ZebOS-XP®
Network Platform

Version 1.4
Extended Performance

System Management
Configuration Guide

December 2015

IP Infusion Inc.
3965 Freedom Circle, Suite 200
Santa Clara, CA 95054
+1 408-400-1900
http://www.ipinfusion.com/

For support, questions, or comments via E-mail, contact:
support@ipinfusion.com

Contents

Preface

This guide describes how to use ZebOS-XP to configure network services in the Linux operating system.

Audience

This guide is intended for network administrators and other engineering professionals who configure network services in the Linux operating system.

Conventions

Table P-1 shows the conventions used in this guide.

Table P-1: Conventions

Convention	Description
Italics	Emphasized terms; titles of books
Note:	Special instructions, suggestions, or warnings
`monospaced type`	Code elements such as commands, functions, parameters, files, and directories

Contents

This guide contains these chapters:

- Chapter 1, *TACACS Server Host Configuration*
- Chapter 2, *User Configuration*
- Chapter 3, *RADIUS Server Host Configuration*
- Chapter 4, *SSH Client Server Host Configuration*
- Chapter 5, *Syslog Configuration*
- Chapter 6, *DNS Client Configuration*
- Chapter 7, *DHCP Client Configuration*
- Chapter 8, *DHCP Relay Agent Configuration*
- Chapter 9, *NTP Client Configuration*

Related Documents

Use this guide with the *System Management Command Reference* for details about the commands used in the configurations.

Note: All ZebOS-XP technical manuals are available to licensed customers at http://www.ipinfusion.com/support/document_list.

Chapter Organization

The chapters in this guide are organized into these major sections:

- An overview that explains a configuration in words
- Topology with a diagram that shows the devices and connections used in the configuration
- Configuration steps in a table for each device where the left-hand side shows the commands you enter and the right-hand side explains the actions that the commands perform
- Validation which shows commands and their output that verify the configuration

Support

For support-related questions, contact support@ipinfusion.com.

Comments

If you have comments, or need to report a problem with the content, contact techpubs@ipinfusion.com.

CHAPTER 1 TACACS Server Host Configuration

Overview

This chapter explains the concept of TACACS Server Host Configuration. Terminal Access Controller Access Control System (TACACS) is a remote authentication protocol that is used to communicate with an authentication server commonly used in UNIX networks. With TACACS, a network device communicates to an authentication server to determine whether a particular user should be allowed access to the device.

The TACACS+ protocol is the latest generation of TACACS. TACACS+ uses TCP for its transport. The daemon should listen at port 49 which is the "LOGIN" port assigned for the TACACS protocol. This port is reserved in the assigned numbers RFC for both UDP and TCP. Current TACACS and extended TACACS implementations use port 49.

The TACACS package should be installed in the Server machine. After installation, make server related config and run the TACACS server. There can be multiple TACACS server connected to DUT. The DUT is know to be TACACS client.

TACACS Server Authentication

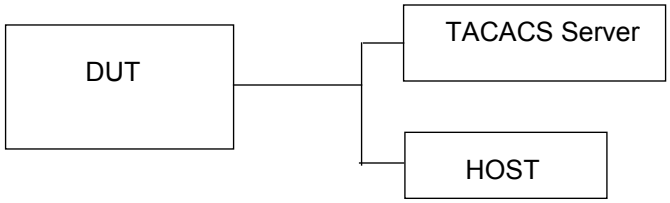

Figure 1-1: TACACS Server Host Configuration

DUT

`#configure terminal`	Enter Configure mode.
`(config)#feature tacacs+`	Enable the feature tacacs+.
`(config)# tacacs-server host 10.16.19.2 key testing`	Specify the tacacs server ipv4 address to be configured with shared key. The same key should be present on the server config file.
`(config)#aaa authentication login default group tacacs+`	Enable authentication for tacacs server configured.
`(config)#username-remote test password test12345`	Create username and password for authentication purpose. The same user should be present in the tacacs server config file.

To verify TACACS authentication process, do ssh or telnet form host machine to DUT IP with the user created and provide tacacs server password and check whether the client validates the user with corresponding username and password and enters into imish via tacacs authentication.

Validation Commands

`show tacacs-server, show running-config aaa, show running-config tacacs+`

TACACS Server Accounting

Following authentication user can configure accounting to measure the resources a user consumes during access.

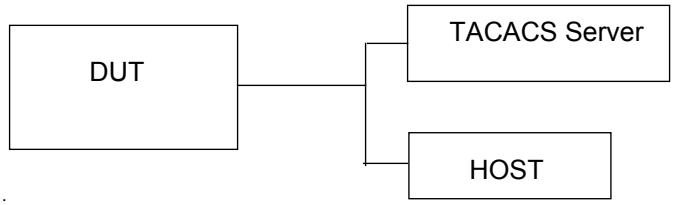

Figure 1-2: TACACS Server Host Configuration

DUT

`#configure terminal`	Enter Configure mode.
`(config)#feature tacacs+`	Enable the feature tacacs+.
`(config)# tacacs-server host 10.16.19.2 key testing`	Specify the tacacs server ipv4 address to be configured with shared key. The same key should be present on the server config file.
`(config)#aaa accounting login default group tacacs+`	Enable accounting for tacacs server configured.
`(config)#username-remote test password test12345`	Create username and password for accounting purpose. The same user should be present in the tacacs server config file.

To verify TACACS accounting process, do ssh or telnet form host machine to DUT IP with the user created and provide tacacs server password and check whether the client validates the user with corresponding username and password and enters into imish via tacacs accounting.

Validation Commands

`show tacacs-server, show running-config aaa, show running-config tacacs+`

CHAPTER 2 User Configuration

Overview

The following configuration helps you to create a user.

User Configuration

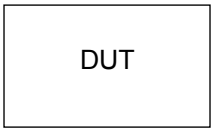

Figure 2-1: User Configuration

DUT

`#configure terminal`	Enter configure mode.
`(config)#username-remote fred_smith password encrypted W3g7y&6yV}JH6&5EYIah?779IT9iV2`	Enter a user name and encrypted password.

Validation Commands

```
show user-account
```

CHAPTER 3 RADIUS Server Host Configuration

Overview

Remote Authentication Dial In User Service (RADIUS) is a remote authentication protocol that is used to communicate with an authentication server commonly used in UNIX networks.

A RADIUS Client-Server Model is used like – the RADIUS server is responsible for getting user connection requests, authenticating the user and then returning all configuration information necessary for the client to deliver service to the user.

The key points for RADIUS authentication are:

Transactions between client and server are authenticated through the use of a shared key and this key is never sent over the network.

Password is encrypted before sending it over network.

RADIUS Server Authentication

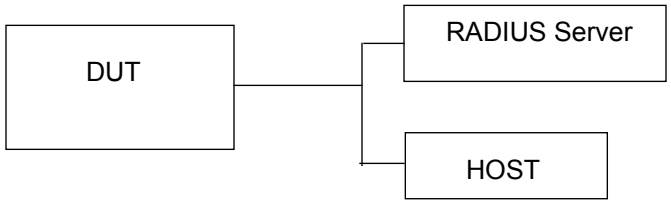

Figure 3-1: RADIUS Server Host Configuration

DUT

`#configure terminal`	Enter Configure mode.
`(config)# radius-server host 10.16.19.2 key testing`	Specify the radius server ipv4 address to be configured with shared key. The same key should be present on the server config file.
`(config)#aaa authentication login default group radius`	Enable authentication for radius server configured.
`(config)#username-remote test password test12345`	Create username and password for authentication purpose. The same user should be present in the radius server config file.

To verify radius authentication process, do ssh or telnet form host machine to DUT IP with the user created and provide radius server password and check whether the client validates the user with corresponding username and password and enters into imish via radius authentication.

Validation Commands

`show radius-server, show running-config aaa, show running-config radius`

RADIUS Server Accounting

Following authentication user can configure accounting to measure the resources a user consumes during access.

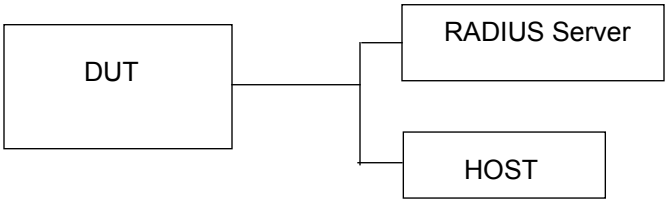

Figure 3-2: RADIUS Server Host Configuration

DUT

`#configure terminal`	Enter Configure mode.
`(config)# radius-server host 10.16.19.2 key testing`	Specify the radius server ipv4 address to be configured with shared key. The same key should be present on the server config file.
`(config)#aaa accounting login default group radius`	Enable accounting for radius server configured.
`(config)#username-remote test password test12345`	Create username and password for accounting purpose. The same user should be present in the radius server config file.

To verify radius accounting process, do ssh or telnet form host machine to DUT IP with the user created and provide radius server password and check whether the client validates the user with corresponding username and password and enters into imish via radius accounting.

Validation Commands

`show radius-server, show running-config aaa, show running-config radius`

CHAPTER 4 SSH Client Server Host Configuration

Overview

SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices.SSH was designed as a replacement for Telnet and other insecure remote shells, which send information, notably passwords, in plaintext, rendering them susceptible to packet analysis.[2] The encryption used by SSH is intended to provide confidentiality and integrity of data over an unsecured network, such as the Internet.SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user.

SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding TCP ports and X11 connections; it can transfer files using the associated SFTP or SCP protocols. SSH uses the client-server model

The standard TCP port 22 has been assigned for contacting SSH servers. Here in this document covering the ssh server configuration to enable ssh service and key generation CLI commands and ssh client configuration for remote login to server.

SSH Login Attempts

The ssh is enabled by default..

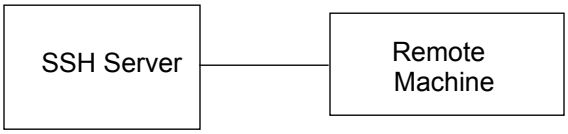

Figure 4-1: SSH Server Host Configuration

SSH Server

`#configure terminal`	Enter Configure mode.
`(config)#no feature ssh`	Disable the feature ssh.
`(config)# ssh login-attempts 5`	Set Login-attempts 5. Default is 3.
`(config)#feature ssh`	Enable the feature ssh.
`(config)#exit`	Exit from the configuration mode.

The login-attempt is set to 5 which means that the five times the password can be re-entered. The feature ssh should be disabled while configuring the login-attempts and it should be enabled before creating the SSH session.

Validation Commands

`show ssh server, show running-config ssh server`

SSH Keys

Use this ssh keys to generates new RSA/DSA keys for SSH server. This command can only be executed when the SSH server is disabled. By default the system has RSA/DSA public/private key pair placed in /etc/ssh/. If the user wants to regenerate the keys the force option must be specified. The length option can only be used with RSA keys; DSA has a constant key length of 1024bits.

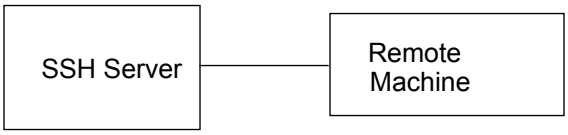

Figure 4-2: SSH Server Host Configuration

SSH Server

`#configure terminal`	Enter Configure mode.
`(config)#no feature ssh`	Disable the feature ssh.
`(config)# ssh key rsa force`	The force option is used if the user wants to regenerate the ssh rsa keys. The same thing applies for dsa also.
`(config)#feature ssh`	Enable the feature ssh.
`(config)#exit`	Exit from the configuration mode.

Validation Commands

`show ssh key`

Note: The newly created rsa/dsa key can be verified by logging into DUT from remote machine and checking whether the newly created key's fingerprint matches with the logging session fingerprint.

SSH Client session

When DUT acting as ssh client supports both ssh ipv4 and ipv6 sessions to login to remote machine.

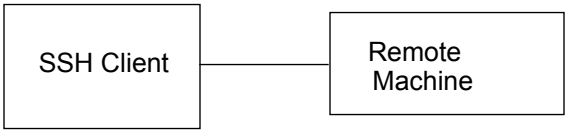

Figure 4-3: SSH Server Host Configuration

SSH Client

`#ssh root@10.10.10.1`	Logging into remote machine using ipv4 address.
`#ssh6 root@3ffe::1`	Logging into remote machine using ipv6 address.

CHAPTER 5 Syslog Configuration

Overview

Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It also provides devices which would otherwise be unable to communicate, a means to notify administrators of problems or performance.

ZebOS-XP supports logging messages to a syslog server in addition to logging to a file or the console (local or ssh/ telnet console). ZebOS-XP messages can either be logged to local syslog server (the machine on which ZebOS-XP executes) or to one more more remote syslog servers. Remote syslog servers can either be configured as IP addresses (IPv4 IPv6) or hostname.

Logging to a File

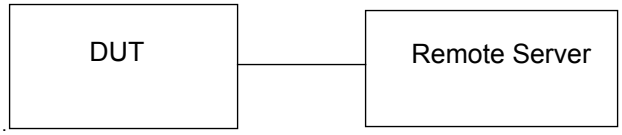

Figure 5-1: Syslog Configuration

DUT

`#configure terminal`	Enter Configure mode.
`(config)# logging level hostp 7`	This enable debug messages for hostp module.
`(config)#logging logfile xyz 7`	This creates the log file where the logs will be saved. The path of the file will be in the directory /log/xyz.txt
`(config)#debug radius`	This enables the debugging on radius-client configurations.
`(config)#radius-server host 10.10.10.1`	This adds the radius server host.
`(config)#exit`	Exit from the configuration mode.

To verify this, do some radius configuration and view the messages in the log file or with the `show logging logfile` command.

Validation Commands

`show logging logfile, show logging level`

Logging to the Console

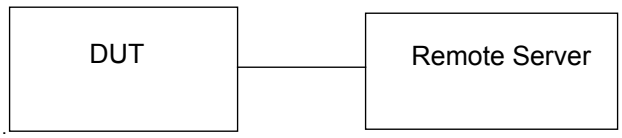

Figure 5-2: Syslog Configuration

DUT

`#configure terminal`	Enter Configure mode.
`(config)# logging level hostp 7`	This enable debug messages for hostp module.
`(config)#debug radius`	This enables the debugging on radius-client configurations.
`(config)#logging console 7`	This enables the console logs.
`(config)#radius-server host 10.10.10.1`	This adds the radius server host.
`(config)#exit`	Exit from the configuration mode.

To verify this, do some radius configuration and view the messages in the console.

Validation Commands

`show logging console, show logging level`

Logging to a Server

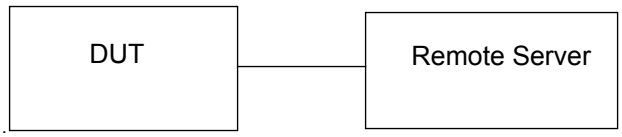

Figure 5-3: Syslog Configuration

DUT

`#configure terminal`	Enter Configure mode.
`(config)# logging level hostp 7`	This enable debug messages for hostp module.
`(config)#debug radius`	This enables the debugging on radius-client configurations.
`(config)#logging server 10.16.2.1`	Redirects the log messages to the server configured.
`(config)#radius-server host 10.10.10.1`	This adds the radius server host.
`(config)#exit`	Exit from the configuration mode.

Validation Commands

`show logging server, show logging level`

CHAPTER 6 DNS Client Configuration

Overview

The DHCP Relay feature was designed to forward DHCP broadcast requests as unicast packets to a configured DHCP server or servers for redundancy.

DHCP Relay for IPv4

Before configuring DHCP Relay, make sure DHCP server and client configurations are done, and dhclient and dhcpd is running in client and server respectively.

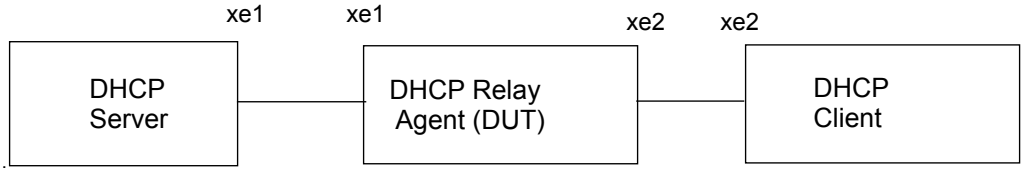

Figure 6-1: DHCP Relay Configuration

DUT

`#configure terminal`	Enter Configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This is enabled by default.
`(config)#ip dhcp relay`	By default this will be enabled. It starts the ip dhcp relay service.
`(config)#interface xe1`	Specify the interface(xe1) to be configured and enter the interface mode.
`(config-if)#ip address 10.10.10.1/24`	Configure ipv4 address on the interface xe1.
`(config if)#exit`	Exit from the interface mode.
`(config)#interface xe2`	Specify the interface(xe2) to be configured and enter the interface mode.
`(config-if)#ip address 20.20.20.1/24`	Configure ipv4 address on the interface xe2.
`(config-if)#ip dhcp relay address 10.10.10.2`	The relay address configured should be server interface address connected to DUT machine.
`(config if)#exit`	Exit from the interface mode.

Validation Commands

`show running-config dhcp, show ip dhcp relay, show ip dhcp relay address, show ip dhcp relay address interface INTERFACE`

DHCP Relay for IPv6

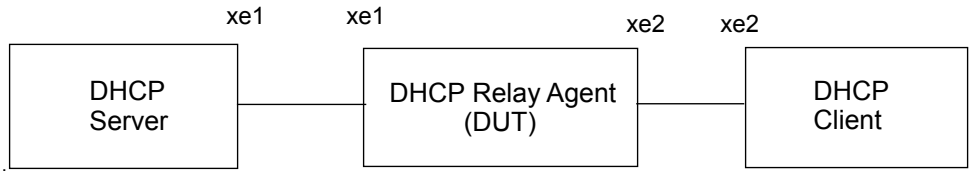

Figure 6-2: DHCP Relay Configuration

DUT

`#configure terminal`	Enter Configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This is enabled in default.
`(config)#ipv6 dhcp relay`	By default this will be enabled. It starts the ipv6 dhcp relay service.
`(config)#interface xe1`	Specify the interface(xe1) to be configured and enter the interface mode.
`(config-if)#ipv6 address 2001::1/64`	Configure ipv6 address on the interface xe1.
`(config if)#exit`	Exit from the interface mode.
`(config)#interface xe2`	Specify the interface(xe2) to be configured and enter the interface mode.
`(config-if)#ipv6 address 2002::1/64`	Configure ipv6 address on the interface xe2.
`(config-if)#ipv6 dhcp relay address 2001::2`	The relay address configured should be server interface address connected to DUT machine.
`(config if)#exit`	Exit from the interface mode.

Validation Commands

`show running-config dhcp, show ipv6 dhcp relay, show ipv6 dhcp relay address, show ipv6 dhcp relay address interface INTERFACE`

CHAPTER 7 DHCP Client Configuration

Overview

Dynamic Host Configuration Protocol (DHCP) protocol is used for assigning dynamic IP addresses to systems on a network. Dynamic addressing allows a system to have an IP address each time it connects to the network. DHCP makes network administration easier by removing the need to manually assign a unique IP address every time a new system is added to the network. It is especially useful to manage mobile users. Once a system is configured to use DHCP, it can be automatically configured on any network that has a DHCP server.

DHCP uses a client-server model, in which the DHCP server centrally manages the IP addresses used in the network. DHCP clients obtain an IP address on lease from the DHCP server.

DHCP Client Configuration for IPv4

Before Configuring DHCP in client (DUT), make sure that DHCP server is ready and also dhcpd is running on the server machine.

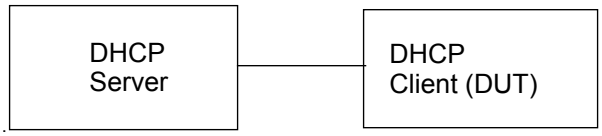

Figure 7-1: DHCP Client Configuration

DUT

`#configure terminal`	Enter Configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This will be enabled by default.
`(config)#interface xe1`	Specify the interface(xe1) to be configured and enter the interface mode.
`(config-if)#ip address dhcp`	The client requests for the IP address to the server, once it receives the Acknowledgement from the server, it assigns the IP address to the interface in which this command is enabled.
`(config if)#exit`	Exit from the interface mode.

Validation Commands

`show running-config dhcp, show ip interface brief`

DHCP Client Configuration for IPv6

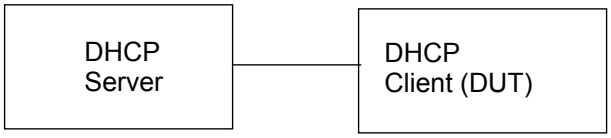

Figure 7-2: DHCP Client Configuration

DUT

`#configure terminal`	Enter Configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This will be enabled by default
`(config)#interface xe1`	Specify the interface(xe1) to be configured and enter the interface mode.
`(config-if)#ipv6 address dhcp`	The client requests for the IPv6 address to the server, once it receives the Acknowledgement from the server, it assigns the IPv6 address to the interface in which this command is enabled.
`(config if)#exit`	Exit from the interface mode.

Validation Commands

`show running-config dhcp, show ipv6 interface brief`

CHAPTER 8 DHCP Relay Agent Configuration

Overview

The DHCP Relay feature was designed to forward DHCP broadcast requests as unicast packets to a configured DHCP server or servers for redundancy.

DHCP Relay for IPv4

Before configuring DHCP Relay, make sure DHCP server and client configurations are done, and dhclient and dhcpd is running in client and server respectively.

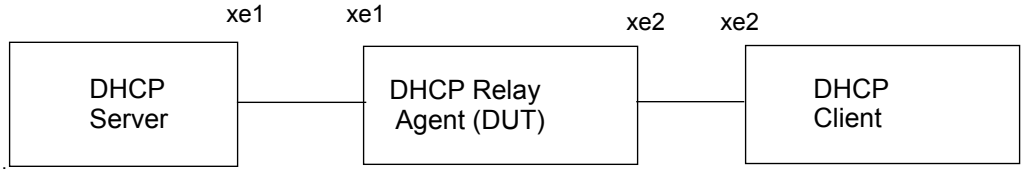

Figure 8-1: DHCP Relay Configuration

DUT

`#configure terminal`	Enter Configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This is enabled by default.
`(config)#ip dhcp relay`	By default this will be enabled. It starts the ip dhcp relay service.
`(config)#interface xe1`	Specify the interface(xe1) to be configured and enter the interface mode.
`(config-if)#ip address 10.10.10.1/24`	Configure ipv4 address on the interface xe1.
`(config if)#exit`	Exit from the interface mode.
`(config)#interface xe2`	Specify the interface(xe2) to be configured and enter the interface mode.
`(config-if)#ip address 20.20.20.1/24`	Configure ipv4 address on the interface xe2.
`(config-if)#ip dhcp relay address 10.10.10.2`	The relay address configured should be server interface address connected to DUT machine.
`(config if)#exit`	Exit from the interface mode.

Validation Commands

`show running-config dhcp, show ip dhcp relay, show ip dhcp relay address, show ip dhcp relay address interface INTERFACE`

DHCP Relay for IPv6

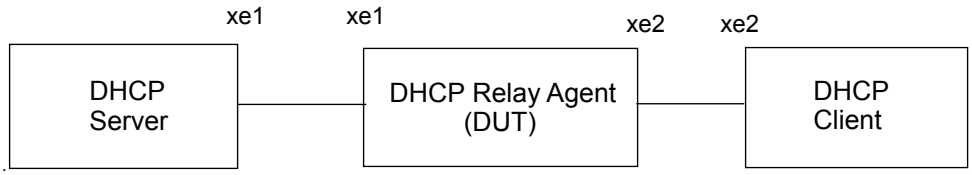

Figure 8-2: DHCP Relay Configuration

DUT

`#configure terminal`	Enter Configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This is enabled in default.
`(config)#ipv6 dhcp relay`	By default this will be enabled. It starts the ipv6 dhcp relay service.
`(config)#interface xe1`	Specify the interface(xe1) to be configured and enter the interface mode.
`(config-if)#ipv6 address 2001::1/64`	Configure ipv6 address on the interface xe1.
`(config if)#exit`	Exit from the interface mode.
`(config)#interface xe2`	Specify the interface(xe2) to be configured and enter the interface mode.
`(config-if)#ipv6 address 2002::1/64`	Configure ipv6 address on the interface xe2.
`(config-if)#ipv6 dhcp relay address 2001::2`	The relay address configured should be server interface address connected to DUT machine.
`(config if)#exit`	Exit from the interface mode.

Validation Commands

`show running-config dhcp, show ipv6 dhcp relay, show ipv6 dhcp relay address, show ipv6 dhcp relay address interface INTERFACE`

CHAPTER 9 NTP Client Configuration

Overview

Time is inherently important to the function of routers and networks. It provides the only frame of reference between all devices on the network. This makes synchronized time extremely important. Without synchronized time, accurately correlating information between devices becomes difficult, if not impossible. When it comes to security, if you cannot successfully compare logs between each of your routers and all your network servers, you will find it very hard to develop a reliable picture of an incident.

NTP modes differ based on how NTP allows communication between systems. NTP communication consists of time requests and control queries. Time requests provide the standard client/server relationship in which a client requests time synchronization from an NTP server. Control queries provide ways for remote systems to get configuration information and reconfigure NTP servers.

SNTP is a simplified form of NTP that does not reach the level of accuracy compared to a full implementation of NTP. SNTP can be used for simple applications where the requirements for accuracy and reliability are not too demanding. ZebOS-XP supports SNTP version 4 defined in RFC 2030.

Note: ZebOS-XP uses “ntp” for the SNTP command names instead of “sntp”.

NTP Modes

Client

An NTP client is configured to let its clock be set and synchronized by an external NTP timeserver. NTP clients can be configured to use multiple servers to set their local time and are able to give preference to the most accurate time sources. They do not, however, provide synchronization services to any other devices.

Server

An NTP server is configured to synchronize NTP clients. Servers can be configured to synchronize any client or only specific clients. NTP servers, however, will accept no synchronization information from their clients and therefore will not let clients update or affect the server's time settings.

Peer

With NTP peers, one NTP-enabled device does not have authority over the other. With the peering model, each device shares its time information with the other, and each device can also provide time synchronization to the other.

Access Lists

Once a router is synchronized to an NTP time source, it automatically acts as an NTP for any client that requests synchronization or informational control queries.

NTP allows you to configure ACLs to restrict access to the NTP services on the router. These ACLs can be configured to restrict access based on IP and the following four restrictions:

Peer

Allows time synchronization requests and control queries and allows the router to synchronize itself to remote systems that pass the ACL

Server

Allows time synchronization requests and control queries, but does not allow the router to synchronize itself to remote systems that pass the ACL

Serve-only

Allows only time synchronization requests from systems that pass the ACL

Query-only

Allows only NTP control queries from systems that pass the ACL

The two ACLs generally used to restrict access for security reasons are the *peer* and *serve-only* options--for example, if you are using the hierarchical model with the core routers *RouterOne* and *RouterTwo*providing NTP services for the rest of the routers in your network.

Authentication

For additional security, you can configure your NTP servers and clients to use authentication. DUT routers support MD5 authentication for NTP. To enable a router to do NTP authentication:

Enable NTP authentication with the *ntp authenticate* command.

Define an NTP authentication key with the *ntp authentication-key* command. A unique number identifies each NTP key. This number is the first argument to the *ntp authentication-key* command.

Use the *ntp trusted-key* command to tell the router which keys are valid for authentication. If a key is trusted, this system will be ready to synchronize to a system that uses this key in its NTP packets. Trusted key should be a already configured authentication key.

NTP Configuration

The DUT acts as a NTP client, user can configure an association with a remote server, in this mode the client clock can synchronize to the remote server

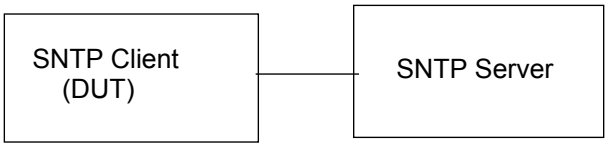

Figure 9-1: SNTP Configuration

DUT

`#configure terminal`	Enter Configure mode.
`(config)# ntp enable`	This feature enables ntp. This will be enabled in default.
`(config)#ntp server 10.10.10.1`	Configure ntp server ip address.
`(config)#exit`	Exit from the Configure Mode.

After configuring ntp servers, few minutes later verify that clock synchronisation is successful. When the clock synchronisation is actually happened, there will be '*' symbol along with the interface while you give the "show ntp peers" command.

Validation Commands

`show ntp peers, show ntp peer-status`

Maxpoll and Minpoll Configuration

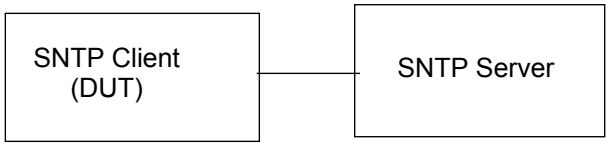

Figure 9-2: Maxpoll and Minpoll Configuration

DUT

`#configure terminal`	Enter Configure mode.
`(config)# ntp enable`	This feature enables ntp. This will be enabled in default.
`(config)#ntp server 10.10.10.1 maxpoll 6 minpoll 4`	Configure minpoll and maxpoll range for ntp server.
`(config)#exit`	Exit from the Configure Mode.

The maximum poll interval are specified in defaults to 6 (64 s), but can be increased by the maxpoll option to an upper limit of 16 (18.2 h). The minimum poll interval defaults to 4 (16 s), and this is also the minimum value of the minpoll option.

The client will retry between minpoll and maxpoll range configured for synchronisation with the server.

Validation Commands

`show ntp peers, show ntp peer-status`

NTP Authentication

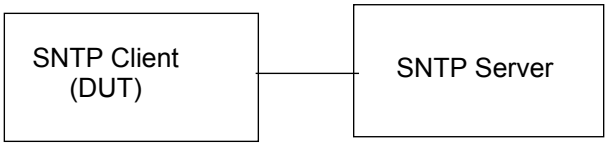

Figure 9-3: NTP Authentication

DUT

`#configure terminal`	Enter Configure mode.
`(config)# ntp enable`	This feature enables ntp. This will be enabled in default.
`(config)#ntp server 10.10.10.1`	Configure ntp server ip address.
`(config)#ntp authenticate`	Enable NTP Authenticate. NTP authentication is disabled by default.
`(config)#ntp authentication-key 14 md5 PASS`	Configure ntp authentication key along with md5 value.
`(config)#exit`	Exit from the Configure Mode.

When you enable NTP authentication, the device synchronizes to a time source only if the source carries the authentication keys specified with the source by key identifier. The device drops any packets that fail the authentication check and prevents them from updating the local clock.

Validation Commands

`show ntp authentication-status, show ntp authentication-keys`

Index