Configuration Examples for Configuration File Management Using SNMP

Keywords: SNMP, NMS, agent, FTP, TFTP, current configuration, configuration file for the next system startup

Abstract: Net-SNMP is a set of open source implementation tools of the SNMP protocol and can function as the NMS or the agent. This document introduces the configuration file management through SNMP by using Net-SNMP as the NMS. Configuration file management includes the following operations: upload, download, and run configuration file on the agent (H3C device).

Acronyms:

Acronym	Full spelling
SNMP	Simple Network Management Protocol
NMS	Network Management System
MIB	Management Information Base
FTP	File Transfer Protocol
TFTP	Trivial File Transfer Protocol

Table of Contents

Overview

The SNMP protocol defines the communication rules between network management stations (NMSs) and network agents (programs that reside in the managed devices). An NMS gets and reconfigures the value of one or more objects in the agent Management Information Base (MIB) by means of the Get and Set operations, thus realizing remote management and monitoring to agents.

There are various NMS products on the market, and the Net-SNMP is widely used as an open source implementation. It provides a complete set of applications and realizes SNMPv1, SNMPv2c and SNMPv3 functions. This document describes how to use the Net-SNMP operations to manage configuration files by accessing the MIB objects. The following are the Net-SNMP operations:

- running2Startup: Saves the current configuration to the configuration file for the next system startup.
- startup2Running: Updates the current configuration of the system with the configuration file for the next system startup.
- running2Net: Backs up the current configuration of the system to the FTP or TFTP server.
- net2Running: Downloads the configuration file from the FTP or TFTP server to the local host and executes it immediately.
- net2Startup: Downloads the configuration file from the FTP or TFTP server to the local host to replace the current startup configuration file.
- startup2Net: Backs up the configuration file for the next system startup to the FTP or TFTP server.

 Note

A startup configuration file contains a set of commands for system startup. After the configuration is saved to the configuration file for the next system startup, the system will read and execute the commands in the startup configuration file during the startup process, and thus the device can be restored to the specified configuration state.

Introduction to Net-SNMP

This document describes the snmpset and snmpwalk functions of Net-SNMP.

- The snmpset function: Executes a Set operation to set the value of a specified MIB object of the agent. The command format is **snmpset [OPTIONS] AGENT OID TYPE VALUE [OID TYPE VALUE]**.
- The snmpwalk function: Executes a Walk operation to get values of multiple MIB objects of the agent. The command format is **snmpwalk [OPTIONS] AGENT [OID]**.

The following table describes the parameters in the above two commands:

Parameter	Description
snmpset	This keyword indicates to execute the Set operation.
snmpwalk	This keyword indicates to execute the Walk operation.
OPTIONS	Command line options (see Table 1 for commonly used options).
AGENT	IP address of the agent
OID	OID of the MIB object in the agent
TYPE	MIB object type, the value can be i, u, t, a, o, s, x, d, b, or n. The following three are used in this document: ● The value **i** indicates an integer. ● The value **a** indicates an IP address. ● The value **s** indicates a character string.
VALUE	The value to be configured for the MIB object
[OID TYPE VALUE]...	Indicates that you can set the values of multiple variables and a group of OID TYPE VALUEs determines the value of a variable.

Table 1 Commonly used options of Net-SNMP command line tool

Option	Description	Example
-h	Displays command line help information.	-h
-v	Specifies the SNMP version, the value of which can be 1, 2c, or 3.	-v 1
-c	Sets the community name.	-c public
-a	Sets authentication protocol type, the value of which can be MD5 or SHA.	-a MD5
-A	Sets the authentication password.	-A 12345678
-e	Sets the security engine ID.	-e 800063A203000056000000
-u	Sets the username.	-u v3user
-x	Sets the privacy protocol type, the value of which is DES.	-x DES
-X	Sets the privacy password.	-X 12345678
-m	Loads the MIB table, the value of which is the MIB file name. If the value is **ALL**, it indicates to load all files.	● -m ALL ● -m d:/net-snmp/xxx.mib
-M	Specifies the directory of the MIB file.	-M d:/nets-snmp

📝 **Note**

For detailed introduction of Net-SNMP tools used in this document, access the website http://www.net.snmp.org/.

Related MIB Nodes

This document helps you to realize configuration file management by accessing the H3C private MIB. You can access MIB nodes with either their OIDs or their names. For the latter, you need to download related MIB files to the NMS from the H3C website, and then compile these files on the NMS; otherwise, you can only access MIB nodes with their OIDs.

Related MIB files include **rfc2578.sm2**, **rfc2579.sm2**, **rfc2580.sm2**, **hh3c-oid.mib** or **huawei-3com-oid.mib**, and **hh3c-config-man.mib** or **h3c-config-man.mib**. Where

- **rfc2578.sm2**, **rfc2579.sm2**, **rfc2580.sm2**, and **hh3c-oid.mib** are used for compiling **hh3c-config-man.mib**.
- **rfc2578.sm2**, **rfc2579.sm2**, **rfc2580.sm2**, and **huawei-3com-oid.mib** are used for compiling **h3c-config-man.mib**.
- Actually, MIB objects in **hh3c-config-man.mib** or **h3c-config-man.mib** are accessed.

hh3c-oid.mib and **hh3c-config-man.mib** are H3C new-style MIB files, and **huawei-3com-oid.mib** and **h3c-config-man.mib** are H3C compatible-style MIB files. The MIB file used depends on the current MIB style of the device. You can view the MIB style of the device by executing the **display mib-snmp** command on the agent. The **Current MIB style** field is displayed as one of the following:

- new for H3C new-style.
- compatible for H3C compatible-style.

For a node in the H3C new-style MIB files, its name starts with **hh3c**, and its OID starts with **1.3.6.1.4.1.25506**; for a node in the H3C compatible-style MIB files, its name starts with **h3c**, and its OID starts with **1.3.6.1.4.1.2011.10**. For example, node **hh3cCfgOperateType** with the OID of **1.3.6.1.4.1.25506.2.4.1.2.4.1.2** is in file **hh3c-config-man.mib**, and node **h3cCfgOperateType** with the OID of **1.3.6.1.4.1.2011.10.2.4.1.2.4.1.2** is in file **h3c-config-man.mib**. Both of the two nodes indicate the same variable in the agent, but they are in different MIB style.

By default, devices use H3C new-style MIB files; therefore, the following introduces MIB nodes in file **hh3c-config-man.mib**.

hh3cCfgOperateTable

This table realizes configuration file operations between the NMS and the devices using SNMP.

hh3cCfgOperateTable is an operation table that has multiple column objects, each of which contains multiple entities in different rows. The OID of an entity is in the format of **Column-OID.n**, where **n** is the entity number that is provided by the user. Therefore, entities with the same value of **n** in their OIDs are in the same row, and the row index is the entity number **n**. You can perform an operation to all entities of a row by defining the status of the row.

hh3cCfgOperateTable defines multiple MIB objects. The following describes MIB objects related to configuration file management.

hh3cCfgOperateType (1.3.6.1.4.1.25506.2.4.1.2.4.1.2)

Object	hh3cCfgOperateType
OID	1.3.6.1.4.1.25506.2.4.1.2.4.1.2
Description	Specifies configuration file operation type, such as running2Startup, and startup2Running.
Remarks	For value descriptions of this object, refer to Table 2.
Type	Column object (type of the entities contained in this column is integer)

Table 2 hh3cCfgOperateType value description

Value	Operation	Description
1	running2Startup	• Saves the current configuration to the configuration file for the next system startup. This operation is equal to the execution of the **save** command. • If the configuration file for the next system startup does not exist, you can create a default configuration file, and then save the current configuration to the file (the name of the created file depends on the device model)
2	startup2Running	Updates the current configuration of the system with the configuration file for the next system startup, that is, executes the commands contained in this configuration file. If the configuration file for the next system startup does not exist, the operation fails and error code 13 (opFileOpenError) is returned.
3	running2Net	Sends the current configuration of the system to the file with the specified location on the remote server.
4	net2Running	Updates the current configuration of the system with the configuration file obtained through some file transfer protocol, that is, executes this configuration file on the agent.
5	net2Startup	Replaces the current startup configuration file with the configuration file obtained through some file transfer protocol, and sets this file as the configuration file for the next system startup. If the startup configuration file does not exist, you can create a default configuration file, and then save the content of the transferred file (the name of the created file depends on the device model)
6	startup2Net	Uploads the configuration file for the next system startup to a specified location on the network through some file transfer protocol. If the startup configuration file does not exist, the operation fails and error code 13 (opFileOpenError) is returned.

hh3cCfgOperateProtocol (1.3.6.1.4.1.25506.2.4.1.2.4.1.3)

Object	hh3cCfgOperateProtocol
OID	1.3.6.1.4.1.25506.2.4.1.2.4.1.3
Description	Specifies a file transfer protocol. If the value of this object is not specified, the FTP protocol is adopted.

Remarks	The value of this object can be:
	• 1: FTP protocol.
	• 2: TFTP protocol.
Type	Column object (type of the entities contained in this column is integer)

hh3cCfgOperateFileName (1.3.6.1.4.1.25506.2.4.1.2.4.1.4)

Object	hh3cCfgOperateFileName
OID	1.3.6.1.4.1.25506.2.4.1.2.4.1.4
Description	Specifies the name of the configuration file.
Remarks	If the value of the object **hh3cCfgOperateType** is 3, 4, or 5, you must provide the file name (the file path can be provided or not).
	• If the value of the object **hh3cCfgOperateType** is 3, the value of the **hh3cCfgOperateFileName** object is the name of the target file.
	• If the value of the object **hh3cCfgOperateType** is 4 or 5, the value of the **hh3cCfgOperateFileName** object is the name of the source file to be transferred.
	For other situations, you do not need to specify the file name.
Type	Column object (type of the entities contained in this column is string)

hh3cCfgOperateServerAddress (1.3.6.1.4.1.25506.2.4.1.2.4.1.5)

Object	hh3cCfgOperateServerAddress
OID	1.3.6.1.4.1.25506.2.4.1.2.4.1.5
Description	Specifies the IP address of the FTP/TFTP server.
Remarks	• If the value of the object **hh3cCfgOperateType** is 3, 4, 5, or 6, you must specify the IP address (which cannot be all 0s and all Fs) of the server.
	• For other situations, you do not need to specify the IP address of the server.
Type	Column object (type of the entities contained in this column is IP address)

hh3cCfgOperateUserName (1.3.6.1.4.1.25506.2.4.1.2.4.1.6)

Object	hh3cCfgOperateUserName
OID	1.3.6.1.4.1.25506.2.4.1.2.4.1.6
Description	Specifies the FTP username.
Remarks	If the value of the object **hh3cCfgOperateType** is 3, 4, 5, or 6, and the value of the **hh3cCfgOperateProtocol** object is 1, you need to use this object to provide the name of the user to log in.
Type	Column object (type of the entities contained in this column is string)

hh3cCfgOperateUserPassword (1.3.6.1.4.1.25506.2.4.1.2.4.1.7)

Object	hh3cCfgOperateUserPassword
OID	1.3.6.1.4.1.25506.2.4.1.2.4.1.7
Description	Sets a password for the user specified by the **hh3cCfgOperateUserName** object.
Remarks	If the value of the object **hh3cCfgOperateType** is 3, 4, 5, or 6, and the value of the **hh3cCfgOperateProtocol** object is 1, you need to use this object to provide the password for the user.
Type	Column object (type of the entities contained in this column is string)

hh3cCfgOperateRowStatus (1.3.6.1.4.1.25506.2.4.1.2.4.1.9)

Object	hh3cCfgOperateRowStatus
OID	1.3.6.1.4.1.25506.2.4.1.2.4.1.9
Description	Sets the status of each row in hh3cCfgOperateTable.
Remarks	The value can be: ● active: Indicates that this row is available for the agent. ● notInService: Indicates that this row exists in the agent, but is unavailable for the managed device. ● notReady: Indicates that this row is already created but is unavailable due to lack of critical information. ● createAndGo: Indicates to create a row and make it available for use. ● createAndWait: Indicates to create a row but not to execute the operation immediately. You can set the status of the row to **active** manually to trigger the operation. ● destroy: Indicates to remove a row.
Type	Column object (type of the entities contained in this column is integer)

hh3cCfgOperateResultTable

This table is used to record the execution results of operations defined in hh3cCfgOperateTable. After you execute an operation through hh3cCfgOperateTable, a row will be created in hh3cCfgOperateResultTable. Each column in this row records the entity number (the row index in hh3cCfgOperateTable), operation type, operation result of operations in hh3cCfgOperateTable. The number of each row is generated by the system automatically, starts from 1 and increases.

hh3cCfgOperateResultTable defines multiple MIB objects. The following describes MIB objects related to configuration file management.

hh3cCfgOperateResultOptIndex (1.3.6.1.4.1.25506.2.4.1.2.5.1.2)

Object	hh3cCfgOperateResultOptIndex
OID	1.3.6.1.4.1.25506.2.4.1.2.5.1.2
Description	Indicates the index of the corresponding row in hh3cCfgOperateTable.

Remarks	None
Type	Column object (type of the entities contained in this column is integer)

hh3cCfgOperateResultOpType (1.3.6.1.4.1.25506.2.4.1.2.5.1.3)

Object	hh3cCfgOperateResultOpType
OID	1.3.6.1.4.1.25506.2.4.1.2.5.1.3
Description	Records the type of the corresponding operation in hh3cCfgOperateTable.
Remarks	None
Type	Column object (type of the entities contained in this column is integer)

hh3cCfgOperateState (1.3.6.1.4.1.25506.2.4.1.2.5.1.4)

Object	hh3cCfgOperateState
OID	1.3.6.1.4.1.25506.2.4.1.2.5.1.4
Description	Records the result of the corresponding operation in hh3cCfgOperateTable.
Remarks	The value can be: • opInProgress: The current operation is on going. If the reading or writing of the device flash is involved in the operation, you will have to wait for a period of time, and the operation status will be returned. • opSuccess: The operation succeeded. • Other values: The operation failed.
Type	Column object (type of the entities contained in this column is integer)

Configuration Example for Configuration File Management Using SNMPv1 or SNMPv2c

📝 **Note**

Configurations for SNMPv1 are similar to those for SNMPv2c, and SNMPv1 is used in this example. For configurations for SNMPv2c, you can change the value of – v from 1 to 2c.

Network Requirements

- As shown in Figure 1, the NMS connects to the agent through an Ethernet.
- The FTP/TFTP server provides file upload and download services.

- Net-SNMP runs on the NMS. The NMS manages the configuration file on the agent with the community name **private** using SNMPv1.

Figure 1 Network diagram for configuration file management using SNMPv1
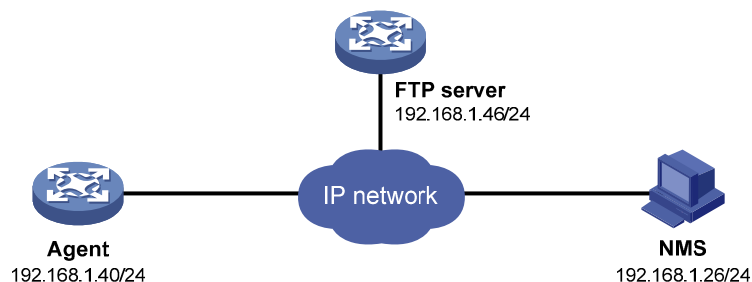
Configuration Considerations

- Configure interface parameters on the agent: configure the IP address of the interface and make sure that there is an available route between the agent and the NMS.
- Configure the SNMP basic information (including SNMP version and community name) on the agent, enabling the inter-access between the NMS and the agent.
- View the MIB style of the agent to determine the MIB objects to be used.
- Save files **snmpset.exe** and **snmpwalk.exe** in Net-SNMP to directory C:\usr\bin, and manage the configuration file through MIB objects.
- The FTP protocol is used in this example; you need to run FTP server software on the FTP server, configure username and password, and set the value of 1.3.6.1.4.1.25506.2.4.1.2.4.1.3.4 to 1.
- If the TFTP protocol is used, you need to run TFTP server software on the TFTP server, and set the value of 1.3.6.1.4.1.25506.2.4.1.2.4.1.3.4 to 2.

Configuration Procedures

Configuration on the FTP Server

An H3C device is used as the FTP server in this example. Enable FTP server function on the device, and configure the FTP username as **ftp** and password as **123123123123**.

```
<System> system-view
[System] local-user ftp
[System-luser-ftp] password simple 123123123123
[System-luser-ftp] authorization-attribute level 3
[System-luser-ftp] service-type ftp
```

Configuration on the Agent

Configure the IP address of the agent as 192.168.1.40/24 and make sure that there is an available route between the agent and the NMS.

- If Ethernet 1/1 is a Layer 3 interface, perform the following configuration:

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] ip address 192.168.1.40 24
```

```
[Sysname-Ethernet1/1] quit
```

- If Ethernet 1/1 is a Layer 2 interface, perform the following configuration:

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] port Ethernet 1/1
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip address 192.168.1.40 24
[Sysname-Vlan-interface2] quit
```

Configure the SNMP version. To avoid the failure of establishing an SNMP connection between the agent and the NMS due to the problem of SNMP version, you are recommended to configure this keyword as **all**, which means SNMPv1, SNMPv2c and SNMPv3 are all supported.

```
<Sysname> system-view
[Sysname]snmp-agent sys-info version all
```

Configure **public** as the read-only community name, and **private** as the read-and-write community name.

```
[Sysname] snmp-agent community read public
[Sysname] snmp-agent community write private
```

View the MIB file style of the device to determine the MIB objects to be used.

```
[Sysname] display mib-style
 Current MIB style: new
 Next reboot MIB style: new
```

The above information indicates that the MIB file style of the device is new; therefore, all MIB objects with the root node of 1.3.6.1.4.1.25506 will be used. (If the current MIB style is displayed as compatible, you need to use 1.3.6.1.4.1.2011.10 to replace 1.3.6.1.4.1.25506 in the following configuration steps.)

Configuration on the NMS

1) Save the current configuration to the configuration file for next system startup (running2Startup).

```
C:\usr\bin> snmpset -v 1 -c private 192.168.1.40 1.3.6.1.4.1.25506.2.4.1.2.4.1.2.1 i 1
1.3.6.1.4.1.25506.2.4.1.2.4.1.9.1 i 4
```

The system returns the following information:

```
iso.3.6.1.4.1.25506.2.4.1.2.4.1.2.1 = INTEGER: 1
iso.3.6.1.4.1.25506.2.4.1.2.4.1.9.1 = INTEGER: 4
```

View the operation result with the **snmpwalk** command.

```
C:\usr\bin> snmpwalk -v 1 -c public 192.168.1.40 1.3.6.1.4.1.25506.2.4.1.2.5.1
```

The system returns the following information:

```
iso.3.6.1.4.1.25506.2.4.1.2.5.1.2.1 = INTEGER: 1
iso.3.6.1.4.1.25506.2.4.1.2.5.1.3.1 = INTEGER: 1
iso.3.6.1.4.1.25506.2.4.1.2.5.1.4.1 = INTEGER: 2
iso.3.6.1.4.1.25506.2.4.1.2.5.1.5.1 = Timeticks: (245) 0:00:02.45
iso.3.6.1.4.1.25506.2.4.1.2.5.1.6.1 = Timeticks: (214998) 0:35:49.98
```

The above information indicates that the running2Startup operation succeeded.

2)   Back up the current configuration information to the FTP server (running2Net)

Use FTP to back up the current configuration on the agent to the FTP server (192.168.1.46) with the user name **ftp**, password **123**, and file name **aa.cfg**.

```
C:\usr\bin> snmpset -v 1 -c private 192.168.1.40 1.3.6.1.4.1.25506.2.4.1.2.4.1.2.2 i 3
1.3.6.1.4.1.25506.2.4.1.2.4.1.3.2  i  1  1.3.6.1.4.1.25506.2.4.1.2.4.1.4.2  s  aa.cfg
1.3.6.1.4.1.25506.2.4.1.2.4.1.5.2 a 192.168.1.46 1.3.6.1.4.1.25506.2.4.1.2.4.1.6.2 s ftp
1.3.6.1.4.1.25506.2.4.1.2.4.1.7.2 s 123123123123 1.3.6.1.4.1.25506.2.4.1.2.4.1.9.2 i 4
```

The system returns the following information:

```
iso.3.6.1.4.1.25506.2.4.1.2.4.1.2.2 = INTEGER: 3
iso.3.6.1.4.1.25506.2.4.1.2.4.1.3.2 = INTEGER: 1
iso.3.6.1.4.1.25506.2.4.1.2.4.1.4.2 = STRING: "aa.cfg"
iso.3.6.1.4.1.25506.2.4.1.2.4.1.5.2 = IpAddress: 192.168.1.46
iso.3.6.1.4.1.25506.2.4.1.2.4.1.6.2 = STRING: "ftp"
iso.3.6.1.4.1.25506.2.4.1.2.4.1.7.2 = STRING: "123123123123"
iso.3.6.1.4.1.25506.2.4.1.2.4.1.9.2 = INTEGER: 4
```

View the operation result with the **snmpwalk** command.

```
C:\usr\bin> snmpwalk -v 1 -c public 192.168.1.40 1.3.6.1.4.1.25506.2.4.1.2.5.1
```

The system returns the following information:

```
iso.3.6.1.4.1.25506.2.4.1.2.5.1.2.1 = INTEGER: 2
iso.3.6.1.4.1.25506.2.4.1.2.5.1.3.1 = INTEGER: 3
iso.3.6.1.4.1.25506.2.4.1.2.5.1.4.1 = INTEGER: 2
iso.3.6.1.4.1.25506.2.4.1.2.5.1.5.1 = Timeticks: (243) 0:00:02.43
iso.3.6.1.4.1.25506.2.4.1.2.5.1.6.1 = Timeticks: (181608) 0:30:16.08
```

The above information indicates that the **running2Net** operation succeeded.

Or, to view whether the operation is successful, you can use the **dir** command to view whether file **aa.cfg** is on the FTP server (192.168.1.46), and then use the **more** aa.cfg command to view whether the contents of the file are correct.

3)   Download the configuration file on the FTP server to the device and execute the file (net2Running)

```
C:\usr\bin> snmpset -v 1 -c private 192.168.1.40 1.3.6.1.4.1.25506.2.4.1.2.4.1.2.3 i 4
1.3.6.1.4.1.25506.2.4.1.2.4.1.3.3  i  1  1.3.6.1.4.1.25506.2.4.1.2.4.1.4.3  s  test.cfg
1.3.6.1.4.1.25506.2.4.1.2.4.1.5.3 a 192.168.1.46 1.3.6.1.4.1.25506.2.4.1.2.4.1.6.3 s ftp
1.3.6.1.4.1.25506.2.4.1.2.4.1.7.3 s 123123123123 1.3.6.1.4.1.25506.2.4.1.2.4.1.9.3 i 4
```

The system returns the following information:

```
iso.3.6.1.4.1.25506.2.4.1.2.4.1.2.3 = INTEGER: 4
iso.3.6.1.4.1.25506.2.4.1.2.4.1.3.3 = INTEGER: 1
iso.3.6.1.4.1.25506.2.4.1.2.4.1.4.3 = STRING: "test.cfg"
iso.3.6.1.4.1.25506.2.4.1.2.4.1.5.3 = IpAddress: 192.168.1.46
iso.3.6.1.4.1.25506.2.4.1.2.4.1.6.3 = STRING: "ftp"
iso.3.6.1.4.1.25506.2.4.1.2.4.1.7.3 = STRING: "123123123123"
iso.3.6.1.4.1.25506.2.4.1.2.4.1.9.3 = INTEGER: 4
```

View the operation result with the **snmpwalk** command.

```
C:\usr\bin> snmpwalk -v 1 -c public 192.168.1.40 1.3.6.1.4.1.25506.2.4.1.2.5.1
```

The system returns the following information:

```
iso.3.6.1.4.1.25506.2.4.1.2.5.1.2.1 = INTEGER: 3
iso.3.6.1.4.1.25506.2.4.1.2.5.1.3.1 = INTEGER: 4
iso.3.6.1.4.1.25506.2.4.1.2.5.1.4.1 = INTEGER: 2
iso.3.6.1.4.1.25506.2.4.1.2.5.1.5.1 = Timeticks: (1083) 0:00:10.83
iso.3.6.1.4.1.25506.2.4.1.2.5.1.6.1 = Timeticks: (470443) 1:18:24.43
```

The above information indicates that the net2Running operation succeeded.

You can use the **display current-configuration** command on the agent (192.168.1.40) to view the current configurations, including not only the configurations of the current startup configuration file but also configurations in file **test.cfg**.

4)   Download the configuration file **test.cfg** on the FTP server to the flash of the device (net2Startup)

Replace the content of the current configuration file of the agent with the content of file **test.cfg** and specify the current configuration file as the configuration file for the next system startup.

```
C:\usr\bin> snmpset -v 1 -c private 192.168.1.40 1.3.6.1.4.1.25506.2.4.1.2.4.1.2.4 i 5
1.3.6.1.4.1.25506.2.4.1.2.4.1.3.4  i  1  1.3.6.1.4.1.25506.2.4.1.2.4.1.4.4  s  test.cfg
1.3.6.1.4.1.25506.2.4.1.2.4.1.5.4 a 192.168.1.46 1.3.6.1.4.1.25506.2.4.1.2.4.1.6.4 s ftp
1.3.6.1.4.1.25506.2.4.1.2.4.1.7.4 s 123123123123 1.3.6.1.4.1.25506.2.4.1.2.4.1.9.4 i 4
```

The system returns the following information:

```
iso.3.6.1.4.1.25506.2.4.1.2.4.1.2.4 = INTEGER: 5
iso.3.6.1.4.1.25506.2.4.1.2.4.1.3.4 = INTEGER: 1
iso.3.6.1.4.1.25506.2.4.1.2.4.1.4.4 = STRING: "test.cfg"
iso.3.6.1.4.1.25506.2.4.1.2.4.1.5.4 = IpAddress: 192.168.1.46
iso.3.6.1.4.1.25506.2.4.1.2.4.1.6.4 = STRING: "ftp"
iso.3.6.1.4.1.25506.2.4.1.2.4.1.7.4 = STRING: "123123123123"
iso.3.6.1.4.1.25506.2.4.1.2.4.1.9.4 = INTEGER: 4
```

View the operation result with the **snmpwalk** command.

```
C:\usr\bin> snmpwalk -v 1 -c public 192.168.1.40 1.3.6.1.4.1.25506.2.4.1.2.5.1
```

The system returns the following information:

```
iso.3.6.1.4.1.25506.2.4.1.2.5.1.2.1 = INTEGER: 4
iso.3.6.1.4.1.25506.2.4.1.2.5.1.3.1 = INTEGER: 5
iso.3.6.1.4.1.25506.2.4.1.2.5.1.4.1 = INTEGER: 2
iso.3.6.1.4.1.25506.2.4.1.2.5.1.5.1 = Timeticks: (264) 0:00:02.64
iso.3.6.1.4.1.25506.2.4.1.2.5.1.6.1 = Timeticks: (418007) 1:09:40.07
```

The above information indicates that the net2Startup operation succeeded.

You can see that the content of the current configuration file is the same with that of file **test.cfg** using the **more** command on the agent (192.168.1.40), and see that the configuration file for the next system startup is the same with the current configuration file using the **display startup** command.

5)   Back up the startup configuration file in the flash of the device to the FTP server (startup2Net)

```
C:\usr\bin> snmpset -v 1 -c private 192.168.1.40 1.3.6.1.4.1.25506.2.4.1.2.4.1.2.5 i 6
1.3.6.1.4.1.25506.2.4.1.2.4.1.3.5   i   1   1.3.6.1.4.1.25506.2.4.1.2.4.1.4.5   s   bb.cfg
1.3.6.1.4.1.25506.2.4.1.2.4.1.5.5 a 192.168.1.46 1.3.6.1.4.1.25506.2.4.1.2.4.1.6.5 s ftp
1.3.6.1.4.1.25506.2.4.1.2.4.1.7.5 s 123123123123 1.3.6.1.4.1.25506.2.4.1.2.4.1.9.5 i 4
```

The system returns the following information:

```
iso.3.6.1.4.1.25506.2.4.1.2.4.1.2.5 = INTEGER: 6
iso.3.6.1.4.1.25506.2.4.1.2.4.1.3.5 = INTEGER: 1
iso.3.6.1.4.1.25506.2.4.1.2.4.1.4.5 = STRING: "bb.cfg"
iso.3.6.1.4.1.25506.2.4.1.2.4.1.5.5 = IpAddress: 192.168.1.46
iso.3.6.1.4.1.25506.2.4.1.2.4.1.6.5 = STRING: "ftp"
iso.3.6.1.4.1.25506.2.4.1.2.4.1.7.5 = STRING: "123123123123"
iso.3.6.1.4.1.25506.2.4.1.2.4.1.9.5 = INTEGER: 4
```

View the operation result with the **snmpwalk** command.

```
C:\usr\bin> snmpwalk -v 1 -c public 192.168.1.40 1.3.6.1.4.1.25506.2.4.1.2.5.1
```

The system returns the following information:

```
iso.3.6.1.4.1.25506.2.4.1.2.5.1.2.1 = INTEGER: 5
iso.3.6.1.4.1.25506.2.4.1.2.5.1.3.1 = INTEGER: 6
iso.3.6.1.4.1.25506.2.4.1.2.5.1.4.1 = INTEGER: 2
iso.3.6.1.4.1.25506.2.4.1.2.5.1.5.1 = Timeticks: (11) 0:00:00.11
iso.3.6.1.4.1.25506.2.4.1.2.5.1.6.1 = Timeticks: (356309) 0:59:23.09
```

The above information indicates that the startup2Net operation succeeded.

To view whether the operation is successful, you can use the **dir** command to view whether file **bb.cfg** is on the FTP server (192.168.1.46), and then use the **more bb.cfg** command to view whether the contents of the file are correct.

Configuration Example for Configuration File Management Using SNMPv3

Network Requirements

- As shown in Figure 2, the NMS connects to the agent through an Ethernet.
- The FTP/TFTP server provides file upload and download services.
- Net-SNMP runs on the NMS. The NMS uses SNMPv3 to manage the configuration file on the agent with the community name as **v3user**, authentication protocol as **MD5**, authentication password as **aaaaaaaaaa**, privacy protocol as **DES56**, and privacy password as **bbbbbbbbbb**.

Figure 2 Network diagram for configuration file management using SNMPv3
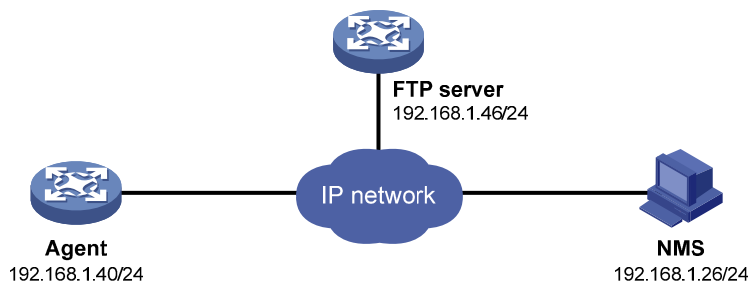
Configuration Considerations

- Configure interface parameters on the agent: configure the IP address of the interface and make sure that there is an available route between the agent and the NMS.
- Configure the SNMP basic information (including SNMP version, group, user, and authentication and encryption parameters) on the agent, enabling the inter-access between the NMS and the agent.
- View the MIB style of the agent to determine the MIB objects to be used.
- Save files **snmpset.exe** and **snmpwalk.exe** in Net-SNMP to directory C:\usr\bin, and manage the configuration file through MIB objects.
- The FTP protocol is used in this example; you need to run FTP server software on the FTP server, configure username and password, and set the value of 1.3.6.1.4.1.25506.2.4.1.2.4.1.3.4 to 1.
- If the TFTP protocol is used, you need to run TFTP server software on the TFTP server, and set the value of 1.3.6.1.4.1.25506.2.4.1.2.4.1.3.4 to 2.

Configuration Procedures

Configuration on the FTP Server

An H3C device is used as the FTP server in this example. Enable FTP server function on the device, and configure the FTP username as **ftp** and password as **123123123123**.

```
<System> system-view
[System] local-user ftp
[System-luser-ftp] password simple 123123123123
[System-luser-ftp] authorization-attribute level 3
[System-luser-ftp] service-type ftp
```

Configuration on the Agent

Configure the IP address of the agent as 192.168.1.40/24 and make sure that there is an available route between the agent and the NMS.

- If Ethernet 1/1 is a Layer 3 interface, perform the following configuration:

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] ip address 192.168.1.40 24
[Sysname-Ethernet1/1] quit
```

- If Ethernet 1/1 is a Layer 2 interface, perform the following configuration:

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] port Ethernet 1/1
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip address 192.168.1.40 24
[Sysname-Vlan-interface2] quit
```

Configure the SNMP version. To avoid the failure of establishing an SNMP connection between the agent and the NMS due to the problem of SNMP version, you are recommended to configure this keyword as **all**, which means SNMPv1, SNMPv2c and SNMPv3 are all supported.

```
<Sysname> system-view
[Sysname]snmp-agent sys-info version all
```

Set SNMP parameters: set the user name to **v3user**, authentication protocol to **MD5**, authentication password to **aaaaaaaaaa**, privacy protocol to **DES56**, and privacy password to **bbbbbbbbbb**.

- You can select whether to authenticate and encrypt the SNMP packets as needed. In this example, authentication with privacy is used.
- To make the configured authentication and privacy passwords valid after the system startup, you need to encrypt the plain text password, and then when you create the user, use the encrypted password in your configuration.

```
[Sysname] snmp-agent calculate-password aaaaaaaaaa mode md5 local-engineid
 The secret key is: 17CED5A1298DF35A643D81EC14E0E816
[Sysname] snmp-agent calculate-password bbbbbbbbbb mode md5 local-engineid
 The secret key is: 5D3250992503990147EEB03B04CF2190
[Sysname] snmp-agent group v3 test
[Sysname] snmp-agent usm-user v3 v3user test cipher authentication-mode md5
17CED5A1298DF35A643D81EC14E0E816 privacy-mode des56 5D3250992503990147EEB03B04CF2190
```

Configuration on the NMS

Refer to , and you need to replace **snmpset -v 1 -c private** in the configuration procedures with **snmpset -v 3 -a MD5 -A aaaaaaaaaa -u v3user -x DES -X bbbbbbbbbb**, and **snmpwalk -v 1 -c private** in the configuration procedures with **snmpwalk -v 3 -a MD5 -A aaaaaaaaaa -u v3user -x DES -X bbbbbbbbbb**.