**Configuring Automatic Enterprise Network O&M**

Student Version



Huawei Technologies Co., Ltd.

|  |
| --- |
| **Copyright © Huawei Technologies Co., Ltd. 2020. All rights reserved.**  No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.  **Trademarks and Permissions**  HW_POS_RBG_Vertical-150ppi.png and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.  All other trademarks and trade names mentioned in this document are the property of their respective holders.  **Notice**  The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.  The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. |

|  |  |
| --- | --- |
| Huawei Technologies Co., Ltd. | |
| Address: | Huawei Industrial Base  Bantian, Longgang  Shenzhen 518129  People's Republic of China |
| Website: | <https://e.huawei.com/> |

**Huawei Certification System**

Huawei Certification follows the "platform + ecosystem" development strategy, which is a new collaborative architecture of ICT infrastructure based on "Cloud-Pipe-Terminal". Huawei has set up a complete certification system consisting of three categories: ICT infrastructure certification, platform and service certification, and ICT vertical certification. It is the only certification system that covers all ICT technical fields in the industry. Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE). Huawei Certification covers all ICT fields and adapts to the industry trend of ICT convergence. With its leading talent development system and certification standards, it is committed to fostering new ICT talent in the digital era, and building a sound ICT talent ecosystem.

Huawei Certified ICT Associate-Datacom (HCIA-Datacom) is designed for Huawei's frontline engineers and anyone who want to understand Huawei's datacom products and technologies. The HCIA-Datacom certification covers routing and switching principles, basic WLAN principles, network security basics, network management and O&M basics, SDN and programmability and automation basics.

The Huawei certification system introduces the industry, fosters innovation, and imparts cutting-edge datacom knowledge.



# Configuring Automatic Enterprise Network O&M

## Background

An enterprise has three office areas for Technology, Finance, and Marketing departments. Three routers are deployed for these departments respectively, and are connected to each other. Open Shortest Path First (OSPF) needs to be configured for the router in each single area so that all PCs in the office areas can communicate with each other. To ensure security, the company needs to change the management passwords of all network devices and automatically back up the routers' configurations every day. Figure 1 shows the project network topology. The specific requirements are as follows:

OSPF is configured on all the routers to implement network connectivity.

SNMP is enabled on each router so that you can manage the routers, change their passwords, and back up their configurations every day on the NMS.

IP addresses and interfaces are configured for the network management PC and routers according to information shown in the following topology.

## Objectives

Upon completion of this task, you will be able to:

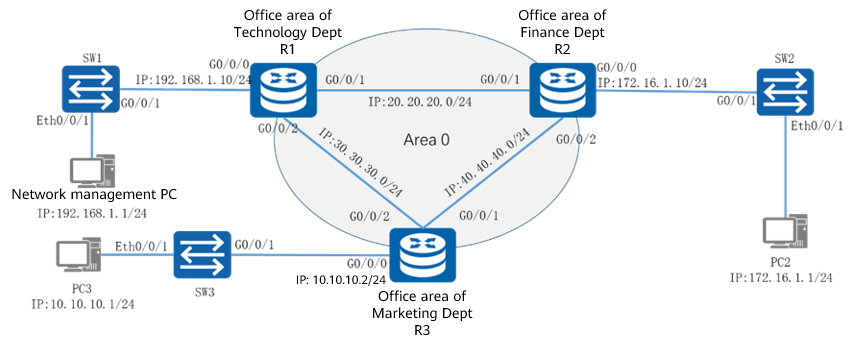
Learn how to use python to compile a password change script

Learn how to use python to compile a configuration backup script.

Learn how to use python to configure a scheduled task

## Topology

Lab Topology



The three office areas can communicate with each other. OSPF routes are configured for the router in each single area so that all PCs in the office areas can communicate with each other. SSH is enabled on all network devices. A network management PC is deployed in the Technology department to ensure normal communication between the network management PC and network devices.

The IP address planning and interface planning can be referred in the appendix.

## Implementation

### Roadmap

1. Configure router interfaces.
2. Deploy a single-area OSPF network.
3. Configure SSH login on the routers.
4. Install the Paramiko module on the network management PC.
5. Use Python to compile a password change script.
6. Use Python to compile a configuration backup script.
7. Configure a scheduled task.
8. Configure IP addresses for all the PCs.

### Procedure

Configure router interfaces.

#Configure R1.

[Huawei]system-view

[Huawei]sysname R1

[R1]interface GigabitEthernet 0/0/0

[R1-GigabitEthernet0/0/0]ip address 192.168.1.10 255.255.255.0

[R1]interface GigabitEthernet 0/0/1

[R1-GigabitEthernet0/0/1]ip address 20.20.20.1 255.255.255.0

[R1]interface GigabitEthernet 0/0/2

[R1-GigabitEthernet0/0/2]ip address 30.30.30.1 255.255.255.0

# Configure R2.

[Huawei]system-view

[Huawei]sysname R2

[R2]interface GigabitEthernet 0/0/0

[R2-GigabitEthernet0/0/0]ip address 172.16.1.10 255.255.255.0

[R2]interface GigabitEthernet 0/0/1

[R2-GigabitEthernet0/0/1]ip address 20.20.20.10 255.255.255.0

[R2]interface GigabitEthernet 0/0/2

[R2-GigabitEthernet0/0/2]ip address 40.40.40.10 255.255.255.0

# Configure R3.

[Huawei]system-view

[Huawei]sysname R3

[R3]interface GigabitEthernet 0/0/0

[R3-GigabitEthernet0/0/0]ip address 10.10.10.2 255.255.255.0

[R3]interface GigabitEthernet 0/0/1

[R3-GigabitEthernet0/0/1]ip address 40.40.40.1 255.255.255.0

[R3]interface GigabitEthernet 0/0/2

[R3-GigabitEthernet0/0/2]ip address 30.30.30.10 255.255.255.0

Deploy single-area OSPF networks.

Create and run an OSPF process on each router. Create an area and enter the OSPF area view. Specify the interface that runs OSPF and the area to which the interface belongs.

# Configure R1.

[R1]ospf 1

[R1-ospf-1]area 0

[R1-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255

[R1-ospf-1-area-0.0.0.0]network 20.20.20.0 0.0.0.255

[R1-ospf-1-area-0.0.0.0]network 30.30.30.0 0.0.0.255

#Configure R2.

[R2]ospf 1

[R2-ospf-1]area 0

[R2-ospf-1-area-0.0.0.0]network 172.16.1.0 0.0.0.255

[R2-ospf-1-area-0.0.0.0]network 20.20.20.0 0.0.0.255

[R2-ospf-1-area-0.0.0.0]network 40.40.40.0 0.0.0.255

# Configure R3.

[R3]ospf 1

[R3-ospf-1]area 0

[R3-ospf-1-area-0.0.0.0]network 10.10.10.0 0.0.0.255

[R3-ospf-1-area-0.0.0.0]network 40.40.40.0 0.0.0.255

[R3-ospf-1-area-0.0.0.0]network 30.30.30.0 0.0.0.255

Configure SSH login on the routers.

# Configure R1.

[R1]rsa local-key-pair create

The key name will be: Host

% RSA keys defined for Host already exist.

Confirm to replace them? (y/n)[n]:y

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

NOTES: If the key modulus is greater than 512,

It will take a few minutes.

Input the bits in the modulus[default = 512]:2048

[R1]aaa

[R1-aaa]local-user admin password cipher 123456

[R1-aaa]local-user admin privilege level 3

[R1-aaa]local-user admin service-type ssh

[R1-aaa]stelnet server enable

Info: Succeeded in starting the STELNET server.

[R1]ssh user admin authentication-type password

Authentication type setted, and will be in effect next time

[R1]user-interface vty 0 4

[R1-ui-vty0-4]authentication-mode aaa

#Configure R2.

[R2]rsa local-key-pair create

The key name will be: Host

% RSA keys defined for Host already exist.

Confirm to replace them? (y/n)[n]:y

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

NOTES: If the key modulus is greater than 512,

It will take a few minutes.

Input the bits in the modulus[default = 512]:2048

[R2]aaa

[R2-aaa]local-user admin password cipher 123456

[R2-aaa]local-user admin privilege level 3

[R2-aaa]local-user admin service-type ssh

[R2-aaa]stelnet server enable

Info: Succeeded in starting the STELNET server.

[R2]ssh user admin authentication-type password

Authentication type setted, and will be in effect next time

[R2]user-interface vty 0 4

[R2-ui-vty0-4]authentication-mode aaa

[R2-ui-vty0-4]protocol inbound ssh

#Configure R3.

[R3]rsa local-key-pair create

The key name will be: Host

% RSA keys defined for Host already exist.

Confirm to replace them? (y/n)[n]:y

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

NOTES: If the key modulus is greater than 512,

It will take a few minutes.

Input the bits in the modulus[default = 512]:2048

[R3]aaa

[R3-aaa]local-user admin password cipher 123456

[R3-aaa]local-user admin privilege level 3

[R3-aaa]local-user admin service-type ssh

[R3-aaa]stelnet server enable

Info: Succeeded in starting the STELNET server.

[R3]ssh user admin authentication-type password

Authentication type setted, and will be in effect next time

[R3]user-interface vty 0 4

[R3-ui-vty0-4]authentication-mode aaa

[R3-ui-vty0-4]protocol inbound ssh

Install the Paramiko module on the network management PC.

Install the Paramiko module on the network management PC that is connected to the Internet.

[root@manage ~]# curl "https://bootstrap.pypa.io/get-pip.py" -o "get-pip.py"

[root@manage ~]# python get-pip.py

[root@manage ~]# pip install paramiko

Use Python to compile a password change script.

Compile Python script changepassword.py to change the passwords of R1 to R3.

[root@manage ~]# vi changepassword.py

## Import the Paramiko, time, and getpass modules.

#!/usr/bin/python

import paramiko

import time

import getpass

## Use the raw\_input() function to obtain the SSH user name entered by the user and assign a value to username.

username = raw\_input('Username:')

## Use the getpass() function in the getpass module to obtain the character string entered by the user as the password and assign a value to password.

password = getpass.getpass('Password:')

for i in ["192.168.1.2","172.16.1.2","10.10.10.2"]:

ip=str(i)

ssh\_client=paramiko.SSHClient()

ssh\_client.set\_missing\_host\_key\_policy(paramiko.AutoAddPolicy())

ssh\_client.connect(hostname=ip,username=username,password=password)

command=ssh\_client.invoke\_shell()

## Invoke switches to run commands.

command.send("system-view" +"\n")

command.send("user-interface console 0"+"\n")

command.send("set authentication password cipher 234567"+"\n")

## After the login password is changed, return to the user view and save the configuration.

command.send("return"+"\n")

command.send("save"+"\n")

command.send("Y"+"\n")

command.send("\n")

## Wait for 2 seconds. Assign the command execution process to the output object, and run the print output statement to display the command output.

time.sleep(2)

output=command.recv(65535)

print output

## Disconnect the SSH session.

ssh\_client.close()

Use Python to compile a configuration backup script.

On the network management PC, compile Python script backup.py to back up configurations.

[root@manage ~]# vi backup.py

## Import the Paramiko, time, and datetime modules.

#!/usr/bin/python

import paramiko

import time

from datetime import datetime

## Set the SSH user name and password.

username ="admin"

password ="234567"

## Run the for statement to traverse the values 1, 2, 3, and 4 of i, and run the ip="192.168.100." + str(i) statement to log in to switches in SSH mode.

for i in range(1,5):

ip="192.168.100." + str(i)

ssh\_client=paramiko.SSHClient()

ssh\_client.set\_missing\_host\_key\_policy(paramiko.AutoAddPolicy())

ssh\_client.connect(hostname=ip,username=username,password=password)

command=ssh\_client.invoke\_shell()

## The SSH login is successful.

print "ssh "+ ip +" successfully"

## Disable split-screen display of the command output.

command.send("screen-length 0 temporary " +"\n")

## Obtain the running configurations of switches.

output=(command.send("display current-configuration" +"\n"))

## The program is suspended for 2 seconds.

time.sleep(2)

## Read the current time.

now=datetime.now()

## Open the backup file.

backup=open("/root/backup/"+str(now.year)+"-"+str(now.month)+"-"+str(now.day)+"-"+ip+".txt","a+")

## The backup is in progress.

print "backuping"

## Assign the output of the command for querying the running configuration to the recv object.

recv=command.recv(65535)

## Write the command output to the backup object, which is equivalent to writing the command output to the backup file.

backup.write(recv)

## Close the opened file.

backup.close()

## Disconnect the SSH session.

ssh\_client.close()

Configure a scheduled task.

Configure a scheduled task to automatically execute the backup script at 01:00 every day.

[root@manage ~]# vi /etc/crontab

## Add the following content to the end of the file and exit:

00 1 \* \* \* root python /root/backup.py

[root@manage ~]# mkdir /root/backup

[root@manage ~]# systemctl restart crond

[root@manage ~]# systemctl enable crond

Configure IP addresses for all the PCs.

Configure the IP addresses of PCs referred by the appendix.

* 1. **Verification**

Verify the password change function.

Run the **changepassword.py** script to verify that the password change function takes effect.

[root@manage ~]# ./changepassword.py

Username:admin

Password:

-----------------------------------------------------------------------------

User last login information:

-----------------------------------------------------------------------------

Access Type: SSH

IP-Address : 192.168.1.130 ssh

Time : 2020-02-29 10:31:35-08:00

-----------------------------------------------------------------------------

<R1>system-view

Enter system view, return user view with Ctrl+Z.

[R1]user-interface console 0

[R1-ui-console0]set authentication password cipher 234567

[R1-ui-console0]return

<R1>save

The current configuration will be written to the device.

Are you sure to continue? (y/n)[n]:Y

It will take several minutes to save configuration file, please wait...

-----------------------------------------------------------------------------

User last login information:

-----------------------------------------------------------------------------

Access Type: SSH

IP-Address : 192.168.1.130 ssh

Time : 2020-02-29 10:31:38-08:00

-----------------------------------------------------------------------------

<R2>system-view

Enter system view, return user view with Ctrl+Z.

[R2]user-interface console 0

[R2-ui-console0]set authentication password cipher 234567

[R2-ui-console0]return

<R2>save

The current configuration will be written to the device.

Are you sure to continue? (y/n)[n]:Y

It will take several minutes to save configuration file, please wait...

-----------------------------------------------------------------------------

User last login information:

-----------------------------------------------------------------------------

Access Type: SSH

IP-Address : 192.168.1.130 ssh

Time : 2020-02-29 10:31:41-08:00

-----------------------------------------------------------------------------

<R3>system-view

Enter system view, return user view with Ctrl+Z.

[R3]user-interface console 0

[R3-ui-console0]set authentication password cipher 234567

[R3-ui-console0]return

<R3>save

The current configuration will be written to the device.

Are you sure to continue? (y/n)[n]:Y

It will take several minutes to save configuration file, please wait...

Check the backup file after a scheduled task is executed.

#Check files in the **/root/backup** directory.

[root@manage ~]# cd /root/backup

[root@manage backup]# ls

2020-2-28-10.10.10.2.txt 2020-2-28-172.16.1.2.txt 2020-2-28-192.168.1.2.txt

[root@manage backup]# ll

total 12

-rw-r--r--. 1 root root 1786 Feb 28 1:00 2020-2-28-10.10.10.2.txt

-rw-r--r--. 1 root root 1809 Feb 28 1:00 2020-2-28-172.16.1.2.txt

-rw-r--r--. 1 root root 1762 Feb 28 1:00 2020-2-28-192.168.1.2.txt

#Check the detailed file content.

[root@manage backup]# cat 2020-2-28-10.10.10.2.txt

-----------------------------------------------------------------------------

User last login information:

-----------------------------------------------------------------------------

Access Type: SSH

IP-Address : 192.168.1.130 ssh

Time : 2020-02-29 10:32:24-08:00

-----------------------------------------------------------------------------

<R3>screen-length 0 temporary

Info: The configuration takes effect on the current user terminal interface only.

<R3>display current-configuration

[V200R003C00]

#

sysname R3

#

snmp-agent local-engineid 800007DB03000000000000

snmp-agent

#

clock timezone China-Standard-Time minus 08:00:00

#

portal local-server load flash:/portalpage.zip

#

drop illegal-mac alarm

#

wlan ac-global carrier id other ac id 0

#

set cpu-usage threshold 80 restore 75

#

aaa

authentication-scheme default

authorization-scheme default

accounting-scheme default

domain default

domain default\_admin

local-user admin password cipher %$%$YgN!G\*Q\*}0tjsqA"g~X(T{]!%$%$

local-user admin privilege level 3

local-user admin service-type ssh

#

firewall zone Local

priority 15

#

interface GigabitEthernet0/0/0

ip address 10.10.10.2 255.255.255.0

#

interface GigabitEthernet0/0/1

ip address 40.40.40.2 255.255.255.0

#

interface GigabitEthernet0/0/2

ip address 30.30.30.2 255.255.255.0

#

interface NULL0

#

ospf 1

area 0.0.0.0

network 10.10.10.0 0.0.0.255

network 30.30.30.0 0.0.0.255

network 40.40.40.0 0.0.0.255

#

stelnet server enable

#

user-interface con 0

authentication-mode password

set authentication password cipher %$%$v:.{Vo~Vt;s;grBK&HD9,%S$wJDM)zzk69v.\&X&+%jX%S',%$%$

user-interface vty 0 4

authentication-mode aaa[root@manage backup]#

The preceding output indicates that the R3's configuration is backed up.

## Appendix

**IP address planning**

| Device | Interface | IP Address |
| --- | --- | --- |
| R1 | G0/0/0 | 192.168.1.2/24 |
| R1 | G0/0/1 | 20.20.20.1/24 |
| R1 | G0/0/2 | 30.30.30.1/24 |
| R2 | G0/0/0 | 172.16.1.2/24 |
| R2 | G0/0/1 | 20.20.20.2/24 |
| R2 | G0/0/2 | 40.40.40.1/24 |
| R3 | G0/0/0 | 10.10.10.2/24 |
| R3 | G0/0/1 | 40.40.40.2/24 |
| R3 | G0/0/2 | 30.30.30.2/24 |
| Network management PC | Eth0/0/1 | 192.168.1.1/24 |
| PC2 | Eth0/0/1 | 172.16.1.1/24 |
| PC3 | Eth0/0/1 | 10.10.10.1/24 |

**Interface planning**

| Local Device | Local Interface | Peer Device | Peer Interface |
| --- | --- | --- | --- |
| R1 | G0/0/0 | SW1 | G0/0/1 |
| R1 | G0/0/1 | R2 | G0/0/1 |
| R1 | G0/0/2 | R3 | G0/0/2 |
| R2 | G0/0/0 | SW2 | G0/0/1 |
| R2 | G0/0/1 | R1 | G0/0/1 |
| R2 | G0/0/2 | R3 | G0/0/1 |
| R3 | G0/0/0 | SW3 | G0/0/1 |
| R3 | G0/0/1 | R2 | G0/0/2 |
| R3 | G0/0/2 | R1 | G0/0/2 |
| SW1 | G0/0/1 | R1 | G0/0/0 |
| SW1 | Eth0/0/1 | Network management PC | Eth0/0/1 |
| SW2 | G0/0/1 | R2 | G0/0/0 |
| SW2 | Eth0/0/1 | PC2 | Eth0/0/1 |
| SW3 | G0/0/1 | R3 | G0/0/0 |
| SW3 | Eth0/0/1 | PC3 | Eth0/0/1 |
| Network management PC | Eth0/0/1 | SW1 | Eth0/0/1 |
| PC2 | Eth0/0/1 | SW2 | Eth0/0/1 |
| PC3 | Eth0/0/1 | SW3 | Eth0/0/1 |