**Basic Experiment on Network Device Management**

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.



# Basic Experiment on Network Device Management

## Background

On the live network of an enterprise, a network management system (NMS) is used to manage network devices. A new router is deployed on the network for service expansion.

The enterprise wants to use the existing network resources to manage this new router. Based on service requirements, the NMS should be allowed to manage only the DNS objects on the router.

## Objectives

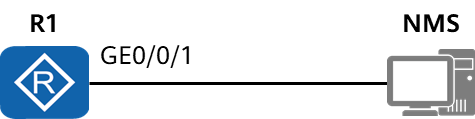
Upon completion of this task, you will be able to:

Understand the working mechanism of SNMPv3.

Configure SNMPv3 on a router.

## Topology

Lab Topology



The enterprise has high security requirements. Therefore, configure the new router to use SNMPv3 to communicate with the NMS, and enable the authentication and encryption functions on the router.

## Implementation

### Roadmap

1. Configure the router to run SNMPv3.
2. Configure SNMP user permissions so that the NMS can manage DNS objects on the router.
3. Configure the trap function to allow the router to send traps to the NMS. To help quickly identify faults according to traps and reduce unwanted traps, configure the router to send only the traps of the modules that are enabled by default.

### Procedure

Configure an IP address for the router's interface connected to the NMS and enable network connectivity with the NMS.

<Huawei> system-view

[Huawei] sysname Router

[Router] interface gigabitethernet 1/0/0

[Router-GigabitEthernet1/0/0] ip address 10.1.2.1 24

Enable the SNMP agent function.

[Router]

Set the SNMP version to SNMPv3 on the router.

[Router]

Configure the MIB view.

[Router]snmp-agent mib-view dnsmib include 1.3.6.1.4.1.2011.5.25.194

Configure the source interface of the router for sending traps.

[Router]

Configure a user group and a user, and enable data authentication and encryption.

[Router]

[Router] snmp-agent group v3 testgroup privacy write-view dnsmib notify-view dnsmib

Configure the trap function.

[Router]

* 1. **Verification**

Check user group information.

<Router> display snmp-agent group testgroup

Group name: testgroup

Security model: v3 AuthPriv

Readview: ViewDefault

Writeview: dnsmib

Notifyview: dnsmib

Storage type: nonVolatile

Check user information.

<Router> display snmp-agent usm-user

User name: testuser

Engine ID: 800007DB03548998F3A458

Group name: testgroup

Authentication mode: sha, Privacy mode: aes128

Storage type: nonVolatile

User status: active

Total number is 1

Check MIB view information.

<Router> display snmp-agent mib-view dnsmib

View name: dnsmib

MIB subtree: hwDnsMIB

Subtree mask:

Storage type: nonVolatile

View type: included

View status: active

Check information about the target host that receives traps.

<Router> display snmp-agent target-host

Traphost list:

Target host name: nms

Traphost address: 10.1.2.2

Traphost portnumber: 162

Target host parameter: trapnms

Total number is 1

Parameter list trap target host:

Parameter name of the target host: trapnms

Message mode of the target host: SNMPV3

Trap version of the target host: v3

Security name of the target host: %@%@\_=XqAFC\_94uCS,3'<gYC\*ZU6%@%@

Security level of the target host: privacy

Total number is 1