

INTELBRAS Access Controllers

HTTPS Login Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring HTTPS login	1
Network requirements	1
Configuration restrictions and guidelines.....	1
Configuration procedures	2
Configuring the AC.....	2
Configuring the switch	4
Verifying the configuration	5
Configuration files.....	5
Related documentation	7

Introduction

The following information provides an HTTPS login configuration example.

Prerequisites

This document applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of WLAN access and HTTPS login.

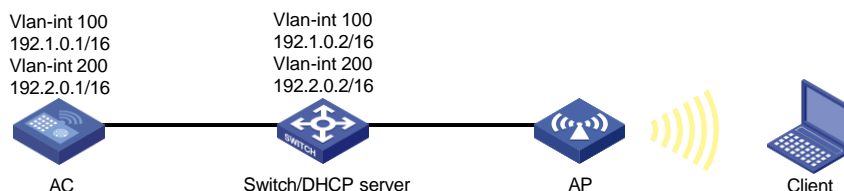
Example: Configuring HTTPS login

Network requirements

As shown in [Figure 1](#), configure the switch and the AC to achieve the following goals:

- The AC allows only authorized users to access the Web interface by using HTTPS.
- The switch acts as the DHCP server to assign IP addresses to the AP and client.
- The AP and AC use VLAN 100 to establish a CAPWAP tunnel.
- The client uses VLAN 200 to access the wireless network.

Figure 1 Network diagram



Configuration restrictions and guidelines

When you configure HTTPS login, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- In this example, the CA certificate and local certificate for the AC are transferred in advance to the AC in offline mode. Make sure the certificates have not expired.
- Only a certificate file in the PKCS#12 or PEM format might contain key pairs.

Configuration procedures

Configuring the AC

1. Configure interfaces of the AC:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AC will use this IP address to establish CAPWAP tunnels with APs.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.1.0.1 16
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. The AC will use VLAN 200 for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.2.0.1 16
[AC-Vlan-interface200] quit
```

Configure the interface that is connected to the switch as a trunk port, and assign the port to VLAN 100 and VLAN 200.

```
[AC] interface gigabitEthernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure the wireless service:

Create wireless service template 1 and enter its view.

```
[AC] wlan service-template 1
```

Set the SSID to **service**.

```
[AC-wlan-st-1] ssid service
```

Assign clients coming online through service template 1 to VLAN 200.

```
[AC-wlan-st-1] vlan 200
```

Specify the AKM mode as PSK, and configure the preshared key as 12345678 in plain text.

```
[AC-wlan-st-1] akm mode psk
```

```
[AC-wlan-st-1] preshared-key pass-phrase simple 12345678
```

Specify the cipher suite as CCMP and the security IE as RSN.

```
[AC-wlan-st-1] cipher-suite ccmp
```

```
[AC-wlan-st-1] security-ie rsn
```

Configure the AC to forward client data traffic. (Skip this step if the client data traffic forwarder is the AC by default.)

```
[AC-wlan-st-1] client forwarding-location ac
```

Enable service template 1.

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

3. Configure the AP:

NOTE:

In large-scale networks, configure AP groups instead of single APs as a best practice.

Create AP `ap1`. Set the model and serial ID.

```
[AC] wlan ap ap1 model AP 3620
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-ap1] quit
```

Create AP group `group1` and add AP 1 to AP group `group1`.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap ap1
```

Bind service template 1 to radio 1 in AP group `group1`.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template 1
```

Enable radio 1.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1]radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1]quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]quit
[AC-wlan-ap-group-group1]quit
```

4. Configure HTTPS login:**# Create PKI domain 1 and disable CRL checking. (If CRL checking is required, enable CRL checking.)**

```
[AC] pki domain 1
[AC-pki-domain-1] undo crl check enable
[AC-pki-domain-1] quit
```

Import CA certificate file `root.pem` in PEM format to PKI domain 1.

```
[AC] pki import domain 1 pem ca filename root.pem
Please input the password:****
```

Import local certificate file `radius.pem` in PEM format to PKI domain 1.

```
[AC] pki import domain 1 pem local filename radius.pem
Please input the password:****
```

Create SSL server policy `myssl` and specify PKI domain 1 for the policy.

```
[AC] ssl server-policy myssl
[AC-ssl-server-policy-myssl] pki-domain 1
[AC-ssl-server-policy-myssl] quit
```

Apply SSL server policy `myssl` to the HTTPS service.

```
[AC] ip https ssl-server-policy myssl
```

Enable the HTTPS service.

```
[AC] ip https enable
```

Add device management user `usera` and set the password. Assign the HTTPS service type and network-admin user role to the user.

```
[AC] local-user usera
[AC-luser-manage-usera] password simple 123
[AC-luser-manage-usera] service-type https
[AC-luser-manage-usera] authorization-attribute user-role network-admin
[AC-luser-manage-usera] quit
```

Configuring the switch

1. Configure interfaces of the switch:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The switch will use VLAN 100 to forward AC traffic.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.1.0.2 16
[Switch-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. The switch will use VLAN 200 to forward client traffic.

```
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.2.0.2 16
[Switch-Vlan-interface200] quit
```

Configure the interface that is connected to the AC as a trunk port, and assign the port to VLAN 100 and VLAN 200.

```
[Switch] interface gigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

Configure the interface that is connected to the AP as a trunk port, set its PVID to VLAN 100, and assign it to VLAN 100.

```
[Switch] interface gigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100
```

Enable PoE on the interface that is connected to the AP.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

2. Configure the DHCP server:

Enable the DHCP service.

```
[Switch] dhcp enable
```

Create DHCP address pool 100. Specify the 192.1.0.0/16 subnet and the 192.1.0.2 gateway for the pool.

```
[Switch] dhcp server ip-pool 100
[Switch-dhcp-pool-100] network 192.1.0.0 16
[Switch-dhcp-pool-100] gateway-list 192.1.0.2
```

Use option 43 to assign the IP address of the AC to the AP. (The last four bytes of the hexadecimal option content are c0010001, which represents 192.1.0.1.)

```
[Switch-dhcp-pool-100] option 43 hex 8007000001c0010001
[Switch-dhcp-pool-100] quit
```

Create DHCP address pool 200. Specify subnet 192.2.0.0/16, gateway 192.2.0.2, and DNS server 192.2.0.2 for the pool. In this example, the DNS server and gateway is assumed by the same device.

```
[Switch] dhcp server ip-pool 200
```

```
[Switch-dhcp-pool-200] network 192.2.0.0 16
[Switch-dhcp-pool-200] gateway-list 192.2.0.2
[Switch-dhcp-pool-200] dns-list 192.2.0.2
[Switch-dhcp-pool-200] quit
```

Verifying the configuration

On the client, launch the Web browser and enter **https://192.2.0.1** in the address bar. (Details not shown.)

When the Web login page appears, enter username **usera** and password **123** to log in to the Web interface of the AC. (Details not shown.)

Configuration files

- AC:


```
#
vlan 100
#
vlan 200
#
wlan service-template 1
    ssid service
    vlan 200
    client forwarding-location ac
    akm mode psk
    preshared-key pass-phrase cipher $c$3$UNilHD1Uals7hLtpCnoR3C+FKI5auwq0rO7/
    cipher-suite ccmp
    security-ie rsn
    service-template enable
#
interface Vlan-interface100
    ip address 192.1.0.1 255.255.0.0
#
interface Vlan-interface200
    ip address 192.2.0.1 255.255.0.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 200
#
local-user usera class manage
    password hash
    $h$6$FOrfdnZ2QRORxu7o$OK/dcQ/N/S7m+zrhpyh+xDm2aerS7vvN8WwFVuhQuk8hdeFjDtqzPJthCen
    1ylElTkE7OqbCG5YhiRnjHtEr0g==
    service-type https
    authorization-attribute user-role network-admin
#
pki domain 1
```

```

undo cri check enable
#
ssl server-policy myssl
  pki-domain 1
#
  ip https ssl-server-policy myssl
  ip https enable
#
wlan ap-group group1
  ap ap1
  ap-model AP 3620
    radio 1
      radio enable
      service-template 1
    radio 2
#
wlan ap ap1 model AP 3620
  serial-id 219801A28N819CE0002T
  vlan 1
  radio 1
#

```

- **Switch:**

```

#
  dhcp enable
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
  ip address 192.1.0.2 255.255.0.0
#
interface Vlan-interface200
  ip address 192.2.0.2 255.255.0.0
#
dhcp server ip-pool 100
  gateway-list 192.1.0.2
  network 192.1.0.0 mask 255.255.0.0
  option 43 hex 8007000001C0010001
#
dhcp server ip-pool 200
  gateway-list 192.2.0.2
  network 192.2.0.0 mask 255.255.0.0
  dns-list 192.2.1.2
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200

```



```
#
interface GigabitEthernet1/0/2
poe enable
port link-type trunk
    port trunk permit vlan 100
    port trunk pvid vlan 100
#
```

Related documentation

- *Fundamentals Command Reference in INTELBRAS Access Controllers Command References*
- *Fundamentals Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Security Command Reference in INTELBRAS Access Controllers Command References*
- *Security Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*
- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers SSH Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring the AC as an Stelnet server (password authentication)1	
Network configuration	1
Procedures	1
Verifying the configuration	3
Example: Configuring the AC as an Stelnet server (publickey authentication)3	
Network configuration	3
Analysis	4
Procedures	4
Verifying the configuration	7
Example: Configuring the AC as an Stelnet client (password authentication) 9	
Network configuration	9
Procedures	10
Verifying the configuration	11
Example: Configuring the AC as an Stelnet client (publickey authentication)13	
Network configuration	13
Analysis	13
Procedures	13
Verifying the configuration	15
Example: Configuring the AC as an SFTP server (password authentication)15	
Network configuration	15
Procedures	16
Verifying the configuration	17
Example: Configuring the AC as an SFTP client (publickey authentication)· 18	
Network configuration	18
Analysis	18
Procedures	18
Verifying the configuration	20
Example: Configuring SCP with password authentication	21
Network configuration	21
Procedures	21
Verifying the configuration	23
Example: Configuring NETCONF over SSH with password authentication ··	23
Network configuration	23
Procedures	23
Verifying the configuration	25
Related documentation	26

Introduction

The following information provides SSH configuration examples.

Prerequisites

This document applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of WLAN and SSH.

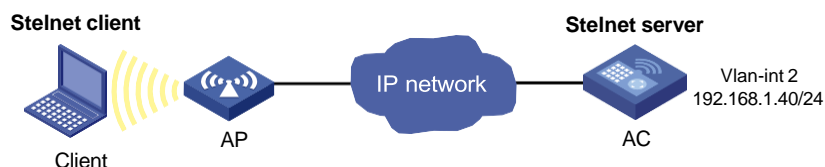
Example: Configuring the AC as an Stelnet server (password authentication)

Network configuration

As shown in [Figure 1](#):

- The route between the wireless client and the AC is reachable.
- The AC acts as the Stelnet server and uses password authentication to authenticate the Stelnet client. The username and password of the Stelnet client are saved on the AC.
- The wireless client acts as the Stelnet client, using Stelnet client software (SSH2). After the user on the wireless client logs in to the AC through Stelnet, the user can configure and manage the AC as a network administrator.

Figure 1 Network diagram



Procedures

Generate RSA key pairs.

```
<AC> system-view
```

```
[AC] public-key local create rsa
```

The range of public key size is (512 ~ 2048).

If the key modulus is greater than 512, it will take a few minutes.

Press CTRL+C to abort.

```
Input the modulus length [default = 1024]:
```

```
Generating Keys...
```

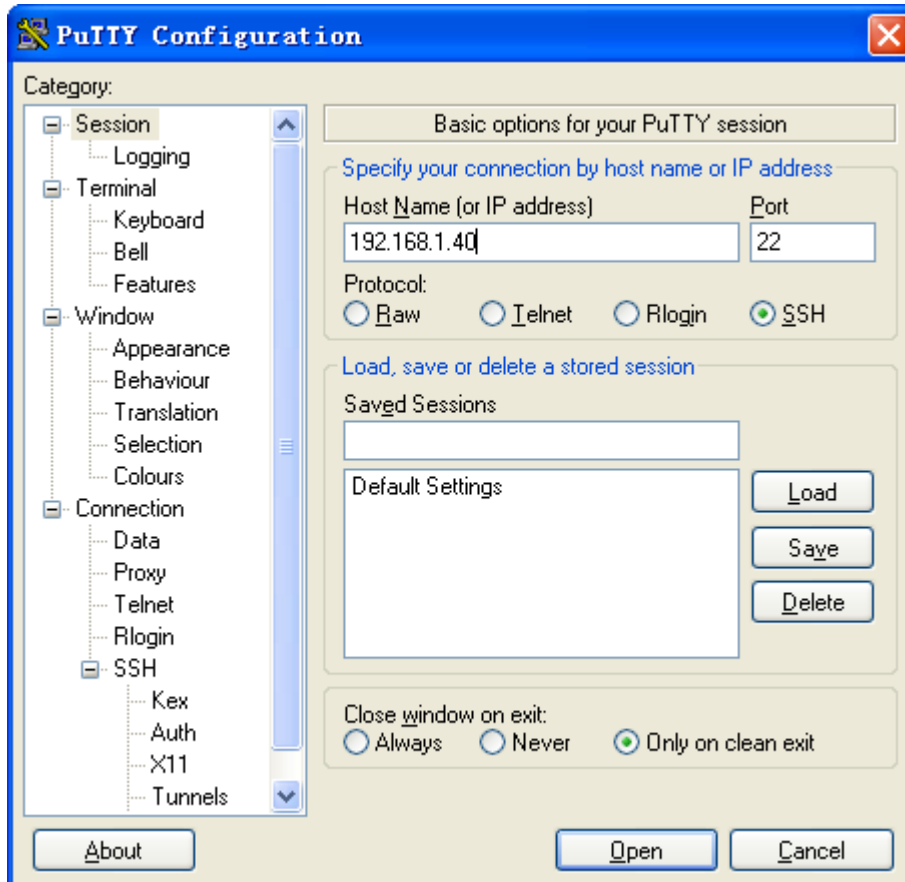

Verifying the configuration

There are different types of Stelnet client software, such as PuTTY and OpenSSH. This example uses an Stelnet client that runs PuTTY version 0.58 to verify the configuration.

To verify that you can log in to the Stelnet server from the Stelnet client:

1. Launch PuTTY.exe to enter the page shown in [Figure 2](#).
2. In the **Host Name (or IP address)** field, enter IP address **192.168.1.40** of the Stelnet server.
3. Click **Open**.

Figure 2 Connecting to the Stelnet server



4. Enter username **client001** and password **aabbcc** to log in to the Stelnet server.

Example: Configuring the AC as an Stelnet server (publickey authentication)

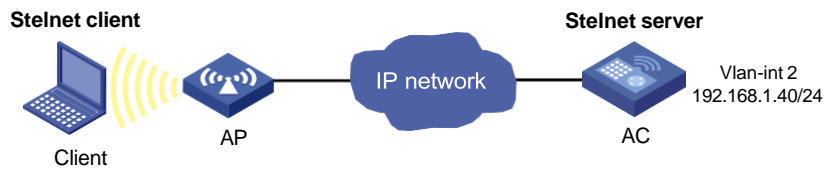
Network configuration

As shown in [Figure 3](#):

- The route between the wireless client and the AC is reachable.
- The AC acts as the Stelnet server, and it uses publickey authentication and the RSA public key algorithm.

- The wireless client acts as the Stelnet client, using Stelnet client software (SSH2). After the user on the wireless client logs in to the AC through Stelnet, the user can configure and manage the AC as a network administrator.

Figure 3 Network diagram



Analysis

Because the client's host public key is required in the server configuration, you must generate RSA key pairs on the client before configuring the Stelnet server.

Procedures

There are different types of Stelnet client software, such as PuTTY and OpenSSH. This example uses an Stelnet client that runs PuTTY version 0.58.

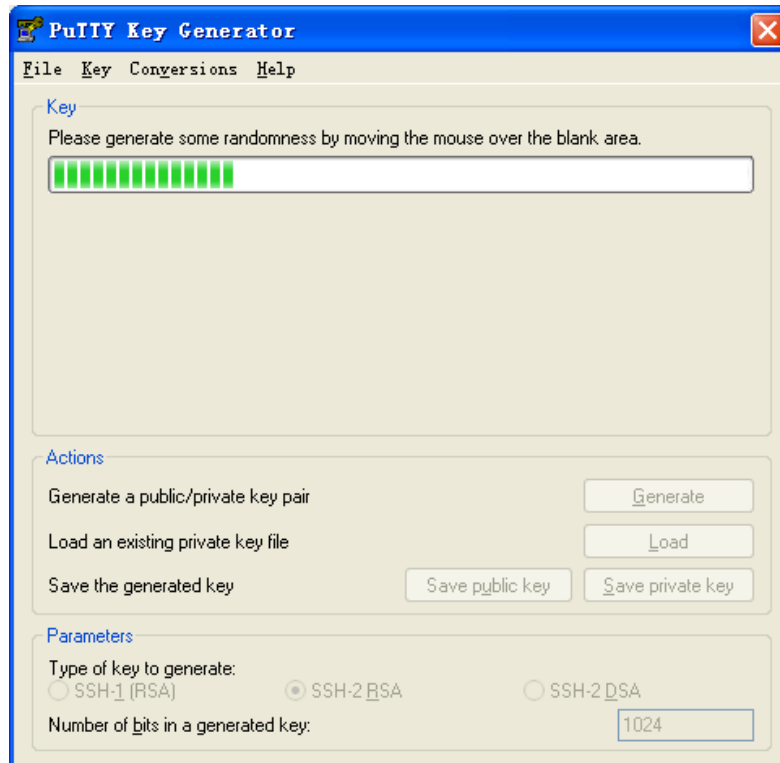
1. Generate RSA key pairs on the Stelnet client:
 - a. Run PuTTYGen.exe on the client, select **SSH-2 RSA**, and then click **Generate**.

Figure 4 Generating a key pair on the client



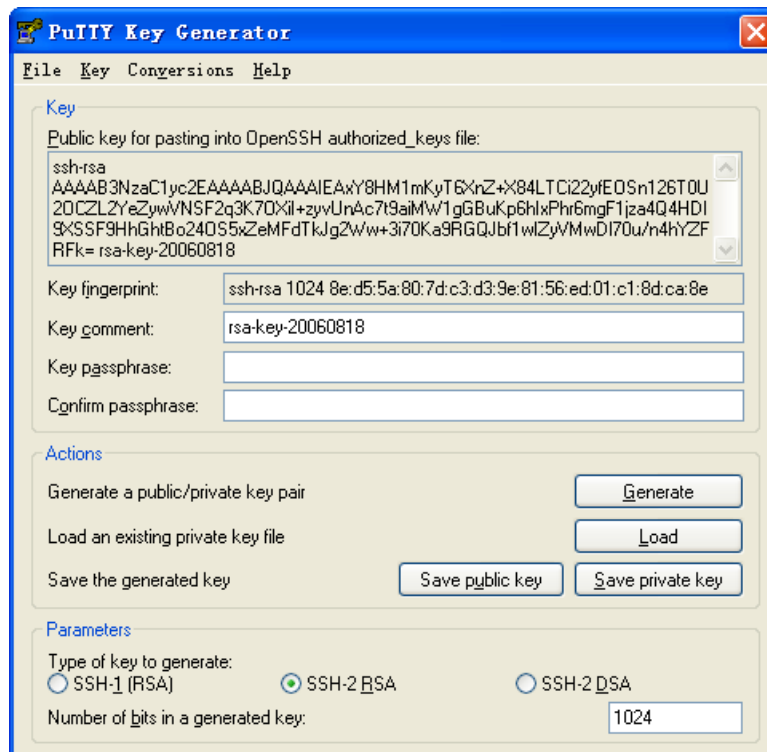
- b. Continue moving the mouse during the key generating process, but do not place the mouse over the green progress bar shown in Figure 5. Otherwise, the progress bar stops moving and the key pair generating progress stops.

Figure 5 Generating process

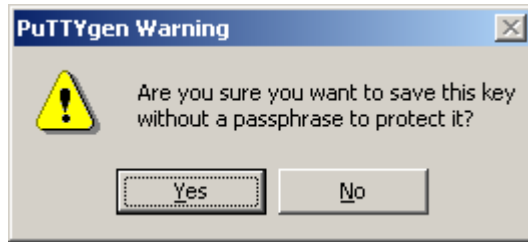


- c. After the key pair is generated, click **Save public key** to save the public key, as shown in [Figure 6](#).
A file saving page opens.

Figure 6 Saving a key pair on the client



- d. Enter a file name (**key.pub** in this example), and then click **Save**.
- e. On the page as shown in [Figure 6](#), click **Save private key** to save the private key. A confirmation dialog box opens, as shown in [Figure 7](#).



- ## 2. Configure the Stelnet server:

```
<AC> system-view
```

The range of public key size is (512 ~ 2048).

Press CTRL+C to abort.

Generating Keys...

. ++++++

. ++++++

```
# Generate a DSA key pair.
```

The range of public key size is (512 ~ 2048).

Press CTRL+C to abort.

Generating Keys...

Create the key pair successfully.

```
[AC] public-key local create ecdsa secp256r1
```

•

Create the key pair successfully.

```

[AC] ssh server enable

# Assign an IP address to VLAN-interface 2. The Stelnet client uses this IP address as the
destination for SSH connection.
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[AC-Vlan-interface2] quit

# Set the authentication mode to AAA for user lines.
[AC] line vty 0 63
[AC-line-vty0-63] authentication-mode scheme
[AC-line-vty0-63] quit

# Import the client's public key from the public key file key.pub and name it ackey.
[AC] public-key peer ackey import sshkey key.pub

# Create an SSH user named client002. Specify the authentication method as publickey for
the user, and assign the public key ackey to the user.
[AC] ssh user client002 service-type stelnet authentication-type publickey assign
publickey ackey

# Create a local device management user named client002.
[AC] local-user client002 class manage

# Authorize local user client002 to use the SSH service.
[AC-luser-manage-client002] service-type ssh

# Assign the network-admin user role to local user client002.
[AC-luser-manage-client002] authorization-attribute user-role network-admin
[AC-luser-manage-client002] quit

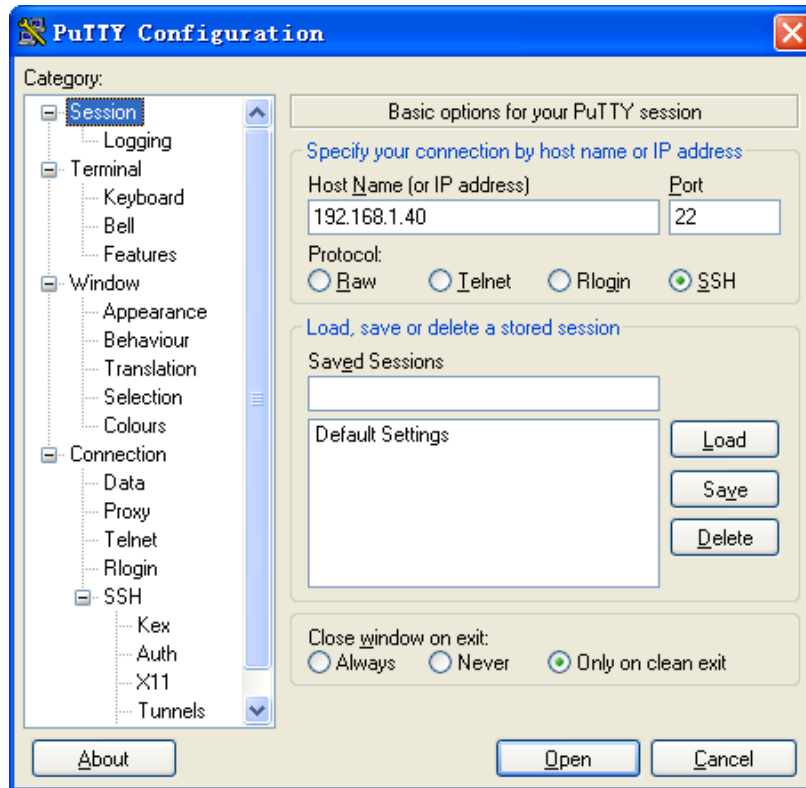
```

Verifying the configuration

To verify that you can log in to the Stelnet server from the Stelnet client:

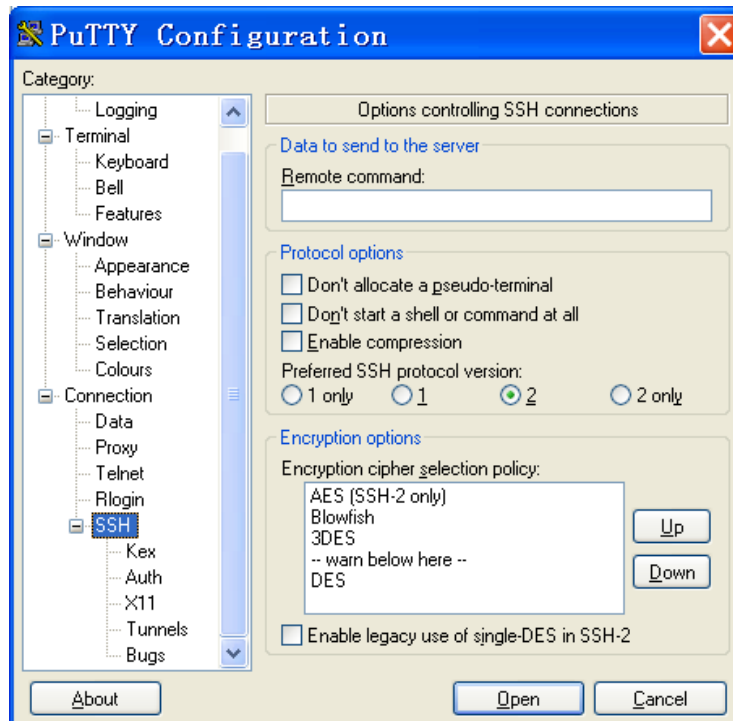
1. Launch PuTTY.exe on the Stelnet client to enter the page shown in [Figure 8](#).
2. In the **Host Name (or IP address)** field, enter IP address **192.168.1.40** of the Stelnet server.

Figure 8 Specifying the host name (or IP address)



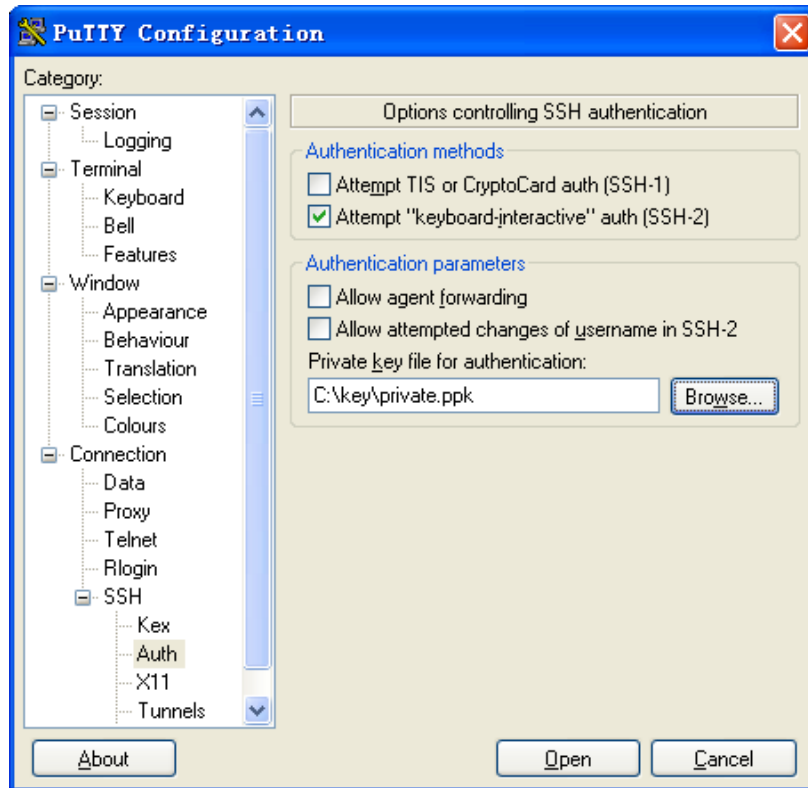
3. From the navigation tree, select **Connection > SSH**.
The page shown in Figure 9 opens.
4. Set **Preferred SSH protocol version** to 2.

Figure 9 Specifying the preferred SSH version



5. From the navigation tree, select **Connection > SSH > Auth**.
The page shown in [Figure 10](#) opens.
6. Click **Browse...** to open the file selection page, and then select the private key file (**private.ppk** in this example).
7. Click **Open**.

Figure 10 Specifying the private key file



8. Enter username **client002** to log in to the Stelnet server.

Example: Configuring the AC as an Stelnet client (password authentication)

Network configuration

As shown in [Figure 11](#):

- The switch acts as the Stelnet server and uses password authentication to authenticate the Stelnet client. The username and password of the client are saved on the switch.
- The AC acts as the Stelnet client. After the user on the AC logs in to the switch through Stelnet, the user can configure and manage the switch as a network administrator.

Stelnet server

Stelnet client

Vlan-int2 192.168.1.40/24

Vlan-int2 192.168.1.56/24

Switch

AC

1. Configure the Stelnet server:

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
. ....+++++
. ....+++++
..+++++++
. ....+++++++
```

```
# Generate a DSA key pair.
```

```
[Switch] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++
.....+. ....+. ....+. .....
..+. ....+. ....+. ..+
```

Create the key pair successfully.

```
# Generate an ECDSA key pair.
```

```
[Switch] public-key local create ecdsa secp256r1
Generating Keys...
```

Create the key pair successfully.

```
# Enable the Stelnet server.
```

```
[Switch] ssh server enable
```

Assign an IP address to VLAN-interface 2. The Stelnet client uses this address as the destination address of the SSH connection.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface2] quit
```

```
# Set the authentication mode to AAA for user lines.
```

```
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit
# Create a local device management user named client001.
[Switch] local-user client001 class manage
# Set the password to aabbcc in plain text for local user client001.
[Switch-luser-manage-client001] password simple aabbcc
# Authorize local user client001 to use the SSH service.
[Switch-luser-manage-client001] service-type ssh
# Assign the network-admin user role to local user client001.
[Switch-luser-manage-client001] authorization-attribute user-role network-admin
[Switch-luser-manage-client001] quit
# Create an SSH user named client001. Specify the service type as stelnet and the
authentication method as password for the user.
[Switch] ssh user client001 service-type stelnet authentication-type password
```

2. Assign an IP address to VLAN-interface 2 on the AC:

```
<AC> system-view
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
[AC-Vlan-interface2] quit
[AC] quit
```

Verifying the configuration

On the AC, use one of the following methods to establish a connection to the Stelnet server and verify the configuration:

- Establish a connection to the Stelnet server, enter username **client001**, and then enter **y** to access the server and download the server's host public key.

```
<AC> ssh2 192.168.1.40
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:y
client001@192.168.1.40's password:

Enter a character ~ and a dot to abort.

*****
* Copyright (c) 2024 Intelbras S.A All rights reserved.*
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
*****

<Switch>
```

After you enter password **aabbcc**, you can log in to the switch successfully. At the next connection attempt, the client authenticates the server by using the server's host public key that is locally saved on the client.

- Configure the server's host public key on the client, and then connect to the Stelnet server:
Use the **display public-key local dsa public** command on the server to display the server's host public key. (Details not shown.)

Enter public key view of the client and copy the server's host public key to the client.

```
[AC] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
[AC-pkey-public-key-key1]308201B73082012C06072A8648CE3804013082011F0281810
0D757262C4584C44C211F18BD96E5F0
[AC-pkey-public-key-key1]61C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE
65BE6C265854889DC1EDBD13EC8B274
[AC-pkey-public-key-key1]DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B0
6FD60FE01941DDD77FE6B12893DA76E
[AC-pkey-public-key-key1]EBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B3
68950387811C7DA33021500C773218C
[AC-pkey-public-key-key1]737EC8EE993B4F2DED30F48EDACE915F0281810082269009E
14EC474BAF2932E69D3B1F18517AD95
[AC-pkey-public-key-key1]94184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD35D02
492B3959EC6499625BC4FA5082E22C5
[AC-pkey-public-key-key1]B374E16DD00132CE71B020217091AC717B612391C76C1FB2E
88317C1BD8171D41ECB83E210C03CC9
[AC-pkey-public-key-key1]B32E810561C21621C73D6DAAC028F4B1585DA7F42519718CC
9B09EEF0381840002818000AF995917
[AC-pkey-public-key-key1]E1E570A3F6B1C2411948B3B4FFA256699B3BF871221CC9C5D
F257523777D033BEE77FC378145F2AD
[AC-pkey-public-key-key1]D716D7DB9FCABB4ADBF6FB4FDB0CA25C761B308EF53009F71
01F7C62621216D5A572C379A32AC290
[AC-pkey-public-key-key1]E55B394A217DA38B65B77F0185C8DB8095522D1EF044B465E
8716261214A5A3B493E866991113B2D
[AC-pkey-public-key-key1]485348
[AC-pkey-public-key-key1] peer-public-key end
[AC] quit
```

Establish an SSH connection to the server, and specify the host public key of the server as **key1**.

```
<AC> ssh2 192.168.1.40 public-key key1
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
client001@192.168.1.40's password:
Enter a character ~ and a dot to abort.
```

```
*****
* Copyright (c) 2024 Intelbras S.A All rights reserved.*
* Without the owner's prior written consent,
* no decompiling or reverse-engineering shall be allowed.
*****
```

```
<Switch>
```

After you enter username **client001** and password **aabbcc**, you can log in to the switch successfully.

Network configuration

- The switch acts as the Stelnet server, and it uses publickey authentication and the DSA public key algorithm.
- The AC acts as the Stelnet client. After the user on the AC logs in to the switch through Stelnet, the user can configure and manage the switch as a network administrator.

Stelnet server

Vlan-int2
192.168.1.40/24

Switch

Stelnet client

Vlan-int2
192.168.1.56/24

AC

Because the client's host public key is required in the server configuration, you must generate a DSA key pair on the client before configuring the Stelnet server.

1. Configure the Stelnet client:

```
# Assign an IP address to VLAN-interface 2.
```

```
<AC> system-view
```

```
[AC] interface vlan-interface 2
```

```
[AC-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
```

```
[AC-Vlan-interface2] quit
```

```
# Generate a DSA key pair.
```

```
[AC] public-key local create dsa
```

The range of public key size is (512 ~ 2048).

If the key modulus is greater than 512, it will take a few minutes.

Press CTRL+C to abort.

Input the modulus length [default = 1024]:

Generating Keys...

.+++++*****

Create the key pair successfully.

```
# Export the DSA host public key to a public key file named key.pub.
```

```
[AC] public-key local export dsa ssh2 key.pub
```

```
[AC] quit
```



```
# Create a local device management user named client002.
[Switch] local-user client002 class manage

# Authorize local user client002 to use the SSH service.
[Switch-luser-manage-client002] service-type ssh

# Assign the network-admin user role to local user client002.
[Switch-luser-manage-client002] authorization-attribute user-role network-admin
[Switch-luser-manage-client002] quit
```

Verifying the configuration

Verify that you can log in to the Stelnet server from the Stelnet client.

```
<AC> ssh2 192.168.1.40
```

```
Username: client002
```

```
Press CTRL+C to abort.
```

```
Connecting to 192.168.1.40 port 22.
```

```
The server is not authenticated. Continue? [Y/N]:y
```

```
Do you want to save the server public key? [Y/N]:n
```

```
Enter a character ~ and a dot to abort.
```

```
*****
* Copyright (c) 2024 Intelbras S.A All rights reserved.*
* Without the owner's prior written consent,
* no decompiling or reverse-engineering shall be allowed.
*****
```

```
<Switch>
```

After you enter username **client002** and then enter **y** to continue accessing the server, you can log in to the server successfully.

Example: Configuring the AC as an SFTP server (password authentication)

Network configuration

As shown in [Figure 13](#):

- The route between the wireless client and the AC is reachable.
- The AC acts as the SFTP server and uses password authentication to authenticate the SFTP client. The username and password of the client are saved on the AC.
- The wireless client acts as the SFTP client. After the user on the client logs in to the AC through SFTP, the user can perform file management and transfer operations on the AC as a network administrator.

The diagram illustrates the SFTP client architecture. On the left, a laptop icon is labeled "Client". To its right, yellow curved lines represent a wireless signal connecting to a blue cube icon labeled "AP" (Access Point). The AP is connected to a blue cloud icon labeled "IP network". The IP network is connected to a blue cube icon labeled "AC" (Access Controller). Finally, the AC is connected to a server icon labeled "SFTP server".

```
# Generate RSA key pairs.
```

```
# Generate a DSA key pair.
```

```
# Generate an ECDSA key pair.
```

```
# Enable the SFTP server.
```

Assign an IP address to VLAN-interface 2. The SFTP client uses this address as the destination for SSH connection.

```
# Create a local device management user named client002.
```

```
[AC] local-user client002 class manage

# Set the password to aabbcc in plain text for local user client002.
[AC-luser-manage-client002] password simple aabbcc

# Authorize local user client002 to use the SSH service.
[AC-luser-manage-client002] service-type ssh

# Assign the network-admin user role and working directory cfa0:/ to local user client002.
[AC-luser-manage-client002] authorization-attribute user-role network-admin
work-directory cfa0:/
[AC-luser-manage-client002] quit

# Create an SSH user named client002. Specify the authentication method as password and
service type as sftp for the user.
[AC] ssh user client002 service-type sftp authentication-type password
```

Verifying the configuration

The device supports different types of SFTP client software. This example uses an SFTP client that runs PSFTP of PuTTY version 0.58 to connect to the SFTP server and verify the configuration.

NOTE:

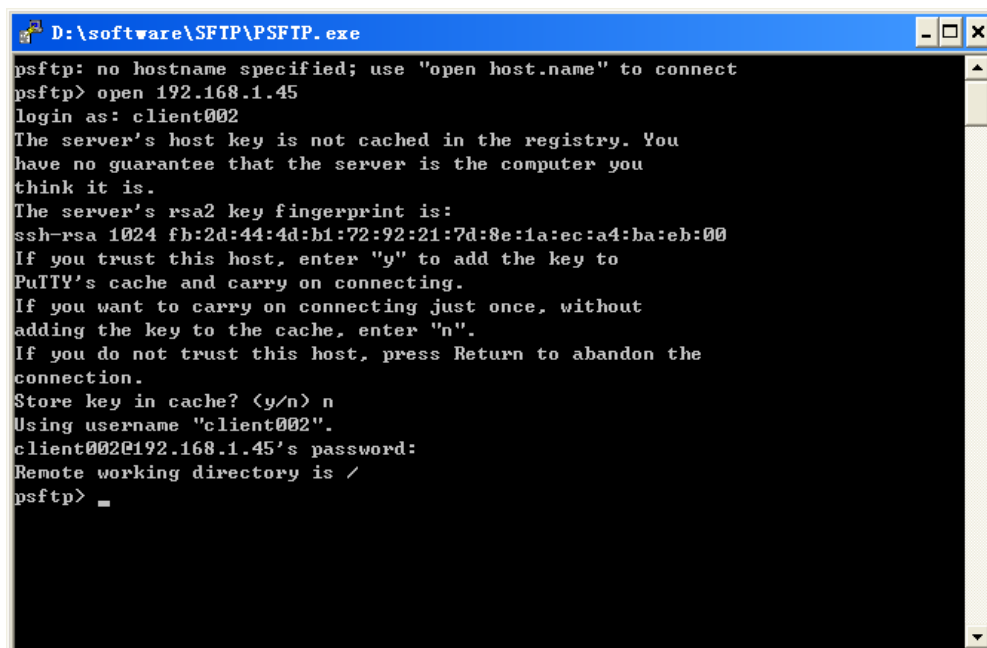
PSFTP supports only password authentication.

To verify that you can log in to the SFTP server from the SFTP client:

1. Run **psftp.exe** to launch the client interface shown in [Figure 14](#), and enter the following command:

```
open 192.168.1.45
```
2. Enter username **client002** and password **aabbcc** to log in to the SFTP server.

Figure 14 SFTP client interface



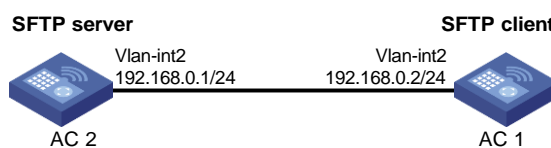
Example: Configuring the AC as an SFTP client (publickey authentication)

Network configuration

As shown in [Figure 15](#):

- AC 2 acts as the SFTP server, and it uses publickey authentication and the RSA public key algorithm.
- AC 1 acts as the SFTP client. After the user on AC 1 logs in to AC 2 through SFTP, the user can perform file management and transfer operations on AC 2 as a network administrator.

Figure 15 Network diagram



Analysis

Because the client's host public key is required in the server configuration, you must generate RSA key pairs on the client before configuring the SFTP server.

Procedures

1. Configure the SFTP client:

Assign an IP address to VLAN-interface 2.

```
<AC1> system-view
[AC1] interface vlan-interface 2
[AC1-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
[AC1-Vlan-interface2] quit
```

Generate RSA key pairs.

```
[AC1] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
```

```
. . . . .+++++
. . . . .+++++
..+++++
. . . . .+++++
```

Create the key pair successfully.

Export the host public key to a public key file named **pubkey**.

```
[AC1] public-key local export rsa ssh2 pubkey
```

```
# Transmit the public key file pubkey to the server through FTP or TFTP. (Details not shown.)
```

```
# Generate RSA key pairs.
```

```
# Authorize local user client001 to use the SSH service.
```

```
[AC2-luser-manage-client001] service-type ssh
# Assign the network-admin user role and working directory cfa0:/ to local user client001.
[AC2-luser-manage-client001] authorization-attribute user-role network-admin
work-directory cfa0:/
[AC2-luser-manage-client001] quit
```

Verifying the configuration

Verify that you can log in to the SFTP server from the SFTP client.

```
<AC1> sftp 192.168.0.1 identity-key rsa
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
sftp>
```

Display files under the current directory of the server, delete file **z**, and verify the result.

```
sftp> dir -l
-rwxrwxrwx  1 noone  nogroup  1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup   225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup   283 Aug 24 07:39 pubkey
drwxrwxrwx  1 noone  nogroup    0 Sep 01 06:22 new
-rwxrwxrwx  1 noone  nogroup   225 Sep 01 06:55 pub
-rwxrwxrwx  1 noone  nogroup    0 Sep 01 08:00 z
sftp> delete z
Removing /z
sftp> dir -l
-rwxrwxrwx  1 noone  nogroup  1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup   225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup   283 Aug 24 07:39 pubkey
drwxrwxrwx  1 noone  nogroup    0 Sep 01 06:22 new
-rwxrwxrwx  1 noone  nogroup   225 Sep 01 06:55 pub
```

Add a new directory named **new1**, and verify the result.

```
sftp> mkdir new1
sftp> dir -l
-rwxrwxrwx  1 noone  nogroup  1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup   225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup   283 Aug 24 07:39 pubkey
drwxrwxrwx  1 noone  nogroup    0 Sep 01 06:22 new
-rwxrwxrwx  1 noone  nogroup   225 Sep 01 06:55 pub
drwxrwxrwx  1 noone  nogroup    0 Sep 02 06:30 new1
```

Change the name of directory **new1** to **new2**, and verify the result.

```
sftp> rename new1 new2
sftp> dir -l
-rwxrwxrwx  1 noone  nogroup  1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup   225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup   283 Aug 24 07:39 pubkey
```



```

drwxrwxrwx   1 noone   nogroup           0 Sep 01 06:22 new
-rwxrwxrwx   1 noone   nogroup          225 Sep 01 06:55 pub
drwxrwxrwx   1 noone   nogroup           0 Sep 02 06:33 new2
# Download file pubkey2 from the server, and save it as a local file named public.
sftp> get pubkey2 public
Fetching / pubkey2 to public
/pubkey2                                     100% 225      1.4KB/s   00:00
# Upload local file pu to the server, save it as puk, and verify the result.
sftp> put pu puk
Uploading pu to / puk
sftp> dir -l
-rwxrwxrwx   1 noone   nogroup          1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone   nogroup           225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone   nogroup           283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone   nogroup           0 Sep 01 06:22 new
drwxrwxrwx   1 noone   nogroup           0 Sep 02 06:33 new2
-rwxrwxrwx   1 noone   nogroup           283 Sep 02 06:35 pub
-rwxrwxrwx   1 noone   nogroup           283 Sep 02 06:36 puk
sftp>
# Exit SFTP client view.
sftp> quit
<AC1>

```

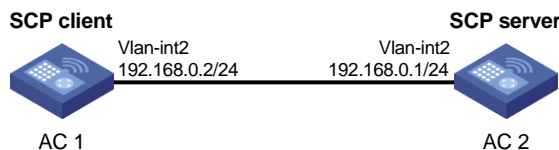
Example: Configuring SCP with password authentication

Network configuration

As shown in [Figure 16](#):

- AC 2 acts as the SCP server and uses password authentication to authenticate the SCP client. The client's username and password are saved on AC 2.
- AC 1 acts as the SCP client. After the user on AC 1 logs in to AC 2 through SCP, the user can transfer files between AC 1 and AC 2 as a network administrator.

Figure 16 Network diagram



Procedures

1. Configure the SCP server:
 - # Generate RSA key pairs.
 - <AC2> system-view

```
[AC2] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
```

```
. . . . .+++++
. . . . .+++++
..+++++++
. . . . .+++++++
Create the key pair successfully.
```

Generate a DSA key pair.

```
[AC2] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
```

```
. ++++++*****
.....+.....+.....+ .....+
...+.....+.....+ ...+.
Create the key pair successfully.
```

Generate an ECDSA key pair.

```
[AC2] public-key local create ecdsa secp256r1
Generating Keys...
```

```
.
Create the key pair successfully.
```

Enable the SCP server.

```
[AC2] scp server enable
```

Assign an IP address to VLAN-interface 2. The client uses this address as the destination for SCP connection.

```
[AC2] interface vlan-interface 2
[AC2-Vlan-interface2] ip address 192.168.0.1 255.255.255.0
[AC2-Vlan-interface2] quit
```

Create a local device management user named **client001**.

```
[AC2] local-user client001 class manage
```

Set the password to **aabbcc** in plain text for local user **client001**.

```
[AC2-luser-manage-client001] password simple aabbcc
```

Authorize local user **client001** to use the **SSH** service.

```
[AC2-luser-manage-client001] service-type ssh
```

Assign the **network-admin** user role to local user **client001**.

```
[AC2-luser-manage-client001] authorization-attribute user-role network-admin
[AC2-luser-manage-client001] quit
```

Create an SSH user named **client001**. Specify the service type as **scp** and the authentication method as **password** for the user.

```
[AC2] ssh user client001 service-type scp authentication-type password
```

2. Assign an IP address to VLAN-interface 2 on AC 1.

```
<AC1> system-view
```

```
[AC1] interface vlan-interface 2
[AC1-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
[AC1-Vlan-interface2] quit
[AC1] quit
```

Verifying the configuration

Verify that you can log in to the SCP server, download file **remote.bin** from the server, and save it locally with the name **local.bin**.

```
<AC1> scp 192.168.0.1 get remote.bin local.bin
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
client001@192.168.0.1's password:
remote.bin                                100% 2875      2.8KB/s   00:00
```

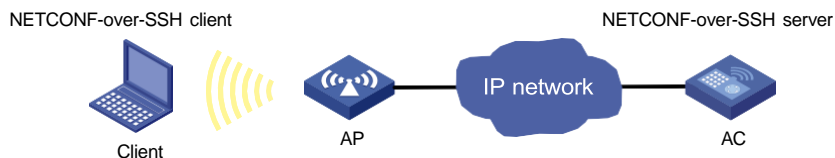
Example: Configuring NETCONF over SSH with password authentication

Network configuration

As shown in [Figure 17](#):

- The route between the wireless client and the AC is reachable.
- The AC acts as the NETCONF-over-SSH server and uses password authentication to authenticate the client. The client's username and password are saved on the AC.
- The wireless client acts as the NETCONF-over-SSH client, using SSH2 client software. After the user on the wireless client logs in to the AC through NETCONF over SSH, the user can perform NETCONF operations on the AC as a network administrator.

Figure 17 Network diagram



Procedures

Generate RSA key pairs.

```
<AC> system-view
[AC] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
```

Input the modulus length [default = 1024]:

Generating Keys...

```
..... ++++++
..... ++++++
..+++++++
..... ++++++
```

Create the key pair successfully.

Generate a DSA key pair.

[AC] public-key local create dsa

The range of public key size is (512 ~ 2048).

If the key modulus is greater than 512, it will take a few minutes.

Press CTRL+C to abort.

Input the modulus length [default = 1024]:

Generating Keys...

```
.+*****+*
.....+. ....+
...+. ....+ ..+.
```

Create the key pair successfully.

Generate an ECDSA key pair.

[AC] public-key local create ecdsa secp256r1

Generating Keys...

.

Create the key pair successfully.

Enable NETCONF over SSH.

[AC] netconf ssh server enable

Assign an IP address to VLAN-interface 2. The client uses this address as the destination for NETCONF-over-SSH connection.

[AC] interface vlan-interface 2

[AC-Vlan-interface2] ip address 192.168.100.49 255.255.255.0

[AC-Vlan-interface2] quit

Set the authentication mode to AAA for user lines.

[AC] line vty 0 63

[AC-line-vty0-63] authentication-mode scheme

[AC-line-vty0-63] quit

Create a local device management user named **client001**.

[AC] local-user client001 class manage

Set the password to **aabbcc** in plain text for local user **client001**.

[AC-luser-manage-client001] password simple aabbcc

Authorize local user **client001** to use the **SSH** service.

[AC-luser-manage-client001] service-type ssh

Assign the **network-admin** user role to local user **client001**.

[AC-luser-manage-client001] authorization-attribute user-role network-admin

[AC-luser-manage-client001] quit

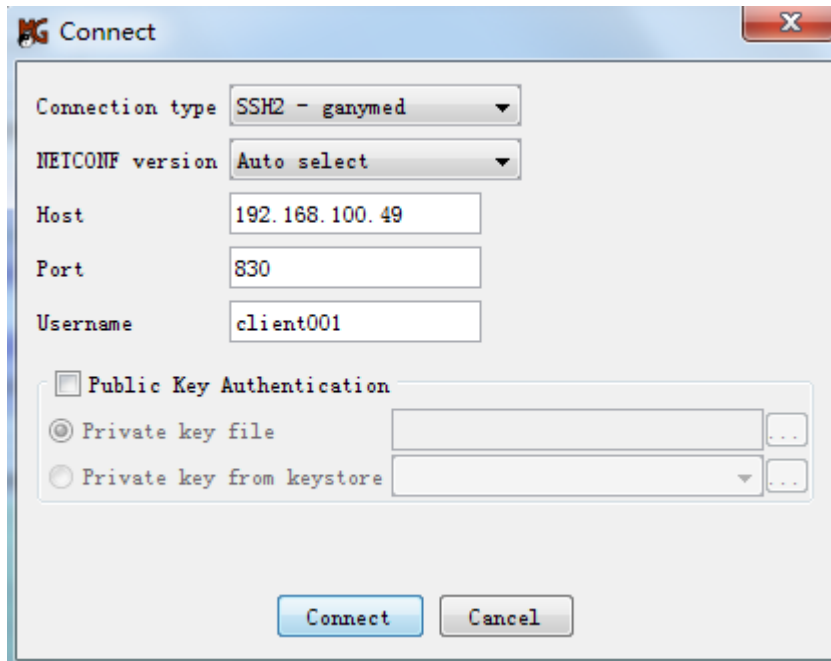
Create an SSH user named **client001**. Specify the service type as **NETCONF** and the authentication method as **password** for the user.

[AC] ssh user client001 service-type netconf authentication-type password

Verifying the configuration

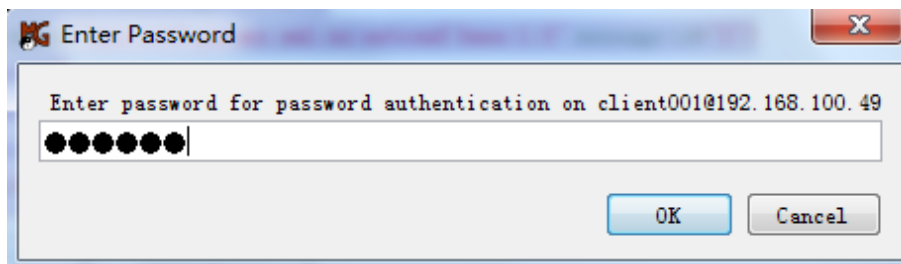
1. Launch a client that supports NETCONF over SSH.
This example uses NetConf Browser 2015 (version 3.1).
2. Select **File > Connect...** from the menu.
The **Connect** page opens, as shown in [Figure 18](#).
3. Configure connection parameters as follows:
 - a. Select a connection type from the **Connection type** list.
This example uses **SSH2-ganymed**.
 - b. Select **Auto select** from the **NETCONF version** list.
 - c. Enter **192.168.100.49** in the **Host** field.
 - d. Enter **830** in the **Port** field.
 - e. Enter **client001** in the **Username** field.
 - f. Use the default setting for the **Public Key Authentication** area.
4. Click **Connect**.

Figure 18 Connecting to the device



5. Enter password **aabbcc**, and then click **OK**, as shown in [Figure 19](#).

Figure 19 Entering the password



The NETCONF configuration interface opens when the client successfully establishes an NETCONF-over-SSH connection to the device. The **Log** tab of the interface displays the connection information, as shown in [Figure 20](#).

Figure 20 Logging in to the device

Log	Notifications	Session History
<pre> 2018/02/08 19:19:10 Connection successful: //client001@192.168.100.49:830?type=SSH2&version=auto&pk=keystore-file-path=C:\%CUsers\%Cwk6397\%C.mnetconfbrowser\%Cconfig\%Csecurity\%Ckeystore. 2018/02/08 19:19:10 NETCONF version 1.0 (XPC4741) 2018/02/08 19:19:10 Server session id: 1 2018/02/08 19:19:10 Client session id: ec85e9bf-0828-4a2e-93b5-d71e94d533af 2018/02/08 19:19:10 Client advertised these capabilities: 2018/02/08 19:19:10 urn:ietf:params:netconf:base:1.0 2018/02/08 19:19:10 urn:ietf:params:netconf:base:1.1 2018/02/08 19:19:10 Server advertised these capabilities: 2018/02/08 19:19:10 urn:hp:params:netconf:capability:hp-netconf-ext:1.0 2018/02/08 19:19:10 urn:hp:params:netconf:capability:hp-save-point:1.0 2018/02/08 19:19:10 urn:ietf:params:netconf:base:1.0 2018/02/08 19:19:10 urn:ietf:params:netconf:capability:interleave:1.0 2018/02/08 19:19:10 urn:ietf:params:netconf:capability:notification:1.0 2018/02/08 19:19:10 urn:ietf:params:netconf:capability:rollback-on-error:1.0 2018/02/08 19:19:10 urn:ietf:params:netconf:capability:validate:1.0 </pre>		

6. Verify that you have obtained the permissions of the **network-admin** user role:

In the **Command XML** area of the NETCONF configuration interface, enter **<get-sessions/>**, and then click **Send**.

The following message is displayed in the **Output XML** area.

```

<?xml version="1.0" encoding="utf-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="2">
  <get-sessions>
    <Session>
      <SessionID>1</SessionID>
      <Line>vty1</Line>
      <UserName>client001</UserName>
      <Since>2011-01-01T08:36:27</Since>
      <LockHeld>false</LockHeld>
    </Session>
  </get-sessions>
</rpc-reply>

```

Related documentation

- *Security Command Reference in INTELBRAS Access Controllers Command References*
- *Security Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*