SSH Configuration

Contents

Chapter 1 SSH Terminal Services

1.1 Introduction to SSH

Secure Shell (SSH) can provide information security and powerful authentication to prevent such assaults as IP address spoofing, plain-text password interception when users log on to the Switch remotely through an insecure network environment.

SSH can take the place of the Telnet to provide safe management and configuration.

A Switch can connect to multiple SSH clients, and currently supports SSHv2.0 version.

The communication process between the server and client includes these five stages:

Version negotiation stage: These operations are completed at this stage:

- The client sends TCP connection requirement to the server.
- When TCP connection is established, both ends begin to negotiate the SSH version.
- If they can work together in harmony, they enter the key algorithm negotiation stage. Otherwise the server clears the TCP connection.

Key algorithm negotiation stage. These operations are completed at this stage:

- The server sends the public key in a randomly generated RSA key pair to the client.
- The client figures out session key based on the public key from the server and the random number generated locally.
- The client encrypts the random number with the public key from the server and sends the result back to the server.
- The server then decrypts the received data with the server private key to get the client random number.
- The server then uses the same algorithm to work out the session key based on server public key and the returned random number.

Then both ends get the same session key without data transfer over the network, while the key is used at both ends for encryption and decryption.

Authentication method negotiation stage: These operations are completed at this stage:

- The client sends its username information to the server.
- The server authenticates the username information from the client.
- The client authenticates information from the user at the server till the authentication succeeds or the connection is turned off due to authentication timeout.

Session request stage: The client sends session request messages to the server which processes the request messages.

Interactive session stage: Both ends exchange data till the session ends

1.2 SSH Server Configuration

A Switch, as a SSH server, can connect to multiple SSH clients. SSH clients can be both LAN users and WAN users. The switches can only SSH server and support SSH v2.

The following table describes SSH server configuration tasks.

Table 1-1 Configure SSHv2.0 server

Operation	Command	Description
Enable SSH	**ssh**	Use this command in global configuration mode. By default, this function is disabled.
Configure the default key	**cry generate rsa**	Use this command in privileged mode.
Load SSH key	**cry refresh rsa**	Use this command in privileged mode. This command will cover current key.
Clear configured key	**cry zeroize rsa**	Use this command in privileged mode.
Load/upload the key (public or private) through TFTP	{*load* | *upload*} **keyfile** {*private* | *public*} **TFTP** *A.B.C.D file_name*	Use this command in privileged mode.
Load/upload the key (public or private) through FTP	{*load* | *upload*} **keyfile** {*private* | *public*} **FTP** *A.B.C.D file_name Username Password*	Use this command in privileged mode.
Show SSH	**show ssh**	
Show SSH key	**show keyfile** {*public* | *private*}	

1.3 Log in Switch from SSH Client

To successfully establish SSH connection, pay attention to following points:

1. Create the connection between SSH client and server.
2. The version of client and server should be the same.
3. The key matched.
4. SSH function in server should be enabled.

By default, there is a pair of keys saved in switch. The loaded key can also be used. Pay attention to followings:

1. The configured keyfile must be RSA. The keyfile includes public key and private key. It can be default key or loaded keyfile through ftp/tftp. No keyfile is configured in initiation. The default key can be used only after generating by command. The configured key is saved in Flash and can only be used after loading when rebooting.

2. User cannot log in device through SSH client if the configured key is not RSA key or the public and private key are not matched.

3. There can be comment line and key content in the keyfile. Comment line should contain ":" or space. Key content contain the key encoded by Base64 coding, without ":" and space. Public key cannot be in private keyfile and private keyfilecannot be encrypted by password.

1.4 SSH Server Configuration Example

1.1.1 Use Default Key

i. Network requirements

As shown in Figure 1-1, The PC (SSH Client) runs the client software which supports SSHv2.0, establish a local connection with the switch (SSH Server) and ensure the security of data exchange.

ii. Network diagram

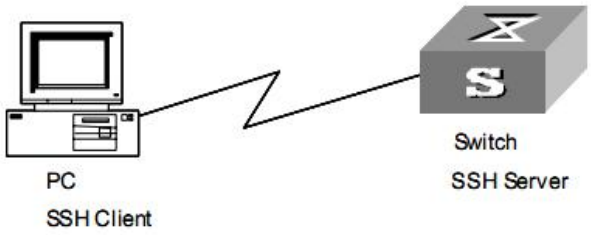

Figure 1-1. Network diagram for SSH server configuration

iii. Configuration procedure

1. Enable SSH

```
Switch(config)#ssh
Config SSH state successfully.
Switch(config)#
```

2. Display SSH configuration to ensure the keyfile can be used.

```
Switch(config)#show ssh
ssh version    : 2.0
ssh state      : on
ssh key file : available
```

3. Open SSH client in PC and log in switch

1.1.2 Use Loaded Key

iv. Network requirements

As shown in Figure 1-2, The PC (SSH Client) runs the client software which supports SSHv2.0, establish a local connection with the switch (SSH Server) and ensure the security of data exchange.

v. Network diagram

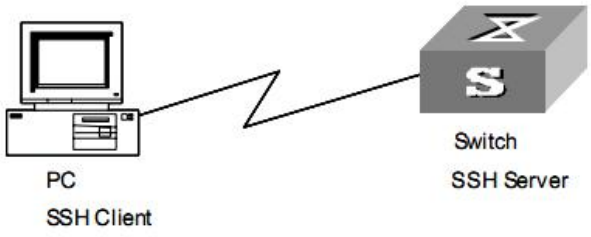

Figure 1-2. Network diagram for SSH server configuration

vi. Configuration procedure

1. Use key generated tool to generate a pair of RSA key as Figure 1-3.

```
PuTTY-User-Key-File-2: ssh-rsa
Encryption: none
Comment: rsa-key-20090624
Private-Lines: 8
AAAAgGtls5qVyP9TEpW+HfiYWRfaKCrhH2EYsQke/r21hjz7BTwzmg8Y/gatMTBw
mMjtn1eAI9MQk5siPkJEkt6jucJBAL1dpQn50Xw+ZTDZ+LEKEMEXGK8CfM6nXPZQ
a3Fmx6RjgHuI9Ey09bD9HvKZDnh9pSuoi8pL1XniFFVV0SSJAAAAQQD1WXgoFLCM
uDsHA/Ysls6nqRzAYjCvPyt8PVpjuz7CETO4Ii5Zxo/jhey6qtEmSvdfYo+dxSzx
BEodj+rrnWGHAAAAQQCl2QrR5hZvY/cM1DDxhTFjPkNiuXrCGdYEYpPbws5jxJT1
wtYpyW5yisImMxc5WpVVNGNukww2iNbuzQxO8XtzAAAAQBaM4z8kTff8SMpc60vL
q9rjapCTrfPU9QN0I00LiILO3ju2E0dgrK1qF00QA1o2AMcfA+Hp1HBHY424fTRx
FJ0=
Private-MAC: 37b49b5d489ff022fa3de91b2330fd89a74eaeff
```

Figure 1-3. Example of correct private key form

2. Load key

Switch#load keyfile private tftp 1.1.1.1 private.ppk

SSH key file will be updated, are you sure(y/n)? [n]y

Loading SSH key file via TFTP...

Load SSH key file via TFTP successfully.

Switch#load keyfile public tftp 1.1.1.1 public.pub

SSH key file will be updated, are you sure(y/n)? [n]y

Loading SSH key file via TFTP...

Load SSH key file via TFTP successfully.

3. Enable SSH

Switch(config)#ssh

Config SSH state successfully.

4. Display SSH configuration to ensure the keyfile can be used.

Switch(config)#show ssh

ssh version : 2.0

ssh state : on

ssh key file : available

5. Ensure current key is the loaded key (if it is not the loaded key, use cry key refresh to refresh it)

Switch#show key private

PuTTY-User-Key-File-2: ssh-rsa

Encryption: none

Comment: rsa-key-20090624

Private-Lines: 8

AAAAgGtls5qVyP9TEpW+HfiYWRfaKCrhH2EYsQke/r21hjz7BTwzmg8Y/gatMTBw

mMjtn1eAI9MQk5siPkJEkt6jucJBAL1dpQn50Xw+ZTDZ+LEKEMEXGK8CfM6nXPZQ

a3Fmx6RjgHuI9Ey09bD9HvKZDnh9pSuoi8pL1XniFFVV0SSJAAAAQQD1WXgoFLCM

uDsHA/Ysls6nqRzAYjCvPyt8PVpjuz7CETO4Ii5Zxo/jhey6qtEmSvdfYo+dxSzx

BEodj+rrnWGHAAAAQQCl2QrR5hZvY/cM1DDxhTFjPkNiuXrCGdYEYpPbws5jxJTl

wtYpyW5yisImMxc5WpVVNGNukww2iNbuzQxO8XtzAAAAQBaM4z8kTff8SMpc60vL

q9rjapCTrfPU9QN0I00LiILO3ju2E0dgrK1qF00QA1o2AMcfA+Hp1HBHY424fTRx

FJ0=

Private-MAC: 37b49b5d489ff022fa3de91b2330fd89a74eaeff

Switch#show key public

---- BEGIN SSH2 PUBLIC KEY ----

Comment: "rsa-key-20090624"

AAAAB3NzaC1yc2EAAAABJQAAAIEAnvKtp1iP4Ee/WH/F9QpvYL3AkWGpUkNDc+Yx

VjWdtmlFMCNpIJWg6yllzM+acQ3C3akqx7xfk62PV9YhDBEIsHZIFh4seZbNHSiC

ZS2B0txcVPNe6+WrUhHsExzp3fEmNsrB5E5BPKmQyU0+6QS691oQhZUnHN93J1r1

8GelrKU=

---- END SSH2 PUBLIC KEY ----

6. Open SSH client in PC and log in switch.