**Securely Interconnecting a Company and Its Branches Through CHAP Authentication**

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.



# Securely Interconnecting a Company and Its Branches Through CHAP Authentication

## Background

The company Jan16 built a branch for service development and rented private lines for interconnection between the headquarters and branch. To ensure the data security of communication lines, security authentication needs to be configured on the egress routers at the headquarters and branch. Figure 1-1 shows the topology. The following requirements must be met:

R1 at the headquarters connects to R2 at the branch through S4/0/0.

PPP is used and CHAP authentication is enabled on S4/0/0 of R1 for secure access of the branch.

The entire network is interconnected using OSPF.

The IP addresses and interfaces of PCs and routers are shown in the following topology.

## Objectives

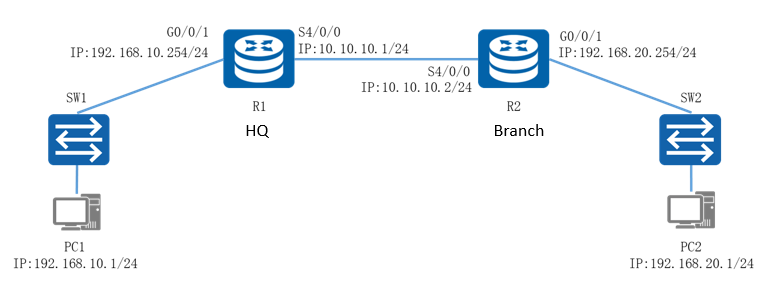
Upon completion of this task, you will be able to:

Learn how to configure CHAP authentication on authenticator device

Learn how to configure CHAP authentication on authenticate device

## Topology

Lab topology



Serial links use the PPP encapsulation protocol by default. CHAP authentication can be used to set up links more securely. In CHAP authentication, the authentication server sends an authentication request to the authenticated device and authenticates the user name and password of the peer. R1 at the headquarters functions as the authenticator. You need to create a local user named Jan16 in the AAA view, set the password to 123456, and configure CHAP authentication for S4/0/0. R2 at the branch is the authenticated device. You need to configure CHAP authentication on the interface of R2, and configure the user name and password that are the same as those on the authenticator to implement link authentication.

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

## Implementation

### Roadmap

1. Configure interfaces on the routers.
2. Build an OSPF network.
3. Configure CHAP authentication on R1.
4. Configure CHAP authentication on R2.
5. Configure IP addresses for PCs.

### Procedure

Configure interfaces on the routers.

#Configure R1.

[Huawei]system-view

[Huawei]sysname R1

[R1]int G0/0/1

[R1-GigabitEthernet0/0/1]ip add 192.168.10.254 24

[R1]interface Serial 4/0/0

[R1-Serial4/0/0]ip add 10.10.10.1 24

#Configure R2.

[Huawei]system-view

[Huawei]sysname R2

[R1]int G0/0/1

[R1-GigabitEthernet0/0/1]ip add 192.168.20.254 24

[R1]interface Serial 4/0/0

[R1-Serial4/0/0]ip add 10.10.10.2 24

Build an OSPF network.  
#Configure R1.

[R1]ospf 1

[R1-ospf-1]area 0

[R1-ospf-1-area-0.0.0.0]network 192.168.10.0 0.0.0.255

[R1-ospf-1-area-0.0.0.0]network 10.10.10.0 0.0.0.255

#Configure R2.

[R2]ospf 1

[R2-ospf-1]area 0

[R2-ospf-1-area-0.0.0.0]network 192.168.20.0 0.0.0.255

[R2-ospf-1-area-0.0.0.0]network 10.10.10.0 0.0.0.255

Configure CHAP authentication on R1.

#R1 functions as the authenticator and needs to be configured with CHAP authentication. Run the aaa command to enter the AAA view, and configure the user name and password for CHAP authentication.

[R1]aaa

[R1-aaa]

[R1-aaa]

[R1]interface Serial 4/0/0

[R1-Serial4/0/0]

[R1-Serial4/0/0]

#After the configuration is complete, shut down the interface connecting R1 to R2 for a period of time and then enable the interface to renegotiate the link between R1 and R2. Check the link status and connectivity.

[R1]interface Serial 4/0/0

[R1-Serial4/0/0]shutdown

[R1-Serial4/0/0]undo shutdown

[R1]display ip interface brief

\*down: administratively down

^down: standby

(l): loopback

(s): spoofing

The number of interface that is UP in Physical is 3

The number of interface that is DOWN in Physical is 3

The number of interface that is UP in Protocol is 2

The number of interface that is DOWN in Protocol is 4

Interface IP Address/Mask Physical Protocol

GigabitEthernet0/0/0 unassigned down down

GigabitEthernet0/0/1 192.168.10.254/24 up up

GigabitEthernet0/0/2 unassigned down down

NULL0 unassigned up up(s)

Serial4/0/0 10.10.10.1/24 up down

Serial4/0/1 unassigned down down

[R1]ping 10.10.10.2

PING 10.10.10.2: 56 data bytes, press CTRL\_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

--- 10.10.10.2 ping statistics ---

5 packet(s) transmitted

0 packet(s) received

100.00% packet loss

The preceding output shows that R1 and R2 cannot communicate with each other. The link physical status is normal, but the link layer protocol status is abnormal. This is because CHAP authentication on the PPP link fails.

Configure CHAP authentication on R2.

R2 functions as the authenticated device and requires the user name and password to be configured on S4/0/0 for CHAP authentication.

[R2]int s4/0/0

[R2-Serial4/0/0]

[R2-Serial4/0/0]

[R2-Serial4/0/0]

Configure IP addresses for PCs.

Configure the IP addresses of PCs referred by the appendix.

* 1. **Verification**

Check the link status.

Check the link status of R2.

[R2]display ip interface brief

\*down: administratively down

^down: standby

(l): loopback

(s): spoofing

The number of interface that is UP in Physical is 3

The number of interface that is DOWN in Physical is 3

The number of interface that is UP in Protocol is 3

The number of interface that is DOWN in Protocol is 3

Interface IP Address/Mask Physical Protocol

GigabitEthernet0/0/0 unassigned down down

GigabitEthernet0/0/1 192.168.20.254/24 up up

GigabitEthernet0/0/2 unassigned down down

NULL0 unassigned up up(s)

Serial4/0/0 10.10.10.2/24 up up

Serial4/0/1 unassigned down down

The preceding output shows that the link layer protocol status between R1 and R2 is normal.

Test the interoperability of PCs.

#Ping PC2 from PC1.

[C:\~]$ ping 192.168.20.1

Ping 192.168.20.1: 32 data bytes, Press Ctrl\_C to break

From 192.168.20.1: bytes=32 seq=1 ttl=126 time=63 ms

From 192.168.20.1: bytes=32 seq=2 ttl=126 time=62 ms

From 192.168.20.1: bytes=32 seq=3 ttl=126 time=47 ms

From 192.168.20.1: bytes=32 seq=4 ttl=126 time=78 ms

From 192.168.20.1: bytes=32 seq=5 ttl=126 time=78 ms

--- 192.168.20.1 ping statistics ---

5 packet(s) transmitted

5 packet(s) received

0.00% packet loss

round-trip min/avg/max = 47/65/78 ms

The preceding output shows that the PCs communicate with each other normally.

## Appendix

IP address planning

| Device | Interface | IP Address |
| --- | --- | --- |
| R1 | G0/0/1 | 192.168.10.254/24 |
| R1 | S4/0/0 | 10.10.10.1/24 |
| R2 | G0/0/1 | 192.168.20.254/24 |
| R2 | S4/0/0 | 10.10.10.2/24 |
| PC1 | E0/0/1 | 192.168.10.1/24 |
| PC2 | E0/0/1 | 192.168.20.1/24 |

Interface planning

| Local Device | Local Interface | Peer Device | Peer Interface |
| --- | --- | --- | --- |
| R1 | G0/0/0 | SW1 | G0/0/1 |
| R1 | S4/0/0 | R2 | S4/0/0 |
| R2 | G0/0/0 | SW2 | G0/0/1 |
| R2 | S4/0/0 | R2 | S4/0/0 |