Alibaba Cloud Smart Access Gateway

Best Practices

Issue: 20190516

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.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

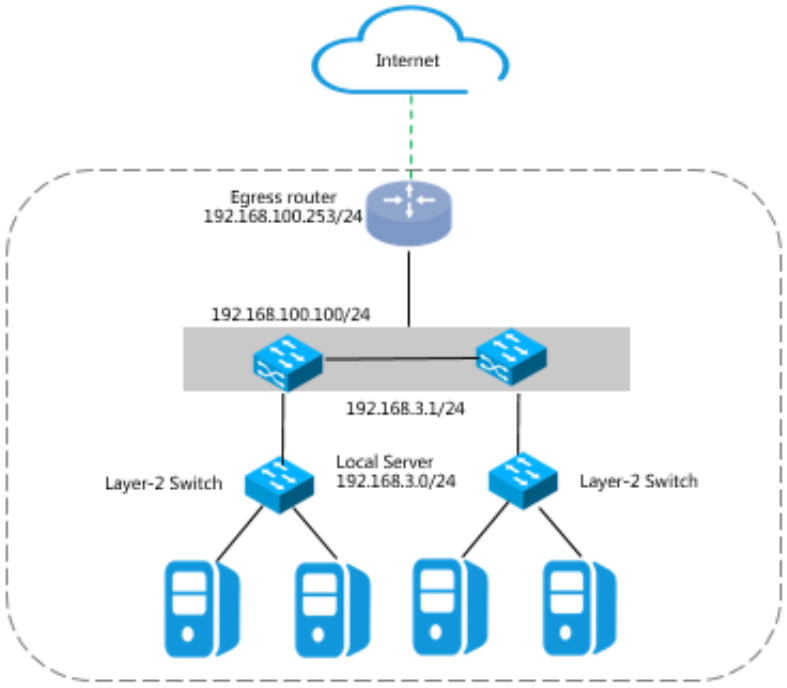
1 SAG-1000 stand-alone one-arm static route configuration tutorial

1.1 Configuration overview

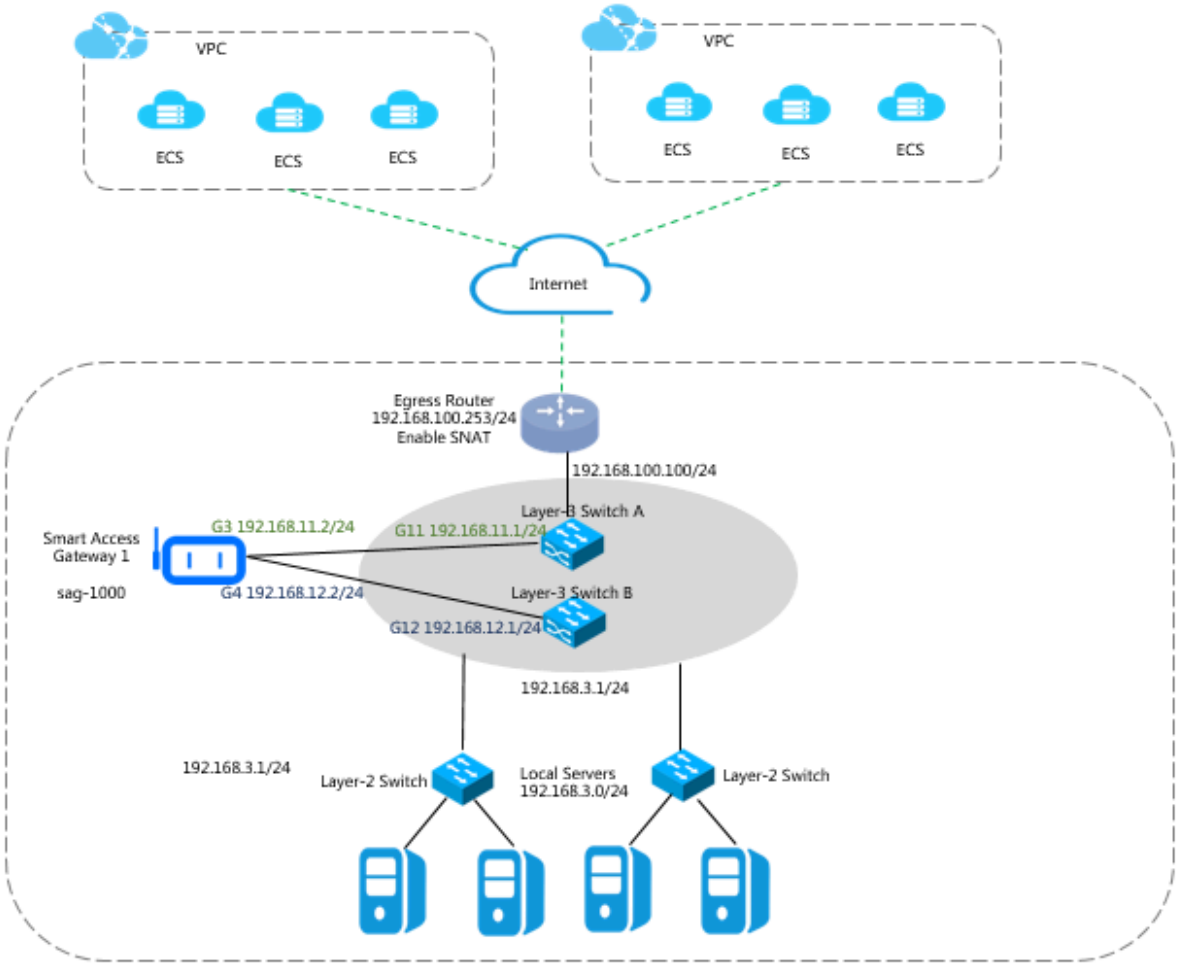
This tutorial guides you in how to connect your headquarters or branches to Alibaba Cloud through SAG-1000 Smart Access Gateway.

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, 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.
- IPs of local servers/clients

  Plan the IPs of the local servers/clients according to your needs. In this tutorial, the IP 192.168.3.0/24 is used.
- IPs used by the device to communicate with the Layer-3 switches

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

- Service IP

  Plan the service IP of the Smart Access Gateway device. We recommend that you set the mask to /32. In this tutorial, the service port IP 192.168.101.1 is used.

- Administration port IP

  Plan the administration port IP of the Smart Access Gateway device. You can use an independent administrator port IP or use the service port IP as the administrator port IP. In this tutorial, 192.168.0.1/24 is used as the administration port IP.

Table 1-1: 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 Smart Access Gateway	192.168.3.1/24
IPs of the ports of the Smart Access Gateway	G3 192.168.11.2/24 G4 192.168.12.2/24
IPs of the ports on the peer switches of the Smart Access Gateway	G11 192.168.11.1/24 G12 192.168.12.1/24
The CIDR block of local servers	192.168.3.0/24

1.2 Step 1: Buy 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 Hardware*.

   > 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.

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

This tutorial shows you how to configure the Smart Access Gateway device (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* 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.

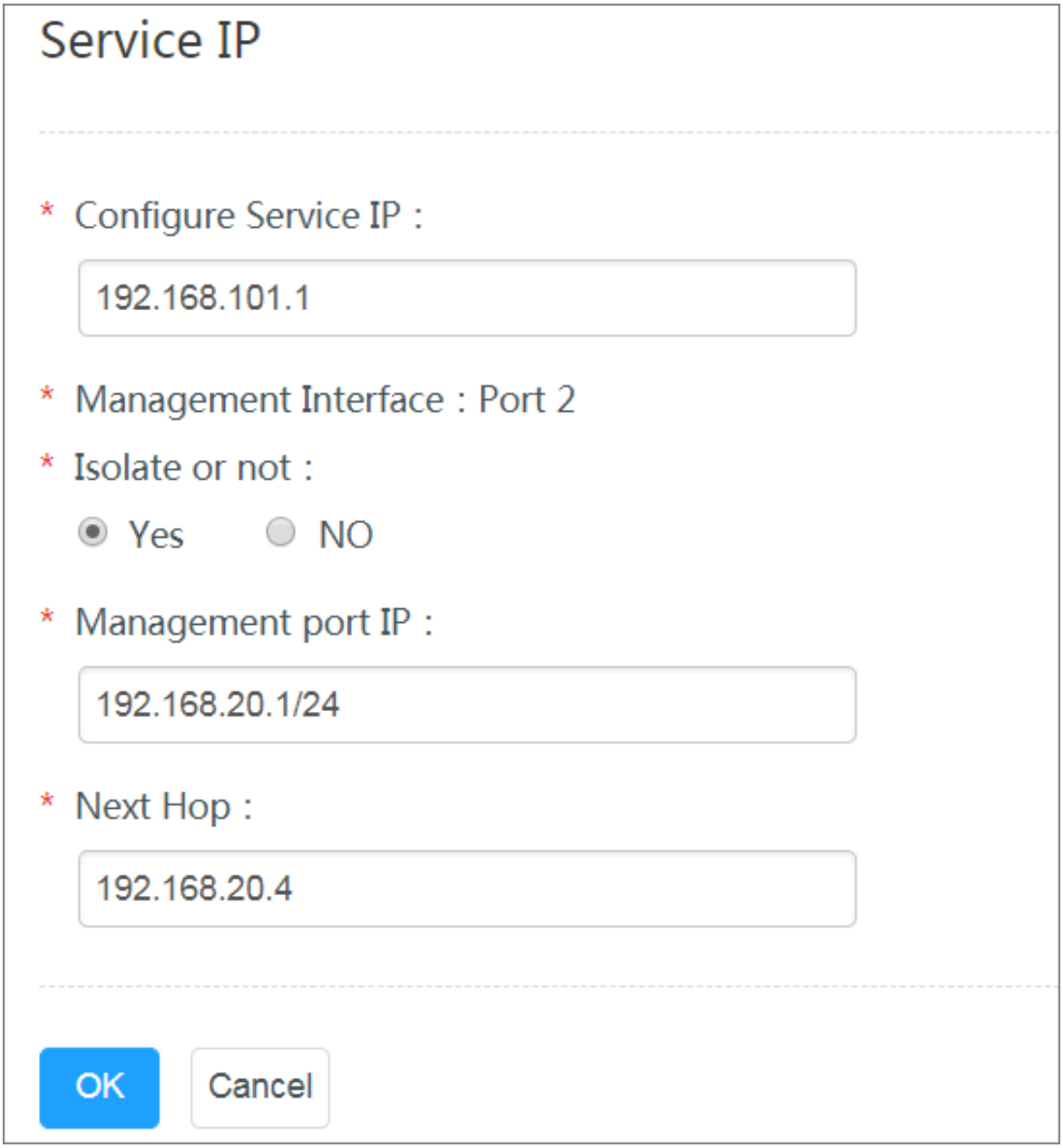
   The default address is https: // 192.168.0.1. For more information, see *Log on to the web configuration page*.

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

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

    Note:

Make sure that the specified service IP address can 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.



Configuration	Description
Service IP address	The service IP address is used to establish the VPN tunnel. Notice: Make sure that the specified service IP can access the Internet.
Administration port	The administration port is used for local clients to access the Web console. By default, port 2 is the administration port.

Configuration	Description
Administration IP	The administration IP is used for web access of the local client.
Whether to isolate	Select whether to isolate the service port from the administration port: · Yes: This port can only be used as a local web administration port and cannot be used as a service port. In the isolation mode, the service traffic and the administration traffic do not have impact on each other, so higher security is achieved. · No: This port is used as both the local web administration port and the service port.
Next hop	If you choose to isolate the service port from the administration port, specify the next hop of the administration 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 other device manufacturers, see the corresponding device manuals.

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
  of   the   port   on   the   peer   switch   of   Smart   Access
Gateway

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

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

```
ip   route   192 . 168 . 101 . 2   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
```

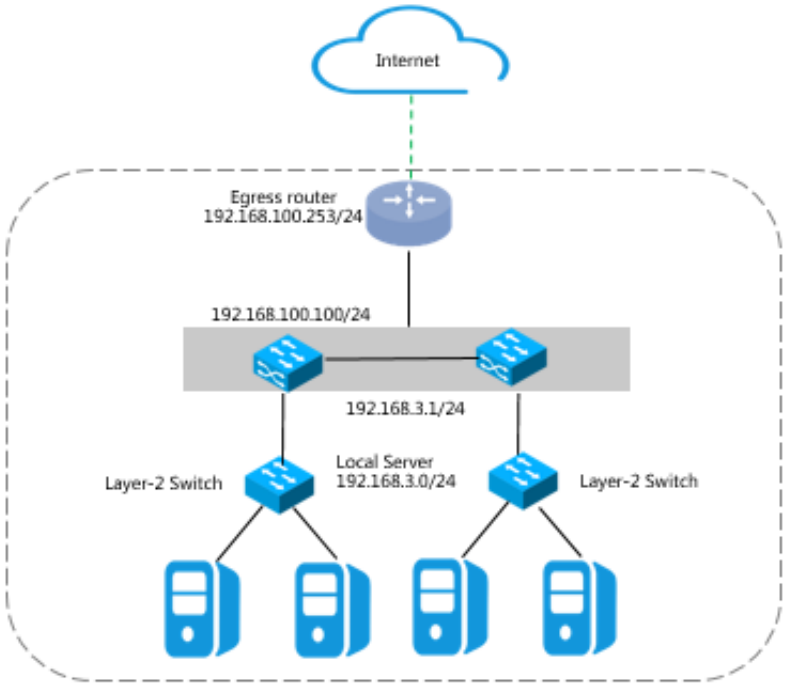
2 SAG-1000 dual-device one-arm mode configuration tutorial

2.1 Configuration overview

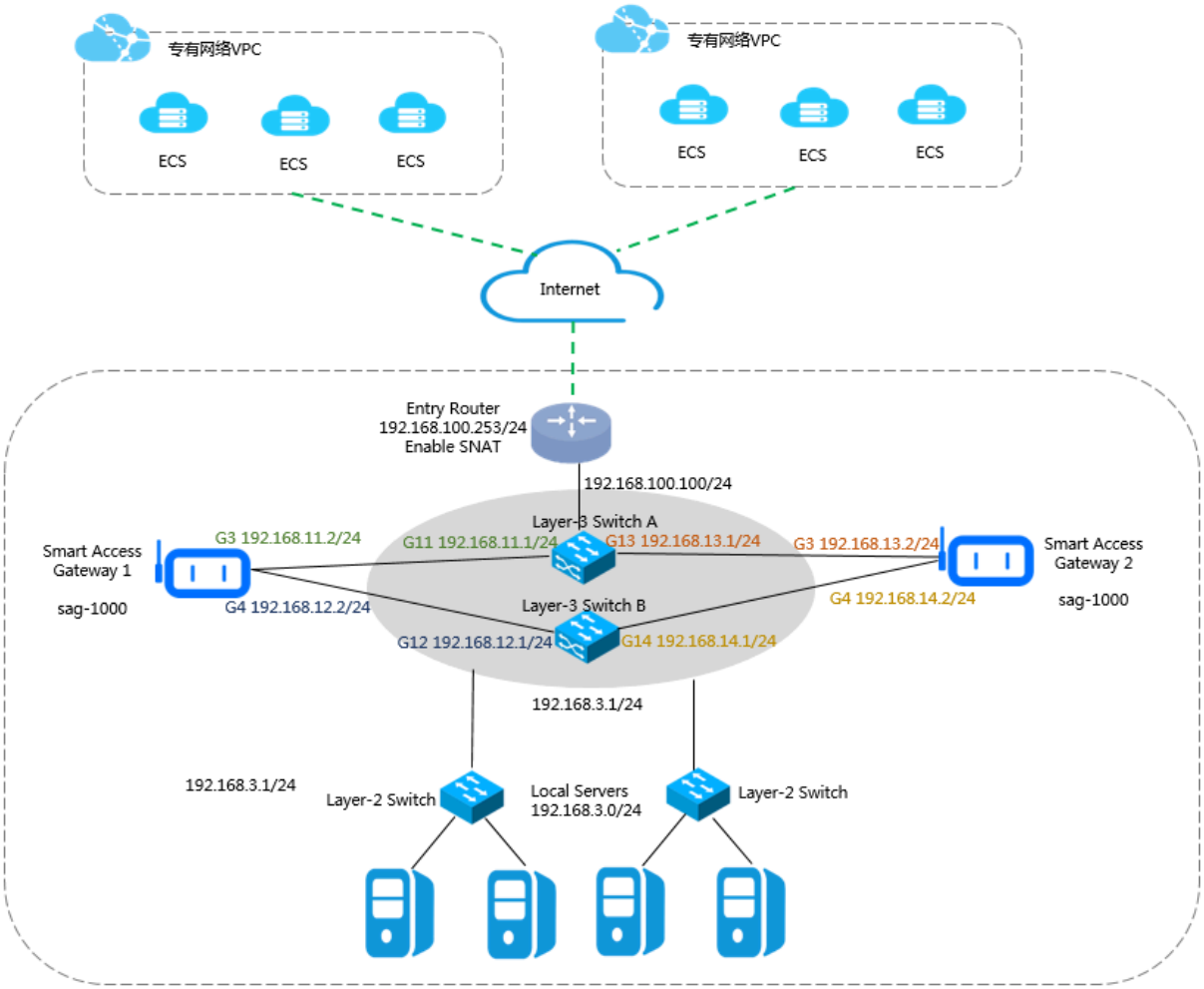
This tutorial guides you in how to connect your headquarters or branches to Alibaba Cloud through the SAG-1000 Smart Access Gateway.

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 the 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.
- IPs of local servers/clients

  Plan the IPs of the local servers/clients according to your needs. In this tutorial, the IP 192.168.3.0/24 is used.
- IPs used by the device to communicate with the Layer-3 switches

  Plan the IPs of the ports used by the Smart Access Gateway device to connect the Layer-3 switches. We recommend that you set the mask to /30. In this tutorial, the port IPs used by the device are 192.168.11.2/24 and 192.168.12.2/24.

- Service IP

  Plan the service IP of the Smart Access Gateway device. We recommend that you set the mask to /32. In this tutorial, the service port IP 192.168.101.2 is used.

- Administration port IP

  Plan the administration port IP of the Smart Access Gateway device. You can use an independent administrator port IP or use the service port IP as the administrator port IP. In this tutorial, 192.168.0.0/24 is used as the administration port IP.

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 Smart Access Gateway	192.168.3.1/24
Port IPs of Smart Access Gateway device 1	G3 192.168.11.2/24 G4 192.168.12.2/24
Port IPs of Smart Access Gateway device 2	G3 192.168.13.2/24 G4 192.168.14.2/24
Port IPs of the peer switches of the Smart Access Gateways	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

2.2 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 Hardware*.

   > 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.

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

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

Configure the SAG device

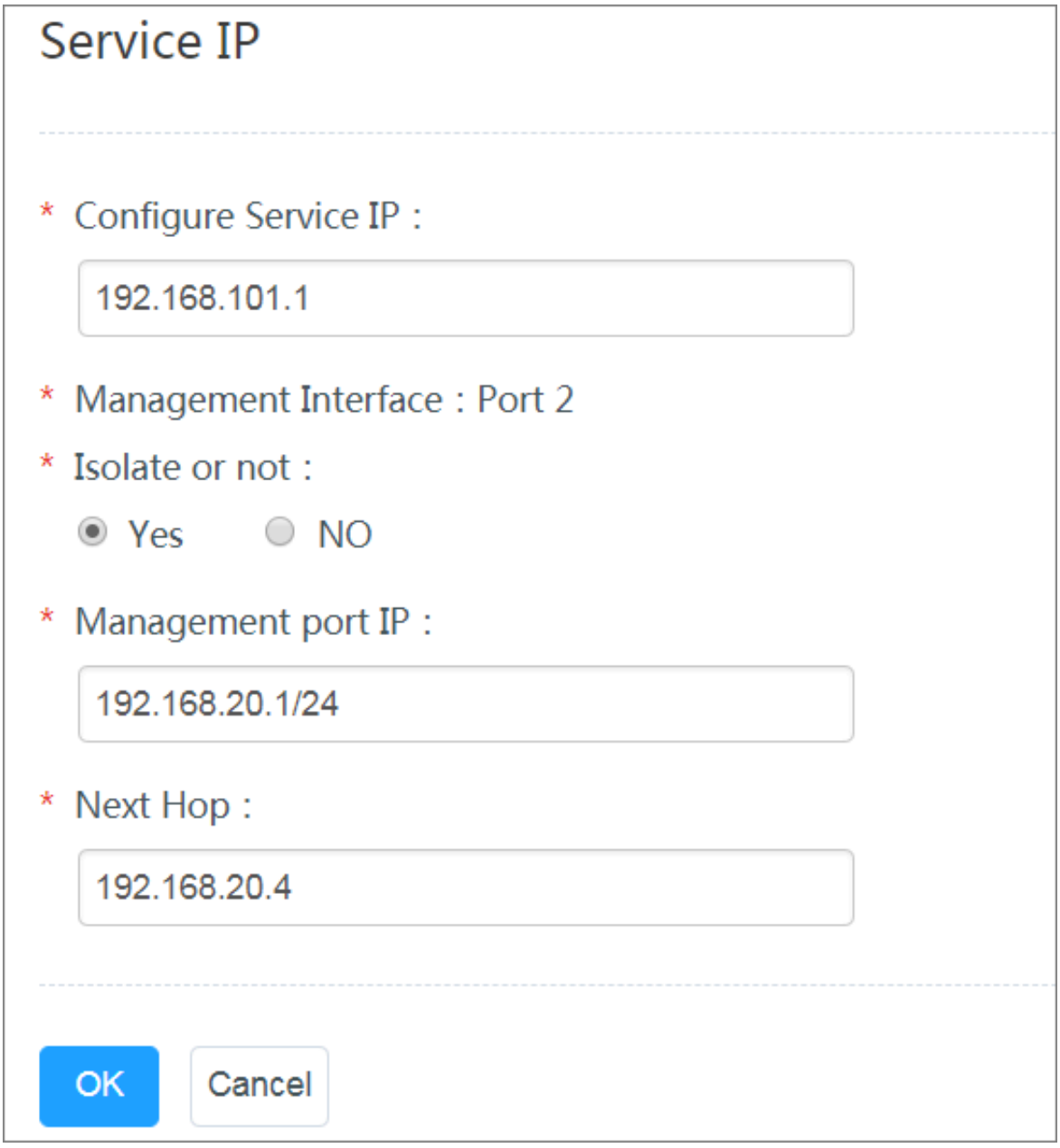
To configure device 1, follow these steps:

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 administration port.

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



Configuration	Description
Service IP	The service IP address is used to establish the VPN tunnel.
Administration port	The administration port is used for local web access. Port 2 is the administration port by default.
Administration IP	The administration IP address is used for the local client to access the Web console.

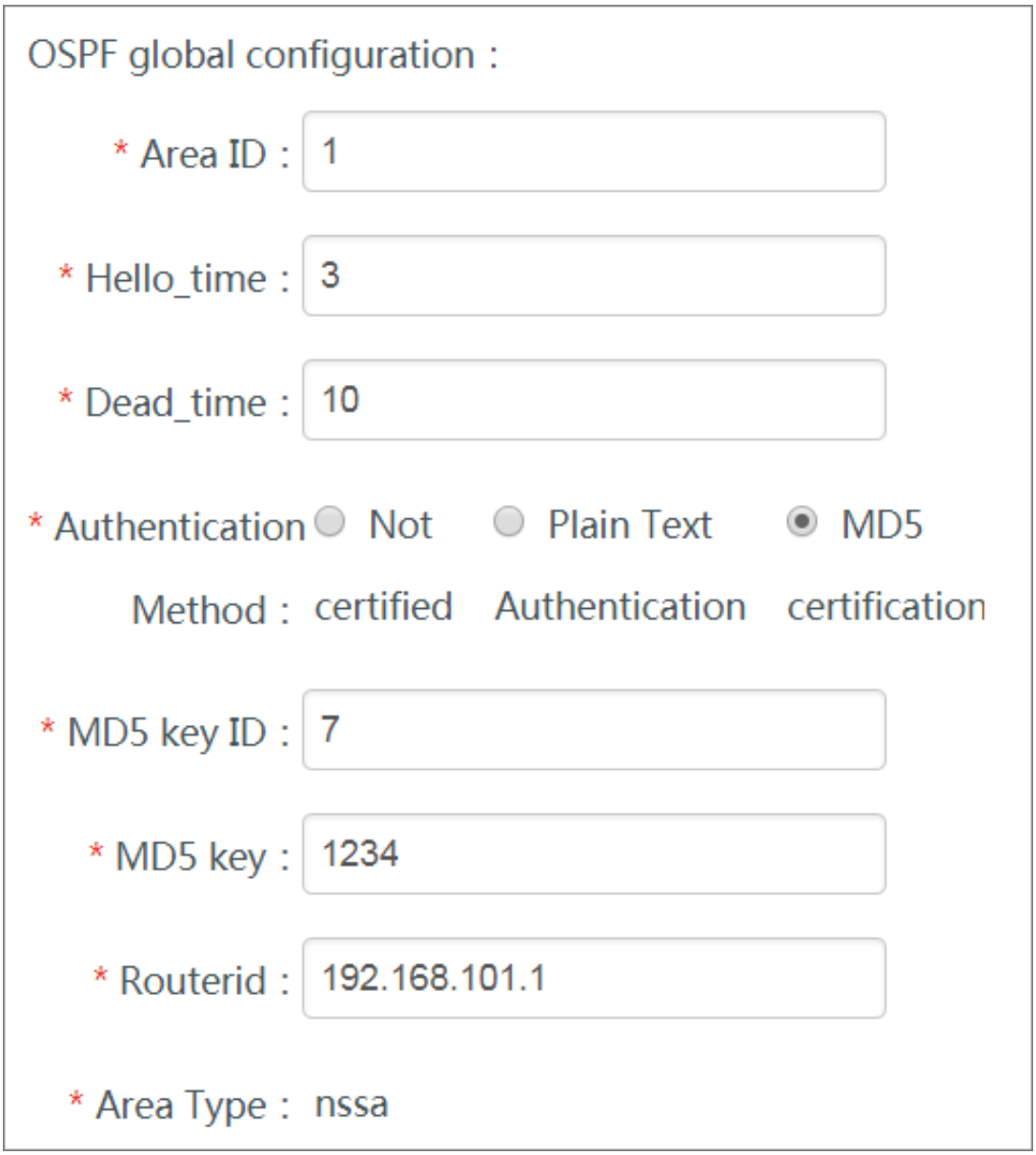
Configuration	Description
Whether to isolate	Select whether to isolate the service port from the administration port: · Yes: This port can only be used as a local web administration port and cannot be used as a service port. In the isolation mode, the service traffic and the administration traffic do not communicate with each other, thus achieving a higher level of security. · No: This port is used as both the local web administration port and the service port.
Next hop	If you choose to isolate the service port from the administration port, specify the next hop of the administration port.

6. Configure the ports used to communicate with the switches:
   - Connection Mode: Select static or dynamic routing. In this tutorial, select Dynamic Routing.
   - Port: Click the Edit option in the Configuration Information 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.

7. **Configure OSPF.**

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



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

Configuration	Description
Port	Click the Edit option in the Configuration Information area, enter the IP of the port used for communication and select whether to enable OSPF. Port 2 is the default administrator port.
OSPF routing configuration	
Area ID	The ID of the area. Make sure that area IDs of Smart Access Gateway 1 and Smart Access Gateway 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. · 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.
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 brands, see the device manual 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 GigabitEth ernet 0 / 11
```

```
 no   switchport
 ip   ospf   network   point - to - point
 ip   ospf   authentica  tion   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
Smart   Access   Gateway
interface   GigabitEth  ernet   0 / 12
 no   switchport
 ip   ospf   network   point - to - point
 ip   ospf   authentica  tion   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   Smart   Access   Gateway
```

- **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   2   nssa   translator   always   default - informatio  n -
originate
 area   1   nssa   translator   always   default - informatio  n -
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   communicat  ing
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  Smart  Access
Gateway
```

Configure the peer switches (Cisco)

Add route configurations for the peer switches of device 1 according to the following configurations. For switches of other brands, see the device manual 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  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  Smart  Access  Gateway
  ip  ospf  network  point - to - point
  ip  ospf  authentica  tion  message - digest
  ip  ospf  message - digest - key  7  md5  1234
  ip  ospf  dead - interval  10
  ip  ospf  hello - interval  3
!
 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  Smart  Access  Gateway
  ip  ospf  network  point - to - point
  ip  ospf  authentica  tion  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 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   2   nssa   default - informatio  n - originate   no -
 summary          Advertise   default   routes   to   the   Smart
 Access   Gateway
  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 . 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 . 12 . 0   0 . 0 . 0 . 255   area   1
  default - informatio  n   originate   always
!
```

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

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

Configure the SAG device

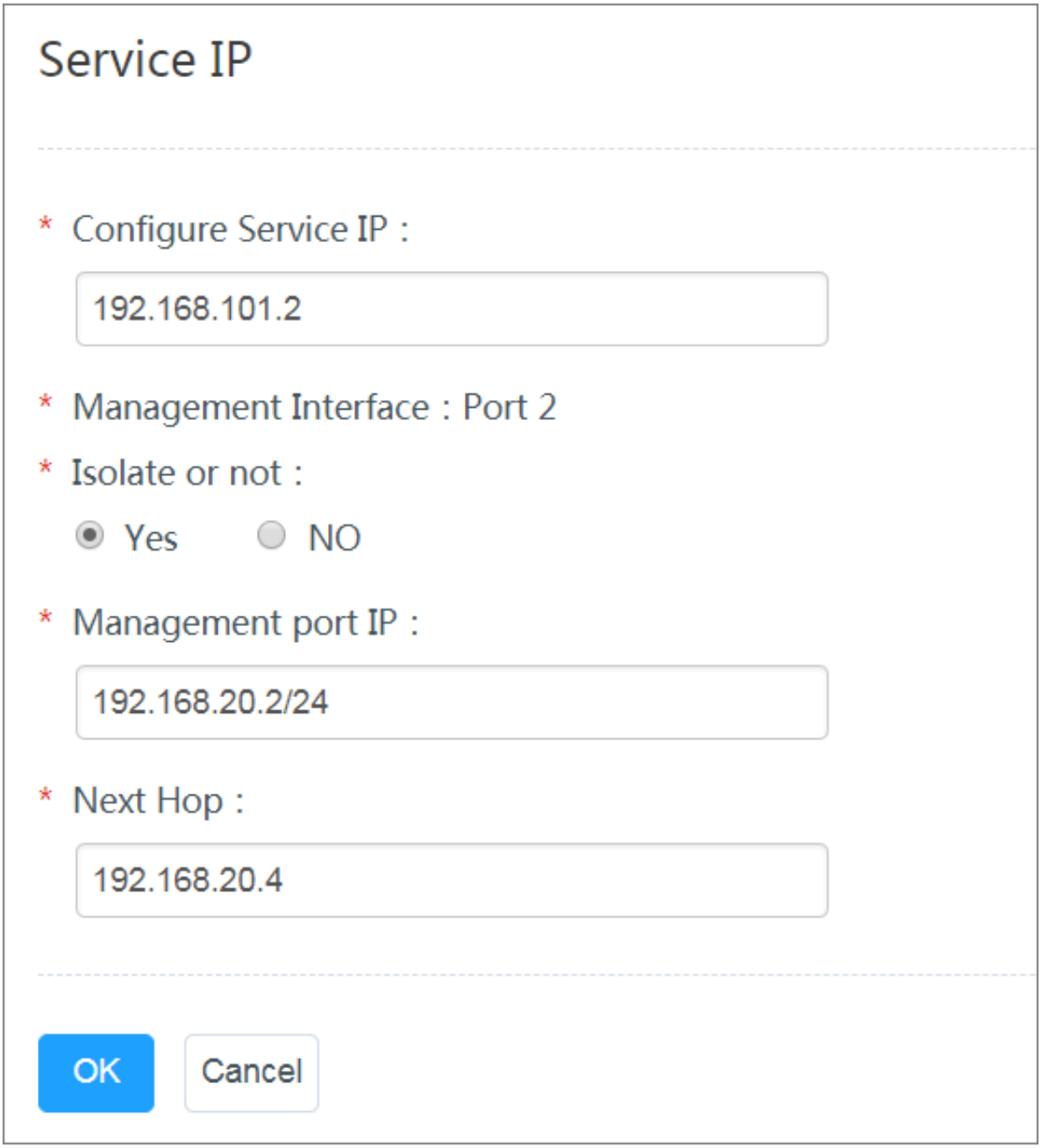
To configure device 2, follow these steps:

1. After receiving device 2, check that all accessories are provided and then power on the device. For more information about the SAG device, see *SAG-1000*.
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 administration port.

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



Configuration	Description
Service IP	The service IP address is used to establish the VPN tunnel.
Administration port	The administration port that the local client uses to access the Web console. Port 2 is the administration port by default.
Administration IP	The administration IP address that the local client uses to access the Web console.

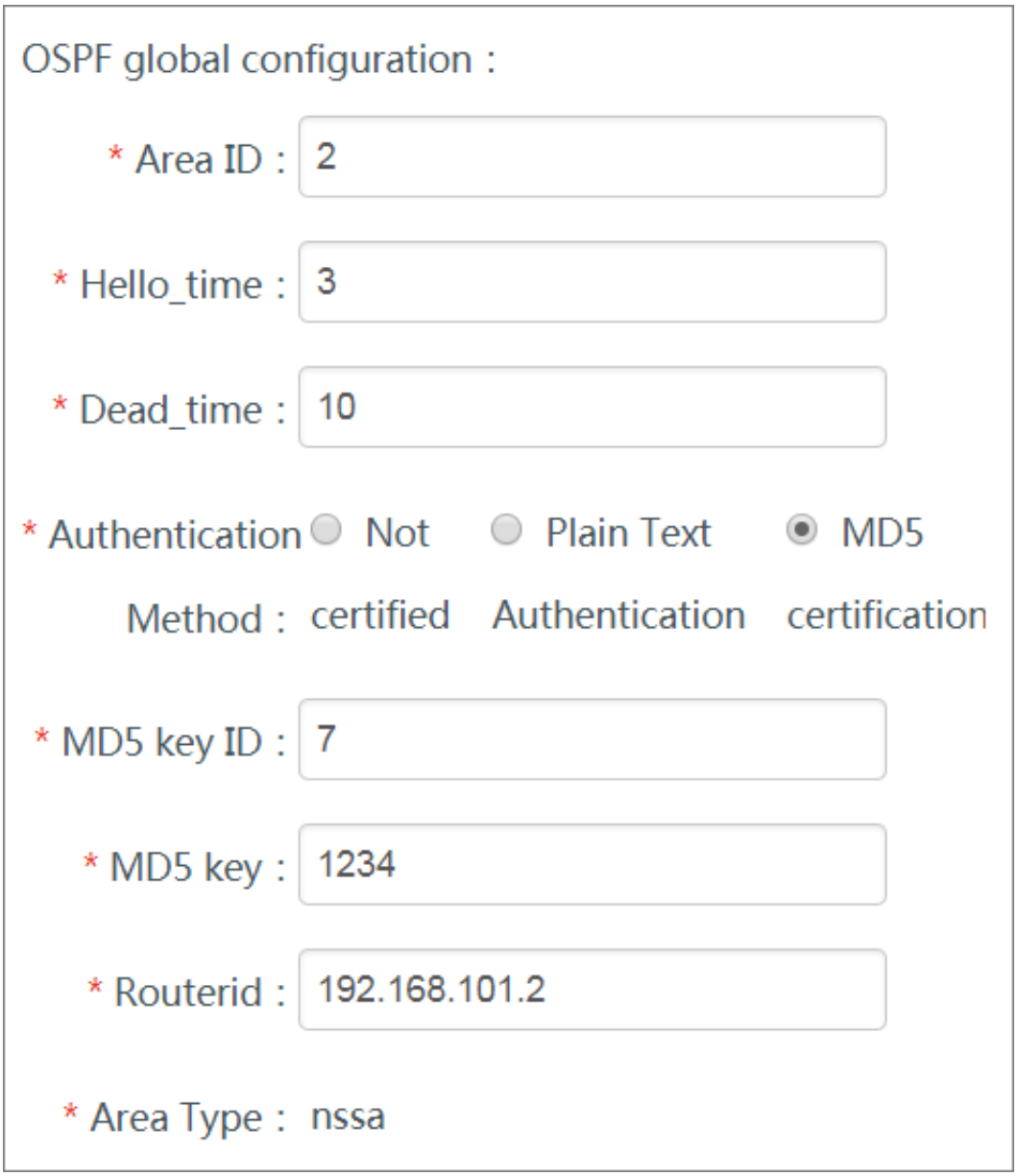
Configuration	Description
Whether to isolate	Select whether to isolate the service port from the administration port: · Yes: This port can only be used as a web administration port and cannot be used as a service port. In the isolation mode, the service traffic and the administration traffic do not affect each other, which achieves higher network security. · No: This port is used as both the web administration port and the service port.
Next hop	If you choose to isolate the service port from the administration port, you must specify the next hop of the administration port.

6. Configure the ports used to communicate with the switches:
   - Connection Mode: Select static or dynamic routes. In this tutorial, select Dynamic Routing.
   - Port: Click the Edit option in the Configuration Information 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 IP addresses of the ports used for communicating with the switches are 192.168.13.2/24 and 192.168.14.2/24.

7. **Configure OSPF.**

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



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

Configuration	Description
Port	Click the Edit option in the Configuration Information area, enter the IP of the port used for communication and select whether to enable OSPF. Port 2 is the default administrator port.
OSPF routing configuration	
Area ID	The ID of the area. Make sure that area IDs of Smart Access Gateway 1 and Smart Access Gateway 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. · 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.
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 brands, see the device manual 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 GigabitEth ernet 0 / 13
```

```
 no   switchport
 ip   ospf   network   point - to - point
 ip   ospf   authentica  tion   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   the   port   on   the   peer   switch   of
the   Smart   Access   Gateway   device
interface   GigabitEth  ernet   0 / 14
 no   switchport
 ip   ospf   network   point - to - point
 ip   ospf   authentica  tion   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   Smart   Access   Gateway   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 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 . 4
       The   router   ID   of   the   switch
 area   0
 area   1
 area   2
 area   2   nssa   translator   always   default - informatio  n -
originate
 area   1   nssa   translator   always   default - informatio  n -
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   communicat  ing
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   Smart   Access
Gateway   device
```

3 Tutorial for configuring Smart Access Gateway as the backup of a physical connection

3.1 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.

Scenario

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 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:

- Currently, only an SAG-1000 device can form active/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. Link switching due to health checks is not supported.

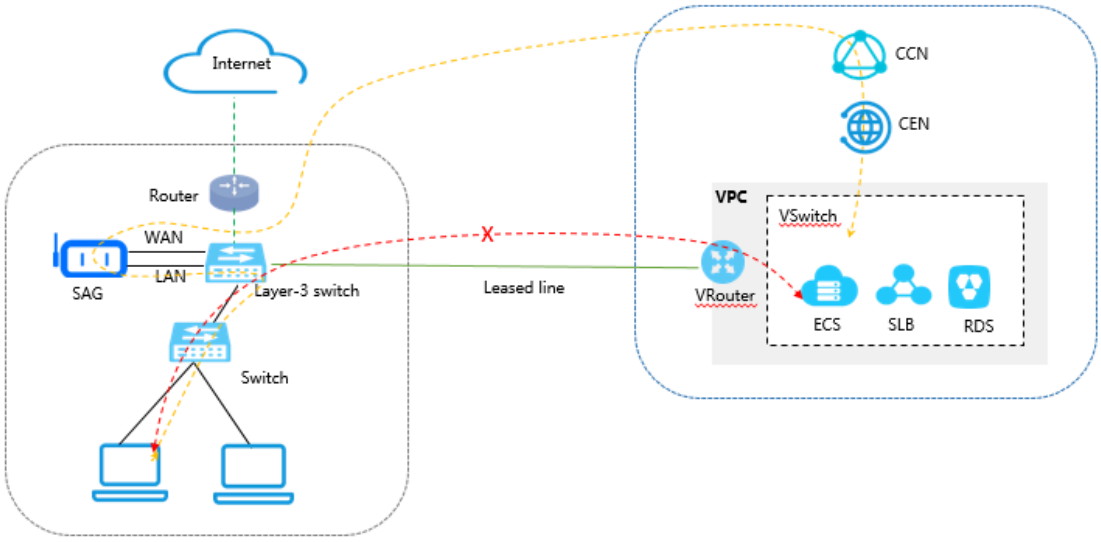
The flow direction of network traffic in this tutorial is as follows:

- 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 according to your needs. 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 172.16.0.254 to access Alibaba Cloud.

Table 3-1: 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 Smart Access Gateway	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

3.2 Step 1: Buy 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 *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.

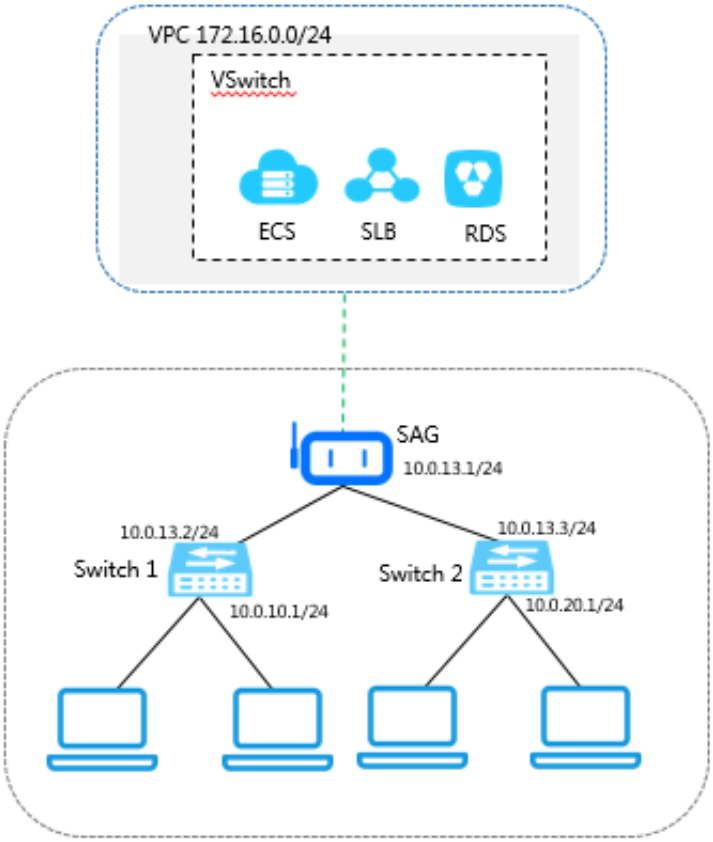
4 Tutorial for configuring local branches or headquarters with multiple CIDR blocks

4.1 Configuration overview

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

Scenarios

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.



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

  Plan the IP 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 device

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

  Plan the IP addresses used by each switch to communicate with the Smart Access Gateway and the IP addresses used by each switch to communicate with Alibaba Cloud.

Table 4-1: Example values in this tutorial

Configuration	Example value
The CIDR block of the VPC	172.25.0.0/24
The IP addresses of the ports on the Smart Access Gateway	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 Smart Access Gateway
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 Smart Access Gateway: 10.0.20.1/24

4.2 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 *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.

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

After receiving the gateway device, you need to configure its WAN and LAN ports and add related routing configurations to the switch.

Configure the Smart Access Gateway device

To configure the Smart Access Gateway device, follow these steps:

1. After receiving the gateway device, follow *SAG-100WM overview* to check if all accessories are provided and then power on the gateway device.
2. Connect the WAN port of Smart Access Gateway 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 Smart Access Gateway device.

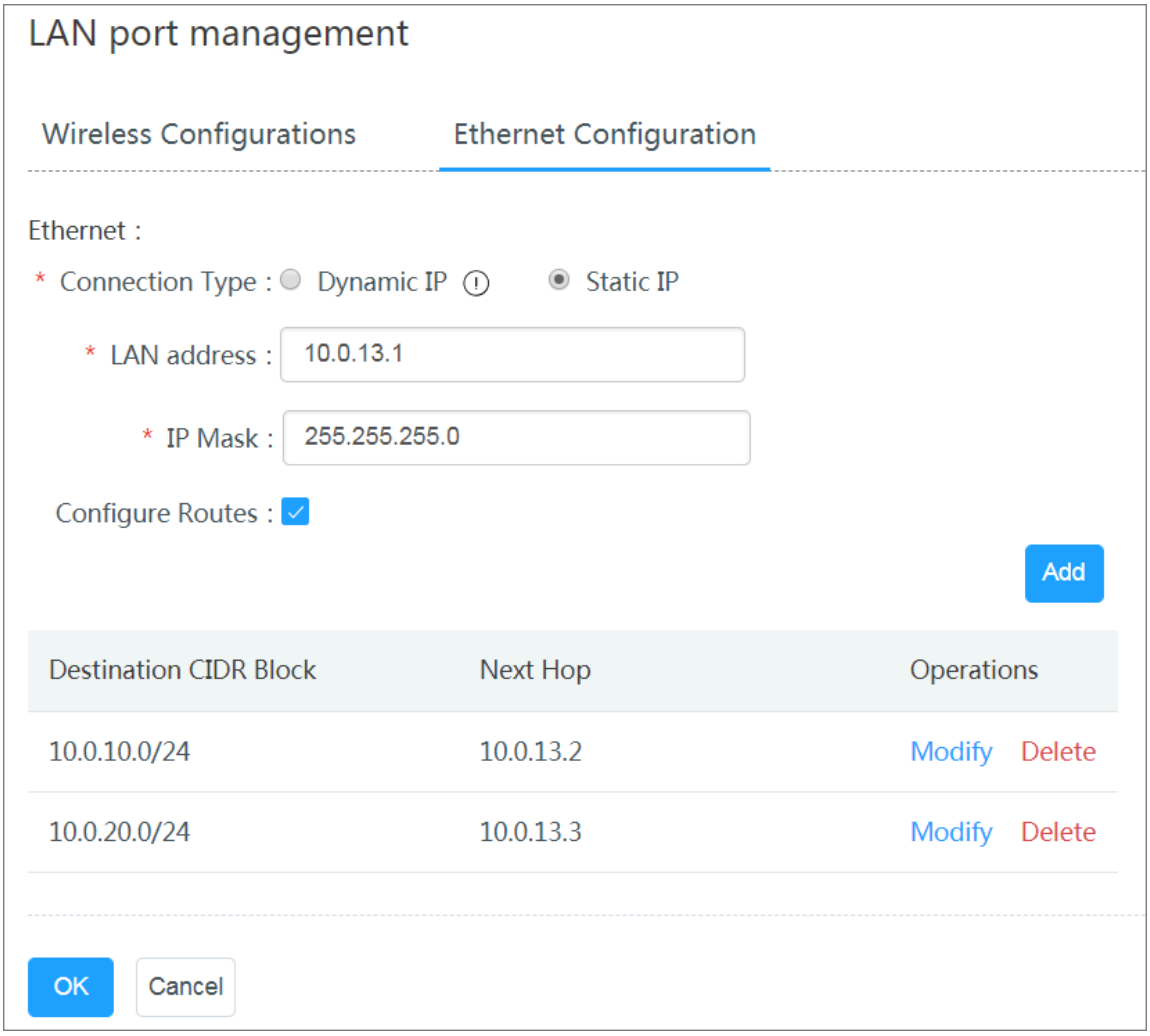
   The default address is https: // 192.168.0.1. For more information, see *Log on to the web configuration page*.

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.
   - Route Configuration: Click Route Configuration 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 gateway device.



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 gateway 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 Cross-region access to VPC

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

Scenarios

For access of local branches in the Mainland China area, you only need to attach the CCN associated with the Smart Access Gateway 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 tasks:

1. Purchase a Smart Access Gateway device.
2. Connect the gateway device.
3. Activate the gateway device.
4. Configure the network connection.
5. Configure the CEN.
6. Configure the security group.
7. Perform an access test.

Prerequisites

- You have created a CEN instance.
- You have created a VPC in the Hangzhou region and a VPC in the US (Silicon Valley) region, and have added the two VPCs to the same CEN instance.
  1. Log on to the *Smart Access Gateway console*.
  2. Select Quick Links > VPC.
  3. Select the China (Hangzhou) region and click the ID of the VPC 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.

- You have created a CCN instance. For more information, see *Create a CCN instance*.

Step 1: Buy a Smart Access Gateway device

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

To buy a Smart Access Gateway device, follow these steps:

1. 登录##########。
2. 单击创建智能接入网关。
3. Configure the Smart Access Gateway device and click Buy Now.

   For more information, see*Buy a Smart Access Gateway Hardware*.

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

4. 核对订单信息，然后单击去支付。
5. 在弹出的收货地址对话框，填写网关设备的收货地址，然后单击下单。

   您可以在智能接入网关实例页面查看是否下单成功。系统会在下单后两天内发货。如果超期，您可以提交工单查看物流状态。

Step 2: Connect the gateway device

After you receive the gateway device, check if all accessories are provided according to *Gateway device description*. After you start the gateway 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 the gateway devices, so you can use the default gateway configurations. If you need to configure the WAN port and LAN ports, see*Configure a Smart Access Gateway device*.

Step 3: Activate the gateway device

After receiving the gateway device, you must activate it.

To activate the gateway 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 Smart Access Gateway 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.

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, 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. Because each local branch uses the default gateway configuration, the IP address used by the local client to access Alibaba Cloud is allocated from the 172.16.0.0/12 CIDR block. For more information, see *Network configuration*.

      
      Note:
      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, select the default CCN instance. 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.

   In this tutorial, the CEN instance associated with the Hangzhou VPC and the US (Silicon Valley) VPC is selected.

   > Note:
   > Make sure that the CCN instance and the CEN instance are in the same area. For more information, see *CCN areas*.

6. Click OK.

Step 5: Configure the CEN

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

1. Log on to the *Smart Access Gateway console*.
2. In the left-hand navigation pane, select Quick connect > Cloud Enterprise Network.
3. On the CEN page, click the Networks tab page to view whether the Hangzhou VPC, the US (Silicon Valley) VPC and the CCN are attached to the CEN.

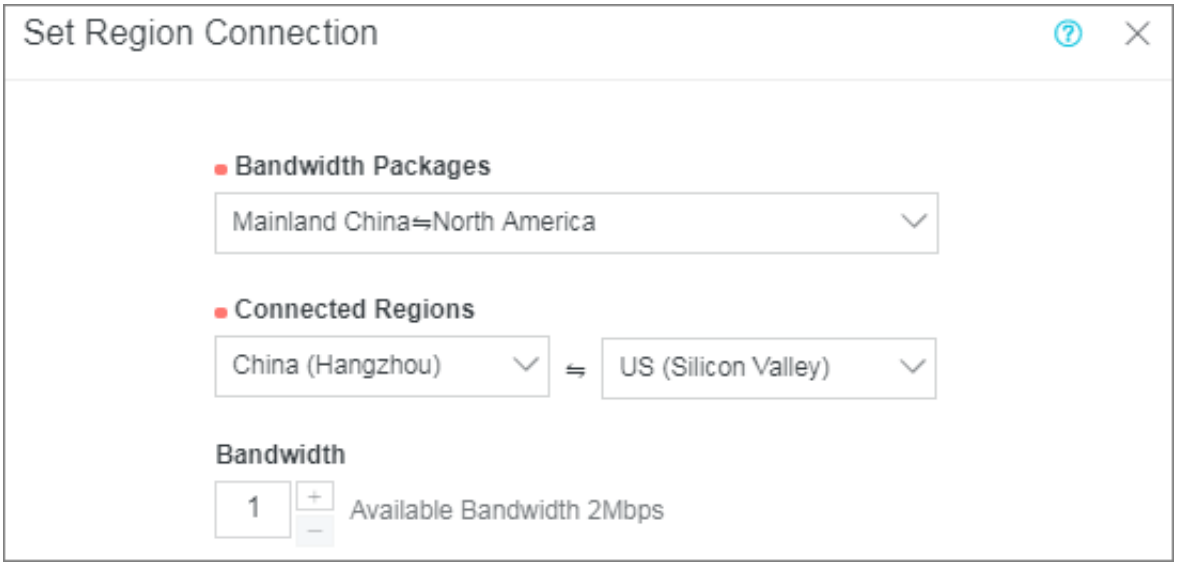
4. Click the Bandwidth Packages tab page and click Buy Bandwidth Package (Pay-As-You-Go) to buy a Pay-As-You-Go Bandwidth package.
5. On the CEN (Pay-As-You-Go page, configure the bandwidth package.
   - Cloud Enterprise Network: Select the CEN associated with the VPCs and the CCN.
   - Area A and Area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

     Here, Mainland China and North America are selected.
   - Bandwidth: Select the bandwidth of the region connection according to your needs.
   - Bandwidth Package Name: Enter the name of the bandwidth package.

6. Click Buy Now to buy 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 package: Select the bandwidth package that is used by the CEN instance. Here, select Mainland China ⇋ North American.
   - Connected Regions: Select the regions to be connected with each other. Here, select China (Hangzhou) and US (Silicon Valley).
   - Bandwidth: Enter the bandwidth according to your needs.

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



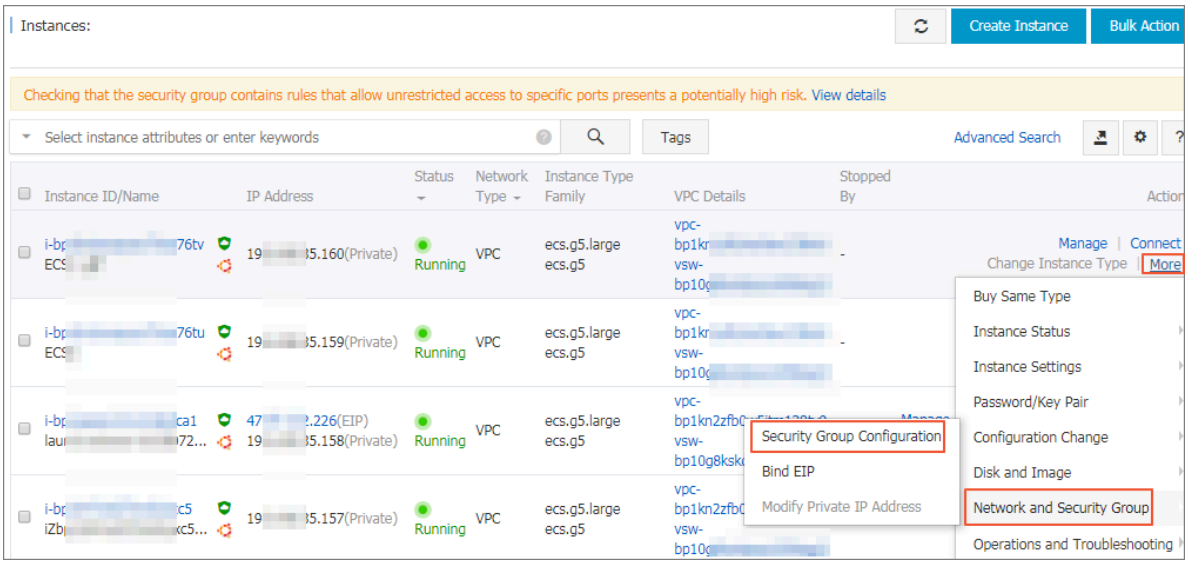
Step 6: Configure a security group

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

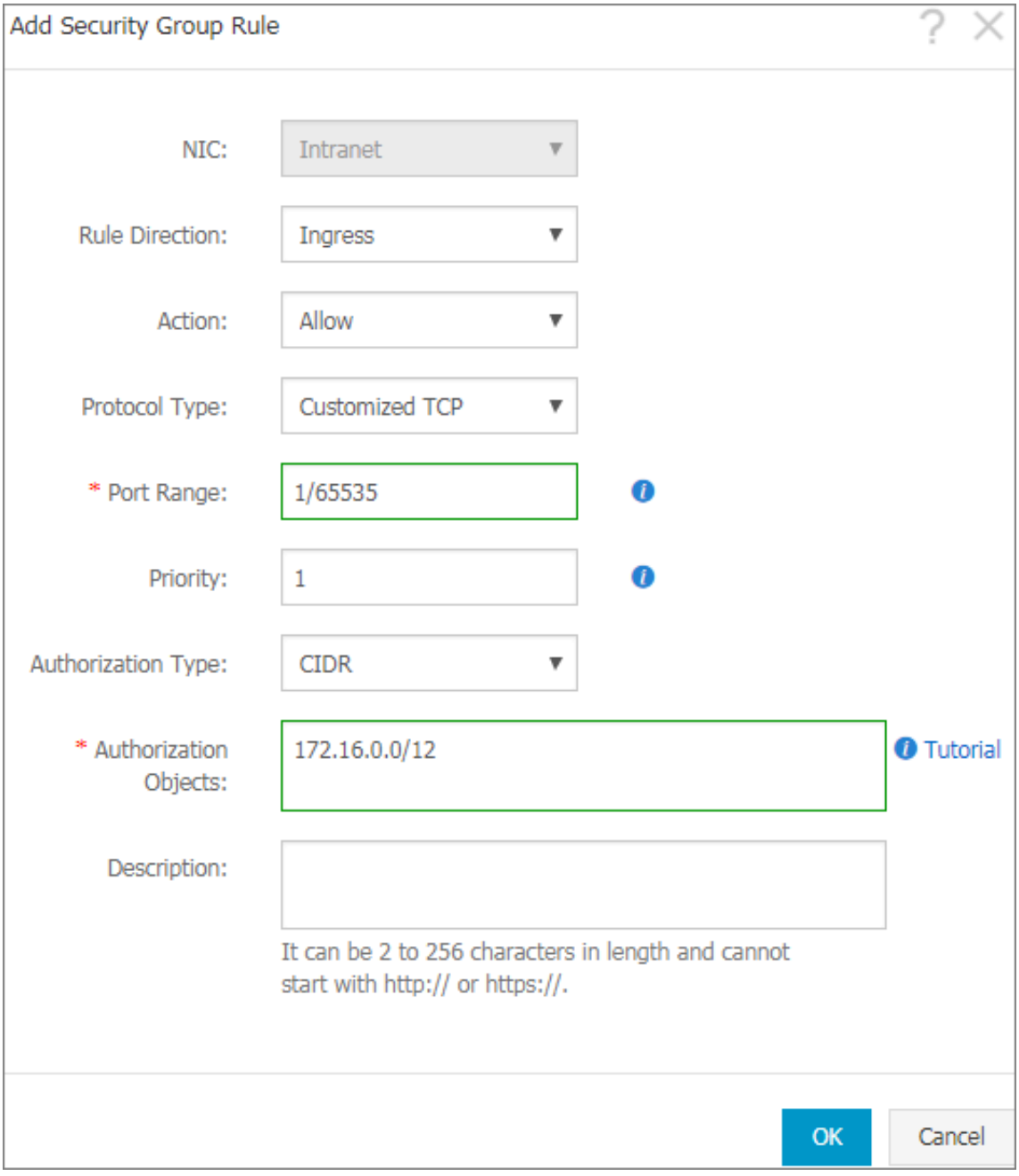
3. Locate the ECS instance in the target VPC, and then click More > Network and Security Group > Configure Security Group.



4. Click Add Rules and then 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.



Step 7: Test the access

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