**ACL Configuration**

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.



# ACL Configuration

## Background

An Access Control List (ACL) is a collection of one or more rules. A rule refers to a judgment statement that describes a packet matching condition, which may be a source address, destination address, or port number.

An ACL is a rule-based packet filter. Packets matching an ACL are processed based on the policy defined in the ACL.

## Objectives

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

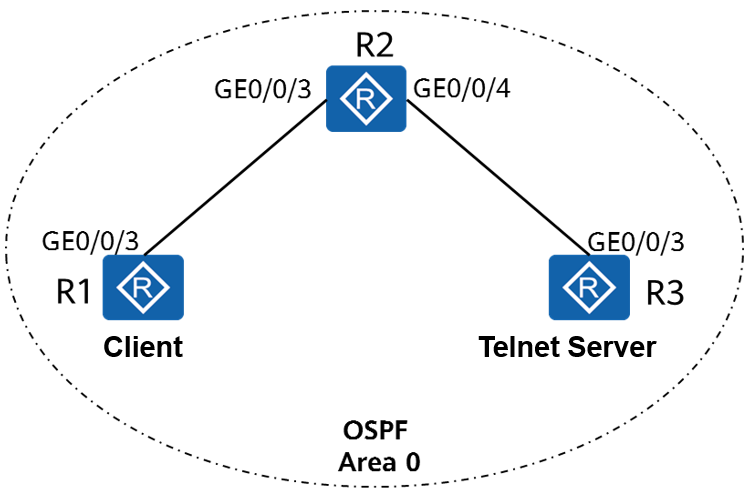
Learn how to configure ACLs

Learn how to apply an ACL on an interface

Understand the basic methods of traffic filtering

## Topology

Lab topology for ACL configuration



As shown in the networking diagram, R3 functions as the server, R1 functions as the client, and they are reachable to reach other. The IP addresses of the physical interfaces connecting R1 and R2 are 10.1.2.1/24 and 10.1.2.2/24 respectively, and the IP addresses of the physical interfaces connecting R2 and R3 are 10.1.3.2/24 and 10.1.3.1/24, respectively. In addition, two logical interfaces LoopBack 0 and LoopBack 1 are created on R1 to simulate two client users. The IP addresses of the two interfaces are 10.1.1.1/24 and 10.1.4.1/24, respectively.

One user (Loopback 1 of R1) needs to remotely manage R3. You can configure Telnet on the server, configure password protection, and configure an ACL to ensure that only the user that meets the security policy can log in to R3.

## Implementation

### Roadmap

1. Configure IP addresses.
2. Configure OSPF to ensure network connectivity.
3. Create an ACL to match desired traffic.
4. Configure traffic filtering.

### Procedure

Configure IP addresses.

# Configure IP addresses for R1, R2, and R3.

[R1]

[R2]

[R3]

Configure OSPF to ensure network connectivity.

# Configure OSPF on R1, R2, and R3 and assign them to area 0 to enable connectivity.

[R1]

[R2]

[R3]

# Run the ping command on R3 to test network connectivity.

<R3>ping 10.1.1.1

PING 10.1.1.1: 56 data bytes, press CTRL\_C to break

Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=254 time=40 ms

Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=254 time=40 ms

Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=254 time=20 ms

Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=254 time=40 ms

Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=254 time=30 ms

--- 10.1.1.1 ping statistics ---

5 packet(s) transmitted

5 packet(s) received

0.00% packet loss

round-trip min/avg/max = 20/34/40 ms

<R3>ping 10.1.2.1

PING 10.1.2.1: 56 data bytes, press CTRL\_C to break

Reply from 10.1.2.1: bytes=56 Sequence=1 ttl=254 time=30 ms

Reply from 10.1.2.1: bytes=56 Sequence=2 ttl=254 time=30 ms

Reply from 10.1.2.1: bytes=56 Sequence=3 ttl=254 time=30 ms

Reply from 10.1.2.1: bytes=56 Sequence=4 ttl=254 time=30 ms

Reply from 10.1.2.1: bytes=56 Sequence=5 ttl=254 time=50 ms

--- 10.1.2.1 ping statistics ---

5 packet(s) transmitted

5 packet(s) received

0.00% packet loss

round-trip min/avg/max = 30/34/50 ms

<R3>ping 10.1.4.1

PING 10.1.4.1: 56 data bytes, press CTRL\_C to break

Reply from 10.1.4.1: bytes=56 Sequence=1 ttl=254 time=50 ms

Reply from 10.1.4.1: bytes=56 Sequence=2 ttl=254 time=30 ms

Reply from 10.1.4.1: bytes=56 Sequence=3 ttl=254 time=40 ms

Reply from 10.1.4.1: bytes=56 Sequence=4 ttl=254 time=30 ms

Reply from 10.1.4.1: bytes=56 Sequence=5 ttl=254 time=30 ms

--- 10.1.4.1 ping statistics ---

5 packet(s) transmitted

5 packet(s) received

0.00% packet loss

round-trip min/avg/max = 30/36/50 ms

Configuration R3 as a server.

# Enable the Telnet function on R3, set the user level to 3, and set the login password to Huawei@123.

[R3]

The **telnet server enable** command enables the Telnet service.

[R3]user-interface vty 0 4

The **user-interface** command displays one or multiple user interface views.

The Virtual Type Terminal (VTY) user interface manages and monitors users logging in using Telnet or SSH.

[R3-ui-vty0-4]user privilege level 3

[R3-ui-vty0-4] set authentication password cipher

Warning: The "password" authentication mode is not secure, and it is strongly recommended to use "aaa" authentication mode.

Enter Password(<8-128>):Huawei@123

Confirm password:Huawei@123

[R3-ui-vty0-4] quit

Configure an ACL to match desired traffic.

Method 1: Configure an ACL on the VTY interface of R3 to allow R1 to log in to R3 through Telnet using the IP address of loopback 1.

# Configure an ACL on R3.

[R3]

# Filter traffic on the VTY interface of R3.

[R3]

# Display the ACL configuration on R3.

[R3]display acl 3000

The **display acl** command displays the ACL configuration.

Advanced ACL 3000, 2 rules

An advanced ACL is created. It is numbered 3000 and contains two rules.

Acl's step is 5

The step between ACL rule numbers is 5.

rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet

Rule 5 allows matched traffic to pass through. If no packet matches the rule, the **matches** field is not displayed.

rule 10 deny tcp

Method 2: Configure an ACL on the physical interface of R2 to allow R1 to log in to R3 through Telnet from the IP address of the physical interface.

# Configure an ACL on R2.

[R2]

# Filter traffic on GE0/0/3 of R3.

[R2]

# Display the ACL configuration on R2.

[R2]display acl 3001

Advanced ACL 3001, 2 rules

Acl's step is 5

rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet (21 matches)

Rule 5 allows matched traffic to pass through, and 21 packets have matched the rule.

rule 10 deny tcp (1 matches)

**----End**

* 1. **Verification**

Test the Telnet access and verify the ACL configuration.

1. On R1, telnet to the server with the source IP address 10.1.1.1 specified.

<R1>telnet -a 10.1.1.1 10.1.3.1

The **telnet** command enables a user to use the Telnet protocol to log in to another device.

-a *source-ip-address*: specifies the source IP address. Users can communicate with the server from the specified IP address.

Press CTRL\_] to quit telnet mode

Trying 10.1.3.1 ...

Error: Can't connect to the remote host

1. On R1, telnet to the server with the source IP address 10.1.4.1 specified.

<R1>telnet -a 10.1.4.1 10.1.3.1

Press CTRL\_] to quit telnet mode

Trying 10.1.3.1 ...

Connected to 10.1.3.1 ...

Login authentication

Password:

<R3>quit