAN port to a client used for web configuration.
3. Open your browser and enter the web configuration address of the SAG device.

The default address is `https://192.168.0.1`. For more information, see [Log on to the web configuration page](#).

4. Click WAN Port Management to configure the method for connecting to the Internet.

In this tutorial, the WAN port uses a dynamic IP address allocated from the Internet router through DHCP to access the Internet. For more information, see [Configure the WAN port](#):

5. Click LAN Port Management. In this tutorial, disable the wireless function. The configurations are as follows:
 - Connection Type: Select Static IP.
 - LAN Address: In this tutorial, enter 10.0.13.1.
 - Configure Routes: Click Configure Routes and add two static routes. The destination CIDR block of each route is the CIDR block of the corresponding

client and the next hop of each route is the IP address of the port on the peer switch connected to the SAG device.

LAN port management

Wireless Configurations
Ethernet Configuration

Ethernet :

* Connection Type : ☐ Dynamic IP ⓘ ☒ Static IP

* LAN address :

* IP Mask :

Configure Routes : ☒

Add

Destination CIDR Block	Next Hop	Operations
10.0.10.0/24	10.0.13.2	Modify Delete
10.0.20.0/24	10.0.13.3	Modify Delete

OK
Cancel

Configure the switches

Add two routes on each switch and one of them is the default route. The next hop of the default route is the static IP address of the LAN port of the SAG device and the next hop of the other route is the IP address of the port on the peer switch.

Route configuration of switch 1:

```
ip route 0 . 0 . 0 . 0 / 0 10 . 0 . 13 . 1
ip route 10 . 0 . 20 . 0 / 24 10 . 0 . 13 . 3
```

Route configuration of switch 2:

```
ip route 0 . 0 . 0 . 0 / 0 10 . 0 . 13 . 1
ip route 10 . 0 . 10 . 0 / 24 10 . 0 . 13 . 2
```

5.4 Step 3: Console configuration

After you have configured the Smart Access Gateway (SAG) device, you need to activate the SAG device in the console and attach the CCN instance where the device belongs to the CEN instance where the physical connection belongs to access cloud services.

Step 1: Activate the SAG device

To activate the SAG device, follow these steps:

1. Log on to the [Smart Access Gateway console](#).
2. On the SmartAG page, find the target gateway instance.
3. Click Activate in the Actions column.

Step 2: Configure the network connection

After activating the SAG device, you must attach the SAG instance to the CCN instance and then attach the CCN instance to the CEN instance where the target VPC belongs.

To configure the network, follow these steps:

1. Log on to the [Smart Access Gateway console](#).
2. On the SAG page, find the target gateway instance.
3. Click Configure Network in the Actions column.
4. On the Configure Network page, configure the following parameters:
 - a. **Private CIDR Block:** Configure the private CIDR blocks used by the local gateway device to access Alibaba Cloud. Make sure all private CIDR blocks do not conflict with one other. In this tutorial, the following three private CIDR blocks are added:
 - 10.0.13.0/24
 - 10.0.10.0/24
 - 10.0.20.0/24



Note:

Configuring a CIDR block with a 32-bit mask is not supported.

Because the static IP address of the LAN port of the SAG device is 10.0.13.1, 10.0.13.0/24 is added as the first private CIDR block in this tutorial.

- If the LAN port of the SAG device uses a dynamic IP address and DHCP is enabled on the client, the IP address used by the local client is allocated from the first private CIDR block specified by you.
- If the LAN port of the SAG device uses a static IP address, the static IP address must be in the specified private CIDR block.

b. CCN Instance ID/Name: Add the gateway instance to the CCN instance. Then gateway devices in the CCN instance can communicate with one another.

In this tutorial, the default CCN is used. For more information, see [Cloud Connect Network](#).

5. Bind CEN Instance: Select the CEN instance to attach. After the CCN instance is attached to the CEN instance, gateway devices in the CCN instance can communicate with networks (VPCs and VBRs) attached to the CEN instance.
6. Click OK.

Step 4: Configure a security group

Configure a security group to allow local branches to access the VPCs.

To configure the security group, follow these steps:

1. Log on to the [ECS Console](#).
2. In the left-side navigation pane, click Instances.
3. Find the target ECS instance in the target VPC, and then choose More > Network and Security Group > Configure Security Group.
4. Click Add Rules and click Add Security Group Rule.
5. Configure a security group rule that allows access from local branches.

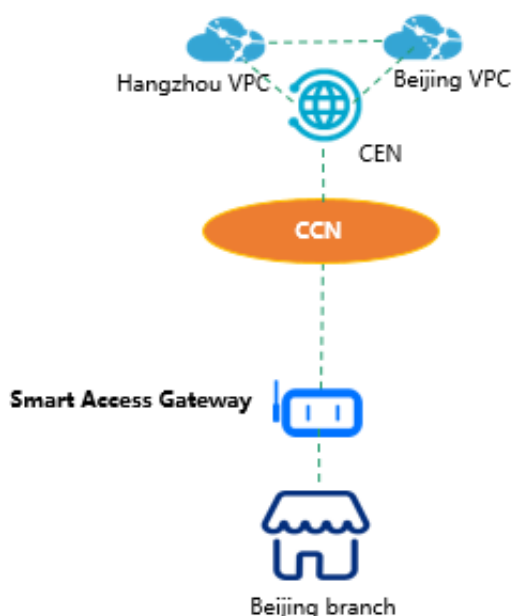
Enter the private CIDR blocks of local branches as the authorization objects. In this tutorial, enter 10.0.13.0/24, 10.0.10.0/24, and 10.0.20.0/24.

6 Cross-region access to VPC

This tutorial uses a Beijing branch as an example to describe how to connect local branches to VPCs in Hangzhou and US (Silicon Valley) through a Smart Access Gateway (SAG). After you connect local branches to VPCs, clients of the local branches can directly access the VPCs through the SAG.

Scenario

For access of local branches in Mainland China, you only need to attach the CCN associated with the SAG device to the CEN in the same area and configure the region connection between the Hangzhou VPC and the US (Silicon Valley) VPC.



To do so, complete the following steps:

1. Purchase an SAG device.
2. Connect the SAG device.
3. Activate the SAG device.
4. Configure the network connection.
5. Associate the CCN instance with a CEN instance.
6. Configure the CEN.
7. Configure a security group.
8. Perform an access test.

Prerequisites

- A CEN instance is created.
- A VPC in the Hangzhou region and a VPC in the US (Silicon Valley) region are created and are attached to the same CEN instance.
 1. Log on to the [Smart Access Gateway console](#).
 2. Choose Quick Links > VPC.
 3. Select the China (Hangzhou) region and click the ID of the target VPC instance in Hangzhou.
 4. On the VPC Details page, click Attach to CEN, and then select the target CEN instance.
 5. Repeat the preceding steps to add the VPC in US (Silicon Valley) to the same CEN instance.
- A CCN instance is created. For more information, see [Create a CCN instance](#).

Step 1: Purchase an SAG device

After you purchase an SAG device on the console, Alibaba Cloud delivers the device to you and creates an SAG instance for you.

To purchase an SAG device, follow these steps:

1. Log on to the [Smart Access Gateway console](#).
2. Click Create SmartAG.
3. Configure the SAG device and click Buy Now.

For more information, see [Buy a Smart Access Gateway](#).



Note:

In this tutorial, the SAG-100WM specification and the Stand-alone usage method are selected.

4. Confirm the order information, and then click Buy Now.
5. On the displayed Address dialog box, enter the shipping address of the gateway device and click Order Now.

You can check whether the order is successfully placed on the SAG page. The system will deliver the device within 48 hours after the order is placed. If you do

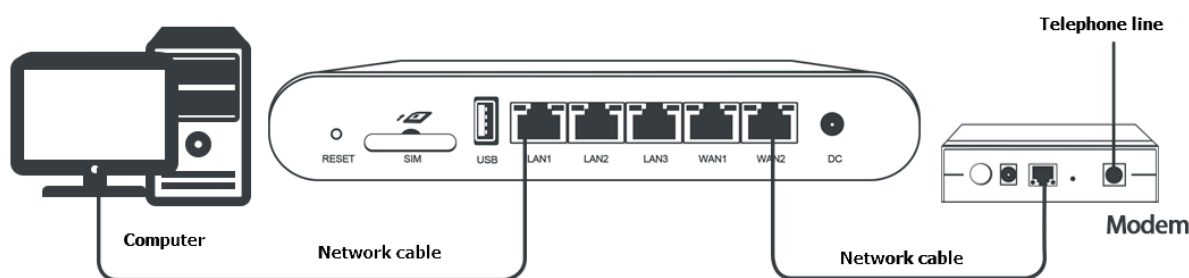
not receive the device within 48 hours, you can open a ticket to check the delivery status.

Create SmartAG <input type="button" value="C"/>		Instance ID <input type="text"/> Enter <input type="button" value="Q"/>				
Instance ID/Name	CCN Instance ID/Name	Peak Bandwidth	Status	Private CIDR Block	Expires At	Actions
sag-ke3k-connectN		1Mbps Change Specification	Ordered			Configure Network Notify Delivery Renew ...

Step 2: Connect the SAG device

After you receive the SAG device, check whether all accessories are provided according to [SAG-100WM overview](#). After you start the SAG device, connect the WAN port to the network cable and connect the LAN ports to local clients.

In this tutorial, the clients in the Hangzhou and US (Silicon Valley) branches can be directly connected to Alibaba Cloud through SAG devices, so you can use the default gateway configurations. If you need to configure the WAN port and LAN ports, see [Step 3: Configure the WAN ports](#).



Step 3: Activate the SAG device

Before you can use the SAG device, you must activate it.

To activate the SAG device, follow these steps:

1. Log on to the [Smart Access Gateway console](#).
2. On the SmartAG page, find the target gateway instance.
3. Click Activate in the Actions column.

Step 4: Configure the network connection

After you activate and connect the SAG device, you also need to add the SAG device to a CCN.

To configure the network, follow these steps:

1. Log on to the [Smart Access Gateway console](#).

2. In the left-side navigation pane, click Smart Access Gateway, and then click the target instance ID or click Configure Network in the Actions column.
3. Configure the synchronization method for on-premises routes.

- a. Click Method to Synchronize with On-premises Routes.
- b. Select Static Routing, and then click Add Static Routing.

In this example, enter 172.16.0.0/12.

- c. Click OK.

4. Associate the SAG instance with a CCN

- a. Click Network Instance Details.
- b. Click Add Network Instance, and then select the target CCN. The SAG instances in the CCN can communicate with each other.

In this example, the default CCN is used. For more information, see [Cloud Connect Network](#).

- c. Click OK.

Step 5: Associate the CCN instance with a CEN instance

To associate the CCN instance with a CEN instance, follow these steps:

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, click CCN.
3. Find the target CCN instance, and then click Bind CEN Instance in the Actions column.
4. On the Bind CEN instance page, select the target CEN instance. After the CCN instance is associated with the CEN instance, the SAG devices in the CCN instance

can communicate with the network instances (VPCs and VBRs) attached to the CEN instance.

The screenshot shows a dialog box titled "Bind CEN Instance" with a question mark icon and a close button (X) in the top right corner. Inside the dialog, there is a label "Name/ID" above a text input field containing "ccn-bvt-sa". Below this is a section header "* Bind CEN Instance" with a question mark icon. Underneath is a dropdown menu showing "bvt-test/cen-3" with a downward arrow. At the bottom right of the dialog are two buttons: "OK" (blue) and "Cancel" (gray). On the right side of the dialog, there is a vertical "Contact Us" button with a speech bubble icon.

Step 6: Configure the CEN

To connect networks in different regions, you must purchase a bandwidth package and set the cross-region interconnection bandwidth.

1. Log on to the [Smart Access Gateway console](#).
2. In the left-side navigation pane, choose Quick Links > CEN.

3. On the CEN page, click the Networks tab page to check whether the Hangzhou VPC, the US (Silicon Valley) VPC, and the CCN are attached to the CEN.

Networks						
Attach Network Refresh						
Instance ID/Name	Region	Network Type	Account ID	attach time	Status	Actions
	China (Hangzhou)	VPC	120123456789	10/16/2018, 16:46:00	● Attached	Detach
	US (Silicon Valley)	VPC	120123456789	10/16/2018, 16:47:00	● Attached	Detach
	China (Qingdao)	VPC	120123456789	01/20/2019, 15:57:00	● Attached	Detach

4. Click the Bandwidth Packages tab page and click Buy Bandwidth Package (Pay-As-You-Go) to purchase a Pay-As-You-Go Bandwidth package.
5. On the CEN (Pay-As-You-Go) page, configure the bandwidth package.
 - Cloud Enterprise Network: Select the CEN associated with the VPCs and the CCN.
 - Area A and Area B: Select the areas of the VPCs that need to communicate with each other.

In this example, Mainland China and North America are selected.
 - Bandwidth: Select the bandwidth of the region connection as needed.
 - Bandwidth Package Name: Enter the name of the bandwidth package.
6. Click Buy Now to purchase a bandwidth package.
7. Click the Region Connections tab page and then click Set Region Connection.
8. Set the region connection. The sum of all region connections under a bandwidth package cannot be greater than the bandwidth of the bandwidth package.
 - Bandwidth Packages: Select the bandwidth package that is used by the CEN instance. In this example, select Mainland China \rightleftharpoons North American.
 - Connected Regions: Select the regions to be connected. In this example, select China (Hangzhou) and US (Silicon Valley), and also select Mainland China and US (Silicon Valley).
 - Bandwidth: Enter the bandwidth as needed.



Note:

The sum of all region connections under a bandwidth package cannot be greater than the bandwidth of the bandwidth package.

Figure 6-1: Region connection 1

The screenshot shows a dialog box titled "Set Region Connection". It contains three sections:

- Bandwidth Packages:** A dropdown menu showing "Mainland China⇌North America".
- Connected Regions:** Two dropdown menus separated by a double-headed arrow. The left dropdown shows "China (Hangzhou)" and the right dropdown shows "US (Silicon Valley)".
- Bandwidth:** A numeric input field with the value "1", plus and minus buttons, and the text "Available Bandwidth 2Mbps".

Figure 6-2: Region connection 2

The screenshot shows a dialog box titled "Set Region Connection". It contains three sections:

- Bandwidth Packages:** A dropdown menu showing "Mainland China⇌North America".
- Connected Regions:** Two dropdown menus separated by a double-headed arrow. The left dropdown shows "Mainland China" and the right dropdown shows "US (Silicon Valley)".
- Bandwidth:** A numeric input field with the value "1", plus and minus buttons, and the text "Available Bandwidth 2Mbps".

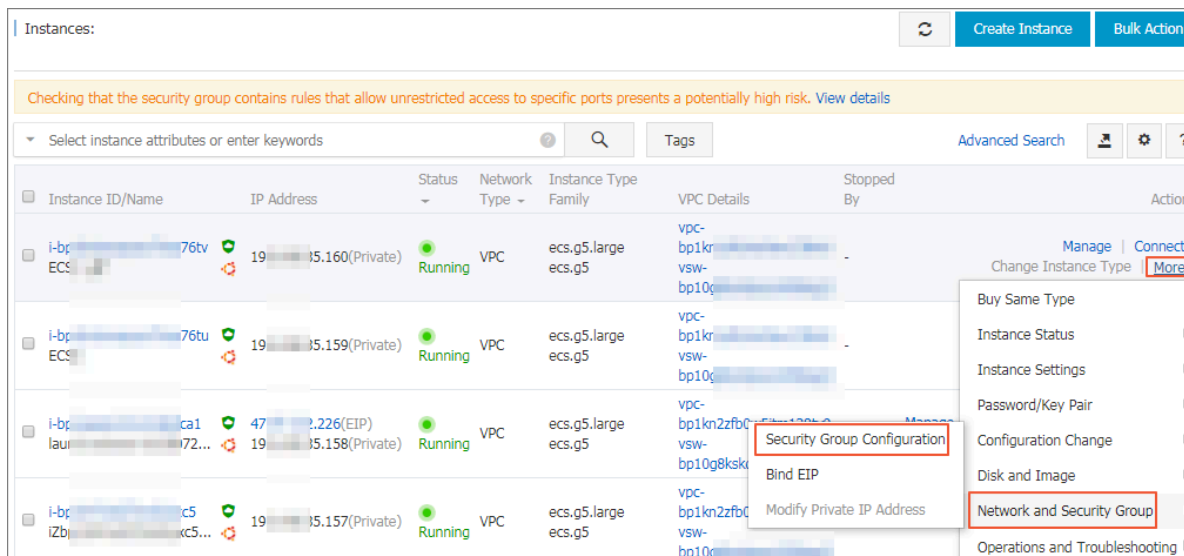
Step 7: Configure a security group

To allow local branches to access the VPC, you must configure a security group.

To configure a security group, follow these steps:

1. Log on to the [ECS Console](#).
2. In the left-side navigation pane, click Instances.

- Find the target ECS instance in the target VPC, and then choose More > Network and Security Group > Configure Security Group.



- Click Add Rules and click Add Security Group Rule.

5. Configure a security group rule that allows access from local branches.

The following figure shows the security group configurations in this tutorial. You must enter the private CIDR blocks of the local branches as the authorization objects.

Add Security Group Rule

NIC: Intranet

Rule Direction: Ingress

Action: Allow

Protocol Type: Customized TCP

* Port Range: 1/65535

Priority: 1

Authorization Type: CIDR

* Authorization Objects: 172.16.0.0/12

Description:

It can be 2 to 256 characters in length and cannot start with http:// or https://.

OK Cancel

Step 8: Perform an access test

After you complete the preceding configurations, you can access cloud resources deployed in the connected VPCs from local clients to check whether the new configurations take effect.