Configuration guide

HP Network Simulator

Lab 1—Basic management system

Table of contents

Introduction

This configuration guide describes how to create, configure, and connect virtual HP Comware v7 devices using the HP Network Simulator (HNS) tool.

This guide will teach readers how to:

- Configure the management interface IP address
- Configure and test Telnet
- Configure and test TFTP client configuration

Background information

Comware v7 is a network operating system that runs on HP high-end network devices. The HNS is an ideal Comware v7 learning tool. With the HNS, users can create:

- Fixed form-factor and modular routers
- Stackable and modular switches
- LAN and WAN links

This lab assumes that HNS has been downloaded and installed according to the user guide provided with the download. Installation of the HNS tool is outside the scope of this document. This lab also assumes that the reader has read the HNS Basics and configuration examples provided in the user guide.

Requirements

The following hardware is required:

- A PC with:
  - CPU frequency: 3.0 GHz or more
  - Memory: 4 GB or more
  - Hard disk: 80 GB or more
  - Operating system: Windows® 7/8 or Ubuntu (32-bit or 64-bit)

The following software is required:

- HP Network Simulator
- Oracle VM VirtualBox release 4.2.18 or later

Note:

1. If running HNS on Windows, use the name “VirtualBox Host-Only Ethernet Adapter” for the VirtualBox Ethernet adapter.
2. If running HNS on Ubuntu, use the name “vboxnet0” for the VirtualBox Ethernet adapter.

Create

1. Copy paste the following within the HNS tool to create a switch.

```
#*********************************************************************
# Switch A
device_id = 1
# Device type: 32-bit centralized device
device_model = SIM2100
# Card model: SIM2101
board = SIM2101 : memory_size 1024
# Connect the Switch to the Virtual Box Ethernet adapter
device 1: interface 1 <--> host : "VirtualBox Host-Only Ethernet Adapter"
#*********************************************************************
```

2. Save and run the file.
3. A simulated switch will be created in VirtualBox Manager.
4. Start the switch.

Configure management interface

This section focuses on configuring the VirtualBox Ethernet adapter and simulated switch. The table below provides the IP parameters that should be used.

Table 1: Device parameters

	IP address	Mask length	Default gateway
Switch A	10.0.1.1	24	
VirtualBox Ethernet adapter	10.0.1.101	24	10.0.1.1

1. Assign an IP address to the switch management interface.

```
[switch] interface M-Ethernet 1/0/1
[switch-M-Ethernet1/0/1] ip address 10.0.1.1 24
```

Verify

1. Verify that the IP address has been assigned correctly.

```
[switch] display ip interface brief
*down: administratively down
(s): spoofing  (l): loopback
--------------------------------------------------------------------------
Interface      Physical     Protocol     IP Address      Description
M-E1/0/1         up             up         10.0.1.1           --
--------------------------------------------------------------------------
```

2. Further verify the configuration by pinging between the PC and virtual switch.
   A. On the PC use a command line window (cmd) in Windows or terminal in Ubuntu

```
ping 10.0.1.1
```

   B. On the Switch

```
[switch] ping 10.0.1.101
```

Troubleshoot

If the switch is unable to ping the PC, turn off the Windows firewall and repeat the ping to see if the issue is resolved.

Configure Telnet

This section focuses on configuring and securing Telnet access on the virtual switch.

By default, Telnet login is disabled on the device. To control Telnet access to the device, configure login authentication, and user privilege levels/roles for Telnet users.

The following are authentication modes available for controlling Telnet logins:

- None—Requires no authentication. This mode is insecure.
- Password—Requires a password for accessing the CLI. If your password was lost, log in to the device through the console port to re-set the password.
- Scheme—Uses the AAA module to provide local or remote authentication. You must provide a username and password for accessing the CLI. If the password configured in the local user database was lost, log in to the device through the console port and re-set the password. If the username or password configured on a remote server was lost, contact the server administrator for help.

Password

1. Enable Telnet globally on the switch

```
[switch] telnet server enable
```

2. Set the authentication mode and password for Telnet

```
[switch] user-interface vty 0 4
[switch-ui-vty0-4] authentication-mode password
[switch-ui-vty0-4] set authentication password simple pass
[switch-ui-vty0-4] user-role level-0
[switch-ui-vty0-4] quit
```

Verify

1. Verify that the authentication mode and password have been configured correctly.
   A. The column labeled Auth should have “P” listed, for password authentication.

```
[switch] display user-interface vty 0
Idx     Type     Tx/Rx     Modem     Auth     Int     Location
+ 84    VTY 0              —       P       —       1/0


  +    : Line is active.
  F    : Line is active and in async mode.
  Idx  : Absolute index of line.
  Type : Type and relative index of line.
  Auth : Login authentication mode.
  Int  : Physical port of the line.
  A    : Authentication use AAA.
  N    : No authentication is required.
  P    : Password authentication.
```

2. Further verify the configuration by telnetting from the PC to the switch.
   A. Open a terminal utility and Telnet to 10.0.1.1
   B. Once prompted by the switch, login by entering the password pass
   C. Logout of the Telnet session

```
<switch> quit
```

Note:
This lab was verified using the Putty Telnet/SSH client.

Super password

Super password allows for the Telnet user to switch to a higher user privilege level.

Note:
See Appendix A for more details on user roles.

1. Configure a super password `super`, in plain text.

```
[switch] super password role network-admin simple super
```

Verify

1. Verify that the role and password have been set properly

```
[switch] display user-interface vty 0
Idx     Type     Tx/Rx     Modem     Auth     Int     Location
+ 84    VTY 0               —       P       —       1/0

  +    : Line is active.
  F    : Line is active and in async mode.
  Idx  : Absolute index of line.
  Type : Type and relative index of line.
  Auth : Login authentication mode.
  Int  : Physical port of the line.
  A    : Authentication use AAA.
  N    : No authentication is required.
  P    : Password authentication.
```

2. Further verify the configuration by telnetting from the PC to the switch.
   A. Open a terminal utility and Telnet to 10.0.1.1
   B. Once prompted by the switch, login by entering the password pass
   C. Switch to “super” level

```
<switch> super
```

   D. Logout and close the Telnet session

```
<switch> quit
```

Local scheme authentication

Multiple authentication modes can be set to further secure Telnet connectivity. In the following example, scheme will be configured. With scheme, the device sends the username and password to a HWTACACS or RADIUS server for remote authentication or to the local user/password database stored in the switch. This lab uses the local scheme mode.

1. Configure the authentication mode on the simulated switch

```
[switch] user-interface vty 0 4
[switch-ui-vty0-4] authentication-mode scheme
[switch-ui-vty0-4] quit
```

2. Create a new user with the following requirements:

- username: level0
- password: 12345
- user level: 0

```
[switch] local-user level0
  New local user added
[switch-luser-level0] service-type telnet
```

```
[switch-luser-level0] authorization-attribute user-role level-0
[switch-luser-level0] password simple 12345
[switch-luser-level0] quit
```

3. Create a second user with:

- username: level3
- password: 12345
- user level: 3

```
[switch] local-user level3
  New local user added
[switch-luser-level3] service-type telnet
[switch-luser-level3] authorization-attribute user-role network-admin
[switch-luser-level3] password simple 12345
[switch-luser-level3] quit
```

Verify

1. Verify the configuration by telnetting from the PC to the switch.
   A. Open a terminal utility and Telnet to 10.0.1.1
2. When prompted, login as user level3
   A. username: level3
   B. password: 12345
3. Logout and close the Telnet session

```
<switch> quit
```

4. Telnet again to 10.0.1.1
5. Login as user level0
   A. username: level0
   B. password: 12345
6. Switch to “super” level

```
<switch> super
```

7. Logout and close the Telnet session

```
<switch> quit
```

Configure TFTP client

The TFTP client feature allows for files, such as configuration files or firmware, to be uploaded from the device to a TFTP server, or downloaded from the TFTP server to the device.

In order to verify that the TFTP client feature is configured correctly, steps to create a file on the virtual switch are provided below.

1. Generate and save the diagnostics file.
   A. Press enter when asked to input the file name and the default file name will be used.

```
<switch> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:y
Please input the file name(*.gz)[flash:/diag.gz]:
Diagnostic information is outputting to flash:/diag.gz.
Please wait...
Save successfully.
<switch> quit
```

2. Ensure that the TFTP server is enabled.
3. Configure the TFTP Server to store the received file on the desktop.

Note:
It is assumed that readers have a TFTP server installed on their PC. Downloading, installing, and configuring the TFTP server is outside the scope of this document.

---

4. Copy the diagnostics file to the PC using TFTP

```
<switch> tftp 10.0.1.101 put flash:/diag.gz
```

Verify

1. From the TFTP server window, ensure the transmission finished successfully.
2. On the PC, navigate to the folder containing the diag.gz file, unzip the file, and open it using WordPad.
3. Ensure that the file contains the appropriate information.

Appendix A: Predefined user roles and permissions matrix

The system provides 18 predefined user roles. All these user roles have access to all system resources (interfaces, VLANs, and VPNs), but their command access permissions differ.

Among all the predefined user roles, only the network-admin and level-15 user roles can access the RBAC feature and change the settings including user-role, authentication-mode, protocol, and set authentication password in user interface view.

Among all the predefined user roles, level-0 to level-14 users can modify their own permissions for any commands except for the display history-command all command.

Table 2. Permissions matrix

User role name	Permissions
network-admin	Accesses all features and resources in the system.
network-operator	Accesses the display commands (except display history-command all) for all features and resources in the system.
level-n (n = 0 to 15)	• Level-0—Has access to the commands of ping. `Tracert, ssh, telnet, and super`. Level-0 access rights are configurable. • Level-1—Has access to the display commands (except display history-command all) of all features and resources in the system, in addition to all access rights of the user role level-0. Level-1 access rights are configurable. • Level-2 to level-8, and level-10 to level-14—Have no access rights by default. Access rights are configurable. • Level-9—Has access to all features and resources except RBAC, local users, file management, device management, and the display history-command all command. If you are logged in with a local user account that has a level-9 user role, you can change the password in the local user account. Level-9 access rights are configurable. • Level-15—Has the same access rights as the role network-admin. Commands described as accessible to network-admin are also accessible to the Level-15 user role.

Additional links

End User License Agreement

HNS configurations are similar to those of the HP 5900 Switch Series. See the HP 5900 Switch Series manuals for configuration guidance.

Learn more at
hp.com/networking/hns

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA5-5630ENW, November 2014